Utrecht University

Departement of Mathematics

Master Thesis

Analogies between the BSD Conjecture and the Analytic Class Number Formula

Author:
Dylan Feenstra

To fulfill the requirements for the degree of Master of Science in Mathematical Sciences at Utrecht University.

Supervisor:
Prof. Dr. G.L.M. Cornelissen
Utrecht University

Second Reader:
Dr. V.Z. Karemaker
Utrecht University

July 15, 2022

Abstract

One of the central objects in number theory are the so-called L-series. For instance, on $\mathbb{Q}$ we have the famous Riemann zeta function. This function has a generalization to an arbitrary number field K, often denoted as $\zeta_K(s)$, which is called the Dedekind zeta function. This function has an analytic continuation to the entire complex plane with a simple pole at $s = 1$. Its residue at $s = 1$ involves many of the basic invariants of the number field. For instance the regulator, the class group, the finite torsion subgroup of the ring of integers, and the discriminant of the number field appear in the residue. In other words, this function encodes a lot of fundamental information about the number field.

The L-series of an elliptic curve defined over a number field is the analogue of the Dedekind zeta function for a number field. Both series can be defined by an Euler product, i.e., a product indexed by the primes, on a part of the complex plane. It is conjectured that this function also has an analytic continuation to the entire complex plane. It is moreover conjectured by Bryan John Birch and Peter Swinnerton-Dyer that it has a zero of order equal to the rank of the elliptic curve at $s = 1$. The first non-zero coefficient of the corresponding Taylor expansion at $s = 1$ is conjectured to consist of multiple basic invariants concerning the set of global points on the elliptic curve, in particular the regulator, the Tate-Shafarevich group, the torsion subgroup of the global points, and the period of the elliptic curve.

In this thesis we will provide the required theory for understanding the two formulae, and to obtain as many similarities as possible between them. The obtained analogies could function as a helping hand for a better understanding of the BSD conjecture.

Acknowledgements

In writing this thesis, I have attempted to present the required theory for understanding the mathematical invariants appearing in the BSD conjecture and the analytic class number formula. Moreover, I wanted to make an accessible source for comparing both formulae, whose comparison up to now has been widely scattered. During this process, I have consulted many great sources for which I want to acknowledge my gratitude to the authors.

I want to show my sincere gratitude and appreciation to Prof. Dr. G.L.M Cornelissen for introducing me to this wonderful remarkable bridge between the world of elliptic curves and number fields. I moreover would like to thank him for his guidance and encouraging words during writing this thesis. The educative and companionable bi-weekly meetings gave me a comfortable feeling in finishing this thesis, for which I am truly grateful. Furthermore, I would like to thank Dr. V. Karemaker for proofreading my work as a second examiner.

Finally, I would like to thank my parents and sister for creating a warm environment in which I felt the moral support in writing this thesis. There are no words to express my gratitude for the continuous support and the possibilities my parents have given me.

Contents

Introduction **vii**

1 Basic Algebraic Number Theory **1**

1.1 Archimedean and non-Archimedean Places on a Field 1

1.2 Topology Induced by Absolute Value 4

1.3 Valuations 7

1.4 Completions 10

1.5 Lattices 14

1.6 Arithmetic on Number Fields 15

1.7 Ideal Factorization on Extensions of Dedekind Domains. 23

2 Adele Rings And Idele Groups **26**

2.1 Final Topology 26

2.2 Restricted Direct Product 28

2.3 Adele Rings and Idele Groups 32

2.4 Tamagawa Measure 36

3 Galois Cohomology **40**

3.1 Field Extensions 40

3.2 Galois Theory 44

3.3 Basic Group Cohomology 49

3.4 Cohomology for Profinite Groups 52

4 L-series and the BSD conjecture **55**

4.1 Reduction of Elliptic Curves 55

4.2 L-Series 59

4.3 The Regulator of an Elliptic Curve 61

4.4 The Tate-Shafarevich Group of an Elliptic Curve 65

4.5 The Period of an Elliptic Curve 69

5 Classical Analytic Class Number Formula **73**

5.1 The Dedekind Zeta Function 74

5.2 The Regulator of a Number Field 76

5.3 The Tate-Shafarevich Group of a Number Field 78

5.4 The Period of a Number Field 84

Discussion **88**

Appendix A Haar Measures **91**

A.1 Quotient Space 92

A.2 Restricted Direct Product 92

Index **98**

Introduction

When an equation is given, one of the primal instincts of many mathematicians is wondering what the solutions are. One of the many examples of this is the well-known Fermat's Last Theorem, which states that any equation of the form

$$x^n + y^n = z^n \text{ for } n > 2,$$

has no non-trivial solutions with $x, y, z \in \mathbb{Z}_{\geq 1}$. This was formulated as a conjecture by Fermat in the 17th century, and after multiple generations of mathematicians it has been successfully proven by Andrew Wiles in 1994.

Another example of finding solutions of a given equation, are the broadly studied elliptic curves. Every elliptic curve defined over a number field K can be given by a Weierstrass equation, which is an equation of the form

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$, together with a point at infinity O_E. One of the central objects of an arbitrary elliptic curve E is their corresponding set of K-rational points, denoted by $E(K)$, which in fact admits a group structure. This group is also called the Mordell-Weil group, which comes together with the natural question whether it is computable or not. Until now there is no general method known for computing this group. However, more is known about its abstract structure. Namely, the group $E(K)$ is finitely generated. This result was obtained by Mordell and Weil, and in particular tells us that $E(K)$ has the form

$$E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^{r_E},$$

where the torsion subgroup is finite and the rank r_E of $E(K)$ a non-negative integer. The difficult part that remains is finding the rank.

One method commonly used to study the solutions to a given equation, is to find solutions modulo primes. In this way the possibilities are restricted to finitely many, making it into a trial and error process. During the first half of the 1960s, at the time when computers were booming, Peter Swinnerton-Dyer was interested in determining the solutions of an elliptic curve when considered modulo a prime. He used a computer for this, in the hope to find remarkable patterns. Birch eventually noticed an interesting pattern in the data obtained by Swinnerton-Dyer. For this he considered the number of solutions found modulo a prime and divided this by the concerned prime. After multiplying the obtained fractions up to a fixed prime, he recognized a certain asymptotic behaviour. Namely, he observed that

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \log(x)^r \text{ for } x \to \infty,$$

where N_p is the number of rational points on the considered elliptic curve E defined over a field of p elements. Moreover, C is a constant depending on E and r the rank of the considered elliptic curve. This rank was known for the curves considered by Birch and Swinnerton-Dyer.

This formula eventually led to an even more detailed conjecture about the behaviour of the L-series of a given elliptic curve E defined over a number field K at $s = 1$.

Such an L-series, often denoted as $L(E, s)$, is a function defined on a part of the complex plane, and encodes a lot of information about the reduction of the curve modulo every prime. The theory about L-series plays an important role in analytic number theory, despite the fact that it is still largely conjectural. Generally, it is not even known that the function is defined at $s = 1$, but only for $\mathrm{Re}(s) > 3/2$. Nevertheless, it has been proven for curves with complex multiplication and curves over $\mathbb{Q}$ that it has an analytic continuation to the entire complex plane. This property has been conjecturally generalized to arbitrary elliptic curves defined over a number field K.

Based on this generalization, the modern formulation of the BSD conjecture is given by:

BSD conjecture 0.0.1. (cf. [Groty, Conj.2.10]) *Let E/K be an elliptic curve over a number field K, and assume that $L(E, s)$ has an analytic continuation to the entire complex plane.*

(i) If r_E is the rank of the finitely generated abelian group $E(K)$, then

$$ord_{s=1}L(E, s) = r_E.$$

(ii) Assume that the Tate-Shafarevich group $Ш(E/K)$ is finite, then

$$\lim_{s\to 1} \frac{L(E, s)}{(s-1)^{r_E}} = P(E/K) \cdot \frac{\#(Ш(E/K)) \cdot R_{E/K}}{\#(E_{tors}(K))^2},$$

where $P(E/K)$ is the period, $R_{E/K}$ the regulator, and $Ш(E/K)$ the Tate-Shafarevich group.

This conjecture is one of the \$1,000,000 Millennium Prize problems listed by the Clay Mathematics Institute [Wil]. Besides the remarkable conjectural property that multiple basic invariants of E/K appear in the first non-zero coefficient of the Taylor expansion of $L(E, s)$ at $s = 1$, it also provides a hypothetical value for the generally difficult to compute order of $Ш(E/K)$. Additionally, it provides a method to calculate the rank r_E by computing the derivatives of $L(E, s)$ at $s = 1$.

It moreover hands us an equivalent characterization for the finiteness of the group $E(K)$. Namely,

$$\begin{aligned} &\text{if } L(E, 1) \neq 0 \implies r_E = 0 \implies E(K) \text{ finite} \\ &\text{if } L(E, 1) = 0 \implies r_E \geq 1 \implies E(K) \text{ infinite.} \end{aligned}$$

More on the consequences of this conjecture, and about the evidence for the conjecture to hold, can be found in [Wil] and [Sil09]. To get a better overview of the history of the BSD conjecture, one is suggested to read [Ste13].

The number theoretical analogue of the L-series of an elliptic curve E/K is the Dedekind zeta function of a number field. This function, often denoted as $\zeta_K(s)$, encodes a lot of fundamental information about the considered number field. This is a generalized version of the Riemann zeta function, which is known from the famous Riemann hypothesis[1]. The Dedekind zeta function was originally defined on the part $\mathrm{Re}(s) > 1$ of the complex plane. The mathematician Erich Hecke was the first to prove that $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}$, with a simple pole at $s = 1$. The residue at that pole is known as the analytic class number formula. Similar to the formula in the BSD conjecture, this expression consists of multiple basic invariants for number fields.

[1] This conjecture is also one of the \$1,000,000 Millennium Prize problems listed by the Clay Mathematics Institute [Bom00]

Theorem 0.0.2 (Analytic Class Number Formula)**.** (cf. [Neu99, Cor.VII.5.11]) *Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and $2r_2$ the number of complex embeddings. The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}\backslash\{1\}$ with a simple pole at $s = 1$. The residue of $\zeta_K(s)$ at $s = 1$ is given by*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot h_K\cdot R_K}{\sqrt{|\Delta_K|}\cdot\#(\mathcal{O}_K^\times)_{tors}},$$

where h_K is the class number of K, R_K the regulator, Δ_K the discriminant, and $(\mathcal{O}_K^\times)_{tors}$ the finite torsion subgroup of the ring of integers of K.

Our goal in this thesis is to obtain an answer to the question:

What are the similarities between the analytic class number formula and the BSD conjecture?

It turns out that the following template can be used to express both formulae:

$$\frac{\text{Period} \ \times \ |\text{Tate-Shafarevich group}| \ \times \ \text{Regulator}}{|\text{torsion group}|^{\text{power}}}$$

The formulations of the analytic class number formula and the BSD conjecture already indicate a certain analogy between them. Namely, they both contain the order of a finite torsion group $(\mathcal{O}_K^\times)_{\text{tors}}$ and $E_{\text{tors}}(K)$, respectively. Moreover, they contain the regulator of the considered algebraic structure, which in both cases is defined as a volume. We will see that even more similarities can be obtained, which are summarized below:

BSD	correspondence	Analytic Class Number Formula
$E_{\text{tors}}(K)$	$\longleftrightarrow$	$(\mathcal{O}_K^\times)_{\text{tors}}$
$R_{E/K}$	$\longleftrightarrow$	R_K
$Ш(E/K)$	$\longleftrightarrow$	$\text{Cl}(\mathcal{O}_K) \cong Ш(K)$
$P(E/K) = \text{vol}(E(\mathbb{A}_K))$	$\longleftrightarrow$	$P(K) = \text{vol}(\mathcal{O}_{\mathbb{A}_K}^\times) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{\|\Delta_K\|}}$

.

Structure

One of the main objects returning in this thesis are normed fields, and completions of these type of fields. In particular, number fields play a key role in this thesis for which we prove that the associated completions are locally compact. Chapter 1 is devoted to introduce the reader to the stated topics.

In Chapter 2 we introduce more advanced topics such as the adele ring and idele group of a certain type of fields. We start this chapter by introducing the final topology and the notion of taking restricted direct products, which are needed to define the adele ring and idele group. At last, we give the so-called Tamagawa measure for which the general construction can be found in [Wei82].

In Chapter 3 the theory about Galois cohomology is discussed briefly. To give the reader enough knowledge, we start with recalling the general concepts about field extensions and Galois theory.

The main purpose of Chapter 4 is to introduce the reader to elliptic curves, and state the BSD conjecture. Moreover, we define the regulator, Tate-Shafarevich group, and the period of an elliptic curve.

The final chapter, Chapter 5, starts with an introduction to the Dedekind zeta function together with the analytic class number formula. The remaining part of this chapter is written in view of obtaining as many similarities as possible between the appearing mathematical invariants in the BSD conjecture and the analytic class number formula. The following represents the places where the analogies can be found

Sections	BSD		ACNF	Sections
4.3	$R_{E/K}$	$\longleftrightarrow$	R_K	5.2
4.4	$\text{Ш}(E/K)$	$\longleftrightarrow$	$\mathrm{Cl}(\mathcal{O}_K) \cong \text{Ш}(K)$	5.3
4.5	$P(E/K) = \mathrm{vol}(E(\mathbb{A}_K))$	$\longleftrightarrow$	$P(K) = \mathrm{vol}(\mathcal{O}_{\mathbb{A}_K}^{\times}) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{\lvert\Delta_K\rvert}}$	5.4

We end this thesis with a summary of the found similarities.

Prerequisites

This thesis is mainly written with the purpose to be self-contained. The main references used are listed at the start of the chapters and sections. The theory discussed is restricted to the required amount needed. If the reader feels the necessity to consult a more complete description of the discussed theory, one is suggested to take a look at the listed references.

Basic knowledge about groups, rings and fields is required which can be found in any algebra book (e.g. [Lan02]).

Despite the fact that an abridged version of basic algebraic number theory will be given, it will not harm the reader to consult the books [Neu99] and [Kna07] for any clarifications about the discussed theory.

It is moreover beneficial to have any familiarities with elliptic curves. Most of the required definitions and results will be given, paraphrased from [Sil09].

Other prerequisites include basic knowledge about topology. One is supposed to be familiar with the notions of being locally compact, Hausdorff, a topological group, a topological ring, and a topological field. The latter three are algebraic structures endowed with a topology such that the corresponding operations are continuous with respect to the given topology.

Chapter 1

Basic Algebraic Number Theory

The fundamental algebraic structure considered in this thesis is that of a field. In particular, we will be mainly interested in number fields. A *number field* is a finite extension of the field of rational numbers $\mathbb{Q}$. The main purpose of this chapter is to provide the reader with sufficient knowledge about basic algebraic number theory needed for the rest of this thesis. The definitions and results will be formulated for general fields, global fields, or number fields in particular. These *global fields* are either number fields, or a finite field extension of $\mathbb{F}_p(t)$ for some prime p. The choice to extend results and definitions to global fields instead of restricting to number fields, depends on whether the extension brings additional difficulties or not.

Sections 1.1-1.4 are dedicated to introduce the notion of absolute values on a field, the corresponding induced topology on the field, valuations, and the completion of a normed field. The reader who is interested in a more complete description of this theory can consult [Kna07] and [Claa].

In Sections 1.5-1.7 we give an abridged discussion of the theory about lattices, arithmetic on number fields, and ideal factorization on extensions of Dedekind domains. As a main reference for these sections we use [Neu99], [Sut15], and [Kna07].

1.1 Archimedean and non-Archimedean Places on a Field

On the real numbers $\mathbb{R}$ we have the well-known standard absolute value, which is a mapping $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$, given by

$$|x| := \begin{cases} x & \text{if } x \in \mathbb{R}_{\geq 0} \\ -x & \text{otherwise.} \end{cases}$$

This map satisfies four fundamental properties, namely it is non-negative, positive-definite, multiplicative and subadditive. These fundamental properties can be used to give a definition of an absolute value on an arbitrary field. The main references for this section are [Kna07] and [Claa].

Definition 1.1.1 (Absolute Value)**.** Let K be a field. Then an *absolute value* on K is a mapping $|\cdot| : K \to \mathbb{R}$ that satisfies the following properties:

(i) (*Non-negativity*) $|x| \geq 0$ for all $x \in K$.

(ii) (*Positive-definite*) $|x| = 0$ if and only if $x = 0$.

(iii) (*Multiplicativity*) $|xy| = |x||y|$ for all $x, y \in K$.

(iv) (*Subadditivity*) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Some of the absolute values satisfy a slightly stronger property than just being subadditive, also known as the ultrametric inequality. These absolute values are also called non-Archimedean.

Definition 1.1.2 (Non-Archimedean Absolute Value)**.** Let K be a field and $|\cdot|$ an absolute value on K. Then $|\cdot|$ is said to be *non-Archimedean* if it satisfies the *ultrametric inequality*, i.e., if for all $x, y \in K$ we have

$$|x+y| \leq \max(|x|, |y|).$$

If $|\cdot|$ does not satisfy this inequality, it is called an Archimedean absolute value.

Example 1.1.3.

- Let $K = \mathbb{Q}$. Then besides the standard absolute value $|\cdot|_\infty$ which is Archimedean, we also have the so-called *p-adic absolute values*. Let p be a prime, then every rational number r can be written as $r = p^m ab^{-1}$ for some integers a and b relatively prime to p and a unique integer m. Thus we can define a map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as $|0|_p = 0$ and $|r|_p = p^{-m}$. This defines a non-Archimedean absolute value on $\mathbb{Q}$, called the p-adic absolute value.

- Let $K = \mathbb{F}_p(t)$. For $c \in (0,1)$ we define the maps

$$|\cdot|_\infty : \mathbb{F}_p(t) \to \mathbb{R}_{\geq 0}, r(t) \mapsto c^{-\deg(r(t))}$$
$$|\cdot|_\pi : \mathbb{F}_p(t) \to \mathbb{R}_{\geq 0}, r(t) \mapsto c^{\operatorname{ord}_\pi(r(t))},$$

for some monic irreducible $\pi(t) \in \mathbb{F}_p[t]$. Note that $r(t) = f(t)/g(t)$ for some polynomials $f(t), g(t) \in \mathbb{F}_p[t]$, and $\deg(r(t)) := \deg(f(t)) - \deg(g(t))$. Moreover, for the order map we have $\operatorname{ord}_\pi(r(t)) := \operatorname{ord}_\pi(f(t)) - \operatorname{ord}_\pi(g(t))$. The maps $|\cdot|_\infty$ and $|\cdot|_\pi$ define non-Archimedean absolute values on $\mathbb{F}_p(t)$. The absolute value $|\cdot|_\pi$ is similar to the p-adic absolute value on $\mathbb{Q}$, and it is often called the *π-adic absolute value.*

The following proposition gives us a way to check whether an absolute value is non-Archimedean or not.

Proposition 1.1.4. *Let K be a field and $|\cdot|$ an absolute value on K. Then the following are equivalent:*

(i) $|\cdot|$ is non-Archimedean.

(ii) The set $|\mathbb{Z} \cdot 1|$ is bounded, i.e., there exists $C \in \mathbb{R}_{>0}$ such that $|n \cdot 1| \leq C$ for all $n \in \mathbb{Z}$.

Proof. "(i) $\implies$ (ii)" Suppose that $|\cdot|$ is non-Archimedean. Then it follows directly from the ultrametric inequality that $|n \cdot 1| = |\sum_{i=1}^n 1| \leq 1$.

"(ii) $\implies$ (i)" Suppose that there exists a $C > 0$ such that $|n \cdot 1| \leq C$ for all $n \in \mathbb{Z}$, then notice by the binomial theorem that

$$|x+y|^m = \left|\sum_{i=0}^m \binom{m}{i} x^{m-i} y^i\right| \leq C \sum_{i=0}^m |x|^{m-i}|y|^i < C \sum_{i=0}^m \max\{|x|, |y|\}^m = C(m+1)\max\{|x|, |y|\}^m$$

for all $x, y \in K$ and $m \in \mathbb{Z}_{\geq 0}$. This implies the desired inequality,

$$|x+y| \leq \lim_{m\to\infty} C^{1/m}(m+1)^{1/m} \max\{|x|, |y|\} = \max\{|x|, |y|\}.$$

■

The equivalent property of being non-Archimedean in particular implies that extensions of absolute values are non-Archimedean if and only if the original absolute value is non-Archimedean. In other words, for a given field extension of normed fields $(L, |\cdot|_L) \subset (K, |\cdot|_K)$ with $|\cdot|_{K|_L} = |\cdot|_L$, the absolute value $|\cdot|_L$ is non-Archimedean if and only if $|\cdot|_K$ is non-Archimedean.

Let $\mathcal{A}(K)$ be the set of all absolute values on a field K. Then we can actually define a binary relation $\sim$ on $\mathcal{A}(K)$. This can be achieved by saying that $|\cdot|_1 \sim |\cdot|_2$ if and only if there exists a $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^\lambda$ with $|\cdot|_1, |\cdot|_2 \in \mathcal{A}(K)$. It appears that this binary relation is actually an equivalence relation on $\mathcal{A}(K)$.

Proposition 1.1.5. *Let K be a field. The binary relation $\sim$ defined above on the set $\mathcal{A}(K)$, consisting of all absolute values on K, is an equivalence relation.*

Proof. We have to check that the binary relation is reflexive, symmetric and transitive. Let $|\cdot|_1, |\cdot|_2, |\cdot|_3 \in \mathcal{A}(K)$,

- (Reflexivity) It is clear that $|\cdot|_1 \sim |\cdot|_1$.
- (Symmetry) Suppose that $|\cdot|_1 \sim |\cdot|_2$, then $|\cdot|_2 = |\cdot|_1^\lambda$ for some $\lambda \in \mathbb{R}_{>0}$. This implies that $|\cdot|_1 = |\cdot|_2^{1/\lambda}$, and thus $|\cdot|_2 \sim |\cdot|_1$.
- (Transitivity) Suppose that $|\cdot|_1 \sim |\cdot|_2$ and $|\cdot|_2 \sim |\cdot|_3$, then there exist $\lambda_1, \lambda_2 \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^{\lambda_1}$ and $|\cdot|_3 = |\cdot|_2^{\lambda_2}$. This implies that $|\cdot|_3 = |\cdot|_1^{\lambda_1\lambda_2}$, so indeed $|\cdot|_1 \sim |\cdot|_3$.

■

Definition 1.1.6. An equivalence class determined by an arbitrary non-trivial absolute value in $\mathcal{A}(K)$ under $\sim$ is also called a *place v* on the field K. The set of all places v on K is denoted by M_K.

One important class invariant property under the equivalence relation $\sim$ on $\mathcal{A}(K)$ is being (non-)Archimedean. This leads us to the following proposition.

Proposition 1.1.7. *Let K be a field and $(\mathcal{A}(K), \sim)$ the corresponding set of absolute values together with the binary relation defined above. Let $|\cdot|_1 \in \mathcal{A}(K)$. Then $|\cdot|_1$ is non-Archimedean (resp. Archimedean) if and only if every equivalent absolute value is non-Archimedean (resp. Archimedean).*

Proof. Note that it is enough to only proof the statement for the non-Archimedean case. The other case will follow directly from this statement.

“ $\Longrightarrow$ ” Suppose that $|\cdot|_1$ is non-Archimedean, and let $|\cdot|_2 \in \mathcal{A}(K)$ such that it is equivalent to $|\cdot|_1$. Then there exists $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^\lambda$. Now notice that for all $x, y \in K$ we have

$$|x+y|_2 = |x+y|_1^\lambda \leq \max(|x|_1, |y|_1)^\lambda = \max(|x|_1^\lambda, |y|_1^\lambda) = \max(|x|_2, |y|_2).$$

This shows that $|\cdot|_2$ also satisfies the ultrametric inequality, and therefore it is non-Archimedean.

“ $\Longleftarrow$ ” Suppose that every equivalent absolute value to $|\cdot|_1$ is non-Archimedean. Then since $\sim$ is an equivalence relation on $\mathcal{A}(K)$, it is reflexive and therefore $|\cdot|_1$ is equivalent to itself. And thus by assumption $|\cdot|_1$ is non-Archimedean. ■

Let $\mathcal{A}_{\mathrm{NA}}(K)$ be the set of non-Archimedean absolute values on K. Then the proposition above tells us that the equivalence relation $\sim$ on $\mathcal{A}(K)$ also defines an equivalence relation on $\mathcal{A}_{\mathrm{NA}}(K)$. Similarly for the set $\mathcal{A}_{\mathrm{A}}(K)$ consisting of Archimedean absolute values. In other words, it makes sense to talk about (non-)Archimedean places of a field K.

Definition 1.1.8. The set of non-Archimedean places on a field K, also known as the *finite places*, is denoted as M_K^0.

The set of Archimedean places, also known as *infinite places*, is denoted as M_K^∞.

There are certain fields for which the collections of places are well-known. The most important ones for now are the ones for $\mathbb{Q}$ and $\mathbb{F}_p(T)$, due to the mathematician Alexander Ostrowski.

Remark 1.1.9. Ostrowski's Theorem[Kna07, Thm 6.15] tells us that every non-trivial absolute value on $\mathbb{Q}$ is either equivalent to the standard absolute value $|\cdot|_\infty$ or the p-adic absolute value $|\cdot|_p$ for some prime p. A variant of this theorem [Con, Cor.4] implies that every non-trivial absolute value on $\mathbb{F}_p(t)$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_\pi$ as given in Example 1.1.3.

1.2 Topology Induced by Absolute Value

This section is devoted to putting a topology on a normed field induced by the corresponding absolute value. We again use [Kna07] and [Claa] as our main references.

Let K be a field and $|\cdot|$ an absolute value on K. The tuple $(K, |\cdot|)$ is called a normed field. Note that the absolute value $|\cdot|$ induces a metric on K, given by $d : K \times K \to \mathbb{R}, (x, y) \mapsto |x-y|$. This metric induces corresponding open balls for $x \in K$ of radius r given by

$$B_d(x, r) := \{y \in K \mid d(x, y) < r\}.$$

A basis of open neighborhoods of x induced by d is now given by $\mathcal{B}_d(x) := \{B_d(x, r) \mid r \in \mathbb{R}_{>0}\}$. For simplicity, we write $B_d[x, r]$ for the closed ball $\{y \in K | d(x, y) \leq r\}$. This topology makes K into a topological field, which is proven in the following proposition.

Proposition 1.2.1. *Let $(K, |\cdot|)$ be a normed field, topologized by the associated metric $d_{|\cdot|}$. This topology makes K into a topological field.*

Proof. We have to show that the addition, multiplication and inversion operations on K are continuous. Let us start with the continuity of the addition and multiplication operations. Since we work with metric spaces, these maps are continuous if and only if they are sequentially continuous. Now let $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ be convergent sequences in $(K, |\cdot|)$ with limits x and y, respectively. As a consequence of the fact that $(y_n)_{n\in\mathbb{N}}$ is a convergent sequence, there exists a $C \geq 0$ such that $|y_n| < C$ for all $n \in \mathbb{N}$. Therefore we find that

$$\lim_{n\to\infty} |(x_n + y_n) - (x + y)| \leq \lim_{n\to\infty} |x_n - x| + |y_n - y| = 0$$
$$\lim_{n\to\infty} |x_n y_n - xy| = \lim_{n\to\infty} |(x_n - x)y_n + (y_n - y)x| \leq \lim_{n\to\infty} C|x_n - x| + |x||y_n - y| = 0,$$

proving that addition and multiplication on K are continuous.

For the inversion map $x \mapsto x^{-1}$ on $K^\times$ to $K^\times$, let $a \in K^\times$. Let $\varepsilon > 0$ be given, and choose $\delta = \frac{1}{2}\min\{|a|, \varepsilon|a|^2\}$. Then for all $x \in K^\times$ with $|x - a| < \delta$, we have $|x| > |a| - \delta > \frac{1}{2}|a|$. Consequently, we find that

$$|x^{-1} - a^{-1}| = |x^{-1}||a^{-1}||x - a| < 2|a^{-2}|\delta < \varepsilon.$$

Since we took $a \in K^\times$ arbitrarily, this proves that the inversion map is also continuous. ■

During the construction of the adele rings, we consider completions of a field K with respect to some place on that field. For this to make sense we need to know that absolute values that are equivalent, induce the same topology on K. To show this, we need the following lemma consisting of an equivalent condition to see whether two absolute values are equivalent or not.

Lemma 1.2.2. *Let K be a field and $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K. Then $|\cdot|_1 \sim |\cdot|_2$ if and only if $\{x \in K \mid |x|_1 < 1\} = \{x \in K \mid |x|_2 < 1\}$.*

Proof. " $\implies$ " Suppose that $|\cdot|_1 \sim |\cdot|_2$. Then there exists $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^\lambda$. Therefore, for all $x \in K$ we have

$$|x|_2 < 1 \iff |x|_1^\lambda < 1 \iff |x|_1 < 1.$$

" $\impliedby$ " This part of the proof closely follows the proof of Theorem 1.8 (iv) to (i) in [Claa]. Suppose that $\{x \in K \mid |x|_1 < 1\} = \{x \in K \mid |x|_2 < 1\}$. First assume that either $|\cdot|_1$ or $|\cdot|_2$ is the trivial absolute value. Then the assumption immediately implies that $|\cdot|_1 = |\cdot|_2$ and so the statement is proven. Now assume that both $|\cdot|_1$ and $|\cdot|_2$ are non-trivial. Then there exists a $\xi \in K$ such that $0 < |\xi|_1 < 1$, and consequently also $0 < |\xi|_2 < 1$ by assumption. Thus we can define

$$\lambda := \frac{\log|\xi|_2}{\log|\xi|_1}.$$

The claim is that $|x|_1^\lambda = |x|_2$ for all $x \in K$. Let $x \in K$, and notice that for $x = 0$ it is clearly true. Therefore, we can assume that $x \neq 0$. We observe that it is equivalent to show that $\lambda \log|x|_1 = \log|x|_2$ since the logarithm is injective on $\mathbb{R}_{>0}$. In other words, we want to show that

$$z_1 := \frac{\log|x|_1}{\log|\xi|_1} = \frac{\log|x|_2}{\log|\xi|_2} =: z_2.$$

Since $\mathbb{Q}$ is dense in $\mathbb{R}$ it is enough to show that there is no rational number between both real numbers. Let $r \in \mathbb{Z}$ and $s \in \mathbb{Z}_{>0}$, then

$$\begin{aligned} \frac{r}{s} < \frac{\log|x|_1}{\log|\xi|_1} &\Leftrightarrow \log(|\xi|_1^r) > \log(|x|_1^s) \Leftrightarrow |\xi|_1^r > |x|_1^s \Leftrightarrow 1 > \left|\frac{x^s}{\xi^r}\right|_1 \\ \Leftrightarrow 1 > \left|\frac{x^s}{\xi^r}\right|_2 &\Leftrightarrow |\xi|_2^r > |x|_2^s \Leftrightarrow \log(|\xi|_2^r) > \log(|x|_2^s) \Leftrightarrow \frac{r}{s} < \frac{\log|x|_2}{\log|\xi|_2}. \end{aligned}$$

This implies that there indeed does not exist a rational number between z_1 and z_2, and thus $z_1 = z_2$. Consequently, this proves the claim that $|x|_1^\lambda = |x|_2$ for all $x \in K$, so $|\cdot|_1 \sim |\cdot|_2$. ■

Proposition 1.2.3. *Let K be a field and $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K. Then the following are equivalent:*

(i) $|\cdot|_1 \sim |\cdot|_2$

(ii) The topologies induced by the metrics d_1 and d_2 are identical. With d_1 and d_2 we mean the metrics induced by respectively $|\cdot|_1$ and $|\cdot|_2$.

Proof. "(i) $\implies$ (ii)" Suppose that $|\cdot|_1 \sim |\cdot|_2$. Then there exists $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^\lambda$. Note that it is enough to show that for all $x \in K$ the bases of open neighborhoods of x induced by d_1 and d_2 coincide to conclude that the metrics induce the same topology on K. Let $x \in K$ and $B_{d_1}(x, r) \in \mathcal{B}_{d_1}(x)$ for some arbitrary $r \in \mathbb{R}_{>0}$. Observe that

$$B_{d_1}(x, r) = \{y \in K \mid d_1(x, y) < r\} = \{y \in K \mid d_2(x, y) < r^\lambda\} = B_{d_2}(x, r^\lambda).$$

Since we took r to be arbitrary, we find $\mathcal{B}_{d_1}(x) \subset \mathcal{B}_{d_2}(x)$. The other inclusion follows in a similar way. Thus the two bases of neigborhoods of x coincide and therefore the induced topologies on K by d_1 and d_2 are identical.

"(ii) $\implies$ (i)" Suppose that the topologies on K induced by d_1 and d_2 coincide. We consider the sets

$$B_{d_i}(0,1) := \{y \in K \mid |y|_i < 1\}$$

for $i = 1, 2$. If $x \in B_{d_1}(0,1)$, then $|x|_1 < 1$, and therefore the sequence $(x^n)_{n\in\mathbb{N}}$ converges to 0 in (K, d_1). Since (K, d_1) is a metric space, this implies that for every open U in (K, d_1) containing x, there exists a $N_U \in \mathbb{N}$ such that for all $n \geq N_U$, $x^n \in U$. Since $B_{d_2}(0,1)$ is also an open in (K, d_1), there exists a $N \in \mathbb{N}$ such that for all $n \geq N$ we have $x^n \in B_{d_2}(0,1)$. This implies that $|x^N|_2 < 1$ and thus $|x|_2 < 1$. This shows that $B_{d_1}(0,1) \subset B_{d_2}(0,1)$. Similarly, we can show that $B_{d_2}(0,1) \subset B_{d_1}(0,1)$. Lemma 1.2.2 now implies that $|\cdot|_1 \sim |\cdot|_2$. ■

Given a normed field $(K, |\cdot|)$, we will always endow it with the topology induced by the metric $d_{|\cdot|}$, unless mentioned otherwise. For simplicity we will just write d for the metric induced by $|\cdot|$, and drop the metric in the subscript of the open (and closed) balls in the corresponding topology. In the case that $|\cdot|$ is non-Archimedean, we have the following remarkable property.

Proposition 1.2.4. *Let $(K, |\cdot|)$ be a normed field with $|\cdot|$ a non-trivial non-Archimedean absolute value. Then, every open ball is closed, and every closed ball is open.*

Proof. Let $x \in K$ and $\delta > 0$. We start by showing that every open ball is closed. We will show that the open ball $B(x, \delta)$ is closed by showing that the complement $(B(x,\delta))^C$ in K is open. Let $y \in (B(x,\delta))^C$, which means that $|x - y| \geq \delta$. By using the non-Archimedean property of $|\cdot|$ we find for any $z \in B(y, \delta)$ that,

$$\delta \leq |x - y| = |(x - z) + (z - y)| \leq \max\{|x - z|, |z - y|\} = |x - z|.$$

This implies that $z \notin B(x, \delta)$. Therefore,

$$(B(x,\delta))^C = \bigcup_{y \in (B(x,\delta))^C} B(y, \delta),$$

implying that the open ball $B(x, r)$ is closed.

For proving that every closed ball is open, we will prove that $B[x, \delta]$ is open. Note that for every $y \in B[x, \delta]$ and $z \in B(y, \delta)$ we have

$$|z - x| = |z - y + y - x| \leq \max\{|z - y|, |y - x|\} \leq \delta,$$

which means that $z \in B[x, \delta]$. For that reason, we can write

$$B[x, \delta] = \bigcup_{y \in B[x,\delta]} B(y, \delta),$$

which proves that $B[x, \delta]$ is open.

Since we took $x \in K$ and $\delta > 0$ arbitrarily we find the desired results. ■

1.3 Valuations

In this section the notion of valuation rings is introduced. These type of rings are useful tools for the construction of adele rings. They moreover provide a way to assign sizes to elements and compare them by their sizes. A more thorough treatment of this material can be found in [Kna07], [Claa], and [AM69].

Definition 1.3.1 (Valuation)**.** Let K be a field. A (rank one) *valuation* on a field K is given by a map $v : K \to \mathbb{R} \cup \{\infty\}$ satisfying the properties:

(i) $v(x) = \infty$ if and only if $x = 0$.

(ii) For all $x, y \in K$, $v(xy) = v(x) + v(y)$.

(iii) For all $x, y \in K$, $v(x + y) \geq \min(v(x), v(y))$.

Notice that the final property becomes an equality when $v(x) \neq v(y)$. Namely, under the assumption that $v(x) > v(y)$, we see that $v(x) \geq \min(v(x + y), v(y)) = v(x + y)$.

Consider the set $\mathcal{O}_{K,v} = \{x \in K \mid v(x) \geq 0\}$. The properties of the valuation make sure that this set is a ring, and therefore called the *valuation ring* of v. The subset $\Gamma_v := v(K^\times)$ of $(\mathbb{R}, +)$ is actually a subgroup. This is a direct consequence of the second property of a valuation. This group Γ_v is called the *value group* of v. Another important group is the group of units. Notice that $x \in \mathcal{O}_{K,v}$ is a unit if and only if there exists a $y \in \mathcal{O}_{K,v}$ such that $xy = 1$. This is the case if and only if $v(x) + v(y) = v(xy) = v(1) = 0$. Therefore, the unit group is given by $\mathcal{O}_{K,v}^\times = \{x \in K \mid v(x) = 0\}$, since $v(x), v(y) \geq 0$. When it is clear from the context which valuation is considered, it is also convenient to just write $\mathcal{O}_K$ for the valuation ring.

Lemma 1.3.2. *The valuation ring $\mathcal{O}_{K,v} = \{x \in K \mid v(x) \geq 0\}$ is a local ring, with unique maximal ideal*

$$\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}.$$

Proof. Let $\mathfrak{m}_v$ be defined as above. First notice from the discussion above that $\mathfrak{m}_v = \mathcal{O}_{K,v} \backslash \mathcal{O}_{K,v}^\times$. If $\mathfrak{m}_v$ is an ideal, then this implies that it has to be the unique maximal ideal. Now notice that

(i) $v(0) = \infty$, and thus $0 \in \mathfrak{m}_v$.

(ii) For all $x, y \in \mathfrak{m}_v$, $v(x - y) \geq \min(v(x), v(-y)) = \min(v(x), v(y)) > 0$. Therefore $x - y \in \mathfrak{m}_v$.

(iii) For all $x \in \mathfrak{m}_v$ and $y \in \mathcal{O}_{K,v}$, $v(xy) = v(x) + v(y) > 0$.

This shows that $\mathfrak{m}_v$ is an ideal. Thus $\mathcal{O}_{K,v}$ is a local ring, with unique maximal ideal $\mathfrak{m}_v$. ■

Definition 1.3.3. Let R be a local ring with maximal ideal m. Then the *residue field* is the quotient ring $R/\mathfrak{m}$.

We call two valuations v and v' equivalent if there exists a $\lambda \in \mathbb{R}_{>0}$ such that $v' = \lambda v$. If v is a valuation and $\lambda \in \mathbb{R}_{>0}$, then $v' := \lambda v$ is also a valuation. This binary relation defines an equivalence relation on the set of valuations on K, denoted by $\mathcal{V}(K)$.

Theorem 1.3.4. *Let $c \in \mathbb{R}_{>1}$ and K a field. The following map is a bijection*

$$\begin{aligned} \varphi : (\mathcal{V}(K), \sim) &\longrightarrow (\mathcal{A}_{NA}(K), \sim) \\ [v] &\longmapsto [| \cdot |_v], \end{aligned}$$

where $| \cdot |_v : K \to \mathbb{R}_{\geq 0}$ is given by $|x|_v = c^{-v(x)}$.

Proof. That the map $|\cdot|_v$ is a non-Archimedean absolute value follows easily from the properties of the valuation v. To conclude well-definedness, we are left to show that φ is well-defined on the equivalence classes. Suppose that $v_2 = \lambda v_1$ for some $\lambda \in \mathbb{R}_{>0}$ and $v_1, v_2 \in \mathcal{V}(K)$, then $|x|_{v_2} = c^{-\lambda v_1(x)} = |x|_{v_1}^{\lambda}$. Therefore $[|\cdot|_{v_1}] = [|\cdot|_{v_2}]$, and thus φ is well-defined.

We will now show that φ is a bijection. For injectivity, suppose that $\varphi([v_1]) = \varphi([v_2])$ for some $v_1, v_2 \in \mathcal{V}(K)$. Then there exists $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_{v_2} = c^{-v_2(x)} = c^{-\lambda v_1(x)} = |\cdot|_{v_1}^{\lambda}$. After applying $-\log_c(\cdot)$ to the previous equation we find that $v_2 = \lambda v_1$. This implies that $[v_1] = [v_2]$, which means that φ is indeed injective. For surjectivity, let $|\cdot| \in \mathcal{A}_{\mathrm{NA}}(K)$. Define

$$v : K \to \mathbb{R} \cup \{\infty\},\ v(x) := \begin{cases} \infty & \text{if } x = 0 \\ -\log_c |x| & \text{if } x \neq 0, \end{cases}$$

and note that this clearly defines a valuation on K, since $|\cdot|$ is a non-Archimedean absolute value. Now note that $\varphi([v]) := [|\cdot|]$, and thus φ is indeed surjective. ■

This theorem gives a relation between the non-Archimedean absolute values and the valuations on a field K. Every time we encounter a field with a non-Archimedean absolute value it makes sense to consider a corresponding valuation. There is freedom of choice for the number c in the map φ defined above, since for a fixed valuation the corresponding absolute values for different choices of c are equivalent. Note that for a given valuation v the corresponding class of absolute values $[|\cdot|_v]$ satisfy $\mathcal{O}_{K,v} = \{x \in K \mid |\cdot|_v^{\lambda} \leq 1\}$ for every $\lambda \in \mathbb{R}_{>0}$. Thus we can also denote the valuation ring by $\mathcal{O}_{K,|\cdot|_v}$ where $|\cdot|_v$ is a corresponding absolute value to the valuation v. The following example gives the valuation ring of the non-Archimedean absolute values given in Example 1.1.3.

Example 1.3.5.

- Let $K = \mathbb{Q}$ and $|\cdot|_p$ be the p-adic absolute value on $\mathbb{Q}$ for some prime number p. Then $\mathcal{O}_{K,|\cdot|_p} = \mathbb{Z}_{(p)}$, i.e., the localization of $\mathbb{Z}$ at (p).
- Let $K = \mathbb{F}_p(t)$ and $|\cdot|_\pi$ be the π-adic absolute value for some monic irreducible $\pi(t) \in \mathbb{F}_p[t]$. Then the valuation ring is given by $\mathcal{O}_{K,|\cdot|_\pi} = \mathbb{F}_p[t]_{(\pi(t))}$, i.e., the localization of $\mathbb{F}_p[t]$ at the maximal ideal $(\pi(t))$. The valuation ring for the absolute value $|\cdot|_\infty$ on K is given by $\mathcal{O}_{K,|\cdot|_\infty} = \left\{\frac{f(t)}{g(t)} \mid \deg(f(t)) \leq \deg(g(t))\right\}$.

We call a valuation v *discrete* if the corresponding value group Γ_v is a non-trivial discrete subgroup of $(\mathbb{R}, +)$. The following shows that every discrete valuation is equivalent to a valuation with value group $\mathbb{Z}$.

Lemma 1.3.6. *Let v be a discrete valuation on K, then it is equivalent to a valuation with value group $\mathbb{Z}$.*

Proof. We first show that every non-trivial discrete subgroup H of $(\mathbb{R}, +)$ is infinite cyclic. We define the subset $H^+ = H \cap \mathbb{R}_{>0}$ of H. This subset is non-empty, since H is a non-trivial subgroup. Moreover, it is a non-empty subset of $\mathbb{R}$ that is bounded below by 0, and therefore H^+ has an infimum. Define $\eta := \inf H^+$, which is a limit point of H^+. We now use the fact that every discrete subgroup of $\mathbb{R}$ is closed to conclude that $\eta \in H$. Since H is discrete, there exists a $\varepsilon > 0$ such that $B(0, \varepsilon) \cap H = \{0\}$. Therefore, we have $B(0, \varepsilon) \cap H^+ = \emptyset$, and thus 0 is not a limit point of H^+. This implies that $\eta \in H^+$, since $0 < \eta \in H$. Consequently, we observe that η is the smallest positive element of H. Let $h \in H$, then by using Euclid's divisions lemma we can write $h = \eta x + r$ for some $x \in \mathbb{Z}$ and $0 \leq r < \eta$. Since H is a subgroup we have $r = \eta x - h \in H$. But since η is the smallest positive element of H this implies that $r = 0$. This proves that $H = \eta\mathbb{Z}$, and thus H is indeed infinite cyclic.

Now let v be a discrete valuation on K, meaning that Γ_v is a non-trivial discrete subgroup of $(\mathbb{R}, +)$. Then by the above we know that $\Gamma_v = \eta\mathbb{Z}$ for some $\eta \in \mathbb{R}_{>0}$. We can now define the valuation

$$v' : K \to \mathbb{R} \cup \{\infty\}, x \mapsto \eta^{-1}v(x),$$

which is equivalent to v. This gives the desired equivalent valuation with value group $\mathbb{Z}$, since $\Gamma_{v'} = \eta^{-1}\Gamma_v = \mathbb{Z}$. ■

The above tells us that every time we work with discrete valuations, we can just assume them to have value group $\mathbb{Z}$. Closely related to such discrete valuations is the notion of a discrete valuation ring. An integral domain R is called a discrete valuation ring (DVR) if there exists a discrete valuation v on its field of fractions K, such that $\mathcal{O}_{K,v} = R$. The following theorem gives some equivalent conditions for R being a discrete valuation ring. A more complete version can be found in [AM69, Prop.9.2].

Theorem 1.3.7. *Let R be a Noetherian local domain of Krull dimension one with fraction field K, and unique maximal ideal $\mathfrak{m}$. Then the following are equivalent:*

(i) R is a discrete valuation ring.

(ii) Every non-zero ideal is of the form $\mathfrak{m}^n$ for some $n \geq 0$.

(iii) There exists $\pi \in R$ such that $\mathfrak{m} = (\pi)$, then π is also called a uniformizer.

(iv) R is a principal ideal domain.

Proof. "(i) $\Longrightarrow$ (ii)" Suppose that R is a discrete valuation ring, then by Lemma 1.3.6 we have a discrete valuation v on K with value group $\mathbb{Z}$ such that $R = R_v = \{x \in K | v(x) \geq 0\}$. Thus there exists a $\pi \in K$ such that $v(\pi) = 1$. This also implies that $\pi \in R$, and that π is not a unit in R. Consequently, the inclusion $(\pi) \subset \mathfrak{m}$ holds. Now let $x \in \mathfrak{m}$, then $v(x) \geq 1$ by Lemma 1.3.2. Then by the properties of a valuation we see that $v(x\pi^{-1}) = v(x) - v(\pi) \geq 0$, and thus $x\pi^{-1} \in R$. Therefore $x = x\pi^{-1}\pi \in (\pi)$. This shows that $\mathfrak{m} = (\pi)$.

