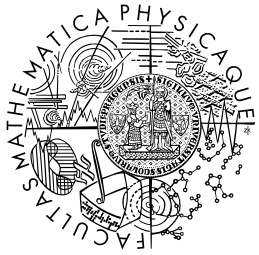


FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Bára Tížková

Adèles and class fields

Department of Algebra

Supervisor of the master thesis: doc. Mgr. Vítězslav Kala, Ph.D.

Study programme: Mathematical Structures

Study branch: Mathematical Structures

Prague 2023

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

First of all, I would like to thank my supervisor Vítězslav Kala for his guidance, dedicated time and patience with answering all of my questions. I want to extend my sincere thanks to Daniel Beďatš for his willingness to discuss anything anytime, proofreading and useful tips. I am also grateful to Alexander Slávik for his comments and topology related insights. Lastly, many thanks go to my parents for their support throughout my studies.

Title: Adèles and class fields

Author: Bára Tížková

Department: Department of Algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The first aim of the thesis is to study the ring of adèles and the group of idèles and work out their topology in detail. We explain the relation between the restricted product topology and other topologies which might seem natural on these objects. Further, we study their compactness properties. The second aim of the thesis is to summarize the main results of class field theory, both in the language of ideals and of idèles, and to provide examples illustrating new notions and concepts. Roughly speaking, class field theory describes all abelian extensions of a number field in terms of some "inner arithmetic" of the field. First, we demonstrate how the description works on two particular types of abelian extensions and then generalize the notions for any abelian extension. In order to present the general class field theory in a clear and straightforward manner, we unify the content of various sources and literature. The classical approach via ideals is more natural; however, some inconveniences arise when we have to take into account which primes ramify in the extension. This is handled by the idèlic approach described in the last chapter.

Keywords: adèles, idèles, class field, Artin reciprocity

Contents

Introduction

The goal of class field theory, which we will often abbreviate as CFT, is to describe all abelian extensions of a fixed number field together with their Galois groups.

It all started when Kronecker was reading Abel's work and noticed that certain values arising from elliptic functions generate abelian extensions of imaginary quadratic fields. He wondered if all abelian extensions can be obtained in this way and so, as the first one, asked the key question of CFT.

However, we can also view CFT as a discipline connecting many themes of algebraic number theory. It connects notions such as density of primes, decomposition of primes in field extensions, reciprocity laws... For example, the Gauss' quadratic reciprocity enables us to describe the sets of prime numbers which split completely in quadratic extensions and, as we will see, this set says a lot about abelian extensions.

We can gain some insight into what CFT deals with by looking at two particular types of abelian extensions. The first one, abelian extensions of $\mathbb{Q}$, can be handled easily due to the Kronecker-Weber Theorem saying that each abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field. Hence, by applying Fundamental Theorem of Galois Theory, we obtain an order reversing bijection between abelian extensions contained in $\mathbb{Q}(\zeta_m)$ and the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ which is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$. This means, we are able to classify Galois groups of abelian extensions in terms of the "inner arithmetic" of $\mathbb{Q}$ by which we mean the family of groups $(\mathbb{Z}/m\mathbb{Z})^\times$ in this situation.

We are lucky to have a similar theorem in the case of unramified abelian extensions. This theorem yields existence of a maximal unramified abelian extension for a number field K, called the Hilbert class field. Since the Galois group of the Hilbert class field is isomorphic to the ideal class group Cl_K, we obtain an order reversing bijection between unramified abelian extensions and the subgroups of Cl_K.

Since we also care about extensions other than the unramified ones, we need to find a way to generalize this. For a fixed number field we prescribe a set of ideals which we allow to ramify and then consider all the abelian extensions which are unramified outside this set. For each such prescribed set we obtain a generalization of Hilbert class field and a generalization of the ideal class group. We canonically realize Galois groups of abelian extensions via Artin map in the main theorem of class field theory called the Artin Reciprocity Law.

It is somewhat natural to work with ideals when describing abelian extensions; however, the case distinction according to the set of possibly ramified primes is rather unconvenient. We would like to have a more universal description of abelian extensions, to describe all of them at the same time. This led Chevalley to reformulate the main results of CFT in terms of objects called idèles.

Group of idèles is a group of invertible elements of another object called the ring of adèles defined as a restricted product of all completions of a fixed number field. Considering restricted product instead of the product of topological spaces yields nice compactness properties. We are going to investigate some of them even if we do not see immediate application in this thesis.

Chapter 1 provides a brief summary of notions from algebraic number theory and commutative algebra which we will need.

In **Chapter 2** we take a closer look at the ring of adèles and the group of idèles. In Section 2.1 we carefully work out the topology on adèles and point out the difference between the restricted product topology and the product topology. In Section 2.2 we present claims from [1] leading to the group isomorphism between adèles and a certain product of adèles over $\mathbb{Q}$. Another goal is to get familiar with a tensor product point of view on adèles. What follows in Section 2.3 is showing local compactness of adèles over $\mathbb{Q}$ and then using the results from Section 2.2 to prove local compactness for adèles over a general number field. In Section 2.4 we introduce the group of idèles and investigate its topology. Although it is a subset of adèles, it turns out that taking the subspace topology is not the right choice.

In **Chapter 3** we present the main CFT results formulated in terms of ideals. We do not follow only one source; we always choose a way of introducing new concepts most suitable to our exploration. The first two sections 3.1 and 3.2 serve to get the initial insight into CFT via dealing with two particular types of abelian extensions. In 3.1 we investigate abelian extensions of $\mathbb{Q}$, in 3.2 we investigate only those abelian extensions of a number field which are unramified. In both sections, we introduce (their respective versions of) the Artin map, the main hero of CFT. In Section 3.3 we generalize notions introduced in 3.1 and 3.2. We define the ray class group and a general Artin map and check that these are indeed generalizations of notions defined in 3.1 and 3.2. We state Artin Reciprocity Law and Existence Theorem.

The aim of Section 3.4 is to introduce the conductor and use it to specify primes which split completely in abelian extensions. First, we choose the approach of [2] to define the conductor of a congruence divisor class groups and then relate it to the conductor of a field extension. On the way to do so we work out some properties concerning congruence subgroups and their equivalence.

We include a table comparing the two particular cases of CFT with the general one at the end of the chapter.

In **Chapter 4** we use the strategy of [3] to define the Artin map on idèles and state the idèlic version of the Artin Reciprocity Law.

Personal contribution

The thesis has a summarizing character and the goal is mainly to enrich the theory with examples, motivate new concepts and write down some of the proofs in more detail and with explanations that hopefully makes reading them easier. Namely, I give more detailed proofs of lemmas 1.24, 2.9, 2.30 compared to the literature where I found them and provide examples 3.16, 3.30 and 4.7 which are of more extensive character. Another challenge was to unify and summarize the content of various sources in Chapter 3, including the notation.

Finally, let me enumerate the statements whose proofs I worked out independently. They are not very deep or innovative; however, they helped me to become familiar with the topic: Lemma 1.41, Lemma 2.2, Lemma 2.5, Lemma 2.6, Lemma 2.7, Lemma 2.8, Lemma 2.18, Lemma 2.26, Lemma 3.23, Lemma 3.32, Proposition 3.35, Lemma 4.3, Lemma 4.11.

1. Preliminaries

Most of the material in this introductory chapter was taken from [4].

1.1 Number fields, Galois extensions

We will always work with number fields, that is finite extensions of $\mathbb{Q}$. Alternatively we can view number fields as $\mathbb{Q}(\alpha)$ for α algebraic. Recall that an element of K is integral if it is a root of some monic polynomial in $\mathbb{Z}[x]$. The integral elements of K form a ring which we denote by $\mathcal{O}_K$.

Example 1.1. For $K = \mathbb{Q}(\sqrt{D})$, with $D \neq 0, 1$ square-free we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Definition 1.2. Let L/K be a field extension. An element $\alpha \in L$ is *separable* if its minimal polynomial over K is separable, that is, all of its roots are distinct in the algebraic closure of K. A field extension L/K is *separable* if all elements of L are separable.

Theorem 1.3. *Each finite separable extension is simple.*

Because we work with number fields only and all polynomials over number fields are separable, the definition of a Galois extension becomes simpler than the general one.

Definition 1.4. An extension of number fields L/K is said to be *Galois* if L is a splitting field of some polynomial in $K[x]$. We call the extension L/K *abelian* if it is Galois and $\mathrm{Gal}(L/K)$ is abelian.

Abelian extensions are the only extensions which class field theory cares about. Therefore, all the advantages stemming from restricting ourselves to Galois extensions will be available for us.

Theorem 1.5. *For a Galois extension L/K it holds that $[L : K] = |\mathrm{Gal}(L/K)|$.*

A key feature Galois extensions possess is the one-to-one correspondence with certain subgroups. Namely, there is an order reversing bijection

$$\begin{aligned} \{M \text{ field} \mid K \leq M \leq L\} &\longleftrightarrow \{\text{subgroups } H < \mathrm{Gal}(L/K)\} \\ M &\longmapsto \mathrm{Gal}(L/M) \\ \mathrm{Fix}(L, H) &\longmapsfrom H \end{aligned}$$

where $\mathrm{Fix}(L, H)$ is the subfield of L which is fixed by the subgroup H. We will refer to this correspondence as *Galois correspondence*.

We will come across many notions of norm maps on the way through this work. We start with the simplest one. The notion of trace will be needed later in the definition of discriminant.

Definition 1.6. Let L/K be a Galois extension and $\alpha \in L$. Then we define the *norm* of α as

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$$

and the *trace* of α as

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Remark. The maps $\mathrm{N}_{L/K} : L^\times \to K^\times$ and $\mathrm{Tr}_{L/K} : L(+) \to K(+)$ are group homomorphisms, where $K^\times$ denotes the multiplicative group of invertible elements of K and $K(+)$ denotes the additive group of K, similarly for L. Also, for a Galois extension $K \subset L \subset M$ we have that $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$ and $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

Next, the set of integral elements is closed under the trace. The same holds for norms; however, we will need only the trace version.

Lemma 1.7. *Let L/K be a Galois extension. Then $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$ for each $\alpha \in \mathcal{O}_L$.*

1.2 Ideal class group

Let K be a number field and $\mathcal{O}_K$ its ring of integers in the whole section.

Definition 1.8. A *fractional ideal* is a nonzero $\mathcal{O}_K$-module $I \subset K$ such that there exists a nonzero element $r \in \mathcal{O}_K$ such that $rI \subset \mathcal{O}_K$.

Remark. Equivalently, we can define a fractional ideal to be a subset $\{0\} \neq I \subset K$ such that for some nonzero $r \in \mathcal{O}_K$ the set rI forms an ideal of $\mathcal{O}_K$.

Definition 1.9. A *principal fractional ideal* is a set of the form $a\mathcal{O}_K$ where $a \in K^\times$. We denote it by (a).

Remark. By "ideal" or "ideal of K" we always mean an integral ideal, that is an ideal in the ring $\mathcal{O}_K$.

Since all ideals are fractional ideals, the notion of fractional ideal generalizes the notion of ideal. We also generalize the ideal multiplication by defining the product of two fractional ideals I, J as

$$I \cdot J = \{i_1 j_1 + i_2 j_2 + \cdots + i_m j_m \mid i_k \in I, j_k \in J \text{ for all } 1 \leq k \leq m,\ m \in \mathbb{N}\}.$$

It can be shown that all fractional ideals of a number field K form a group (see [4, Chapter 3, Thm. 3.20]) which we will denote by I_K. Hence, the principal fractional ideals form a subgroup of I_K which we will denote by P_K. The group I_K is abelian and by taking the quotient by P_K we get an object of great importance.

Definition 1.10. The *ideal class group* Cl_K is the quotient $Cl_K = I_K/P_K$. The size of Cl_K is called the *class number* of K and denoted by h_K.

Lemma 1.11. *Cl_K is trivial if and only if $\mathcal{O}_K$ is a unique factorization domain.*

Roughly speaking, the size of the ideal class group measures the extent to which the prime factorization in $\mathcal{O}_K$ is unique. Moreover, it is always finite, which we obtain as a by-product of certain compactness properties of idèles in Section 2.4.

1.3 Factorization in field extensions

Let K be a number field. Unlike elements of $\mathcal{O}_K$, which do not have to factor uniquely as products of prime elements, each ideal of $\mathcal{O}_K$ can always be written uniquely as a product of prime ideals. The proof can be found for example in [5].

Let L/K be an extension of number fields and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Since each ideal of $\mathcal{O}_L$ factors uniquely, we have a unique expression

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}$$

where $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are prime ideals of $\mathcal{O}_L$ and $e_i \geq 1$ for each i. We say that these prime ideals *divide* or *lie over* $\mathfrak{p}$ and denote it by $\mathfrak{P}_i|\mathfrak{p}$.

Next, we call

- $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ the *ramification index*, and
- $f(\mathfrak{P}_i/\mathfrak{p}) = f_i \coloneqq [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ the *inertia degree* of $\mathfrak{p}$ in $\mathfrak{P}$.

What comes next is sometimes called the "efg Theorem":

Theorem 1.12. *Let L/K be an extension of number fields with $[L : K] = n$. Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ be all the prime ideals in $\mathcal{O}_L$ dividing a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with corresponding ramification indices $e_1, e_2, \ldots, e_g$ and inertia degrees $f_1, f_2, \ldots, f_g$. Then*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Moreover, if L/K is a Galois extension then $\boldsymbol{e} = e_1 = e_2 = \cdots = e_g$, $\boldsymbol{f} = f_1 = f_2 = \cdots = f_g$, and thus $\boldsymbol{ef}g = n$.

In case when L/K is Galois we write

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdots \mathfrak{P}_g)^e$$

and call the unique e, f from Theorem 1.12 the ramification index and the inertia degree of $\mathfrak{p}$, respectively.

Since we will work with Galois extensions only, we formulate the following definition for this setting.

Definition 1.13. Let L/K be Galois extension and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. Then we say that

$$\mathfrak{p} = \begin{cases} \textit{(completely) splits} & \text{if } g = n, e = 1, \\ \textit{ramifies} & \text{if } e \geq 2, \\ \text{is } \textit{inert} & \text{if } g = 1, e = 1. \end{cases}$$

When describing abelian extensions, we will also focus on the set of primes which split completely. Why? Such primes actually fully characterize the Galois extension.

Notation. Let $\mathrm{Spl}(L/K)$ denote the set of prime ideals in $\mathcal{O}_K$ which split completely in $\mathcal{O}_L$.

Theorem 1.14 (Bauer)**.** *Let L_1, L_2 be two Galois extensions of a number field K. Then $L_1 = L_2$ if and only if $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$.*

Let us mention one more feature of Galois extensions which we will need later in Section 3.2 when defining the Artin symbol. It is the transitive action of the Galois group on prime ideals dividing a fixed prime ideal of the base field.

Proposition 1.15. *Let L/K be a Galois extension and $\mathfrak{P}_1, \mathfrak{P}_2$ prime ideals of $\mathcal{O}_L$ dividing prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.*

Ramification in quadratic number fields

Example 1.16. Let $K = \mathbb{Q}, L = \mathbb{Q}(i)$, in which case we have $\mathcal{O}_K = \mathbb{Z}, \mathcal{O}_L = \mathbb{Z}[i]$. Then 13 splits, $(13) = (2+3i)(2-3i)$, the prime 3 is inert, that is, (3) stays a prime ideal in $\mathbb{Z}[i]$, and 2 ramifies, $(2) = (1+i)^2$.

We present a more general description of prime decomposition in quadratic fields. We do so to demonstrate the connection between splitting of primes and the law of quadratic reciprocity which can be derived from the Artin reciprocity law (the main theorem of class field theory, to be analyzed in Section 3.3). Recall that the *Legendre symbol* for $a \in \mathbb{Z}$ and an odd prime $p \in \mathbb{Z}$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \ \ \& \ \ a \text{ is a square mod } p, \\ -1 & \text{if } p \nmid a \ \ \& \ \ a \text{ is not a square mod } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The following lemma describing the splitting behaviour of primes in quadratic extensions in terms of Legendre symbols yields a tool to find the set of primes which split completely. For simplicity we consider only odd primes, for 2 we would have to add some additional conditions modulo 8.

Lemma 1.17. *Let $p \in \mathbb{Z}$ be an odd prime and let $D \neq 0, 1$ be a square-free integer. Then*

- *p splits in $\mathbb{Q}(\sqrt{D})$ $\iff$ $\left(\frac{D}{p}\right) = 1$,*
- *p ramifies in $\mathbb{Q}(\sqrt{D})$ $\iff$ $\left(\frac{D}{p}\right) = 0$,*
- *p is inert in $\mathbb{Q}(\sqrt{D})$ $\iff$ $\left(\frac{D}{p}\right) = -1$.*

Example 1.18. Suppose that an odd prime $p \in \mathbb{Z}$ splits in $K = \mathbb{Q}(\sqrt{2})$. We will show that then $\left(\frac{2}{p}\right) = 1$.

Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ is a principal ideal domain, we can assume that $p = \alpha \cdot \beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ are non-units. Since the norm

$$\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2$$

is multiplicative and $\mathrm{N}_{K/\mathbb{Q}}(p) = p^2$, necessarily $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}(\beta) = \pm p$. This means that there are $x, y \in \mathbb{Z}$ such that $x^2 - 2y^2 = \pm p$, which implies the existence of $x, y \in \mathbb{Z}$ such that $x^2 - 2y^2 \equiv 0 \pmod{p}$. Note that $p \nmid y$ (otherwise p would divide x and the left-hand side would be divisible by p^2). This means there are $x, y \in \mathbb{Z}$ such that $\frac{x^2}{y^2} \equiv 2 \pmod{p}$, meaning $\left(\frac{2}{p}\right) = 1$.

Recall that (one of the equivalent versions of) the quadratic reciprocity law says that for odd primes p, q and an integer a such that $p \nmid a$ we have

$$p \equiv \pm q \pmod{4a} \implies \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

We can deduce that the factorization of an odd prime in $\mathbb{Q}(\sqrt{D})$ depends only on the residue modulo $4D$.

Example 1.19. We will find the set of (integer) primes which split completely in $\mathbb{Q}(\sqrt{2})$. We know that 2 ramifies in $\mathbb{Q}(\sqrt{2})$ and, by Lemma 1.17, no further primes ramify. Since $2 \equiv 4^2 \pmod 7$, and hence $\left(\frac{2}{7}\right) = 1$, for all primes p congruent to ± 7 modulo $4 \cdot 2 = 8$ we have $\left(\frac{2}{p}\right) = 1$ by quadratic reciprocity. On the other hand, 2 is not a square modulo 3, that is $\left(\frac{2}{3}\right) = -1$ and so for all primes p congruent to ± 3 modulo 8 we have $\left(\frac{2}{p}\right) = -1$ by quadratic reciprocity. Therefore, Lemma 1.17 yields that

$$p \text{ splits completely in } \mathbb{Q}(\sqrt{2}) \iff p \equiv 1, 7 \pmod 8.$$

1.4 Ideal norm

We already mentioned that all fractional ideals form an abelian group I_K. Moreover, I_K is the free abelian group generated by nonzero prime ideals of K, again by [4, Chapter 3, Thm. 3.20]. Due to this fact, the norm map $\mathcal{N}_{L/K} : I_L \to I_K$ is determined by images of prime ideals.

Definition 1.20. Let L/K be an extension of number fields, $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. We define the *norm* of $\mathfrak{P}$ as

$$\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$$

where $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is the inertia degree of $\mathfrak{p}$ in $\mathfrak{P}$. We extend the norm map from the set of prime ideals to the whole I_L multiplicatively.

The ideal norm $\mathcal{N}_{L/K} : I_L \to I_K$ is defined so that it is compatible with the norm $\mathrm{N}_{L/K} : L^\times \to K^\times$. That is, the following diagram commutes:

$$\begin{array}{ccc} L^\times & \xrightarrow{a \mapsto (a)} & I_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ K^\times & \xrightarrow{b \mapsto (b)} & I_K \end{array}$$

1.5 Discriminants and differents

Describing the set $\mathrm{Spl}(L/K)$ for L/K can be considered as one of the goals of class field theory. Characterizing the set of primes which ramify was known already before the main goals of class field theory were stated. The ramification is captured by discriminants of a field extension. We distinguish between absolute and relative discriminant when defining it but their purpose in terms of describing the ramified primes is the same.

Definition 1.21. An *integral basis* for a number field K is a tuple $(a_1, a_2, \ldots, a_n)$ of elements of K such that it is a basis for K as a vector space over $\mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$.

The *(absolute) discriminant* of K is defined as

$$\Delta_K = \Delta_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = \det((\mathrm{Tr}(a_i a_j))_{n\times n})$$

where $(a_1, a_2, \ldots, a_n)$ is an integral basis for K.

Let us skip the details such as the existence of an integral basis for K or the well-definedness of the discriminant. An interested reader can find them in [4, Chapter 2].