Now let I be a non-zero ideal of R, and $x \in I$ such that $v(x) = n$ is as small as possible. Then $v(x\pi^{-n}) = 0$, and thus $x\pi^{-n} = u$ for some unit $u \in R$. Therefore $\pi^n = u^{-1}x \in I$, and thus $(\pi^n) = \mathfrak{m}^n \subset I$. Let $0 \neq y \in I$, then $v(y) = k \geq n$ for some $k \in \mathbb{R}_{>0}$. By the same reasoning as before we see that $y\pi^{-k} = u'$ for some unit $u' \in R$. By minimality of n we find that $b = u'\pi^k \in \mathfrak{m}^k \subset \mathfrak{m}^n$. Thus $I = \mathfrak{m}^n$, which shows that every non-zero ideal indeed is a power of $\mathfrak{m}$.

"(ii) $\Longrightarrow$ (iii)" Suppose that every non-zero ideal is a power of $\mathfrak{m}$. We first show that $\mathfrak{m} \neq \mathfrak{m}^2$, meaning that $\mathfrak{m}\backslash\mathfrak{m}^2 \neq \emptyset$. Suppose that $\mathfrak{m} = \mathfrak{m}^2$, and notice that $\mathfrak{m}$ is a finitely generated R-module since R is Noetherian. Then by Nakayama's lemma[1] we find that $\mathfrak{m} = 0$, which is a contradiction. Let $\pi \in \mathfrak{m}\backslash\mathfrak{m}^2$, then by assumption $(\pi) = \mathfrak{m}^n$ for some $n \geq 0$. Now notice that π is not a unit, and thus $n \neq 0$. Also notice that $\pi \notin \mathfrak{m}^n$ for $n \geq 2$, since $\pi \notin \mathfrak{m}^2$. This shows that $(\pi) = \mathfrak{m}$.

"(iii) $\Longrightarrow$ (iv)" Suppose that $\mathfrak{m} = (\pi)$ for some $\pi \in R$. We first show that $\cap_{n=0}^{\infty}\mathfrak{m}^n = 0$. Let $x \in \cap_{n=0}^{\infty}\mathfrak{m}^n$, then for all $n \in \mathbb{Z}_{\geq 0}$ there exists $x_n \in R$ such that $x = x_n\pi^n$. Consequently, $x = x_n\pi^n = x_{n+1}\pi^{n+1}$, which implies that $x_n = x_{n+1}\pi$. Therefore we have an ascending chain of

[1] Nakayama's lemma can be found in [AM69, Prop.2.6]

ideals $(x_0) \subset (x_1) \subset \cdots \subset (x_n) \subset (x_{n+1}) \subset \cdots$. Note that every ascending chain of ideals is stationary, since R is Noetherian. This means that there exists $N \in \mathbb{Z}_{\geq 0}$ such that $(x_N) = (x_{N+1})$. Then $x_N = x_{N+1}\pi = x_N c_N \pi$ for some $c_N \in R$, and thus $(1 - c_N\pi)x_N = 0$. Since π is not a unit, we have $c_N\pi \neq 1$. This implies that $x_N = 0$, since R is a domain. Therefore $x = x_N\pi^N = 0$, which shows that $\cap_{n=0}^{\infty}\mathfrak{m}^n = 0$.

"(iv) $\implies$ (i)" Let R be a principal ideal domain, then $\mathfrak{m} = (\pi)$ for some $\pi \in R$. Note that since R is a principal ideal domain, it is also a unique factorization domain. Therefore the maximal ideals are precisely the ideals generated by the irreducible elements. Thus π is the only irreducible element of R (up to multiplication by units). Thus every non-zero element $a \in R$ can be written uniquely (up to units and ordering of factors) as $u\pi^n$ for some $n \geq 0$ and unit $u \in R$. Thus we can define a map $\nu : R \to \mathbb{Z} \cup \{\infty\}$ by putting $\nu(a) = n$ for $a \in R\backslash\{0\}$ and $\nu(0) = \infty$. Then ν satisfies the properties $(i) - (iii)$ of Definition 1.3.1 for $x, y \in R$. This map can be extended to a map $v : K \to \mathbb{Z} \cup \{\infty\}$ by putting $v(ab^{-1}) = \nu(a) - \nu(b)$ for $a \in R$ and $b \in R\backslash\{0\}$. We have to check that this map is well-defined. Note that $ab^{-1} = cd^{-1}$ in K implies that $ad = bc$. Therefore since ν satisfies properties $(i) - (iii)$ of Definition 1.3.1 for $x, y \in R$ we have

$$v(ab^{-1}) - v(cd^{-1}) = \nu(a) - \nu(b) - \nu(c) + \nu(d) = \nu(ad) - \nu(bc) = 0,$$

so v is indeed well-defined. That v satisfies the properties of a valuation follows from the fact that ν has these properties on R. It is clear that $v(K^\times) = \mathbb{Z}$, and that R is the valuation ring of v. ■

As mentioned earlier, during this paper we consider finite extensions of a certain field. These extensions are in particular algebraic extensions. For these type of field extensions we have the following result about valuations which will come in handy in the proof of Theorem 1.4.6.

Lemma 1.3.8. *Suppose that K/L is an algebraic field extension. Then a valuation v on K is trivial if and only if $v_{|_L}$ is trivial on L.*

Proof. " $\implies$ " This direction is clear.
" $\impliedby$ " Suppose that a valuation v on K is trivial on the subfield L. Let $\alpha \in K$, then α is algebraic over L. Note that without loss of generality we can assume that $v(\alpha) \geq 0$. Since α is algebraic over L we have $\sum_{i=0}^{n} a_n\alpha^n = 0$ for some $a_i \in L$ with $a_n = 1$, and $a_0 \neq 0$. Therefore

$$v(\alpha) + v\left(\sum_{i=1}^{n} a_i\alpha^{i-1}\right) = v\left(\sum_{i=1}^{n} a_i\alpha^{i}\right) = v(a_0) = 0, \tag{1.1}$$

since $a_0 \in L$ and v is trivial on L. By assumption we have $v(\alpha) \geq 0$, and since v is a valuation we find that

$$v\left(\sum_{i=1}^{n} a_i\alpha^{i-1}\right) \geq \min_{i=1,\ldots,n}(v(a_i\alpha^{i-1})) = \min_{i=1,\ldots,n}(v(a_i) + (i-1)v(\alpha)) \geq 0.$$

Thus (1.1) implies that $v(\alpha) = 0$, so v is trivial on K. ■

1.4 Completions

In this section we consider the completions of normed fields. For a more detailed description, one could consult [Kna07, VI.4]. Let $(K, |\cdot|)$ be a normed field. This is a metric space, and therefore it inherits the notion of being a complete metric space. Thus $(K, |\cdot|)$ is complete if and only if every Cauchy sequence converges with respect to $|\cdot|$. The only thing we further demand from the completion of a normed field, is that it still has the structure of a normed field.

Definition 1.4.1. A *completion* of a normed field $(K, |\cdot|_K)$ is a complete normed field $(\widehat{K}, |\cdot|_{\widehat{K}})$ such that:

1. there exists a *homomorphism of normed fields* $\iota : (K, |\cdot|_K) \to (\widehat{K}, |\cdot|_{\widehat{K}})$, i.e., a field homomorphism that is also an isometry.
2. the image $\iota(K)$ is dense in $\widehat{K}$.

Such a completion always exists, and is unique up to isomorphism. The uniqueness is a consequence of the following universal property of a completion.

Theorem 1.4.2. (cf. [Kna07, Thm.6.25]) *Let $(\widehat{K}, |\cdot|_{\widehat{K}})$ be a completion of the normed field $(K, |\cdot|_K)$ with the corresponding isometric homomorphism $\iota : (K, |\cdot|_K) \to (\widehat{K}, |\cdot|_{\widehat{K}})$. Let $\varphi : (K, |\cdot|_K) \to (L, |\cdot|_L)$ be another isometric homomorphism with $(L, |\cdot|_L)$ complete, then there exists a unique isometric homomorphism $\Phi : (\widehat{K}, |\cdot|_{\widehat{K}}) \to (L, |\cdot|_L)$ such that $\varphi = \Phi \circ \iota$. In other words, Φ makes the diagram*

$$\begin{tikzcd}
(K, |\cdot|_K) \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & (\widehat{K}, |\cdot|_{\widehat{K}}) \arrow[d, "\Phi"] \\
 & (L, |\cdot|_L),
\end{tikzcd}$$

commute.

As proven in Proposition 1.2.3, equivalent absolute values induce the same metric topologies. Thus if $|\cdot|_1 \sim |\cdot|_2$ on a field K, then a sequence is a $|\cdot|_1$-Cauchy sequence if and only if it is a $|\cdot|_2$-Cauchy sequence. Moreover, the choice for $|\cdot|_1$ or $|\cdot|_2$ does not affect the convergence of a sequence. As a consequence, it is easily seen that equivalent absolute values on a field K induce isomorphic completions. It therefore makes sense to talk about a completion of a field K with respect to a place v on that field. The notation we will use for such a completion is K_v. Let v be a place on K and $|\cdot|_v$ a representing absolute value. The goal of this section is to prove that the completion of a normed global field $(K, |\cdot|_v)$ is locally compact. Before we can prove this, a few results are needed.

Lemma 1.4.3. *Let K be a normed field with non-trivial non-Archimedean absolute value $|\cdot|_v$. Then the completion of the valuation ring $\mathcal{O}_{K,v}$ equals (up to isomorphism) the valuation ring $\mathcal{O}_{K_v}$ of the completion K_v of K.*

Proof. Note that we have an isometry $\varphi : K \to K_v$, such that $\varphi(K)$ is dense in K_v. This map induces an isometry on the valuation rings, i.e., we have an isometry $\psi := \varphi|_{\mathcal{O}_{K,v}} : \mathcal{O}_{K,v} \to \mathcal{O}_{K_v}$.

To finish the proof, it suffices to show that $\psi(\mathcal{O}_{K,v})$ is dense in $\mathcal{O}_{K_v}$ by the universal property of the completion. Let $x \in \mathcal{O}_{K_v}$, and $\varepsilon > 0$. Define $\delta_\varepsilon := \min\{1, \varepsilon\}$. Then, since $\varphi(K)$ is dense in K_v, we find a $z \in B(x, \delta) \cap \varphi(K)$. Thus $z = \varphi(y)$ for some $y \in K$. By using the facts that $|x|_{K_v} \leq 1$ and $|z - x|_{K_v} < \delta$, we find by the non-Archimedean property that

$$|y|_v = |\varphi(y)|_{K_v} = |z|_{K_v} = |z - x + x|_{K_v} \leq \max\{|z - x|_{K_v}, |x|_{K_v}\} \leq 1.$$

Therefore, $y \in \mathcal{O}_{K,v}$ and $\varphi(y) = \psi(y) \in \mathcal{O}_{K_v}$. This implies that $z \in B(x, \delta) \cap \psi(\mathcal{O}_{K,v})$, and thus $\psi(\mathcal{O}_{K,v})$ is dense in $\mathcal{O}_{K_v}$. ■

Lemma 1.4.4. *Let K/L be a finite extension of non-trivially normed non-Archimedean fields of degree $[K:L]=n$. Then the residue field k_K is a finite extension of k_L of degree at most n.*

Proof. Note that we have normed fields $(L, |\cdot|_{v_{|L}})$ and $(K, |\cdot|_v)$, where $|\cdot|_{v_{|L}} = (|\cdot|_v)_{|L}$. Therefore, we see that for the corresponding valuation rings we have $\mathcal{O}_{L,v_{|L}} \subset \mathcal{O}_{K,v}$, and for the maximal ideals $\mathfrak{m}_{v_{|L}} = \mathfrak{m}_v \cap \mathcal{O}_{L,v_{|L}}$. This means that we also have an injection from $k_L = \mathcal{O}_{L,v_{|L}}/\mathfrak{m}_{v_{|L}} \hookrightarrow \mathcal{O}_{K,v}/\mathfrak{m}_v = k_K$. Thus k_K is indeed a field extension of k_L.

We will now show that $[k_K : k_L] \leq n$. Let $[x_1]_v, ..., [x_{n+1}]_v \in k_K$. Then the representatives $x_1, ..., x_{n+1} \in \mathcal{O}_{K,v} \subset K$ have to be linearly dependent over L, since $\dim_L(K) = [K:L] = n$. Equivalently, there exists $\lambda_1, ..., \lambda_{n+1} \in L$ not all equal to zero such that $\sum_{i=1}^{n+1} \lambda_i x_i = 0$. Without loss of generality we can assume that $\lambda_{n+1} \neq 0$, and thus if we define $\mu_i = \lambda_i \lambda_{n+1}^{-1}$, then

$$x_{n+1} + \sum_{i=1}^{n} \mu_i x_i = 0.$$

Now define $J := \{j \in \{1, ..., n+1\} \mid v(\mu_j) < 0\}$, and $\mu := \prod_{j \in J} \mu_j^{-1}$. Multiplying the equation above by μ gives

$$\mu x_{n+1} + \sum_{i=1}^{n} \mu \mu_i x_i = 0,$$

and clearly by construction and the properties of a valuation, $v(\mu) > 0$ and $v(\mu\mu_i) \geq 0$. After defining $\nu_i := \mu\mu_i$ for $i = 1, ..., n$ and $\nu_{n+1} := \mu$, we see that $\nu_i \in \mathcal{O}_L$ for $1 \leq i \leq n+1$ and

$$\sum_{i=1}^{n+1} [\nu_i]_{v_{|L}} [x_i]_v = [0]_v.$$

Thus we have found $[\nu_1]_{v_{|L}}, ..., [\nu_{n+1}]_{v_{|L}} \in \mathcal{O}_{L,v_{|L}}/\mathfrak{m}_{v_{|L}}$ not all equal to zero such that the above is satisfied. Therefore, $[x_1]_v, ..., [x_{n+1}]_v \in k_K$ are linearly dependent over k_L, and consequently $[k_K : k_L] \leq n$. ∎

Lemma 1.4.5. *Let $(K, |\cdot|_v)$ be a non-trivially normed field, where $|\cdot|_v$ is induced by a discrete valuation v. Suppose that $(K, |\cdot|_v)$ is complete and has a finite residue field k. Then K is locally compact.*

Proof. Note that $\mathcal{O}_{K,v} = \{x \in K | v(x) \geq 0\} = \{x \in K | |x|_v \leq 1\}$ is a closed ball in the complete metric space $(K, |\cdot|_v)$. Therefore the subset $\mathcal{O}_{K,v}$ with the induced subspace topology is also complete. By [AM69, CH.10] we have an isomorphism of topological rings

$$\mathcal{O}_{K,v} = \widehat{\mathcal{O}}_{K,v} \cong \varprojlim_{n \to \infty} \mathcal{O}_{K,v}/\pi^n \mathcal{O}_{K,v}, \tag{1.2}$$

where π is a uniformizer of $\mathcal{O}_{K,v}$. The cardinality of $\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}$ can be deduced from the cardinality of the residue field $k = \mathcal{O}_{K,v}/\pi\mathcal{O}_{K,v}$. Namely, we have canonical isomorphisms

$$\pi^{n-1}\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v} \cong k, \text{ and } (\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}) / \left(\pi^{n-1}\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}\right) \cong \mathcal{O}_{K,v}/\pi^{n-1}\mathcal{O}_{K,v}.$$

As a consequence, we have $|\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}| = |k||\mathcal{O}_{K,v}/\pi^{n-1}\mathcal{O}_{K,v}|$. Using induction arguments yields the expression $|\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}| = |k|^n$. Therefore $\mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}$ is compact for every $n \geq 0$, since every open covering must already be finite. By Tychonoff's theorem we therefore find that $\prod_{n=0}^{\infty} \mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}$ is compact. Now notice that $\varprojlim_n \mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}$ is a closed subset of the compact space $\prod_{n=0}^{\infty} \mathcal{O}_{K,v}/\pi^n\mathcal{O}_{K,v}$, and therefore is itself compact. Thus by (1.2) the closed unit ball $\mathcal{O}_{K,v}$ is a compact subset of K.

For $y \in K$, we have a continuous translation map $x \mapsto x + y$ on K mapping $\mathcal{O}_{K,v}$ to $B[y,1]$. As a consequence, we see that y is contained in the compact closed ball $B[y,1]$. This immediately implies that K is locally compact. ■

Theorem 1.4.6. *Suppose that $(K, |\cdot|_v)$ is a normed global field, with non-trivial absolute value $|\cdot|_v$. Then the completion K_v of K with respect to $|\cdot|_v$ is locally compact.*

Proof. In this proof we will distinguish between the case that $|\cdot|_v$ is Archimedean, and the case that it is non-Archimedean.

- Suppose that $|\cdot|_v$ is Archimedean. By [Kna07, Prop.6.14], we know that fields K with an Archimedean absolute value have characteristic zero. Thus the prime field of K is isomorphic to $\mathbb{Q}$. Therefore K has to be a finite extension of $\mathbb{Q}$, since it is a global field. Let $|\cdot|_{K_v}$ be the corresponding absolute value of the completion K_v of K with respect to $|\cdot|_v$. Note that the Archimedean property is preserved under taking completions, and thus $(K_v, |\cdot|_{K_v})$ is a complete field with a non-trivial Archimedean absolute value. Ostrowski's Theorem [Neu99, Thm.II.4.2] states that $(K_v, |\cdot|_{K_v})$ is either isomorphic to $\mathbb{R}$ or $\mathbb{C}$ together with the standard absolute value, often denoted as $|\cdot|_\infty$. Since both $(\mathbb{R}, |\cdot|_\infty)$ and $(\mathbb{C}, |\cdot|_\infty)$ are locally compact, we find that the completion K_v of K with respect to the Archimedean absolute value is also locally compact.

- Suppose that $|\cdot|_v$ is non-Archimedean. Every non-Archimedean absolute value on a global field is discrete[2], meaning that $|K^\times|_v$ is a discrete subgroup of the multiplicative group $(\mathbb{R}_{>0}, \cdot)$. By the proof of Lemma 1.3.6 we know that every discrete subgroup of $(\mathbb{R}, +)$ is infinite cyclic. Therefore the group isomorphism $\psi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$ implies that every discrete subgroup of $(\mathbb{R}_{>0}, \cdot)$ is also infinite cyclic. Since $|\cdot|_v$ is non-trivial we now know that $|K^\times|_v = r^{\mathbb{Z}}$ for some $r > 1$, and a corresponding valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ can be given by $v(0) = \infty$ and $v(x) = -\log_r |x|_v$. Note that the value group of v is given by $\mathbb{Z}$, and thus v is a discrete valuation. By Lemma 1.3.8 we see that the restriction of v to L also defines a non-trivial valuation that is discrete. Recall that K is a finite extension of $L = \mathbb{Q}$ or $L = \mathbb{F}_p(t)$ for some prime p. Since $|\cdot|_v$ is induced by a non-trivial discrete valuation, Lemma 1.4.4 implies that the residue field k_K is a finite extension of k_L. We now consider the two distinct possibilities for the subfield L.

  - K is a finite extension of $L = \mathbb{Q}$. Ostrowski's Theorem [Kna07, Thm.6.15] implies that the non-Archimedean absolute value $|\cdot|_{v_{|L}}$ is equivalent to the p-adic absolute value $|\cdot|_p$ for some prime p. Therefore, the valuation ring $\mathcal{O}_{L,v_{|L}}$ is given by $\mathbb{Z}_{(p)}$ (see Example 1.3.5), with corresponding maximal ideal $(p)_{(p)}$. Note that we have a short exact sequence

$$0 \to (p) \to \mathbb{Z} \to \mathbb{Z}/(p) \to 0$$

    and, since taking localizations is an exact functor, the sequence

$$0 \to (p)_{(p)} \to \mathbb{Z}_{(p)} \to (\mathbb{Z}/(p))_{(p)} \to 0$$

    is also exact. This means that $\mathbb{Z}_{(p)}/(p)_{(p)} \cong (\mathbb{Z}/(p))_{(p)} \cong \mathbb{Z}/(p)$. Therefore the residue field of L, denoted as $k_L = \mathcal{O}_{L,v_L}/\mathfrak{m}_{v_{|L}} \cong \mathbb{Z}/(p)$ is finite.

[2] That every non-Archimedean absolute value on a global field is discrete can be found in Cor.6.21 and 6.22 of [Kna07]

- K is a finite extension of $L = \mathbb{F}_p(t)$ for some prime p. As mentioned in Remark 1.1.9, the absolute value $|\cdot|_{v_{|L}}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_\pi$ for some monic irreducible $\pi(t) \in \mathbb{F}_p[t]$. By example 1.3.5 we know that for the π-adic absolute value the valuation ring is given by $\mathcal{O}_{L,v_{|L}} = \mathbb{F}_p[t]_{(\pi(t))}$. Similarly as for the p-adic absolute value on $\mathbb{Q}$ we find that the residue field

  $$k_L = \mathbb{F}_p[t]_{(\pi(t))}/(\pi(t))_{(\pi(t))} \cong (\mathbb{F}_p[t]/(\pi(t)))_{(\pi(t))} \cong \mathbb{F}_p[t]/(\pi(t)) \cong \mathbb{F}_{p^{\deg(\pi)}}$$

  is finite. The valuation ring of L with respect to the absolute value $|\cdot|_\infty$ is given by

  $$\mathcal{O}_{L,v_{|L}} = \left\{ \frac{f(t)}{g(t)} \;\middle|\; \deg(f(t)) \leq \deg(g(t)),\ f(t), g(t) \in \mathbb{F}_p[t] \right\}.$$

  Note that every $f(t)/g(t) \in \mathcal{O}_{L,v_{|L}}$ can be written as $\frac{f(t)}{g(t)} = \frac{f_d t^d + f_{d-1}t^{d-1} + ... + f_0}{t^d + g_{d-1}t^{d-1} + ... + g_0}$ for some $f_i, g_i \in \mathbb{F}_p$, where $d = \deg(g(t))$. Define the map

  $$\varphi : \mathcal{O}_{L,v_{|L}} \to \mathbb{F}_p,\ \frac{f(t)}{g(t)} \mapsto f_d.$$

  This is a well-defined surjective ring homomorphism, with $\ker(\varphi) = \mathfrak{m}_{v_{|L}}$. Therefore we find that $k_L \cong \mathbb{F}_p$.

The above shows that the residue fields k_L of the subfield $L \subset K$ are finite. And therefore by the earlier mentioned property that k_K is a finite extension of k_L, we conclude that k_K is also finite. To apply Lemma 1.4.5, we need to know that the residue field of the completion K_v of K is also finite. For this we observe that we have an isomorphism $k_K = \mathcal{O}_{K,v}/\mathfrak{m}_v \cong \widehat{\mathcal{O}}_{K,v}/\widehat{\mathfrak{m}}_v$, see [AM69, Cor.10.4]. Lemma 1.4.3 now implies that $k_K \cong \widehat{\mathcal{O}}_{K,v}/\widehat{\mathfrak{m}}_v \cong \mathcal{O}_{K_v}/\mathfrak{m}_{K_v} = k_{K_v}$. Thus by Lemma 1.4.5 we find that the completion K_v of K with respect to $|\cdot|_v$ is indeed locally compact.

■

1.5 Lattices

Before we can go to some main properties of algebraic number fields, we give a brief discussion of a requisite part of the foundation of algebraic number theory. Namely, the theory about lattices inside a real vector space. Besides giving the definition of a lattice, we also introduce a method to associate a volume to those lattices, with respect to a certain symmetric bilinear form. This discussion is based on [Neu99, CH.I.4].

Definition 1.5.1. Let V be a n-dimensional $\mathbb{R}$-vector space. A *lattice* in V is a subgroup of the form

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

with linearly independent vectors $v_1, ..., v_m$ of V. The m-tuple $(v_1, ..., v_m)$ is called a *basis* and the set

$$F = \{x_1 v_1 + ... + x_m v_m \mid 0 \leq x_i < 1\}$$

a *fundamental domain*. This lattice is said to have *full rank* if $m = n$.

One easily checks that the fundamental domain F corresponding to a full lattice Γ satisfies

$$V = \bigcup_{\gamma \in \Gamma} (F + \gamma),$$

with $(F + \gamma) \cap (F + \gamma') = \emptyset$ if $\gamma \neq \gamma'$.

A *bilinear form* on V is a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ such that

$$\langle av + bw, v' \rangle = a\langle v, v' \rangle + b\langle w, v' \rangle,$$
$$\langle v, av' + bw' \rangle = a\langle v, v' \rangle + b\langle v, w' \rangle,$$

for all $v, v', w, w' \in V$ and $a, b \in \mathbb{R}$. In other words, $\langle \cdot, \cdot \rangle$ is linear in both variables. It is moreover called *symmetric* if $\langle v, w \rangle = \langle w, v \rangle$ for all $v, w \in V$, and it is said to be *positive definite* if $\langle v, v \rangle \geq 0$ for all $v \in V$, with equality if and only if $v = 0$.

If such a vector space possesses a symmetric positive definite bilinear form

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R},$$

then a notion of volume on V is induced. For a parallelepiped

$$F = \{x_1 v_1 + ... + x_n v_n \; | 0 \leq x_i < 1\}$$

spanned by $v_1, v_2, ..., v_n$, the volume is defined by

$$\text{vol}(F) := |\det\left((\langle v_i, v_j \rangle)_{i,j=1}^n\right)|^{1/2} \text{vol}([0,1]^n) = |\det\left((\langle v_i, v_j \rangle)_{i,j=1}^n\right)|^{1/2}.$$

Note that the volume here is calculated with respect to the unique Haar measure giving the unit cube volume 1.

Similarly, for a full lattice Γ spanned by $v_1, v_2, ..., v_n$ we define $\text{vol}(\Gamma) := \text{vol}(F)$, where F is the corresponding fundamental domain. The thing we have to check is whether this notion of volume depends on the chosen set of spanning vectors $\{v_1, v_2, ..., v_n\}$. Let $\{w_1, ..., w_n\}$ be another basis for Γ, then we have $v_i = \sum_{j=1}^n \lambda_{ij} w_j$ for some $\lambda_{ij} \in \mathbb{Z}$. If we write $\Lambda := (\lambda_{ij})_{i,j=1}^n$, then we find by easy calculations that

$$\Lambda(\langle w_i, w_j \rangle)_{i,j=1}^n \Lambda^T = (\langle v_i, v_j \rangle)_{i,j=1}^n.$$

Note that the transition matrix Λ has integer coefficients, as well as its inverse. The observation that can now be made is that $\det(\Lambda), \det(\Lambda^{-1}) \in \mathbb{Z}$, and thus $\det(\Lambda) = \pm 1$. Combining this with the above yields,

$$|\det(\langle v_i, v_j \rangle)_{i,j=1}^n|^{1/2} = |\det(\Lambda(\langle w_i, w_j \rangle)_{i,j=1}^n \Lambda^T)|^{1/2} = |\det(\langle w_i, w_j \rangle)_{i,j=1}^n|^{1/2}.$$

1.6 Arithmetic on Number Fields

An algebraic number field is a finite field extension of $\mathbb{Q}$, as we have seen before. Since these are the types of fields mainly considered in this paper, we will restrict to them unless stated otherwise. The leading source for this section is [Sut15]. We start by introducing an extension of the ideal concept. For this we assume R to be a domain with field of fractions K. In the case that R is a subring of a number field K, we call R a *number ring*. For a commutative ring R, an R-ideal is the same as a subset of R that is an R-module. For such ideals we have the notion of ideal division. We say that an ideal I divides J if there exists an ideal I_0 of R such that $II_0 = J$. Since the domain R is contained in its field of fractions K, division of non-zero elements of R can be performed inside K. A natural extension of R-ideals for a domain R can now be given.

Definition 1.6.1. Let R be domain inside its field of fractions K. Then a *fractional R-ideal* I is a non-zero R-submodule of K such that $xI \subset R$ for some $x \in K^\times$.

In some circumstances it is convenient to take the element x from the above definition to lie in R. It is clear that this can always be done. The word "fractional" is justified by the fact that such a fractional R-ideal I is contained in $x^{-1}R$ for some $x \in K^\times$. In other words, it consists of fractions $x^{-1}r$ for some $r \in R$. In particular, the usual R-ideals are fractional ideals. To distinguish them, we call fractional R-ideals I that are contained in R *integral*. Any element $x \in K^\times$ generates a fractional R-ideal, namely xR. These type of ideals are also called *principal* fractional R-ideals.

For arbitrary fractional ideals I and J we have the so-called *ideal quotient*, which consists of all $x \in K$ such that $xJ \subset I$. This set is denoted by $I : J$, and also defines a fractional R-ideal. Other operations possible between fractional R-ideals are: the sum $I + J$, the product IJ, and the intersection $I \cap J$. The importance of the ideal quotients is clarified by the ideal quotient $R : I$, which is denoted by I^{-1}. To substantiate the notation I^{-1}, we consider the notion of *invertible* fractional R-ideals. A fractional R-ideal I is said to be invertible if there exists a fractional R-ideal J such that $IJ = R$. Moreover, if this is the case, then one can show that $J = I^{-1}$. Thus an equivalent way to define invertible fractional R-ideals, is by calling a fractional R-ideal I invertible if $II^{-1} = R$.

We denote $\mathcal{I}(R)$ for the set of invertible fractional R-ideals. This set forms a group under ideal multiplication. Moreover, the set $\mathcal{P}(R)$ of principal fraction R-ideals forms a subgroup of $\mathcal{I}(R)$.

Lemma 1.6.2. *Let R be a domain with field of fractions K and $\mathcal{P}(R)$ be the group of principal fractional R-ideals. Then $\mathcal{P}(R)$ is canonically isomorphic to $K^\times/R^\times$.*

Proof. Note that we have a natural surjective group homomorphism

$$\varphi : K^\times \to \mathcal{P}(R), \; x \mapsto xR,$$

with kernel $R^\times$. Therefore, we get by the first isomorphism theorem for groups that $K^\times/R^\times$ is isomorphic to $\mathcal{P}(R)$. ■

The quotient of the groups $\mathcal{I}(R)$ and $\mathcal{P}(R)$ is a way to measure the principality of the invertible fractional R-ideals. This group is also called the *Picard group* of R, and denoted as $\mathrm{Pic}(R)$.

Another topic of interest is whether any invertible fractional R-ideal can uniquely be written as product of powers of prime ideals. In general, this appears not to be true. Nevertheless, for Dedekind domains R this is achievable. Recall that a *Dedekind domain* is a domain R that satisfies one of the following equivalent conditions:

Proposition 1.6.3. (cf. [CF67, Prop.1, p.6]) *Let R be a domain. The following are equivalent:*

(i) R is a one-dimensional integrally closed Noetherian domain.

(ii) R is Noetherian, and for every non-zero prime ideal $\mathfrak{p}$, the local ring $R_\mathfrak{p}$ is a discrete valuation ring.

(iii) All fractional R-ideals are invertible.

As proven in [Ste20, Cor.2.12] number rings are Noetherian, and every non-zero prime ideal is maximal. Thus a number ring is a Dedekind domain if and only if for every non-zero prime ideal $\mathfrak{p}$, the corresponding local ring $R_\mathfrak{p}$ is a discrete valuation ring. This suggests that we have to consider the behaviour of the fractional R-ideals inside the localizations. For simplicity, when considering a one-dimensional domain R, we call the non-zero prime ideals the *primes* of R. We note that for primes $\mathfrak{p}$ of R, the localizations $I_\mathfrak{p}$ of a fractional ideal I define fractional $R_\mathfrak{p}$-ideals. Moreover, the localizations respect the arithmetic discussed before for fractional ideals. To rephrase it, for primes $\mathfrak{p}$ of R and fractional R-ideals I and J, we have

$$(I+J)_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p},\ (IJ)_\mathfrak{p} = I_\mathfrak{p}J_\mathfrak{p},\ (I:J)_\mathfrak{p} = (I_\mathfrak{p} : J_\mathfrak{p}).$$

The following proposition gives a characterization of the fractional R-ideals for a discrete valuation ring R.

Proposition 1.6.4. *Let R be a discrete valuation ring with uniformizer π. Then the fractional R-ideals are precisely given by $\pi^k R$ for $k \in \mathbb{Z}$. Moreover, they are clearly distinct.*

Proof. It is clear that for every $k \in \mathbb{Z}$ the R-submodule $\pi^k R$ of K defines a fractional R-ideal. Now let I be an arbitrary fractional R-ideal. Then there exists $x \in K^\times$ such that xI is an integral R-ideal. Since R is a discrete valuation ring, Theorem 1.3.7 implies that $xI = \pi^n R$ for some $n \geq 0$. Moreover, there exists a unit $u \in R^\times$ and unique $k \in \mathbb{Z}$ such that $x = u \cdot \pi^k$. As a consequence, we find that $I = \pi^{n-k}R$. ■

The proposition above induces a way to associate a value to an arbitrary fractional R-ideal for Dedekind domains R. Namely, for each fractional ideal I of R, the localization $I_\mathfrak{p}$ defines a fractional ideal of the discrete valuation ring $R_\mathfrak{p}$ for each prime $\mathfrak{p}$ of R. Therefore, $I_\mathfrak{p} = (\pi^k)$ for some unique $k \in \mathbb{Z}$ and uniformizer $\pi \in R_\mathfrak{p}$. Moreover, in a Dedekind domain every fractional ideal is invertible. And thus the set of fractional ideals equals the group of invertible ideals denoted by $\mathcal{I}(R)$. The natural group homomorphism that arises for a prime $\mathfrak{p}$ of R is the map $v_\mathfrak{p} : \mathcal{I}(R) \to \mathbb{Z}$ given by $v_\mathfrak{p}(I) := k$. Moreover, this map is clearly order-reversing. Thus for any $I, J \in \mathcal{I}(R)$ with $I \subset J$, we have $I_\mathfrak{p} \subset J_\mathfrak{p}$ and in particular $v_\mathfrak{p}(I) \geq v_\mathfrak{p}(J)$. By means of this map the unique prime ideal factorization on a Dedekind domain is now obtained.

Theorem 1.6.5. (cf. [Sut15, Thm.3.23]) *Let R be a Dedekind domain. Then there is an isomorphism*

$$\mathcal{I}(R) \xrightarrow{\sim} \bigoplus_{\substack{\mathfrak{p} \subset R \\ prime}} \mathbb{Z}$$
$$I \mapsto (v_\mathfrak{p}(I))_\mathfrak{p},$$

and every $I \in \mathcal{I}(R)$ can be uniquely written as the product $I = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(I)}$.

A number ring that plays a central role in the algebraic number theory, is the *ring of integers* of a number field K. This ring is defined as the integral closure of $\mathbb{Z}$ in K, and denoted as $\mathcal{O}_K$. Thus,

$$\mathcal{O}_K = \{x \in K \mid \text{there exists a monic } f \in \mathbb{Z}[X] \text{ such that } f(x) = 0\}.$$

As mentioned before, a number ring is a one-dimensional Noetherian domain. To be a Dedekind domain, the number ring is demanded to be integrally closed. For the ring of integers of a number field, this is the case by definition. The unique prime factorization on $\mathcal{O}_K$ induces a valuation on K. Namely, for each prime $\mathfrak{p}$ in $\mathcal{O}_K$ we have a so-called $\mathfrak{p}$-*adic valuation*, which is a generalized version of the p-adic valuations on $\mathbb{Q}$.

Proposition 1.6.6. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. For $x \in \mathcal{O}_K \backslash \{0\}$, define $v_\mathfrak{p}(x) := n$ where $x\mathcal{O}_K = \mathfrak{p}^n I$ for some $n \geq 0$ and ideal I satisfying $\mathfrak{p} \not| I$. Moreover, extend this definition to K by*

$$v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\},\ \alpha \mapsto \begin{cases} v_\mathfrak{p}(x) - v_\mathfrak{p}(y) & \text{if } \alpha = \frac{x}{y} \\ \infty & \text{if } \alpha = 0. \end{cases}$$

Then $v_\mathfrak{p}$ defines a discrete valuation on K, which is called the $\mathfrak{p}$-adic valuation.

Proof. By the unique prime factorization on $\mathcal{O}_K$ we clearly see that $v_\mathfrak{p}$ is a well-defined function on $\mathcal{O}_K$ that is moreover a homomorphism. To conclude well-definedness on K, assume that $\alpha \in K^\times$ equals $\frac{x}{y}$ and $\frac{x'}{y'}$ for some $x, x', y, y' \in \mathcal{O}_K \backslash \{0\}$. In that case we have $xy' = x'y$, and thus

$$v_\mathfrak{p}(x) + v_\mathfrak{p}(y') = v_\mathfrak{p}(xy') = v_\mathfrak{p}(x'y) = v_\mathfrak{p}(x') + v_\mathfrak{p}(y).$$

This implies that $v_\mathfrak{p}(\frac{x}{y}) = v_\mathfrak{p}(\frac{x'}{y'})$. In addition, we note that $v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta)$, which is a direct consequence of the fact that $v_\mathfrak{p}$ defines a homomorphism on $\mathcal{O}_K$.

To finish the conclusion that $v_\mathfrak{p}$ defines a valuation, we have to show that for all $\alpha, \beta \in K$ we have $v_\mathfrak{p}(\alpha+\beta) \geq \min(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta))$. The non-trivial case is when $\alpha, \beta \in K^\times$ such that $\alpha+\beta \neq 0$. Write $\alpha = \frac{x}{y}$ and $\beta = \frac{x'}{y'}$ for some $x, x', y, y' \in \mathcal{O}_K \backslash \{0\}$. Moreover, denote $\min(v_\mathfrak{p}(xy'), v_\mathfrak{p}(x'y))$ by m. Then notice that $\mathfrak{p}^m | xy'\mathcal{O}_K$ and $\mathfrak{p}^m | x'y\mathcal{O}_K$. In other words, $xy', x'y \in \mathfrak{p}^m$ which implies that $xy' + x'y \in \mathfrak{p}^m$. Thus we find that

$$v_\mathfrak{p}(xy' + x'y) \geq \min(v_\mathfrak{p}(xy'), v_\mathfrak{p}(x'y)).$$

By using this property, we acquire the desired inequality

$$\begin{aligned} v_\mathfrak{p}(\alpha+\beta) = v_\mathfrak{p}\left(\frac{xy'+x'y}{yy'}\right) &\geq \min(v_\mathfrak{p}(xy'), v_\mathfrak{p}(x'y)) - v_\mathfrak{p}(yy') \\ &= \min(v_\mathfrak{p}(xy') - v_\mathfrak{p}(yy'), v_\mathfrak{p}(x'y) - v_\mathfrak{p}(yy')) = \min(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta)). \end{aligned}$$

The surjectivity can be obtained from the fact that for every $x \in \mathfrak{p} \backslash \mathfrak{p}^2$ we have $v_\mathfrak{p}(x) = 1$. ■

Those $\mathfrak{p}$-adic valuations induce corresponding absolute values. Namely, by fixing a $c \in \mathbb{R}_{>1}$ and defining $|\alpha|_\mathfrak{p} := c^{-v_\mathfrak{p}(\alpha)}$ and $|0|_\mathfrak{p} = 0$. On $\mathbb{Q}$ we had a way to classify all the equivalent non-zero absolute values by p-adic absolute values, formulated in Remark 1.1.9. On number fields, a generalized version of this statement is true.

Theorem 1.6.7. (cf. [Con10, Thm.3.3]) *Every non-trivial non-Archimedean absolute value on K is equivalent to a $\mathfrak{p}$-adic valuation for a unique prime $\mathfrak{p}$ of $\mathcal{O}_K$. Moreover, each non-trivial Archimedean absolute value on K is equivalent to an absolute value induced by a real or complex embedding of K into $\mathbb{C}$.*

These $\mathfrak{p}$-adic valuations satisfy an approximation property.

Theorem 1.6.8 (The Strong Approximation Theorem)**.** (cf. [Kna07, Thm.6.44]) *Let K be a number field, and $\mathcal{O}_K$ be its ring of integers. Moreover, let $\mathfrak{p}_1, ..., \mathfrak{p}_r$ be non-zero prime ideals in $\mathcal{O}_K$ with corresponding valuations v_i on K and the completion K_{v_i}. If $e_1, ..., e_r$ are in $\mathbb{Z}$ and if $x_i \in K_{v_i}$ for all $1 \leq i \leq r$, then there exists a $y \in K$ such that*

$$\begin{aligned} v_i(\iota_{v_i}(y) - x_i) &\geq e_i \textit{ for } 1 \leq i \leq r \\ v_\mathfrak{q}(\iota_{v_\mathfrak{q}}(y)) &\geq 0 \textit{ for all other non-zero primes } \mathfrak{q}. \end{aligned}$$

It is sometimes convenient to take a certain normalization of the corresponding absolute values. To each place corresponds a specific choice of normalization. For Archimedean places $v \in M_K^\infty$, we recall that a number field K of degree n, comes together with r_1 real embeddings and r_2 pairs of complex embeddings such that $r_1 + 2r_2 = n$. Let $\{\sigma_i\}_{i=1}^{r_1+r_2}$ be a complete set of pairwise non-conjugate embeddings, ordered in such a way that σ_i is a real embedding for $1 \leq i \leq r_1$. This are the embeddings that induce all pairwise inequivalent Archimedean absolute values. We define the *normalized absolute values* as follows:

$$\|\cdot\|_v : K \to \mathbb{R}_{\geq 0},\ x \mapsto \begin{cases} |\sigma_i(x)|_\mathbb{R} & 1 \leq i \leq r_1, \\ |\sigma_i(x)|_\mathbb{C}^2 & r_1 + 1 \leq r_1 + r_2 \\ |x|_\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|^{-v_\mathfrak{p}(x)} & \mathfrak{p} \subset \mathcal{O}_K \text{ prime,} \end{cases} \tag{1.3}$$

where $|\cdot|_{\mathbb{R}}$ and $|\cdot|_{\mathbb{C}}$ denote the standard absolute values, and $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation. Note that for complex places $v \in M_K^\infty$, the normalized absolute value is actually not an absolute value. Namely, it does not satisfy the triangle inequality. Nevertheless, it is still convenient to call it an absolute value. To simplify notation, we will mostly write the normalizations as $|\cdot|_v$. It will be clear from the context whether we are working with the normalizations or not. To substantiate the chosen normalizations, we give one of the most important properties.

Theorem 1.6.9 (Product Formula). *Let K be a number field, and $|\cdot|_v$ be the normalized absolute value corresponding to a place v, then*

$$\prod_{v \in M_K} |x|_v = 1$$

for all $x \in K^\times$.

Let L/K be a finite field extension, which means that L can be viewed as a finite dimensional K-vector space. For $x \in L$, let $T_x : L \to L$ be the K-linear multiplication map $\alpha \mapsto x\alpha$, which can be described by a matrix with coefficients in K. As a consequence, we obtain a trace and norm map on the field extension.

Definition 1.6.10. Let L/K be a field extension of degree n. For $x \in L$, let T_x be the multiplication map as stated above. Then the *trace* and *norm* of x are respectively given by

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \;\; N_{L/K}(x) = \det(T_x).$$

It is easily seen from the properties of the trace and determinant, that $\mathrm{Tr}_{L/K}$ defines a homomorphism between L and K, and $N_{L/K}$ gives a homomorphism between $L^\times$ and $K^\times$.

Example 1.6.11. Consider the field extension $\mathbb{C}/\mathbb{R}$ of degree 2. For $z = a + bi \in \mathbb{C}$, we have

$$T_z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

implying that

$$N_{\mathbb{C}/\mathbb{R}}(z) = a^2 + b^2 = |z|^2.$$

Together with the $n \times n$ matrix T_x comes the corresponding *characteristic polynomial*

$$f^x_{L/K}(X) = \det(X \cdot \mathrm{id}_L - T_x) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in K[X],$$

where $a_{n-1} = -\mathrm{Tr}_{L/K}(x)$ and $a_0 = (-1)^n N_{L/K}(x)$. For separable finite extensions L/K, this polynomial can be described by using the K-embeddings L into $\overline{K}$. We moreover obtain an additional way to compute the trace and norm of an element $x \in L$ based on the set $\mathrm{Hom}_K(L, \overline{K})$ of cardinality $[L : K]$.

Proposition 1.6.12. (cf. [Neu99, Prop.I.2.6]) *If L/K is a finite separable extension, then*

(i) $f^x_{L/K}(X) = \prod_{\sigma \in Hom_K(L,\overline{K})}(X - \sigma(X))$,

(ii) $Tr_{L/K}(x) = \sum_{\sigma \in Hom_K(L,\overline{K})} \sigma(x)$,

(iii) $N_{L/K}(x) = \prod_{\sigma \in Hom_K(L,\overline{K})} \sigma(x)$.

Staying in the situation of a separable extension L/K, we obtain another fundamental invariant from the trace map, called the *discriminant*.

Definition 1.6.13. Let L/K be a separable extension of degree n with basis $x_1, ..., x_n$. Then the *discriminant* of this basis is given by

$$\Delta(x_1, ..., x_n) = \det\left(\mathrm{Tr}_{L/K}(x_i x_j)\right)_{i,j=1}^n.$$

We observe that under these circumstances the discriminant depends on the chosen basis. Namely, let $y_1, ..., y_n$ be another basis defined by $y_i = \sum_{j=1}^n \lambda_{ij} x_j$ for some invertible matrix $\Lambda = (\lambda_{ij})_{i,j=1}^n \in \mathrm{GL}_n(K)$. Then we get

$$\begin{aligned}\Delta(y_1, ..., y_n) &= \det\left(\mathrm{Tr}_{L/K}(y_i y_j)\right)_{i,j=1}^n = \det\left(\sum_{k=1}^n \lambda_{ik}\mathrm{Tr}_{L/K}(x_k x_l)\sum_{l=1}^n \lambda_{jl}\right)_{i,j=1}^n \\ &= \det\left(\Lambda\left(\mathrm{Tr}_{L/K}(x_i x_j)\right)_{i,j=1}^n \Lambda^T\right) = \det(\Lambda)^2\Delta(x_1, ..., x_n). \qquad (1.4)\end{aligned}$$

As a consequence of Proposition 1.6.12 we get the following equivalent way of determining the discriminant of a basis.

Proposition 1.6.14. *Let L/K be a separable extension of degree n. Moreover, let $\sigma_1, ..., \sigma_n \in$ $Hom_K(L, \overline{K})$ be the K-embeddings of L in $\overline{K}$. Then one has*

$$\Delta(x_1, ..., x_n) = \left(\det(\sigma_i(x_j))_{i,j=1}^n\right)^2$$

for every basis $x_1, ..., x_n$ of L/K.

Proof. Write $X := (\sigma_i(x_j))_{i,j=1}^n$, and multiply this matrix by its transpose. If we moreover apply the description of the trace map from Proposition 1.6.12, then we find

$$X^T \cdot X = \left(\sum_{k=1}^n \sigma_k(x_i x_j)\right)_{i,j=1}^n = \left(\mathrm{Tr}_{L/K}(x_i x_j)\right)_{i,j=1}^n.$$

Taking the determinant on both sides of this equation, hands us the desired result. ■

Now let A be an integrally closed domain with field of fractions K, and B the integral closure of A in the finite separable extension L of K. With an *integral basis*, we mean a system of elements $\omega_1, ..., \omega_n \in B$ such that each $b \in B$ can be uniquely written in the form

$$b = a_1\omega_1 + ... + a_n\omega_n$$

for some $a_i \in A$. Note that such an integral basis also clearly defines a K-basis for L. It therefore makes sense to take the discriminant of such an integral basis. One of the main applications of this discussion, is the integral closure $\mathcal{O}_K \subset K$ of the integers $\mathbb{Z} \subset \mathbb{Q}$ for some algebraic number field K.

Proposition 1.6.15. (cf. [Neu99, Prop.I.2.10]) *If K is a number field of degree n, then there exists an integral basis $\omega_1, ..., \omega_n$ for $\mathcal{O}_K$ over $\mathbb{Z}$, for which we have*

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + ... + \mathbb{Z}\omega_n.$$

Now let $\omega_1', ..., \omega_n'$ be another integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$, then $\omega_i' = \sum_{j=1}^n \lambda_{ij}\omega_j$ for some $\Lambda = (\lambda_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$. By the observation that $\det(\Lambda), \det(\lambda)^{-1} \in \mathbb{Z}$, we see that $\det(\Lambda) = \pm 1$. Implementing this into (1.4), we find that

$$\Delta(\omega_1', ..., \omega_n') = (\det(\Lambda))^2\Delta(\omega_1, ..., \omega_n) = \Delta(\omega_1, ..., \omega_n).$$

This shows that the discriminant is independent of the chosen $\mathbb{Z}$-basis. As a consequence, we can define the discriminant of a number field in a unique way.

Definition 1.6.16. Let K be a number field, and $\omega_1, ..., \omega_n$ an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$. The *discriminant* of a number field is defined by

$$\Delta_K = \Delta(\mathcal{O}_K) = \Delta(\omega_1, ..., \omega_n).$$

Another result that can be obtained from the existence of an integral basis for $\mathcal{O}_K$ over $\mathbb{Z}$, is that any non-zero ideal of $\mathcal{O}_K$ has finite index.

Proposition 1.6.17. (cf. [Kna07, Prop.5.3]) *Let I be a non-zero ideal of $\mathcal{O}_K$. Then I has finite index in $\mathcal{O}_K$, i.e., $[\mathcal{O}_K : I] = |\mathcal{O}_K/I| < \infty$.*

Proof. Let K be a number field of degree $m \geq 1$, and I a non-zero ideal of $\mathcal{O}_K$. Moreover, pick a non-zero element $x \in I$. Since x is in $\mathcal{O}_K$, it satisfies a monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0,$$

for some $a_i \in \mathbb{Z}$. Consequently, we see that

$$a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1),$$

which in particular implies that $a = |a_0|$ is a positive integer contained in I. We thus have the chain of inclusions $a\mathcal{O}_K \subset I \subset \mathcal{O}_K$. This hands us a surjective map between $\mathcal{O}_K/a\mathcal{O}_K$ and $\mathcal{O}_K/I$. Thus, to show that $\mathcal{O}_K/I$ is finite, it suffices to prove that $\mathcal{O}_K/a\mathcal{O}_K$ is finite. For this, we consider the set

$$S_a := \left\{ \sum_{i=1}^{m} b_i \omega_i \;\middle|\; 0 \leq b_i < a \right\},$$

and we will show that this forms a complete set of coset representatives for $\mathcal{O}_K/a\mathcal{O}_K$. Here the ω_i are taken as an integral basis of $\mathcal{O}_K$, which exists by Proposition 1.6.15. We thus want to show that the map

$$\varphi : S_a \to \mathcal{O}_K/a\mathcal{O}_K, \; s \mapsto [s]$$

is bijective. To prove surjectivity, we pick an arbitrary $x \in \mathcal{O}_K$. Since $\{\omega_1, ..., \omega_m\}$ is an integral basis of $\mathcal{O}_K$, there exists $a_1, ..., a_m \in \mathbb{Z}$ such that $x = \sum_{i=1}^m a_i\omega_i$. By Euclid's division lemma there exists integers q_i and r_i suh that $a_i = aq_i + r_i$ with $0 \leq r_i < a$. Then we obtain

$$x = \sum_{i=1}^{m} a_i\omega_i = a\sum_{i=1}^{m} q_i\omega_i + \sum_{i=1}^{m} r_i\omega_i.$$

After observing that $\sum_{i=1}^m r_i\omega_i$ is in S_a, we see that

$$\varphi\left(\sum_{i=1}^{m} r_i\omega_i\right) = [x].$$

We are left to prove the injectivity of φ. Suppose that $\varphi(s) = \varphi(s')$, i.e.,

$$s = \sum_{i=1}^{m} b_i\omega_i = \sum_{i=1}^{m} b_i'\omega_i + a\sum_{i=1}^{m} c_i\omega_i = s' + a\sum_{i=1}^{m} c_i\omega_i,$$

for some $c_i \in \mathbb{Z}$. Since the ω_i form an integral basis, this immediately implies that $b_i - b_i' = ac_i$. This in particular means that $a|(b_i - b_i')$. By the condition that $0 \leq b_i, b_i' < a$, we now obtain that $b_i = b_i'$. In other words, φ is injective. By construction of S_a, and by summarizing the obtained results, we have

$$|\mathcal{O}_K/I| \leq |\mathcal{O}_K/a\mathcal{O}_K| = |S_a| = a^n.$$

■

The finiteness of this index justifies the following definition of a map on the ideals of $\mathcal{O}_K$.

Definition 1.6.18. The *absolute norm* map on the set of ideals of $\mathcal{O}_K$, denoted by $I(\mathcal{O}_K)$, is defined by

$$N : I(\mathcal{O}_K) \to \mathbb{Z}_{\geq 0}, I \mapsto \begin{cases} [\mathcal{O}_K : I] = |\mathcal{O}_K/I| & \text{if } I \neq (0) \\ 0 & \text{if } I = (0). \end{cases}$$

To clarify its name, the absolute norm map measures in some sense the size of an ideal I in $\mathcal{O}_K$. This map comes together with some useful features.

Proposition 1.6.19. (cf. [Kna07, Prop.5.4]) *The absolute norm map N on $I(\mathcal{O}_K)$ satisfies:*

(i) If $I \subset J$ are non-zero ideals in $\mathcal{O}_K$, then $N(J)$ divides $N(I)$, and $I = J$ if and only if $N(I) = N(J)$.

(ii) If I and J are non-zero ideals, then $N(IJ) = N(I)N(J)$.

(iii) If $I = (x)$ for some $x \in \mathcal{O}_K$, then $N(I) = |N_{K/\mathbb{Q}}(x)|$. This in particular means that $N(R) = 1$.

The second property gives us a canonical way to extend the norm to the set of all fractional ideals. Moreover, the third feature indicates that this norm is actually a generalization of the field norm defined at Definition 1.6.10.

For Dedekind domains, the Picard group $\text{Pic}(R)$ is also called the *ideal class group* of R and represented by $\text{Cl}(R)$. The class group of a number field K is defined to be the class group of $\mathcal{O}_K$, i.e.,

$$\text{Cl}(K) = \text{Cl}(\mathcal{O}_K),$$

and its order is known to be finite.

Theorem 1.6.20. (cf. [Neu99, Thm.I.6.3]) *The ideal class group of a number field K is finite. Furthermore, the order*

$$h_K = \#\text{Cl}(K)$$

is called the class number of K.

Aside from the class group of the ring of integers, another inevitable mathematical invariant of interest is the group of units of $\mathcal{O}_K$. This group itself is not always finite, but it appears to be finitely generated of a certain rank. This rank depends on the number of real and complex embeddings of K into $\mathbb{C}$. Note that the number of distinct embeddings of a number field K into $\mathbb{C}$ is precisely the degree $n = [K : \mathbb{Q}]$. This is an easy consequence of the Primitive Element theorem. Such an embedding is called real if it is completely mapped into $\mathbb{R}$, and called complex otherwise. Let r_1 be the number of real embeddings, and r_2 be the number of pairs of complex conjugate embeddings. In that case, we have $n = r_1 + 2r_2$. The classical formulation of the fact that $\mathcal{O}_K^\times$ is finitely generated is as follows.

Theorem 1.6.21 (Dirichlet's Unit Theorem)**.** (cf. [Neu99, Thm.I.7.4]) *The group of units $\mathcal{O}_K^\times$ of the ring of integers of a number field K is a finitely generated abelian group of the form*

$$\mathcal{O}_K^\times \cong (\mathcal{O}_K^\times)_{tors} \times \Gamma,$$

where $(\mathcal{O}_K^\times)_{tors}$ is the finite group consisting of roots of unity contained in K, and Γ is a free abelian group of rank $r_1 + r_2 - 1$.

1.7 Ideal Factorization on Extensions of Dedekind Domains.

In the previous section, we have discussed ideal factorizations on a Dedekind domain. We can expand this theory by considering the relations between prime ideal factorizations in extensions of Dedekind domains. In general, the setting is a Dedekind domain A, its field of fractions K, a finite separable field extension L/K, and the integral closure B of A inside L. In particular, this integral closure is again a Dedekind domain [Neu99, Prop.I.8.1]. Nevertheless, we restrict ourselves to number fields and their corresponding ring of integers. The following lemma tells us that for a finite extension of number fields, we remain in the same situation of the general case.

Proposition 1.7.1. *Let L/K be a finite extension of number fields. Then the integral closure C of $\mathcal{O}_K$ inside L equals the ring of integers $\mathcal{O}_L$.*

Proof. First note that the integral closure C is defined as the set

$$C := \{x \in L \mid \text{there exists a monic } f \in \mathcal{O}_K[X] \text{ such that } f(x) = 0\}.$$

As a consequence, the inclusion $\mathcal{O}_L \subset C$ follows directly from the definitions.

For the converse, let $x \in L$ be integral over $\mathcal{O}_K$. Then $\mathcal{O}_K[x]$ is finitely generated as $\mathcal{O}_K$-module. Since $\mathcal{O}_K$ is finitely generated as $\mathbb{Z}$-module, we find that $\mathcal{O}_K[x]$ is also finitely generated as $\mathbb{Z}$-module. Thus x is integral over $\mathbb{Z}$, implying that $x \in \mathcal{O}_L$. ■

For a more detailed description of the extension of Dedekind domains, consider the reference [Neu99, CH.I.8]. Now let L/K be a finite extension of number fields, and consider the corresponding ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. We again conventionally call the non-zero prime ideals of $\mathcal{O}_K$, the *primes* of $\mathcal{O}_K$. Then for a prime $\mathfrak{p} \subset \mathcal{O}_K$ we have a corresponding proper ideal $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$. By the unique prime ideal factorization in $\mathcal{O}_L$ we find that

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{n} \mathfrak{q}_i^{e_i}$$

for some primes $\mathfrak{q}_i \subset \mathcal{O}_L$ and $e_i \geq 1$. The exponents e_i are called the *ramification indices* of the primes $\mathfrak{q}_i$ over $\mathfrak{p}$. To clarify the notation $\mathfrak{p}\mathcal{O}_L$, we define for an arbitrary ideal I in $\mathcal{O}_K$ the set

$$I\mathcal{O}_L := \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in I,\ y_i \in \mathcal{O}_L \right\}.$$

It is easily verified that this defines an ideal in $\mathcal{O}_L$. Moreover, it is called the *extension* of I to $\mathcal{O}_L$. In addition, we have a counterpart of such extensions called the restrictions of an ideal. The *restriction* of an ideal J in $\mathcal{O}_L$ to K is defined as $J \cap \mathcal{O}_K = J \cap K$, and we see that this defines an ideal in $\mathcal{O}_K$. The restriction of a non-zero ideal is again a non-zero ideal. Furthermore, the extension of a proper ideal is again a proper ideal in the extension.

Before we dive deeper into the ideal factorizations in the extensions, we give some practical algebraic properties inside the Dedekind domain $\mathcal{O}_K$.

Proposition 1.7.2. *For ideals I and J of $\mathcal{O}_K$, we have $I|J$ if and only if $J \subset I$.*

Proof. It immediately follows from the definition that if $I|J$ inside $\mathcal{O}_K$, then $J \subset I$.

For the other direction, suppose that $J \subset I$. Recall that for all primes of $\mathcal{O}_K$, the map $v_\mathfrak{p}$ on $\mathcal{I}(\mathcal{O}_K)$ is order-reversing. This means that $v_\mathfrak{p}(J) \geq v_\mathfrak{p}(I)$. And thus

$$J = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(J)} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(J)-v_\mathfrak{p}(I)} \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(I)} = I_0 I,$$

where $I_0 := \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(J)-v_\mathfrak{p}(I)}$ clearly defines an ideal of $\mathcal{O}_K$. ■

For a finite extension L/K and primes $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_L$ and $\mathcal{O}_K$, respectively, we now say that $\mathfrak{q}$ *lies above* $\mathfrak{p}$ if $\mathfrak{q}|\mathfrak{p}\mathcal{O}_L$. When considering $\mathfrak{p}$ as an ideal in $\mathcal{O}_L$, it canonically means that we have to consider $\mathfrak{p}\mathcal{O}_L$. Therefore, it is convenient to just write $\mathfrak{q}|\mathfrak{p}$ when $\mathfrak{q}$ lies above $\mathfrak{p}$. This leads to the following property that tells something about the appearance of primes in the prime ideal factorization of the extensions of primes.

Proposition 1.7.3. *Let $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathfrak{q} \subset \mathcal{O}_L$ be primes. Moreover, let $\prod_{i=1}^n \mathfrak{q}_i^{e_i}$ be the unique prime ideal factorization in $\mathcal{O}_L$. Then $\mathfrak{q}$ appears in the unique prime factorization of $\mathfrak{p}\mathcal{O}_L$ if and only if $\mathfrak{q}|\mathfrak{p}$ if and only if $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.*

Proof. We will first focus on the first equivalent statement. Suppose that $\mathfrak{q}$ is in the unique prime factorization of $\mathfrak{p}\mathcal{O}_L$. Then we immediately observe that $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$, and thus $\mathfrak{q}|\mathfrak{p}$ by Proposition 1.7.2.

Now assume that $\mathfrak{q}|\mathfrak{p}$. In that case, we have $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$. Recalling the fact that $v_\mathfrak{q}$ on $\mathcal{I}(\mathcal{O}_L)$ is order-reversing, we find that $v_\mathfrak{q}(\mathfrak{p}\mathcal{O}_L) \geq v_\mathfrak{q}(\mathfrak{q}) = 1$. In other words, $\mathfrak{q}$ appears in the unique prime factorization of $\mathfrak{p}\mathcal{O}_L$.

We are left to show that $\mathfrak{q}|\mathfrak{p}$ if and only if $\mathfrak{q}\cap\mathcal{O}_K = \mathfrak{p}$. Note that if $\mathfrak{q}|\mathfrak{p}$, we have $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$. In particular, we obtain $\mathfrak{p} \subset \mathfrak{q} \cap \mathcal{O}_K \neq \mathcal{O}_K$. But by the maximality of all the primes in a Dedekind domain, we conclude that $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$.

For the converse, we immediately note that $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$ implies that $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$. In other words, $\mathfrak{q}|\mathfrak{p}$. ■

To put the above in another way, we can write the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ in the following way

$$\mathfrak{p}\mathcal{O}_L = \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \mathfrak{q}\subset\mathcal{O}_L}} \mathfrak{q}^{e_\mathfrak{q}},$$

where $e_\mathfrak{q} \geq 1$ denotes the *ramification index* of $\mathfrak{q}$ over $\mathfrak{p}$. Observe that from this prime factorization, it follows that for every prime $\mathfrak{p}$ of $\mathcal{O}_K$, there exists a prime $\mathfrak{q}$ in $\mathcal{O}_L$ that lies above $\mathfrak{p}$. Moreover, the proposition above tells us that every prime $\mathfrak{q}$ in $\mathcal{O}_L$ lies above a unique prime $\mathfrak{p}$ in $\mathcal{O}_K$.

Corollary 1.7.4. *Let I be a proper ideal of $\mathcal{O}_K$, and $\mathfrak{q} \subset \mathcal{O}_L$ prime. Then $\mathfrak{q}|I\mathcal{O}_L$ if and only if $\mathfrak{q}|\mathfrak{p}$ for some prime $\mathfrak{p}$ in $\mathcal{O}_K$ dividing I.*

Proof. This is a direct consequence of Proposition 1.7.3. ■

Lemma 1.7.5. *Let I and J be ideals of $\mathcal{O}_K$ such that $I\mathcal{O}_L|J\mathcal{O}_L$. Then $I|J$.*

Proof. This is clearly true when either I or J equals (0) or $\mathcal{O}_K$. Therefore, we can assume I and J to be proper non-zero ideals of $\mathcal{O}_K$. Then notice that

$$I\mathcal{O}_L = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \mathfrak{p}^{v_\mathfrak{p}(I)}\mathcal{O}_L = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \mathfrak{q}\subset\mathcal{O}_L}} \mathfrak{q}^{e_q v_\mathfrak{p}(I)} = \prod_{\mathfrak{q}\subset\mathcal{O}_L} \mathfrak{q}^{v_q(I\mathcal{O}_L)}.$$

Since every prime $\mathfrak{q}$ in $\mathcal{O}_L$ lies above a unique prime $\mathfrak{p}$ in $\mathcal{O}_K$, we find by the uniqueness of the prime factorization that $e_{\mathfrak{q}}v_{\mathfrak{p}}(I) = v_{\mathfrak{q}}(I\mathcal{O}_L)$ for all primes $\mathfrak{q}$ satisfying $\mathfrak{q}|\mathfrak{p}$. Similarly for J, we find that $e_{\mathfrak{q}}v_{\mathfrak{p}}(J) = v_{\mathfrak{q}}(J\mathcal{O}_L)$ for all primes $\mathfrak{p}$ and primes $\mathfrak{q}$ lying above $\mathfrak{p}$. The order-reversing property of $v_{\mathfrak{q}}$ for primes $\mathfrak{q}$ above $\mathfrak{p}$ now implies that

$$e_{\mathfrak{q}}v_{\mathfrak{p}}(J) = v_{\mathfrak{q}}(J\mathcal{O}_L) \geq v_{\mathfrak{q}}(I\mathcal{O}_L) = e_{\mathfrak{q}}v_{\mathfrak{p}}(I),$$

meaning that $v_{\mathfrak{p}}(J) \geq v_{\mathfrak{p}}(I)$ for all primes $\mathfrak{p}$ in $\mathcal{O}_K$. This shows that $J \subset I$, and thus $I|J$. ■

Proposition 1.7.6. *For an ideal I of $\mathcal{O}_K$, we have $I = I\mathcal{O}_L \cap \mathcal{O}_K$. In other words, the ideals of $\mathcal{O}_K$ are invariant under taking the restriction of an extension.*

Proof. This follows directly from Lemma 1.7.5, after defining $J := I\mathcal{O}_L \cap \mathcal{O}_K$. ■

Inside a finite Galois extension even more can be said about the unique prime factorizations. For now, let L/K be a finite Galois extension of number fields. Take $\sigma \in \mathrm{Gal}(L/K)$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime. In addition, let $\mathfrak{q} \subset \mathcal{O}_L$ be a prime such that $\mathfrak{q}|\mathfrak{p}$. Observe that σ defines a ring isomorphism on $\mathcal{O}_L$, and that ring isomorphisms map prime ideals to prime ideals. In particular, we have that $\sigma(\mathfrak{q}) \subset \mathcal{O}_L$ defines a prime. Since σ fixes K, we clearly see that $\sigma(\mathfrak{q})|\mathfrak{p}$. In other words, $\mathrm{Gal}(L/K)$ acts on the set $Q_{\mathfrak{p}} := \{\mathfrak{q} \subset \mathcal{O}_L \text{ prime } : \mathfrak{q}|\mathfrak{p}\}$.

Theorem 1.7.7. (cf. [Neu99, Prop.I.9.1]) *Let L/K be a finite Galois extension. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime with prime factorization $\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}}}$ in $\mathcal{O}_L$. Then the* $\mathrm{Gal}(L/K)$*-action described above acts transitively on $Q_{\mathfrak{p}} := \{\mathfrak{q} \subset \mathcal{O}_L : \mathfrak{q}|\mathfrak{p}\}$, i.e., for any pair $\mathfrak{q}, \mathfrak{q}' \in Q_{\mathfrak{p}}$ there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Moreover, $e_{\mathfrak{q}} = e_{\mathfrak{q}'}$ for all $\mathfrak{q}, \mathfrak{q}' \in Q_{\mathfrak{p}}$.*

Proof. We will give a proof by contradiction. Suppose that there is a pair $\mathfrak{q}, \mathfrak{q}' \in Q_{\mathfrak{p}}$ such that $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in \mathrm{Gal}(L/K)$. In that case $\sigma(\mathfrak{q})$ and $\mathfrak{q}'$ are relatively prime for all $\sigma \in \mathrm{Gal}(L/K)$, since in a Dedekind domain all non-zero prime ideals are maximal. Moreover, this implies that for $\sigma, \sigma' \in \mathrm{Gal}(L/K)$ we either have that $\sigma(\mathfrak{q}) = \sigma'(\mathfrak{q})$, or $\sigma(\mathfrak{q})$ and $\sigma'(\mathfrak{q})$ are relatively prime. Therefore, by the Chinese remainder theorem we can find a $x \in \mathcal{O}_L$ such that

$$\begin{aligned} x &\equiv 0 \mod \mathfrak{q}', \text{ and} \\ x &\equiv 1 \mod \sigma(\mathfrak{q}) \text{ for all } \sigma \in \mathrm{Gal}(L/K). \end{aligned}$$

Now consider $y = N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathfrak{q}' \cap K = \mathfrak{q}' \cap \mathcal{O}_K = \mathfrak{p}$, where $N_{L/K}$ denotes the norm on the Galois extension L/K. This norm maps into K by construction. Observe that $\sigma(x) \notin \mathfrak{q}$ for all $\sigma \in \mathrm{Gal}(L/K)$, this in particular implies that $y = \prod_{\sigma} \sigma(x) \notin \mathfrak{q}$ by primality of $\mathfrak{q}$. Thus $y \notin \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$, which leads to a contradiction. This shows that $\mathrm{Gal}(L/K)$ indeed acts transitively on $Q_{\mathfrak{p}}$.

For the last statement, notice that $\mathrm{Gal}(L/K)$ fixes $\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}}}$. This in particular implies that for each $\sigma \in \mathrm{Gal}(L/K)$ the action on $Q_{\mathfrak{p}}$ has to be injective and surjective. Moreover, by the first part of this theorem we know that for $\mathfrak{q}, \mathfrak{q}' \in Q_{\mathfrak{p}}$ there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Combining this with the fact that the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ is unique, we conclude that $e_{\mathfrak{q}} = e_{\mathfrak{q}'}$. ■

Chapter 2

Adele Rings And Idele Groups

This chapter is devoted to defining the adele ring and idele group of a global field. A classical method to do analysis on a number field was to embed it into the standard metric completion $\mathbb{R}$ or $\mathbb{C}$, and use the known analysis techniques here. The adele rings provide a way to embed the number field in a space where all the absolute values are taken into account, and where we still have access to many analytic techniques. These adele rings and idele groups are for instance locally compact Hausdorff. Therefore, they carry natural measures also known as Haar measures. Thus embedding a number field into an adele ring already opens up the possibility to apply measure theory.

We start this chapter by defining the final topology and direct limits of a collection consisting of locally compact Hausdorff spaces in Section 2.1. This topology is the usual topology put on such a direct limit.

In Section 2.2 we introduce the restricted direct product of a collection of locally compact Hausdorff spaces. This is an essential construction used for obtaining the adele rings and idele groups. Those products can also be obtained as a direct limit endowed with the final topology. We will in particular see that such a restricted direct product remains locally compact and Hausdorff.

As a result, we will be able to define the adele rings and idele groups as such restricted direct products in Section 2.3. Moreover, some properties will be given which will be useful for defining the eventual Tamagawa measure.

Section 2.4 will be the final section of this chapter, in which we will define the Tamagawa measure on adele rings, idele groups, and the adelic points of an elliptic curve. The latter is an algebraic structure which will be treated in Chapter 4 in more details. The construction of this Tamagawa measure is based on a more general construction for non-singular algebraic varieties as discussed in [Wei82]. Nevertheless, we restrict to the mentioned cases and refer to [Wei82] if the reader is interested in the general construction.

2.1 Final Topology

In this section the final topology will be introduced. In the category of topological spaces the direct limit is given by putting the final topology on the underlying set-theoretic direct limit. To ensure the existence of the direct limit we can consider a directed system of topological spaces. It turns out to be possible to define the adele rings as such a direct limit, and therefore the topology we can put on the adele rings is the final topology. This section is based on [Sut17].

Definition 2.1.1 (Final Topology)**.** Let $\{X_i\}_{i \in I}$ be a collection of topological spaces, and τ_i be the corresponding topology. Let Y be a set and $f_i : X_i \to Y$ be given functions for $i \in I$. Then the *final topology* σ_{fin} induced on Y is given by the finest topology making all the f_i continuous.

The final topology can be characterized as follows:

Lemma 2.1.2. *A subset $U \subset Y$ is open with respect to the final topology σ_{fin} if and only if $f_i^{-1}(U) \in \tau_i$ for all $i \in I$. Or equivalently,*

$$\sigma_{\mathit{fin}} = \{U \subset Y \mid f_i^{-1}(U) \in \tau_i \textit{ for all } i \in I\}.$$

Proof. We first show that the right hand side of the equation defines a topology on Y. We denote this by τ_Y for simplicity. It is clear that $\emptyset$ and Y are in τ_Y.

Let U and V be sets in τ_Y, then both $f_i^{-1}(U)$ and $f_i^{-1}(V)$ are contained in τ_i for all $i \in I$. In particular, this means that $f_i^{-1}(U \cap V) = f_i^{-1}(U) \cap f_i^{-1}(V) \in \tau_i$ for all $i \in I$.

Let $\mathcal{U}$ be an arbitrary collection of sets U contained in τ_Y. Then we observe that $f_i^{-1}(\bigcup_{U\in\mathcal{U}} U) = \bigcup_{U\in\mathcal{U}} f_i^{-1}(U) \in \tau_Y$ for all i.

Thus the collection τ_Y of subsets of Y defines a topology on Y. By definition it is clear that τ_Y is the finest topology on Y making all the f_i continuous. In other words, $\sigma_{\text{fin}} = \tau_Y$. ■

Definition 2.1.3 (Directed Set)**.** A set I together with a binary relation $\leq$ is called *directed* if the following properties are satisfied:

(i) $\leq$ is *reflexive*, i.e., $i \leq i$ for all $i \in I$.

(ii) $\leq$ is *transitive*, i.e., if $i_1 \leq i_2$ and $i_2 \leq i_3$, then $i_1 \leq i_3$ for all $i_1, i_2, i_3 \in I$.

(iii) Every pair of elements has an upper bound, i.e., for all $i_1, i_2 \in I$ there exists $i_3 \in I$ such that $i_1 \leq i_3$ and $i_2 \leq i_3$.

Definition 2.1.4 (Directed System of Topological Spaces)**.** Let I be a directed set and $\{X_i\}_{i\in I}$ a collection of topological spaces. Suppose that for each pair of indices (i, j) with $i \leq j$ in I we have continuous maps $\varphi_{ij} : X_i \to X_j$. Then (X_i, φ_{ij}) is called a *directed system over* I, and the continuous maps φ_{ij} satisfy the following properties:

(i) $\varphi_{ii} = \mathrm{id}_{X_i}$ for all $i \in I$.

(ii) The diagram below commutes,

$$\begin{tikzcd} X_i \arrow[r, "\varphi_{ij}"] \arrow[dr, "\varphi_{ik}"'] & X_j \arrow[d, "\varphi_{jk}"] \\ & X_k, \end{tikzcd}$$

or equivalently $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$ when $i \leq j \leq k$.

The *direct limit (or colimit)* of the directed system defined above is given by the underlying set-theoretic direct limit together with the final topology. The direct limit of such a directed system is often denoted as $\varinjlim X_i$. Nevertheless, the direct limit is actually a pair $(\varinjlim X_i, f_i)$ consisting of a set $\varinjlim X_i$, and continuous maps $f_i : X_i \to \varinjlim X_i$ such that $f_i = f_j \circ \varphi_{ij}$ whenever $i \leq j$. And this direct limit is unique up to isomorphism. In our case the direct limit is given by

$$\varinjlim X_i = \coprod_{i\in I} X_i \Big/ \sim,$$

together with the final topology. Here $\sim$ is the binary relation defined by $X_i \ni x_i \sim x_j \in X_j$ if and only if there exists a $k \in I$ with $i, j \leq k$ and such that $\varphi_{ik}(x_i) = \varphi_{jk}(x_j)$. This relation is actually an equivalence relation.

The direct limit of the direct system (X_i, φ_{ij}) has the universal property that for any topological space Y with continuous maps $\psi_i : X_i \to Y$ that satisfy $\psi_i = \psi_j \circ \varphi_{ij}$ for $i \leq j$, there exists a unique continuous map $u : \varinjlim X_i \to Y$ such that $u \circ f_i = \psi_i$ for each i. Thus the following diagram

$$\begin{tikzcd}
X_i \arrow[rr, "\varphi_{ij}"] \arrow[dr, "f_i"] \arrow[ddr, bend right, "\psi_i"'] & & X_j \arrow[dl, "f_j"'] \arrow[ddl, bend left, "\psi_j"] \\
& \varinjlim X_i \arrow[d, "u"] & \\
& Y &
\end{tikzcd}$$

will commute for all i, j.

2.2 Restricted Direct Product

In this section we give the general method needed to construct the adele rings together with the idele groups. The adele rings are special cases of the restricted direct product of a collection of locally compact Hausdorff topological spaces. Therefore we will restrict ourselves already to the desired environment by only considering restricted direct products for these type of topological spaces. As a main reference for providing the required theory about restricted direct product, we use [Sut17].

Definition 2.2.1 (Restricted Direct Product)**.** Let $\{X_i\}_{i\in I}$ be a non-empty collection of locally compact Hausdorff topological spaces. Let C_i be an open compact subset of X_i for almost all[1] $i \in I$. For the other $i \in I$, we define $C_i := X_i$. *The restricted direct product* of the X_i's with respect to the C_i's is given by the topological space

$$X := \prod_{i\in I}(X_i, C_i) := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \;\middle|\; x_i \in C_i \text{ for almost all } i \in I \right\},$$

with basis of opens

$$\mathcal{B}_{\text{rstr}} = \left\{ \prod_{i\in I} V_i \;\middle|\; V_i \subset X_i \text{ open for all } i \in I, \text{ and } V_i = C_i \text{ for almost all } i \in I \right\}.$$

We call this topology the *restricted direct product topology.*

We will now view a different method to construct the restricted direct product of a non-empty collection of locally compact Hausdorff spaces $\{X_i\}_{i\in I}$, with respect to some C_i satisfying the properties from the definition above.

For each finite set $S \subset I$, we have the open subspace $X(S)$ of X endowed with the induced subspace topology, given by

$$X(S) := \prod_{i\in S} X_i \times \prod_{i\notin S} C_i. \tag{2.1}$$

Note that for $S \subset T$ finite subsets of I, we have $X(S) \subset X(T)$. Therefore, the collection of topological spaces $\{X(S) \mid S \subset I \text{ finite}\}$ together with the inclusion maps $\iota_{ST} : X(S) \to X(T)$

[1] With *for almost all* we mean, for all but finitely many.

for $S \subset T$ finite subsets of I form a directed system over all finite subsets of I. For simplicity, we define $\mathcal{I} := \{S \subset I \mid S \text{ finite}\}$. The corresponding direct limit is now given by

$$\varinjlim_{S\in\mathcal{I}} X(S) = \coprod_{S\in\mathcal{I}} X(S)/\sim,$$

together with the final topology. The coproduct is the set-theoretic disjoint union together with the equivalence relation $\sim$ given by $X(S) \ni (x_i)_{i\in I} \sim (x_i')_{i\in I} \in X(T)$ if and only if there exists $R \subset I$ finite such that $S, T \subset R$ and $\iota_{SR}((x_i)_{i\in I}) = \iota_{TR}((x_i')_{i\in I})$.

For every $x \in X$, we have a finite set $S(x) := \{i \in I \mid x_i \notin C_i\}$. During the construction of this direct limit a natural map arises, namely

$$\varphi : X \to \varinjlim_{S\in\mathcal{I}} X(S) = \coprod_{S\in\mathcal{I}} X(S)/\sim, \; x \mapsto [(x, S(x))].$$

The following proposition states that this map actually defines a homeomorphism of topological spaces.

Proposition 2.2.2. (cf. [Sut17, Prop.25.5]) *The map φ between the restricted direct product and the direct limit defined in the discussion above, is a homeomorphism of topological spaces.*

Proof. For φ to be a homeomorphism of topological spaces, we have to show that it is a bijection, continuous map, and an open map.

We first show that φ is surjective. Let $[(y,T)] \in \coprod_{S\in\mathcal{I}} X(S)/\sim$, this means that the element $y \in X(T) = \prod_{i\in T} X_i \times \prod_{i\notin T} C_i$. Now notice that $S(y) := \{i \in I \mid y_i \notin C_i\} \subset T$, implying that $y \in X(S(y)) \subset X(T)$. Therefore by the equivalence relation on $\coprod_{S\in\mathcal{I}} X(S)$, we find that $[(y,T)] = [(y, S(y))] = \varphi(y)$.

For injectivity, we suppose that $[(x, S(x))] = [(y, S(y))]$. Consequently, there exists $T \in \mathcal{I}$ such that $S(x), S(y) \subset T$ with $x = \iota_{S(x)T}(x) = \iota_{S(y)T}(y) = y$. This immediately implies that φ is injective.

We now show that φ is continuous. Let $U \subset \coprod_{S\in\mathcal{I}} X(S)/\sim$ be open. Note that for every $T \in \mathcal{I}$ we have a continuous injection $\iota_T : X(T) \to \coprod_{S\in\mathcal{I}} X(S)$, and we have the continuous quotient map $\pi : \coprod_{S\in\mathcal{I}} X(S) \to \coprod_{S\in\mathcal{I}} X(S)/\sim$. We want to show that $\varphi^{-1}(U)$ is open in X. Note that

$$\varphi(x) \in U \Leftrightarrow [(x, S(x))] \in U \Leftrightarrow \pi(\iota_{S(x)}(x)) \in U \Leftrightarrow \pi(\iota_T(x)) \in U \text{ for some } T \in \mathcal{I}.$$

If we put $V_T = \iota_T^{-1}(\pi^{-1}(U))$, then we see by the above that

$$\varphi^{-1}(U) = \bigcup_{T\in\mathcal{I}} V_T.$$

Thus $\varphi^{-1}(U)$ is open in X by continuity of ι_T and π, proving that φ is continuous.

At last we prove that φ is an open mapping. Let $U \subset X$ be open, and notice that we have $\bigcup_{T\in\mathcal{I}} X(T) = X$. Therefore, we can write

$$U = \bigcup_{T\in\mathcal{I}} X(T) \cap U = \bigcup_{T\in\mathcal{I}} U(T),$$

where $U(T) := X(T) \cap U$ is open. By the definition of φ, we see that

$$\varphi(U) = \varphi\big(\bigcup_{T\in\mathcal{I}} U(T)\big) = \bigcup_{T\in\mathcal{I}} \varphi(U(T)) = \bigcup_{T\in\mathcal{I}} \pi(\iota_T(U(T))) = \pi\left(\bigcup_{T\in\mathcal{I}} \iota_T(U(T))\right) = \coprod_{S\in\mathcal{I}} U(S)/\sim .$$

By the definition of the final topology on $\varinjlim_{S\in\mathcal{I}} X(S)$, we have $\varphi(U) = \coprod_{S\in\mathcal{I}} U(S)/{\sim}$ open if and only if $\iota_T^{-1}(\pi^{-1}(\varphi(U)))$ open in $X(T)$ for all $T \in \mathcal{I}$.

We will now show that $\pi^{-1}\left(\coprod_{S\in\mathcal{I}} U(S)/{\sim}\right) = \coprod_{S\in\mathcal{I}} U(S)$. Note that the inclusion " $\supseteq$ " is clear. For the other inclusion, suppose that $(x, S_1) \in \coprod_{S\in\mathcal{I}} X(S)$ such that $\pi(x, S_1) = [(x, S_1)] \in \coprod_{S\in\mathcal{I}} U(S)/{\sim}$. Then there exists some $S_2 \in \mathcal{I}$ and $y \in U(S_2)$ such that $[(x, S_1)] = [(y, S_2)]$. This implies that $x = y$ in U, and thus $x \in U(S_1)$. Consequently, $(x, S_1) \in \coprod_{S\in\mathcal{I}} U(S)$, which proves that

$$\pi^{-1}\left(\coprod_{S\in\mathcal{I}} U(S)/{\sim}\right) = \coprod_{S\in\mathcal{I}} U(S).$$

After taking the preimage of ι_T for $T \in \mathcal{I}$ on both sides of the equation above, we find that $\iota_T^{-1}(\pi^{-1}(\varphi(U))) = U(T)$. Recall that this set is open for all $T \in \mathcal{I}$, and therefore by definition of the final topology we can conclude that $\varphi(U)$ is open in $\varinjlim_{S\in\mathcal{I}} X(S)$. ■

Proposition 2.2.3. (cf. [Sut17, Prop.25.6]) *Let $\{X_i\}_{i\in I}$ be a non-empty collection of locally compact Hausdorff spaces. Let $\{C_i\}_{i\in I}$ a collection of open compact subsets of X_i for almost all $i \in I$, such that for the other i we have $C_i := X_i$.*

1. *Then the restricted direct product $X := \prod_{i\in I}(X_i, C_i)$ is locally compact.*

2. *Moreover, if the X_i's and C_i's are topological rings, then the restricted direct product X is also a topological ring.*

3. *If the X_i's and C_i's are topological groups, then the restricted direct product X is also a topological group.*

Proof. 1. First notice that a basis for the induced subspace topology on $X(S)$ for $S \subset I$ finite, defined in (2.1), is given by

$$\mathcal{B}_S := \left\{ \prod_{i\in I} V_i \;\middle|\; V_i \subset \mathrm{pr}_i(X(S)) \text{ open, and } V_i = C_i = \mathrm{pr}_i(X(S)) \text{ for almost all } i \in I \right\},$$

where pr_i is the projection map onto the i-th coordinate. Note that this set of basis elements is equal to the set of basis elements for the product topology on $X(S)$, i.e., $X(S)$ is topologized with the product topology. Now let $(x_i)_{i\in I} \in X(S)$, then by the locally compact property of the X_i, there exists an open $U_i \in X_i$ and a compact $K_i \subset X_i$ such that $x_i \in U_i \subset K_i$ for all $i \in S$. Now note that

$$(x_i)_{i\in I} \in \prod_{i\in S} U_i \times \prod_{i\notin S} C_i \subset \prod_{i\in S} K_i \times \prod_{i\notin S} C_i \subset X(S).$$

Since S is finite, we find that $\prod_{i\in S} U_i \times \prod_{i\notin S} C_i$ is open in $X(S)$. By Tychonoff's theorem we find that any collection of compact sets is again compact in the product topology. Consequently, the set $\prod_{i\in S} K_i \times \prod_{i\notin S} C_i$ is compact in $X(S)$. Since we took $(x_i)_{i\in I} \in X(S)$ arbitrarily, this proves that $X(S)$ is locally compact.

Let $x \in X = \bigcup_{S\in\mathcal{I}} X(S)$, where $\mathcal{I}$ is the set of finite subsets of I. Then $x \in X(S(x))$ with $S(x) = \{i \in I \mid x_i \notin C_i\}$ as defined before. Since $X(S(x))$ is locally compact, there exists an open $U \subset X(S(x))$ and $K \subset X(S(x))$ compact such that $x \in U \subset K$. Since the inclusion map $\iota_{S(x)} : X(S(x)) \to X$ is continuous and $X(S(x))$ is open, we find that K is compact in X and U is open in X. Thus X is also locally compact.

2. Suppose that the X_i's and C_i's are topological rings. Note that the $X(S)$ form open subsets of X for every finite subset $S \subset I$, and therefore $X(S) \times X(S)$ is open in $X \times X$ with respect to the product topology. Let $(x, y) \in X \times X$, then $x \in X(S)$ and $y \in X(T)$ for some $S, T \in \mathcal{I}$. By definition we immediately see that $x, y \in X(S \cup T)$, implying that $X \times X = \bigcup_{S \in \mathcal{I}} X(S) \times X(S)$.

   We will now start by proving that the sets $X(S)$ defined at (2.1), are topological rings with respect to the component-wise induced operations. Let $f_{S,i} : X(S)_i \times X(S)_i \to X(S)_i$ play the role of the addition operation, or the multiplication operation on $X(S)_i$. Both cases won't affect any argument in the rest of the proof. The map $f_{S,i}$ is continuous by assumption. Let $\pi_{S,i} : X(S) \times X(S) \to X(S)_i \times X(S)_i$ be the canonical projection, and note that this map is continuous by the definition of the product topology. The induced operation on $X(S)$ is now given by

$$f_S = (f_{S,i} \circ \pi_{S,i})_{i \in I} : X(S) \times X(S) \to X(S).$$

   This map defines a continuous map, since all the components $f_{S,i} \circ \pi_{S,i}$ are continuous, making $X(S)$ into a topological ring. Let $\iota_S : X(S) \to X$ be the continuous inclusion of $X(S)$ into X. Then notice that $\iota_S \circ f_S$ defines a continuous map from $X(S) \times X(S)$ to X. Observe that these maps agree on overlaps, i.e.,

$$(\iota_S \circ f_S)(x, y) = (\iota_T \circ f_T)(x, y)$$

   for all $(x, y) \in (X(S) \times X(S)) \cap (X(T) \times X(T))$. Since $X(S) \times X(S)$ is open in $X \times X$ we find by the gluing lemma for open subsets that there exists a unique continuous map

$$f : X \times X \to X,$$

   such that $f_{|X(S) \times X(S)} = \iota_S \circ f_S$. By construction, this map is the naturally induced component-wise addition or multiplication operation on X. This proves that X is indeed also a topological ring.

3. Suppose that X_i and C_i are topological groups for all $i \in I$. To show that X is also a topological group, it is enough to show that the map $f : X \times X \to X, (x, y) \mapsto xy^{-1}$ is continuous. The proof of this goes similarly as the proof for the topological rings. Hereby, we have to define the $f_{S,i}$ maps as $f_{S,i}(x_i, y_i) := x_i y_i^{-1}$. The rest of the proof will be analogous.

■

Note that the restricted direct product as defined in Definition 2.2.1 is a subset of the product space $\prod_{i \in I} X_i$, but not endowed with the inherit subspace topology. It appears that the restricted direct product topology is finer than the subspace topology induced by the product space, which will be a part of the proof of the following proposition.

Proposition 2.2.4. *Let $\{X_i\}_{i \in I}$ and $\{C_i\}_{i \in I}$ be collections as in Definition 2.2.1. Then the restricted direct product $X := \prod_{i \in I}(X_i, C_i)$ is Hausdorff.*

Proof. Recall that $X \subset \prod_{i \in I} X_i$, and a basis for the induced subspace topology on X is given by

$$\mathcal{B}_{\text{prod},X} = \left\{ X \cap \prod_{i \in I} U_i \;\middle|\; U_i \subset X_i \text{ open } \forall i \in I, \text{ and } U_i = X_i \text{ for almost all } i \in I \right\}.$$

Note that $\prod_{i\in I} X_i$ is clearly Hausdorff with respect to the product topology, and therefore it suffices to show that the restricted direct product topology on X is finer than the induced subspace topology on X to conclude that X is Hausdorff.

It is enough that show that every basis open in $\mathcal{B}_{\mathrm{prod},X}$ is also open in X with respect to the restricted direct product topology. Let $X \cap \prod_{i\in I} U_i \in \mathcal{B}_{\mathrm{prod},X}$, and $\mathcal{I} := \{S \subset I \mid S \text{ finite}\}$. For $S \in \mathcal{I}$ and $i \in I$ we define

$$V_{S,i} := \begin{cases} U_i & \text{if } i \in S \\ U_i \cap C_i & \text{if } i \notin S. \end{cases}$$

Note that $V_{S,i}$ is open in X_i for all $i \in I$, and $V_{S,i} = C_i$ for almost all $i \in I$. Therefore $\prod_{i\in I} V_{S,i}$ is open in the restricted direct product topology on X. We clearly see that

$$\bigcup_{S\in\mathcal{I}} \prod_{i\in I} V_{S,i} \subset X \cap \prod_{i\in I} U_i, \tag{2.2}$$

by construction. For the other inclusion, let $x = (x_i)_{i\in I} \in X \cap \prod_{i\in I} U_i$. Then $x_i \in U_i$ for all $i \in I$, and $x_i \in C_i$ for almost all $i \in I$. Therefore, after defining $S(x) := \{i \in I | x_i \notin C_i\}$, we find that $x \in \prod_{i\in I} V_{S(x),i}$. This implies that the inclusion at (2.2) is actually an equality, meaning that $X \cap \prod_{i\in I} U_i$ is also open in X with respect to the restricted direct product topology. ■

2.3 Adele Rings and Idele Groups

In this section we define the adele ring and idele group of a global field. We moreover treat some of their properties. For a more thorough description of this theory, one could consult [Kna07] and [Claa].

Let K be a global field, and v a place of K. Then we have a completion K_v of K with respect to an absolute value $|\cdot|_v$ representing the place v. As proven in Theorem 1.4.6, the completions K_v are locally compact. Thus $\{K_v\}_{v\in M_K}$ forms a non-empty collection of locally compact Hausdorff topological spaces, where the index ranges over all places on K. Note that every $v \in M_K$ is either non-Archimedean or Archimedean. Recall that K is a finite extension of $L = \mathbb{Q}$ or $L = \mathbb{F}_p(t)$ for some prime p, and that $|\cdot|_v$ is (non)-Archimedean if and only if $|\cdot|_{v_{|_L}}$ is (non)-Archimedean. By the classification of the places on L as given in Remark 1.1.9, the only Archimedean place is represented by the standard absolute value $|\cdot|_\infty$ on $\mathbb{Q}$. If K is a finite extension of $\mathbb{Q}$ of degree n, then there are at most n extensions of the absolute value $|\cdot|_{\mathbb{Q}}$ to K (see [CF67, CH II, Theorem, p.57]). Therefore, there are only finitely many Archimedean places on K. For the non-Archimedean places v, we can consider the valuation ring $\mathcal{O}_{K_v}$ of K_v. The following Lemma tells us that $\mathcal{O}_{K_v}$ is an open compact subset of K_v.

Lemma 2.3.1. *Let v be a non-Archimedean place of K represented by a non-trivial absolute value $|\cdot|_v$, and K_v be the completion of K with respect to $|\cdot|_v$. Then $\mathcal{O}_{K_v}$ is an open compact subset of K_v.*

Proof. Note that $\mathcal{O}_{K_v}$ is the closed ball in K_v, and therefore by Proposition 1.2.4 it is open.

For the compactness, we recall that K_v is locally compact (see Theorem 1.4.6). Since $|\cdot|_{K_v}$ is non-trivial, there exists $\xi \in K_v$ such that $|\xi|_{K_v} < 1$. By the locally compact property of K_v we can find $n \in \mathbb{N}$ such that the closed ball $B_{|\cdot|_{K_v}}[0, |\xi|^n_{K_v}] \subset C$ for some compact set C in K_v. Hence $B_{|\cdot|_{K_v}}[0, |\xi|^n_{K_v}]$ is a closed subset of a compact set, and therefore compact. Note that the map $f : K_v \to K_v$ defined by mapping x to $\xi^{-n}x$ is a continuous map, such that $f(B_{|\cdot|_{K_v}}[0, |\xi|^n_{K_v}]) = B_{|\cdot|_{K_v}}[0, 1] = \mathcal{O}_{K_v}$. This finishes the proof, since the image of a compact set under a continuous map is again compact. ■

By the discussion above we have a non-empty collection $\{K_v\}_{v\in M_K}$ of locally compact Hausdorff spaces, and open compact subsets $\mathcal{O}_{K_v}$ of K_v for all but finitely many places v. This justifies the following definition of an adele ring.