Proposition 1.22. [4, Thm. 3.35] *Let K be a number field. Then*

$$p \in \mathbb{Z} \text{ ramifies in } K \iff p \text{ divides } \Delta_K.$$

To define the relative discriminant for a field extension L/K we need to introduce an ideal called the (relative) different. And to define the different we need the following two lemmas, both taken from [2, Chapter 2, Section 8]. We include the proof of Lemma 1.24 in order to provide a more detailed explanation than the book does.

Lemma 1.23. *Let L/K be an extension of number fields. Then every K-linear map $L \to K$ is of the form $\alpha \mapsto \mathrm{Tr}_{L/K}(\alpha\beta)$ for some $\beta \in L$.*

Lemma 1.24. *Let L/K be an extension of number fields and*

$$S = \{\beta \in L \mid \mathrm{Tr}_{L/K}(\alpha\beta) \in \mathcal{O}_K \text{ for each } \alpha \in \mathcal{O}_L\}.$$

Then the set $S^{-1} = \{a \in L \mid aS \subset \mathcal{O}_L\}$ forms an ideal in $\mathcal{O}_L$.

Proof. First, observe that S is an $\mathcal{O}_L$-module. Indeed, $S(+)$ forms a group by linearity of trace map and for each $\beta \in S, r \in \mathcal{O}_L, \alpha \in \mathcal{O}_L$ we have $\mathrm{Tr}_{L/K}(\alpha(r\beta)) = \mathrm{Tr}_{L/K}((\alpha r)\beta) \in \mathcal{O}_K$.

Second, let us show that $S \subset \Delta_L^{-1}\mathcal{O}_L$. We know there is an integral basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ for $\mathcal{O}_L$; that means, it is a basis for L as a vector space over $\mathbb{Q}$ and $\mathcal{O}_L = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Let $\beta \in S$. Then $\mathrm{Tr}_{L/K}(\mathcal{O}_L\beta) \subset \mathcal{O}_K$ which implies that $\mathrm{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L\beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{L/K}(\mathcal{O}_L\beta)) \subset \mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subset \mathbb{Z}$. Thus,

$$S \subset R = \{\beta \in L \mid \mathrm{Tr}_{L/\mathbb{Q}}(\mathcal{O}_L\beta) \subset \mathbb{Z}\}.$$

From viewing $\mathrm{Tr}_{L/\mathbb{Q}}$ as a bilinear form on the vector space L over $\mathbb{Q}$

$$\mathrm{Tr}_{L/\mathbb{Q}} : (\alpha, \beta) \mapsto \mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta)$$

we obtain the dual basis $\beta_1, \beta_2, \ldots, \beta_n$ with respect to this form i.e. a basis of L over $\mathbb{Q}$ satisfying $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\beta_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta function. Moreover, $R = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$. Indeed, for $\beta = \sum_{i=1}^n q_i\beta_i$ with $q_i \in \mathbb{Q}$ we have

$$\beta \in R \iff \mathrm{Tr}_{L/\mathbb{Q}}(\alpha_j(\sum_{i=1}^{n} q_i\beta_i)) \in \mathbb{Z} \text{ for all } j\text{'s}$$

$$\iff \sum_{i=1}^{n} q_i \mathrm{Tr}_{L/\mathbb{Q}}(\alpha_j \beta_i) \in \mathbb{Z} \text{ for all } j\text{'s}$$
$$\iff q_j \in \mathbb{Z} \text{ for all } j\text{'s}.$$

Now, it suffices to show that for each i we have $\beta_i \in \Delta_L^{-1}\mathcal{O}_L$, because then we obtain the desired inclusion

$$S \subset R = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z} \subset \Delta_L^{-1}\mathcal{O}_L.$$

We can write $\beta_i = \sum_j \alpha_j q_{ji}$ for some $q_{ji} \in \mathbb{Q}$. Then

$$(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))(q_{ij}) = I_n \tag{1.1}$$

since on the coordinate (i,j) of this product we have

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i(\alpha_1 q_{1j} + \alpha_2 q_{2j} + \cdots + \alpha_n q_{nj})) = \mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\beta_j) = \delta_{ij}.$$

Using the formula

$$A\,\mathrm{adj}(A) = \det(A)I$$

for a square matrix A and its adjugate matrix $\mathrm{adj}(A)$, we can rewrite (1.1) as

$$\begin{aligned}(q_{ij}) &= (\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))^{-1}\\ (q_{ij}) &= \frac{\mathrm{adj}(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))}{\det(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))}\\ \Delta_L(q_{ij}) &= \mathrm{adj}(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j)).\end{aligned}$$

Since $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$ for all i,j, we obtain $\Delta_L q_{ij} \in \mathbb{Z}$ for each ij meaning that $\beta_i = \sum_j \alpha_j q_{ji} \in \sum_j \alpha_j \Delta_L^{-1}\mathbb{Z} \subset \Delta_L^{-1}\mathcal{O}_L$ as we wanted.

Now, because $S \subset \Delta_L^{-1}\mathcal{O}_L$ and it is an $\mathcal{O}_L$-module, it must be a fractional ideal in L. Moreover, since $\mathcal{O}_L \subset S$, for its inverse fractional ideal

$$S^{-1} = \{a \in L \mid aS \subset \mathcal{O}_L\}$$

we have the inclusion $S^{-1} \subset \mathcal{O}_L$. This is true because for each $a \in S^{-1}$ we particularly have $a\mathcal{O}_L \subset \mathcal{O}_L$ implying that $a \in \mathcal{O}_L$. Thus, S^{-1} is, as a fractional ideal contained in $\mathcal{O}_L$, an integral ideal. □

Definition 1.25. Let L/K be an extension of number fields and

$$S = \{\beta \in L \mid \mathrm{Tr}_{L/K}(\alpha\beta) \in \mathcal{O}_K \text{ for each } \alpha \in \mathcal{O}_L\}.$$

The *different* of L/K is then defined as the ideal $\delta_{L/K} = S^{-1}$.

Proposition 1.26. [2, Section 8, Thm. 21] *Let $\mathfrak{p}, \mathfrak{P}$ be prime ideals of K, L respectively and let $e > 0$ be the largest integer such that $\mathfrak{P}^e \mid \mathfrak{p}$. Then $\mathfrak{P}^{e-1} \mid \delta_{L/K}$.*

We can view the different as an ideal identifying the "bad" primes and measuring how "bad" they are. The reason why we call the ramified primes "bad" will be clearer in Section 3.3. The Artin map, the key map realizing the desired description of abelian extensions, can be defined only for ideals not divisible by any ramified prime ideals.

Definition 1.27. The *relative discriminant* $\Delta_{L/K}$ of L/K is the norm of the different of L/K, i.e.

$$\Delta_{L/K} = \mathcal{N}_{L/K}(\delta_{L/K}).$$

Proposition 1.28. [6, Chapter III, Cor. 2.10] *For an extension of number fields $K < L < M$ it holds that*

$$\Delta_{M/K} = \mathcal{N}_{L/K}(\Delta_{M/L})\Delta_{L/K}^{[M:L]}.$$

Proposition 1.29. [4, Thm. 3.35] *Let L/K be an extension of number fields and let $\mathfrak{p}$ be a prime ideal of K. Then*

$$\mathfrak{p} \textit{ ramifies in } L \iff \mathfrak{p} \textit{ divides } \Delta_{L/K}.$$

We see that by taking the norm of different we lose some information - we are only able to identify those primes which ramify. The different itself contains also information about the exact power in which a prime $\mathfrak{P}$ from $\mathcal{O}_L$ divides a prime $\mathfrak{p}$ from $\mathcal{O}_L$.

1.6 Absolute values

Since we will need the notion of completion of a number field to define the objects called adèles and work with them, let us spend some time by defining this notion thoroughly. On the way to do so, we mention other useful tools, such as Product Formula or Weak Approximation Theorem.

Definition 1.30. An *absolute value* on a field K is a function $K \to \mathbb{R}, x \mapsto |x|$ satisfying

(a) $|x| > 0$ for all $x \neq 0$, $|0| = 0$,

(b) $|xy| = |x||y|$,

(c) $|x + y| \leq |x| + |y|$.

If moreover $|x+y| \leq \max\{x, y\}$, we call the absolute value *non-archimedean.* We call it *archimedean* otherwise.

An absolute value $|\cdot|$ is said to be *discrete* if $|K^\times|$ is a discrete subset of $\mathbb{R}^+$ with respect to the Euclidean metric.

Example 1.31. Let K be a number field.

- For an embedding $\sigma : K \hookrightarrow \mathbb{C}$ we can define an absolute value as $|a| = |\sigma(a)|$, where the latter is the usual absolute value on $\mathbb{C}$. This absolute value is archimedean.

- For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ we define the $\mathfrak{p}$-*adic absolute value* of $a \in K^\times$ as

  $$|a|_\mathfrak{p} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p} a}$$

  where $\mathrm{ord}_\mathfrak{p} a$ denotes the exponent of $\mathfrak{p}$ in the factorization of $a\mathcal{O}_K$. We define $\mathrm{ord}_\mathfrak{p} 0 = \infty$, and so we obtain $|0|_\mathfrak{p} = 0$. This absolute value is non-archimedean.

It can be shown that for a discrete non-archimedean absolute value $|\cdot|$ on a number field K the set $A = \{\alpha \in K \mid |\alpha| \leq 1\}$ forms a ring and it has a unique maximal ideal $M = \{\alpha \in K \mid |\alpha| < 1\}$ which is generated by some element $\pi \in K$ with the largest absolute value less than 1. We call this element a *uniformizer*.

Example 1.32. Consider a p-adic absolute value on $\mathbb{Q}$ where p is a prime number. Then $A = \mathbb{Z}$ and the unique maximal ideal M is generated by p because the integers z satisfying $|z|_p < 1$ are precisely those divisible by p. Hence, p is the uniformizer.

From now on, we will turn our attention on the equivalence classes of absolute values rather than on absolute values themselves. Let us define the equivalence first.

Because an absolute value $|\cdot|$ on K also defines a metric d on K via putting $d(a, b) = |a - b|$ we obtain an induced topology on K from this metric. The basic open sets are open balls $B(a, r) = \{x \in K \mid |x - a| < r\}$ with $a \in K$ and $r > 0$.

We will say that an absolute value is *trivial* if $|a| = 1$ for each $a \neq 0$.

Proposition 1.33. *Let $|\cdot|_1, |\cdot|_2$ be absolute values on a field K where $|\cdot|_1$ is non-trivial. Then the following statements are equivalent:*

(a) $|\cdot|_1, |\cdot|_2$ *define the same topology,*

(b) $|a|_1 < 1$ *implies* $|a|_2 < 1$,

(c) $|\cdot|_2 = |\cdot|_1^c$ *for some* $c > 0$.

Definition 1.34. We call the absolute values $|\cdot|_1, |\cdot|_2$ on a field K *equivalent* if the conditions from Proposition 1.33 are satisfied. An equivalence class of a non-trivial absolute values on a number field K is called a *prime* or a *place* of K.

The following theorem gives a classification of all places of a given number field.

Theorem 1.35. *Let K be a number field. Then there is exactly one place*

- *for each prime ideal* $\mathfrak{p}$,
- *for each embedding* $\sigma : K \hookrightarrow \mathbb{R}$,
- *for each conjugate pair of complex embeddings* $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$.

We distinguish between *finite* (or *non-archimedean*) *primes* which correspond to a prime ideal of $\mathcal{O}_K$ and *infinite* (or *archimedean*) *primes* which correspond to a real or complex embedding of K. In each class of equivalence we can choose a normalized absolute value:

- for a prime ideal $\mathfrak{p}$, choose $|a|_\mathfrak{p} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p} a}$,
- for an embedding $\sigma : K \hookrightarrow \mathbb{R}$, choose $|a|_\sigma = |\sigma(a)|$ where the latter is the Euclidean absolute value on $\mathbb{R}$,
- for a pair of complex embeddings $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$, choose $|a|_\sigma = |\sigma(a)|^2$ (this is in fact not an absolute value but it is a convenient choice for the Product Formula which is stated below).

A prime of a number field is usually denoted by v and the normalized absolute value from its equivalence class by $|\cdot|_v$.

Theorem 1.36 (Product Formula)**.** *Let α be a nonzero element of a number field K. Then*

$$\prod_v |a|_v = 1$$

where the product is taken over all normalized places v.

Notation. Let L/K be number fields and $|\cdot|_v, |\cdot|_w$ absolute values of K, L, respectively. If $|\cdot|_v$ is the restriction of $|\cdot|_w$ to K, we say that w *lies over* v and denote this fact by $w \mid v$.

Theorem 1.37 (Weak Approximation Theorem)**.** *Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be nontrivial mutually inequivalent absolute values of a field K and let $a_1, a_2, \ldots, a_n \in K$. Then for each $\epsilon > 0$ there exists $\alpha \in K$ such that $|\alpha - a_i|_i < \epsilon$ for every $1 \leq i \leq n$.*

1.7 Completions

Let us have a field K with a nontrivial absolute value $|\cdot|$. We call K *complete* if each Cauchy sequence has a limit in K. Recall that a sequence $(a_n)_{n=1}^{\infty}$ in K is Cauchy if for each $\epsilon > 0$ there is $N \in \mathbb{N}$ such that for all $m, n > N$ it holds that $|a_m - a_n| < \epsilon$.

Example 1.38. Let $K = \mathbb{Q}$. Then the sequence $1, 11, 111, 1111, \ldots$ is Cauchy with respect to the 2-adic topology since $|a_m - a_n|_2 = 2^{-n}$ for $m > n$.

Notation. Let $(K, |\cdot|_K)$ denote a field K which is equipped with an absolute value $|\cdot|_K$.

Theorem 1.39. [4, Thm. 7.23] *Let K be a field and $|\cdot|_K$ an absolute value on K. Then there is a complete field $(\hat{K}, |\cdot|_{\hat{K}})$ and a homomorphism $\varphi : K \to \hat{K}$ preserving $|\cdot|_K$,i.e. $|\varphi(a)|_{\hat{K}} = |a|_K$ for every $a \in K$. Moreover, φ has the following universal property:*

Every homomorphism $K \to L$ for some complete field $(L, |\cdot|_L)$ preserving $|\cdot|_K$ extends to a unique homomorphism $\hat{K} \to L$ preserving $|\cdot|_{\hat{K}}$.

$$\begin{array}{ccc} (K, |\cdot|_K) & \longrightarrow & (L, |\cdot|_L) \\ \big\downarrow{\scriptstyle \varphi} & \nearrow_{\exists!} & \\ (\hat{K}, |\cdot|_{\hat{K}}) & & \end{array}$$

Definition 1.40. The complete field $\hat{K}$ from Theorem 1.39 is unique up to a unique isomorphism. We call it the *completion* of a field K with respect to an absolute value $|\cdot|$.

Let us remark that we get the same completions for equivalent absolute values. Therefore, it makes sense to talk about the completion with respect to a place/prime.

Notation. For a field K and a place v we denote the completion of K with respect to the absolute value $|\cdot|_v$ by K_v. If the place v corresponds to a prime ideal $\mathfrak{p}$, we may also write $K_\mathfrak{p}$ for the completion.

How does this complete field K_v look? It can be shown that it consists of all equivalence classes of Cauchy sequences in K. We say that two Cauchy sequences $(r_n), (s_n)$ are equivalent if and only if $\lim_{n\to\infty}|r_n - s_n|_v = 0$ and denote the equivalence class containing (r_n) by $[(r_n)]_{\sim_v}$. It can be further shown that the operations are just

$$\begin{aligned}[(r_n)]_{\sim_v} \pm [(s_n)]_{\sim_v} &= [(r_n \pm s_n)]_{\sim_v},\\ [(r_n)]_{\sim_v} \cdot [(s_n)]_{\sim_v} &= [(r_n \cdot s_n)]_{\sim_v},\\ [(r_n)]_{\sim_v}^{-1} &= [(r_n^{-1})]_{\sim_v}\end{aligned}$$

and that v is extended from K to K_v via putting $|[(r_n)]_{\sim_v}|_v = \lim_{n\to\infty}|r_n|_v$ where $(r_n), (s_n)$ are Cauchy sequences in K. Note that $|K_\mathfrak{p}|_\mathfrak{p} = |K|_\mathfrak{p}$ from the discreteness of the $\mathfrak{p}$-adic absolute value.

Notation. When speaking about an element of K_v we will write (r_n) instead of $[(r_n)]_{\sim_v}$.

We have a natural inclusion $K \hookrightarrow K_v$ mapping $r \in K$ to the sequence $(r, r, r \dots)$. We will identify K with its image in K_v.

Let us get more familiar with viewing the elements of the completion as sequences by proving the following easy lemma.

Lemma 1.41. *$\mathbb{Q}$ is a dense subset of $\mathbb{Q}_v$ for each place v.*

Proof. If v is infinite, it corresponds to the Euclidean absolute value on $\mathbb{R}$. It corresponds to a p-adic absolute value for a prime p otherwise.

For the Euclidean absolute value the completion of $\mathbb{Q}$ is $\mathbb{R}$ and the density is a basic fact from mathematical analysis.

For a p-adic absolute value we will show that all elements of $\mathbb{Q}_p$ are limit points of elements of $\mathbb{Q}$. Take a sequence $(q_1, q_2, q_3, \dots) \in \mathbb{Q}_p$. This means, $q_1, q_2, q_3, \dots$ is a Cauchy sequence of elements in $\mathbb{Q}$. Then it is a limit of the sequence

$$(q_1, q_1, q_1, \dots), (q_2, q_2, q_2, \dots), (q_3, q_3, q_3, \dots), \dots$$

in $\mathbb{Q}$ since

$$\begin{aligned}&\lim_{n\to\infty}|(q_1, q_2, q_3, \dots) - (q_n, q_n, q_n, \dots)|_p =\\ &= \lim_{n\to\infty}|(q_1 - q_n, q_2 - q_n, q_3 - q_n, \dots)|_p =\\ &= \lim_{n\to\infty}\lim_{j\to\infty}|q_j - q_n|_p =\\ &= 0\end{aligned}$$

where we used the Cauchy property of the sequence $(q_n)_n$ in the last equality. □

Remark. Let us add a few more observations about $\mathbb{Q}_p$ and $\mathbb{Z}_p = \{q \in \mathbb{Q}_p \mid |q|_p \leq 1\}$.

- Any point inside an open ball $B(a, r)$ in $\mathbb{Q}_p$ is at the same time its centre, i.e. $B(a, r) = B(q, r)$ for each $q \in B(a, r)$.

- For any $k \in \mathbb{Q}_p$ with $|k|_p = 1$ it holds that $B(ka, r) = B(a, r)$.
- $\{p^n\mathbb{Z}_p \mid n \in \mathbb{N}\}$ is a fundamental system of neighbourhoods of 0 in $\mathbb{Q}_p$.

Definition 1.42. The *valuation ring* of K_v where v is a finite prime is the set

$$\mathcal{O}_v = \{x \in K_v \mid |x|_v \leq 1\}.$$

If v is an infinite prime then let $\mathcal{O}_v = K_v$.

Remark. We use the same letter for valuation rings as for rings of integers. Why? The ring of integers of K_v (where v corresponds to a prime ideal $\mathfrak{p}$) is defined as the integral closure of $\mathbb{Z}_p$ where $p = \mathbb{Z} \cap \mathfrak{p}$. However, this definition coincides with the definition of the valuation ring $\mathcal{O}_v$.

We give two more useful facts which we will need later in some proofs. The first of them is known as Hensel's lemma.

Proposition 1.43. [4, Prop. 7.31] *Let v be a finite prime of a number field K and π be a uniformizer of the valuation ring $\mathcal{O}_v$ of K_v i.e. an element generating the unique maximal ideal $\{x \in K_v \mid |x|_v < 1\}$. Assume that a polynomial $f(x) \in \mathcal{O}_v[x]$ has a simple root a_0 modulo π. Then there is a unique root $a \in \mathcal{O}_v$ of $f(x)$ such that $a \equiv a_0 \ (mod\ \pi)$.*

Theorem 1.44. [1, p. 56,57] *Let K be complete with respect to the place v and let L be a finite separable extension of K. Then there is exactly one extension w of v to L and L is complete with respect to w.*

1.8 Unramified field extensions

Let L/K be a Galois extension. We already know what it means for prime ideals of K to ramify in L. Hence, we can easily define a finite place v to be *unramified* if the corresponding prime ideal $\mathfrak{p}$ does not ramify. To define the unramified extensions, we need to introduce the ramification of infinite primes as well.

Definition 1.45. Let L/K be a field extension and σ be an infinite prime of K, that is σ corresponds either to an embedding of K into $\mathbb{R}$ or a pair of complex embeddings of K into $\mathbb{C}$. We say that σ *ramifies* in L if it is real but has an extension to L which is complex. We call σ *unramified* otherwise.