Definition 2.3.2 (Adele Ring)**.** Let K be a global field and consider the non-empty collection, $\{K_v\}_{v\in M_K}$, of completions of K. For non-Archimedean places v, we consider the valuation rings $\mathcal{O}_{K_v}$. For the Archimedean places, we define $\mathcal{O}_{K_v} := K_v$. Then the *adele ring* of K, denoted as $\mathbb{A}_K$, is given by the restricted direct product of the K_v's with respect to the valuation rings $\mathcal{O}_{K_v}$. In other words,

$$\mathbb{A}_K := \prod_{v\in M_K}(K_v, \mathcal{O}_{K_v}) = \left\{(x_v)_{v\in M_K} \in \prod_{v\in M_K} K_v \;\middle|\; x_v \in \mathcal{O}_{K_v} \text{ for almost all } i \in I\right\}.$$

The commutative ring structure on $\mathbb{A}_K$ is given by the canonical componentwise operations. Proposition 2.2.3 and 2.2.4 tell us that the adele rings are locally compact Hausdorff spaces and topological rings.

As discussed in Section 2.2, the adele rings can also be constructed by using direct limits. The sets over which the direct limit is taken are the so-called *S-adeles*, given by

$$\mathbb{A}_K(S) := \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v},$$

where $S \subset M_K$ is finite.

Another intuitive set to consider is the unit group $\mathbb{A}_K^\times$ of $\mathbb{A}_K$. In general, this unit group does not have to be a topological group if it is endowed with the subspace topology it inherits from the adele ring $\mathbb{A}_K$. The unit group of $\mathbb{A}_K$ is given by the set consisting of $(x_v)_{v\in M_K} \in \prod_{v\in M_K} K_v^\times$ such that $x_v \in \mathcal{O}_{K_v}^\times$ for almost all $v \in M_K$. Intuitively, one could wonder if this set can be defined as the restricted direct product of the spaces $K_v^\times$ with respect to the unit groups $\mathcal{O}_{K_v}^\times$. The following lemma makes sure that we can at least take the restricted direct product of the $K_v^\times$'s with respect to the $\mathcal{O}_{K_v}^\times$'s.

Lemma 2.3.3. *Let $v \in M_K$ be a place on K. The spaces $K_v^\times$ are locally compact Hausdorff spaces. If v is non-Archimedean, then $\mathcal{O}_{K_v}^\times$ is an open compact subset of $K_v^\times$.*

Proof. Note that $K_v^\times = K_v \backslash \{0\}$ is open in K_v, since all singletons are closed in Hausdorff spaces. Thus $K_v^\times$ is an open subset of the locally compact Hausdorff space K_v, and therefore $K_v^\times$ is locally compact Hausdorff[2].

If v is non-Archimedean, then by Proposition 1.2.4 every open ball is closed, and every closed ball is open. Now notice that we have

$$\mathcal{O}_{K_v}^\times = B_{|\cdot|_{K_v}}(0,1)^C \cap \mathcal{O}_{K_v},$$

implying that $\mathcal{O}_{K_v}^\times$ is open and closed in K_v. Since $\mathcal{O}_{K_v}^\times \subset K_v^\times$, it is also open in $K_v^\times$.

For the compactness, notice that $\mathcal{O}_{K_v}^\times$ is a closed subset of the compact set $\mathcal{O}_{K_v}$ (Lemma 2.3.1). Therefore, $\mathcal{O}_{K_v}^\times$ is compact in K_v as well. Since $\mathcal{O}_{K_v}^\times \subset K_v^\times \subset K_v$, it is also compact in $K_v^\times$. ■

As mentioned before, the unit group $\mathbb{A}_K^\times$ does not have to be a topological group with respect to the subspace topology induced from $\mathbb{A}_K$. The lemma above ensures that we can take the restricted direct product of the $K_v^\times$'s with respect to the unit groups $\mathcal{O}_{K_v}^\times$. This endows the unit group $\mathbb{A}_K^\times$ with the so-called restricted direct product topology. We will see that this topology makes $\mathbb{A}_K^\times$ into a topological group.

[2] This fact can be found in [Wil04, Thm.18.4], together with a proof.

Definition 2.3.4 (Idele Group)**.** Let K be a global field, and $\{K_v^\times\}_{v\in M_K}$ be the non-empty collection of completions of K with respect to some place v. For non-Archimedean places v, we have the unit groups $\mathcal{O}_{K_v}^\times$. In the Archimedean case, we put $\mathcal{O}_{K_v}^\times := K_v^\times$. Then the *idele group* $\mathbb{I}_K$ of K is defined as the restricted direct product of the $K_v^\times$'s with respect to the $\mathcal{O}_{K_v}^\times$'s,

$$\mathbb{I}_K := \prod_{v\in M_K} (K_v^\times, \mathcal{O}_{K_v}^\times) = \left\{ (x_v)_{v\in M_K} \in \prod_{v\in M_K} K_v^\times \;\middle|\; x_v \in \mathcal{O}_{K_v}^\times \text{ for almost all } v \in M_K \right\}.$$

The group structure will again be defined componentwise. By Proposition 2.2.3, this makes $\mathbb{I}_K$ into a topological group. The same proposition, together with Proposition 2.2.4, also ensure that $\mathbb{I}_K$ is a locally compact Hausdorff space. This allows us to define a Haar measure on it, as we will see in the next section. Just as for the adeles, we also have the notion of *S-ideles*, which are given by

$$\mathbb{I}_K(S) := \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v},$$

for some finite set $S \subset M_K$.

For the rest of this thesis, we assume K to be a number field. Moreover, we now consider the normalized absolute values as defined in Section 1.6 such that the product formula is satisfied.

One of the main important properties of $\mathbb{A}_K$ (or $\mathbb{I}_K$), is that K (respectively $K^\times$) embeds diagonally into it. We start by observing the first embedding. It is obvious that an embedding $\iota : K \to \prod_{v\in M_K} K_v$ can be formed by defining $\iota(x) = (\iota_v(x))_v$, where ι_v is the canonical embedding of K into K_v. The following lemma tells us that ι actually maps into $\mathbb{A}_K$.

Lemma 2.3.5. *Consider the diagonal embedding*

$$\iota : K \to \prod_{v\in M_K} K_v,\ \ \iota(x) = (\iota_v(x))_v,$$

then $\iota(K) \subset \mathbb{A}_K$.

Proof. For $x \in K$, we have to show that $|\iota_v(x)|_v = |x|_v \leq 1$ for all but finitely many places v. We will actually be able to proof a stronger property, namely that $|x|_v = 1$ for all but finitely many v. Inside the ring of integers $\mathcal{O}_K$, we have a unique prime ideal factorization of $x\mathcal{O}_K$ (Theorem 1.6.5). The non-Archimedean places of K correspond to the non-zero prime ideals of $\mathcal{O}_K$ (Theorem 1.6.7). We moreover see that $|x|_v = 1$ except for the places v corresponding to a prime ideal appearing in the factorization of $x\mathcal{O}_K$. But this are only finitely many places. Since there are also only finitely many Archimedean places, we see that $|x|_v = 1$ for all but finitely many $v \in M_K$. In other words, $\iota(x) \in \mathbb{A}_K$. ■

Similarly for the idele group, we have a canonical embedding $\iota : K^\times \to \prod_{v\in M_K} K_v^\times$. Now the observation that can be made, is that the proof of the above also provides the required arguments to show that $\iota(K^\times) \subset \mathbb{I}_K$.

The properties we are discussing, mostly have a point of interest when considering Haar measures on the adeles and ideles, which we will do in the next section. Additionally to the embeddings, one can show that the images $\iota(K)$ and $\iota(K^\times)$ form discrete subspaces of $\mathbb{A}_K$ and $\mathbb{I}_K$, respectively.

Theorem 2.3.6. (cf. [Kna07, Thm.6.52 and 6.53]) *The images of the maps $\iota : K \to \mathbb{A}_K$, and $\iota : K^\times \to \mathbb{I}_K$ are discrete.*

Proof. We first note that for topological groups G we have that the canonical translation maps on G are homeomorphisms. Thus to show that a subgroup H is discrete in G, i.e., that there exists for every $x \in G$ an open neighborhood U_x of x such that $U_x \cap H = \{x\}$, it suffices to show the latter for a single element.

We start by proving that $\iota(K)$ is discrete. By the above it is sufficient to construct an open neighborhood U of $\{0\}$ such that $U \cap \iota(K) = \{0\}$. We consider the set

$$U := \{(x_v)_v \in \mathbb{A}_K \mid |x_v|_v < 1 \text{ for } v \in M_K^\infty \text{ and } |x_v|_v \leq 1 \text{ for } v \in M_K^0\}.$$

We observe that this set is clearly open in $\mathbb{A}_K(S_\infty)$, where S_∞ is the set of Archimedean places. As a consequence, we see that U is also open in $\mathbb{A}_K$. By the product formula (Theorem 1.6.9) we know that for all $y \in K^\times$, we have $\prod_{v \in M_K} |\iota_v(y)|_v = \prod_{v \in M_K} |y|_v = 1$. But since $\prod_{v \in M_K} |x_v|_v < 1$ for $(x_v)_v \in U$, we obtain that $U \cap \iota(K) = \{0\}$.

For $\iota(K^\times)$, we define the set

$$U := \{(x_v)_v \in \mathbb{I}_K \mid |x_v - 1|_v < 1 \text{ for } v \in M_K^\infty \text{ and } |x_v - 1| \leq 1 \text{ for } v \in M_K^0\}.$$

This is an open subset of $\mathbb{I}_K(S_\infty)$ containing 1, and therefore also open in $\mathbb{I}_K$. For $y \in K^\times$ with $y \neq 1$, we notice that $\iota_v(y) - 1 = \iota_v(y-1) \neq 0$. Again by the product formula, we obtain that $\prod_{v \in M_K} |\iota_v(y-1)| = \prod_{v \in M_K} |y-1|_v = 1$. To the contrary, all the $(x_v)_v \in U$ satisfy $\prod_{v \in M_K} |x_v - 1|_v < 1$, which implies that $U \cap \iota(K^\times) = \{1\}$. ■

Another useful topological property is that the quotient $\mathbb{A}_K/\iota(K)$ is compact, which we state as a theorem where we omit the proof.

Theorem 2.3.7. (cf. [Kna07, Thm.6.52]) *The quotient of the adeles $\mathbb{A}_K$ by the image $\iota(K)$ forms a compact additive group.*

One might wonder whether the group $\mathbb{I}_K/\iota(K^\times)$, also known as the *idele class group*, is also compact. Nevertheless, to get a compact quotient of the ideles a little restriction has to be made. For this, we define the natural homomorphism *idele-norm*

$$\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}, \ (x_v)_v \mapsto \prod_{v \in M_K} |x_v|_v.$$

Note that this map is well-defined, since for all but finitely many v we have $|x_v| = 1$.

Lemma 2.3.8. *The idele-norm is continuous.*

Proof. By the topology on $\mathbb{I}_K$, we know that a subset U is open in $\mathbb{I}_K$ if and only if $U \cap \mathbb{I}_K(S)$ is open for all finite subsets S of M_K. Now notice that the maps $|\cdot|_v : K_v \to \mathbb{R}$ are continuous for all v, and that the idele-norm on $\mathbb{I}_K(S)$ is just a finite product of these continuous maps, and therefore itself continuous. This shows that for all $V \subset \mathbb{R}_{>0}$, we have that $\|\cdot\|^{-1}(V) \cap \mathbb{I}_K(S)$ is open. This in particular means that $\|\cdot\|^{-1}(V)$ is open in $\mathbb{I}_K$. ■

It is clear that this map is surjective, by considering the surjectivity of the absolute values on the Archimedean places. Another observation that can be made is that all the elements in the subgroup $\iota(K^\times)$ of $\mathbb{I}_K$ have norm one. Combining these observations leads to the fact that $\mathbb{I}_K/\iota(K^\times)$ also maps surjectively onto $\mathbb{R}_{>0}$, which by the continuity of the idele-norm in particular means that the quotient cannot be compact. To obtain a compact quotient, we consider the so-called *ideles of norm* 1, i.e.

$$\mathbb{I}_K^1 := \{x \in \mathbb{I}_K \mid \|x\| = 1\} = \ker\{\|\cdot\|\}.$$

This is a closed subgroup of $\mathbb{I}_K$, and the quotient $\mathbb{I}_K^1/\iota(K^\times)$ is compact.

Theorem 2.3.9. (cf. [Kna07, Thm.6.53]) *The quotient of the norm* 1 *ideles $\mathbb{I}_K^1$ by the image $\iota(K^\times)$ forms a compact multiplicative group.*

2.4 Tamagawa Measure

This section will be dedicated to put a Haar measure on the adeles, ideles, and the adelic points of an elliptic curve defined over a number field. The reader is supposed to have knowledge about measure theory and its connection with integration. For full details, one is suggested to read [Coh13]. Nevertheless, we will give a brief introduction to Haar measures in Appendix A.

Let K be a number field, and $\mathbb{A}_K$ the corresponding adele ring. The sets on which we want to put a Haar measure, are examples of the adelic points of certain non-singular algebraic varieties. We will now closely follow [Wei82] to define the Tamagawa measure on the adeles, ideles, and the adelic points of an elliptic curve E defined over K. Since we are only interested in doing computations with this measure on specific varieties, we omit the details for the general construction. To give an overview of the varieties of main interest for this thesis, we state them as an example together with the corresponding set of adelic points.

Example 2.4.1.
1. The *additive group* of K, $V = \mathbb{G}_a$. In this case we have $V(\mathbb{A}_K) = \mathbb{A}_K$, i.e., the adele ring.
2. The *multiplicative group* of K, $V = \mathbb{G}_m$. In this case we have $V(\mathbb{A}_K) = \mathbb{I}_K$, i.e., the idele group.
3. An elliptic curve E defined over K, $V = E$. Then $V(\mathbb{A}_K) = E(\mathbb{A}_K) = \prod_{v\in M_K} E(K_v)$ [3].

It is well known that there exists an invariant differential form of degree 1, that is everywhere holomorphic and non-zero on the varieties considered in the example. They are listed below for the specific varieties.

Example 2.4.2.
1. $V = \mathbb{G}_a$, $\omega = \mathrm{d}x$,
2. $V = \mathbb{G}_m$, $\omega = \mathrm{d}x/x$,
3. $V = E$, ω is the invariant differential associated to a Weierstrass equation for E. This will be defined in Definition 4.1.2.

These differentials induce a left invariant measure ω_v on the local groups $V(K_v)$[4] in the usual way as described in [Wei82, CH 2.2]. For this, the Haar measures μ_v on the additive groups K_v have to be fixed for all $v \in M_K$. For the eventual construction of the Tamagawa measure it is required that:

(i) $\mu_v(\mathcal{O}_{K_v}) = 1$ for almost all finite places v.

(ii) If $\mu = \prod_{v\in M_K} \mu_v$ is the product measure on $\mathbb{A}_K$ as obtained by Theorem A.2.1, and if $\iota(K)$ is endowed with the counting measure, then $\mathbb{A}_K/\iota(K)$ has volume 1 with respect to the induced quotient measure by Theorem A.1.2.

We give our choice of normalizations for the Haar measures μ_v on K_v as a definition.

Definition 2.4.3. The *normalized Haar measures* μ_v on the additive group K_v for $v \in M_K$, are taken as follows:

- For $v \in M_K^0$, we demand $\mu_v(\mathcal{O}_{K_v}) = 1$.
- For real places $v \in M_K^\infty$, we have $K_v \cong \mathbb{R}$, and take μ_v as the usual Lebesgue measure on $\mathbb{R}$.

[3] The last equality can be found in [AS21, Lem.2.1]

[4] The explicit local induced measures of the considered varieties are given in Section 4.5 and Section 5.4

- For complex places $v \in M_K^\infty$, we have $K_v \cong \mathbb{C}$, and take μ_v as twice the Lebesgue measure on $\mathbb{C}$.

In this way, we obtain a canonical Haar measure on $\mathbb{A}_K$, defined as the measure which induces in each $\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v}$ for finite $S \subset M_K$ containing the Archimedean places the (convergent) product measure $\prod_{v\in M_K} \mu_v$, see Theorem A.2.1. Note that the normalizations described above make sure that this product converges. This measure induces a unique measure ν on the quotient $\mathbb{A}_K/\iota(K)$ that is compatible, in the sense of Theorem A.1.2, with the exact sequence

$$0 \longrightarrow \iota(K) \longrightarrow \mathbb{A}_K \to \mathbb{A}_K/\iota(K) \longrightarrow 0,$$

where $\iota(K)$ is endowed with the counting measure.

An invariant appearing in the definition of the Tamagawa measure is $\nu(\mathbb{A}_K/\iota(K))$. The reason for this, is that under the normalizations given in Definition 2.4.3 the property $\nu(\mathbb{A}_K/\iota(K)) = 1$ is not satisfied. Our next goal is to compute the volume of $\mathbb{A}_K/\iota(K)$ with respect to ν. Recall by Theorem 2.3.7 and the regularity of the Haar measure that $\nu(\mathbb{A}_K/\iota(K))$ is finite. It therefore makes sense to compute it, for which we need the following lemma. The proof of this lemma is based on the proof of Theorem 2.3.7 as given in [Kna07, Thm.6.52].

Lemma 2.4.4. *Let $\iota : K \to \mathbb{A}_K$ be the canonical diagonal embedding. Then we have the equalities*

$$\mathbb{A}_K = \iota(K) + \mathbb{A}_K(S_\infty),$$
$$\iota(\mathcal{O}_K) = \iota(K) \cap \mathbb{A}_K(S_\infty).$$

Proof. Let $(x_v)_v \in \mathbb{A}_K$, then $x_v \in \mathcal{O}_{K_v}$ for all but finitely many $v \in M_K^0$. Let T be the finite set of places $v \in M_K^0$ such that $|x_v|_v > 1$. By the strong approximation theorem 1.6.8 there exists a $y \in K$ such that

$$|\iota_v(y) - x_v|_v \leq 1 \text{ for all } v \in T$$
$$|\iota_v(y)|_v \leq 1 \text{ for all } v \in M_K^0 \backslash T.$$

Consequently, we obtain that $|\iota_v(y) - x_v|_v \leq 1$ for all $v \in M_K^0$, which in particular means that $(x_v)_v - \iota(y) \in \mathbb{A}_K(S_\infty)$. Hence $(x_v)_v = \iota(y) + ((x_v)_v - \iota(y))$, which proves the first equality.

For the second equality, we first prove the inclusion "$\subseteq$". Let $x \in \mathcal{O}_K$, then

$$x^n + \sum_{i=1}^{n-1} a_i x^i = -a_0$$

for some $a_i \in \mathbb{Z}$. Now suppose that $v(x) < 0$ for $v \in M_K^0$. Then we observe that $v(a_i x^i) > v(x^n)$, since $v(a_i) \geq 0$ for all $a_i \in \mathbb{Z}$. As a consequence, we see that

$$0 \leq v(a_0) = v\left(x^n + \sum_{i=1}^{n-1} a_i x^i\right) = v(x^n) < 0,$$

which gives a contradiction. We therefore see that $v(x) \geq 0$, and thus $\iota_v(x) \in \mathcal{O}_{K_v}$. This in particular means that $\iota(x) \in \iota(K) \cap \mathbb{A}_K(S_\infty)$.

For the other inclusion, let $x \in K$ such that $\iota(x) \in \mathbb{A}_K(S_\infty)$. Then by definition, we see that $|x|_v = |\iota_v(x)|_v \leq 1$ for all $v \in M_K^0$. As an easy consequence of the unique prime ideal factorization in K, we find that $x \in \mathcal{O}_K$ (see [Kna07, Cor.6.6]). ■

Proposition 2.4.5. *The volume of $\mathbb{A}_K/\iota(K)$ with respect to the measure ν induced by the product measure $\mu = \prod_{v \in M_K} \mu_v$ equals $\sqrt{|\Delta_K|}$.*

Proof. The proof of this proposition is based on [CF67, Lem.XV.4.1.4 & Thm.XV.4.1.3].

Let ι_∞ denote the infinite part of ι, i.e., $\iota_\infty : K \to \prod_{v \in M_K^\infty} K_v$. Now let $\omega_1, ..., \omega_n$ be a basis of the ring of integers $\mathcal{O}_K$. Moreover, let $\sigma_i : K \to \mathbb{C}$ be all the distinct embeddings of K into $\mathbb{C}$. Then we recall that we have r_1 real embeddings and $2r_2$ complex embeddings such that $r_1 + 2r_2 = [K : \mathbb{Q}] = n$. We define $\{\tau_i\}_{i=1}^{r_1+r_2}$ as a complete set of pairwise non-conjugate embeddings of K into $\mathbb{C}$, ordered in such a way that the first r_1 embeddings are the real ones. The first observation that can be made is that

$$\iota_\infty : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \; x \mapsto (\tau_1(x), ..., \tau_{r_1+r_2}(x)).$$

Or, after identifying $\mathbb{C}^{r_2}$ with $\mathbb{R}^{2r_2}$, we have

$$\begin{aligned} \iota_\infty &: K \to \mathbb{R}^{r_1+2r_2}, \\ &x \mapsto (\tau_1(x), ..., \tau_{r_1}(x), \mathrm{Re}(\tau_{r_1+1}(x)), \mathrm{Im}(\tau_{r_1+1}(x)), ..., \mathrm{Re}(\tau_{r_2}(x)), \mathrm{Im}(\tau_{r_2}(x))), \text{ where} \\ \mathrm{Re}(\tau_j(x)) &= \frac{\tau_j(x) + \overline{\tau_j}(x)}{2}, \\ \mathrm{Im}(\tau_j(x)) &= \frac{\tau_j(x) - \overline{\tau_j}(x)}{2i}. \end{aligned}$$

Recalling that $\omega_1, ..., \omega_n$ is a basis of $\mathcal{O}_K$, we obtain a full lattice Γ_∞ inside $\mathbb{R}^{r_1+2r_2}$ spanned by $\iota_\infty(\omega_j)$ for $1 \le j \le n$. And thus we see that

$$\left(\prod_{v \in M_K^\infty} \mu_v\right)(\Gamma_\infty) = \mathrm{vol}(\Gamma_\infty) = |\det(A)| \cdot \mathrm{vol}([0,1]^n) = |\det(A)| \cdot \left(\prod_{v \in M_K^\infty} \mu_v\right)([0,1]^n),$$

where A is the matrix with columns given by $\iota_\infty(\omega_j)$. After doing obvious row operations, and after remembering that for complex places $v \in M_K^\infty$ we have twice the usual Lebesgue measure, we obtain that

$$\mathrm{vol}(\Gamma_\infty) = |\det(A)| \cdot 2^{r_2} = |(-2i)^{-r_2} \det(\sigma_k(\omega_l))_{k,l=1}^n| \cdot 2^{r_2} = \sqrt{|\Delta_K|}.$$

Let F_∞ be the fundamental domain corresponding to Γ_∞. This in particular means that the projection map $\prod_{v \in S_\infty} K_v \to \left(\prod_{v \in S_\infty} K_v\right)/\iota_\infty(\mathcal{O}_K)$ is bijective when restricted to F_∞. We now claim that the projection map $\pi_K : \mathbb{A}_K \to \mathbb{A}_K/\iota(K)$ is bijective after restricting to

$$F := F_\infty \times \prod_{v \notin S_\infty} \mathcal{O}_{K_v}.$$

For any $x \in \mathbb{A}_K$, there exists a $\iota(k) \in \iota(K)$ such that $x - \iota(k) \in \mathbb{A}_K(S_\infty)$ by the first equality in Lemma 2.4.4. As a consequence of the second equation in Lemma 2.4.4, we see that another element $\iota(k') \in \iota(K)$ has the same property if and only if $\iota(k) - \iota(k') \in \iota(\mathcal{O}_K)$. Therefore, the element $\iota(k)$ is unique modulo $\iota(\mathcal{O}_K)$. We can now choose $\iota(k)$ appropiately such that the infinite part $(x_v)_{v \in M_K^\infty}$ of x lies in F_∞, since F_∞ is a fundamental domain for $\left(\prod_{v \in S_\infty} K_v\right)/\iota_\infty(\mathcal{O}_K)$. This moreover implies that this choice for $\iota(k)$ is unique. We have now shown that for $[x] \in \mathbb{A}_K/\iota(K)$, there exists precisely one $y \in F$ such that $\pi_K(y) = [x]$. This in particular means that for every $x \in \mathbb{A}_K$ there exists precisely one $\iota(k) \in \iota(K)$ such that $x + \iota(k) \in F$.

Combining the above with Theorem A.1.2 yields the equality

$$\begin{aligned} \mu(F) = \int_{\mathbb{A}_K} \chi_F(x) \mathrm{d}\mu(x) &= \int_{\mathbb{A}_K/\iota(K)} \sum_{\iota(k) \in \iota(K)} \chi_F(x + \iota(k)) \mathrm{d}\nu([x]) \\ &= \int_{\mathbb{A}_K/\iota(K)} \mathrm{d}\nu([x]) = \nu(\mathbb{A}_K/\iota(K)). \end{aligned}$$

By the definition of the measure μ on $\mathbb{A}_K$, we now obtain the desired result as follows:

$$\nu(\mathbb{A}_K/\iota(K)) = \mu(F) = \left(\prod_{v\in M_K^\infty} \mu_v\right)(F_\infty) \cdot \prod_{v\in M_K} \mu_v(\mathcal{O}_{K_v}) = \sqrt{|\Delta_K|}.$$

■

Before we can give the Tamagawa measure on $V(\mathbb{A}_K)$, we have to introduce the so-called convergence factors.

Definition 2.4.6. Let V be a non-singular variety from Example 2.4.1, and ω an invariant differential 1-form. For each place v, let ω_v be the induced local measure on $V(K_v)$. A set $\{\lambda_v\}_{v\in M_K}$ of positive real numbers, i.e., $\lambda_v \in \mathbb{R}_{>0}$, with $\lambda_v = 1$ for $v \in M_K^\infty$ is called a *set of convergence factors* if the product

$$\prod_{v\in M_K^0} \lambda_v^{-1}\omega_v(V(\mathcal{O}_{K_v})) \tag{2.3}$$

is absolutely convergent.

Remark 2.4.7. Note that one could always take $\lambda_v = \omega_v(V(\mathcal{O}_{K_v}))$ for $v \in M_K^0$, unless there is a more desirable option.

In the sense of Theorem A.2.1, we obtain a unique measure on the adelic points of the varieties from Example 2.4.1, as a consequence of the absolute convergence of (2.3).

Definition 2.4.8. If $\{\lambda_v\}_{v\in M_K}$ is a set of convergence factors for V, then the *Tamagawa measure* τ (relative to the λ_v) derived from the invariant differential ω on $V(\mathbb{A}_K)$ is defined as the Haar measure inducing in each product

$$\prod_{v\in S} V(K_v) \times \prod_{v\notin S} V(\mathcal{O}_{K_v}),$$

where $S \subset M_K$ is a finite set containing S_∞, the product measure

$$|\Delta_K|^{-1/2} \prod_{v\in M_K} \lambda_v^{-1}\omega_v,$$

where ω_v are the induced local measures.

Following the constructions described in [Wei82], one sees that this definition is independent of the chosen differential ω. Namely, for any other differential $\omega' = c\omega$, we have that

$$|\Delta_K|^{-1/2} \prod_{v\in M_K} \lambda_v^{-1}\omega_v' = |\Delta_K|^{-1/2} \prod_{v\in M_K} \lambda_v^{-1}|c|_v\omega_v = |\Delta_K|^{-1/2} \prod_{v\in M_K} \lambda_v^{-1}\omega_v,$$

by the product formula 1.6.9.

Remark 2.4.9. The Tamagawa measure gives the impression to depend on the choice of the local Haar measures on K_v. Nevertheless, by the additional restriction that the volume of the quotient $\mathbb{A}_K/\iota(K)$ equals one, this dependency is eliminated. Since by Proposition 2.4.5 the quotient $\mathbb{A}_K/\iota(K)$ has volume $|\Delta_K|^{-1/2}$ with respect to the induced quotient measure ν by our chosen normalized Haar measures, we have to add the constant $|\Delta_K|^{-1/2}$ to our definition of the Tamagawa measure.

Chapter 3

Galois Cohomology

One of the fundamental connections between fields and groups is the so-called Galois theory. This theory is concerned with symmetries in the roots of a polynomial, but it is also useful to obtain results for extensions of fields. Évariste Galois introduced the theory, now known as Galois theory, for studying the roots of polynomials. In particular, the algebraic relations between them. It is well known that there are existing radical formulas for the roots of quadratic, cubic, and quartic polynomials. One of the main results obtained by Galois, is the proof of the general unsolvability of quintic equations. More precisely, not all roots of a quintic equation can be written as a radical expression. More on this can be found in [Mil21].

The setting will be an algebraic field extension L/K which is normal and separable. We therefore recall the basic theory about field extensions concerning these properties in Section 3.1.

A field extension that satisfies these properties is called a Galois extension. The central object corresponding to these extensions are the Galois groups, which possess many important fundamental properties. Section 3.2 is devoted to introduce the Galois theory.

An application of Galois theory can be found in cohomology theory. This theory is concerned with sequences of abelian groups. The Galois group associated to a certain field extension acts in a natural way on some abelian groups. One example of this can be found on elliptic curves, as we will see later in Section 4.4. In Sections 3.3 and 3.4 we give the constructions of basic group cohomology and cohomology for profinite groups, respectively. The latter one is needed for Galois groups of infinite Galois extensions, which are examples of profinite groups.

3.1 Field Extensions

We start with some theory about field extensions. This is needed to construct the notion of being a Galois extension. Before we continue with the definition of a Galois extension, we restate the meaning of being an algebraic extension, normal extension and a separable extension. We will closely follow [Cox12], and one could consult this source for any more detailed descriptions of this theory.

Definition 3.1.1 (Algebraic Extension)**.** A field extension L/K is *algebraic* if every $\alpha \in L$ is algebraic over K, i.e., there exists a non-constant polynomial $f \in K[X]$ such that $f(\alpha) = 0$.

Common examples of an algebraic extension, are finite extensions. Namely, if the degree $[L : K] = n < \infty$, then the elements $\{1, \alpha, ..., \alpha^n\}$ with $\alpha \in L$ are linearly dependent over K. Therefore, they satisfy an equation of the form $k_0 + k_1\alpha + ... + k_n\alpha^n = 0$ for some $k_i \in K$.

Definition 3.1.2. (cf. [Mil21, Prop.1.42, Def.1.43]) A field K is called *algebraically closed* if it satisfies one of the following equivalent conditions,

(i) Every non-constant $f \in K[X]$ splits in K.

(ii) Every non-constant $f \in K[X]$ has at least one root in K.

(iii) The irreducible $f \in K[X]$ are the polynomials of degree 1.

(iv) If L/K is a finite extension, then $L = K$.

Moreover, a field L is called an *algebraic closure* of a subfield K if it is algebraic over K, and algebraically closed.

Definition 3.1.3 (Splitting Field)**.** Let K be a field and $f \in K[X]$ be a non-constant polynomial. An extension L/K is called a *splitting field* for f over K if:

(i) f *splits completely* over L (into linear factors), i.e., $f = c(X-\alpha_1)(X-\alpha_2)...(X-\alpha_{\deg(f)})$ for some $c \in K$ and $\alpha_1, ..., \alpha_{\deg(f)} \in L$.

(ii) f does not split completely over any proper subfield F of L containing K.

This captures the notion of the smallest extension L/K over which a non-constant polynomial $f \in K[X]$ splits completely. The smallest such extension is clearly given by $L = K(\alpha_1, ..., \alpha_{\deg(f)})$, which is unique up to isomorphism.

Lemma 3.1.4. *Let $\varphi : K \to K'$ be a field isomorphism. Then we have an induced isomorphism $\widetilde{\varphi} : K[X] \to K'[X]$. Suppose that $f \in K[X]$ is irreducible, and let α be a zero of f in an extension of K. Moreover, let β be a zero of $\widetilde{\varphi}(f)$ in an extension of K'. Then there exists an isomorphism*

$$\Phi : K(\alpha) \to K'(\beta),$$

such that $\Phi_{|_K} = \varphi$ and $\Phi(\alpha) = \beta$.

Proof. Notice that $\widetilde{\varphi}$ maps the ideal (f) to $(\widetilde{\varphi}(f))$. Consequently, it clearly induces a well-defined field isomorphism

$$\psi : K[X]/(f) \to K'[X]/(\widetilde{\varphi}(f)),\ [g] \mapsto [\widetilde{\varphi}(g)],$$

since f is irreducible. Moreover, we have the canonical isomorphisms

$$\rho_\alpha : K[X]/(f) \to K(\alpha), [X] \mapsto \alpha$$
$$\rho_\beta : K[X]/(f) \to K(\beta), [X] \mapsto \beta.$$

As a consequence, we see that we have an isomorphism $\Phi := \rho_\beta \circ \psi \circ \rho_\alpha^{-1} : K(\alpha) \to K(\beta)$ satisfying

$$\Phi(k) = \rho_\beta(\psi([k])) = \rho_\beta([\varphi(k)]) = \varphi(k)$$

for all $k \in K$, and $\Phi(\alpha) = \beta$. ■

Proposition 3.1.5. *Let $\varphi : K \to K'$ be a field isomorphism, and $\widetilde{\varphi}$ the induced isomorphism between $K[X]$ and $K'[X]$. Let $f \in K[X]$, and L/K be a splitting field for f. Moreover, if L'/K' is a splitting field for $\widetilde{\varphi}(f)$, then there is an isomorphism from L to L' which extends φ.*

Proof. Write $f = \prod_{i=1}^{n} p_i$ as product of irreducibles $p_i \in K[X]$. Then $\widetilde{\varphi}(f) = \prod_{i=1}^{n} \widetilde{\varphi}(p_i)$, and each $\widetilde{\varphi}(p_i)$ is irreducible in $K'[X]$. If $[L : K] = 1$, then f already splits completely over K. As a consequence, we easily see that $[L' : K'] = 1$ as well, implying that $\varphi : L \to L'$ is the desired isomorphism.

Suppose that $[L : K] > 1$, and that the result holds for all polynomials of degree strictly smaller than $[L : K]$. Note that f splits completely in $L[X]$, i.e., $f = c\prod_{i=1}^{n}(X - \alpha_i)$ where each α_i is a root of f. Let $p_1 \in K[X]$ be the minimal polynomial of α_1, then it is irreducible and it divides f. Now notice that $\widetilde{\varphi}(p_1)$ is also irreducible in $K'[X]$, and a divisor of $\widetilde{\varphi}(f)$. Consequently, since $\widetilde{\varphi}(f)$ splits completely in L', $\widetilde{\varphi}(p_1)$ has a root β_1 in L'. Thus by the previous lemma, we get a field isomorphism $\Phi_1 : K(\alpha_1) \to K'(\beta_1)$ satisfying $\Phi_{1|_K} = \varphi$ and $\Phi_1(\alpha_1) = \beta_1$.

Now let $\beta_2, ..., \beta_n$ be the remaining roots of $\widetilde{\varphi}(f)$. Note that in $K(\alpha_1)[X]$, f factors as $f = (X - \alpha_1)h$ for some polynomial $h \in K(\alpha_1)[X]$ of degree $n - 1$. As a consequence, we see that $\widetilde{\varphi}(f) = \widetilde{\Phi_1}(f) = (X - \beta_1)\widetilde{\Phi_1}(h)$ in $K'(\beta_1)[X]$. In $L[X]$ we have

$$(X - \alpha_1)h = f = c\prod_{i=1}^{n}(X - \alpha_i),$$

which implies that $h = c\prod_{i=2}^{n}(X - \alpha_i)$. Consequently, we observe that $L/K(\alpha_1)$ is a splitting field for h. Similarly, $L'/K'(\beta_1)$ is a splitting field for $\widetilde{\Phi_1}(h)$. Since $[L : K(\alpha_1)] < [L : K]$, we find by the induction hypothesis a field isomorphism $\Phi : L \to L'$ satisfying $\Phi_{|_{K(\alpha_1)}} = \Phi_1$. Which in particular means that $\Phi_{|_K} = \Phi_{1|_K} = \varphi$. ■

Corollary 3.1.6. *Let K be a field and $f \in K[X]$ a non-constant polynomial. If L and L' are splitting fields of f over K, then there is an isomorphism $\Phi : L \to L'$ that is the identity on K.*

Proof. This is a direct consequence of Proposition 3.1.5, since we can just take $\varphi = \mathrm{id}_K$. ■

Definition 3.1.7 (Normal Extension)**.** An algebraic extension L/K is called *normal*, if every irreducible polynomial in $K[X]$ having a root in L splits completely over L.

Proposition 3.1.8. *Let L/K be a field extension. Then L is a splitting field for some non-constant $f \in K[X]$ if and only if L/K is a finite normal extension.*

Proof. Suppose that L/K is a finite normal extension. Then $L = K(\alpha_1, ..., \alpha_n)$, where $\{\alpha_1, ..., \alpha_n\}$ forms a basis of the K-vector space L. Let $p_i \in K[X]$ be the minimal polynomial of α_i. Then p_i is irreducible with a root $\alpha \in L$. Therefore, p_i splits completely over L by the normality of the extension L/K. As a consequence, the polynomial $f = \prod_{i=1}^{n} p_i$ also splits completely over L. It follows that L/K is a splitting field for $f \in K[X]$.

For the converse, assume that L is a splitting field for some nonconstant $f \in K[X]$. Then $f = c\prod_{i=1}^{n}(X - \alpha_i)$ for some $\alpha_i \in L$ and $c \in K$. Moreover, we have $L = K(\alpha_1, ..., \alpha_n)$. Thus the extension L/K is finite, see [Cox12, Thm.4.4.3]. Let $p \in K[X]$ be an irreducible polynomial that has a root $\alpha \in L$. Moreover, let F be a splitting field of the polynomial $p \in K[X]$ over L. Then we are left to show that $F = L$, to conclude that L is a normal extension of K. Note that we are in the following situation,

$$\begin{tikzcd}
 & F & \\
L(\alpha) \arrow[ur, hook] & & L(\beta) \arrow[ul, hook] \\
 & L \arrow[uu, hook] \arrow[ul, hook] \arrow[ur, hook] & \\
K(\alpha) \arrow[uu, hook] \arrow[ur, hook] & & K(\beta) \arrow[uu, hook] \\
 & K \arrow[uu, hook] \arrow[ul, hook] \arrow[ur, hook] & .
\end{tikzcd}$$

Let $\beta \in F$ be another root of p, then we would like to show that $\beta \in L$. Since p is irreducible, and both α and β are zeros of p, we find by Lemma 3.1.4 that there exists an isomorphism $\Phi : K(\alpha) \to K(\beta)$ that is an identity on K. Therefore, the extensions $K(\alpha)/K$ and $K(\beta)/K$ are isomorphic, meaning that $[K(\alpha) : K] = [K(\beta) : K]$. Moreover, $L(\alpha)$ is clearly a splitting field for f over $K(\alpha)$. Similarly, $L(\beta)$ is also a splitting field for f, but now over $K(\beta)$. Notice that Φ induces a natural map $\widetilde{\Phi} : K(\alpha)[X] \to K(\beta)[X]$, and that $\widetilde{\Phi}(f) = f$ since $f \in K[X]$. We now find by Proposition 3.1.5 that there is an isomorphism $\Psi : L(\alpha) \to L(\beta)$ which extends Φ. This means that the field extensions $L(\alpha)/K(\alpha)$ and $L(\beta)/K(\beta)$ are isomorphic, implying that $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$. From the tower law applied to the diagram above, combined with the results found, we find that

$$[L(\alpha) : L][L : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = [L(\beta) : K(\beta)][K(\beta) : K] = [L(\beta) : L][L : K].$$

Thus $[L(\alpha) : L] = [L(\beta) : L]$, and since $\alpha \in L$ this implies that $[L(\beta) : L] = 1$. Consequently, $\beta \in L$ which finishes the proof. ■

Proposition 3.1.9. *Let L/K be a field extension. Then L is a splitting field of a collection of polynomials $\mathcal{F}$ over K if and only if L/K is a normal extension.*

Proof. “ $\Longrightarrow$ ” Suppose that L is a splitting field of a collection of polynomials $\mathcal{F}$ over K. Let $Z_{\mathcal{F}}$ be the set consisting of the roots of the polynomials in $\mathcal{F}$ in L, then $L = K(Z_{\mathcal{F}})$. Now let $f \in K[X]$ be an irreducible polynomial with root $\alpha \in L$. Then α is contained in $K(Z_\alpha)$ for some finite subset Z_α of $Z_{\mathcal{F}}$. Consider the set M_{Z_α} consisting of the minimal polynomials over K of the elements in Z_α. Moreover, define the finite set

$$Z := \{x \in Z_{\mathcal{F}} \mid g(x) = 0 \text{ for some } g \in M_{Z_\alpha}\}.$$

As a consequence, we find that $K(Z)$ is a splitting field of the finite collection M_{Z_α} of polynomials over K. Therefore, by Proposition 3.1.8 we conclude that $K(Z)/K$ is a normal extension. Recall that $\alpha \in K(Z_\alpha) \subset K(Z)$. Therefore, by normality of $K(Z)/K$ the polynomial f splits completely over $K(Z)$, and thus also over L. Since f was arbitrary, we conclude that L/K is also a normal extension.

“ $\Longleftarrow$ ” Assume that L/K is a normal extension. Let $\alpha \in L$, and $f_\alpha \in K[X]$ be the corresponding minimal polynomial. Then by the normality of L/K we see that f_α splits completely over L. Whence, L is clearly the splitting field of the collection of minimal polynomials $\mathcal{F} = \{f_\alpha \in K[X] \mid f_\alpha \text{ minimal polynomial for } \alpha \in L\}$. ■

Definition 3.1.10 (Separable Polynomial)**.** A non-constant polynomial $f \in K[X]$ is called *separable* over the field K if it has no repeated roots in a splitting field L of f. That means that $f = c\prod_{i=1}^{n}(X - \alpha_i)$, where each $\alpha_1, ..., \alpha_n$ are distinct roots in a splitting field L of K.

Definition 3.1.11 (Separable Extension)**.** Let L/K be an algebraic extension. An element $\alpha \in L$ is called *separable* over K if its minimal polynomial p has no repeated roots in a splitting field of p. The extension L/K is called *separable* if each $\alpha \in L$ is separable over K.

Definition 3.1.12. (cf. [Mil21, Def.6.10]) A field L is called *separably closed* if every non-constant separable polynomial in $L[X]$ splits in L. Moreover, a field L is called a *separable closure* over K, if L/K is algebraic and separable, and L is separably closed.

Remark 3.1.13. Every field K has a corresponding unique (up to isomorphism) separable closure and algebraic closure. This is proven in [Mil21, CH.6]. These will be denoted by K^{sep} and K^{alg}, respectively.

Definition 3.1.14. A field K is called *perfect*, if it has characteristic 0, or else it has characteristic $p > 0$ and every element of K is a p-th power.

Proposition 3.1.15. (cf. [Kna07, Prop.7.15]) *A field K is perfect if and only if every algebraic extension of K is separable.*

Remark 3.1.16. The above in particular implies that the separable and algebraic closure of a perfect field K coincide. It is therefore convenient to write $\overline{K}$ for $K^{\text{sep}} = K^{\text{alg}}$.

3.2 Galois Theory

In the previous section we have discussed different structures of field extensions. One of the basic algebraic tools of those field extensions, is their connection with certain groups. This theory is also known as Galois theory. The main idea is that the Galois theory applies to splitting fields of certain polynomials, and studies the permutations of the corresponding roots. Main references for this section are [DF04] and [Mil21].

We start by providing the definition of one of the main objects of interest.

Definition 3.2.1. Let L/K be a field extension. An *K-automorphism* on L is a field isomorphism $\sigma : L \to L$ with the additional property that $\sigma(x) = x$ for all $x \in K$. We define the *automorphism group* on L that fixes K as

$$\text{Aut}(L/K) := \{\sigma \in \text{Aut}(L) \mid \sigma(x) = x, \text{ for all } x \in K\}.$$

It is easily verified that $\text{Aut}(L/K)$ indeed defines a group. We call this group the *Galois group* of L over K, denoted as $\text{Gal}(L/K)$.

For now, we restrict to finite Galois theory, i.e., we assume L/K to be a finite extension. Moreover, for $H \leq \text{Gal}(L/K)$, we write $L^H := \{x \in L \mid hx = x, \ \forall h \in H\}$ for the fixed field under H. It is easily verified that L^H is a subfield of L containing K. These fields will play an important role in the fundamental theorem of Galois theory.

Theorem 3.2.2. (cf. [DF04, CH.14]) *Let L/K be a finite extension. The following conditions are equivalent:*

(i) L is the splitting field of a separable polynomial in $K[X]$.

(ii) $K = \{x \in L \mid \sigma(x) = x$ for all $\sigma \in \text{Gal}(L/K)\}$.

(iii) *L/K is a normal, and separable extension.*

(iv) $|\operatorname{Gal}(L/K)| = [L : K]$.

Definition 3.2.3. We call a finite extension L/K a *Galois extension*, if it satisfies any of the equivalent conditions from Theorem 3.2.2.

Theorem 3.2.4 (Fundamental Theorem of Finite Galois Theory)**.** *Let L/K be a finite Galois extension. Then there is a bijection*

$$\{F \text{ field} \mid K \subset F \subset L\} \longleftrightarrow \{H \leq \operatorname{Gal}(L/K)\},$$

given by the correspondence,

$$\begin{aligned} F &\longrightarrow \operatorname{Gal}(L/F), \\ L^H &\longleftarrow H. \end{aligned}$$

Let F be an intermediate field of L and K, and H be the corresponding subgroup of $\operatorname{Gal}(L/K)$*. Then under this one-to-one correspondence we also have*

(i) $[L : F] = |\operatorname{Gal}(L/F)|$ *and* $[F : K] = |\operatorname{Gal}(L/K) : \operatorname{Gal}(L/F)|$,

(ii) *L/F is Galois,*

(iii) *F/K is Galois if and only if H is a normal subgroup of* $\operatorname{Gal}(L/K)$*. Moreover, then* $\operatorname{Gal}(F/K) \cong \operatorname{Gal}(L/K)/H$*.*

Proof. We omit the proof of this theorem. For an expanded version of this theorem, and a proof one could take a look at [DF04, Thm.14, p.574]. ■

Now that we have seen Galois theory for finite extensions, we can expand it to algebraic extensions in general. These type of extensions may be infinite. By considering Theorem 3.2.2 (iii), one natural way to extend the definition of a Galois extension to algebraic extensions is as follows.

Definition 3.2.5. We call an algebraic extension L/K a *Galois extension* if it is normal and separable. Then $\operatorname{Aut}(L/K)$ is called the *Galois group* of L/K, also denoted as $\operatorname{Gal}(L/K)$.

Example 3.2.6. One of the commonly encountered Galois extensions is the separable closure K^{sep} of K. The corresponding Galois group $\operatorname{Gal}(K^{\text{sep}}/K)$ is also called the *absolute Galois group* of K.

One would like the fundamental theorem of finite Galois theory (Theorem 3.2.4) to still hold for infinite Galois extensions. Nevertheless, it turns out that a little bit more has to be done. This can be seen by an example also given in [DF04, p.651].