Example 1.46. The infinite prime $\sigma : \mathbb{Q} \hookrightarrow \mathbb{R}$ (which is simply an inclusion) is unramified in $\mathbb{Q}(\sqrt{2})$ because both embeddings of $\mathbb{Q}(\sqrt{2})$ into $\mathbb{C}$ are real. On the other hand, σ ramifies in $\mathbb{Q}(\sqrt{-2}) \not\subset \mathbb{R}$.

Definition 1.47. An extension L/K is *unramified* if it is unramified at all of its primes, both finite and infinite.

2. Adèles and idèles

The aim of this chapter is to get familiar with an object called the ring of adèles and its subgroup of invertible elements called idèles, together with their topological properties. We already know that there are several absolute values on a number field and adèles enable us to consider all of them at the same time. But instead of defining adèles as a product of all completions of a number field we use another construction, so called restricted product, to obtain some useful compactness properties. Adèles have a rich application far beyond this work; however, we will meet them again in Chapter 4 when formulating the main results of class field theory in idèlic setting.

2.1 Adèles

Before defining the adèle ring, let us first equip ourselves with the notion of restricted product.

Definition 2.1. The *restricted product* $\prod'_{i\in I} X_i$ of topological spaces X_i with respect to a family $\{U_i \subset X_i\}$ of open sets is the subset of $\prod_i X_i$ consisting of those elements $(x_i)_{i\in I}$ for which $x_i \in U_i$ for all but finitely many i. The basic open sets are of the form

$$\prod_{i\in S} V_i \times \prod_{i\notin S} U_i$$

for $V_i \subset X_i$ open and S finite.

Typically, we will use just the notation $\prod'_i X_i$ if it is clear from the context what the open sets U_i are.

Lemma 2.2. *Let K be a number field with a place v. Then $\mathcal{O}_v$ is an open set in K_v.*

Proof. If v is an infinite place, then $\mathcal{O}_v = K_v$ is open in K_v. If v is a finite place corresponding to the prime ideal $\mathfrak{p}$ then we can use the discreteness of $\mathfrak{p}$-adic absolute value (namely, that $\mathrm{ord}_{\mathfrak{p}} x \in \mathbb{Z}$) and write

$$\begin{aligned}\mathcal{O}_v &= \{x \in K_v \mid |x|_v \leq 1\} = \\ &= \{x \in K_v \mid \mathrm{ord}_{\mathfrak{p}} x \geq 0\} = \\ &= \{x \in K_v \mid \mathrm{ord}_{\mathfrak{p}} x > -1\} = \\ &= \{x \in K_v \mid |x|_v < \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})\}.\end{aligned}$$

□

Recall that topological ring is a ring and a topological space at the same time such that the addition and multiplication are continuous with respect to the given topology.

Definition 2.3. Let K be a number field, P be the set of places of K and K_v be the completion of K at the place v. Then the *ring of adèles* $\mathbb{A}_K$ of K is the topological ring where

- the underlying topological space is defined as the restricted product $\prod'_{v\in P} K_v$ with respect to the open sets $\{\mathcal{O}_v \subset K_v\}$,
- the ring operations are defined component-wise.

In other words, $\mathbb{A}_K = \prod'_{v\in P} K_v$ consists of elements $(a_v)_{v\in P}$ with $|a_v|_v \leq 1$ for all but finitely many places v.

Notation. We write $(a_v)_v$ instead of $(a_v)_{v\in P}$ to denote an element of adèles.

Example 2.4. In $\mathbb{Q}$ each finite place corresponds to a prime number p and there is exactly one infinite place corresponding to the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. Let us index the places of $\mathbb{Q}$ by p, including the infinite place $p = \infty$. Then

$$\mathbb{A}_{\mathbb{Q}} = \{(a_p)_p \mid a_p \in \mathbb{Z}_p \text{ for all but finitely many prime numbers } p\} \subset \mathbb{R} \times \prod_{p<\infty} \mathbb{Q}_p.$$

First of all, we need to check that Definition 2.1 is correct, i.e. the ring of adèles is indeed a topological ring. Before doing so, we give one auxiliary lemma:

Lemma 2.5. *There is a homeomorphism of topological spaces*

$$\prod_{v\in P}{}' K_v \times \prod_{w\in P}{}' K_w \cong \prod_{v\in P}{}'(K_v \times K_v)$$

where $\prod_{v\in P}(K_v \times K_v)$ *is restricted with respect to the family* $\{\mathcal{O}_v \times \mathcal{O}_v \subset K_v \times K_v\}$.

Proof. Let the homeomorphism identify an element $((a_v)_v, (b_w)_w) \in \prod'_{v\in P} K_v \times \prod'_{w\in P} K_w$ with $(a_v, b_v)_v \in \prod'_{v\in P}(K_v \times K_v)$. This is clearly well-defined and bijective. We now show that each open set of one topology is open in the other one under this identification.

- Basic open sets of $\prod'_{v\in P} K_v \times \prod'_{w\in P} K_w$ are sets of the form

$$(\prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v) \times (\prod_{w\in S'} V_w \times \prod_{w\notin S'} \mathcal{O}_w) \tag{2.1}$$

  where $U_v \subset K_v, V_w \subset K_w$ are open and S, S' are finite sets.

- Basic open sets of $\prod'_{v\in P}(K_v \times K_v)$ are sets of the form

$$\prod_{v\in \widetilde{S}} (\widetilde{U_v} \times \widetilde{V_v}) \times \prod_{v\notin \widetilde{S}} (\mathcal{O}_v \times \mathcal{O}_v) \tag{2.2}$$

  where $\widetilde{U_v} \times \widetilde{V_v}$ are open in $K_v \times K_v$, this means, they are unions of sets of the form $U \times V \subset K_v \times K_v$ where U, V are open in K_v and $\widetilde{S}$ is finite.

Each set (2.1) has (under the identification) $\mathcal{O}_v \times \mathcal{O}_v$ at each coordinate $v \in P \setminus (S \cup S')$, hence on all but finitely many coordinates v. On the rest there is $U_v \times V_v$ where $U_v, V_v \subset K_v$ are open in K_v. One of them can possibly be equal to $\mathcal{O}_v$ but this is also open by Lemma 2.2.

Conversely, each set (2.2) is clearly writable as union of sets of the form (2.1) where we set $S = S' = \widetilde{S}$ and where we choose open $U_v, V_v \subset K_v$ such that the union of their products at each coordinate gives $\widetilde{U_v} \times \widetilde{V_v}$. □

Lemma 2.6. *Let K be a number field. Then $\mathbb{A}_K$ indeed forms a topological ring. That is, the operations of component-wise addition and multiplication on $\mathbb{A}_K$ are continuous in the $\mathbb{A}_K$-topology.*

Proof. We will show only the continuity of addition as we want to primarily demonstrate that all we need is the component-wise continuity. Consider the map

$$\begin{aligned} f : \prod_{v\in P}{}' K_v \times \prod_{w\in P}{}' K_w &\to \prod_{v\in P}{}' K_v \\ ((a_v)_v, (b_w)_w) &\mapsto (a_v + b_v)_v \end{aligned}$$

and define

$$\begin{aligned} f_v : K_v \times K_v &\to K_v \\ (a_v, b_v) &\mapsto a_v + b_v. \end{aligned}$$

We need to check that $f^{-1}(\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} \mathcal{O}_v)$ for S finite is open in $\prod'_{v\in P} K_v \times \prod'_{v\in P} K_v$. By Lemma 2.6 we can check it to be open in $\prod'_{v\in P}(K_v \times K_v)$ instead. Since the addition is defined component-wise, we have the equality

$$f^{-1}(\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} \mathcal{O}_v) = \prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in P\setminus S} f_v^{-1}(\mathcal{O}_v).$$

As the **first step**, let us show that $f_v^{-1}(U_v)$ is open in $K_v \times K_v$ for $U_v \subset K_v$ open. First, assume that v is non-archimedean. To verify that $f_v^{-1}(U_v)$ is open we need to find an open set around each $(\tilde{x}, \tilde{y}) \in f_v^{-1}(U_v)$ inside $f_v^{-1}(U_v)$. Let $a = \tilde{x} + \tilde{y}$. Since U_v is open, we can find $r > 0$ such that $B(a, r) = \{z \in K_v \mid |z - a|_v < r\} \subset U_v$. We can write

$$\begin{aligned} f_v^{-1}(B(a,r)) &= \{(x,y) \in K_v \times K_v \mid |x + y - a|_v < r\} \supseteq \\ &\supseteq \{(x,y) \in K_v \times K_v \mid |x - \tilde{x}|_v < r, |y - \tilde{y}|_v < r\} = \\ &= B(\tilde{x}, r) \times B(\tilde{y}, r) \end{aligned}$$

where the inclusion follows from the fact that v is non-archimedian which means that

$$|x + y - a|_v = |x + y - \tilde{x} - \tilde{y}|_v \leq \max\{|x - \tilde{x}|_v, |y - \tilde{y}|_v\}.$$

If v is archimedean then K_v is either $\mathbb{R}$ or $\mathbb{C}$. We know from mathematical analysis that addition is continuous on both $\mathbb{R}$ and $\mathbb{C}$, hence $f_v^{-1}(U_v)$ is again open for U_v open in $\mathbb{R}$ or $\mathbb{C}$.

As the **second step**, we show that

$$\prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in P\setminus S} f_v^{-1}(\mathcal{O}_v) = \bigcup_{\substack{S' \text{ finite} \\ S\cap S' = \emptyset}} (\prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in S'} f_v^{-1}(\mathcal{O}_v) \times \prod_{\substack{v\notin S \\ v\notin S'}} (\mathcal{O}_v \times \mathcal{O}_v)).$$

Each set of the union on the right-hand side is a basic open set in $\prod'_v(K_v \times K_v)$ since there is an open set at finitely many components and $\mathcal{O}_v \times \mathcal{O}_v$ on the rest. We obtain that the union, and hence the set $\prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in P\setminus S} f_v^{-1}(\mathcal{O}_v)$, are open.

Take $(a_v, b_v)_v \in \prod_{v\in S} f_v^{-1}(U_v)\times\prod_{v\in P\setminus S} f_v^{-1}(\mathcal{O}_v)$. Since it is also in $\prod'_v(K_v\times K_v)$ we know that $(a_v, b_v) \in \mathcal{O}_v \times \mathcal{O}_v$ for all but finitely many v's, say for all $v \in P \setminus \widetilde{S}$ for $\widetilde{S}$ finite. Let $S' = \widetilde{S} \setminus S$ to see that $(a_v, b_v)_v$ belongs to one of the sets of the union.

Conversely, we have an inclusion

$$\prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in S'} f_v^{-1}(\mathcal{O}_v) \times \prod_{\substack{v\notin S\\ v\notin S'}} (\mathcal{O}_v \times \mathcal{O}_v) \subset \prod_{v\in S} f_v^{-1}(U_v) \times \prod_{v\in P\setminus S} f_v^{-1}(\mathcal{O}_v)$$

for each finite S' with $S \cap S' = \emptyset$. This concludes the proof of the continuity of addition.

For the continuity of multiplication we would have to verify that the preimage of an open set U_v is open in $K_v \times K_v$ under the multiplication map and then use the same argument as in the second step. □

We have seen that there is a canonical embedding $K \hookrightarrow K_v$. This can be extended to the canonical embedding $K \hookrightarrow \mathbb{A}_K$ sending $a \in K$ to $(a_v)_v \in \mathbb{A}_K$ where $a_v = (a, a, a, \dots) \in K_v$.

Topology on adèles

Since the underlying set of the ring of adèles is a subset of the product of all completions, one could wonder if the restricted product topology and the subspace topology are the same. However, this is not the case. In fact, the restricted product topology is strictly finer, which we are going to show now.

Here we work only with products of completions; nevertheless, what we state about the restricted product topology and the subspace topology holds for general topological spaces. Let K be a number field and P the set of places on K. Keep in mind that we always restrict the product $\prod'_{v\in P} K_v$ with respect to the open sets $\{\mathcal{O}_v \subset K_v\}$.

Recall that the product topology on $\prod_{v\in P} K_v$ is defined to be the weakest topology such that the canonical projections $\pi_v : \prod_{w\in P} K_w \to K_v$ are continuous. In other words, the collection of the sets $\{\pi_v^{-1}(U_v) \mid U_v \subset K_v \text{ open}, v \in P\}$ forms a subbase, i.e. each open set is a union of finite intersections of these sets. Hence, the basis of the product topology consists of the sets of the form

$$\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v$$

where $U_v \subset K_v$ are open and the set S is finite.

By the subspace topology on $\prod'_{v\in P} K_v$ we will always mean the subspace topology inherited from $\prod_{v\in P} K_v$. If we gave $\prod'_{v\in P} K_v$ the subspace topology, each basic open set would be an intersection of a basic open set of $\prod_{v\in P} K_v$ with $\prod'_{v\in P} K_v$, that is

$$(\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v) \cap \prod_{v\in P}' K_v \tag{2.3}$$

for some $U_v \subset K_v$ open and some finite S. We will first show that the restricted product topology is finer than the subspace topology.

Lemma 2.7. *Each set of the form* (2.3) *is open in the restricted product topology.*

Proof. Let us show that for finite $S \subset P$ we have the equality

$$(\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v) \cap \prod_{v\in P}{}' K_v = \bigcup_{\substack{S' \text{ finite} \\ S\cap S'=\emptyset}} (\prod_{v\in S} U_v \times \prod_{v\in S'} K_v \times \prod_{v\in P\setminus(S\cup S')} \mathcal{O}_v).$$

Let

$$(a_v)_v \in (\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v) \cap \prod_{v\in P}{}' K_v.$$

Then $a_v \in U_v$ for each $v \in S$ and $a_v \in \mathcal{O}_v$ for all but finitely many v's, say for every $v \in P \setminus S''$ for S'' finite. Set $S' = S'' \setminus S$. Then

$$(a_v)_v \in \prod_{v\in S} U_v \times \prod_{v\in S'} K_v \times \prod_{v\in P\setminus(S\cup S')} \mathcal{O}_v.$$

Conversely, we immediately see that

$$\prod_{v\in S} U_v \times \prod_{v\in S'} K_v \times \prod_{v\in P\setminus(S\cup S')} \mathcal{O}_v \subset (\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v)$$

and also

$$\prod_{v\in S} U_v \times \prod_{v\in S'} K_v \times \prod_{v\in P\setminus(S\cup S')} \mathcal{O}_v \subset \prod_{v\in P}{}' K_v$$

for each S' finite, $S \cap S' = \emptyset$. Hence we have the inclusion for the whole union.

Since all sets in the union are open in the restricted product topology, we get the desired claim. □

We have the inclusion of the subspace topology in the restricted product topology, the following lemma concludes the strict inclusion.

Lemma 2.8. *The set $\prod_{v\in P} \mathcal{O}_v$ is an open subset of $\mathbb{A}_K$ in the restricted product topology but it is not open in the subspace topology.*

Proof. The openness in the restricted product topology is clear. If $\prod_{v\in P} \mathcal{O}_v$ was open in the subspace topology, it would be possible to write it as a union of sets of the form

$$(\prod_{v\in S} U_v \times \prod_{v\in P\setminus S} K_v) \cap \prod_{v\in P}{}' K_v$$

for some $U_v \subset K_v$ open and some finite S. But each such set contains some elements which are not in $\prod_{v\in P} \mathcal{O}_v$ as we allow $a_v \in K_v \setminus \mathcal{O}_v$ to finitely many places v. □

2.2 Isomorphism of $\mathbb{A}_K(+)$ and $\mathbb{A}_{\mathbb{Q}}^d(+)$

A *topological group* is a group and a topological space at the same time such that the group operations are continuous with respect to the given topology. An *isomorphism of topological groups* is a group isomorphism and a homeomorphism at the same time.

Notation. When introducing adèles we denoted the (topological) ring of adèles by $\mathbb{A}_K$. Let us use the notation $\mathbb{A}_K(+)$ for the same structure where we forget the multiplication, that is the additive topological group with the same underlying set and the topology of restricted product.

The goal of this chapter is to show the isomorphism of topological groups $\mathbb{A}_K(+) \cong \mathbb{A}_{\mathbb{Q}}^d(+)$ for a number field K of degree d. This result holds more general for any extension of number fields (see [1, Chapter II, Section 14]) but we stick with the basic version since this is the only one we will need.

This section is inspired by [1, Chapter II] from where we took Lemmas 2.9, 2.10 and 2.12. For this reason, some details in the proofs will be skipped and others will be carried out differently than in the book.

Since claims and facts leading to this isomorphism can be more easily formulated in terms of tensor products, let us make a little digression into them.

(1) Tensor products of algebras – first definition

Let A, B be commutative rings containing a field K that gives them a structure of K-algebras. First, let us view A, B as K-modules, for which the tensor product $A \otimes_K B$ consists of all finite sums of the form

$$\sum_i a_i \otimes b_i, \quad a_i \in A, b_i \in B$$

such that

- $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$,
- $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$,
- $k(a \otimes b) = ka \otimes b = a \otimes kb$

for every $a, a_1, a_2 \in A, b, b_1, b_2 \in B, k \in K$. Now, we give $A \otimes_K B$ the ring structure by defining

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$$

and extending to the whole $A \otimes_K B$ linearly.

(2) Tensor products of algebras – second definition

Another approach to the notion of the tensor product of algebras is viewing it as extending one of the algebras by "lifting" the coefficients from K to the other ring.

Again, let us have K-algebras A, B and let $b_1, b_2, \ldots, b_n$ be a basis for B as a vector space over K, i.e. each element of B can be written as

$$\sum_{i=1}^{n} k_i b_i, k_i \in K.$$

Let $k_{ij}^m \in K$ be the structure constants of B, that means elements satisfying

$$b_i b_j = \sum_m k_{ij}^m b_m.$$

Then we can define a ring C consisting of all elements of the form

$$\sum_i a_i \overline{b}_i, a_i \in A,$$

where the elements $\bar{b}_i$ have the same multiplication rule as b_i, i.e.

$$\bar{b}_i\bar{b}_j = \sum_{m=1}^{n} k_{ij}^m \bar{b}_m$$

and we extend the multiplication A-linearly.

Less formally speaking, we lift the coefficients from K to A in the unique expressions of elements of B and then we rename the basis so that C is a different object. We write $C = A \otimes_K B$.

It is not difficult to see that the two definitions above coincide: Assume B has a basis $b_1, b_2, \ldots, b_n$ as a vector space over K. Then it suffices to check that

$$\sum_{i=1}^{n} a_i \otimes b_i \mapsto \sum_{i=1}^{n} a_i \bar{b}_i$$

is the desired ring isomorphism.

From now on, we work with the second definition only.

Remark. There are the following embeddings of rings A, B into $A \otimes_K B$:

$$\begin{aligned} A &\hookrightarrow A \otimes_K B & \qquad B &\hookrightarrow A \otimes_K B \\ a &\mapsto a\bar{b}_1 & \qquad \sum_i k_i b_i &\mapsto \sum_i k_i \bar{b}_i. \end{aligned}$$

If we now assume A to be a topological ring, we can impose the product topology on C via identifying $\sum_i a_i b_i$ with $(a_1, \ldots, a_n) \in A^n$, call it the *tensor product topology.*

Now, let us see what the tensor product looks like if A, B are moreover fields.

Lemma 2.9. *Let A, B be fields containing a field K such that the extension B/K is finite separable. Then we have a ring isomorphism*

$$A \otimes_K B \cong L_1 \times \cdots \times L_m$$

where $L_i's$ are some finite extensions of A and contain an isomorphic image of B.

Proof. Due to Theorem 1.3 we can write $B = K(b)$ for some $b \in B$. Say the degree of B over K is n. Then $1, b, b^2, \ldots, b^{n-1}$ form a basis for B/K. Moreover, b is a root of some irreducible separable polynomial $f(x) \in K[x]$ and $A \otimes_K B = A[\bar{b}]$ for some $\bar{b}$ satisfying $f(\bar{b}) = 0$. We can factor

$$f(x) = g_1(x)g_2(x)\cdots g_m(x)$$

where $g_1, g_2, \ldots, g_m \in A[x]$ are irreducible and pairwise distinct from separability of $f(x)$. For each i define $L_i = A(b_i)$ where b_i is a root of $g_i(x)$. We can define ring homomorphisms

$$\lambda_i : A \otimes_K B \to L_i$$

by sending the element $h(\bar{b})$ to $h(b_i)$ where $h(x) \in A[x]$. It remains to verify that

$$\lambda_1 \times \cdots \times \lambda_m : A \otimes_K B \to L_1 \times \cdots \times L_m$$

is a bijection. Let us show the injectivity first. Suppose $(\lambda_1 \times \cdots \times \lambda_m)(h(\bar{b})) = 0$; that is, $h(b_i) = 0$ for each i. But since $g_i(x)$ are minimal polynomials for b_i over A, the assumption yields that $h(x)$ is divisible by $g_i(x)$ for each i, and thus by $f(x)$. However, $f(\bar{b}) = 0$, and so $h(\bar{b}) = 0$.

Let us look at the dimensions of both sides as vector spaces over A. The dimension of $A \otimes_K B = A[\bar{b}]$ equals the degree of $f(x)$, the dimension of $L_1 \times \cdots \times L_m$ equals the sum of degrees of g_i's, thus the same thing. We can conclude that $\lambda_1 \times \cdots \times \lambda_m$ is a bijection and thus the desired isomorphism.

Finally, we show that the ring homomorphisms

$$B \hookrightarrow A \otimes_K B \xrightarrow{\lambda_i} L_i$$
$$\sum_{j=0}^{n-1} k_j b^j \mapsto \sum_{j=0}^{n-1} k_j \bar{b}^j \quad \mapsto \sum_{j=0}^{n-1} k_j b_i^j$$

are injective. Assume that $\sum_{j=0}^{n-1} k_j b_i^j = 0$ for some $k_0, k_2, \ldots, k_{n-1} \in K$. That means that $h(x) = \sum_{j=0}^{n-1} k_j x^j$ is divisible by $g_i(x)$ in $A[x]$. But at the same time $h(x) \in K[x]$, and so it is divisible by the irreducible polynomial $f(x) \in K[x]$. This is because $(g_i(x))_{A[x]} \cap K[x]$ is an ideal in $K[x]$, where $(g_i(x))_{A[x]}$ denotes the ideal generated by $g_i(x)$ in the ring $A[x]$. Hence, it is principal with generator $f(x)$. Since $f(b) = 0$, also $h(b) = \sum_{j=0}^{n-1} k_j b^j = 0$. □

Lemma 2.10. *Let K be a number field of degree d and v be a place of $\mathbb{Q}$. Then there are at most d extensions $w_1, \ldots, w_m$ of v to K and there is an isomorphism of topological rings*

$$\mathbb{Q}_v \otimes_{\mathbb{Q}} K \cong K_{w_1} \times \cdots \times K_{w_m},$$

where $K_{w_1} \times \cdots \times K_{w_m}$ is equipped with the product topology.

Proof. (sketch) First, let us show the ring isomorphism. By Lemma 2.9,

$$\mathbb{Q}_v \otimes_{\mathbb{Q}} K \cong L_1 \times \cdots \times L_{m'}$$

for some $L_i's$ finite extensions of $\mathbb{Q}_v$ and some m'. We need to show that those $L_i's$ are completions of K. By Lemma 1.44, the place v of $\mathbb{Q}_v$ extends uniquely to some place w_i on L_i and L_i is complete with respect to w_i. Let $|\cdot|_i$ denote the normalized absolute value of w_i. Now, we can define the absolute values $\|\cdot\|_i$ on K as

$$\|a\|_i = |\mu_i(a)|_i$$

where

$$\mu_i : K \hookrightarrow \mathbb{Q}_v \otimes_{\mathbb{Q}} K \to L_i$$

is the embedding from the proof of Lemma 2.9.

For L_i to be a completion of K with respect to $\|\cdot\|_i$ it suffices to show that $K \cong \mu_i(K)$ is dense in L_i with respect to $\|\cdot\|_i$:

Let $\alpha_1, \ldots, \alpha_d$ be a basis for K over $\mathbb{Q}$. In Lemma 1.41 we checked that $\mathbb{Q}$ is dense in $\mathbb{Q}_v$. This yields the density of $\mathbb{Q} \otimes_{\mathbb{Q}} K$ in $\mathbb{Q}_v \otimes_{\mathbb{Q}} K$ since an element $\sum_i q_i \alpha_i \in \mathbb{Q}_v \otimes_{\mathbb{Q}} K$ is the limit point of the sequence $(\sum_i q_{i,n} \alpha_i)_n$ where q_i's are limits of sequences $(q_{i,n})_n, q_{i,n} \in \mathbb{Q}$. Now, $K = \mathbb{Q} \otimes_{\mathbb{Q}} K$ being dense in $\mathbb{Q}_v \otimes_{\mathbb{Q}} K \cong L_1 \times \cdots \times L_{m'}$ implies $\mu_i(K)$ being dense in L_i when looking at the i-th projection of the product.

What is left to show is the 1-1 correspondence between $L_i's$ and $K'_{w_i}s$; that means, that the absolute values $\|\cdot\|_i$ are pairwise disjoint and the only extensions of v. Finally, we need to check that the isomorphism is a homeomorphism. You can find all the details and the rest of the proof in [1, Chapter II]. □

Let us illustrate the steps leading to Lemma 2.10 on the following example where we see explicitely what the fields $L_1, L_2, \ldots, L_m$ from Lemma 2.9 look like.

Example 2.11. Let $K = \mathbb{Q}(i)$ and consider 5-adic absolute value on $\mathbb{Q}$. Then, since $5 = (2+i)(2-i)$, the extensions of 5-adic absolute value to K are precisely the absolute values associated to prime ideals $(2+i), (2-i)$. Hence, we wish to end with

$$\mathbb{Q}_5 \otimes_{\mathbb{Q}} K \cong K_{(2+i)} \times K_{(2-i)}$$

where $K_{(2+i)}, K_{(2-i)}$ are the corresponding completions. Following the proof of Lemma 2.9, consider $f(x) = x^2 + 1$, the minimal polynomial for i over $\mathbb{Q}$. Since $f(x)$ has a simple root modulo 5, Proposition 1.43 allows us to write $f(x) = (x-a)(x-b)$ for some $a, b \in \mathbb{Z}_5$. Set $L_1 = \mathbb{Q}_5(a) = \mathbb{Q}_5, L_2 = \mathbb{Q}_5(b) = \mathbb{Q}_5$. Hence, by Lemma 2.9,

$$\mathbb{Q}_5 \otimes_{\mathbb{Q}} K \cong \mathbb{Q}_5 \times \mathbb{Q}_5$$

and all we need to show is

$$\mathbb{Q}_5 \cong K_{(2+i)} \cong K_{(2-i)}.$$

Now, we have ring homomorphisms

$$\begin{aligned} \mu_1 : K \hookrightarrow \mathbb{Q}_5 \otimes_{\mathbb{Q}} K &\to \mathbb{Q}_5 \\ x + iy \mapsto \quad x + iy \quad &\mapsto x + ay \end{aligned}$$

$$\begin{aligned} \mu_2 : K \hookrightarrow \mathbb{Q}_5 \otimes_{\mathbb{Q}} K &\to \mathbb{Q}_5 \\ x + iy \mapsto \quad x + iy \quad &\mapsto x + by \end{aligned}$$

and extensions $\|\cdot\|_1, \|\cdot\|_2$ of $|\cdot|_5$ to K by putting $\|z\|_1 = |\mu_1(z)|_5, \|z\|_2 = |\mu_2(z)|_5$. By proof of Lemma 2.10 we have that $\mathbb{Q}_5$ is a completion of K with respect to $\|\cdot\|_1, \|\cdot\|_2$. Therefore, our task reduces to showing that, without loss of generality, $\|\cdot\|_1, |\cdot|_{(2+i)}$ are equivalent and $\|\cdot\|_2, |\cdot|_{(2-i)}$ are equivalent absolute values on K since then we obtain $K_{(2+i)} \cong \mathbb{Q}_5$ and $K_{(2-i)} \cong \mathbb{Q}_5$ from Theorem 1.39.

Proof of the following statement would require dealing with traces in extensions of completions and some more properties of discriminant. Let us refer to [1, Chapter II, Section 12] instead.

Lemma 2.12. *Let K be a number field and let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be its basis over $\mathbb{Q}$. Then for all but finitely many places v on $\mathbb{Q}$ the isomorphism from Lemma 2.10 induces an isomorphism of topological rings*

$$\alpha_1\mathbb{Z}_v \times \alpha_2\mathbb{Z}_v \times \cdots \times \alpha_d\mathbb{Z}_v \cong \mathcal{O}_{w_1} \times \mathcal{O}_{w_2} \times \cdots \times \mathcal{O}_{w_m}$$

where $w_1, w_2, \ldots, w_m$ are all the places of K lying over v and the left hand side is canonically identified with $\{\sum_{i=1}^{d} q_i\alpha_i \mid q_i \in \mathbb{Z}_v \text{ for all } i\} \subset \mathbb{Q}_v \otimes_{\mathbb{Q}} K$.

Lemma 2.13. *Let K be a number field of degree d. There is an isomorphism of topological groups*

$$(\mathbb{Q}_v \otimes_{\mathbb{Q}} K)(+) \cong \mathbb{Q}_v^d(+).$$

Proof. In this case we can construct the isomorphism explicitly. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the basis for K over $\mathbb{Q}$. Define

$$\begin{aligned} \varphi : \mathbb{Q}_v \otimes_{\mathbb{Q}} K &\to \mathbb{Q}_v^d \\ \sum_{i=1}^{d} q_i \alpha_i &\mapsto (q_1, \ldots, q_d) \end{aligned}$$

which is an addition-preserving bijection. Moreover, φ, φ^{-1} are continuous by definiton of the topology on tensor products saying that $U \subset \mathbb{Q}_v \otimes_{\mathbb{Q}} K$ is open if and only if $\varphi(U) \subset \mathbb{Q}_v^d$ is open. □

Now we can put together Lemma 2.10 and Lemma 2.13.

Corollary 2.14. *There is an isomorphism of topological groups*

$$(K_{w_1} \times \cdots \times K_{w_m})(+) \cong \mathbb{Q}_v^d(+).$$

Let us add another example in order to warn that the isomorphism from Corollary 2.14 does not preserve multiplication.

Example 2.15. $K = \mathbb{Q}(i), p = 3$. Since 3 is inert in $\mathcal{O}_K = \mathbb{Z}[i]$ the only absolute values on K extending the 3-adic one is the one given by the prime ideal (3) in $\mathcal{O}_K$, so we get $K_3 \cong \mathbb{Q}_3^2$ from Corollary 2.14. Since K_3 is a field and $\mathbb{Q}_3^2$ is not, the multiplication cannot be preserved.

Theorem 2.16. *There is an isomorphism of topological groups*

$$\mathbb{A}_K(+) \cong \mathbb{A}_{\mathbb{Q}}^d(+).$$

Proof. (sketch) First, observe that $\mathbb{A}_{\mathbb{Q}}^d = (\prod_v' \mathbb{Q}_v)^d = \prod_v' \mathbb{Q}_v^d$ where the latter product is restricted with respect to the family of open subsets $\{\mathbb{Z}_v^d \subset \mathbb{Q}_v^d\}$. The proof is analogous to the one of Lemma 2.5.

Second, it holds that

$$\prod_w{}' K_w = (\prod_v \prod_{w|v})' K_w = \prod_v{}' (K_{w_1} \times \cdots \times K_{w_m})$$

where the latter product is restricted with respect to the family of open subsets $\{\mathcal{O}_{w_1} \times \cdots \times \mathcal{O}_{w_m} \subset K_{w_1} \times \cdots \times K_{w_m}\}$ and $w_1, w_2, \ldots, w_m$ appearing at the coordinate indexed by v are precisely those places which lie over v. The proof is again analogical to the one of Lemma 2.5.

By Corollary 2.14 we have $(K_{w_1} \times \cdots \times K_{w_m})(+) \cong \mathbb{Q}_v^d(+)$. Therefore, to prove the isomorphism

$$\prod_v{}' (K_{w_1} \times \cdots \times K_{w_m})(+) \cong \prod_v{}' \mathbb{Q}_v^d(+)$$

it remains to use Lemma 2.12 saying that

$$\mathcal{O}_{w_1} \times \cdots \times \mathcal{O}_{w_m} \cong \alpha_1 \mathbb{Z}_v \times \alpha_2 \mathbb{Z}_v \times \cdots \times \alpha_d \mathbb{Z}_v \cong \mathbb{Z}_v^d$$

under the isomorphism from Corollary 2.14. □

2.3 Local compactness of $\mathbb{A}_K(+)$

Definition 2.17. We say that a topological space X is *locally compact* if we can find a compact neighbourhood around each point; that is, for each $x \in X$ there is an open set U and a compact set C such that $x \in U \subset C$.

We say that topological group is *locally compact* if the underlying topological space is Hausdorff and locally compact.

Let us recall two well-known topological statements:

- Tychonoff's theorem: Any product of compact spaces is compact (with respect to the product topology).
- A finite product of locally compact spaces is locally compact.

The results we present now hold for any completion of a number field and its valuation ring. However, we show them only for $\mathbb{Z}_p$ and $\mathbb{Q}_p$ to keep things simple and more familiar. We will prove that the topological group $\mathbb{A}_{\mathbb{Q}}(+)$ is locally compact, the local compactness of $\mathbb{A}_K(+)$ will be deduced from the isomorphism $\mathbb{A}_K(+) \cong \mathbb{A}_{\mathbb{Q}}^d(+)$ given in the previous section.

Lemma 2.18. *$\mathbb{Z}_p$ is a compact topological space.*

Proof. Assume there is a cover $\{U_\alpha\}_{\alpha \in A}$ of open sets with no finite subcover. Let us decompose $\mathbb{Z}_p$ as a disjoint union in the following way:

$$\mathbb{Z}_p = \bigsqcup_{0 \leq i \leq p-1} (i + p\mathbb{Z}_p).$$

Due to our assumption we know there is $0 \leq i_1 \leq p-1$ such that $i_1 + p\mathbb{Z}_p$ cannot be contained in just one of the sets from $\{U_\alpha\}_{\alpha \in A}$. We proceed by writing

$$i_1 + p\mathbb{Z}_p = \bigsqcup_{0 \leq i \leq p-1} (i + p^2\mathbb{Z}_p)$$

and again use our assumption to find i_2 such that $i_2 + p^2\mathbb{Z}_p$ cannot be contained in just one of the sets from $\{U_\alpha\}_{\alpha \in A}$.

By continuing this argument we obtain an infinite chain

$$(i_1 + p^1\mathbb{Z}_p) \supset (i_2 + p^2\mathbb{Z}_p) \supset \cdots \supset (i_k + p^k\mathbb{Z}_p) \supset \ldots$$

where each set cannot be contained in just one of the sets from $\{U_\alpha\}_{\alpha \in A}$. Now, consider

$$\lim_{k \to \infty} i_k = z \in \mathbb{Z}_p.$$

There must be a set $V \in \{U_\alpha\}_{\alpha \in A}$ containing z and k_0 large enough satisfying $z + p^{k_0}\mathbb{Z}_p \subset V$. But this is a contradiction, since $z + p^{k_0}\mathbb{Z}_p = i_{k_0} + p^{k_0}\mathbb{Z}_p$. □

Corollary 2.19. *$\mathbb{Q}_p$ is a locally compact topological space.*

Proof. It suffices to show that we can find a compact neighbourhood around 0. We can translate this set to get a neighbourhood of any point since translations are homeomorphisms. However, $\{p^n\mathbb{Z}_p \mid n \in \mathbb{N}\}$ is a fundamental system of neighbourhoods of 0 and $\mathbb{Z}_p$ is compact by Lemma 2.18. □

Consider the product $\prod_p \mathbb{Q}_p$. Although all $\mathbb{Q}_p$'s are locally compact, the product is not. This is also the motivation behind working with the restricted product instead.

Proposition 2.20. *The group $\mathbb{A}_\mathbb{Q}(+)$ is a locally compact topological group.*

Proof. To show that $\mathbb{A}_\mathbb{Q}$ is Hausdorff let us consider $(a_p)_p \neq (b_p)_p \in \mathbb{A}_\mathbb{Q}$. Let p be such that $a_p \neq b_p$. Then $d = |a_p - b_p|_p > 0$ and so $B(a_p, d), B(b_p, d)$ are disjoint open sets separating a_p, b_p. Indeed, if $x \in B(a_p, d)$ then

$$d = |a_p - b_p|_p = |a_p - x + x - b_p|_p \leq \max\{|a_p - x|_p, |x - b_p|_p\}.$$

But since $|a_p - x|_p < d$, necessarily $|x - b_p|_p \geq d$, and hence $x \neq B(b_p, d)$.

For the local compactness, observe that the set

$$U_S = \mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p$$

is locally compact for each finite subset S of primes. This is because $\prod_{p \notin S} \mathbb{Z}_p$ is compact as a product of compact spaces, which implies that U_S is a finite product of locally compact spaces.

Now, each $(a_p)_p \in \mathbb{A}_\mathbb{Q}$ lies in the set U_S for some S. Thus, we can find a compact neighbourhood around $(a_p)_p$ in U_S which is also a compact neighbourhood in the whole $\mathbb{A}_\mathbb{Q}$ as U_S is an open subset of $\mathbb{A}_\mathbb{Q}$. □

Why do we care about local compactness of the additive group $\mathbb{A}_K(+)$? It gives us the existence of a specific measure on $\mathbb{A}_K(+)$ which is invariant under translation.

Definition 2.21. A *Haar measure* μ on a locally compact abelian group G is a nonzero Borel measure satisfying

- $\mu(S) < \infty$ for each $S \subset G$ compact,
- $\mu(S) = \inf\{\mu(U) \mid S \subset U,\ U \text{ is open}\}$ for each S measurable,
- $\mu(S) = \sup\{\mu(C) \mid C \subset S,\ C \text{ is open}\}$ for each S open,
- $\mu(S) = \mu(g + S) = \mu(\{g + s \mid s \in S\})$ for each S measurable and $g \in G$.

Theorem 2.22 (Weil)**.** *Let G be a locally compact abelian group. Then there exists a Haar measure μ on G which is unique up to scaling. This means that for two Haar measures μ_1, μ_2 on G there is $c > 0$ such that $\mu_1 = c\mu_2$.*

Having the Haar measure enables us to do analysis on adèles. Namely, we can define L-functions, a generalization of Riemann zeta function, which encodes information about how primes are distributed. L-functions are, together with cohomology theory, used to prove main theorems of global class field theory. The analytical proofs are to be found for example in the notes [3].

2.4 Idèles

Definition 2.23. The *group of idèles* is the group of units of the ring of adèles; that is, $\mathbb{I}_K = \mathbb{A}_K^\times$.

And what does an element of $\mathbb{I}_K$ look like?

Lemma 2.24. *The idèle group consists of all elements of the form $(a_v)_v$ where $a_v \neq 0$ for all v's and $a_v \in \mathcal{O}_v^\times$ for all but finitely many v's.*

Proof. If the two conditions hold then $(a_v)_v$ is clearly invertible.

Conversely, suppose $(a_v)_{v\in P} \in \mathbb{I}_K$, i.e. there is $(b_v)_v$ such that $(a_v)_v(b_v)_v = 1$. Since $a_v, b_v \in \mathcal{O}_v$ for all but finitely many v, also $a_v, b_v \in \mathcal{O}_v^\times$ for all but finitely many v's. The nonzero condition comes from $a_v \in K_v^\times$ for all v's. □

This yields another description of idèles; namely, we can write $\mathbb{I}_K = \prod_v' K_v^\times$ (so far this is just equality of sets) where we restrict with respect to the groups of units $\{\mathcal{O}_v^\times \subset K_v^\times\}$.

Topology on idèles

We have to be careful about the topology on $\mathbb{I}_K$ as want $\mathbb{I}_K$ to be a topological group with respect to multiplication. If we took the $\mathbb{A}_K$-subset topology, the inverse map would fail to be continuous.

Example 2.25. Consider the sequence $(a_v)_v^{(2)}, (a_v)_v^{(3)}, (a_v)_v^{(5)}, \dots$ in $\mathbb{A}_\mathbb{Q}$ where $(a_v)_v^{(p)} = (1, \dots, 1, p, 1, \dots)$ has p in the p-th component and 1 everywhere else. This sequence converges to $1 \in \mathbb{A}_\mathbb{Q}$ because for each open neighborhood of 1 of the form

$$U = V \times \prod_{p\in S} U_p \times \prod_{p\notin S} \mathbb{Z}_p$$

with $1 \in V, 1_p \in U_p$ for each p and S finite, we can find a prime p_0 such that $(a_v)_v^{(p)} \in U$ for each prime $p \geq p_0$.

On the other hand, the inverses do not converge to $1^{-1} = 1$ because for an open neighborhood U of 1 there are infinitely many primes p such that $((a_v)_v^{(p)})^{-1} = (1, \dots, 1, p^{-1}, 1, \dots) \notin U$.

Instead, we consider the map

$$\begin{aligned} i : \mathbb{I}_K &\to \mathbb{A}_K \times \mathbb{A}_K \\ (a_v)_v &\mapsto ((a_v)_v, (a_v)_v^{-1}) \end{aligned}$$

which is injective. Hence, we can give $\mathbb{I}_K$ the subset topology induced by the product topology on $\mathbb{A}_K \times \mathbb{A}_K$ and the map i. This topology is finer than the $\mathbb{A}_K$-subset topology and we call it the *idèlic topology*. Moreover, this topology coincides with the restricted product topology. Before proving this claim, let us remark that we again consider the topology induced by a place v on $K_v^\times$. Then the set $\mathcal{O}_v^\times$ is open in $K_v^\times$, the proof is analogous to the one in Lemma 2.2.