Example 3.2.7. Consider the splitting field K of the set of polynomials

$$\{f_p = X^2 - p \in \mathbb{Q}[X] \mid p \in \mathbb{Z}^+ \text{ prime}\}$$

over $\mathbb{Q}$. Then notice that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, ...) = \mathbb{Q}[\sqrt{2}, \sqrt{3}, ...]$. This extension is clearly infinite, algebraic and separable. The normality of the extension follows from Proposition 3.1.9, which means that $K/\mathbb{Q}$ is a Galois extension. Let α be a zero of $f_p(x)$ and $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$, then

$$0 = \sigma(f_p(\alpha)) = \sigma(\alpha)^2 - p = f(\sigma(\alpha)).$$

Therefore, we see that σ permutes the zeros of f_p for all $p \in \mathbb{Z}^+$. This means that σ maps $\sqrt{p}$ to $\sqrt{p}$ or $-\sqrt{p}$ for all $p \in \mathbb{Z}^+$. Moreover, σ is uniquely determined by these permutations, and in this case all permutations of the zeros occur in the Galois group. In addition, note that $\sigma^2 = \mathrm{id}_K$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. This induces the following group isomorphism,

$$\psi : \mathrm{Aut}(K/\mathbb{Q}) \longrightarrow \prod_{\substack{p \in \mathbb{Z}^+ \\ p \text{ prime}}} \mathbb{Z}/2\mathbb{Z},$$

$$\sigma \mapsto (x_{\sigma,p})_p, \; x_{\sigma,p} := \begin{cases} 0 & \text{if } \sigma(\sqrt{p}) = \sqrt{p} \\ 1 & \text{if } \sigma(\sqrt{p}) = -\sqrt{p}. \end{cases}$$

This implies that $\mathrm{Gal}(K/\mathbb{Q})$ can be viewed as an infinite dimensional vector space over the finite field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Now consider the so-called dual space of $\mathrm{Aut}(K/\mathbb{Q})$, which is given by

$$\mathrm{Aut}(K/\mathbb{Q})^* = \mathrm{Hom}_{\mathbb{F}_2}(\mathrm{Aut}(K/\mathbb{Q}), \mathbb{F}_2) = \{\varphi : \mathrm{Aut}(K/\mathbb{Q}) \to \mathbb{F}_2 \text{ linear transformation}\}.$$

The dual space of an infinite dimensional vector space has dimension strictly bigger than the vector space itself[1]. This means that $\dim(\mathrm{Aut}(K/\mathbb{Q})^*) > \dim(\mathrm{Aut}(K/\mathbb{Q}))$, which in turn implies that there are uncountably many linear transformations from $\mathrm{Aut}(K/\mathbb{Q})$ to $\mathbb{F}_2$.

Note that any pair of distinct $\varphi, \varphi' \in \mathrm{Aut}(K/\mathbb{Q})^*$ have different kernels. Therefore, the cardinality of $\{\ker(\varphi) \mid \varphi \in \mathrm{Aut}(K/\mathbb{Q})^*\}$ and $\mathrm{Aut}(K/\mathbb{Q})^*$ are the same. Here we note that the cardinality equals $2^{\mathbb{N}}$, meaning that it is uncountably infinite. Note also that these kernels are subgroups of index 2 of $\mathrm{Aut}(K/\mathbb{Q})$, since $\mathrm{Aut}(K/\mathbb{Q})/\ker(\varphi) \cong \mathbb{F}_2$.

Under the Galois correspondence as in Theorem 3.2.4, each $\ker(\varphi)$ should correspond to a different intermediate field $\mathbb{Q} \subset F \subset K$ such that $[F : \mathbb{Q}] = 2$. Nevertheless, the only quadratic field extensions of $\mathbb{Q}$ contained in K are given by $\mathbb{Q}(\sqrt{q})$ for some prime q. These are only countably many, while we already found uncountably many subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ of index 2. As a consequence, we see that the fundamental theorem as stated in Theorem 3.2.4 does not hold in the infinite case.

The example above suggests that there are probably a lot more subgroups of $\mathrm{Gal}(L/K)$ than intermediate fields of L and K. Therefore, we have to find a way to filter out the subgroups that do form a one-to-one correspondence with the intermediate fields. We will see that this can be done by putting a topology on the Galois groups, which will be called the Krull topology. The construction of this topology relies on the fact that the Galois group can be given as an inverse limit of finite Galois groups. The inverse limit will depend on an inverse system for which we need the notion of the composite of fields.

Definition 3.2.8. Let L/K be a field extension and F_1, F_2 be two intermediate fields of L and K. The *composite* of F_1 and F_2 in L is defined as the smallest subfield of L containing both F_1 and F_2, or equivalently

$$F_1F_2 = \bigcap_{\substack{F \text{ field s.th} \\ F_1, F_2 \subset F \subset L}} F.$$

Lemma 3.2.9. *Let L/K be a Galois extension, and $\mathcal{F}$ be the collection of finite Galois extensions F/K with F contained in L. Suppose that $F_1, F_2 \in \mathcal{F}$, then $F_1F_2 \in \mathcal{F}$. Moreover,* $\mathrm{Gal}(L/F_1) \cap \mathrm{Gal}(L/F_2) = \mathrm{Gal}(L/F_1F_2)$.

[1] This is stated as a Theorem in 3.12 in [Rom07].

Proof. If $F_1, F_2 \in \mathcal{F}$, then F_1 and F_2 are both splitting fields of a separable polynomial $f_1, f_2 \in K[X]$ respectively. Then F_1F_2 is the splitting field of the polynomial f_1f_2 over K. This polynomial can have multiple roots. We therefore consider the separable polynomial $g := (f_1f_2)/\gcd(f_1, f_2)$, which by the Euclidean algorithm lies in $K[X]$. We then observe that F_1F_2 is the splitting field of the separable polynomial g over K, meaning that $F_1F_2 \in \mathcal{F}$.

For the other part of this lemma, note that the set $L^{\langle\sigma\rangle} := \{x \in L \mid \sigma(x) = x\}$ is a fixed field for the subgroup $\langle\sigma\rangle < \mathrm{Aut}(L/K)$. Consequently, we find by definition of the compositum of two fields, that

$$\sigma \in \mathrm{Gal}(L/F_1) \cap \mathrm{Gal}(L/F_2) \Leftrightarrow F_1, F_2 \subset L^{\langle\sigma\rangle} \Leftrightarrow F_1F_2 \subset L^{\langle\sigma\rangle} \Leftrightarrow \sigma \in \mathrm{Gal}(L/F_1F_2).$$

■

Suppose that L/K is a Galois extension, and define

$$\mathcal{F} := \{F \text{ field} \mid K \subset F \subset L, \text{ and } F/K \text{ finite Galois extension}\}. \tag{3.1}$$

Note that $\mathcal{F}$ together with the inclusion ordering is a partially ordered directed set. Namely, for each $F_1, F_2 \in \mathcal{F}$ we have $F_1, F_2 \subset F_1F_2$, the compositum of both fields in L. If $F_1, F_2 \in \mathcal{F}$ are such that $F_1 \subset F_2$, then we can define the group homomorphism

$$\varphi_{F_1F_2} : \mathrm{Gal}(F_2/K) \longrightarrow \mathrm{Gal}(F_1/K),\ \sigma \mapsto \sigma_{|F_1}.$$

Thus $(\mathrm{Gal}(F/K), \varphi_{F_1F_2})_{\mathcal{F}}$ defines an inverse system indexed with $\mathcal{F}$ of finite groups. The inverse limit in the category of groups is given by

$$\varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K) = \left\{ (\sigma_F)_{F\in\mathcal{F}} \in \prod_{F\in\mathcal{F}} \mathrm{Gal}(F/K) \;\middle|\; \varphi_{F_1F_2}(\sigma_{F_2}) = \sigma_{F_1} \text{ if } F_1 \subset F_2 \right\}.$$

Now notice that the group homomorphisms φ_{FL} induce a group homomorphism

$$\Phi : \mathrm{Gal}(L/K) \longrightarrow \prod_{F\in\mathcal{F}} \mathrm{Gal}(F/K),\ \sigma \mapsto (\sigma_{|F})_{F\in\mathcal{F}}.$$

Theorem 3.2.10. *Let L/K be a Galois extension. The map Φ, defined above, determines a group isomorphism between* $\mathrm{Gal}(L/K)$ *and the inverse limit* $\varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K)$.

Proof. It is clear that Φ indeed defines a group homomorphism and that it maps into the inverse limit $\varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K)$. We are left to show that Φ is a bijection between the desired sets.

For injectivity, first be aware of the fact that $L = \bigcup_{F\in\mathcal{F}} F$. Now if $\Phi(\sigma) = \tau$, then $\sigma_{|F} = \tau_{|F}$ for all $F \in \mathcal{F}$. Thus we have $\sigma = \tau$, proving that Φ is injective.

For surjectivity, let $(\sigma_F)_{F\in\mathcal{F}} \in \varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K)$. Define $\sigma(x) = \sigma_F(x)$ for $x \in F$, which gives a definition on all of $L = \bigcup_{F\in\mathcal{F}} F$. We have to show that σ is well-defined. Suppose that $x \in E := F_1 \cap F_2$ for some $F_1, F_2 \in \mathcal{F}$. Note that the intersection of normal/separable extensions is again normal/separable. Therefore, E is also a finite Galois extension of K. Consequently, we find by definition of the inverse limit that $\varphi_{EF_1}(\sigma_{F_1}) = \sigma_E = \varphi_{EF_2}(\sigma_{F_2})$. So $\sigma_{F_1}(x) = \sigma_{F_2}(x)$, showing that σ is well-defined. By construction, we now have the desired $\sigma \in \mathrm{Gal}(L/K)$ satisfying $\Phi(\sigma) = (\sigma_F)_{F\in\mathcal{F}}$. ■

In general, if we have an inverse system of topological groups, the corresponding inverse limit coincides with the inverse limit in the category of groups endowed with the subspace topology it inherits from the product topology. In the case of a Galois extension L/K we get such an inverse system by putting the discrete topology on each $\mathrm{Gal}(F/K)$ for every finite Galois extension $K \subset F \subset L$. Consequently, we get a natural topology on the inverse limit of these Galois groups. Therefore, the isomorphism Φ from Theorem 3.2.10 induces a topology on the Galois group $\mathrm{Gal}(L/K)$, leading to the following definition.

Definition 3.2.11 (Krull Topology)**.** Let L/K be a Galois extension. Give $\varprojlim_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$ the subspace topology it inherits from $\prod_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$, where $\operatorname{Gal}(F/K)$ is endowed with the discrete topology. Then the naturally induced topology by the isomorphism Φ between $\operatorname{Gal}(L/K)$ and $\varprojlim_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$ is called the *Krull topology.*

Proposition 3.2.12. *A basis for the Krull topology on* $\operatorname{Gal}(L/K)$ *is given by the collection* $\mathcal{B} := \{\sigma H \mid \sigma \in \operatorname{Gal}(L/K),\ H = \operatorname{Gal}(L/F) \textit{ with } F \in \mathcal{F}\}$*, where* $\mathcal{F}$ *is the collection as defined in (3.1).*

Proof. Note that $\operatorname{Gal}(L/K)$ is isomorphic to the inverse limit $\varprojlim_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$ under Φ. The Krull topology on $\operatorname{Gal}(L/K)$ is induced by the map Φ. To make things more easy, we can view Φ as a map from $\operatorname{Gal}(L/K)$ to the product space $\prod_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$. This clearly will not affect the induced Krull topology by Φ. Now a basis for the Krull topology will be given by the collection of opens $\Phi^{-1}(U)$, where U is in the basis of the product space $\prod_{F\in\mathcal{F}} \operatorname{Gal}(F/K)$. The basis opens U are of the form

$$\prod_{F\in\mathcal{F}_0} \{\rho_F\} \times \prod_{F\notin\mathcal{F}_0} \operatorname{Gal}(F/K),$$

where $\mathcal{F}_0 \subset \mathcal{F}$ is finite and $\rho_F \in \operatorname{Gal}(F/K)$. Moreover, by construction of Φ, we find that

$$\Phi^{-1}(U) = \left(\bigcap_{F\in\mathcal{F}_0} \operatorname{res}_F^{-1}(\{\rho_F\})\right) \cap \left(\bigcap_{F\notin\mathcal{F}_0} \operatorname{res}_F^{-1}(\operatorname{Gal}(F/K))\right) = \left(\bigcap_{F\in\mathcal{F}_0} \operatorname{res}_F^{-1}(\{\rho_F\})\right).$$

Each $\rho_F \in \operatorname{Gal}(F/K)$ has a lifting automorphism $\sigma_F \in \operatorname{Gal}(L/K)$ such that $\sigma_{F|_F} = \rho_F$[2]. Now note that $\operatorname{res}_F^{-1}(\{\rho_F\}) = \{\tau \in \operatorname{Gal}(L/K) \mid \tau_{|_F} = \sigma_{F|_F} = \rho_F\} = \sigma_F \operatorname{Gal}(L/F)$. As a consequence, we see that a basis for the Krull topology is given by

$$\mathcal{B}^{'} := \left\{ \bigcap_{F\in\mathcal{F}_0} \sigma_F \operatorname{Gal}(L/F) \;\middle|\; \mathcal{F}_0 \subset \mathcal{F} \text{ finite},\ \sigma_F \in \operatorname{Gal}(L/K)\right\}.$$

We will now show that $\mathcal{B}' = \mathcal{B}$. The inclusion $\mathcal{B} \subset \mathcal{B}'$ is clear. Let $\bigcap_{F\in\mathcal{F}_0} \sigma_F \operatorname{Gal}(L/F) \in \mathcal{B}'$ be non-empty, then there exists a $\sigma \in \bigcap_{F\in\mathcal{F}_0} \sigma_F \operatorname{Gal}(L/F)$, meaning that $\sigma_{|_F} = \sigma_{F|_F}$ for all $F \in \mathcal{F}_0$. Now notice that

$$\begin{aligned}\bigcap_{F\in\mathcal{F}_0} \sigma_F \operatorname{Gal}(L/F) = \bigcap_{F\in\mathcal{F}_0} \{\tau \in \operatorname{Gal}(L/K) \mid \tau_{|_F} = \sigma_{F|_F}\} &= \bigcap_{F\in\mathcal{F}_0} \{\tau \in \operatorname{Gal}(L/K) \mid \tau_{|_F} = \sigma_{|_F}\} \\ &= \sigma \left(\bigcap_{F\in\mathcal{F}_0} \operatorname{Gal}(L/F)\right).\end{aligned}$$

Since the index set $\mathcal{F}_0$ is finite, we can apply Lemma 3.2.9 finitely many times to induce that

$$\sigma\left(\bigcap_{F\in\mathcal{F}_0} \operatorname{Gal}(L/F)\right) = \sigma \operatorname{Gal}(L/F_0),$$

where F_0 is the compositum of the fields $F \in \mathcal{F}_0$. This implies that every element in $\mathcal{B}'$ is contained in $\mathcal{B}$, which finishes the proof. ■

[2] For a proof of this statement, one could consult Corollary A.2 in [Con20]

Theorem 3.2.13 (Fundamental Theorem for Infinite Galois Theory)**.** (cf. [Mil21, Thm.7.12]) *Let L/K be a Galois extension. Then there is a bijection*

$$\{F \text{ field} \mid K \subset F \subset L\} \longleftrightarrow \{H \leq \mathrm{Gal}(L/K) \text{ closed with respect to the Krull topology}\}$$

given by the correspondence,

$$\begin{aligned} F &\longrightarrow \mathrm{Gal}(L/F), \\ L^H &\longleftarrow H. \end{aligned}$$

Moreover,

(i) for closed subgroups H_1, H_2 of $\mathrm{Gal}(L/K)$ we have, $H_1 \supset H_2 \Leftrightarrow L^{H_1} \subset L^{H_2}$.

(ii) a closed subgroup H of $\mathrm{Gal}(L/K)$ is open if and only if $[L^H : K] < \infty$, in which case $|\mathrm{Gal}(L/K) : H| = [L^H : K]$.

(iii) for $\sigma \in \mathrm{Gal}(L/K)$, if a closed subgroup H corresponds to a intermediate field F under the bijection, then $\sigma H \sigma^{-1}$ corresponds to σF, i.e., $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$, or equivalently $\mathrm{Gal}(L/\sigma F) = \sigma \,\mathrm{Gal}(L/F)\sigma^{-1}$.

(iv) a closed subgroup $H \leq \mathrm{Gal}(L/K)$ is normal if and only if L^H is Galois over K, in which case $\mathrm{Gal}(L^H/K) \cong G/H$.

3.3 Basic Group Cohomology

In this section we treat some basic group cohomology theory. The highest cohomology groups we will restrict ourselves to is the first cohomology group. For a more detailed description of cohomology theory for groups, one could consult [CF67, p.94-115]. We will mostly follow [Sil09, Appendix B], in which is also restricted to the first two cohomology groups.

Definition 3.3.1. Let G be a group. A *G-module* consists of an abelian group M together with an *action of* G on M, i.e., a map $\mu : G \times M \to M$ such that

(i) $\sigma(m + m') = \sigma m + \sigma m'$, for all $\sigma \in G$ and $m, m' \in M$.

(ii) $(\sigma\tau)(m) = \sigma(\tau m)$, for all $\sigma, \tau \in G$ and $m \in M$.

(iii) $1m = m$ for all $m \in M$.

Moreover, a morphism $\varphi : M \to N$ of G-modules is a group homomorphism φ that is also *G-equivariant*, i.e., $\varphi(\sigma m) = \sigma\varphi(m)$ for all $\sigma \in G$ and $m \in M$.

In terms of category theory we have a functor $H^0(G, -) : \mathbf{G\text{-}mod} \to \mathbf{Ab}$, that maps a G-module M to the subgroup $M^G = \{m \in M \mid \sigma m = m, \ \forall \sigma \in G\}$ of M. The submodule M^G is also called the G-invariant subgroup of M. The functor $H^0(G, -)$ associates a morphism $\varphi : M \to N$ of G-modules to the morphism

$$H^0(G, \varphi) : M^G \to N^G, \ m \mapsto \varphi(m).$$

Note that this morphism is well-defined, since $\sigma\varphi(m) = \varphi(\sigma m) = \varphi(m)$ for all $\sigma \in G$ and $m \in M^G$. This map clearly preserves the identity morphism and the composition of morphisms, and thus $H^0(G, -)$ is indeed a functor. For simplicity, we write $\varphi^G := H^0(G, \varphi)$ since it is just the restriction of φ to the G-invariant submodule of M.

We will not be interested in any higher cohomology groups than the first cohomology group. Before we can construct this functor, we need some definitions.

Definition 3.3.2 (Crossed Homomorphism)**.** A map $x : G \to M$ is called a *crossed homomorphism* (or 1-*cocycle*), if $x(\sigma\tau) = \sigma x(\tau) + x(\sigma)$ for all $\sigma, \tau \in G$. These 1-cocycles form an abelian group, denoted as $Z^1(G, M)$.

Definition 3.3.3 (Principal Crossed Homomorphism)**.** The crossed homomorphisms of the form $x(\sigma) = \sigma m - m$ for some $m \in M$ are called *principal* (or 1-*coboundaries*). These 1-coboundaries also form an abelian group, which is denoted as $B^1(G, M)$.

The first cohomology is now given as a functor $H^1(G, -) : \textbf{G-mod} \to \textbf{Ab}$, mapping a G-module M to the abelian group $Z^1(G, M)/B^1(G, M)$. To a morphism $\varphi : M \to N$ of G-modules, it associates the morphism

$$H^1(G, \varphi) : Z^1(G, M)/B^1(G, M) \to Z^1(G, N)/B^1(G, N),\ [x] \mapsto [\varphi \circ x].$$

It is easily seen that this morphism is well-defined, and that $H^1(G, -)$ preserves the identity and composition of morphisms.

Definition 3.3.4. The *zeroth* and *first cohomology groups* of the G-module M are respectively given by,

$$H^0(G, M) := M^G,\ H^1(G, M) := Z^1(G, M)/B^1(G, M).$$

Given an exact sequence of G-modules

$$0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} P \to 0, \tag{3.2}$$

there is a canonical map $\delta : P^G \to H^1(G, M)$. Namely, let $p \in P^G$. Then by surjectivity of ψ there exists a $n_p \in N$ such that $\psi(n_p) = p$. Note that we have a principal crossed homomorphism $x_p : G \to N$ defined as $x_p(\sigma) = \sigma n_p - n_p$. Then

$$(\psi \circ x_p)(\sigma) = \psi(\sigma n_p - n_p) = \sigma p - p = 0,$$

since $p \in P^G$. Therefore, we have $x_p(\sigma) \in \ker(\psi) = \operatorname{im}(\varphi)$. By injectivity of φ, we now find a unique $m_\sigma \in M$ such that $\varphi(m_\sigma) = x_p(\sigma)$. Consequently, we can define a map $y_p : G \to M$ mapping σ to $m_\sigma = \varphi^{-1}(x_p(\sigma))$. Note that

$$\varphi(m_{\sigma\tau}) = x_p(\sigma\tau) = \sigma x_p(\tau) + x_p(\sigma) = \sigma\varphi(m_\tau) + \varphi(m_\sigma) = \varphi(\sigma m_\tau + m_\sigma),$$

implying that $y_p(\sigma\tau) = m_{\sigma\tau} = \sigma m_\tau + m_\sigma = \sigma y_p(\tau) + y_p(\sigma)$. Thus $y_p \in Z^1(G, M)$. This suggest that we can define the map $\delta : P^G \to H^1(G, M)$ as $\delta(p) = [y_p]$, where y_p is the crossed homomorphism as constructed above. For this map to be well-defined, we need to show independency of the choice of n_p.

Lemma 3.3.5. *Let $p \in P^G$, and $n_p \in N$ such that $\psi(n_p) = p$. Moreover, let $x_p : G \to N$ be given by mapping σ to $\sigma n_p - n_p$ as constructed above. Then the class of the crossed homomorphism $y_p := \varphi^{-1} \circ x_p : G \to M$ in $H^1(G, M)$, as constructed above, is independent of the choice of n_p.*

Proof. Suppose that $n'_p \in N$ is such that $\psi(n'_p) = p = \psi(n_p)$. By the exact sequence (3.2) we have $N/\varphi(M) \cong P$ induced by ψ, and thus $n'_p = n_p + \varphi(m)$ for some $m \in M$. Then we have another induced crossed homomorphism $y'_p : G \to M, \sigma \mapsto m'_\sigma$ with m'_σ the unique element in M such that

$$\varphi(m'_\sigma) = \sigma n'_p - n'_p = \sigma(n_p + \varphi(m)) - n_p - \varphi(m) = \varphi(m_\sigma) + \sigma\varphi(m) - \varphi(m).$$

By injectivity of φ, we now have $m'_\sigma - m_\sigma = \sigma m - m$. Thus $(y'_p - y_p)(\sigma) = m'_\sigma - m_\sigma = \sigma m - m$, proving that $[y_p] = [y'_p]$. ■

This independency also makes sure that δ defines a group homomorphism between P^G and $H^1(G,M)$. The map δ is also called the boundary map, and induces a long exact sequence between the cohomology groups.

Proposition 3.3.6. *Given an exact sequence of G-modules*

$$0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} P \to 0,$$

there is an exact sequence

$$0 \longrightarrow M^G \xrightarrow{\varphi^G} N^G \xrightarrow{\psi^G} P^G \xrightarrow{\delta} H^1(G,M) \xrightarrow{H^1(G,\varphi)} H^1(G,N) \xrightarrow{H^1(G,\psi)} H^1(G,P).$$

Proof. The exactness at M^G and N^G follow almost directly from the given exact sequence of G-modules.

We will start with proving the exactness at P^G. In other words, we would like to show that $\mathrm{im}(\psi^G) = \ker(\delta)$. Let $p \in \mathrm{im}(\psi^G)$, then $\psi^G(n_p) = p$ for some $n_p \in N^G$. Then $\delta(p) = [y_p]$, where $y_p : G \to M$ maps σ to the unique $m_\sigma \in M$ satisfying $\varphi(m_\sigma) = \sigma n_p - n_p = 0$, since $n_p \in N^G$. Therefore, by injectivity of φ we have $m_\sigma = 0$. Consequently, $\delta(p) = [y_p] = [0]$ which implies that $p \in \ker(\delta)$.

Conversely, let $p \in \ker(\delta)$. This means that $\delta(p) = [y_p] = 0$, or equivalently y_p is a principal crossed homomorphism. By surjectivity of ψ, there exists $n_p \in N$ such that $\psi(n_p) = p$. As a consequence of Lemma 3.3.5, the representative y_p can be chosen such that $\varphi(y_p(\sigma)) = \sigma n_p - n_p$ for all $\sigma \in G$. Moreover, $y_p(\sigma) = \sigma m - m$ for some $m \in M$. These equalities leads to the following equation,

$$\sigma n_p - n_p = \varphi(y_p(\sigma)) = \sigma\varphi(m) - \varphi(m).$$

Rewriting this equation gives $\sigma(n_p - \varphi(m)) = n_p - \varphi(m)$. Hence, we have $n_p - \varphi(m) \in N^G$, and $\psi(n_p - \varphi(m)) = \psi(n_p) = p$. Thus $p \in \mathrm{im}(\psi^G)$, which finishes the proof of the exactness at P^G

We will now show exactness at $H^1(G,M)$. Let $[x] \in \mathrm{im}(\delta)$, then $\delta(p) = [x]$ for some $p \in P^G$. By construction of δ we have $\delta(p) = y_p$, with $y_p(\sigma) = m_\sigma$ for the unique $m_\sigma \in M$ such that $\varphi(m_\sigma) = \sigma n_p - n_p$. Here n_p is an element of the preimage of p under ψ, which exists by surjectivity of ψ. Now notice that

$$H^1(G,\varphi)([x]) = H^1(G,\varphi)(\delta(p)) = [\varphi \circ y_p] = [0],$$

which implies that $[x] \in \ker(H^1(G,\varphi))$.

Contrarily, let $[x] \in \ker(H^1(G,\varphi))$. Then $\varphi(x(\sigma)) = \sigma n - n$ for some $n \in N$ for all $\sigma \in G$. Therefore, we have

$$\sigma\psi(n) = \psi(\sigma n) = \psi(\varphi(x(\sigma)) + n) = \psi(n)$$

for all $\sigma \in G$. In the last equality we used that $\mathrm{im}(\varphi) = \ker(\psi)$. The above implies that $\psi(n) \in P^G$. By definition of δ and the injectivity of φ, we now find that $\delta(\psi(n)) = [y_{\psi(n)}] = [x]$. Thus $[x] \in \mathrm{im}(\delta)$, and the sequence is exact at $H^1(G,M)$.

We are left to show that the sequence is exact at $H^1(G,N)$. Let $[y] \in \mathrm{im}(H^1(G,\varphi))$, which means that $[y] = [\varphi \circ x]$ for some $[x] \in H^1(G,M)$. Since $\mathrm{im}(\varphi) = \ker(\psi)$, we find that $\psi(\varphi(x(\sigma))) = 0$ for all $\sigma \in G$. This immediately shows that $[y] \in \ker(H^1(G,\psi))$.

Let $[y] \in \ker(H^1(G,\psi))$, then there exists $p \in P$ such that $(\psi \circ y)(\sigma) = \sigma p - p$ for all $\sigma \in G$. By surjectivity of ψ, we can again write $p = \psi(n_p)$ for some $n_p \in N$. Implementing this in the equality $\psi(y(\sigma)) = \sigma p - p$ leads to $\psi(y(\sigma) - \sigma n_p + n_p) = 0$. Since $\ker(\psi) = \mathrm{im}(\varphi)$, we find that

$y(\sigma) - \sigma n_p + n_p = \varphi(m_\sigma)$ for some unique $m_\sigma \in M$. We now define the map $x : G \to M$ by putting $x(\sigma) = m_\sigma$. Now notice that

$$\varphi(x(\sigma\tau)) = y(\sigma\tau) - \sigma\tau n_p + n_p = \sigma y(\tau) - \sigma\tau n_p + \sigma n_p + y(\sigma) - \sigma n_p + n_p = \sigma\varphi(x(\tau)) + \varphi(x(\sigma)),$$

where we used that y is a crossed homomorphism. By injectivity of φ, we find that the equality $x(\sigma\tau) = \sigma(x(\tau)) + x(\sigma)$ holds, which implies that x is also a crossed homomorphism. By construction of x, we have $[y] = [\varphi \circ x] \in \mathrm{im}(H^1(G, \varphi))$. ■

3.4 Cohomology for Profinite Groups

In the previous section we have seen cohomology theory for groups. When considering Galois groups, a slightly different definition for cohomology is used. Galois groups are special cases of the so-called profinite groups, which are topological groups that can be written as an inverse limit over finite discrete groups. The Galois cohomology is based on the cohomology theory defined for profinite groups. The main difference with the cohomology groups from before, is that we are implementing conditions on continuity of certain maps. We will again restrict ourselves to the first two cohomology groups. For a more detailed description of the theory for all cohomology groups for profinite groups, see [SW08].

Definition 3.4.1. A *profinite group* is a group G that can be written as an inverse limit of a system of finite groups, endowed with the inverse limit topology induced by the discrete topology on the finite groups. The topology on G is also called the *profinite topology.*

The discrete topology on finite groups makes sure that the inverse system in the definition of a profinite group consists of compact Hausdorff spaces. As a consequence, the inverse limit is also a compact Hausdorff space. Moreover, multiplication and inversion are continuous on the finite groups in the inverse system. Therefore, as mentioned before in the construction of the Krull topology, the inverse limit of this system is again a topological group. These properties hands us the following characterization of open subgroups of a profinite group.

Lemma 3.4.2. *Let G be a profinite group. Then $H \leq G$ is open if and only if H is closed and has finite index in G.*

Proof. " $\implies$ " Suppose that H is an open subgroup of G. The maps $G \to G, x \mapsto \sigma x$ form homeomorphisms on G for all $\sigma \in G$, since G is a topological group. In particular, the cosets σH of the open subgroup H are open in G. In general, a group G can be covered by the left cosets of a fixed subgroup H. In this case, this leads to an open cover $G = \bigcup_{\sigma \in G} \sigma H$ of G. The compactness of G now implies that $G = \bigcup_{i=1}^{n} \sigma_i H$ for some $\sigma_i \in G$. It follows that $|G : H| < \infty$, and $G \backslash H = \bigcup_{\sigma \in G \backslash H} \sigma H$. Meaning that H is closed and has finite index in G.

" $\impliedby$ " For the converse, assume that $H \leq G$ is closed and has finite index in G. Then we can write $G = \bigcup_{i=0}^{n} \sigma_i H$ for some $\sigma_i \in G$ with $\sigma_0 = e$. Note again that the maps $f_i : G \to G, x \mapsto \sigma_i^{-1} x$ are homeomorphisms for all σ_i. Consequently, the inverse images $f_i^{-1}(H) = \sigma_i H$ are closed in G. By using this, we indeed find that $H = G \backslash \bigcup_{i=1}^{n} \sigma_i H$ is open. ■

Definition 3.4.3. Let G be a profinite group. A G-module M is called *discrete* if the G action on M is continuous for the discrete topology on M. Moreover, a *morphism of discrete G-modules* is just a morphism of G-modules.

The following lemma gives an equivalent condition for showing that a G-module M is discrete.

Lemma 3.4.4. *Let M be a G-module. Then M is discrete if and only if the stabilizer* $\mathrm{Stab}_G(m) := \{\sigma \in G \mid \sigma m = m\}$ *is open for all $m \in M$ if and only if* $\mathrm{Stab}_G(m)$ *is closed and has finite index in G for all $m \in M$.*

Proof. " $\Longrightarrow$ " Suppose that the G-action μ on M is continuous, and let $m \in M$. Then $\mu^{-1}(\{m\}) \cap G \times \{m\} = \mathrm{Stab}_G(m) \times \{m\}$ is open in $G \times M$ for all $m \in M$. Therefore, $\mathrm{Stab}_G(m)$ is an open subgroup of G.

" $\Longleftarrow$ " For the converse, assume that the stabilizers $\mathrm{Stab}_G(m)$ are open in G for all $m \in M$. Note that the G-action μ on M is continuous if and only if it is locally constant, since it maps into a discrete topological space. Now let $(\sigma_0, m_0) \in G \times M$, and consider the open $\sigma_0 \, \mathrm{Stab}_G(m_0) \times \{m_0\}$ in $G \times M$. Then $\mu(\sigma, m_0) = \sigma_0 m_0$ for all $(\sigma, m_0) \in \sigma_0 \, \mathrm{Stab}_G(m_0) \times \{m_0\}$, implying that μ is locally constant, and thus continuous.

The other "$\Leftrightarrow$" statement is a direct consequence of Lemma 3.4.2. ■

In the previous section about group cohomology, we constructed functors $H^0(G, -)$ and $H^1(G, -)$ between the category of G-modules and the category of abelian groups. In a similar way, we can construct functors $H^0_c(G, -)$ and $H^1_c(G, -)$ from the category of discrete G-modules to the category of abelian groups. For a profinite group G, the functor $H^0_c(G, -) : \mathbf{G^{dis}\text{-}mod} \to \mathbf{Ab}$ is defined just as $H^0(G, -)$ in the case of general G-modules.

For the functor $H^1_c(G, -) : \mathbf{G^{dis}\text{-}mod} \to \mathbf{Ab}$, we recall the 1-cocycles and 1-coboundaries as defined in Definitions 3.3.2 and 3.3.3. The definition of $H^1_c(G, -)$ is similar to the definition of $H^1(G, -)$, the difference lies in the fact that we are working with a profinite group G and that the modules are discrete. Therefore, we can put the restriction of being continuous on the allowable 1-cocycles and 1-coboundaries. Note that a map into a discrete space is continuous if and only if it is locally constant. Therefore the G-action on a discrete G-module M is locally constant, which implies that every 1-coboundary is locally constant, or equivalently continuous. Thus we can only put a meaningful restriction on the 1-cocycles with respect to the continuity. The functor $H^1_c(G, -)$ now maps a discrete G-module M to the abelian group $Z^1_c(G, M)/B^1(G, M)$, where $Z^1_c(G, M) := \{x \in Z^1(G, M) \mid x \text{ continuous}\}$.

Definition 3.4.5. The *zeroth* and *first cohomology groups* of the discrete G-module M are given by,

$$H^0_c(G, M) := M^G, \;\; H^1_c(G, M) := Z^1_c(G, M)/B^1(G, M).$$

Proposition 3.4.6. *Given an exact sequence of discrete G-modules*

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0,$$

there is a natural exact sequence

$$0 \longrightarrow M^G \xrightarrow{\varphi^G} N^G \xrightarrow{\psi^G} P^G \xrightarrow{\delta_c} H^1_c(G, M) \xrightarrow{H^1_c(G,\varphi)} H^1_c(G, N) \xrightarrow{H^1_c(G,\psi)} H^1_c(G, P),$$

where δ_c is the same map as the map δ in Proposition 3.3.6.

Proof. We need to show that δ indeed maps into $H^1_c(G, M)$. Recall that δ originally defined a map from P^G to $H^1(G, M)$, by sending $p \in P^G$ to the class of $y_p := \varphi^{-1} \circ x_p$ in $H^1(G, M)$. The map $x_p : G \to N$ maps σ to $\sigma n_p - n_p$ for some $n_p \in \psi^{-1}(\{p\})$, which exists by surjectivity of ψ. As mentioned before, the 1-coboundaries are continuous. Moreover, the inverse of a continuous injective function between discrete topological spaces is also continuous. As a direct consequence, we see that $y_p := \varphi^{-1} \circ x_p$ is a continuous 1-cocycle, and thus δ actually maps into $H^1_c(G, M)$.

The rest of the proof is a natural extension of the proof of Proposition 3.3.6. ■

As mentioned before, we are mostly interested in the case where the profinite group G is the Galois group of a certain Galois extension L/K. We will mainly encounter discrete $\mathrm{Gal}(L/K)$-modules M satisfying $M \subset L^n$ for some $n \in \mathbb{N}$. For simplicity, we write $G_{L/K} := \mathrm{Gal}(L/K)$. The following proposition shows that an arbitrary $G_{L/K}$-module M of this type is discrete.

Proposition 3.4.7. *Let L/K be a Galois extension, and $M \subset L^n$ for some $n \in \mathbb{N}$ be a $G_{L/K}$-module. Then every stabilizer $\mathrm{Stab}_{G_{L/K}}(m)$ with $m \in M$ is closed, and has finite index. Moreover, M is a discrete $G_{L/K}$-module.*

Proof. We will first show that for all $m = (m_1, ..., m_n) \in M \subset L^n$, the stabilizer $\mathrm{Stab}_{G_{L/K}}(m)$ has finite index in $G_{L/K}$. Observe that

$$\mathrm{Stab}_{G_{L/K}}(m) = \{\sigma \in G_{L/K} \mid \sigma m_i = m_i,\ 1 \leq i \leq n\} = \mathrm{Gal}(L/K(m_1, ..., m_n)).$$

We now take a look at the map

$$\pi : \mathrm{Gal}(L/K) \to \mathrm{Aut}(K(m_1, ..., m_n)/K),\ \sigma \mapsto \sigma_{|_{K(m_1,...,m_n)}},$$

which is a surjective group homomorphism (see [Con20, Cor.A.2]). The kernel of this map is clearly given by $\mathrm{Gal}(L/K(m_1, ..., m_n)) = \mathrm{Stab}_{G_{L/K}}(m)$. Consequently, we get an isomorphism

$$\mathrm{Gal}(L/K)/\,\mathrm{Stab}_{G_{L/K}}(m) \cong \mathrm{Aut}(K(m_1, ..., m_n)/K),$$

which shows that $\mathrm{Stab}_{G_{L/K}}(m)$ has finite index in $\mathrm{Gal}(L/K)$.

For the closedness, let $\mathcal{F} := \{F \text{ field } | K \subset F \subset L \text{ finite Galois extension}\}$. It is clear that every point of L is contained in a finite Galois extension, therefore we have

$$\bigcup_{F \in \mathcal{F}} F = L.$$

As a result, for $m = (m_1, ..., m_n) \in M$, we have $m_i \in F_i$ for some $F_i \in \mathcal{F}$. By the definition of the Krull topology we find that the map

$$\pi_{F_i} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F_i/K),\ \sigma \mapsto \sigma_{|_{F_i}}$$

is continuous. Moreover, this map is surjective. Note that $\mathrm{Gal}(F_i/K(m_i))$ is a subgroup of $\mathrm{Gal}(F_i/K)$, and therefore it is closed in the discrete topology. As a consequence, we see that the set

$$\begin{aligned}\pi_{F_i}^{-1}(\mathrm{Gal}(F_i/K(m_i))) &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma_{|_{K(m_i)}} = \mathrm{id}_{K(m_i)}\} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma m_i = m_i\} \\ &= \mathrm{Stab}_{G_{L/K}}(m_i)\end{aligned}$$

is closed by continuity of π_{F_i}. For this reason, we deduce that

$$\mathrm{Stab}_{G_{L/K}}(m) = \bigcap_{i=1}^{n} \mathrm{Stab}_{G_{L/K}}(m_i)$$

is also closed, which finishes the proof by Lemma 3.4.4. ■

Chapter 4

L-series and the BSD conjecture

In this chapter we will construct the L-series of an elliptic curve. Moreover, we introduce the Birch and Swinnerton-Dyer conjecture, which is one of the seven $1,000,000 Millennium Prize Problems listed by the Clay Mathematics Institute. Before we construct the L-series of an elliptic curve, we recall some theory about elliptic curves in Section 4.1.

In Section 4.2, we will construct the L-series and give the BSD conjecture. This conjecture gives a formula for the leading coefficient of the Taylor expansion of the L-series of a given elliptic curve defined over a number field at $s = 1$. This formula contains the corresponding regulator $R_{E/K}$, the Tate-Shafarevich group $Ш(E/K)$, and the period $P(E/K)$. These quantities will be defined in Sections 4.3-4.5.

It is convenient for the reader to have basic knowledge about elliptic curves. To acquire a sufficient amount of consciousness about elliptic curves, the book of Silverman [Sil09] is recommended. This will also be the main source of the theory discussed in this chapter, unless stated otherwise.

4.1 Reduction of Elliptic Curves

Assume that K is a perfect field. As proven in [Sil09, Prop.III.3.1], every elliptic curve defined over K can be given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$. Here we have to remember that there is an extra point at infinity $O = [0, 1, 0]$. The Weierstrass equation comes together with a number of algebraic quantities listed below.

$$\begin{aligned} &b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6, \\ &b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ &c_4 = b_2^2 - 24b_4, \\ &\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ &\omega = \frac{\mathrm{d}x}{2y + a_1x + a_3} = \frac{\mathrm{d}y}{3x^2 + 2a_2x + a_4 - a_1y}. \end{aligned} \tag{4.1}$$

Definition 4.1.1. The quantity Δ, as given above, is called the *discriminant* of the Weierstrass equation.

Definition 4.1.2. The quantity ω is the *invariant differential* of an elliptic curve associated to the Weierstrass equation.

Define $f(x,y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ with $a_i \in \overline{K}$, and let $P = (x_0, y_0)$ be a zero of this polynomial in the algebraic closure $\overline{K}$ of K. Then P is a singular point on the curve $f(x,y) = 0$ if and only if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Notice that the corresponding Taylor expansion at the singular point $P = (x_0, y_0)$ can be rewritten in the form

$$f(x,y) = f(x_0,y_0) + ((y-y_0) - \alpha(x-x_0))((y-y_0) - \beta(x-x_0)) - (x-x_0)^3,$$

for some $\alpha, \beta \in \overline{K}$. The singular point P is called a *node* if $\alpha \neq \beta$. Otherwise, it is called a *cusp*.

The following proposition gives a way to check whether a curve given by a Weierstrass equation has singular points or not.

Proposition 4.1.3. (cf. [Sil09, Prop.III.1.1.4]) *A curve given by a Weierstrass equation satisfies the following properties:*

(i) It is non-singular if and only if $\Delta \neq 0$.

(ii) It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.

(iii) It has a cusp if and only if $\Delta = 0 = c_4$.

Definition 4.1.4. An *elliptic curve* is a pair consisting of a non-singular curve E of genus one and a base point $O \in E$. The elliptic curve E is said to be *defined over* K, denoted as E/K, if E is defined over K as a curve, and $O \in E(K)$.

The discussion about the connection of elliptic curves with certain Weierstrass equations, is a consequence of the following proposition.

Proposition 4.1.5. (cf. [Sil09, Prop.III.3.1]) *Let E be an elliptic curve defined over K.*

(a) There exist functions $x, y \in K(E)$ such that the rational map

$$\varphi : E \to \mathbb{P}^2, \ \phi = [x, y, 1],$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where $a_i \in K$ and $\phi(O) = [0, 1, 0]$.

(b) Any two different Weierstrass equations for E with coefficients in K are related by a linear change of variables of the form

$$X = u^2X' + r, \ Y = u^3Y' + su^2X' + t,$$

with $u \in K^\times$ and $r, s, t \in K$.

(c) Every smooth cubic curve C given by a Weierstrass equation with coefficients in K is an elliptic curve defined over K with base point $O = [0, 1, 0]$.

Definition 4.1.6. The *torsion subgroup* of E, denoted by E_{tors}, is the set of points of finite order,

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m],$$

where

$$E[m] = \{P \in E \mid [m]P = O\}$$

is the *m-torsion.* If E is defined over K, then $E_{\text{tors}}(K)$ are the points of finite order in $E(K)$.

For now we assume K to be a number field, and M_K to be the set consisting of places on the number field K. We denote M_K^0 for the non-Archimedean places on K, also called finite places. Similarly, we write M_K^∞ for the Archimedean places, also known as infinite places. Recall that the finite places on a number field K correspond to discrete valuations, as discussed in the proof of Theorem 1.4.6.

Let $v \in M_K^0$, and K_v be the corresponding completion of K with respect to v. We assume v to be represented by a normalized discrete valuation, i.e., $v(\pi_v) = 1$ where π_v is the uniformizer of $\mathfrak{m}_v$. This comes down to saying that the value group of v equals $\mathbb{Z}$, which can be done by Lemma 1.3.6. For an elliptic curve E/K_v, we have a corresponding Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K_v$. This equation can be transformed into an equation with all coefficients in $\mathcal{O}_{K_v}$. This can be accomplished by substituting $(x, y) \mapsto (u^{-2}x, u^{-3}y)$, where u is divisible by a sufficiently large power of the uniformizer π of $\mathfrak{m}_v$. The new equation is given by replacing the coefficients a_i by $u^i a_i$. Now notice that the discriminant of the obtained Weierstrass equation becomes an element of the ring $\mathcal{O}_{K_v}$, and thus $v(\Delta) \geq 0$. Moreover, since v is discrete for finite places, we can take the minimum among all such Weierstrass equations with coefficients in $\mathcal{O}_{K_v}$.

Definition 4.1.7. Let E/K_v be an elliptic curve. Then a Weierstrass equation for E is called a *minimal Weierstrass equation* for E at v if $v(\Delta)$ is minimized over all Weierstrass equations defining E with coefficients in $\mathcal{O}_{K_v}$.

Now that we have obtained a minimal Weierstrass equation for E/K_v, we can reduce its coefficients modulo $\mathfrak{m}_v = (\pi_v)$. This can be done by using the natural reduction map from $\mathcal{O}_{K_v}$ into the residue field $k_v := \mathcal{O}_{K_v}/\mathfrak{m}_v$, by mapping $t \mapsto \tilde{t}$. Consequently, we derive a curve $\tilde{E}_v$ over k_v given by

$$\tilde{E}_v : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

The curve $\tilde{E}_v/k_v$ is called the reduction of E modulo π_v. The obtained reduced curve could be singular. Nevertheless, the set of non-singular points $\tilde{E}_{\text{ns}}$ forms an abelian group (see [Sil09, Prop.III.2.5]). The reduction can be of three different types.

Definition 4.1.8. Let E/K_v be an elliptic curve, and let $\tilde{E}_v$ be the reduction modulo $\mathfrak{m}_v$ of a minimal Weierstrass equation for E.

(a) E has *good reduction* if $\tilde{E}_v$ is non-singular.

(b) E has *multiplicative reduction* if $\tilde{E}_v$ has a node.

(c) E has *additive reduction* if $\tilde{E}_v$ has a cusp.

In the latter two cases one also says that E has bad reduction. Moreover, in case (b) the reduction is said to be split if the slopes of the tangent lines at the node are in k_v, otherwise it is said to be non-split.

Proposition 4.1.9. (cf. [Sil09, Prop.VII.5.1]) *Let E/K_v be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the corresponding discriminant, and c_4 be as defined in (4.1). Then

(a) E has good reduction if and only if $v(\Delta) = 0$. In this case $\tilde{E}_v/k_v$ is an elliptic curve.

(b) E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. In this case $\tilde{E}_{ns}$ is the multiplicative group,

$$\tilde{E}_{ns}(\overline{k_v}) \cong \overline{k_v}^{\times}.$$

(c) E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$. In this case $\tilde{E}_{ns}$ is the additive group,

$$\tilde{E}_{ns}(\overline{k_v}) \cong \overline{k_v}^{+}.$$

The definition of reduction can be generalized to elliptic curves E defined over a number field K. In that case, one has a notion of reduction with respect to a finite place $v \in M_K^0$.

Definition 4.1.10. Let E/K be an elliptic curve where K is a number field. Moreover, let $v \in M_K^0$. Then E is said to have *good* (respectively *bad*) *reduction at v* if E has good (respectively bad) reduction when considered as an elliptic curve over K_v.