Lemma 2.26. *The idèlic topology coincides with the topology of the restricted product $\prod_v' K_v^\times$ with respect to the family of open sets $\{\mathcal{O}_v^\times \subset K_v^\times\}$.*

Proof. **(1)** We describe the basic open sets in the idèlic topology step by step:

- basic open sets in $\mathbb{A}_K \times \mathbb{A}_K$ are of the form $U \times V$ for some basic open sets $U, V \subset \mathbb{A}_K$,
- basic open sets in $(\mathbb{A}_K \times \mathbb{A}_K) \cap i(\mathbb{I}_K)$ are of the form

$$\begin{aligned}&(U \times V) \cap \{(a, a^{-1}) \mid a \in \mathbb{I}_K\} = \\ &= ((U \cap \mathbb{I}_K) \times (V \cap \mathbb{I}_K)) \cap \{(a, a^{-1}) \mid a \in \mathbb{I}_K\} = \\ &= \{(a, a^{-1}) \mid a \in (U \cap \mathbb{I}_K) \cap (V \cap \mathbb{I}_K)^{-1}\},\end{aligned}$$

- to conclude, basic open sets in the idèlic topology are those of the form $(U \cap \mathbb{I}_K) \cap (V \cap \mathbb{I}_K)^{-1}$ (we look at the first component of $i(\mathbb{I}_K)$), which can be alternatively rewritten as $U \cap (V \cap \mathbb{I}_K)^{-1}$ where U, V are basic open sets of $\mathbb{A}_K$.

(2) Recall that the basic open sets of $\prod'_v K_v^\times$ are of the form

$$\prod_S W_v \times \prod_{P \setminus S} \mathcal{O}_v^\times \tag{2.4}$$

for S finite and W_v open in $K_v^\times$.

For one inclusion, a set of the form (2.4) can be written as $U \cap (V \cap \mathbb{I}_K)^{-1}$ for $U = \prod_S W_v \times \prod_{P \setminus S} \mathcal{O}_v$ and $V = \prod_S W_v^{-1} \times \prod_{P \setminus S} \mathcal{O}_v$, both clearly open in $\mathbb{A}_K$.

For the other inclusion, we can write

$$U \cap (V \cap \mathbb{I}_K)^{-1} = \prod_{S'} W_v \times \prod_{P \setminus S'} \mathcal{O}_v^\times$$

for $W_v = U_v \cap (V_v \cap K_v^\times)^{-1}$ open in $K_v^\times$ and some finite set S', as both U, V are basic open sets of $\mathbb{A}_K$ and thus have $\mathcal{O}_v$ in all but finitely many components. This concludes the equality of the sets of basic open sets. □

Idèle class group, Content of idèles

Now we would like to define the idèle class group, the crucial notion for the description of all abelian extensions of a fixed number field in the language of idèles.

As we discussed in Section 2.1, there is a natural embedding $K \hookrightarrow \mathbb{A}_K$. Restricting to the set of invertible elements yields the embedding $K^\times \hookrightarrow \mathbb{I}_K$. We identify $K^\times$ with its image in $\mathbb{I}_K$ and write $K^\times \subset \mathbb{I}_K$.

Lemma 2.27. [1, Chapter II, Section 16] *$K^\times$ is a discrete subgroup of $\mathbb{I}_K$.*

Definition 2.28. The quotient $\mathcal{C}_K = \mathbb{I}_K / K^\times$ is referred to as the *idèle class group*.

Definition 2.29. The *content map* on idèles is the map

$$\begin{aligned}c : \mathbb{I}_K &\to \mathbb{R}^+ \\ (a_v)_v &\mapsto \prod_v |a_v|_v.\end{aligned}$$

Observe, that this map is well-defined since $|a_v|_v = 1$ for all but finitely many v's. Moreover, it is a continuous homomorphism where we consider a multiplicative structure on $\mathbb{R}^+$. It is surjective (from surjectivity of archimedean absolute values) and by Theorem 1.36, $\mathbb{I}_K^1 \coloneqq \mathrm{Ker}(c)$ contains $K^\times$.

Now, let us take a closer look at the subgroup $\mathbb{I}_K^1 \subset \mathbb{I}_K$ and its topology. It makes sense to impose both the $\mathbb{I}_K$-subset topology and the $\mathbb{A}_K$-subset topology on it. In fact, these two topologies coincide upon restriction to $\mathbb{I}_K^1$, which is shown in Lemma 2.31 below.

We again adopt both the upcoming lemmas 2.30 and 2.31 from [1, Chapter II, Section 16]. However, we present the proof of Lemma 2.30 in more detail with every step properly explained.

Lemma 2.30. *$\mathbb{I}_K^1$ is a closed subset of $\mathbb{A}_K$ with respect to the $\mathbb{A}_K$-topology.*

Proof. Let $a = (a_v)_v \in \mathbb{A}_K \setminus \mathbb{I}_K^1$, that is, $\prod_v |a_v|_v \neq 1$. We want to find an open set $U \subset \mathbb{A}_K$ such that $a \in U$ and $U \cap \mathbb{I}_K^1 = \emptyset$. We will distinguish two cases:

(1) Assume $\prod_v |a_v|_v < 1$. Then we can take a finite set F of some places v such that F contains all v's for which $|a_v|_v > 1$ and $\prod_{v\in F} |a_v|_v < 1$. This is possible because

- $|a_v|_v > 1$ for only finitely many v's as $(a_v)_v \in \mathbb{A}_K$,
- if $|a_v|_v < 1$ for finitely many v's we are done,
- if $|a_v|_v < 1$ for infinitely many non-archimedian places v, where each of them is equal to some power of a prime number, observe that $|a_v|_v \leq \frac{1}{2}$ for all such v's, and so their product converges to 0.

Now, define the set U as the set of all $(b_v)_v$ satisfying

- $|b_v - a_v|_v < \varepsilon$ for every $v \in F$ and ε small enough (to be specified later),
- $|b_v|_v \leq 1$ for all $v \notin F$.

Then U is open in $\mathbb{A}_K$ since it is of the form

$$\prod_{v\in F} B_v(a_v, \varepsilon) \prod_{v\in P\setminus F} \mathcal{O}_v$$

and $a \in U$ by definition of F.

Finally, for $(b_v)_v \in U$ we need to verify that $\prod_b |b_v|_v \neq 1$. We use the triangle inequality to get $|b_v|_v < |a_v|_v + \varepsilon$ for each $v \in F$ which enables us to write

$$\prod_b |b_v|_v = \prod_{v\notin F} |b_v|_v \prod_{v\in F} |b_v|_v < 1 \cdot \prod_{v\in F} (|a_v|_v + \varepsilon) = \prod_{v\in F} |a_v|_v + c\varepsilon$$

where c depends on finitely many components of $(a_v)_v$. Since $\prod_{v\in F} |a_v|_v < 1$, we can choose ε small enough such that $\prod_{v\in F} |a_v|_v + \varepsilon \cdot c < 1$, and so, for such choice of ε, we get $U \cap \mathbb{I}_K^1 = \emptyset$.

(2) For $\prod_v |a_v|_v = C > 1$ define F to be the set of

- all places v for which $|a_v|_v \neq 1$,

- all archimedean places,
- all extensions of p-adic absolute values on $\mathbb{Q}$ with $p \leq 2C$.

Since $|a_v|_v \leq 1$ for all but finitely many v and $\prod_v |a_v|_v > 1$, there are only finitely many v's with $|a_v|_v < 1$ (the same argument as in (1)). We get that the first component of F is finite, and hence, by finiteness of the other two components, F is finite. Now, we can again define the set U as the set of all $(b_v)_v$'s satisfying

- $|b_v - a_v|_v < \varepsilon$ for all $v \in F$ and ε small enough (to be specified later),
- $|b_v|_v \leq 1$ for all $v \notin F$

and check that U is open in $\mathbb{A}_K$ and $a \in U$.

Next, we can choose ε small enough so that $1 < \prod_{v \in F} |b_v|_v < 2C$ for each $(b_v)_v \in U$. Notice, that for $v \notin F$ either $|b_v|_v = 1$ or $|b_v|_v < \frac{1}{2C}$. Indeed, v is necessarily an extension of a p-adic absolute value with $p > 2C$ and $|b_v|_v$ is a zero or a negative power of p.

If $|b_v|_v = 1$ for every $v \notin F$, then

$$\prod_b |b_v|_v = \prod_{v \notin F} |b_v|_v \prod_{v \in F} |b_v|_v > 1.$$

If $|b_v|_v < \frac{1}{2C}$ for some $v \notin F$, then

$$\prod_b |b_v|_v = \prod_{v \notin F} |b_v|_v \prod_{v \in F} |b_v|_v < \frac{1}{2C} \cdot 2C = 1.$$

In either case, $U \cap \mathbb{I}_K^1 = \emptyset$. □

As a little side remark, let us observe that $\mathbb{I}_K^1$ is also closed in $\mathbb{I}_K$. By definition, $\mathbb{I}_K^1$ is the preimage of the closed subset $\{1\}$ of $\mathbb{R}^+$. We only have to show that

$$\begin{aligned} c : \mathbb{I}_K &\to \mathbb{R}^+ \\ (a_v)_v &\mapsto \prod_v |a_v|_v. \end{aligned}$$

is continuous. This holds because $(a_v)_v \in \mathbb{I}_K$ has a unit in all but finitely components and the preimage of an open set in $\mathbb{R}^+$ containing $c((a_v)_v)$ is clearly open in the remaining finitely many coordinates. Another reason could be the fact that the idèlic topology is finer than the $\mathbb{A}_K$-subset topology.

Lemma 2.31. [1, Chapter II, Section 16] *The $\mathbb{I}_K$-subset topology coincides with the $\mathbb{A}_K$-subset topology on $\mathbb{I}_K^1$.*

Whereas the idèle class group $\mathcal{C}_K = \mathbb{I}_K / K^\times$ is not compact, we are more lucky with the quotient $\mathbb{I}_K^1 / K^\times$.

Theorem 2.32. *$\mathbb{I}_K^1 / K^\times$ is compact.*

Proof. (sketch) Recall that the image of a compact set under a continuous map between two topological spaces is compact. Since $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$ by Lemma 2.30, its intersection with any compact set is again compact in adèlic topology. Therefore, it is enough to find a compact set $W \subset \mathbb{A}_K$ such that the map $W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1 / K^\times$ is surjective. How the set W is defined can be found in [1, Chapter II, Section 16]. □

Using Theorem 2.32 we can prove the finiteness of the ideal class group Cl_K for a number field K. It can be verified that the map

$$\begin{aligned} \tau_K : \mathbb{I}_K &\to I_K \\ (a_v)_v &\mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}, \end{aligned}$$

which plays an important role in Chapter 4, induces a surjective continuous map $\tau_K : \mathbb{I}_K^1/K^\times \to Cl_K$ where Cl_K is given the discrete topology. Therefore, Cl_K is finite as a compact group with respect to the discrete topology.

3. Classical CFT

The goal of this chapter is to briefly summarize the main results of class field theory (which we will abbreviate as CFT) formulated in terms of ideals. This approach is older and somewhat more natural than the idèlic one. However, we will see that it also brings some inconveniences.

As we advised in the introduction, class field theory describes all abelian extensions of a fixed number field. Namely, we consider the following three goals (adopted from [7]) which are to describe

1. all finite abelian extensions of a number field K,
2. the Galois group $\mathrm{Gal}(L/K)$ for all abelian extensions L of K,
3. decomposition of prime ideals in abelian extensions L/K

in terms of some "inner arithmetic" of the base field K which we will specify later. Let us start with two particular types of abelian extensions before we dive into the general description. At the end of this chapter we give a table comparing those two special situations from sections 3.1,3.2 with the general one.

3.1 CFT over $\mathbb{Q}$

This subsection is inspired by paper [7] of Garbanati who provides this introduction in a nicely organized manner.

The key advantage in the situation when the base field is $\mathbb{Q}$ is having the Kronecker-Weber theorem. Recall that a cyclotomic field is a field of the form $\mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$ is the primitive m-th root of unity.

Theorem 3.1 (Kronecker-Weber)**.** *Each finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field.*

Based on this, we define a series of concepts which we generalize later in Section 3.3. These generalizations will provide an analogous "larger field" also for abelian extensions of a general base field K.

The first terms introduced are defining modulus and conductor for an extension of $\mathbb{Q}$.

Definition 3.2. Let $L/\mathbb{Q}$ be a finite abelian extension. We call any $m \in \mathbb{N}$ such that $L \subset \mathbb{Q}(\zeta_m)$ a *defining modulus* of L. The least such m is called the *conductor* of L and denoted by f_L.

Notation. Let us denote the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ by C_m. This group will be later generalized to something called a ray class group which uses the same notation.

Consider a finite abelian extension $L/\mathbb{Q}$ and its defining modulus m. Now, by the Galois correspondence, $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_m)$ is a fixed field of some subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong C_m$. Denote this subgroup by $I_{L,m}$.

We see that we managed to fulfil the first goal of CFT which is to describe the abelian extensions of $\mathbb{Q}$ in terms of some "inner arithmetic" of $\mathbb{Q}$ by which we mean the multiplicative groups C_m here.

Another concept to be defined is the notion of the Artin symbol and the Artin map. Again, we introduce them first in this concrete situation.

Definition 3.3. Let $L/\mathbb{Q}$ be a finite abelian extension and let m be its defining modulus. The *Artin symbol* for an element $a \in C_m$ is defined to be the restriction of the map $\zeta_m \mapsto \zeta_m^a$ to L and is denoted by $\left(\frac{L}{a}\right)$.

The induced map $\left(\frac{L}{\cdot}\right) : C_m \to \mathrm{Gal}(L/\mathbb{Q})$ is called the *Artin map*.

By verifying that the Artin map is a surjective group homomorphism and its kernel is $I_{L,m}$ we immediately obtain a special case of the CFT key theorem by Artin:

Theorem 3.4 (Artin Reciprocity Law for extensions of $\mathbb{Q}$)**.** *Let $L/\mathbb{Q}$ be a finite abelian extension and let m be its defining modulus. Then we have an isomorphism*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong C_m/I_{L,m}.$$

So we can also describe the Galois group of an abelian extension of $\mathbb{Q}$ using the multiplicative groups C_m, fulfilling the second goal of CFT.

Now we will proceed towards the description of prime splitting behaviour. Our goal is to give some "congruence conditions" stated in terms of the multiplicative groups C_m characterizing those primes which split completely in L. Recall the notation $\mathrm{Spl}(L/\mathbb{Q})$ for the set of primes of $\mathbb{Q}$ which split completely in L.

Here the conductor f_L comes into play. The motivation behind defining this notion is the study of ramification of primes as the following theorem captures:

Theorem 3.5 (Conductor-Ramification Theorem)**.** *Let $L/\mathbb{Q}$ be an abelian extension and let p be a prime of $\mathbb{Z}$. Then*

$$p \text{ ramifies in } L \iff p \mid f_L.$$

Theorem 3.6 (Decomposition Theorem)**.** *Let $L/\mathbb{Q}$ be an abelian extension and let m be its defining modulus. If a prime p does not divide m, then the order of $pI_{L,m}$ in $C_m/I_{L,m}$ is f, the inertia degree of p.*

Consider a Galois extension $L/\mathbb{Q}$, its defining modulus m and a prime p. It follows from theorems 3.5 and 3.6 that $e = 1 \iff p \nmid f_L$ where e is a ramification index of p and $f = 1 \iff p \in I_{L,m}$ for $p \nmid m$. Thus, we get the following characterization of primes which split in terms of $f_L, I_{L,m}$:

$$p \in \mathrm{Spl}(L/\mathbb{Q}) \iff e = f = 1 \iff p \nmid f_L \text{ and } p \in I_{L,f_L}.$$

And how to obtain the previously mentioned congruence conditions to describe $\mathrm{Spl}(L/\mathbb{Q})$? Let $I_{L,f_L} = \{a_1, \ldots, a_j\}$. Then we easily get that

$$p \in \mathrm{Spl}(L/\mathbb{Q}) \iff p \equiv a_i \pmod{f_L} \text{ for some } 1 \leq i \leq j.$$

3.2 Hilbert class field

In this section we will deal with describing all unramified abelian extensions i.e. only a special case of the main goal which is to describe all the abelian ones. We will define the Hilbert class field of a number field and state the Artin Reciprocity theorem for this particular extension. All statements in this section can be found in [8].

We again start with a theorem giving the existence of the "larger field" containing all unramified abelian extensions of a fixed base field. It may remind us of the Kronecker-Weber Theorem except for the abstract way in which we describe it.

Theorem 3.7. *Let K be a number field. Then there is a unique finite Galois extension L of K such that*

- *L/K is unramified abelian,*
- *any unramified abelian extension of K lies in L.*

Definition 3.8. The extension L from Theorem 3.7 is called the *Hilbert class field* of K. We will denote it by $\widetilde{K}$.

The Hilbert class field, or in other words, the maximal unramified abelian extension, will be later generalized. Roughly speaking, there will be a unique extension unramified in all but finitely many places which we prescribe.

Now, we would like to define the Artin symbol for any Galois extension L/K and an unramified prime of K for which we need the following theorem:

Theorem 3.9. *Let L/K be a Galois extension, $\mathfrak{p}$ be an unramified prime of K and $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Then there is a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that*

$$\sigma(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_L$$

where $\mathrm{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the numerical norm of $\mathfrak{p}$.

Definition 3.10. The element σ from Theorem 3.9 is called the *Artin symbol for L/K over $\mathfrak{P}$* and is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$.

Let us observe that in the setting of Theorem 3.9 it holds that

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \sigma^{-1}$$

for all $\sigma \in \mathrm{Gal}(L/K)$. Indeed, for all $\alpha \in \mathcal{O}_L$ we have

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\sigma^{-1}(\alpha)) \equiv (\sigma^{-1}(\alpha))^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}},$$
$$(\sigma \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \sigma^{-1})(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \pmod{\sigma(\mathfrak{P})},$$

and so, by the uniqueness of the Artin symbol, the equality follows. Now, let $\mathfrak{P}_1, \mathfrak{P}_2$ be two primes of L lying over $\mathfrak{p}$. By Proposition 1.15 there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\mathfrak{P}_1 = \sigma(\mathfrak{P}_2)$, and so $\left(\frac{L/K}{\mathfrak{P}_1}\right) = \sigma \circ \left(\frac{L/K}{\mathfrak{P}_2}\right) \circ \sigma^{-1}$. If the Galois extension

L/K is moreover abelian, we get that $\left(\frac{L/K}{\mathfrak{P}_1}\right) = \left(\frac{L/K}{\mathfrak{P}_2}\right)$, in other words, the Artin symbol does not depend on the choice of the particular prime lying over $\mathfrak{p}$. This allows us to define the Artin symbol for L/K over $\mathfrak{p}$. We will denote it by $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Example 3.11. Let $K = \mathbb{Q}, L = \mathbb{Q}(i), p = 5$. Then $5 = (2+i)(2-i)$ and it can be shown that $\mathrm{N}(2+i) = 5$. Hence, we have

$$\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{5}\right)(i) \equiv i^5 \equiv i \pmod{(2+i)}$$

which means that the Artin symbol $\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{5}\right)$ is the identity.

The Artin symbol for a prime $\mathfrak{p}$ captures the splitting behaviour of $\mathfrak{p}$ in $\mathcal{O}_L$ as the following proposition asserts:

Proposition 3.12. *Let L/K be a Galois extension and $\mathfrak{p}$ an unramified prime of K. Then $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$.*

Before defining the Artin map and stating the Artin reciprocity for the Hilbert class field we need to generalize the notion of the Artin symbol to any fractional ideal of K.

Recall that we denote the group of fractional ideals by I_K and its subgroup of principal fractional ideals by P_K. We defined the ideal class group as $Cl_K = I_K/P_K$.

Definition 3.13. Let L/K be an unramified abelian extension and $\mathfrak{a} \in I_K$. Let $\mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i}$ where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$ and $r_i \in \mathbb{Z}$ for each i. Then we define the *Artin symbol* for $\mathfrak{a}$ as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

which induces a map

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

called the *Artin map*.

Theorem 3.14 (Artin Reciprocity Law for the Hilbert Class Field)**.** *Let $\widetilde{K}$ denote the Hilbert class field of a number field K. Then*

- *the Artin map $\left(\frac{\widetilde{K}/K}{\cdot}\right)$ is surjective,*
- *the kernel of $\left(\frac{\widetilde{K}/K}{\cdot}\right)$ is P_K.*

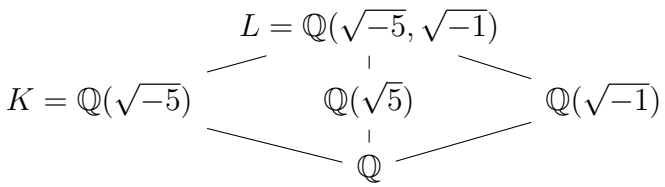
Therefore, the Artin map induces an isomorphism $\mathrm{Gal}(\widetilde{K}/K) \cong Cl_K$.

This result enables us to describe all abelian unramified extensions of a fixed field K in terms of the "inner arithmetic" of K, by which we mean Cl_K, the ideal class group of K.

Corollary 3.15. *Let $\widetilde{K}$ denote the Hilbert class field of a number field K. Then there is one-to-one correspondence*

$$\{K \subset L \subset \widetilde{K} \,\big|\, L/K \text{ unramified abelian}\} \longleftrightarrow \{\text{subgroups } H < Cl_K\}.$$

Example 3.16. Let $K = \mathbb{Q}(\sqrt{-5})$. It can be shown that $h_K = |Cl_K| = 2$ (for example by computing the Minkowski bound). Hence, $|\mathrm{Gal}(\widetilde{K}/K)| = 2$ and $[\widetilde{K} : K] = 2$. We will show that the Hilbert class field for K is $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ for which it suffices to check that all primes of $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ are unramified in L. Let us look at the extension $L/\mathbb{Q}$ first.



Observe that $\Delta_{\mathbb{Q}(\sqrt{-1})} = -4, \Delta_{\mathbb{Q}(\sqrt{-5})} = -20$. By Proposition 1.28 the discriminant $\Delta_{L/\mathbb{Q}}$ is divisible only by primes 2 and 5, and thus, by Proposition 1.29, they are the only ones which ramify in L. From the multiplicativity of ramification indices, no other primes than those dividing $2, 5$ have a chance to ramify in L/K.

The prime 2 ramifies in K. If it ramified further in L/K, its ramification index would be 4. But 2 does not ramify in $\mathbb{Q}(\sqrt{5})$ since $\Delta_{\mathbb{Q}(\sqrt{5})} = 5$ and 2 cannot have the ramification index 4 in a quadratic extension $L/\mathbb{Q}(\sqrt{5})$. We conclude that the primes lying above 2 in K cannot ramify in L.

Similarly, the primes lying over 5 in K do not ramify in L since 5 is unramified in $\mathbb{Q}(\sqrt{-1})$ as 5 does not divide $\Delta_{\mathbb{Q}(\sqrt{-1})} = -4$.

3.3 General version of CFT, Artin reciprocity, ray class field

By going through sections 3.1,3.2 we gained some insight into what CFT deals with. The task now is to define all the notions for a general abelian extension L/K.

Notation. We sometimes denote a finite place by $\mathfrak{p}$ if it corresponds to a prime ideal $\mathfrak{p}$. Similarly, we denote an infinite place by σ is it corresponds to an embedding σ.

Definition 3.17. Let K be a number field. A *modulus* for K is a formal product

$$\mathfrak{m} = \prod_{v \in P} v^{n_v}$$

where P is the set of all places of K, $n_v \in \mathbb{Z}_{\geq 0}$ and

- $n_v = 0$ for almost all v,
- $n_\sigma \leq 1$ for all infinite real places σ,

- $n_\sigma = 0$ for all infinite complex places σ.

We can also write it in the form

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$$

where $\mathfrak{m}_0$ is an ideal in $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a product of infinite real primes.

- Let $A_\mathfrak{m}$ be the subgroup of I_K consisting of all the fractional ideals such that their prime factorizations do not contain any prime ideal dividing $\mathfrak{m}_0$.

Before defining the ray and the congruence subgroup we need to clarify what a congruence means in this setting. Namely, we write $\alpha \equiv 1 \pmod{\mathfrak{m}}$ for $\alpha \in K^\times$ such that $(\alpha) \in A_\mathfrak{m}$ if

1. $\mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq n_\mathfrak{p}$ for all finite primes $\mathfrak{p}$ dividing $\mathfrak{m}_0$,
2. $\sigma(\alpha) > 0$ for all infinite primes σ dividing $\mathfrak{m}_\infty$.

- Let $H^0_\mathfrak{m}$ be the subgroup of $A_\mathfrak{m}$ consisting of principal ideals of the form (α) where $\alpha \equiv 1 \pmod{\mathfrak{m}}$. We call it the *ray modulo* $\mathfrak{m}$.
- Let $H_\mathfrak{m}$ denote any subgroup of $A_\mathfrak{m}$ which contains $H^0_\mathfrak{m}$. We call it a *congruence subgroup for the modulus* $\mathfrak{m}$.

Remark. In other literature you can find a different notation, for example $I^{S(\mathfrak{m})}$ or $I_K^\mathfrak{m}$ instead of $A_\mathfrak{m}$, $i(K_{\mathfrak{m},1})$ or $P_K^\mathfrak{m}$ instead of $H^0_\mathfrak{m}$.

Example 3.18. Let $K = \mathbb{Q}$ and

(1) $\mathfrak{m} = (5)$,
(2) $\mathfrak{m} = (2) \cdot (3) \cdot (7)$.

Then:

(1) $A_\mathfrak{m}$ consists of all fractional ideals (α) where $\alpha = \frac{a}{b}$ and a, b are integers coprime with 5 and $H^0_\mathfrak{m} \subset A_\mathfrak{m}$ consists of $(\alpha), \alpha \in \mathbb{Q}$ with $\alpha \equiv 1 \pmod 5$.

(2) $A_\mathfrak{m}$ consists of all fractional ideals (α) where $\alpha = \frac{a}{b}$ and a, b are integers coprime with 42 and $H^0_\mathfrak{m} \subset A_\mathfrak{m}$ consists of $(\alpha), \alpha \in \mathbb{Q}$ with $\alpha \equiv 1 \pmod{42}$.

Example 3.19. To slightly uncover the motivation behind the definitions given above, let us illustrate the fact that the group $H^0_\mathfrak{m}$ can capture the decomposition of ideals for certain $\mathfrak{m}$. Consider $K = \mathbb{Q}(i), \mathcal{O}_K = \mathbb{Z}[i]$. Then a prime $p \in \mathbb{Z}$ splits in $\mathbb{Z}[i] \Leftrightarrow p \equiv 1 \pmod 4$. Hence, if we set $\mathfrak{m} = (2)^2$ then p splits $\iff (p) \in H^0_\mathfrak{m}$.

Definition 3.20. The quotient $C_\mathfrak{m} = A_\mathfrak{m}/H^0_\mathfrak{m}$ is called the *ray class group modulo* $\mathfrak{m}$.

Now, we again follow the strategy from the paper [7] when stating lemmas 3.21 and 3.23 which confirm that our general concepts are indeed generalizations of the concrete ones defined in the previous two sections. However, we also give detailed proofs of those statements.

It is easy to see that if $\mathfrak{m} = 1$ then $C_\mathfrak{m} = Cl_K$, the ideal class group of K. We will now show that the ray class group $C_\mathfrak{m}$ is also a generalization of the multiplicative group $C_m = (\mathbb{Z}/m\mathbb{Z})^\times$ from Section 3.1.

Lemma 3.21. *Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m)v_\infty$ where $m \in \mathbb{N}$ and v_∞ denotes the only infinite place of $\mathbb{Q}$, that is, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. Then we have a group isomorphism $C_\mathfrak{m} \cong C_m$ where $C_\mathfrak{m} = A_\mathfrak{m}/H^0_\mathfrak{m}$ and $C_m = (\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. Let us define the map

$$\begin{aligned} \varphi : A_\mathfrak{m} &\to (\mathbb{Z}/m\mathbb{Z})^\times \\ (\alpha) &\mapsto ab^{-1} \pmod m \end{aligned}$$

where $\alpha = \frac{a}{b}$ and $a, b \in \mathbb{N}$ are coprime with m. Observe that there always are such a, b by definition of $A_\mathfrak{m}$ and we can choose them to be positive as $(\alpha) = (-\alpha)$. The map is well-defined since $ab^{-1} \pmod m$ indeed lies in $(\mathbb{Z}/m\mathbb{Z})^\times$. It is clearly a group homomorphism and the surjectivity also follows immediately as $(a) \in A_\mathfrak{m}$ for each $1 \leq a \leq m-1$ coprime with m.

Moreover, for $(\alpha) \in A_\mathfrak{m}$ where $\alpha = \frac{a}{b}$ and $a, b \in \mathbb{N}$ are coprime with m we have

$$\begin{aligned} (\alpha) \in \mathrm{Ker}(\varphi) &\iff ab^{-1} \equiv 1 \pmod m \text{ (where } \alpha = \frac{a}{b} > 0) \\ &\iff \alpha \equiv 1 \pmod{\mathfrak{m}} \\ &\iff (\alpha) \in H^0_\mathfrak{m}. \end{aligned}$$

Therefore, φ induces an isomorphism $A_\mathfrak{m}/H^0_\mathfrak{m} \cong (\mathbb{Z}/m\mathbb{Z})^\times$. □

Hence, it appears as a good idea to view $C_\mathfrak{m}$ as that "inner arithmetic" in terms of which we will describe all abelian extensions.

Now we want to define the general version of the Artin map and then proceed to the statement of general Artin's Reciprocity Theorem. Although the definition is analogous to the case with unramified extensions, let us state it properly for the sake of completeness.

Definition 3.22. Let L/K be an abelian extension, $\mathfrak{m}$ be a modulus of K divisible by all the primes which ramify in L and $\mathfrak{a} \in A_\mathfrak{m}$. Let $\mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i}$ where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$ and $r_i \in \mathbb{Z}$ for each i. Then the *Artin symbol* for L/K over $\mathfrak{a}$ is defined as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

where $\left(\frac{L/K}{\mathfrak{p}_i}\right)$ are the Artin symbols from Definition 3.10.

The Artin symbol induces a map

$$\psi_{L/K,\mathfrak{m}} : A_\mathfrak{m} \to \mathrm{Gal}(L/K)$$

called the *Artin map*.

Observe that this definition makes sense since $\mathfrak{p}_i$ are unramified in L. Moreover, it indeed generalizes the definition for unramified extensions, since for $\mathfrak{m} = 1$ we have $A_\mathfrak{m} = I_K$. Now we are going to see that it also generalizes Definition 3.3 saying that, in case of an extension $L/\mathbb{Q}$, the *Artin symbol* for an element $a \in C_m = (\mathbb{Z}/m\mathbb{Z})^\times$ is the restriction of the map $\zeta_m \mapsto \zeta_m^a$ to L.

Lemma 3.23. *Let $L/\mathbb{Q}$ be an abelian extension, $L \subset \mathbb{Q}(\zeta_m)$ and $(\alpha) \in A_{\mathfrak{m}}$ where $\mathfrak{m} = (m)v_\infty$; that is, $\alpha \in \mathbb{Q}^\times$ with numerator and denominator coprime with m. Then*

$$\left(\frac{L/\mathbb{Q}}{(\alpha)}\right) = \left(\frac{L}{\varphi(\alpha)}\right)$$

where φ is the map from the proof of Lemma 3.21 and $\left(\frac{L}{\varphi(\alpha)}\right)$ is the Artin symbol from Definition 3.3, i.e. the restriction of $\zeta_m \mapsto \zeta_m^{\varphi(\alpha)}$ to L.

Proof. We will prove the statement in three steps:

- Let us first prove it for $L = \mathbb{Q}(\zeta_m)$ and $\alpha = p \in \mathbb{Z}$ where p is a prime number such that $p \nmid m$. Then we know that $\mathcal{O}_L = \mathbb{Z}[\zeta_m]$ and that each automorphism of $\mathbb{Q}(\zeta_m)$ is determined by $\zeta_m \mapsto \zeta_m^a$ where $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

  We want to show that $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(p)}\right) = \left(\frac{\mathbb{Q}(\zeta_m)}{\varphi(p)}\right)$. To do this, we need to check that **if** for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ the map $\left(\frac{\mathbb{Q}(\zeta_m)}{a}\right) : \zeta_m \mapsto \zeta_m^a$ satisfies the condition from Theorem 3.9, i.e.

$$\left(\frac{\mathbb{Q}(\zeta_m)}{a}\right)(\beta) \equiv \beta^p \pmod{\mathfrak{P}} \text{ for all } \beta \in \mathbb{Z}[\zeta_m] \text{ and } \mathfrak{P}|p,$$

  then necessarily $a \equiv p \pmod m$. It suffices to verify that for $\beta = \zeta_m$:

  Suppose that $a \not\equiv p \pmod m$ and $\zeta_m^a \equiv \zeta_m^p \pmod{\mathfrak{P}}$. Then $\zeta_m^{a-p} \equiv 1 \pmod{\mathfrak{P}}$, and so $\zeta_m^{a-p} - 1 \equiv 0 \pmod{\mathfrak{P}}$. However, $(\zeta_m^{a-p} - 1) \mid m$ in $\mathbb{Z}[\zeta_m]$, and so it divides both $\mathfrak{P}$ and $m\mathbb{Z}[\zeta_m]$ as an ideal. But since $\mathfrak{P}$ is a prime ideal, this means that $\mathfrak{P} \mid m\mathbb{Z}[\zeta_m]$, and also that $(\mathfrak{P} \cap \mathbb{Z}) \mid (m\mathbb{Z}[\zeta_m] \cap \mathbb{Z})$ in $\mathbb{Z}$. Therefore, $p \mid m$, which contradicts our assumption $p \nmid m$.

- Now, for general field $L \subset \mathbb{Q}(\zeta_m)$ we have $\left(\frac{L/\mathbb{Q}}{(p)}\right) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(p)}\right)|_L$ by definition of Artin symbol, and so

$$\left(\frac{L/\mathbb{Q}}{(p)}\right) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(p)}\right)|_L = \left(\frac{\mathbb{Q}(\zeta_m)}{\varphi(p)}\right)|_L = \left(\frac{L}{\varphi(p)}\right).$$

- For general $(\alpha) = \prod_i (p_i)^{r_i}$ where $p_i \nmid m$ and $r_i \in \mathbb{Z}$ for each i we can write

$$\left(\frac{L/\mathbb{Q}}{(\alpha)}\right) = \prod_i \left(\frac{L/\mathbb{Q}}{(p_i)}\right)^{r_i} = \prod_i \left(\frac{L}{\varphi(p_i)}\right)^{r_i} = \left(\frac{L}{\varphi(\alpha)}\right)$$

  by multiplicativity of the map $\zeta_m \mapsto \zeta_m^a$.

□

Notation. For an extension L/K and a modulus $\mathfrak{m}$ of K, let $A_{L,\mathfrak{m}}$ denote the subgroup of I_L consisting of all fractional ideals such that their prime factorization do not contain any prime ideal dividing $\mathfrak{m}_0\mathcal{O}_L$. Similarly, we define

- $H^0_{L,\mathfrak{m}}$ to be the set of all fractional ideals $(\alpha) \in A_{L,\mathfrak{m}}$ satisfying
  (1) $\alpha \equiv 1 \pmod{\mathfrak{m}_0\mathcal{O}_L}$,
  (2) $\delta(\alpha) > 0$ for each $\delta \mid \sigma$ where σ occurs in $\mathfrak{m}_\infty$,

- $C_{L,\mathfrak{m}} = A_{L,\mathfrak{m}}/H^0_{L,\mathfrak{m}}$.

Observe that the ideal norm $\mathcal{N}_{L/K} : I_L \to I_K$ restrited to $A_{L,\mathfrak{m}}$ gives the norm map $\mathcal{N}_{L/K} : A_{L,\mathfrak{m}} \to A_{\mathfrak{m}}$ which we will now extend to $\mathcal{N}_{L/K} : C_{L,\mathfrak{m}} \to C_{\mathfrak{m}}$. For a prime ideal $\mathfrak{P} \in A_{L,\mathfrak{m}}$, set

$$\mathcal{N}_{L/K}(\mathfrak{P}H^0_{L,\mathfrak{m}}) = \mathcal{N}_{L/K}(\mathfrak{P})H^0_{\mathfrak{m}} \subset C_{\mathfrak{m}}$$

where $\mathfrak{P}H^0_{L,\mathfrak{m}}$ is the image of $\mathfrak{P}$ in $C_{L,\mathfrak{m}} = A_{L,\mathfrak{m}}/H^0_{L,\mathfrak{m}}$ and $\mathcal{N}_{L/K}(\mathfrak{P})H^0_{\mathfrak{m}}$ is the image of $\mathcal{N}_{L/K}(\mathfrak{P})$ in $C_{\mathfrak{m}} = A_{\mathfrak{m}}/H^0_{\mathfrak{m}}$ under the canonical projections. Then extend the norm multiplicatively to the whole $C_{L,\mathfrak{m}}$. Since it can be verified that $\mathcal{N}_{L/K}(H^0_{L,\mathfrak{m}}) \subset H^0_{\mathfrak{m}}$, the induced map on the quotient is well-defined.

Lemma 3.24. [9, Chapter V, Section 3] *Let L/K be a finite abelian extension and let $\mathfrak{m}$ be a modulus of K. Then $\mathcal{N}_{L/K}(A_{L,\mathfrak{m}}) \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$.*

We state the key result of CFT in the same way as you can find it in [9, Chapter V, Section 3].

Theorem 3.25 (Artin Reciprocity Law)**.** *Let L/K be a finite abelian extension. Then there is a modulus $\mathfrak{m}$ of K divisible by all the primes which ramify in L (and possibly some others) such that $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$ and for which the Artin map $\psi_{L/K,\mathfrak{m}}$ induces an isomorphism*

$$A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \cong \mathrm{Gal}(L/K).$$

Remark. For some authors the Artin Reciprocity Law means a weaker version giving the existence of $\mathfrak{m}$ such that $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$. In this formulation we give the precise description of the kernel.

The condition $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$ can be replaced by saying that $\mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$.

The quotient $A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}}))$ from the Theorem above can be rewritten as follows:

$$A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \cong (A_{\mathfrak{m}}/H^0_{\mathfrak{m}})/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})/H^0_{\mathfrak{m}}) \cong C_{\mathfrak{m}}/I_{L/K,\mathfrak{m}}$$

where $I_{L/K,\mathfrak{m}} = \mathcal{N}_{L/K}(C_{L,\mathfrak{m}}) \subset C_{\mathfrak{m}}$. Hence, we obtain the isomorphism

$$C_{\mathfrak{m}}/I_{L/K,\mathfrak{m}} \cong \mathrm{Gal}(L/K).$$

Recall that for the Hilbert class field $\widetilde{K}$ we have $\mathrm{Gal}(\widetilde{K}/K) \cong Cl_K$. Considering general extension L/K instead of the Hilbert class field motivates the following definition:

Definition 3.26. A *generalized ideal class group modulo* $\mathfrak{m}$ is any quotient of the ray class group $C_{\mathfrak{m}}$.

Equivalently (up to group isomorphism), we can say that a generalized ideal class group is any quotient $A_{\mathfrak{m}}/H_{\mathfrak{m}}$ where $H_{\mathfrak{m}}$ is some congruence subgroup for $\mathfrak{m}$.

To sum up, $A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \cong C_{\mathfrak{m}}/I_{L/K,\mathfrak{m}}$ is a generalized ideal class group modulo $\mathfrak{m}$ and $I_{L/K,\mathfrak{m}}$ is a generalization of the subgroup $I_{L,\mathfrak{m}}$ of C_m from Section 3.1.

Let us continue towards generalization of the defining modulus from Section 3.1 and the Hilbert class field from Section 3.2.

Definition 3.27. A *defining modulus for* L/K is any modulus $\mathfrak{m}$ satisfying the condition in Theorem 3.25, i.e.

- it is divisible by all primes which ramify in L,
- $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$.

The following theorem states, in some sense, the "converse" of Artin Reciprocity Law. It is again adopted from [9, Chapter V, Section 3].

Theorem 3.28 (Existence Theorem)**.** *Let K be a number field. Then for each modulus $\mathfrak{m}$ of K and each congruence subgroup $H_{\mathfrak{m}}$ for the modulus $\mathfrak{m}$ there is a unique abelian extension L/K such that*

- *L/K is unramified at all primes which do not divide $\mathfrak{m}$,*
- *$H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}}) = H_{\mathfrak{m}}$ or, equivalently, $I_{L/K,\mathfrak{m}} = H_{\mathfrak{m}}/H^0_{\mathfrak{m}}$.*

Choosing $H_{\mathfrak{m}} = H^0_{\mathfrak{m}}$, we get the unique abelian extension L/K such that such that it is unramified at all places not dividing $\mathfrak{m}$ and $C_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$.

Definition 3.29. The unique abelian extension of K such that $C_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$ is called the *ray class field modulo* $\mathfrak{m}$ and denoted by $K(\mathfrak{m})$.