For a place $v \in M_K$ and an elliptic curve E/K_v, the reduced curve $\tilde{E}_v/k_v$ might be singular. But in any case, the set of non-singular points $\tilde{E}_{\mathrm{ns}}(k_v)$ forms a group. Closely related to this group are the subgroups

$$\begin{aligned}E_0(K_v) &:= \{P \in E(K_v) : \tilde{P} \in \tilde{E}_{\mathrm{ns}}(k_v)\},\\ E_1(K_v) &:= \{P \in E(K_v) : \tilde{P} = \tilde{O}\},\end{aligned}$$

of $E(K_v)$. Namely, we have the following relation between the considered groups.

Proposition 4.1.11. (cf. [Sil09, Prop.VII.2.1]) *There is a short exact sequence of abelian groups*

$$0 \longrightarrow E_1(K_v) \longrightarrow E_0(K_v) \longrightarrow \tilde{E}_{ns}(k_v) \longrightarrow 0,$$

consisting of canonical maps.

This sequence in particular implies that the subgroup $E_1(K_v)$ has finite index in $E_0(K_v)$, since $|\tilde{E}_{\mathrm{ns}}(k_v)|$ is clearly finite. A natural question that arises is whether the subgroup $E_0(K_v)$, and therefore also $E_1(K_v)$, has finite index in $E(K_v)$. This turns out to be true, and we state it as a fact.

Proposition 4.1.12. (cf. [Sil09, Cor.VII.6.2]) *The subgroup $E_0(K_v)$ has finite index in $E(K_v)$.*

The cardinality of the quotient $E(K_v)/E_0(K_v)$ for finite places $v \in M_K^0$, will play an important role in the BSD conjecture, as we will see in Section 4.5.

Definition 4.1.13. For finite places $v \in M_K^0$, we introduce the numbers

$$c(E/K_v) := |E(K_v)/E_0(K_v)|,$$

also known as *Tamagawa numbers.*

Example 4.1.14. Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 = x^3 + 2$$

having discriminant $\Delta = -2^6 3^3$ and $c_4 = 0$. This equation is already minimal for all primes p. By Proposition 4.1.9 we see that it has good reduction for primes $p \neq 2, 3$, and additive reduction for $p = 2, 3$. This means that the Tamagawa numbers for $p \neq 2, 3$ are equal to 1. The others can be computed with Tate's algorithm. This method is used in [LMF22] to obtain

$$c(E/\mathbb{Q}_2) = c(E/\mathbb{Q}_3) = 1.$$

4.2 L-Series

In this section we define the L-series of an elliptic curve defined over a number field. This function records information about the reduction modulo every prime of the given elliptic curve. As we will see, the theory about these L-series is mainly conjectural.

Let K be a number field and E/K an elliptic curve defined over K. For a finite place $v \in M_K^0$ we consider the residue field k_v and the reduction, $\tilde{E}_v$, of E at v. As proven in Theorem 1.4.6, the residue field k_v is finite. Therefore, we can define the integer

$$a_v(E) := q_v + 1 - \#\tilde{E}_v(k_v),$$

where $q_v = \#k_v$. The numbers $a_v(E)$ will play a role as coefficients in the definition of the so called local L-factors of the L-series we want to construct for an elliptic curve.

Definition 4.2.1. The *local L-factor* of the L-series of an elliptic curve E/K at a finite place $v \in M_K^0$ is given by

$$L_v(E/K, T) = \begin{cases} 1 - a_v(E)T + q_v T^2 & \text{if } E \text{ has good reduction at } v, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } v, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } v, \\ 1 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

Moreover, the L-series of an elliptic curve E/K is given by the Euler product expansion

$$L(E/K, s) = \prod_{v \in M_K^0} L_v(E/K, q_v^{-s})^{-1}. \tag{4.2}$$

As an easy consequence of Proposition 4.1.9, we make the observation that for all places $v \in M_K$, we have

$$L_v(E/K, q_v^{-1}) = \#(\tilde{E}_{\text{ns}}(k_v))/q_v.$$

Proposition 4.2.2. (cf. [SZ03, Prop.7.3]) *The L-series defined at (4.2) converges absolutely, and is analytic for all Re(s) > 3/2.*

Theorem 4.2.3. (cf. [SZ03, Thm.7.4]) *Let E/K be an elliptic curve. Then at s with $Re(s) > 3/2$, we have*

$$L(E/K, s) = \sum_{\substack{I \subset \mathcal{O}_K \\ I \neq 0}} \frac{a(I)}{N(I)^s},$$

where the sum ranges over all non-zero ideals of $\mathcal{O}_K$, and $N(I)$ is the absolute norm of I. The integer $a(I)$ is defined as

$$a(I) = a(\mathfrak{p}_1^k) \cdots a(\mathfrak{p}_r^{k_r}),$$

where $\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ is the unique prime ideal decomposition of I. For a prime $\mathfrak{p}$, put

- *$a((1)) = 1$*

- *if E has good reduction at $\mathfrak{p}$:*

$$a(\mathfrak{p}) = N(\mathfrak{p}) + 1 - \#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}),$$
$$a(\mathfrak{p}^k) = a(\mathfrak{p})a(\mathfrak{p}^{k-1}) - N(\mathfrak{p})a(\mathfrak{p}^{k-2}) \text{ for } k \geq 2.$$

- *if E has split multiplicative reduction at $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = 1 \text{ for } k \in \mathbb{N}.$$

- *if E has non-split multiplicative reduction at $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = (-1)^k \text{ for } k \in \mathbb{N}.$$

- *if E has additive reduction at $\mathfrak{p}$:*

$$a(\mathfrak{p}^k) = 0 \text{ for } k \in \mathbb{N}.$$

For elliptic curves over $\mathbb{Q}$ it is proven that the L-series has an analytic continuation to the entire complex plane. This is also conjectured to be true for arbitrary elliptic curves over a number field K.

Conjecture 4.2.4. (cf. [Sil09, Conj.C.16.1]) *The L-series $L(E/K, s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating $L(E/K, s)$ with $L(E/K, 2 - s)$.*

Under the assumption that $L(E/K, s)$ has an analytic continuation to the entire complex plane, the BSD conjecture can be formulated.

BSD conjecture 4.2.5. (cf. [Groty, Conj.2.10]) *Let E/K be an elliptic curve over a number field K, and assume that $L(E/K, s)$ has an analytic continuation to the entire complex plane.*

(i) If r_E is the rank of the finitely generated abelian group $E(K)$, then

$$ord_{s=1} L(E/K, s) = r_E.$$

(ii) Assume that the Tate-Shafarevich group $Ш(E/K)$ is finite, then

$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{r_E}} = P(E/K) \cdot \frac{\#(Ш(E/K)) \cdot R_{E/K}}{\#(E_{tors}(K))^2}.$$

Remark 4.2.6. The symbols appearing in this conjecture still have to be defined. To keep track of the definitions, we give the following table as a guidance for finding the definitions:

Symbols	Sections
$r_E, E_{\text{tors}}(K)$	4.3 (Theorem 4.3.13)
$R_{E/K}$	4.3 (Definition 4.3.14)
$Ш(E/K)$	4.4 (Definition 4.4.2)
$P(E/K)$	4.5 (Definition 4.5.3)

Example 4.2.7. Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 = x^3 + 2.$$

Then from [LMF22], we have

$$\begin{aligned} r_E &= 1 \\ \#(E_{\text{tors}}(\mathbb{Q})) &= 1 \\ R_{E/\mathbb{Q}} &= 0.754576903181227264422071178 46\ldots \\ P(E/K) &= 3.74760672070130830748706766 51\ldots \\ \#(Ш(E/K)) &= 1 \\ L'(E,1) &\approx 2.82785747364794772483423028 20. \end{aligned}$$

Here we note that [LMF22] uses the BSD conjecture to compute r_E and $\#(Ш(E/K))$. It therefore does not prove that the BSD conjecture is satisfied for this curve. However, it indicates that the conjecture can be really helpful for computing the conjectural rank or order of the Tate-Shafarevich group.

4.3 The Regulator of an Elliptic Curve

One of the invariants appearing in the BSD conjecture is the regulator of an elliptic curve. This regulator gives the square of the volume of a fundamental domain for $E(K)/E_{\text{tors}}(K)$, which is finitely generated by Mordell-Weil's theorem. This volume is computed with respect to a certain quadratic form, which depends on the height function defined on the K-rational points of the elliptic curve. So before we can construct the regulator, we need to define a height function on an elliptic curve. This can be accomplished by first defining a height function on a projective space, and then combine it with a morphism from E to $\mathbb{P}^1$.

Recall that we used M_K to denote the set of places on K. From now on, we take for $v \in M_K$ the corresponding normalized absolute values as defined in Section 1.6. The only difference we make, is that we omit the square for the complex places. This will come in handy when considering the relation of the height function on K and the height function on a finite field extension of K.

In preparation for the height function on a projective space, we give some basic results from algebraic number theory.

Theorem 4.3.1. *Let K be a number field and L a finite extension of degree n. Let $v \in M_K$ and for each $w \in M_L$ extending v, define*

$$n_w := [L_w : \mathbb{Q}_w] = [L_w : \mathbb{Q}_v],$$

also known as the local degree at w. Then

$$\sum_{\substack{w\in M_L\\ w|v}} n_w = nn_v,$$

where $w|v$ is a short notation for w extending v.

Proof. This result is an easy consequence of the fact that

$$\sum_{\substack{w\in M_L\\ w|v}} [L_w : K_v] = n,$$

which is proven in [Lan94, Cor.1, p.39]. Namely,

$$\sum_{\substack{w\in M_L\\ w|v}} n_w = \sum_{\substack{w\in M_L\\ w|v}} [L_w : K_v][K_v : \mathbb{Q}_v] = nn_v.$$

■

Theorem 4.3.2 (Product Formula)**.** (cf. [Lan94, CH.5, p.99]) *Let K be a number field and $x \in K^\times$. Then*

$$\prod_{v\in M_K} |x|_v^{n_v} = 1.$$

Definition 4.3.3. Let $P \in \mathbb{P}^N(K)$ be represented by the homogeneous coordinates $P = [x_0, ..., x_N]$, with $x_0, ..., x_N \in K$. The *height of P*, relative to K, is given by

$$H_K : \mathbb{P}^N(K) \to \mathbb{R}_{\geq 1},\ H_K(P) := \prod_{v\in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v}.$$

Proposition 4.3.4. (cf. [Sil09, Prop.VIII.5.4]) *The height function of Definition 4.3.3 is well-defined. Moreover, for a finite extension L/K it satisfies*

$$H_L(P) = H_K(P)^{[L:K]}$$

for every $P = [x_0, ..., x_N] \in \mathbb{P}^N(K)$.

Proof. For the well-definedness we have to show that $H_K(P)$ does not depend on the homogeneous coordinates, and that $H_K(P) \geq 1$. Note that any other representation of P is of the form $[\lambda x_0, ..., \lambda x_N]$ for some $\lambda \in K^\times$. Therefore, we find that

$$\begin{aligned}\prod_{v\in M_K} \max\{|\lambda x_0|_v, ..., |\lambda x_N|_v\}^{n_v} &= \prod_{v\in M_K} |\lambda|_v^{n_v} \prod_{v\in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v} \\ &= \prod_{v\in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v},\end{aligned}$$

where we used Theorem 4.3.2. This shows that $H_K(P)$ indeed does not rely on the homogeneous coordinates chosen for P.

For $H_K(P) \geq 1$, notice that the homogeneous coordinates of P can be chosen such that one of the coordinates equals 1. As a consequence, we immediately see that $H_K(P) \geq 1$.

For the last part of this proposition, let L/K be a finite extension. We deduce the desired property in the following way for every $P = [x_0, ..., x_N] \in \mathbb{P}^N(K)$,

$$H_L(P) = \prod_{w\in M_L} \max\{|x_0|_w, ..., |x_N|_w\}^{n_w} = \prod_{v\in M_K} \prod_{\substack{w\in M_L\\ w|v}} \max\{|x_0|_v, ..., |x_N|_v\}^{n_w} = H_K(P)^{[L:K]}.$$

In the last step we used Theorem 4.3.1. ■

The above proposition induces a so-called absolute height function on $\mathbb{P}^N(\overline{\mathbb{Q}})$. The idea is that this height function does not depend on a chosen number field. Namely, for $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ choose number fields K and L such that $P \in \mathbb{P}^N(K)$ and $P \in \mathbb{P}^N(L)$. Since the composite of two finite field extensions is again a finite field extension, we find by using Proposition 4.3.4 that

$$H_K(P)^{1/[K:\mathbb{Q}]} = H_{LK}(P)^{1/[LK:\mathbb{Q}]} = H_L(P)^{[LK:L]/[LK:\mathbb{Q}]} = H_L(P)^{1/[L:\mathbb{Q}]}.$$

In combination with Proposition 4.3.4, we obtain a well-defined absolute height function independent of the choice of a number field as given in the following definition.

Definition 4.3.5. The *absolute height function* is given by

$$H : \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 1},\ H(P) := H_K(P)^{1/[K:\mathbb{Q}]},$$

where K is a number field chosen in such a way that $P \in \mathbb{P}^N(K)$.

The height function defined above is also known as the multiplicative height function. Moreover, this function induces a natural additive height function. The additivity property appears to be more convenient when working with the additive group $E(\overline{K})$ of $\overline{K}$-rational points on an elliptic curve. This substantiates the following definition.

Definition 4.3.6. The *absolute logarithmic height function* is defined by

$$h : \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0},\ h(P) = \log H(P).$$

To define a height function on an elliptic curve, it is natural to first map the $\overline{K}$-rational points into $\mathbb{P}^1(\overline{K})$ such that we can use our previously defined logarithmic height function. The only problem that arises in this way, is that it will depend on the chosen map.

Definition 4.3.7. Let E/K be an elliptic, and $f \in \overline{K}(E)$ be a function. The *height on E relative to f* is the function

$$h_f : E(\overline{K}) \to \mathbb{R}_{\geq 0},\ h_f(P) = h(f(P)).$$

Despite the fact that this height function depends on the chosen function $f \in \overline{K}(E)$, it lays a foundation for a height function independent of this choice. Namely, the canonical Néron-Tate height on E/K as defined below.

Definition 4.3.8. The *canonical Néron-Tate height* on an elliptic curve E/K is the function

$$\hat{h} : E(\overline{K}) \to \mathbb{R}_{\geq 0},\ \hat{h}(P) = \frac{2}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f([2^N]P),$$

where $f \in K(E)$ is any non-constant even function.

The well-definedness and independency follow from the upcoming proposition proven by John Tate.

Proposition 4.3.9. (cf. [Sil09, Prop.VIII.9.1]) *Let E/K be an elliptic curve, and consider the limit*

$$\frac{2}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f([2^N]P)$$

for some $P \in E(\overline{K})$ and a non-constant even function $f \in K(E)$. Then this limit exists and is independent of f.

Example 4.3.10. An example of a non-constant even function in $K(E)$ is the projection

$$x : E \to \mathbb{P}^1,\ x(P) := \begin{cases} [1,0] & \text{if } P = O, \\ [x,1] & \text{otherwise,} \end{cases}$$

which has degree 2.

Due to Néron and Tate we know that $\hat{h}$ satisfies the parallelogram law and, as a consequence, that it defines a *quadratic form.* The latter means that $\hat{h}$ is an even function, and that the pairing

$$\langle \cdot, \cdot \rangle : E(\overline{K}) \times E(\overline{K}) \to \mathbb{R},\ \langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q),$$

is bilinear. We give a proof of the latter by using the parallelogram law. For an extensive list of properties of $\hat{h}$ together with a proof, one could consult [Sil09, Thm.VIII.9.3].

Theorem 4.3.11 (Néron, Tate)**.** *Let E/K be an elliptic curve, and let $\hat{h}$ be the canonical height on E. Then*

(i) $\hat{h}$ is a quadratic form on E.

(ii) Let $P \in E(\overline{K})$. Then $\hat{h}(P) \geq 0$, and we have $\hat{h}(P) = 0$ if and only if $P \in E_{tors}(\overline{K})$.

Proof. We only give a proof for the first statement. A proof of both statements can be found in [Sil09, Thm.VIII.9.3].

As mentioned, $\hat{h}$ satisfies for all $P, Q \in E(\overline{K})$ the equality

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q),$$

also known as the parallelogram law. By putting $P = O$ in the equation above, we immediately see that $\hat{h}(-Q) = \hat{h}(Q)$. In other words, $\hat{h}$ is an even function. Our goal now is to show that

$$\begin{aligned} &\langle P+R, Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle, \text{ or equivalently} \\ &\hat{h}(P+R+Q) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(R+Q) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R) = 0 \end{aligned} \tag{4.3}$$

for all $P, Q, R \in E(\overline{K})$. To prove this, we apply the parallelogram law to the tuples: $(P+R, Q)$, $(P, R-Q)$, $(P+Q, R)$ and (R, Q). This yields us the equations

$$\begin{aligned} \text{Eq}(1) &:= \hat{h}(P+R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P+R) - 2\hat{h}(Q) = 0 \\ \text{Eq}(2) &:= \hat{h}(P+R-Q) + \hat{h}(P-R+Q) - 2\hat{h}(P) - 2\hat{h}(R-Q) = 0 \\ \text{Eq}(3) &:= \hat{h}(P+R+Q) + \hat{h}(P-R+Q) - 2\hat{h}(P+Q) - 2\hat{h}(R) = 0 \\ \text{Eq}(4) &:= \hat{h}(R+Q) + \hat{h}(R-Q) - 2\hat{h}(R) - 2\hat{h}(Q) = 0. \end{aligned}$$

Combining these results hands us the desired equation (4.3) in the following way,

$$\begin{aligned} 0 &= \frac{1}{2}\left(\text{Eq}(1) - \text{Eq}(2) + \text{Eq}(3) - 2\text{Eq}(4)\right) \\ &= \hat{h}(P+R+Q) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(R+Q) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R). \end{aligned}$$

■

Definition 4.3.12. The *canonical height*, also known as the *Néron-Tate*, *pairing* on E/K is the bilinear form induced by $\hat{h}$, i.e.,

$$\langle \cdot, \cdot \rangle : E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}, \ \langle P, Q \rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

One of the main results for elliptic curves over number fields is the Mordell-Weil theorem. The proof of this theorem makes use of the height function on an elliptic curve as defined in Definition 4.3.7. The notion of a regulator for elliptic curves relies on this theorem.

Theorem 4.3.13 (Mordell-Weil Theorem)**.** (cf. [Sil09, Thm.VIII.6.7]) *Let K be a number field, and E/K be an elliptic curve. Then the group $E(K)$ is finitely generated, i.e.,*

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r,$$

for some non-negative integer r. This integer is also called the rank *of E/K, and sometimes denoted as r_E..*

As a consequence, we see that $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ defines an r-dimensional real vector space. We moreover observe that $E(K)/E_{\text{tors}}(K)$ sits as a lattice inside $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$. Namely, let $\{P_1, ..., P_r\}$ be a basis of the free abelian group $E(K)/E_{\text{tors}}(K)$. Then we get the corresponding lattice

$$(P_1 \otimes_{\mathbb{Z}} 1)\mathbb{Z} + ... + (P_r \otimes_{\mathbb{Z}} 1)\mathbb{Z}$$

inside $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$. As discussed in the beginning of this section, we need a symmetric positive definite bilinear pairing on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ to get an induced volume of this lattice. By Theorem 4.3.11 we see that $\hat{h}$ is a positive definite quadratic form on $E(K)/E_{\text{tors}}(K)$. This can be extended to a positive definite quadratic form on the real vector space $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ such that $\hat{h}(P_i \otimes_{\mathbb{Z}} 1) = \hat{h}(P_i)$ (see [Sil09, Prop.VIII.9.6]), which induces the desired bilinear pairing.

Definition 4.3.14. The *regulator* of an elliptic curve defined over a number field K, denoted by $R(E/K)$, is the square of the volume of a fundamental domain for $E(K)/E_{\text{tors}}(K)$ with respect to the canonical height $\hat{h}$. More precisely, let $P_1, ..., P_r \in E(K)$ be a basis for the free abelian group $E(K)/E_{\text{tors}}(K)$, then

$$R_{E/K} = |\det(\langle P_i, P_j \rangle)_{i,j=1}^r|.$$

If the rank $r = 0$, then we set $R_{E/K} = 1$.

4.4 The Tate-Shafarevich Group of an Elliptic Curve

If E is an elliptic curve over a number field K, then we can define two closely related groups; the Selmer group and the Tate-Shafarevich group (see [Sil09, CH.X.4]). We will restrict to the definition of the Tate-Shafarevich group. This group can be seen as the group of equivalent homogeneous spaces for E/K that possess a K_v-rational point for $v \in M_K$. Such a homogeneous space is in the trivial class if and only if the set of K_v-rational points is not empty. Thus we see that the Tate-Shafarevich group is trivial if and only if finding a K_v-rational point for $v \in M_K$ is equivalent to finding a K-rational point for every homogeneous space. This is also known as Hasse's local-global principle. The Tate-Shafarevich group therefore measures in some sense the failure of Hasse's principle[1].

For each $v \in M_K$, represented by a non-zero absolute value $|\cdot|_v$, we fix an embedding $\iota_v : \overline{K} \to \overline{K_v}$ that extends the natural embedding $\psi_v : K \hookrightarrow K_v \hookrightarrow \overline{K_v}$. For simplicity, we will call embeddings extending ψ_v *K-embeddings.* Under these conditions, we get an embedding of $\text{Gal}(\overline{K_v}/K_v)$ into $\text{Gal}(\overline{K}/K)$.

[1] The precise meaning of homogeneous spaces together with the discussed equivalences can be found in [Sil09, CH.X]

Proposition 4.4.1. *The map*

$$\varphi_{\iota_v} : \mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{K}/K),\ \sigma \mapsto \iota_v^{-1} \circ \sigma \circ \iota_v, \tag{4.4}$$

defines an embedding of topological groups.

Proof. Before any other statement can be proven, we need to show that φ_{ι_v} is well-defined. This comes with verifying two things. Namely, that $\sigma(\iota_v(x)) \in \iota_v(\overline{K})$ for every $x \in \overline{K}$ such that it makes sense to compose it with ι_v^{-1}. Moreover, we need to show that φ_{ι_v} indeed maps into $\mathrm{Gal}(\overline{K}/K)$.

For the first part, let $x \in \overline{K}$ and $f \in K[X]$ be the minimal polynomial of x over K. Note that f splits completely over $\overline{K}$, since $\overline{K}/K$ is a normal extension. In other words, we get $f = \prod_{i=1}^n (X_i - \alpha_i)$ for some $\alpha_i \in \overline{K}$ with $\alpha_i := x$ for some i. Under the embedding ι_v, we get $\iota_v(f) = \prod_{i=1}^n (X_i - \iota_v(\alpha_i))$ satisfying $\iota_v(f) \in K_v[X]$. The latter is the case since $f \in K[X]$ and $\iota_v(K) \subset K_v$. The fact that $f(x) = 0$ now implies that $\iota_v(f)(\iota_v(x)) = \iota_v(f(x)) = 0$. In addition, since $\iota_v(f) \in K_v[X]$, we have for all $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ that

$$\iota_v(f)(\sigma(\iota_v(x))) = \sigma(\iota_v(f)(\iota_v(x)) = 0.$$

This means that $\sigma(\iota_v(x)) = \iota_v(\alpha_i)$ for some $\alpha_i \in \overline{K}$. We thus conclude that $\sigma(\iota_v(x)) \in \iota_v(\overline{K})$ for all $x \in \overline{K}$ and $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$, and thus it makes sense to compose it with ι_v^{-1}.

As mentioned earlier, we are left to show that φ_{ι_v} maps into $\mathrm{Gal}(\overline{K}/K)$ before we can conclude that φ_{ι_v} is well-defined. It is clear that $\varphi_{\iota_v}(\sigma)$ defines a field homomorphism between $\overline{K}$ and $\overline{K}$ that fixes K for every $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$. Thus it remains to prove that $\varphi_{\iota_v}(\sigma)$ is surjective. This follows directly from the observation that σ maps $\iota_v(\overline{K})$ surjectively to $\iota_v(\overline{K})$. The previous statement can be seen from the fact that $\sigma(\iota_v(x)) \in \iota_v(\overline{K})$, and $\sigma^{-1}(\iota_v(x)) \in \iota_v(\overline{K})$ for all $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ and $x \in \overline{K}$.

We will now show that φ_{ι_v} is an embedding of topological groups. It is clear that this map is a group homomorphism. The properties we still have to show are that φ_{ι_v} is continuous and injective. For clarification, since φ_{ι_v} is a map between compact Hausdorff spaces, this will imply that φ_{ι_v} defines a homeomorphism onto its image.

Note that a group homomorphism is continuous if and only if it is continuous at the identity element. Thus let U be a basis neighborhood of $\mathrm{id}_{\overline{K}}$, then $U = \mathrm{Gal}(\overline{K}/F)$ for some finite Galois extension F/K inside $\overline{K}$. We want to show that $\varphi_{\iota_v}^{-1}(U)$ is open in $\mathrm{Gal}(\overline{K_v}/K_v)$. For this, let $\sigma \in \varphi_{\iota_v}^{-1}(U)$ and consider the field $F' := \iota_v(F)K_v \subset \overline{K_v}$. Since F is a finite Galois extension of K, we clearly see that $\iota_v(F)K_v$ is a finite Galois extension of K_v. In other words, $U' = \mathrm{Gal}(\overline{K_v}/F')$ also defines an open in $\mathrm{Gal}(\overline{K_v}/K_v)$. We now claim that $\sigma \in \mathrm{Gal}(\overline{K_v}/F')$ and $\varphi_{\iota_v}(\mathrm{Gal}(\overline{K_v}/F')) \subset \mathrm{Gal}(\overline{K}/F)$. First notice by assumption that

$$F \subset \overline{K}^{\langle \varphi_{\iota_v}(\sigma) \rangle} := \{x \in \overline{K} \mid \varphi_{\iota_v}(\sigma)(x) = x\},$$

and thus under the embedding ι_v we obtain the inclusion $\iota_v(F) \subset \overline{K_v}^{\langle \sigma \rangle} := \{x \in \overline{K_v} \mid \sigma(x) = x\}$. Moreover, by definition $K_v \subset \overline{K_v}^{\langle \sigma \rangle}$ where we note that $\overline{K_v}^{\langle \sigma \rangle}$ is a field. Since $\iota_v(F)K_v$ is the smallest field inside $\overline{K_v}$ containing $\iota_v(F)$ and K_v, we find that $F' = \iota_v(F)K_v \subset \overline{K_v}^{\langle \sigma \rangle}$. This shows that $\sigma \in \mathrm{Gal}(\overline{K_v}/F')$.

To show the inclusion $\varphi_{\iota_v}(\mathrm{Gal}(\overline{K_v}/F')) \subset U = \mathrm{Gal}(\overline{K}/F)$, let $x \in F$ and note that for $\tau \in \mathrm{Gal}(\overline{K_v}/F')$ we have the property

$$\varphi_{\iota_v}(\tau)(x) = \iota_v^{-1}(\tau(\iota_v(x))) = \iota_v^{-1}(\iota_v(x)) = x,$$

which proves the desired inclusion. The above shows that $\varphi_{\iota_v}^{-1}(U) = \mathrm{Gal}(\overline{K_v}/F')$, and thus φ_{ι_v} is indeed continuous.

For the injectivity, we want to show that $\ker(\varphi_{\iota_v}) = \{\mathrm{id}_{\overline{K}}\}$. Note that $\sigma \in \ker(\varphi_{\iota_v})$ if and only if $\sigma \circ \iota_v = \iota_v$, or equivalently $\sigma|_{\iota_v(\overline{K})} = \mathrm{id}_{\iota_v(\overline{K})}$. By a similar argument as in the proof of Lemma 3.2.9, we find that $\sigma \in \ker(\varphi_{\iota_v})$ if and only if $\sigma \in \mathrm{Gal}(\overline{K_v}/\iota_v(\overline{K})K_v)$. But by a corollary of Krasner's lemma ([SW08, Prop.8.1.5]), we have $\overline{K_v} = \iota_v(\overline{K})K_v$. This tells us that $\mathrm{Gal}(\overline{K_v}/\iota_v(\overline{K})K_v) = \ker(\varphi_{\iota_v})$ is trivial, as desired. ■

By Proposition 3.4.7 we clearly see that $E(\overline{K})$ is a discrete $\mathrm{Gal}(\overline{K}/K)$-module, and similarly when K is replaced by K_v. The map φ_{ι_v} as defined in (4.4) now induces a group homomorphism on cohomology groups,

$$\tilde{\beta}_v : H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \to H^1(\mathrm{Gal}(\overline{K_v}/K_v), E(\overline{K_v})),\ [f] \mapsto [\iota_v \circ f \circ \varphi_{\iota_v}].$$

The well-definedness of this map is easily verified. Based on these maps, we can define the Tate-Shafarevich group of an elliptic curve E/K for some number field K.

Definition 4.4.2. The *Tate-Shafarevich group* of an elliptic curve E/K is given by

$$Ш(E/K) := \bigcap_{v \in M_K} \ker\left(H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})) \xrightarrow{\tilde{\beta}_v} H^1(\mathrm{Gal}(\overline{K_v}/K_v), E(\overline{K_v}))\right).$$

Before we can prove that this group is well-defined, i.e., independent of the chosen K-embedding ι_v, we need a characterization of those K-embeddings. We start with a result for finite Galois extensions of a number field.

Proposition 4.4.3. *Let L/K be a finite Galois extension. Moreover, pick an K-embedding $\iota_v : L \to \overline{K_v}$. Then any other K-embedding of L into $\overline{K_v}$ is given by precomposition with an element of* $\mathrm{Gal}(L/K)$.

Proof. Let $\widetilde{\iota_v} : L \to \overline{K_v}$ be another K-embedding. First notice that L/K is a simple extension by the Theorem of the Primitive Element [Cox12, Thm.5.4.1], which means that there exists a $\theta \in L$ such that $L = K(\theta)$. This moreover means that the embeddings ι_v and $\widetilde{\iota_v}$ are completely determined by their images on θ. Let f_θ be the minimal polynomial of θ over K, then $f_\theta = X^n + \sum_{i=0}^{n-1} a_i X^i$ for some $a_i \in K$. Moreover, we observe that $\iota_v(\theta)$ and $\widetilde{\iota_v}(\theta)$ are roots of

$$\iota_v(f_\theta) = X^n + \sum_{i=0}^{n-1} \iota_v(a_i)X^i = X^n + \sum_{i=0}^{n-1} \psi_v(a_i)X^i = X^n + \sum_{i=0}^{n-1} \widetilde{\iota_v}(a_i)X^i = \widetilde{\iota_v}(f_\theta).$$

Note that f_θ has n distinct roots. By injectivity of the embeddings, we find that all those roots are bijectively mapped onto the roots of $\iota_v(f_\theta) = \widetilde{\iota_v}(f_\theta)$. This means that for $\widetilde{\iota_v}(\theta)$, there exists a root θ_0 of f_θ such that $\widetilde{\iota_v}(\theta) = \iota_v(\theta_0)$. Since L/K is a finite Galois extension, the group $\mathrm{Gal}(L/K)$ acts transitively on the roots of f_θ. Thus there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\theta) = \theta_0$. In other words, $\widetilde{\iota_v}(\theta) = \iota_v(\sigma(\theta))$. But, as mentioned before, $\widetilde{\iota_v}$ is completely determined by how it acts on θ. Therefore, this shows that $\widetilde{\iota_v} = \iota_v \circ \sigma$ for some $\sigma \in \mathrm{Gal}(L/K)$. ■

Corollary 4.4.4. *Let $\iota_v : \overline{K} \to \overline{K_v}$ and $\widetilde{\iota_v} : \overline{K} \to \overline{K_v}$ be two K-embeddings, then $\widetilde{\iota_v} = \iota_v \circ \sigma$ for some $\sigma \in \mathrm{Gal}(\overline{K}/K)$.*

Proof. For the sake of simplified notation, we write $\mathcal{F}$ for the collection of intermediate fields $K \subset F \subset \overline{K}$ such that F/K is a finite Galois extension. We first notice that $\overline{K} = \bigcup_{K \subset F \subset \overline{K}} F$. Moreover, by Proposition 4.4.3 we discover that for each $F \in \mathcal{F}$ there exists a $\sigma_F \in \mathrm{Gal}(F/K)$

such that $\widetilde{\iota_v}_{|_F} = \iota_{v|_F} \circ \sigma_F$. We observe that for $F_1, F_2 \in \mathcal{F}$ satisfying $F_1 \subset F_2$, we have $\sigma_{F_1} \in \mathrm{Gal}(F_1/K)$ and $\sigma_{F_2} \in \mathrm{Gal}(F_2/K)$ such that

$$\begin{aligned} \widetilde{\iota_v}_{|_{F_1}} &= \iota_{v|_{F_1}} \circ \sigma_{F_1} \\ \widetilde{\iota_v}_{|_{F_2}} &= \iota_{v|_{F_2}} \circ \sigma_{F_2}. \end{aligned}$$

By injectivity of the K-embeddings, we now find that $\sigma_{F_2|_{F_1}} = \sigma_{F_1}$. In other words, we constructed a $(\sigma_F)_{F\in\mathcal{F}} \in \varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K)$. And thus by the isomorphism

$$\Phi : \mathrm{Gal}(\overline{K}/K) \to \varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/K), \ \sigma \mapsto (\sigma_{|_F})_{F\in\mathcal{F}}$$

from Theorem 3.2.10, we find that there exists a $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that $\sigma_{|_F} = \sigma_F$ for all $F \in \mathcal{F}$. As a result, we conclude that $\widetilde{\iota_v} = \iota_v \circ \sigma$ for some $\sigma \in \mathrm{Gal}(\overline{K}/K)$. ■

Proposition 4.4.5. *The Tate-Shafarevich group* Ш(E/K) *of an elliptic curve E/K is well-defined.*

Proof. To make sure that Ш(E/K) is well-defined we have to show that it is independent of the chosen K-embedding. Recall that Ш(E/K) is defined as the kernel of the map $\tilde{\beta}_v$. The definition of this map seems to dependent on the chosen K-embedding. Nevertheless, we will see that this is not the case. So let $\iota_v, \widetilde{\iota_v} : \overline{K} \to \overline{K_v}$ be two K-embeddings. By Corollary 4.4.4 we know that $\widetilde{\iota_v} = \iota_v \circ \sigma_0$ for some $\sigma_0 \in \mathrm{Gal}(\overline{K}/K)$. Using this property yields the equality

$$\begin{aligned} \widetilde{\iota_v}(f(\varphi_{\widetilde{\iota_v}}(\sigma))) &= \widetilde{\iota_v}(f(\widetilde{\iota_v}^{-1} \circ \sigma \circ \widetilde{\iota_v})) \\ &= \widetilde{\iota_v}(f(\sigma_0^{-1} \circ \iota_v^{-1} \circ \sigma \circ \iota_v \circ \sigma_0)) \\ &= \widetilde{\iota_v}\left(\sigma_0^{-1}\left(f(\iota_v^{-1} \circ \sigma \circ \iota_v \circ \sigma_0)\right) + f(\sigma_0^{-1})\right) \\ &= \widetilde{\iota_v}\left(\sigma_0^{-1}\left(\iota_v^{-1}(\sigma(\iota_v(f(\sigma_0)))) + f(\iota_v^{-1} \circ \sigma \circ \iota_v)\right) + f(\sigma_0^{-1})\right) \\ &= \sigma(\iota_v(f(\sigma_0))) + \iota_v(f(\iota_v^{-1} \circ \sigma \circ \iota_v)) + \iota_v(\sigma_0(f(\sigma_0^{-1}))) \\ &= \sigma(\iota_v(f(\sigma_0))) + \iota_v(f(\varphi_{\iota_v}(\sigma))) - \iota_v(f(\sigma_0)) \\ &= \iota_v(f(\varphi_{\iota_v}(\sigma))) + \sigma(\iota_v(f(\sigma_0))) - \iota_v(f(\sigma_0)) \qquad (4.5) \end{aligned}$$

for $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ and $[f] \in H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$. Here we used that for an arbitrary 1-cocycle $f : \mathrm{Gal}(\overline{K}/K) \to E(\overline{K})$ we have

$$1 = f(\mathrm{id}_{\overline{K}}) = f(\sigma_0\sigma_0^{-1}) = \sigma_0(f(\sigma_0^{-1})) + f(\sigma_0),$$

implying that $f(\sigma_0) = -\sigma_0(f(\sigma_0^{-1}))$. The equality found at (4.5) indicates that $[\widetilde{\iota_v} \circ f \circ \varphi_{\widetilde{\iota_v}}] = [\iota_v \circ f \circ \varphi_{\iota_v}]$, and thus the map $\tilde{\beta}_v$ is independent of the chosen K-embedding. This in particular means that Ш(E/K) is also independent of the chosen K-embedding. ■

Conjecture 4.4.6. *Let E/K be an elliptic curve, where K is a number field. Then* Ш(E/K) *is finite.*

The finiteness has been proven for elliptic curves $E/\mathbb{Q}$ of analytic rank 0 and 1, i.e., $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 0$ or 1. More on this can be found in [Ber10]. For elliptic curves over $\mathbb{Q}$ of bigger ranks, it is also still an open problem.

Theorem 4.4.7. (cf. [Sil09, Thm.X.4.14]) *Let E/K be an elliptic curve and assume that* Ш(E/K) *is finite. Then the order of* Ш(E/K) *is a perfect square.*

As the conjecture about finiteness of Ш(E/K) already suggests, not much is known about the structure of Ш(E/K). Besides the hard to compute order of the group, giving an explicit element of Ш(E/K) is already a difficult task. However, the BSD conjecture provides a conjectural value for the order of Ш(E/K).

4.5 The Period of an Elliptic Curve

As we will see in this section, the final part of the BSD conjecture can be written down as a volume calculation. The computed volume will be called the period of the given elliptic curve. This theory is based on the lectures notes of Benedict H. Gross on the conjecture of Birch and Swinnerton-Dyer [Groty, Lecture 2]. An elliptic curve over a field K is a curve of genus one, and therefore has a unique (up to scalar) everywhere holomorphic non-vanishing invariant differential. So for each place $v \in M_K$, we can pick a non-zero invariant differential ω_v for E/K_v. If we moreover choose a Haar measure $\mathrm{d}x_v$ on K_v, we obtain a Haar measure $|\omega_v|_v$ on the compact group $E(K_v)$ as described in [Wei82, CH.2.2]. Note here that the absolute values $|\cdot|_v$ are taken as the normalized ones from Section 1.6. The following lemma gives the volume of $E(K_v)$ with respect to the constructed Haar measure for finite places v.

Lemma 4.5.1. (cf. [Groty, Lem.2.8]) *Let $v \in M_K^0$, and E/K_v an elliptic curve. Pick a minimal Weierstrass equation for E, and let ω_v be the associated invariant differential. Moreover, let $\mathrm{d}x_v$ be the Haar measure on K_v giving $\mathcal{O}_{K_v}$ volume* 1*. Then we have*

$$\int_{E(K_v)} |\omega_v|_v = [E(K_v) : E_0(K_v)] \frac{|\tilde{E}_{ns}(k_v)|}{q_v} = c(E/K_v) \frac{|\tilde{E}_{ns}(k_v)|}{q_v},$$

where q_v is the cardinality of the residue field k_v.

Proof. We choose a minimal Weierstrass equation for E, i.e., E can be given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in \mathcal{O}_{K_v}$ such that $v(\Delta)$ is minimal. The associated differential is given by

$$\omega_v = \frac{\mathrm{d}x}{2y + a_1x + a_3}.$$

For the rest of the proof we use the theory about formal groups of an elliptic curve. A nice description of this can be found in [Sil09, CH.4]. Let $z = -x/y$, and observe that z is a local uniformizer at O_E, i.e., the function z has a zero of order one at O_E. Inside the formal completion at O_E, which is a power series ring in one variable $K[[z]]$, we obtain

$$\omega_v(z) = \frac{\mathrm{d}x(z)}{2y(z) + a_1x(z) + a_3} = (1 + O(z))\mathrm{d}z.$$

We write $\hat{E}/\mathcal{O}_{K_v}$ for the formal group associated to E. Then by [Sil09, Prop.VII.2.2] we have an isomorphism of groups

$$E_1(K_v) \xrightarrow{\sim} \hat{E}(\pi_v\mathcal{O}_{K_v}),$$

where $\hat{E}(\pi_v\mathcal{O}_{K_v})$ is the group $\pi_v\mathcal{O}_{K_v}$ endowed with the formal addition law. By viewing $E(K_v)$ as a K_v-analytic manifold[2], the isomorphism forms a chart. As a consequence, we get

$$\int_{E_1(K_v)} |\omega_v|_v = \int_{\pi_v\mathcal{O}_{K_v}} |(1 + O(z))\mathrm{d}z|_v = \int_{\pi_v\mathcal{O}_{K_v}} |\mathrm{d}z|_v,$$

where $|\mathrm{d}z|_v$ is the normalized Haar measure on K_v giving $\mathcal{O}_{K_v}$ volume 1. In the above we used that $|1 + O(z)|_v = 1$ for $z \in \pi_v\mathcal{O}_{K_v}$, by the non-Archimedean property. We namely have that

[2] An explanation for $E(K_v)$ being compact and a K_v-analytic manifold can be found in [Clab] and [RR94].

$O(z)$ is a power series of the form $\sum_{n=1}^{\infty} c_n z^n$ for some $c_n \in \mathcal{O}_{K_v}$. This power series clearly converges for $z \in \pi_v \mathcal{O}_{K_v}$, since

$$\sum_{n=1}^{\infty} |c_n z^n|_v \leq \sum_{n=1}^{\infty} |z^n|_v,$$

where the latter one trivially converges for $|z|_v < 1$ as a consequence of the ratio test. We thus observe that

$$|O(z)|_v = \left| \sum_{n=1}^{\infty} c_n z^n \right|_v = \lim_{N\to\infty} \left| \sum_{n=1}^{N} c_n z^n \right|_v \leq \lim_{N\to\infty} \max_{1\leq n\leq N} \{|c_n z^n|_v\} < 1.$$

We now observe that we have a finite partition

$$\bigcup_{i=1}^{q_v} (x_i + \pi_v \mathcal{O}_{K_v})$$

of $\mathcal{O}_{K_v}$ for some $x_i \in \mathcal{O}_{K_v}$, since $q_v = [\mathcal{O}_{K_v} : \pi_v \mathcal{O}_{K_v}]$ is finite. We therefore see by the fact that the differential is translation invariant, that

$$1 = \int_{\mathcal{O}_{K_v}} |\mathrm{d}z|_v = \int_{\bigcup_{i=1}^{q_v}(x_i+\pi_v\mathcal{O}_{K_v})} |\mathrm{d}z|_v = \sum_{i=1}^{q_v} \int_{(x_i+\pi_v\mathcal{O}_{K_v})} |\mathrm{d}z|_v = \sum_{i=1}^{q_v} \int_{\pi_v\mathcal{O}_{K_v}} |\mathrm{d}z|_v = q_v \int_{\pi_v\mathcal{O}_{K_v}} |\mathrm{d}z|_v.$$

And thus, by combining the above, we have

$$\int_{E_1(K_v)} |\omega_v|_v = \int_{\pi_v\mathcal{O}_{K_v}} |\mathrm{d}z|_v = \frac{1}{q_v}.$$

To obtain the volume of $E(K_v)$ with respect to $|\omega_v|_v$, we will use the fact that $E_1(K_v)$ is a finite subgroup of $E(K_v)$. For this, we consider the exact sequence

$$0 \to E_1(K_v) \to E_0(K_v) \to \tilde{E}_{\mathrm{ns}}(k_v) \to 0,$$

as stated in Proposition 4.1.11. This implies that $[E_0(K_v) : E_1(K_v)] = |\tilde{E}_{\mathrm{ns}}(k_v)|$, which is clearly finite. Moreover, by Proposition 4.1.12, the group $E_0(K_v)$ has finite index in $E(K_v)$. In other words, combining these observations, we see that $E_1(K_v)$ is a subgroup of $E(K_v)$ of finite index, meaning that we again have a partition

$$\bigcup_{i=1}^{m} (P_i + E_1(K_v))$$

of $E(K_v)$, for some $P_i \in E(K_v)$ and where $m = [E(K_v) : E_1(K_v)]$. We therefore obtain the desired result as follows,

$$\int_{E(K_v)} |\omega_v|_v = \sum_{i=1}^{m} \int_{E_1(K_v)} |\omega_v|_v = [E(K_v) : E_1(K_v)] \frac{1}{q_v} = c(E/K_v) \frac{|\tilde{E}_{\mathrm{ns}}(k_v)|}{q_v}.$$

■

Remark 4.5.2. The invariant differential associated to a minimal Weierstrass equation is unique up to multiplication by an element of $\mathcal{O}_{K_v}^{\times}$[3]. In other words, the above is independent of the chosen minimal Weierstrass equation. To make this more precise, consider two minimal Weierstrass equations for an elliptic curve E/K_v with associated differentials ω_v and ω_v', then we have $\omega_v = u\omega_v'$ for some $u \in \mathcal{O}_{K_v}^{\times}$. This in particular means that

$$\int_{E(K_v)} |\omega_v|_v = \int_{E(K_v)} |u\omega_v'|_v = \int_{E(K_v)} |\omega_v'|_v.$$

[3] For this, see [Sil09, Prop.VII.1.3]

We are now able to construct the period of an elliptic curve E defined over a number field K in terms of local volumes.

Let ω be a non-zero differential on E/K. Under the canonical embeddings $\iota_v : K \to K_v$, we obtain an invariant differential ω_v on E/K_v for all places $v \in M_K$. Moreover, choose a decomposition

$$\mathrm{d}x = \prod_v \mathrm{d}x_v$$

of the Haar measure $\mathrm{d}x$ on the adeles $\mathbb{A}_K$ with $\int_{\mathbb{A}_K/K} \mathrm{d}x = 1$.

Definition 4.5.3. The *period* of E/K is given by

$$P(E/K) = P(\omega) = \prod_{v \in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v \in M_K^0} (L_v(E/K, q_v^{-1})^{-1} \cdot \int_{E(K_v)} |\omega_v|_v).$$

Multiple choices have been made, so we need some arguments to justify the period being well-defined.

Lemma 4.5.4. *The period $P(E/K)$ of an elliptic curve E/K is well-defined.*

Proof. First of all, consider any Weierstrass equation for E/K,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with discriminant Δ. Then we clearly see that for all but finitely many $v \in M_K^0$, we have

$$v(a_i) \geq 0 \text{ for } i = 1, ..., 6 \text{ and } v(\Delta) = 0.$$

In other words, the equation is already minimal for those v, and the reduced curve $\tilde{E}_v/k_v$ again defines an elliptic curve. This means that E has good reduction at v for almost all $v \in M_K^0$. Therefore, by Lemma 4.5.1 and the fact that

$$L_v(E/K, q_v^{-1}) = \frac{|\tilde{E}_{\mathrm{ns}}(k_v)|}{q_v},$$

we have for almost all $v \in M_K^0$ that the terms in the product defining $P(E/K)$ are equal to 1.