Example 3.30. (a) Let us compute the ray class field of $K = \mathbb{Q}(i)$ for modulus $\mathfrak{m} = (1+i)$. Namely, we will show that $K(\mathfrak{m}) = K(1+i) = K$. Since

$$\mathrm{Gal}(K(1+i)/K) \cong C_{(1+i)} = A_{(1+i)}/H^0_{(1+i)}$$

we need to prove that $C_{(1+i)}$ is trivial, that means the inclusion $A_{(1+i)} \subset H^0_{(1+i)}$. Because $\mathcal{O}_K = \mathbb{Z}[i]$ is a principal ideal domain, all the fractional ideals of $K = \mathbb{Q}(i)$ are of the form $\alpha\mathbb{Z}[i]$ for $\alpha \in \mathbb{Q}(i)$, i.e. cyclic $\mathbb{Z}[i]$-modules. We will write (α) instead of $\alpha\mathbb{Z}[i]$ to be short. So we have that

$$\begin{aligned} A_{(1+i)} &= \{(\alpha) \mid \alpha \in \mathbb{Q}(i)^\times, \mathrm{ord}_{(1+i)}(\alpha) = 0\}, \\ H^0_{(1+i)} &= \{(\alpha) \in A_{(1+i)} \mid \alpha \equiv 1 \pmod{1+i}\}. \end{aligned}$$

Now, observe that $1+i \mid a+bi$ for $a, b \in \mathbb{Z}$ if and only if a, b have the same parity. Indeed,

$$\begin{aligned} &\exists\, x, y \in \mathbb{Z} \text{ such that } (1+i)(x+yi) = (x-y) + (x+y)i = a+bi \\ &\iff \exists\, x, y \in \mathbb{Z} \text{ such that } a = x-y, b = x+y \\ &\iff a, b \text{ have the same parity.} \end{aligned}$$

Take $(\alpha) \in A_{(1+i)}$. By the previous observation we can write $\alpha = \frac{a+bi}{c+di}$ with $a, b, c, d \in \mathbb{Z}$ such that $a+bi, c+di$ are coprime and the pairs a, b and c, d have different parity. This implies that $(a-c)$ and $(b-d)$ have the same parity, and hence, again by the observation, $1+i \mid (a-c)+(b-d)i$. In other words, $\frac{a+bi}{c+di} \equiv 1 \pmod{1+i}$ which concludes $(\alpha) \in H^0_{(1+i)}$.

(b) Let us show that the ray class field of $K = \mathbb{Q}(i)$ for modulus $\mathfrak{m} = (2) = (1+i)^2$ is again the field K itself. We have

$$A_{(2)} = \{(\alpha) \mid \alpha \in \mathbb{Q}(i)^\times, \mathrm{ord}_{(1+i)}(\alpha) = 0\}$$

$$H^0_{(2)} = \{(\alpha) \in A_{(2)} \mid \alpha \equiv 1 \pmod 2\}.$$

Again, take $\alpha = \frac{a+bi}{c+di} \in A_{(2)}$ with $a, b, c, d \in \mathbb{Z}$ such that $a+bi, c+di$ are coprime and the pairs a, b and c, d have different parity. Now, if a, c and b, d have both the same parity, then $2 \mid (a-c)+(b-d)i$, which means $\frac{a+bi}{c+di} \equiv 1 \pmod 2$, and so $(\alpha) \in H^0_{(2)}$. If a, c and b, d have both different parities then we can simply multiply α by i to come back to the first case. Since $(i\alpha) = (\alpha)$ and there are no more options for parities of a, c and b, d, we get that $(\alpha) \in H^0_{(2)}$ in any case.

Let us observe that the ray class field is the desired generalization of the cyclotomic field from the Kronecker-Weber theorem. We want to find the ray class field of $\mathbb{Q}$ for the modulus $\mathfrak{m} = (m)v_\infty$ where $m \in \mathbb{N}$ and v_∞ is the only infinite prime of $\mathbb{Q}$ corresponding to the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. An abelian extension L is the ray class field for $\mathbb{Q}$ modulo $\mathfrak{m}$ if and only if the map $\psi_{L/\mathbb{Q},\mathfrak{m}} : C_\mathfrak{m} \to \mathrm{Gal}(L/\mathbb{Q})$ is an isomorphism. By lemmas 3.21 and 3.23, this happens if and only if the map

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\to \mathrm{Gal}(L/\mathbb{Q}) \\ a &\mapsto (\zeta_m \mapsto \zeta_m^a)|_L\end{aligned}$$

is an isomorphism which is if and only if $L = \mathbb{Q}(\zeta_m)$.

In the same way we can see that the Hilbert class field is the ray class field for $\mathfrak{m} = 1$ and obtain the generalization from the other "direction" as well.

We promised a description of abelian extensions of a fixed number field K in terms of some "inner arithmetic" of K. In the case of abelian extensions of $\mathbb{Q}$, this "inner arithmetic" was a family of the groups $(\mathbb{Z}/m\mathbb{Z})^\times$, in the case of the unramified abelian extensions it was the ideal class group Cl_K. Now we consider it to be a family of the ray class groups $C_\mathfrak{m}$ and fulfil our promise by concluding everything we got in the following corollary:

Corollary 3.31. *Let $\mathfrak{m}$ be a modulus for the number field K. Then there is a one-to-one correspondence*

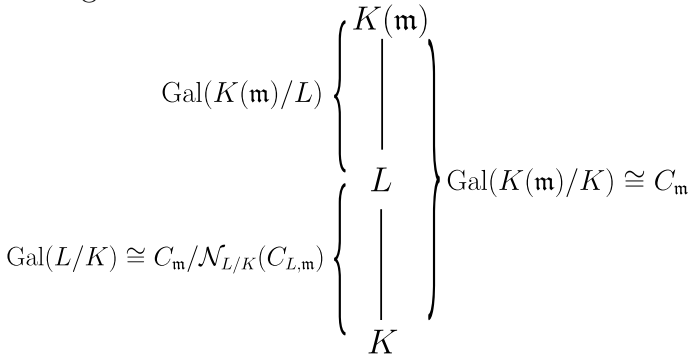
$$\{K \subset L \subset K(\mathfrak{m}) \mid L \text{ abelian extension of } K\} \longleftrightarrow \{\text{subgroups } H < C_\mathfrak{m}\}$$

where L corresponds to the subgroup $I_{L/K,\mathfrak{m}} = \mathcal{N}_{L/K}(C_{L,\mathfrak{m}})$ of $C_\mathfrak{m}$.

Moreover, this is an order reversing bijection, meaning that for two abelian extensions $L_1, L_2 \subset K(\mathfrak{m})$ of K we have

$$L_1 \subset L_2 \iff I_{L_1/K,\mathfrak{m}} \supset I_{L_2/K,\mathfrak{m}}.$$

Proof. All we have to show is that this correspondence coincides with the Galois correspondence, for which we have the order reversing property. In the Galois correspondence L corresponds to $\mathrm{Gal}(K(\mathfrak{m})/L)$. Why $\mathrm{Gal}(K(\mathfrak{m})/L) \cong \mathcal{N}_{L/K}(C_{L,\mathfrak{m}})$ is clear from this diagram:



□

3.4 Congruence divisor class groups, conductor

The goal of this section is to use a slightly different approach to build up the main statements of CFT. The notions involved are adopted from [2].

Whereas in the previous section our steps led from fixing an extension L/K to constructing an object it corresponds to, this approach starts with defining objects related to the base field K and then observing they give rise to certain abelian extensions of K. Specifically, our aim is to first define something called congruence divisor subgroup for the base field K and then attach a class field to each such group. Saying that each abelian extension arises in this way will again yield a correspondence we are looking for.

At the end of this section we go back to our original setting and define the conductor of a field extension. We do it in this section because the well-definedness will be clearer after what we do now.

Notation. For two moduli $\mathfrak{m} = \prod_v v^{i_v}, \mathfrak{n} = \prod v^{j_v}$ for some number field let $\mathfrak{m} \mid \mathfrak{n}$ denote the fact that $i_v \leq j_v$ for each place v.

When talking about moduli we sometimes omit "for some number field". We always consider moduli for some number field which is the same for all of them.

Lemma 3.32. *Suppose $\mathfrak{m} \mid \mathfrak{n}$ and let $H_\mathfrak{m}$ be a congruence subgroup for $\mathfrak{m}$. Then $H_\mathfrak{n} = H_\mathfrak{m} \cap A_\mathfrak{n}$ is a congruence subgroup for $\mathfrak{n}$ and*

$$A_\mathfrak{n}/H_\mathfrak{n} \simeq A_\mathfrak{m}/H_\mathfrak{m}.$$

Proof. First, observe that $A_\mathfrak{n} \subset A_\mathfrak{m}$ since prime ideals in factorizations of elements of $A_\mathfrak{n}$ do not divide $\mathfrak{n}$, and so they do not divide $\mathfrak{m}$ either. Similarly, $H^0_\mathfrak{n} \subset H^0_\mathfrak{m}$, and so $H^0_\mathfrak{n} \subset H^0_\mathfrak{m} \cap A_\mathfrak{n} \subset H_\mathfrak{m} \cap A_\mathfrak{n} = H_\mathfrak{n}$ which means that $H_\mathfrak{n}$ is indeed a congruence subgroup. Now, we can write

$$A_\mathfrak{n}/(H_\mathfrak{m} \cap A_\mathfrak{n}) \simeq A_\mathfrak{n}H_\mathfrak{m}/H_\mathfrak{m} = A_\mathfrak{m}/H_\mathfrak{m}$$

where the isomorphism is obtained by applying the third isomorphism theorem and the inclusion $A_\mathfrak{n}H_\mathfrak{m} \subset A_\mathfrak{m}$ is clear. For the other inclusion it suffices to show that $A_\mathfrak{m} \subset A_\mathfrak{n}H^0_\mathfrak{m}$.

Let $\mathfrak{m} = \prod_v v^{\mu_v}$ and take $I \in A_\mathfrak{m}$, say

$$I = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}} = \prod_{\mathfrak{p} \nmid \mathfrak{n}} \mathfrak{p}^{\nu_\mathfrak{p}} \cdot \prod_{\mathfrak{p} \mid \mathfrak{n}} \mathfrak{p}^{\nu_\mathfrak{p}} = I_1 \cdot I_2.$$

By Theorem 1.37 and the discreteness of a $\mathfrak{p}$-adic absolute value there exists $\beta \in K$ such that

- $\mathrm{ord}_\mathfrak{p}(\beta - 1) \geq \mu_\mathfrak{p}$ if $\mathfrak{p} \mid \mathfrak{m}$,
- $\mathrm{ord}_\mathfrak{p}(\beta) = \nu_\mathfrak{p}$ if $\mathfrak{p} \mid I_2$,
- $\mathrm{ord}_\mathfrak{p}(\beta) = 0$ if $\mathfrak{p} \nmid I, \mathfrak{p} \mid \mathfrak{n}$ and $\mathfrak{p} \nmid \mathfrak{m}$

where by $\mathfrak{p} \mid I$ we mean $\mathrm{ord}_\mathfrak{p} I \neq 0$. But then $I_1 \in A_\mathfrak{n}$ and also $\frac{I_2}{(\beta)} \in A_\mathfrak{n}$. At the same time, $(\beta) \in H^0_\mathfrak{m}$. Thus, the fractional ideal I can be written as a product of something from $A_\mathfrak{n}$ and something from $H^0_\mathfrak{m}$, as we wanted. □

Example 3.33. It might help to see an example illustrating the second part of the proof to grasp what is going on. Let $K = \mathbb{Q}$ and let

$$\begin{aligned}\mathfrak{m} &= (2)(3)^2,\\ \mathfrak{n} &= (2)^2(3)^2(5)(13)^2(19),\\ I &= (5)(7)(11)(13)^3 = (7)(11)\cdot(5)(13)^3 = I_1 \cdot I_2.\end{aligned}$$

Then, by Weak Approximation Theorem, there is $\beta \in \mathbb{Q}$ such that

- $\mathrm{ord}_2(\beta - 1) \geq 1, \mathrm{ord}_3(\beta - 1) \geq 2$; that is,
  $\beta \equiv 1 \pmod 2$ and $\beta \equiv 1 \pmod 9$,
- $\mathrm{ord}_5(\beta) = 1, \mathrm{ord}_{13}(\beta) = 3$; that is,
  $\beta \equiv 0 \pmod 5, \beta \not\equiv 0 \pmod{25}$ and $\beta \equiv 0 \pmod{13^3}, \beta \not\equiv 0 \pmod{13^4}$,
- $\mathrm{ord}_{19}(\beta) = 0$; that is,
  $\beta \not\equiv 0 \pmod{19}$ and $\frac{1}{\beta} \not\equiv 0 \pmod{19}$.

Then $I_1 \in A_{\mathfrak{n}}$ and also $\frac{I_2}{(\beta)} \in A_{\mathfrak{n}}$ (since $\mathrm{ord}_2(\beta) = \mathrm{ord}_3(\beta) = 0$) and $(\beta) \in H^0_{\mathfrak{m}}$.

Definition 3.34. Let $\mathfrak{m}_1, \mathfrak{m}_2$ be two moduli for a number field K and let $H_{\mathfrak{m}_1}, H_{\mathfrak{m}_2}$ be (some of) their associated congruence subgroups. We will call these two groups *equivalent* and write $H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2}$ if there is a common multiple $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ such that

$$A_{\mathfrak{m}} \cap H_{\mathfrak{m}_1} = A_{\mathfrak{m}} \cap H_{\mathfrak{m}_2}.$$

One can easily see that it is indeed an equivalence relation. We can come across various equivalent definitions of the equivalence of congruence subgroups (for example in [10]), let us include them as well.

Proposition 3.35. *The following statements are equivalent:*

1. $H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2}$
2. $A_{\mathfrak{m}_1}/H_{\mathfrak{m}_1} \cong A_{\mathfrak{m}_2}/H_{\mathfrak{m}_2}$
3. $A_{\mathfrak{m}_1} \cap H_{\mathfrak{m}_2} = A_{\mathfrak{m}_2} \cap H_{\mathfrak{m}_1}$

Proof. $1 \Rightarrow 2$: Let us take the common multiple $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ such that $A_{\mathfrak{m}} \cap H_{\mathfrak{m}_1} = A_{\mathfrak{m}} \cap H_{\mathfrak{m}_2}$. Then for $H_{\mathfrak{m}} = A_{\mathfrak{m}} \cap H_{\mathfrak{m}_1} = A_{\mathfrak{m}} \cap H_{\mathfrak{m}_2}$ we get that $A_{\mathfrak{m}_1}/H_{\mathfrak{m}_1} \cong A_{\mathfrak{m}}/H_{\mathfrak{m}} \cong A_{\mathfrak{m}_2}/H_{\mathfrak{m}_2}$ using Lemma 3.32.
$2 \Rightarrow 3$: Take $J \in A_{\mathfrak{m}_1} \cap H_{\mathfrak{m}_2}$. Since the image of J in $A_{\mathfrak{m}_2}/H_{\mathfrak{m}_2}$ under the projection map is trivial, J must also lie in $H_{\mathfrak{m}_1}$. Since $J \in H_{\mathfrak{m}_2} \subset A_{\mathfrak{m}_2}$ we get the inclusion $A_{\mathfrak{m}_1} \cap H_{\mathfrak{m}_2} \subset A_{\mathfrak{m}_2} \cap H_{\mathfrak{m}_1}$. The other inclusion follows from symmetry.
$3 \Rightarrow 1$: It holds for any common multiple $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ that $A_{\mathfrak{m}} \cap A_{\mathfrak{m}_1} = A_{\mathfrak{m}}$ and $A_{\mathfrak{m}} \cap A_{\mathfrak{m}_2} = A_{\mathfrak{m}}$. Hence, we obtain 1 by taking the intersections with $A_{\mathfrak{m}}$ on both left and right hand side. □

Remark. Let us get some intuition for the notion of this equivalence. Talking about equivalent congruence subgroups helps us to deal with the existence of more defining moduli for a field extension L/K. Let us have $\mathfrak{m}_1, \mathfrak{m}_2$ such that they are

both divisible by all primes which ramify in L and $H^0_{\mathfrak{m}_1} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}_1}), H^0_{\mathfrak{m}_2} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}_2})$. Now, by Artin Reciprocity Law,

$$A_{\mathfrak{m}_1}/\mathrm{Ker}(\psi_{L/K,\mathfrak{m}_1}) \cong \mathrm{Gal}(L/K) \cong A_{\mathfrak{m}_2}/\mathrm{Ker}(\psi_{L/K,\mathfrak{m}_2}).$$

Introducing the equivalence relation will remove the ambiguity in describing $\mathrm{Gal}(L/K)$ via identifying the kernels if and only if

$$A_{\mathfrak{m}_1}/\mathrm{Ker}(\psi_{L/K,\mathfrak{m}_1}) \cong A_{\mathfrak{m}_2}/\mathrm{Ker}(\psi_{L/K,\mathfrak{m}_2}).$$

Lemma 3.36. [10, Prop. 21.5] *Let $\mathfrak{m}_1, \mathfrak{m}_2$ be two moduli with congruence subgroups $H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2}$ and let $\mathfrak{m} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$. Then there is a congruence subgroup $H_{\mathfrak{m}}$ such that $H_{\mathfrak{m}} \sim H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2}$.*

Definition 3.37. The equivalence class (with respect to the isomorphism) of any quotient group $A_{\mathfrak{m}}/H_{\mathfrak{m}}$ is called a *congruence divisor class group* and denoted by A/H.

The *conductor* $\mathfrak{f}$ of A/H is then defined as the smallest $\mathfrak{m}$ (with respect to the ordering by divisibility), for which there is some $A_{\mathfrak{m}}/H_{\mathfrak{m}}$ belonging to the equivalence class A/H. Let us denote it by $\mathfrak{f}(A/H)$.

Note that the definition of conductor makes sense - the smallest such $\mathfrak{m}$ indeed exists by Lemma 3.36.

Definition 3.38. A finite algebraic extension L/K is called a *class field for A/H* if the prime ideals $\mathfrak{p}$ in K which split completely in L are precisely the elements of $H_{\mathfrak{f}}$ where $\mathfrak{f} = \mathfrak{f}(A/H)$ and $A_{\mathfrak{f}}/H_{\mathfrak{f}} \in A/H$.

Now we give the key result of CFT in terms of congruence divisor class groups, adopted from [2, Chapter V, Section 17].

Proposition 3.39. *Let K be a number field. There is a one-to-one correspondence*

$$\{L/K \text{ abelian extensions}\} \longleftrightarrow \{\text{congruence divisor class groups } A/H \text{ in } K\}$$

where L/K corresponds to the unique A/H for which L/K is a class field and A/H corresponds to the unique class field L/K for A/H.

Proof. We will show only the easy part - the uniqueness. We start with the uniqueness of A/H assigned to the abelian extension L/K. Suppose that there are $(A/H)^{(1)}, (A/H)^{(2)}$ such that L/K is a class field for both of them. Then we have $\mathrm{Spl}(L/K) = H_{\mathfrak{f}_1} = H_{\mathfrak{f}_2}$ where $\mathfrak{f}_1 = \mathfrak{f}((A/H)^{(1)}), \mathfrak{f}_2 = \mathfrak{f}((A/H)^{(2)})$ and $A_{\mathfrak{f}_1}/H_{\mathfrak{f}_1} \in (A/H)^{(1)}, A_{\mathfrak{f}_2}/H_{\mathfrak{f}_2} \in (A/H)^{(2)}$. Then all fractional ideals of $H_{\mathfrak{f}_1}$ are coprime with $\mathfrak{f}_2$ and vice versa, and therefore

$$A_{\mathfrak{f}_2} \cap H_{\mathfrak{f}_1} = H_{\mathfrak{f}_1} = H_{\mathfrak{f}_2} = A_{\mathfrak{f}_1} \cap H_{\mathfrak{f}_2}.$$

This means $A_{\mathfrak{f}_1}/H_{\mathfrak{f}_1} \cong A_{\mathfrak{f}_2}/H_{\mathfrak{f}_2}$ by Proposition 3.35 and so $(A/H)^{(1)} = (A/H)^{(2)}$.

The uniqueness of the class field for A/H follows immediately from Theorem 1.14. □

In Section 3.1 we defined the conductor of $L/\mathbb{Q}$ to be the smallest m such that $L \subset \mathbb{Q}(\zeta_m)$. We can define the conductor of L/K in the same manner:

Definition 3.40. The *conductor* $\mathfrak{f}_{L/K}$ of an abelian extension L/K is defined as the smallest defining modulus $\mathfrak{m}$ (with respect to the ordering by divisibility).

Again, this definition makes sense due to Lemma 3.36 and discussion in the remark above it.