We are left to show that the period does not depend on the chosen differential. Recall that the holomorphic differentials form a one-dimensional K-vector space. This means that any other non-zero differential on E/K is of the form $\lambda\omega$ for some $\lambda \in K^\times$. And we thus see that $P(E/K)$ remains unchanged by the product formula Theorem 1.6.9. ■

The following statement gives a more explicit description of the period of an elliptic curve E/K.

Corollary 4.5.5. *Let ω be a non-zero differential on E/K. For $v \in M_K^0$, pick a minimal Weierstrass equation for E/K_v, and let ω_v^0 be the associated invariant differential. Moreover, let $\mathrm{d}x_v$ be the Haar measures as in Definition 2.4.3. Then,*

$$P(E/K) = \frac{\prod_{v \in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v \in M_K^0} \left|\frac{\omega_v}{\omega_v^0}\right|_v \cdot c(E/K_v)}{\sqrt{|\Delta_K|}}.$$

Proof. First, recall by Proposition 2.4.5 that these measures induce a measure on $\mathbb{A}_K$ such that $\operatorname{vol}(\mathbb{A}_K/K) = |\Delta_K|^{1/2}$. So, to satisfy the condition that $\int_{\mathbb{A}_K/K} \mathrm{d}x = 1$, we see that

$$P(E/K) = \frac{\prod_{v\in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v\in M_K^0} (L_v(E/K, q_v^{-1})^{-1} \cdot \int_{E(K_v)} |\omega_v|_v)}{\sqrt{|\Delta_K|}}.$$

Now observe that Lemma 4.5.1 can be applied to the differential ω_v^0. By noticing that $\omega_v = u_v\omega_v^0$ for some $u_v \in K_v^\times$, we find that

$$\begin{aligned}
P(E/K) &= \frac{\prod_{v\in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v\in M_K^0} (L_v(E/K, q_v^{-1})^{-1} \cdot \int_{E(K_v)} |\omega_v|_v)}{\sqrt{|\Delta_K|}} \\
&= \frac{\prod_{v\in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v\in M_K^0} (L_v(E/K, q_v^{-1})^{-1} \cdot \left|\frac{\omega_v}{\omega_v^0}\right|_v \cdot \int_{E(K_v)} |\omega_v^0|_v)}{\sqrt{|\Delta_K|}} \\
&= \frac{\prod_{v\in M_K^\infty} \int_{E(K_v)} |\omega_v|_v \cdot \prod_{v\in M_K^0} \left|\frac{\omega_v}{\omega_v^0}\right| c(E/K_v)}{\sqrt{|\Delta_K|}}.
\end{aligned}$$

■

Remark 4.5.6. As proven in [AS21, Lem.2.1], we have $E(\mathbb{A}_K) = \prod_{v\in M_K} E(K_v)$. We are therefore able to make the observation that the period of E is actually a volume calculation with respect to the Tamagawa measure τ relative to the convergence factors $\lambda_v = L_v(E/K, q_v^{-1})$ for $v \in M_K^0$. More precisely, $P(E/K) = \tau(E(\mathbb{A}_K)) = \operatorname{vol}(E(\mathbb{A}_K))$.

Chapter 5

Classical Analytic Class Number Formula

The goal of this chapter is to discuss as many similarities as possible between the leading term of the Taylor expansion of the L-series $L(E/K, s)$ formulated in the BSD conjecture, and the well-known residue formula of the Dedekind zeta function $\zeta_K(s)$ at $s = 1$. The latter one is a proven expression, and formulated in the following theorem:

Theorem 5.0.1 (Analytic Class Number Formula)**.** (cf. [Neu99, Cor.VII.5.11]) *Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and $2r_2$ the number of complex embeddings. The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to the complex plane that is holomorphic except for a simple pole at $s = 1$ with residue*

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot R_K}{\sqrt{|\Delta_K|} \cdot \#(\mathcal{O}_K^\times)_{tors}}.$$

The symbols in this formula represent the class number h_K, the discriminant Δ_K of the number field, and the regulator R_K. The regulator still has to be defined, which will be done in Section 5.2.

As we have seen in the BSD conjecture, one of the central objects is the group of K-rational points, $E(K)$, on the elliptic curve E/K for some number field K. This group is a finitely generated abelian group, as a consequence of Mordell-Weil's theorem 4.3.13. In the world of number fields, there is an analogue of this theorem. Namely, Dirichlet's unit theorem which is stated below:

Theorem 5.0.2. (cf. [Neu99, Thm.I.7.4]) *Let K be a number field, and $\mathcal{O}_K$ be the corresponding ring of integers. Moreover, let r_1 and r_2 be as in Theorem 5.0.1. Then the group of units is a finitely generated abelian group of the form*

$$\mathcal{O}_K^\times \cong (\mathcal{O}_K^\times)_{tors} \times \Gamma,$$

where $(\mathcal{O}_K^\times)_{tors}$ is finite and Γ a free abelian group of rank $r_1 + r_2 - 1$.

This already hands us the first similarity between the two main formulae of this thesis. Namely, they both contain the cardinality of a finite torsion group, more precisely of $E_{\text{tors}}(K)$ and $(\mathcal{O}_K^\times)_{\text{tors}}$. Another conjectural similarity is between the regulators R_K and $R_{E/K}$, which both are related to a volume computation of a certain fundamental domain. Considering the quantities left, one natural question that arises is whether there is a correspondence between the Tate-Shafarevich group of an elliptic curve $Ш(E/K)$, and the class group $\text{Cl}(\mathcal{O}_K)$ of a number field. It appears that there is a cohomological analogue of the Tate-Shafarevich group for number fields, which we denote by $Ш(K)$. Under this definition, we get an isomorphism with the class group of the considered number field. The proof of this will be given later in this chapter, following the methods used in [Kai16].

This chapter starts with an introduction to the Dedekind zeta function and the corresponding analytic class number formula in Section 5.1. The remainder of this chapter is dedicated to indicate the termwise similarities with the BSD conjecture. The structure of this chapter is represented in the following table:

Sections	BSD		ACNF	Sections
4.3	$R_{E/K}$	$\longleftrightarrow$	R_K	5.2
4.4	$Ш(E/K)$	$\longleftrightarrow$	$\mathrm{Cl}(\mathcal{O}_K) \cong Ш(K)$	5.3
4.5	$P(E/K) = \mathrm{vol}(E(\mathbb{A}_K))$	$\longleftrightarrow$	$P(K) = \mathrm{vol}(\mathcal{O}^{\times}_{\mathbb{A}_K}) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{\lvert\Delta_K\rvert}}$	5.4

5.1 The Dedekind Zeta Function

In this section we desire to introduce the so-called Dedekind zeta function of a number field K. This introduction can be viewed as a summary of [Neu99, CH.VII.1 and 3]. This function is a complex analytic function, which encodes a lot of fundamental arithmetic properties of a number field. Before we make this more precise, we restrict to the case that $K = \mathbb{Q}$. Under these circumstances, the corresponding zeta function is the well-known Riemann-zeta function. This function is defined for a complex variable s with $\mathrm{Re}(s) > 1$ by

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It is moreover absolutely and uniformly convergent on the complex right half-plane $\mathrm{Re}(s) > 1$. In 1737 Leonhard Euler discovered the connection between the zeta function and the prime numbers. Nowadays, this is also known as Euler's identity

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{(1-p^{-s})}.$$

In addition, this function has an analytic continuation to $\mathbb{C}\backslash\{1\}$, with a simple pole at $s = 1$. This continuation satisfies the functional equation

$$\zeta_{\mathbb{Q}}(s) = 2(2\pi)^{s-1}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta_{\mathbb{Q}}(1-s),$$

where Γ is the well-known Gamma function. An open question about the Riemann-zeta function is the behaviour of the zeros. By Euler's identity it is clear that $\zeta_{\mathbb{Q}}(s)$ has no zeros on the complex plane with $\mathrm{Re}(s) > 1$. As a consequence of the functional equation, the zeros on $\mathrm{Re}(s) < 0$ are precisely the even negative integers, and these are called the trivial zeros. The behaviour of the zeros on $0 \leq \mathrm{Re}(s) \leq 1$ is nowadays only formulated in a conjecture. This conjecture, by which the Riemann zeta function owns the most of its fame, is also known as the Riemann hypothesis.

Riemann Hypothesis 5.1.1. *The non-trivial zeros of $\zeta_{\mathbb{Q}}(s)$ lie on the line $Re(s) = \frac{1}{2}$.*

The Riemann zeta function can be generalized to an arbitrary number field K of degree n. This generalization is known as the Dedekind zeta function.

Definition 5.1.2. The *Dedekind zeta function* of a number field K is defined as

$$\zeta_K(s) = \sum_{\substack{I \subset \mathcal{O}_K \\ I \neq 0}} \frac{1}{N(I)^s},$$

where the sum ranges over all non-zero ideals $I \subset \mathcal{O}_K$, and $N(I)$ is the absolute norm of I as in Definition 1.6.18.

This function has similar convergence properties as the Riemann zeta function. It moreover also has a representation as an Euler product over the primes of $\mathcal{O}_K$.

Proposition 5.1.3. (cf. [Neu99, Prop.VII.5.2]) *The Dedekind zeta function $\zeta_K(s)$ converges absolutely and uniformly on the domain $Re(s) > 1$, and one has*

$$\zeta_K(s) = \sum_{\substack{I \subset \mathcal{O}_K \\ I \neq 0}} \frac{1}{N(I)^s} = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ prime}} \frac{1}{(1 - N(\mathfrak{p})^{-s})}.$$

In view of the Euler product expansion of $\zeta_K(s)$, we can define the local ζ_K-factors in a similar way as the local L-factors for an elliptic curve E/K.

Definition 5.1.4. The *local ζ_K-factor* of the Dedekind zeta function ζ_K at a finite place $v \in M_K^0$ is given by

$$\zeta_{K,v}(T) := 1 - T \in \mathbb{Z}[T].$$

By writing $q_v := N(\mathfrak{p}_v) = |\mathcal{O}_K/\mathfrak{p}_v|$, where $\mathfrak{p}_v$ is the corresponding prime to v in $\mathcal{O}_K$, we obtain the expression

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{prime}}} \frac{1}{(1 - N(\mathfrak{p})^{-s})} = \prod_{v \in M_K^0} \frac{1}{(1 - q_v^{-s})} = \prod_{v \in M_K^0} \zeta_{K,v}(q_v^{-s})^{-1}$$

on the domain $\mathrm{Re}(s) > 1$. We now turn to one of the main results for the Dedekind zeta function, which relates the function to multiple mathematical invariants of a number field.

Theorem 5.1.5 (Analytic Class Number Formula)**.** (cf. [Neu99, Cor.VII.5.11]) *Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and $2r_2$ the number of complex embeddings. The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}\backslash\{1\}$ with a simple pole at $s = 1$. The residue of $\zeta_K(s)$ at $s = 1$ is given by*

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot R_K}{\sqrt{|\Delta_K|} \cdot \#(\mathcal{O}_K^\times)_{tors}}.$$

where h_K is the class number of K, Δ_K the discriminant, and R_K the regulator of K.

Remark 5.1.6. Recall that in Section 1.6 we discussed all the appearing quantities in the residue formula given above, except for the regulator R_K of K. Section 5.2 will be devoted to defining this regulator.

5.2 The Regulator of a Number Field

In this section we introduce the regulator of a number field. The unit group $\mathcal{O}_K^\times$ induces a lattice inside a subspace of $\mathbb{R}^{r_1+r_2}$ under the logarithmic embedding. The regulator is defined as the volume of the obtained lattice. Recall that the volume of a lattice actually represents the volume of the corresponding fundamental domain. In other words, the regulator measures, in some sense, the density of the group of units. If the regulator is small, then the volume of the fundamental domain is small, meaning that the units are “quite” dense. Besides introducing this regulator, we also aim to construct a bilinear form with respect to which the regulator can be computed just as for elliptic curves.

We define the logarithmic embedding

$$\lambda : K^\times \to \mathbb{R}^{r_1+r_2},\ \alpha \mapsto (\log|\sigma_1(\alpha)|^{n_{\sigma_1}}, ..., \log|\sigma_{r_1+r_2}(\alpha)|^{n_{\sigma_{r_1+r_2}}}),$$

where n_{σ_i} equals 1 if σ_i is a real embedding, and equals 2 if σ_i is a complex embedding. We moreover consider the (r_1+r_2-1)-dimensional hyperplane $H := \{x \in \mathbb{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1+r_2} x_i = 0\}$, and observe that for $\alpha \in \mathcal{O}_K^\times$

$$\sum_{i=1}^{r_1+r_2} \lambda_i(\alpha) = \sum_{i=1}^{r_1+r_2} \log|\sigma_i(\alpha)|^{n_{\sigma_i}} = \log \prod_{i=1}^{r_1+r_2} |\sigma_i(\alpha)|^{n_{\sigma_i}} = \log|N_{K/\mathbb{Q}}(\alpha)| = 0,$$

by Proposition 1.6.12. In other words, $\lambda(\mathcal{O}_K^\times) \subset H$. The subset $\Gamma := \lambda(\mathcal{O}_K^\times)$ of H defines a full lattice inside H, see [Neu99, Thm.I.7.3], which by the Dirichlet's unit theorem is spanned by the linearly independent vectors $\lambda(\eta_1), ..., \lambda(\eta_{r_1+r_2-1})$ for some fundamental units $\eta_1, ..., \eta_{r_1+r_2-1}$ in $\mathcal{O}_K^\times$. Note that H is a Euclidean space, since it is a linear subspace of the Euclidean space $\mathbb{R}^{r_1+r_2}$. It therefore makes sense to take the volume of the full lattice $\lambda(\mathcal{O}_K^\times)$, as discussed in Section 1.5. It is clear from the definition of the volume of a full lattice, that adding an orthogonal vector of length 1 to the spanning vectors, acquires a full lattice with the same volume as the original one. In this case, we observe that

$$\lambda_{r_1+r_2} := \frac{1}{\sqrt{r_1+r_2}}(1, ..., 1) \in \mathbb{R}^{r_1+r_2}$$

is orthogonal to $\lambda_i := \lambda(\eta_i)$ for all i, and $\lambda_{r_1+r_2}$ has length 1. We thus conclude that the full lattice $\tilde{\Gamma}$ spanned by $\lambda(\eta_1), ..., \lambda(\eta_{r_1+r_2-1}), \lambda_{r_1+r_2}$ has the same volume as Γ, i.e.,

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\tilde{\Gamma}).$$

If we write Λ for the matrix where the columns consist of $\lambda(\eta_1), ..., \lambda(\eta_{r_1+r_2-1}), \lambda_{r_1+r_2}$, then we get

$$\begin{aligned}
\mathrm{vol}(\Gamma) = \mathrm{vol}(\tilde{\Gamma}) = |\det(\langle\lambda_i, \lambda_j\rangle)_{i,j=1}^{r_1+r_2}|^{1/2} &= \left|\det\left(\langle \sum_{k=1}^{r_1+r_2} \lambda_{i,k}e_k, \sum_{l=1}^{r_1+r_2} \lambda_{j,l}e_l\rangle\right)_{i,j=1}^{r_1+r_2}\right|^{1/2} \\
&= \left|\det\left(\sum_{k=1}^{r_1+r_2}\sum_{l=1}^{r_1+r_2} \lambda_{i,k}\lambda_{j,l}\langle e_k, e_l\rangle\right)_{i,j=1}^{r_1+r_2}\right|^{1/2} \\
&= \left|\det\left(\sum_{k=1}^{r_1+r_2} \lambda_{i,k}\lambda_{j,k}\right)_{i,j=1}^{r_1+r_2}\right|^{1/2} \\
&= |\det(\Lambda^T\Lambda)|^{1/2} = |\det(\Lambda)|.
\end{aligned}$$

We observe that adding all rows of Λ to the i-th row, gives

$$\sum_{k=1}^{r_1+r_2} \lambda_k(\eta_j) = \sum_{k=1}^{r_1+r_2} \log|\sigma_k(\eta_j)|^{n_{\sigma_k}} = \log|N_{K/\mathbb{Q}}(\eta_j)| = 0,$$
$$\sum_{k=1}^{r_1+r_2} \lambda_{k(r_1+r_2)} = \sum_{k=1}^{r_1+r_2} \frac{1}{\sqrt{r_1+r_2}} = \sqrt{r_1+r_2},$$

for all $1 \leq j \leq r_1+r_2-1$. As a consequence, combining all the above hands us the equality

$$\mathrm{vol}(\Gamma) = |\det(\Lambda)| = \sqrt{r_1+r_2}|\det(M)|,$$

where M is an arbitrary minor of rank r_1+r_2-1 of the matrix

$$\begin{pmatrix} \lambda_1(\eta_1) & \cdots & \lambda_1(\eta_{r_1+r_2-1}) \\ \vdots & \ddots & \vdots \\ \lambda_{r_1+r_2}(\eta_1) & \cdots & \lambda_{r_1+r_2}(\eta_{r_1+r_2-1}) \end{pmatrix}. \tag{5.1}$$

In other words, any two minor matrices M and M' of the above satisfy $|\det(M)| = |\det(M')|$. Together with this comes the notion of the regulator of a number field.

Definition 5.2.1. The *regulator*, R_K, of a number field K is given by the absolute value of the determinant of an arbitrary minor of rank r_1+r_2-1 of the matrix given at (5.1).

Thus, if $\{\sigma_i\}_{i=1}^{r_1+r_2}$ is a complete set of pairwise non-conjugate embeddings of K into $\mathbb{C}$, then the regulator of K is given by the volume of the lattice $\Gamma_{r_1+r_2-1}$ spanned by the linearly independent vectors $v_i := (\log|\sigma_1(\eta_i)|^{n_{\sigma_1}}, ..., \log|\sigma_{r_1+r_2-1}(\eta_i)|^{n_{\sigma_{r_1+r_2-1}}})$. More precisely, we see that

$$R_K = |\det(M)|, \text{ where } M := (\log|\sigma_i(\eta_j)|^{n_{\sigma_i}})_{i,j=1}^{r_1+r_2-1}. \tag{5.2}$$

To obtain a more obvious similarity with the definition of the regulator of an elliptic curve (Definition 4.3.14), we would like to construct an analogue of the Néron-Tate pairing on $\mathcal{O}_K^\times$ such that the regulator of K can be computed with respect to this symmetric bilinear form. For this, we again consider a complete set $\{\sigma_i\}_{i=1}^{r_1+r_2}$ of non-conjugate embeddings of K into $\mathbb{C}$. By Theorem 1.6.7 we know that every Archimedean absolute value on K is equivalent to an absolute value of the form $|x|_{\sigma_i} = |\sigma_i(x)|$, where the latter absolute value is the standard one on $\mathbb{C}$. Moreover, these define all r_1+r_2 inequivalent Archimedean places. For simplicity, we will denote an Archimedean place by v_{σ_i}. The local degree $n_{v_{\sigma_i}} := [K_{v_{\sigma_i}} : \mathbb{Q}_{v_{\sigma_i}}]$ equals 1 for real embeddings, and 2 for complex embeddings. Recall from Section 1.6 that the normalized Archimedean absolute values are given by

$$\|x\|_{v_{\sigma_i}} := |x|_{v_{\sigma_i}}^{n_{v_{\sigma_i}}} = \begin{cases} |\sigma_i(x)| & \text{if } \sigma_i \text{ is real,} \\ |\sigma_i(x)|^2 & \text{if } \sigma_i \text{ is complex.} \end{cases}$$

We now define the map

$$\langle\cdot,\cdot\rangle : \mathcal{O}_K^\times \times \mathcal{O}_K^\times \to \mathbb{R}, \ \langle x, y\rangle := \sum_{i=1}^{r_1+r_2-1} \log\|x\|_{v_{\sigma_i}} \log\|y\|_{v_{\sigma_i}}, \tag{5.3}$$

which is clearly symmetric. Besides being symmetric, the map is also bilinear, since

$$\begin{aligned}\langle x\cdot x', y\rangle &= \sum_{i=1}^{r_1+r_2-1} \log\|x\cdot x'\|_{v_{\sigma_i}} \log\|y\|_{v_{\sigma_i}} = \sum_{i=1}^{r_1+r_2-1} \left(\log\|x\|_{v_{\sigma_i}} + \log\|x'\|_{v_{\sigma_i}}\right) \log\|y\|_{v_{\sigma_i}} \\ &= \langle x, y\rangle + \langle x', y\rangle\end{aligned}$$

for all $x, x', y \in \mathcal{O}_K^\times$. If we reconsider the matrix M defined in (5.2), we detect the equality

$$M^T M = \left(\sum_{k=1}^{r_1+r_2-1} \log \|\eta_i\|_{v_{\sigma_k}} \log \|\eta_j\|_{v_{\sigma_k}} \right)_{i,j=1}^{r_1+r_2-1} = (\langle \eta_i, \eta_j \rangle)_{i,j=1}^{r_1+r_2-1}.$$

We in particular see that the regulator can be computed with respect to the constructed symmetric bilinear pairing (5.3), as follows

$$R_K = |\det(M)| = |\det(M^T M)|^{1/2} = |\det(\langle \eta_i, \eta_j \rangle)_{i,j=1}^{r_1+r_2-1}|^{1/2}.$$

5.3 The Tate-Shafarevich Group of a Number Field

When considering a number field K, one of the central objects to consider is the corresponding ideal class group. This class group measures how far the ring of integers $\mathcal{O}_K$ is from being a principal ideal domain. In a one-dimensional domain, being principal is equivalent to being a unique factorization domain. For an elliptic curve E/K we have the Tate-Shafarevich group $Ш(E/K)$, which also measures a certain defect. To clarify this, we consider an equivalent description of $Ш(E/K)$ in terms of homogeneous spaces as discussed in ([Sil09, CH.X]). For this description a non-zero element of $Ш(E/K)$ is an equivalence class of homogeneous spaces for E/K that possess a K_v-rational point for every $v \in M_K$, but not a K-rational point. This suggests that finding a rational point everywhere locally is equivalent to finding a global point for every homogeneous space if and only if the group $Ш(E/K)$ is trivial. This idea is also known as Hasse's local-global principle. In other words, one could say that $Ш(E/K)$ measures whether Hasse's principle is satisfied or not. In this section, we will connect the two measures by defining a cohomological analogue of the Tate-Shafarevich group for a number field. The methods used are based on [Kai16].

Let $\overline{K}$ be the algebraic closure of K, with ring of integers $\mathcal{O}_{\overline{K}}$. This ring consists of all elements $x \in \overline{K}$ for which there exists a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(x) = 0$. We now observe that there is a canonical $\mathrm{Gal}(\overline{K}/K)$-action on $\mathcal{O}_{\overline{K}}$. Namely, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $x \in \mathcal{O}_{\overline{K}}$ we have

$$f(\sigma(x)) = \sigma(f(x)) = \sigma(0) = 0,$$

for some monic $f \in \mathbb{Z}[X]$. In particular, we get a $\mathrm{Gal}(\overline{K}/K)$-action on the group of units $\mathcal{O}_{\overline{K}}^\times$. The fixed points under this action are precisely the elements of the unit group $\mathcal{O}_K^\times$. Recall that the extension $\overline{K}/K$ is a Galois extension. In particular, by Proposition 3.4.7 the discussed $\mathrm{Gal}(\overline{K}/K)$-modules are actually discrete. As a consequence, the Galois cohomology theory can be applied. For simplicity, we neglect the subscript "c" from the notation of the cohomology functor for profinite groups. Since we only encounter discrete Galois modules, this will not lead to any confusion. One of the reasons why it feels natural to consider $\mathcal{O}_{\overline{K}}^\times$ instead of $\mathcal{O}_{\overline{K}}$ is that by Dirichlet's unit theorem $\mathcal{O}_K^\times$ is a finitely generated abelian group. This suggests that it might replace the role of the group of K-rational points on an elliptic curve, which plays an important role in the construction of the Tate-Shafarevich group.

For each $v \in M_K^0$, let $\mathcal{O}_{\overline{K_v}}$ denote the valuation ring of $\overline{K_v}$. Moreover, for each $v \in M_K^\infty$, let $\mathcal{O}_{\overline{K_v}} := \overline{K_v}$. Then we can define the Tate-Shafarevich group of a number field in a similar way as the Tate-Shafarevich group of an elliptic curve. For this we recall the map

$$\varphi_{\iota_v} : \mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{K}/K),\ \sigma \mapsto \iota_v^{-1} \circ \sigma \circ \iota_v$$

from Proposition 4.4.1. In this case, it induces a well-defined group homomorphism on cohomology groups,

$$\tilde{\beta}_v : H^1(\mathrm{Gal}(\overline{K}/K), \mathcal{O}_{\overline{K}}^\times) \to H^1(\mathrm{Gal}(\overline{K_v}/K_v), \mathcal{O}_{\overline{K_v}}^\times),\ [f] \mapsto [\iota_v \circ f \circ \varphi_{\iota_v}].$$

Definition 5.3.1. The *Tate-Shafarevich group* of a number field K is defined as

$$Ш(K) := \bigcap_{v \in M_K} \ker\left(H^1(\mathrm{Gal}(\overline{K}/K), \mathcal{O}_{\overline{K}}^\times) \xrightarrow{\tilde{\beta}_v} H^1(\mathrm{Gal}(\overline{K_v}/K_v), \mathcal{O}_{\overline{K_v}}^\times) \right).$$

The well-definedness follows in a similar way as for the Tate-Shafarevich group of an elliptic curve over K as we have seen in Section 4.4. To simplify the definition slightly, we can use the following theorem:

Theorem 5.3.2 (Hilbert's Theorem 90)**.** (cf. [SW08, Thm.6.2.1]) *If L/K is a Galois extension, then the first cohomology group is trivial, i.e., $H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$.*

In particular, for each $v \in M_K^\infty$ we have $H^1(\mathrm{Gal}(\overline{K_v}/K_v), \mathcal{O}_{\overline{K_v}}^\times) = \{1\}$. If we moreover write $H^1(K, \mathcal{O}_{\overline{K}}^\times)$ for $H^1(\mathrm{Gal}(\overline{K}/K), \mathcal{O}_{\overline{K}}^\times)$, then our definition of $Ш(K)$ can be reduced to

$$Ш(K) := \bigcap_{v \in M_K^0} \ker\left(H^1(K, \mathcal{O}_{\overline{K}}^\times) \xrightarrow{\tilde{\beta}_v} H^1(K_v, \mathcal{O}_{\overline{K_v}}^\times) \right).$$

The construction of the desired isomorphism between this group and the class group relies on the exact sequence of certain cohomology groups obtained by applying the cohomology functor to an exact sequence of discrete $\mathrm{Gal}(\overline{K}/K)$-modules.

Note that for each number field K we have a canonical exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to \mathcal{I}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K) \to 1, \tag{5.4}$$

consisting of the set of invertible fractional $\mathcal{O}_K$-ideals and the class group of K. Moreover, we have the canonical short exact sequence

$$1 \to \mathcal{O}_{\overline{K}}^\times \to \overline{K}^\times \to \overline{K}^\times/\mathcal{O}_{\overline{K}}^\times \to 1.$$

We make the observation that this exact sequence also defines an exact sequence of discrete $\mathrm{Gal}(\overline{K}/K)$-modules. For the first two groups, this immediately follows from Proposition 3.4.7. The group $\overline{K}^\times/\mathcal{O}_{\overline{K}}^\times$ is a discrete $\mathrm{Gal}(\overline{K}/K)$-module, since the quotient of two discrete $\mathrm{Gal}(\overline{K}/K)$-modules is again discrete. This exact sequence can be slightly modified by using the isomorphism constructed in Lemma 1.6.2. Namely, this gives a group isomorphism between $\overline{K}^\times/\mathcal{O}_{\overline{K}}^\times$ and $\mathcal{P}(\mathcal{O}_{\overline{K}})$. It is moreover easily verified that this isomorphism makes $\mathcal{P}(\mathcal{O}_{\overline{K}})$ into a discrete $\mathrm{Gal}(\overline{K}/K)$-module. We thus get the following short exact sequence of discrete $\mathrm{Gal}(\overline{K}/K)$-modules:

$$1 \to \mathcal{O}_{\overline{K}}^\times \to \overline{K}^\times \to \mathcal{P}(\mathcal{O}_{\overline{K}}) \to 1.$$

By applying Proposition 3.4.6 we get a natural exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to H^0(K, \mathcal{P}(\mathcal{O}_{\overline{K}})) \xrightarrow{\delta} H^1(K, \mathcal{O}_{\overline{K}}^\times) \to H^1(K, \overline{K}^\times) \cong 1. \tag{5.5}$$

The cohomology group $H^0(K, \mathcal{P}(\mathcal{O}_{\overline{K}}))$ consists of all Galois-invariant principal fractional ideals in $\overline{K}$, which are also called *ambiguous* principal ideals. This justifies the simplified notation $\mathrm{Amb}(\overline{K})$ for the group considered. The boundary map is now given by

$$\delta : \mathrm{Amb}(\overline{K}) \to H^1(K, \mathcal{O}_{\overline{K}}^\times),\ x\mathcal{O}_{\overline{K}} \mapsto [f_x], \tag{5.6}$$

where $f_x : \mathrm{Gal}(\overline{K}/K) \to \mathcal{O}_{\overline{K}}^{\times}$ maps σ to $\sigma(x)x^{-1}$.

Our goal is to find an isomorphism between $\mathrm{Cl}(\mathcal{O}_K)$ and $\text{Ш}(K)$. We aim to construct a map from $\mathcal{I}(\mathcal{O}_K)$ to $\mathrm{Amb}(\overline{K})$, and a map from $\mathrm{Cl}(\mathcal{O}_K)$ to $H^1(K, \mathcal{O}_{\overline{K}}^{\times})$ such that (5.4) and (5.5) combine into a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^{\times} \arrow[r] \arrow[d] & K^{\times} \arrow[r] \arrow[d] & \mathcal{I}(\mathcal{O}_K) \arrow[r] \arrow[d] & \mathrm{Cl}(\mathcal{O}_K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathcal{O}_{\overline{K}}^{\times} \arrow[r] & \overline{K}^{\times} \arrow[r] & \mathrm{Amb}(\overline{K}) \arrow[r] & H^1(K, \mathcal{O}_{\overline{K}}^{\times}) \arrow[r] & 1.
\end{tikzcd} \tag{5.7}$$

Moreover, we will show that the final vertical map defines an isomorphism between $\mathrm{Cl}(\mathcal{O}_K)$ and $\text{Ш}(K)$. The following lemma states that the extension of an invertible fractional ideal on K defines a principal ideal on $\overline{K}$.

Lemma 5.3.3. *For any $I \in \mathcal{O}_K$, there exists a finite extension L/K such that $I\mathcal{O}_L$ is principal. Moreover, $I\mathcal{O}_{\overline{K}}$ is principal.*

Proof. Let $I \in \mathcal{I}(\mathcal{O}_K)$ be an invertible ideal of $\mathcal{O}_K$. Recall by Theorem 1.6.20 that the class group is finite, say of cardinality n. Therefore, we have $I^n = \alpha\mathcal{O}_K$ for some $\alpha \in K^{\times}$. Consider the finite extension $L := K(\beta)$, where β is a zero of $X^n - \alpha$. Under these circumstances, we find that

$$(I\mathcal{O}_L)^n = I^n\mathcal{O}_L = \alpha\mathcal{O}_K\mathcal{O}_L = (\beta\mathcal{O}_L)^n.$$

By using the unique prime ideal factorization inside $\mathcal{O}_L$, we find that $I\mathcal{O}_L = \beta\mathcal{O}_L$. Thus the first part of the lemma has been proven.

For the second part, notice that for every $I \in \mathcal{I}(\mathcal{O}_K)$ there exists a finite extension L/K such that $I\mathcal{O}_L = x\mathcal{O}_L$ for some $x \in L^{\times}$. As a consequence, we find that

$$I\mathcal{O}_{\overline{K}} = I\mathcal{O}_L\mathcal{O}_{\overline{K}} = x\mathcal{O}_L\mathcal{O}_{\overline{K}} = x\mathcal{O}_{\overline{K}},$$

since $\mathcal{O}_L \subset \mathcal{O}_{\overline{K}}$. Thus $I\mathcal{O}_{\overline{K}}$ is principal as well. ■

Lemma 5.3.4. *The map $\alpha : \mathcal{I}(\mathcal{O}_K) \to Amb(\overline{K})$ given by $I \mapsto I\mathcal{O}_{\overline{K}}$ is a well-defined injection. Moreover, it induces the well-defined injective function*

$$\beta : \mathrm{Cl}(\mathcal{O}_K) \to H^1(K, \mathcal{O}_{\overline{K}}^{\times}), \ \beta([I]) := \delta(\alpha(I)),$$

where δ is the boundary map given at (5.6).

Proof. We will first show that α is a well-defined map. This comes down to showing that $I\mathcal{O}_{\overline{K}} \in \mathrm{Amb}(\overline{K})$ for every $I \in \mathcal{I}(\mathcal{O}_K)$. The principality follows from Lemma 5.3.3. To prove that $I\mathcal{O}_{\overline{K}}$ is ambiguous, we let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $x \in I\mathcal{O}_{\overline{K}}$. Then x has the form $x = \sum_{i=1}^{n} x_i y_i$ for some $x_i \in I$ and $y_i \in \mathcal{O}_{\overline{K}}$. Consequently, we find that

$$\sigma(x) = \sum_{i=1}^{n} \sigma(x_i)\sigma(y_i) = \sum_{i=1}^{n} x_i\sigma(y_i) \in I\mathcal{O}_{\overline{K}}.$$

In addition, we observe that for $\tilde{x} := \sum_{i=1}^{n} x_i\sigma^{-1}(y_i) \in I\mathcal{O}_{\overline{K}}$ we have $\sigma(\tilde{x}) = x$. This proves that $\sigma(I\mathcal{O}_{\overline{K}}) = I\mathcal{O}_{\overline{K}}$, and thus $I\mathcal{O}_{\overline{K}} \in \mathrm{Amb}(\overline{K})$.

For the injectivity, suppose that $I\mathcal{O}_{\overline{K}} = J\mathcal{O}_{\overline{K}}$ for some $I, J \in \mathcal{I}(\mathcal{O}_K)$. Observe that by Lemma 5.3.3 there clearly exists a finite extension L/K such that $I\mathcal{O}_L = J\mathcal{O}_L$. As a consequence, we find by Proposition 1.7.6 that $I = I\mathcal{O}_L \cap \mathcal{O}_K = J\mathcal{O}_L \cap \mathcal{O}_K = J$, showing that α is indeed injective.

Now consider the map β as defined above. We want to show that $\delta \circ \alpha$ is constant on the equivalence classes in $\mathrm{Cl}(\mathcal{O}_K)$. Assume that $[I] = [J]$ in $\mathrm{Cl}(\mathcal{O}_K)$, then $I = x_0 J$ for some $x_0 \in K^\times$. Note that $\alpha(I) = I\mathcal{O}_{\overline{K}}$ and $\alpha(J) = J\mathcal{O}_{\overline{K}}$ are principal, meaning that there exist $x_I, x_J \in \overline{K}^\times$ such that $I\mathcal{O}_{\overline{K}} = x_I\mathcal{O}_{\overline{K}}$ and $J\mathcal{O}_{\overline{K}} = x_J\mathcal{O}_{\overline{K}}$. By combining all the results, we find that $x_I\mathcal{O}_{\overline{K}} = x_0 x_J \mathcal{O}_{\overline{K}}$. This in particular implies that $x_I = x_0 x_J u$ for some unit $u \in \mathcal{O}_{\overline{K}}^\times$. By writing f_x for the 1-cocycle as in the definition of δ for an arbitrary $x \in \overline{K}^\times$, we find for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ that

$$f_{x_I}(\sigma) = \sigma(x_I)x_I^{-1} = \sigma(x_0 x_J u)u^{-1}x_J^{-1}x_0^{-1} = \sigma(x_J)x_J^{-1}\sigma(u)u^{-1} = f_{x_J}(\sigma)f_u(\sigma).$$

Since f_u is a 1-coboundary, we conclude that $\delta(\alpha(I)) = [f_{x_I}] = [f_{x_J}] = \delta(\alpha(J))$. In other words, β is well-defined.

We are left to show that β is also an injection. We assume that $\beta([I]) = \beta([J])$ for some $I, J \in \mathcal{I}(\mathcal{O}_K)$. Again by Lemma 5.3.3 there exist $x_I, x_J \in \overline{K}^\times$ such that $I\mathcal{O}_{\overline{K}} = x_I\mathcal{O}_{\overline{K}}$ and $J\mathcal{O}_{\overline{K}} = x_J\mathcal{O}_{\overline{K}}$. By assumption we have $[f_{x_I}] = [f_{x_J}]$, which is equivalent to saying that there exists a $u \in \mathcal{O}_{\overline{K}}^\times$ such that $f_{x_I}f_{x_J^{-1}} = f_u$. Thus, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have

$$f_{x_I}(\sigma)f_{x_J^{-1}}(\sigma) = \sigma(x_I)x_I^{-1}\sigma(x_J)^{-1}x_J = \sigma(x_I x_J^{-1})x_I^{-1}x_J = \sigma(u)u^{-1} = f_u(\sigma),$$

implying that $\sigma(x_I x_J^{-1}u^{-1}) = x_I x_J^{-1}u^{-1}$. Owing to the fact that $\overline{K}/K$ is a Galois extension, we find that $x_I x_J^{-1}u^{-1} \in K^\times$. In other words, there exists $x_0 \in K^\times$ such that $x_I = x_0 x_J u$. Consequently, we find that

$$\alpha(I) = I\mathcal{O}_{\overline{K}} = x_I\mathcal{O}_{\overline{K}} = x_0 x_J\mathcal{O}_{\overline{K}} = x_0 J\mathcal{O}_{\overline{K}} = \alpha(x_0 J).$$

The injectivity of α now tells us that $I = x_0 J$. This provides the final argument, i.e. $[I] = [J]$, to conclude that β is injective. ■

It is easily seen that the functions α and β define group homomorphisms. To finish the ingredients of the recipe to prove that β defines an isomorphism with $\text{Ш}(K)$, we need the following result.

Lemma 5.3.5. *Let I be a non-zero proper ideal of $\mathcal{O}_K$. Then every ideal class of K contains an ideal prime to I.*

Proof. We first notice that every ideal class of K can be represented by a non-zero proper ideal $J \subset \mathcal{O}_K$. So let $J \subset \mathcal{O}_K$ be such an ideal, and $[J]$ be the corresponding ideal class in $\mathrm{Cl}(\mathcal{O}_K)$. The goal is to construct an ideal J_0 such that J_0 is relatively prime to I and $[J]^{-1} = [J_0]$, which means that the inverse of any ideal class contains an ideal prime to I. This is equivalent to saying that every ideal class contains an ideal prime to I.

For the construction of J_0, let $\{\mathfrak{p}_1, ..., \mathfrak{p}_l\}$ be the set of primes dividing I which do not divide J. We now define $e(\mathfrak{p}) := \mathrm{ord}_{\mathfrak{p}}(J)$ as the exponent of $\mathfrak{p}$ in the prime decomposition of J. For every prime $\mathfrak{p}|J$, we can choose an element $x_{\mathfrak{p}} \in \mathfrak{p}^{e(\mathfrak{p})}\backslash\mathfrak{p}^{e(\mathfrak{p})+1}$. Note that the ideals $\mathfrak{p}_i$ and $\mathfrak{p}^{e(\mathfrak{p})+1}$ with $i = 1, 2, ..., l$ and $\mathfrak{p}|J$ are coprime. Therefore, the Chinese remainder theorem hands us the existence of an $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv \begin{cases} x_{\mathfrak{p}} \mod \mathfrak{p}^{e(\mathfrak{p})+1} & \text{for } \mathfrak{p}|J, \\ 1 \mod \mathfrak{p}_i & \text{for } i = 1, 2, ..., l. \end{cases}$$

Similarly as the integer $e(\mathfrak{p})$, we define the non-negative integer $\alpha(\mathfrak{p}) := \operatorname{ord}_{\mathfrak{p}}(\alpha\mathcal{O}_K)$ for each prime $\mathfrak{p} \subset \mathcal{O}_K$. Moreover, we deduce the following ideal

$$J_0 := \prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}^{\alpha(\mathfrak{p})-e(\mathfrak{p})}, \text{ where } \alpha(\mathfrak{p}) - e(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p}|J \\ 0 & \text{if } \mathfrak{p} = \mathfrak{p}_i \text{ for some } i = 1, 2, ..., l \\ \alpha(\mathfrak{p}) & \text{otherwise.} \end{cases}$$

By construction we find that $JJ_0 = \alpha\mathcal{O}_K$, meaning that $[J]^{-1} = [J_0]$. On top of that, we see that J_0 and I have no common prime factors, implying that J_0 and I are relatively prime. ■

In the definition of the Tate-Shafarevich group of a number field, we consider non-Archimedean places $v \in M_K^0$ and fix embeddings $\iota_v : \overline{K} \to \overline{K_v}$. As stated in Theorem 1.6.7, every non-Archimedean place can be represented by a $\mathfrak{p}$-adic valuation for some unique prime $\mathfrak{p} \subset \mathcal{O}_K$. Therefore, we can consider

$$Ш(K) = \bigcap_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ \text{prime}}} \ker\left(H^1(K, \mathcal{O}_{\overline{K}}^\times) \xrightarrow{\tilde{\beta}_{\mathfrak{p}}} H^1(K_{\mathfrak{p}}, \mathcal{O}_{\overline{K_{\mathfrak{p}}}}^\times)\right),$$

and extend the diagram at (5.7) to the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d] & K^\times \arrow[r] \arrow[d] & \mathcal{I}(\mathcal{O}_K) \arrow[r] \arrow[d, "\alpha"] & \operatorname{Cl}(\mathcal{O}_K) \arrow[r] \arrow[d, "\beta"] & 1 \\
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d] & K^\times \arrow[r] \arrow[d] & \operatorname{Amb}(\overline{K}) \arrow[r, "\delta"] \arrow[d, "\tilde{\alpha}:=(\tilde{\alpha}_{\mathfrak{p}})_{\mathfrak{p}}"] & H^1(K, \mathcal{O}_{\overline{K}}^\times) \arrow[r] \arrow[d, "\tilde{\beta}:=(\tilde{\beta}_{\mathfrak{p}})_{\mathfrak{p}}"] & 1 \\
1 \arrow[r] & \prod_{\mathfrak{p}} \mathcal{O}_{K_{\mathfrak{p}}}^\times \arrow[r] & \prod_{\mathfrak{p}} K_{\mathfrak{p}}^\times \arrow[r] & \prod_{\mathfrak{p}} \operatorname{Amb}(\overline{K}_{\mathfrak{p}}) \arrow[r, "\tilde{\delta}:=(\tilde{\delta}_{\mathfrak{p}})_{\mathfrak{p}}"] & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, \mathcal{O}_{\overline{K_{\mathfrak{p}}}}^\times) \arrow[r] & 1.
\end{tikzcd} \tag{5.8}$$

Moreover, the rows in this diagram are exact. We now show that β in the diagram defines an isomorphism with $Ш(K)$. For this, knowledge about the extensions of the $\mathfrak{p}$-adic valuations to algebraic extensions of K is needed.

Remark 5.3.6. Let $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal with corresponding $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}$ on K. Then there is a unique extension of $v_{\mathfrak{p}}$ to the completion $K_{\mathfrak{p}}$. Since $K_{\mathfrak{p}}$ is complete with respect to the valuation $v_{\mathfrak{p}}$ we find by [Neu99, Thm.II.4.8] that it can be extended uniquely to the algebraic extension $\overline{K}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$, which we will denote by $\overline{v_{\mathfrak{p}}}$. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ we can fix an embedding $i_{\mathfrak{p}} : \overline{K} \to \overline{K}_{\mathfrak{p}}$. For a finite extension L/K, we clearly have $L \subset \overline{K}$. As a consequence, the valuation $\overline{v_{\mathfrak{p}}}$ on $\overline{K}_{\mathfrak{p}}$ induces a valuation $w = \overline{v_{\mathfrak{p}}}_{|_L}$ on L. In other words, w is an extension of $v_{\mathfrak{p}}$ to L. As discussed in [Neu99, CH.2.8], every extension of $v_{\mathfrak{p}}$ to L is of the form $w_{\mathfrak{q}} = \frac{1}{e_{\mathfrak{q}}} v_{\mathfrak{q}}$ for some prime $\mathfrak{q} \subset \mathcal{O}_L$ with ramification index $e_{\mathfrak{q}} \geq 1$ in the unique prime factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$. Consequently, $w = w_{\mathfrak{q}}$ for some prime $\mathfrak{q} \subset \mathcal{O}_L$ such that $\mathfrak{q}|\mathfrak{p}$.

Theorem 5.3.7. *The map β defined in Lemma 5.3.4 defines an isomorphism between* $\operatorname{Cl}(\mathcal{O}_K)$ *and* $Ш(K)$.

Proof. Observe that $\ker(\tilde{\beta}) = Ш(K)$. Therefore, it suffices to show that $\operatorname{im}(\beta) = \ker(\tilde{\beta})$.

We start by proving the inclusion $\operatorname{im}(\beta) \subset \ker(\tilde{\beta})$. Let $[f] \in \operatorname{im}(\beta)$, then there exists $[I] \in \operatorname{Cl}(\mathcal{O}_K)$ such that $\beta([I]) = [f]$. Lemma 5.3.5 now implies that for every prime $\mathfrak{p} \subset \mathcal{O}_K$ there exists an ideal $J \in [I]$ such that J is relatively prime to $\mathfrak{p}$. In addition, observe that by Lemma 5.3.3 we have $\alpha(J) = x_J\mathcal{O}_{\overline{K}}$ for some $x_J \in \overline{K}^\times$ such that $J\mathcal{O}_L = x_J\mathcal{O}_L$ for the finite extension $L = K(x_J)$ of K. By the discussion in 5.3.6, we know that $\overline{v_{\mathfrak{p}}}_{|_L} = w_{\mathfrak{q}} = \frac{1}{e_{\mathfrak{q}}} v_{\mathfrak{q}}$ for some prime $\mathfrak{q} \subset \mathcal{O}_L$ satisfying $\mathfrak{q}|\mathfrak{p}$. As a direct consequence of the fact that $\mathfrak{p}$ is relatively prime to J, we have that $\mathfrak{p} \not| J$. Corollary 1.7.4 now implies that $\mathfrak{q} \not| J\mathcal{O}_L = x_J\mathcal{O}_L$. Therefore,

$$\overline{v_{\mathfrak{p}}}(x_J) = \overline{v_{\mathfrak{p}}}_{|_L}(x_J) = w_{\mathfrak{q}}(x_J) = \frac{1}{e_{\mathfrak{q}}} v_{\mathfrak{q}}(x_J) = 0,$$

which implies that $x_J \in \mathcal{O}^{\times}_{\overline{K_{\mathfrak{p}}}}$. Recall that $[f] = \beta([I]) = \beta([J]) = [f_{x_J}]$, where the representing 1-cocycle $f_{x_J} : \mathrm{Gal}(\overline{K}/K) \to \mathcal{O}^{\times}_{\overline{K}}$ maps σ to $\sigma(x_J)x_J^{-1}$. As a consequence, we find that $\tilde{\beta}_{\mathfrak{p}}([f])$ is represented by

$$f_{x_J,\mathfrak{p}} : \mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}}) \to \mathcal{O}_{\overline{K_{\mathfrak{p}}}^{\times}}, \ \sigma \mapsto \sigma(x_J)x_J^{-1}.$$

But since $x_J \in \mathcal{O}^{\times}_{\overline{K_{\mathfrak{p}}}}$, this defines a 1-coboundary implying that $\tilde{\beta}_{\mathfrak{p}}([f]) = [f_{x_J,\mathfrak{p}}] = [1]$. Recall that $\mathfrak{p} \subset \mathcal{O}_K$ was taken arbitrarily, meaning that $\tilde{\beta}([f]) = ([1])_{\mathfrak{p}}$. Hence the first inclusion $\mathrm{im}(\beta) \subset \ker(\tilde{\beta}) = \text{Ш}(K)$ is satisfied.

For the other inclusion, let $[f] \in \text{Ш}(K)$. This means that $\tilde{\beta}([f]) = ([1])_{\mathfrak{p}}$. By the exactness of the middle row in (5.8), we know that δ is surjective. Therefore, there exists $t \in \overline{K}^{\times}$ such that $\delta(t\mathcal{O}_{\overline{K}}) = [f]$ with $t\mathcal{O}_{\overline{K}} \in \mathrm{Amb}(\overline{K})$. We want to show that $[f] \in \mathrm{im}(\beta)$, and thus by the latter it suffices to show that $t\mathcal{O}_{\overline{K}} \in \mathrm{im}(\alpha)$. Namely, in that case there exists $I \in \mathcal{I}(\mathcal{O}_K)$ such that $\beta([I]) = \delta(\alpha(I)) = \delta(t\mathcal{O}_{\overline{K}}) = [f]$. The case when $t\mathcal{O}_{\overline{K}} = \mathcal{O}_{\overline{K}}$ is trivial, and we can therefore assume that $t \notin \mathcal{O}^{\times}_{\overline{K}}$. Now notice that

$$\tilde{\delta}(\tilde{\alpha}(t\mathcal{O}_{\overline{K}})) = \tilde{\beta}(\delta(t\mathcal{O}_{\overline{K}})) = ([1])_{\mathfrak{p}}.$$

Subsequently, we find by the exactness of the bottom row in (5.8) that for each $\mathfrak{p} \subset \mathcal{O}_K$ there exists $t_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times}$ such that $t_{\mathfrak{p}}\mathcal{O}_{\overline{K_{\mathfrak{p}}}} = \tilde{\alpha}(t\mathcal{O}_{\overline{K}}) = t\mathcal{O}_{\overline{K_{\mathfrak{p}}}}$. This for instance implies that

$$\overline{v_{\mathfrak{p}}}(t) = \overline{v_{\mathfrak{p}}}(t_{\mathfrak{p}}) = v_{\mathfrak{p}}(t_{\mathfrak{p}}),$$

since $t_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times}$. Recall that $\overline{K}$ can be written as a union consisting of all finite Galois extensions of K. Therefore, we can take a finite Galois extension L/K such that $t \in L$. In particular, $t \notin \mathcal{O}_L^{\times} \subset \mathcal{O}^{\times}_{\overline{K}}$ by assumption. As a consequence, we find by the unique prime factorization in $\mathcal{O}_L$ that

$$t\mathcal{O}_L = \prod_{\mathfrak{q} \subset \mathcal{O}_L} \mathfrak{q}^{a_{\mathfrak{q}}} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \prod_{\substack{\mathfrak{q} \subset \mathcal{O}_L \\ \mathfrak{q}|\mathfrak{p}}} \mathfrak{q}^{a_{\mathfrak{q}}},$$

where $a_{\mathfrak{q}} := v_{\mathfrak{q}}(t)$ and the products are taken over the primes. As proven in [Con20, Cor.A.2], every $\sigma \in \mathrm{Gal}(L/K)$ has a lifting $\tilde{\sigma} \in \mathrm{Gal}(\overline{K}/K)$ such that $\sigma = \tilde{\sigma}_{|_L}$. Thus for $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\sigma(t\mathcal{O}_L) = \tilde{\sigma}_{|_L}(t\mathcal{O}_L) = \tilde{\sigma}(t\mathcal{O}_{\overline{K}} \cap \mathcal{O}_L) = \tilde{\sigma}(t\mathcal{O}_{\overline{K}}) \cap \tilde{\sigma}(\mathcal{O}_L) = t\mathcal{O}_{\overline{K}} \cap \mathcal{O}_L = t\mathcal{O}_L,$$

where we used that $t\mathcal{O}_{\overline{K}} \in \mathrm{Amb}(\overline{K})$. Since $\mathrm{Gal}(L/K)$ acts transitively on the primes in L above a fixed prime $\mathfrak{p}$ of $\mathcal{O}_K$, we obtain by applying the same arguments as in the proof of Theorem 1.7.7, that $a_{\mathfrak{q}} = a_{\mathfrak{q}'}$ for $\mathfrak{q}, \mathfrak{q}'|\mathfrak{p}$. Therefore, we can define $a_{\mathfrak{p}} := a_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$. Because of the fact that L/K is a finite Galois extension, Theorem 1.7.7 implies that the ramification indices $e_{\mathfrak{q}} = e_{\mathfrak{q}'}$ for $\mathfrak{q}, \mathfrak{q}'|\mathfrak{p}$. Consequently, we can also put $e_{\mathfrak{p}} := e_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$. Now let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime and $\mathfrak{q} \subset \mathcal{O}_L$ be the prime induced by the embedding of $\overline{K}$ into $\overline{K_{\mathfrak{p}}}$ as discussed in Remark 5.3.6. Then

$$a_{\mathfrak{p}} = a_{\mathfrak{q}} = v_{\mathfrak{q}}(t) = e_{\mathfrak{q}} w_{\mathfrak{q}}(t) = e_{\mathfrak{p}} \overline{v_{\mathfrak{p}}}_{|_L}(t) = e_{\mathfrak{p}} \overline{v_{\mathfrak{p}}}(t_{\mathfrak{p}}) = e_{\mathfrak{p}} v_{\mathfrak{p}}(t_{\mathfrak{p}}).$$

Since the $\mathfrak{p}$-adic valuation on K has value group $\mathbb{Z}$, the value group of the completion $K_\mathfrak{p}$ is also $\mathbb{Z}$. Combining this with the above yields that $a_\mathfrak{p}/e_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p} \subset \mathcal{O}_K$. As a consequence, by using all the results from above, we find the following

$$t\mathcal{O}_L = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \prod_{\substack{\mathfrak{q}\subset\mathcal{O}_L \\ \mathfrak{q}|\mathfrak{p}}} \mathfrak{q}^{a_\mathfrak{p}\cdot\frac{e_\mathfrak{p}}{e_\mathfrak{p}}} = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \left(\prod_{\substack{\mathfrak{q}\subset\mathcal{O}_L \\ \mathfrak{q}|\mathfrak{p}}} \mathfrak{q}^{e_\mathfrak{p}} \right)^{\frac{a_\mathfrak{p}}{e_\mathfrak{p}}} = \prod_{\mathfrak{p}\subset\mathcal{O}_K} (\mathfrak{p}\mathcal{O}_L)^{\frac{a_\mathfrak{p}}{e_\mathfrak{p}}}.$$

To finish the proof, we note that the ideal $I := \prod_{\mathfrak{p}\subset\mathcal{O}_K} \mathfrak{p}^{a_\mathfrak{p}/e_\mathfrak{p}}$ satisfies $I\mathcal{O}_L = t\mathcal{O}_L$. As a consequence, we conclude that $\alpha(I) = t\mathcal{O}_{\overline{K}}$, as desired. ■

5.4 The Period of a Number Field

As we have seen in Section 4.5, the final part of the BSD conjecture can be written down as a volume calculation of $E(\mathbb{A}_K)$ with respect to the Tamagawa measure. The same can be done for the remaining part of the analytic class number formula, i.e., the term

$$\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}, \tag{5.9}$$

where r_1 is the number of real embeddings of the number field K and r_2 the number of pairwise non-conjugate complex embeddings. The BSD conjecture consists of mathematical invariants concerning the group of rational points $E(K)$. Until now, we have obtained similarities with the analytic class number formula based on the group of units $\mathcal{O}_K^\times$. We will now write (5.9) as the volume of the set $\mathcal{O}_{\mathbb{A}_K}^\times$, which is defined below.

Definition 5.4.1. The subsets $\mathcal{O}_{\mathbb{A}_K}$ and $\mathcal{O}_{\mathbb{A}_K}^\times$ of $\mathbb{A}_K$ and $\mathbb{I}_K$ respectively, are defined by

$$\begin{aligned} \mathcal{O}_{\mathbb{A}_K} &:= \prod_{v\in M_K} \mathcal{O}_{K_v}, \\ \mathcal{O}_{\mathbb{A}_K}^\times &:= \prod_{v\in M_K} \mathcal{O}_{K_v}^\times, \end{aligned}$$

where

$$\begin{aligned} \mathcal{O}_{K_v} &:= \{x \in K_v \mid |x|_v \le 1\}, \\ \mathcal{O}_{K_v}^\times &:= \{x \in K_v^\times \mid |x|_v = 1\}. \end{aligned}$$

We now use the same construction as for the Tamagawa measure in Section 2.4 to obtain a unique Haar measure on the subgroup $\mathcal{O}_{\mathbb{A}_K}^\times$ of $\mathbb{I}_K$. For this, we recall the associated differential $\omega = \mathrm{d}x/x$ of the multiplicative group $\mathbb{G}_m$ defined over K from Example 2.4.2. Similarly as before, we let $\mathrm{d}x_v$ denote the normalized Haar measure on K_v. The local measures ω_v on $K_v^\times$ induced by ω are given by $\omega_v = \mathrm{d}x_v/|x_v|_v$.

For the finite places $v \in M_K^0$, we let $\tilde{\mu}_v$ be the restriction to $\mathcal{O}_{K_v}^\times$ of the local Haar measure ω_v on $K_v^\times$. Notice that with respect to this measure, we have

$$\tilde{\mu}_v(\mathcal{O}_{K_v}^\times) = \int_{\mathcal{O}_{K_v}^\times} \frac{\mathrm{d}x_v}{|x_v|_v} = \int_{\mathcal{O}_{K_v}^\times} \mathrm{d}x_v = \int_{\mathcal{O}_{K_v}} \mathrm{d}x_v - \int_{\pi_v\mathcal{O}_{K_v}} \mathrm{d}x_v = 1 - \frac{1}{q_v} = \zeta_{K,v}(q_v^{-1}),$$

where π_v is a uniformizer for the unique prime ideal $\mathfrak{p}_v$ corresponding to v of index q_v.

A unique Haar measure on $\mathcal{O}_{K_v}^{\times}$ for the infinite places $v \in M_K^{\infty}$ can be obtained by demanding compatibility with the normalized Haar measure on $K_v^{\times}$ and the Lebesgue measure on $\mathbb{R}$ via the exact sequence

$$1 \longrightarrow \mathcal{O}_{K_v}^{\times} \longrightarrow K_v^{\times} \xrightarrow{\log|\cdot|_v} \mathbb{R} \longrightarrow 0, \tag{5.10}$$

as in the sense of Theorem A.1.2. We distinguish between the real case and the complex case.

1. For real places v, we consider the following exact sequence,

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{R}^{\times} \xrightarrow{\log|\cdot|_v} \mathbb{R} \longrightarrow 0.$$

Now let $f \in L^1(\mathbb{R}^{\times})$, then

$$\begin{aligned}\int_{\mathbb{R}^{\times}} \frac{f(x_v)}{|x_v|_v} \mathrm{d}x_v &= \int_{\mathbb{R}_{>0}} \frac{f(x_v)}{x_v} \mathrm{d}x_v - \int_{\mathbb{R}_{<0}} \frac{f(x_v)}{x_v} \mathrm{d}x_v \\ &= \int_{\mathbb{R}_{>0}} \frac{f(x_v) + f(-x_v)}{x_v} \mathrm{d}x_v = \int_{\mathbb{R}} f(e^u) + f(-e^u) \mathrm{d}u \\ &= \int_{\mathbb{R}} \sum_{n \in \{\pm 1\}} f(ne^u) \mathrm{d}u,\end{aligned}$$

where $\mathrm{d}u$ denotes the Lebesgue measure on $\mathbb{R}$. We therefore see that the unique measure on $\mathcal{O}_{K_v}^{\times} = \{\pm 1\}$ that is compatible with the given exact sequence is the usual counting measure.

2. For complex places v, we consider the exact sequence

$$1 \longrightarrow S^1 \longrightarrow \mathbb{C}^{\times} \xrightarrow{\log|\cdot|_v} \mathbb{R} \longrightarrow 0.$$

Let $f \in L^1(\mathbb{C}^{\times})$, then

$$\begin{aligned}\int_{\mathbb{C}^{\times}} \frac{f(x_v)}{|x_v|_v} \mathrm{d}x_v &= \int_{\mathbb{C}^{\times}} \frac{f(x_v)}{|x_v|^2} \mathrm{d}x_v = 2 \int_{(\mathbb{R} \times \mathbb{R}) \setminus \{(0,0)\}} \frac{f(x+iy)}{x^2+y^2} \mathrm{d}x \mathrm{d}y \\ &= 2 \int_{\mathbb{R}_{>0}} \int_0^{2\pi} \frac{f(re^{i\theta})}{r^2} r \mathrm{d}\theta \mathrm{d}r = \int_{\mathbb{R}_{>0}} \int_0^{2\pi} \frac{2f(re^{i\theta})}{r} \mathrm{d}\theta \mathrm{d}r \\ &= \int_{\mathbb{R}} \int_0^{2\pi} f(e^{u/2} e^{i\theta}) \mathrm{d}\theta \mathrm{d}u.\end{aligned}$$

From this we deduce that the standard Haar measure on S^1, as described in Example A.0.5, is the unique Haar measure that is compatible with the considered exact sequence.

Let $\tilde{\mu}_v$ denote the obtained unique Haar measure on $\mathcal{O}_{K_v}^{\times}$ for $v \in M_K^{\infty}$, which is compatible with the exact sequence (5.10). Recall that we wanted to construct a Haar measure on $\mathcal{O}_{\mathbb{A}_K^{\times}}$. For this, we define the set of convergence factors $\{\lambda_v\}_{v \in M_K}$ for $\mathcal{O}_{\mathbb{A}_K^{\times}}$, as

$$\lambda_v := \begin{cases} \tilde{\mu}_v(\mathcal{O}_{K_v}^{\times}) = \zeta_{K,v}(q_v^{-1}) & \text{if } v \in M_K^0 \\ 1 & \text{if } v \in M_K^{\infty}, \end{cases} \tag{5.11}$$

to ensure that

$$\prod_{v \in M_K^0} \lambda_v^{-1} \tilde{\mu}_v(\mathcal{O}_{K_v}^{\times})$$

absolutely converges. We now obtain a unique Haar measure on $\mathcal{O}_{\mathbb{A}_K}^{\times}$ by applying the same construction as for the Tamagawa measure from Section 2.4.

Definition 5.4.2. The *Tamagawa measure* τ (relative to λ_v) on $\mathcal{O}_{\mathbb{A}_K}^\times$ is given by the product measure

$$\tau := |\Delta_K|^{-1/2} \prod_{v \in M_K} \lambda_v^{-1} \tilde{\mu}_v,$$

where the λ_v are defined as (5.11).

Remark 5.4.3. The reason why we cannot just restrict the Tamagawa measure on $\mathbb{I}_K$ to $\mathcal{O}_{\mathbb{A}_K}^\times$ is that this restriction turns out to be the zero measure.

Proposition 5.4.4. *The volume of $\mathcal{O}_{\mathbb{A}_K}^\times$ with respect to the Tamagawa measure τ is given by*

$$\tau(\mathcal{O}_{\mathbb{A}_K}^\times) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}.$$

Proof.

$$\begin{aligned}
\mathrm{vol}(\mathcal{O}_{\mathbb{A}_K}^\times) = \tau(\mathcal{O}_{\mathbb{A}_K}^\times) &= |\Delta_K|^{-1/2} \prod_{v \in M_K} \lambda_v^{-1} \tilde{\mu}_v(\mathcal{O}_{K_v}^\times) = |\Delta_K|^{-1/2} \prod_{v \in M_K^\infty} \tilde{\mu}_v(\mathcal{O}_{K_v}^\times) \\
&= |\Delta_K|^{-1/2} \prod_{\substack{v \in M_K^\infty \\ \text{real}}} \int_{\{\pm 1\}} \mathrm{d}\tilde{\mu}_v(x_v) \cdot \prod_{\substack{v \in M_K^\infty \\ \text{complex}}} \int_{S^1} \mathrm{d}\tilde{\mu}_v(x_v) \\
&= \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}.
\end{aligned}$$

■

Definition 5.4.5. Let K be a number field. Then the *period* of K is given by

$$P(K) := \tau(\mathcal{O}_{\mathbb{A}_K}^\times) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}.$$

Remark 5.4.6. To summarize the analogy with the period of an elliptic curve, we observe that both periods are volume calculations with respect to similarly constructed Tamagawa measures. The chosen set of convergence factors for the Tamagawa measures both consist of the local factors of the corresponding series. More precisely, we have for $v \in M_K^0$ that

$$\lambda_v = \begin{cases} L_v(E/K, q_v^{-1}) & \text{for an elliptic curve } E/K \\ \zeta_{K,v}(q_v^{-1}) & \text{for a number field } K, \end{cases}$$

see Remark 4.5.6.

Remark 5.4.7. We have chosen to write the final part of the analytic class number formula as the volume of $\mathcal{O}_{\mathbb{A}_K}^\times$ with respect to the canonically induced Tamagawa measure. It is also possible to write it as a volume of $\mathcal{O}_{\mathbb{A}_K}$ with respect to the Tamagawa measure on $\mathbb{A}_K$. For this we take the invariant differential 1-form $\omega = \mathrm{d}x$ from Example 2.4.2. The induced local Haar measures for $v \in M_K$ are given by $\omega_v = \mathrm{d}x_v$, where $\mathrm{d}x_v$ is the normalized Haar measure on K_v from Definition 2.4.3. As set of convergence factors $\{\lambda_v\}_{v \in M_K}$, we take $\lambda_v = 1$ for all $v \in M_K$. In this way we obtain the Tamagawa measure $\tilde{\tau}$ on $\mathbb{A}_K$ relative to the λ_v.

Proposition 5.4.8. *The volume of $\mathcal{O}_{\mathbb{A}_K}$ with respect to the Tamagawa measure $\tilde{\tau}$ is given by,*

$$\tilde{\tau}(\mathcal{O}_{\mathbb{A}_K}) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}.$$

Proof.

$$\begin{aligned}
\operatorname{vol}(\mathcal{O}_{\mathbb{A}_K}) &= \tilde{\tau}(\mathcal{O}_{\mathbb{A}_K}) = \int_{\mathcal{O}_{\mathbb{A}_K}} \mathrm{d}\tilde{\tau}(x) = |\Delta_K|^{-1/2} \cdot \prod_{v \in M_K} \int_{\mathcal{O}_{K_v}} \mathrm{d}x_v \\
&= |\Delta_K|^{-1/2} \cdot \prod_{\substack{v \in M_K \\ \text{real}}} \int_{[-1,1]} \mathrm{d}x_v \cdot \prod_{\substack{v \in M_K \\ \text{complex}}} \int_{B_{\leq 1}(0)} \mathrm{d}x_v \cdot \prod_{\substack{v \in M_K \\ \text{finite}}} \int_{\mathcal{O}_{K_v}} \mathrm{d}x_v \\
&= \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta_K|}}.
\end{aligned}$$

■

Discussion

This part is meant to give an overview of the obtained similarities between the formulas

$$\lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^{r_E}} = P(E/K) \cdot \frac{\#(\text{Ш}(E/K)) \cdot R_{E/K}}{\#(E_{\text{tors}}(K))^2},$$
$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot R_K}{\sqrt{|\Delta_K|} \cdot \#(\mathcal{O}_K^\times)_{\text{tors}}}.$$

Both of the considered functions are infinite series defined on a part of the complex plane, where $L(E/K,s)$ has a conjectural analytic continuation to $\mathbb{C}$ and $\zeta_K(s)$ has a proven analytic continuation to $\mathbb{C}\backslash\{1\}$. Despite the fact that the first formula represents the first non-zero Taylor coefficient of $L(E/K,s)$ at $s=1$ and the second a residue formula for $\zeta_K(s)$ at $s=1$, the expressions show a remarkable amount of similarities.

The first and most obvious one is the resemblance between $E_{\text{tors}}(K)$ and $(\mathcal{O}_K^\times)_{\text{tors}}$. This can be seen from the analogy between the Mordell-Weil theorem and Dirichlet's unit theorem. The theorems state that $E(K)$ and $\mathcal{O}_K^\times$ are finitely generated, and additionally that the torsion groups $E_{\text{tors}}(K)$ and $(\mathcal{O}_K^\times)_{\text{tors}}$ are finite.

A second canonical analogy can be found between the regulators $R_{E/K}$ and R_K. The first is the square of the volume of a fundamental domain for $E(K)/E_{\text{tors}}(K)$ with respect to the Néron-Tate pairing $\langle\cdot,\cdot\rangle$ on E/K. This pairing defines a certain bilinear form for which

$$R_{E/K} = |\det(\langle P_i, P_j\rangle)_{i,j=1}^{r}|,$$

where $P_1, ..., P_r \in E(K)$ is a basis for $E(K)/E_{\text{tors}}(K)$.

The regulator R_K is defined as the volume of a full lattice obtained by embedding $\mathcal{O}_K^\times$ into a (r_1+r_2-1)-dimensional hyperplane H of $\mathbb{R}^{r_1+r_2}$. This lattice is spanned by the vectors

$$v_i := (\log|\sigma_1(\eta_i)|^{n_{\sigma_1}}, ..., \log|\sigma_{r_1+r_2-1}(\eta_i)|^{n_{\sigma_{r_1+r_2-1}}}),$$

where $\eta_1, ..., \eta_{r_1+r_2-1}$ is a basis for $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)_{\text{tors}}$. To obtain a better analogy with $R_{E/K}$, we constructed a bilinear form on $\mathcal{O}_K^\times$ such that

$$R_K = |\det(\langle \eta_i, \eta_j\rangle)_{i,j=1}^{r_1+r_2-1}|^{1/2}.$$

A third less obvious analogy can be obtained between $\text{Ш}(E/K)$ and $\text{Cl}(\mathcal{O}_K)$. As discussed briefly in Section 5.3, they both measure the failure of a certain property. The first group being trivial is equivalent to the property that finding rational points everywhere locally is equivalent to finding global points for every homogeneous space. On the other hand, the class group is trivial if and only if the ring of integers $\mathcal{O}_K$ is a principal ideal domain. This is moreover equivalent to saying that every ideal in $\mathcal{O}_K$ that is everywhere locally principal in $\mathcal{O}_{K,v}$, is also principal inside $\mathcal{O}_K$. Thus both groups measure the failure of a certain property. The Tate-Shafarevich group $\text{Ш}(E/K)$ is defined as

$$\text{Ш}(E/K) := \bigcap_{v\in M_K} \ker\left(H^1(\text{Gal}(\overline{K}/K), E(\overline{K})) \longrightarrow H^1(\text{Gal}(\overline{K_v}/K_v), E(\overline{K_v}))\right).$$

As we have seen, there is a cohomological analogue of the Tate-Shafarevich group for number fields. Namely,

$$Ш(K) := \bigcap_{v \in M_K} \ker \left(H^1(\mathrm{Gal}(\overline{K}/K), \mathcal{O}_{\overline{K}}^{\times}) \longrightarrow H^1(\mathrm{Gal}(\overline{K_v}/K_v), \mathcal{O}_{\overline{K_v}}^{\times}) \right).$$

At first sight, this group seems totally different than the class group of K. Nevertheless, it is possible to obtain an isomorphism between $Ш(K)$ and $\mathrm{Cl}(\mathcal{O}_K)$.

At last, we considered the terms $P(E/K)$ and $2^{r_1}(2\pi)^{r_2}|\Delta_K|^{-1/2}$. The period $P(E/K)$ can be written as the volume of $E(\mathbb{A}_K)$ with respect to the Tamagawa measure. Applying the same constructions used for this measure, we are able to obtain a Haar measure on $\mathcal{O}_{\mathbb{A}_K}^{\times}$. We therefore call the obtained measure a Tamagawa measure. The final part of the analytic class number formula can now be written as the volume of $\mathcal{O}_{\mathbb{A}_K}^{\times}$ with respect to the constructed Tamagawa measure. To obtain a similarity in terminology, we call this volume the period $P(K)$ of the considered number field K.

The acquired analogies together with the corresponding sections, are listed below.

Sections	BSD		ACNF	Sections
4.3	$E_{\mathrm{tors}}(K)$	$\longleftrightarrow$	$(\mathcal{O}_K^{\times})_{\mathrm{tors}}$	1.6
4.3	$R_{E/K}$	$\longleftrightarrow$	R_K	5.2
4.4	$Ш(E/K)$	$\longleftrightarrow$	$\mathrm{Cl}(\mathcal{O}_K) \cong Ш(K)$	5.3
4.5	$P(E/K) = \mathrm{vol}(E(\mathbb{A}_K))$	$\longleftrightarrow$	$P(K) = \mathrm{vol}(\mathbb{A}_K) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{\lvert\Delta_K\rvert}}$	5.4

Combining all the obtained results described above, and recalling the template

$$\frac{\text{Period} \ \times \ |\text{Tate-Shafarevich group}| \ \times \ \text{Regulator}}{|\text{torsion group}|^{\text{power}}}$$

mentioned in the introduction, we find that

$$\lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^{r_E}} = P(E/K) \cdot \frac{\#(Ш(E/K)) \cdot R_{E/K}}{\#(E_{\mathrm{tors}}(K))^2},$$
$$\lim_{s\to 1}(s-1)\zeta_K(s) = P(K) \cdot \frac{\#(Ш(K)) \cdot R_K}{\#(\mathcal{O}_K^{\times})_{\mathrm{tors}}}.$$

Current Status of the BSD Conjecture

We end this thesis with a short list of the known results regarding the BSD conjecture. The results are paraphrased from the mentioned sources, in which the references for the original proven statements are given. Most of the stated results about elliptic curves $E/\mathbb{Q}$ originally had the additional assumption that the considered curve was modular. However, in 2001 it was proven that every elliptic curve E defined over $\mathbb{Q}$ is modular, meaning that we can omit the assumption from the earlier obtained results.

1. (cf. [Sil09]) For elliptic curves over $\mathbb{Q}$ it has been proven that the L-series has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating its values at s and $2-s$. Combining the work of Deuring ([Deu53], [Deu55], [Deu56], and [Deu57]) and Weil ([Wei52]), this has first been proven for elliptic curves with complex mulitplication, i.e., curves for which $\mathrm{End}(E)$ is larger than $\mathbb{Z}$. Eichler ([Eic54]) and Shimura ([Shi58], [Shi94]) later proved that it is also true for elliptic curves over $\mathbb{Q}$ that are modular. By the so-called Modularity theorem ([BCDT01], [TW95], [Wil95]), due to Wiles, Taylor, Breuil,

Conrad and Diamond (2001), it turned out that every elliptic curve over $\mathbb{Q}$ is modular. In other words, the modularity assumption can be omitted from the result of Eichler and Shimura.

2. (cf. [Groty]) Isogenous elliptic curves over a global field have the same L-series. In other words, the BSD conjecture can only be true if

$$P(E/K) \cdot \frac{\#(\text{Ш}(E/K)) \cdot R_{E/K}}{\#(E_{\text{tors}}(K))^2} \tag{5.12}$$

is isogeny invariant. Despite the fact that none of the individual terms in the product need to be the same for isogenous curves, Cassels [Cas65] was able to prove that (5.12) is in fact isogeny invariant under the assumption that Ш(E/K) is finite. More on this, together with a generalized version for abelian varieties, can be found in [Mil06].

3. (cf. [CW77]) Let E be an elliptic curve with complex multiplication by the ring of integers of an imaginary quadratic field K with class number one, that is moreover defined over K or $\mathbb{Q}$. If the L-series of E does not vanish at $s = 1$, then the rank r_E of the elliptic curve is equal to zero. This result was obtained by J.Coates and A.Wiles in 1977.

4. (cf. [Rub87]) In 1987, K. Rubin proved that the Tate-Shafarevich group is finite for elliptic curves defined over an imaginary quadratic number field K, with complex multiplication by K, for which $L(E/K, 1) \neq 0$. Moreover, if E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication such that $\text{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$, then the Mordell-Weil rank r_E is equal to $\text{ord}_{s=1} L(E/\mathbb{Q}, s)$.

5. (cf. [Groty]) The Mordell-Weil rank of elliptic curves over $\mathbb{Q}$ for which the analytic rank $\text{ord}_{s=1}L(E/\mathbb{Q}, s)$ is at most 1, equals the analytic rank. Moreover, the Tate-Shafarevich group Ш$(E/\mathbb{Q})$ is finite. This result is obtained due to Kolyvagin [Kol89] in the late 1980s by using the Gross-Zagier theorem [GZ86].

6. (cf. [Groty]) The BSD conjecture can also be formulated for elliptic curves over function fields. In this case, the BSD conjecture holds if and only if the Tate-Shafarevich group Ш(E/K) is finite. A more generalized version of this statement, together with a proof, can be found in [KT03].

Appendix A

Haar Measures

In this appendix we discuss the basic properties used in this thesis about Haar measures. A more complete description can be found in [Coh13], [DE14], and [RV99]. These measures are known as invariant regular Borel measures. To make this more precise, we start by giving some definitions. For this we will assume X to be a locally compact Hausdorff space. As soon as we turn to the Haar measures, X will be replaced by a locally compact Hausdorff topological group G. Recall that a *measure* is a function $\mu : \mathcal{A} \to [0, \infty]$ on a σ-algebra $\mathcal{A}$ that satisfies $\mu(\emptyset) = 0$, and that is countably additive, i.e.,

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu(A_i)$$

for all infinite sequences $\{A_i\}$ of disjoint sets $A_i \in \mathcal{A}$. The σ-algebra we will be interested in is the Borel σ-algebra of a locally compact Hausdorff topological space X.

Definition A.0.1. The *Borel σ-algebra* of X, denoted as $\mathcal{B}(X)$, is the σ-algebra generated by the open subsets of X. With *Borel subsets* of X, we mean the sets belonging to $\mathcal{B}(X)$.

Together with this comes the notion of a *Borel measure* on X, which is a measure whose domain is $\mathcal{B}(X)$. Some of these measures possess a certain approximation property.

Definition A.0.2. Let $\mathcal{A}$ be a σ-algebra on X containing $\mathcal{B}(X)$. Then a measure μ on $\mathcal{A}$ is called *regular*, if

(i) Each compact subset K of X has finite measure, i.e.

$$\mu(K) < \infty.$$

(ii) The measure of each set A in $\mathcal{A}$ can be approximated from below, more precisely

$$\mu(A) = \inf\{\mu(U) : A \subset U \text{ and } U \text{ is open}\}.$$

(iii) Each open subset U of X satisfies

$$\mu(U) = \sup\{\mu(K) : K \subset U \text{ and } K \text{ is compact}\}.$$

Definition A.0.3. Let G be a locally compact Hausdorff group, and μ a non-zero regular Borel measure on G. Then μ is called a *(left) Haar measure* if it is invariant under (left) translations, i.e.

$$\mu(xA) = \mu(A)$$

for each $x \in G$ and $A \in \mathcal{B}(G)$.

Remark A.0.4. One can also define the right Haar measure, but since we will be working with abelian groups they coincide. It therefore makes sense to just call it a Haar measure.

Example A.0.5. (cf. [Coh13, Ex.9.2.1])

1. The Lebesgue measure on the Euclidean space $\mathbb{R}^n$ is a Haar measure.

2. The counting measure on a group G endowed with the discrete topology defines a Haar measure.

3. The naturally induced Lebesgue measure on the unit circle S^1 viewed as subspace of $\mathbb{C}$ is a Haar measure. More precisely, consider the isomorphism $f : [0, 2\pi) \to S^1$ that maps θ to $e^{i\theta}$. Then the Lebesgue measure $\lambda \circ f^{-1}$ is a Haar measure on S^1, where λ is the Lebesgue measure on $\mathbb{R}$ restricted to the Borel subsets of $[0, 2\pi)$.

The following theorem yields us information about the existence and the uniqueness of the Haar measures.

Theorem A.0.6. (cf. [Coh13, Thm.9.2.2 and 9.2.6]) *Let G be a locally compact Hausdorff group, then there exists a left Haar measure on G. Moreover, if μ and ν are left Haar measures on G, then there exists $c \in \mathbb{R}_{>0}$ such that $\nu = c\mu$.*

A.1 Quotient Space

From now on we in addition assume G to be an abelian group, and H a closed subgroup of G. In this case, the quotient space G/H is again locally compact and Hausdorff. In other words, it admits a Haar measure. Let $C_c(G)$ denote the space of continuous functions from G to $\mathbb{C}$ of compact support, i.e., the closure of $\{g \in G : f(g) \neq 0\}$ is compact. Moreover, endow G and H with Haar measures μ and λ, respectively. For every $f \in C_c(G)$, we obtain a well-defined function

$$f^H : G/H \to \mathbb{C},\ [g] \mapsto \int_H f(gh) \mathrm{d}\lambda(h).$$

Lemma A.1.1. (cf. [DE14, Lem.1.5.1]) *We have $f^H \in C_c(G/H)$, and the map $C_c(G) \ni f \mapsto f^H \in C_c(G/H)$ is surjective.*

Theorem A.1.2. (cf. [DE14, Thm.1.5.3]) *Let G be an abelian locally compact Hausdorff group, and H a closed subgroup. Given Haar measures on G and H, say μ and λ respectively. Then there exists a unique Haar measure ν on G/H, such that for every $f \in C_c(G)$ one has the quotient integral formula*

$$\int_G f(g)\mathrm{d}\mu(g) = \int_{G/H} f^H([g])\mathrm{d}\nu([g]) = \int_{G/H} \left(\int_H f(gh)\mathrm{d}\lambda(h) \right) \mathrm{d}\nu([g]).$$

This formula is valid for all $f \in L^1(G)$.

A.2 Restricted Direct Product

The following theorem gives a unique way to put a Haar measure on the restricted direct product of locally compact Hausdorff groups.

Theorem A.2.1. (cf. [RV99, Prop.5.5]) *Let $G = \prod_{v \in I}(G_v, H_v)$ be the restricted direct product of locally compact groups G_v with respect to the family of open compact subgroups $H_v \subset G_v$ for almost all $v \in I$. Let I_∞ denote the finite index set consisting of all $v \in I$ for which we do not take an open compact subgroup H_v. Let μ_v be the Haar measure on G_v such that*

$$\int_{H_v} \mathrm{d}\mu_v = 1$$

for almost all $v \notin I_\infty$. Then there is a unique Haar measure $\mathrm{d}\mu$ *on G such that for each finite subset S of I containing I_∞, the restriction μ_S of μ to*

$$G_S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v$$

is precisely the product measure. We therefore write

$$\mu = \prod_{v \in I} \mu_v.$$

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AS21] Athanasios Angelakis and Peter Stevenhagen. Adelic point groups of elliptic curves. *arXiv preprint arXiv:1703.08427v2*, January 8 2021. Paper available at https://arxiv.org/pdf/1703.08427v2.pdf (accessed online: May 2022).

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over Q: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, May 15 2001. Online available at https://www.ams.org/journals/jams/2001-14-04/S0894-0347-01-00370-8/S0894-0347-01-00370-8.pdf (accessed online: July 2022).

[Ber10] Massimo Bertolini. Report on the Birch and Swinnerton-Dyer conjecture. *Milan journal of mathematics*, 78(1):153–178, 2010. Available at https://link.springer.com/content/pdf/10.1007/s00032-010-0123-6.pdf (online accessed: June 2022).

[Bom00] Enrico Bombieri. Problems of the millennium: The Riemann hypothesis. *Clay Mathematics Institute*, 2000. Available at https://www.claymath.org/sites/default/files/official_problem_description.pdf (accessed online: June 2022).

[Cas65] J.W.S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *Journal für die reine und angewandte Mathematik*, 217:180–199, 1965. Online available at http://eudml.org/doc/150666 (accessed online: June: 2022).

[CF67] J. W. S. Cassels and A. Frohlich. *Algebraic Number Theory.* Academic Press Inc. (London), 1967.

[Claa] Pete L. Clark. Algebraic Number Theory II: Valuations, Local Fields and Adeles. *Notes available at http://alpha.math.uga.edu/~pete/8410FULL.pdf (accessed online: November, 2021).*

[Clab] Pete L. Clark. Supplementary Lecture Notes on Elliptic Curves. Notes available at http://alpha.math.uga.edu/~pete/8430Elliptic_Curves.pdf (accessed online: May, 2022).

[Coh13] Donald L. Cohn. *Measure Theory: Second Edition.* Birkhäuser Advanced Texts Basler Lehrbücher. Birkhäuser Basel, Springer New York Heidelberg Dordrecht London, 2013.

[Con] Keith Conrad. Ostrowski's Theorem for $F(T)$. Notes are available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskiF(T).pdf (accessed online: December, 2021).

[Con10] Keith Conrad. Ostrowski for Number Fields. *Expository papers on Algebraic Number Theory.*, 2010. Online available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf (accessed online: March, 2022).

[Con20] Keith Conrad. Infinite Galois Theory (Draft,CTNT 2020). 2020. Notes are available at https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf (accessed online: January 2022).

[Cox12] David A. Cox. *Galois Theory, Second Edition.* John Wiley & Sons, Inc., Publication, 2012.

[CW77] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, 39(3):223–251, 1977. Online available at https://link.springer.com/content/pdf/10.1007/BF01402975.pdf (accessed online: June 2022).

[DE14] Anton Deitmar and Siegfried Echterhoff. *Principles of Harmonic Analysis.* Springer International Publishing Switzerland, second edition, 2014.

[Deu53] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt.*, pages 85–94, 1953.

[Deu55] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. II. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, pages 13–42, 1955.

[Deu56] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. III. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, pages 37–76, 1956.

[Deu57] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. IV. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, pages 55–80, 1957.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Wiley & Sons, Inc., third edition, 2004.

[Eic54] Martin Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Archiv der Mathematik*, 5(4):355–366, 1954. Online available at https://link.springer.com/article/10.1007/BF01898377 (accessed online: July 2022).

[Groty] Benedict H. Gross. Lectures on the Conjecture of Birch and Swinnerton-Dyer. 2009 American Mathematical Society. Notes are available at https://people.math.harvard.edu/~gross/preprints/lectures-pcmi.pdf (accessed online: May, 2022).

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Inventiones mathematicae*, 84:225–320, 1986. Online available at https://link.springer.com/content/pdf/10.1007/BF01388809.pdf (accessed online: June 2022).

[Kai16] Sameer Kailasa. On The Tate-Shafarevich Group Of a Number Field. 2016. Paper is available at https://math.uchicago.edu/~may/REU2016/REUPapers/Kailasa.pdf (accessed online: january, 2022).

[Kna07] Anthony W. Knapp. *Advanced algebra.* Cornerstones. Birkhäuser Boston, Inc., Boston, MA, 2007. Along with a companion volume *Basic Algebra.*

[Kol89] Viktor Alexandrovich Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Mathematics of the USSR-Izvestiya*, 32(3):523–541, 1989.

[KT03] Kazuya Kato and Fabien Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Inventiones mathematicae*, 153(3):537–592, 2003. Online available at https://link.springer.com/content/pdf/10.1007/s00222-003-0299-2.pdf (accessed online: June 2022).

[Lan94] Serge Lang. *Algebraic Number Theory.* Graduate Texts in Mathematics 110. Springer, second edition, 1994.

[Lan02] Serge Lang. *Algebra.* Graduate Texts in Mathematics 211. Springer-Verlag New York, third edition, 2002.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org/EllipticCurve/Q/1728/n/4 (accessed online: 27 June 2022), 2022.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems.* BookSurge, LLC, second edition, 2006.

[Mil21] J.S. Milne. Fields and Galois Theory. *version 5.00*, June 2021. Notes are available at https://www.jmilne.org/math/CourseNotes/FT.pdf (accessed online: January 2022).

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag Berlin Heidelberg, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rom07] Steven Roman. *Advanced Linear Algebra.* Graduate Texts in Mathematics. Springer, third edition, 2007.

[RR94] Vladimir Platonov, Andrei Rapinchuk, and Rachel Rowen. *Algebraic Groups and Number Theory.* Pure and applied mathematics 139. Academic Press Inc., 1994. Translated by Rachel Rowen.

[Rub87] Karl Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Inventiones mathematicae*, 89(3):527–559, 1987. Online available at https://link.springer.com/content/pdf/10.1007/BF01388984.pdf (accessed online: June 2022).

[RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier Analysis on Number Fields.* Graduate Texts in Mathematics 186. Springer-Verlag New York, first edition, 1999.

[Shi58] Goro Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *Journal of the Mathematical Society of Japan*, 10(1):1–28, 1958.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan.* Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Letures, 1.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106. Springer-Verlag New York, second edition, 2009.

[Ste13] Ian Stewart. *Visions of Infinity : The Great Mathematical Problems.* Basic Books, 2013.

[Ste20] P. Stevenhagen. Number Rings. November 14, 2020. Notes are available at https://websites.math.leidenuniv.nl/algebra/ant.pdf (accessed online: December 2021).

[Sut15] Andrew Sutherland. *18.785 Number Theory I Lecture 3.* September 17 2015. Notes are available at https://math.mit.edu/classes/18.785/2015fa/LectureNotes3.pdf (accessed online: December 2021).

[Sut17] Andrew Sutherland. *18.785 Number Theory I Lecture 25.* December 4 2017. Notes are available at https://math.mit.edu/classes/18.785/2017fa/LectureNotes25.pdf (accessed online: December 2021).

[SW08] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields.* Springer-Verlag Berlin Heidelberg, second edition, 2008.

[SZ03] Susanne Schmitt and Horst G. Zimmer. *Elliptic Curves - a Computational Approach.* De Gruyter Studies in Mathematics. Walter de Gruyter, 2003.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics*, 141(3):553–572, 1995. Online available at https://www.jstor.org/stable/2118560 (accessed online: July 2022).

[Wei52] André Weil. Jacobi sums as “Grossencharaktere”. *Transactions of the American Mathematical Society*, 73(3):487–495, 1952. Online available at https://www.ams.org/journals/tran/1952-073-03/S0002-9947-1952-0051263-0/S0002-9947-1952-0051263-0.pdf (accessed online: July 2022).

[Wei82] Andre Weil. *Adeles and Algebraic Groups*, volume 23 of *Progress in Mathematics.* Birkhäuser Boston, 1982.

[Wil] Andrew Wiles. The Birch and Swinnerton-Dyer Conjecture. *Clay Mathematics Institute.* Online available at https://www.claymath.org/sites/default/files/birchswin.pdf (accessed online: June 2022).

[Wil95] Andrew Wiles. Modular Elliptic Curves and Fermat’s Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995. Online available at https://www.jstor.org/stable/2118559 (accessed online: July 2022).

[Wil04] Stephen Willard. *General Topology.* Dover Publications, reprint edition, 2004. This is a reprint of the original version published by Addison-Wesley Publishing Company, Inc. in 1970.

Index

G-module, 49
L-series of an elliptic curve E/K, 59
S-adele ring, 33
S-ideles, 34
$\mathfrak{p}$-adic valuation, 17

absolute Galois group of a field, 45
absolute height function, 63
absolute logarithmic height function, 63
absolute norm, 22
absolute value, 1
adele ring, 33
algebraic closure of a field, 40
algebraic field extension, 40
algebraically closed field, 40
ambiguous principal ideals, 79
Analytic Class Number Formula, ix, 75
Archimedean absolute value, 2

bilinear form, 15
Borel σ-algebra, 91
Borel measure, 91
BSD conjecture, viii, 60

canonical height (Néron-Tate) pairing, 65
characteristic polynomial, 19
class number, 22
cohomology groups of G-module, 50
cohomology groups of discrete G-modules, 53
completion of a field with respect to a place, 11
completion of a normed field, 11
compositum of fields, 46
crossed homomorphism (1-cocycle), 50
cusp, 56

Dedekind domain, 16
Dedekind zeta function of a number field K, 75
diagonal embedding of K into $\mathbb{A}_K$, 34
direct limit, 27
directed set, 27
directed system of topological spaces, 27
Dirichlet's unit theorem, 22
discrete G-module, 52
discrete valuation, 8
discrete valuation ring, 9
discriminant of a number field, 21
discriminant of field extension, 19
discriminant of Weierstrass equation, 55

elliptic curve, 56
equivalent absolute values, 3
equivalent valuations, 7
extension of ideal, 23

field norm, 19
field trace, 19
final topology, 26
finite Galois extension, 45
finite places on a field, 4
fractional ideal, 16
fundamental domain, 14
fundamental theorem for infinite Galois theory, 49
fundamental theorem of finite Galois theory, 45

Galois group, 44
Galois group as inverse limit, 47
global field, 1

Haar measure, 91
Haar measure on restricted direct product, 93
height on elliptic curve relative to f, 63
height on projective space $\mathbb{P}^N(K)$, 62
Hilbert's Theorem 90, 79
homomorphism of normed fields, 11

ideal class group, 22
ideal division, 15
ideal quotient, 16

idele group, 34
idele-norm, 35
ideles of norm 1, 35
infinite Galois extension, 45
infinite places on a field, 4
integral basis, 20
integral basis of $\mathcal{O}_K$, 20
integral ideal, 16
integral quotient formula, 92
invariant differential of elliptic curve, 55
invertible fractional ideal, 16
isomorphism between class group and Tate-Shafarevich group of a number field, 82
isomorphism between restricted direct product and direct limit, 29

Krull topology, 48

lattice, 14
local ζ_K-factor, 75
local L-factor, 59

measure, 91
minimal Weierstrass equation, 57
Mordell-Weil Theorem, 65

Néron-Tate height on an elliptic curve E/K, 63
node, 56
non-Archimedean absolute value, 2
normal field extension, 42
normalized absolute values, 18, 77
normalized Haar measure on K_v, 36
normed field, 4
number field, 1
number ring, 15

Ostrowski's Theorem, 4
Ostrowski's Theorem for number fields, 18

perfect field, 44
period of elliptic curve E/K, 71
Picard group, 16
place on a field K, 3
positive definite bilinear form, 15
prime ideal factorization, 17
primes of one-dimensional domain, 17
principal crossed homomorphism (1-coboundary), 50
principal fractional ideal, 16
Product Formula, 19
profinite group, 52

quadratic form, 64

ramification index, 23, 24
rank of elliptic curve E/K, 65
reduced elliptic curve, 57
reduction type of elliptic curve over K_v, 57
reduction type of elliptic curve over a number field, 58
regular measure, 91
regulator of a number field, 77
regulator of elliptic curve E/K, 65
residue field, 7
restricted direct product, 28
restriction of ideal, 23
Riemann hypothesis, 74
ring of integers of a number field, 17

separable closed field, 44
separable closure of a field, 44
separable field extension, 44
separable polynomial, 44
set of Archimedean places, 4, 57
set of convergence factors, 39
set of non-Archimedean places, 4, 57
splitting field, 41
symmetric bilinear form, 15

Tamagawa measure, 39
Tamagawa numbers of elliptic curve, 59
Tate-Shafarevich group of a number field, 79
Tate-Shafarevich group of elliptic curve E/K, 67
The Strong Approximation Theorem, 18
torsion subgroup of an elliptic curve, 57

ultrametric inequality, 2
uniformizer, 9

valuation, 7
valuation ring, 7
value group, 7

Weierstrass equation, 55