And what is the relation between conductor of an extension and conductor of a congruence divisor class group? For an abelian extension L/K let A/H be the congruence divisor class group containing all quotients $A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}}))$ where $\mathfrak{m}$ is a defining modulus. Then $\mathfrak{f}(A/H) = \mathfrak{f}_{L/K}$. Indeed, the smallest $\mathfrak{m}$ such that there is a congruence subgroup $H_{\mathfrak{m}}$ with $A_{\mathfrak{m}}/H_{\mathfrak{m}} \in A/H$ is the same as the smallest $\mathfrak{m}$ such that $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$.

Prime decomposition

Now we turn our attention to the description of how primes decompose in a general abelian extension L/K. Recall that the conductor $\mathfrak{f}_{L/K}$ is the smallest modulus such that it is divisible by all primes which ramify in L and $H^0_{\mathfrak{m}} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$. It is true that it actually does not contain any other prime ideals than those which ramify:

Theorem 3.41. [7, Th. 7.15, Conductor-Ramification Theorem] *Let L/K be an abelian extension and $\mathfrak{p}$ be a prime ideal of K. Then*

$$\mathfrak{p} \text{ ramifies in } L \iff \mathfrak{p} \mid \mathfrak{f}_{L/K}.$$

As in the situation with extensions of $\mathbb{Q}$ we can again show that the set $\mathrm{Spl}(L/K)$ is determined by some congruence conditions.

Theorem 3.42. [7, Th. 7.18, Decomposition Theorem] *Let L/K be an abelian extension and $\mathfrak{m}$ be its defining modulus. If a prime ideal $\mathfrak{p}$ of K does not divide $\mathfrak{m}$, then the order of $\mathfrak{p}I_{L/K,\mathfrak{m}}$ in $C_{\mathfrak{m}}/I_{L/K,\mathfrak{m}}$ is f, the inertia degree of p.*

Consider an abelian extension L/K, its defining modulus $\mathfrak{m}$ and a prime ideal $\mathfrak{p}$ of K. We proceed completely analogously as in the case of extensions of $\mathbb{Q}$. It follows from Theorems 3.41 and 3.42 that $e = 1 \iff \mathfrak{p} \nmid \mathfrak{f}_{L/K}$ where e is a ramification index of $\mathfrak{p}$ and $f = 1 \iff \mathfrak{p} \in I_{L/K,\mathfrak{m}}$ for $\mathfrak{p} \nmid \mathfrak{m}$.

Let $\mathfrak{f} = \mathfrak{f}_{L/K}$. We obtain the following characterization of primes which split in terms of $\mathfrak{f}$ and $I_{L/K,\mathfrak{f}}$:

$$\mathfrak{p} \in \mathrm{Spl}(L/K) \iff e = f = 1 \iff \mathfrak{p} \nmid \mathfrak{f} \text{ and } \mathfrak{p} \in I_{L/K,\mathfrak{f}}.$$

And how to obtain the congruence conditions to describe $\mathrm{Spl}(L/K)$? Let $I_{L/K,\mathfrak{m}} = \{a_1 H^0_{\mathfrak{f}}, \ldots, a_j H^0_{\mathfrak{f}}\}$. Then we get

$$\mathfrak{p} \in \mathrm{Spl}(L/K) \iff p \equiv a_i \pmod{\mathfrak{f}} \text{ for some } 1 \leq i \leq j.$$

Let us conclude this chapter by giving a table summarizing the main concepts we introduced. The middle column contains general notions, left and right columns provide particular realizations in the special case of extensions of $\mathbb{Q}$ and in the special case of unramified extensions where we can consider just the trivial modulus.

$\boldsymbol{L/\mathbb{Q}}$ abelian	$\boldsymbol{L/K}$ general abelian	$\boldsymbol{L/K}$ unramified abelian
$m \in \mathbb{N}$ $\mathfrak{m} = (m)v_\infty$	$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ modulus of K	$\mathfrak{m} = 1$
the "inner arithmetic" of K		
$C_m = (\mathbb{Z}/m\mathbb{Z})^\times$	$C_\mathfrak{m} = A_\mathfrak{m}/H^0_\mathfrak{m}$ ray class group	$C_\mathfrak{m} = I_K/P_K = Cl_K$ ideal class group
Artin symbols and maps		
$\left(\frac{L}{a}\right) = (\zeta_m \mapsto \zeta_m^a)\vert_L$	$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$	$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$
$\left(\frac{L}{\cdot}\right) : C_m \to \mathrm{Gal}(L/\mathbb{Q})$	$\psi_{L/K,\mathfrak{m}} : A_\mathfrak{m} \to \mathrm{Gal}(L/K)$	$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$
Artin's Reciprocity Law		
$\mathrm{Gal}(L/\mathbb{Q}) \cong C_m/I_{L,m}$ $I_{L,m} = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/L)$	$\mathrm{Gal}(L/K) \cong C_\mathfrak{m}/I_{L/K,\mathfrak{m}}$ $I_{L/K,\mathfrak{m}} = \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})H^0_\mathfrak{m}$	$\mathrm{Gal}(L/K) \cong Cl_K$
Defining modulus		
any $m \in \mathbb{N}$ such that $L \subset \mathbb{Q}(\zeta_m)$	any $\mathfrak{m}$ such that $\mathfrak{p}$ ramifies in $L \Rightarrow \mathfrak{p}\vert\mathfrak{m}$ and $H^0_\mathfrak{m} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$	
Conductor		
$f_L =$ smallest $m \in \mathbb{N}$ such that $L \subset \mathbb{Q}(\zeta_m)$	smallest $\mathfrak{m}$ such that $\mathfrak{p}$ ramifies in $L \Rightarrow \mathfrak{p}\vert\mathfrak{m}$ and $H^0_\mathfrak{m} \subset \mathrm{Ker}(\psi_{L/K,\mathfrak{m}})$	
The ray class field		
$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\mathfrak{m})$ where $\mathfrak{m} = (m)v_\infty$	unique abelian $K(\mathfrak{m})/K$ s.t. $C_\mathfrak{m} \cong \mathrm{Gal}(K(\mathfrak{m})/K)$	$\widetilde{K} = K(1)$ Hilbert class field

4. Chevalley's reformulation

Let us look at what led Chevalley to reformulate the main results of CFT which we described in Section 3.3 in a different language. One (rather aesthetic) issue lies in considering many different moduli $\mathfrak{m}$ which makes comparing two abelian extensions L_1, L_2 of a number field K quite ugly. We know from Corollary 3.31 that we would have to compare the subgroups $I_{L_1,K,\mathfrak{m}_1} \subset C_{\mathfrak{m}_1}$ and $I_{L_2,K,\mathfrak{m}_2} \subset C_{\mathfrak{m}_2}$ via finding the common multiple $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ and then using the result saying that

$$L_1 \subset L_2 \iff I_{L_1,K,\mathfrak{m}} \supset I_{L_2,K,\mathfrak{m}}.$$

In order to canonically realize abelian extensions, we have to fix a modulus $\mathfrak{m}$ first. Moreover the description will include only subfields of the ray class field modulo $\mathfrak{m}$. Considering the congruence divisor class groups A/H and applying the correspondence from Proposition 3.39 is not very nice either.

Language of idèles helps us to handle this inconvenience. This means, we are able to describe all abelian extensions at the same time, no matter what their defining moduli are.

4.1 Idèle norm

Before stating the Artin reciprocity law in terms of idèles, let us do some preparatory work. Namely, we need to define a norm on the idèle class group $\mathcal{C}_K = \mathbb{I}_K/K^\times$ introduced in Section 2.4.

Let L/K be a Galois extension. There is a natural injection

$$\begin{aligned} i : \mathbb{I}_K &\hookrightarrow \mathbb{I}_L \\ (a_v)_v &\mapsto (a_w)_w \end{aligned}$$

where $a_w = a_v$ for all places w lying above v. We identify $\mathbb{I}_K$ with its image in $\mathbb{I}_L$ and write $\mathbb{I}_K \subset \mathbb{I}_L$.

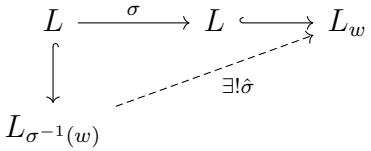
Now, the element $\sigma \in \mathrm{Gal}(L/K)$ induces a natural group action on $\mathbb{I}_L$, namely the map $\sigma : \mathbb{I}_L \to \mathbb{I}_L$ defined coordinate-wise as

$$(\sigma((a_v)_v))_w = \hat{\sigma}(a_{\sigma^{-1}(w)})$$

where $\hat{\sigma}$ is the unique homomorphism

$$\hat{\sigma} : L_{\sigma^{-1}(w)} \to L_w$$

extending $L \xrightarrow{\sigma} L \hookrightarrow L_w$ (and preserving the absolute value). The existence and the uniqueness follow from Theorem 1.39.



Definition 4.1. Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$. We define the *idèle norm* as the map

$$\begin{aligned} \mathcal{N}_{L/K} : \mathbb{I}_L &\to \mathbb{I}_K \\ (a_v)_v &\mapsto \prod_{\sigma \in G} \sigma((a_v)_v). \end{aligned}$$

Remark. The idèle norm can be alternatively defined by

$$(\mathcal{N}_{L/K}((a_w)_w))_v = \prod_{w|v} \mathrm{N}_{L_w/K_v}(a_w)$$

for $(a_w)_w \in \mathbb{I}_L$, as claimed in [6]. This helps to see that the image $\mathcal{N}_{L/K}(\mathbb{I}_L)$ indeed lies in $\mathbb{I}_K$.

Because we switched from the language of ideals to the language of idèles it would be nice to have some kind of compatibility of their norms.

The link between idèles and ideals is the map

$$\begin{aligned} \tau_K : \mathbb{I}_K &\to I_K \\ (a_v)_v &\mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})} \end{aligned}$$

where the product is taken over all prime ideals of $\mathcal{O}_K$. It is sometimes referred to as the *ideal map*, producing an ideal out of an idèle in the most natural way.

Lemma 4.2. [11, p. 2] *Let L/K be a Galois extension. Then the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{\tau_L} & I_L \\ \big\downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \big\downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ \mathbb{I}_K & \xrightarrow{\tau_K} & I_K \end{array}$$

Recall we have an embedding $K^\times \hookrightarrow \mathbb{I}_K$ sending $a \in K^\times$ to $(a_v)_v \in \mathbb{I}_K$ where $a_v = (a, a, a, \dots) \in K_v^\times$ which enables us to write $K^\times \subset \mathbb{I}_K$. We want to extend the definition of the idèle norm to the idèle class group $\mathcal{C}_K = \mathbb{I}_K / K^\times$.

Lemma 4.3. *Let L/K be a Galois extension. Then $\mathcal{N}_{L/K}(L^\times) \subset K^\times$ where $\mathcal{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ is the idèle norm.*

Proof. Let $(a_v)_v \in L^\times$ be an element having $(a, a, a \dots)$ at each coordinate of $\mathbb{I}_L$ for some $a \in L^\times$. By definition of $\mathcal{N}_{L/K}$, the diagram

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ \big\downarrow & & \big\downarrow \\ L_{\sigma^{-1}(w)} & \xrightarrow{\hat{\sigma}} & L_w \end{array}$$

commutes, and therefore, the element $(a_v)_v \in L^\times$ satisfies

$$\hat{\sigma}(a, a, a, \dots) = (\sigma(a), \sigma(a), \sigma(a) \dots)$$

for each $\sigma \in G = \mathrm{Gal}(L/K)$. Thus,

$$\mathcal{N}_{L/K}((a_v)_v) = \prod_{\sigma \in G} (a_w)_w$$

where $a_w = (\sigma(a), \sigma(a), \sigma(a), \dots)$, and so at each coordinate of $\mathcal{N}_{L/K}((a_v)_v)$ we have $(\prod_\sigma \sigma(a), \prod_\sigma \sigma(a), \prod_\sigma \sigma(a), \dots)$. This allows us to identify $\mathcal{N}_{L/K}((a_v)_v)$ with $\prod_\sigma \sigma(a)$ which lies in $K^\times$. □

As a consequence, the idèle norm extends naturally to

$$\mathcal{N}_{L/K} : \mathcal{C}_L \to \mathcal{C}_K$$

by sending $(a_v)_v L^\times$ to $\mathcal{N}_{L/K}((a_v)_v)K^\times$ where $(a_v)_v L^\times$ is the image of $(a_v)_v \in \mathbb{I}_L$ in $\mathcal{C}_L$ and $\mathcal{N}_{L/K}((a_v)_v)K^\times$ is the image of $\mathcal{N}_{L/K}((a_v)_v)$ in $\mathcal{C}_K$ under the canonical projections.

Moreover, the map $\tau_K : \mathbb{I}_K \to I_K$ induces $\tau_K : \mathcal{C}_K \to Cl_K$ as $\tau_K(K^\times) = P_K$, where we recall that P_K denotes the principal fractional ideals of K.

We have also the compatibility of norms of class groups:

Lemma 4.4. [11, p. 2] *Let L/K be a Galois extension. Then the following diagram commutes:*

$$\begin{array}{ccc} \mathcal{C}_L & \xrightarrow{\tau_L} & Cl_L \\ \downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \downarrow{\scriptstyle \mathcal{N}_{L/K}} \\ \mathcal{C}_K & \xrightarrow{\tau_K} & Cl_K \end{array}$$

4.2 Artin map and Artin reciprocity for idèles

In most of literature the Artin map on idèles is defined via local Artin maps. That would mean going into local class field theory, which we avoid by presenting the idèlic class field theory as developed in [3].

We wish to define the Artin map on idèles via composing the ideal map

$$\begin{aligned} \tau_K : \mathbb{I}_K &\to I_K \\ (a_v)_v &\mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})} \end{aligned}$$

with the Artin map on ideals. However, the Artin map on ideals is defined only for fractional ideals with no ramified primes in their prime factorizations. Therefore, we have to work with a defining modulus $\mathfrak{m}$ and consider an auxiliary subgroup $U_{\mathfrak{m}}$ of $\mathbb{I}_K$ which captures the information about the primes which ramify.

The strategy of defining the Artin map on idèles

$$\theta_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

goes as follows: We first introduce a subgroup of idèles $U_{\mathfrak{m}}$ for a modulus $\mathfrak{m}$ and define the Artin map on $U_{\mathfrak{m}}$. Then we claim that $\mathbb{I}_K = K^\times U_{\mathfrak{m}}$ and extend the definition to the whole $\mathbb{I}_K$ by setting $\theta_{L/K}((a_v)_v) = \theta_{L/K}((b_w)_w)$ where $(a_v)_v = k(b_w)_w$ with $k \in K^\times, (b_w)_w \in U_{\mathfrak{m}}$. Of course, the well-definedness needs to be verified.

Definition 4.5. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus for a number field K with $\mathfrak{m}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$. Then we set

$$U_\mathfrak{m} = \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 + \mathfrak{p}^{n_\mathfrak{p}}) \prod_{v|\mathfrak{m}_\infty} K_v^\circ \prod_{v\nmid\mathfrak{m}}{}' K_v^\times$$

where

- $1 + \mathfrak{p}^{n_\mathfrak{p}}$ is the ball with center 1 and radius $|\pi^{n_\mathfrak{p}}|_\mathfrak{p}$ and π is a uniformizer for $K_\mathfrak{p}$ with respect to $|\cdot|_\mathfrak{p}$,
- K_v° is the connected component of 1 in $K_v^\times$; that is, $K_v^\circ = (0, \infty)$ if v corresponds to a real embedding and $K_v^\circ = \mathbb{C}^\times$ if v corresponds to a pair of complex embeddings,
- $\prod'_{v\nmid\mathfrak{m}} K_v^\times$ is the restricted product with respect to the sets $\mathcal{O}_v^\times$.

Remark. Note that $U_\mathfrak{m}$ is a subgroup of $\mathbb{I}_K$ and that $\tau_K(U_\mathfrak{m}) \subset A_\mathfrak{m}$. Indeed, the order of all the primes dividing $\mathfrak{m}_0$ is 0. Moreover, $\tau_K : U_\mathfrak{m} \to A_\mathfrak{m}$ is surjective.

Lemma 4.6. [3, Section 4.1] *Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus for a number field K. Then*

$$\mathbb{I}_K = K^\times U_\mathfrak{m}.$$

Example 4.7. Let us prove Lemma 4.6 for a particular choice $K = \mathbb{Q}, \mathfrak{m} = (2)$. We have that

$$U_{(2)} = B_2(1, \tfrac{1}{2}) \prod_{v\neq 2}{}' \mathbb{Q}_v^\times$$

where $B_2(1, \frac{1}{2})$ is the ball with center 1 and radius $|2|_2 = \frac{1}{2}$ in $\mathbb{Q}_2$. Since the inclusion $\mathbb{I}_K \supset K^\times U_\mathfrak{m}$ is clear, we are left to show that

$$\mathbb{I}_\mathbb{Q} = \mathbb{Q}_2^\times \prod_{v\neq 2}{}' \mathbb{Q}_v^\times \subset \mathbb{Q}^\times B_2(1, \tfrac{1}{2}) \prod_{v\neq 2}{}' \mathbb{Q}_v^\times,$$

in other words, that $\mathbb{Q}_2^\times \subset \mathbb{Q}^\times B_2(1, \frac{1}{2})$.

Take $\boldsymbol{q} = (q_1, q_2, q_3, \dots) \in \mathbb{Q}_2^\times$ and let $|\boldsymbol{q}|_2 = \lim_{n\to\infty} |q_n|_2 = 2^z$ where $z \in \mathbb{Z}$. Let $\boldsymbol{q_n}$ denote the constant sequence $(q_n, q_n, q_n, \dots)$ in $\mathbb{Q}_2$ for every n. By discreteness of the 2-adic absolute value there exists n_0 such that for each $n \geq n_0$

- $\boldsymbol{q_n} \in B_2(\boldsymbol{q}, 2^{z-1})$,
- $|q_n|_2 = 2^z$.

For such n we can write $q_n = k_n 2^{-z}$ where $|k_n|_2 = 1$. By Remark 1.7,

$$\boldsymbol{q_n} \in B_2(\boldsymbol{q}, 2^{z-1}) \iff \boldsymbol{q} \in B_2(k_n 2^{-z}, 2^{z-1}) = B_2(2^{-z}, 2^{z-1}).$$

In fact, we do not need the existence of infinitely many n satisfying the two conditions above. The existence of one such n already yields $\boldsymbol{q} \in B_2(2^{-z}, 2^{z-1})$. But now,

$$\begin{aligned} B_2(2^{-z}, 2^{z-1}) &= \{a \in \mathbb{Q}_2 \mid |a - 2^{-z}|_2 < 2^{z-1}\} = \\ &= \{a \in \mathbb{Q}_2 \mid |2^{-z}\tfrac{a}{2^{-z}} - 2^{-z}|_2 < 2^{z-1}\} = \\ &= \{a \in \mathbb{Q}_2 \mid 2^z|\tfrac{a}{2^{-z}} - 1|_2 < 2^z\tfrac{1}{2}\} = \\ &= 2^{-z} B_2(1, \tfrac{1}{2}), \end{aligned}$$

and thus $\boldsymbol{q} \in 2^{-z} B_2(1, \frac{1}{2}) \subset \mathbb{Q}^\times B_2(1, \frac{1}{2})$.

Notation. For the inclusion map $\iota_K : U_\mathfrak{m} \to \mathbb{I}_K$ let us denote by

$$\bar{\iota}_K : U_\mathfrak{m} \to \mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L))$$

its composition with the quotient map.

Similarly, for $\tau_K : U_\mathfrak{m} \to A_\mathfrak{m}$ let us denote by

$$\overline{\tau}_K : U_\mathfrak{m} \to A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}}))$$

its composition with the quotient map.

The proof of the following theorem provides an explanation why we first define the Artin map on $U_\mathfrak{m}$ as an intermediate step.

Theorem 4.8. *Let L/K be a finite abelian extension and $\mathfrak{m}$ its defining modulus. Then there is an isomorphism*

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \cong A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})).$$

Proof. (sketch) Consider the maps

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \xleftarrow{\bar{\iota}_K} U_\mathfrak{m} \xrightarrow{\overline{\tau}_K} A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})).$$

The map $\bar{\iota}_K$ is surjective since, by Lemma 4.6, $U_\mathfrak{m} \cong \mathbb{I}_K/K^\times$. Also the map $\overline{\tau}_K$ is surjective as $\tau_K : U_\mathfrak{m} \to A_\mathfrak{m}$ is surjective. Hence, it suffices to show that $\mathrm{Ker}(\bar{\iota}_K) = \mathrm{Ker}(\overline{\tau}_K)$ because than the first isomorphism theorem implies the isomorphism from the statement. For the rest we refer to [3, Section 4.2, Thm. 6]. □

The Artin Reciprocity for ideals says that for a defining modulus $\mathfrak{m}$ the Artin map $\psi_{L/K,\mathfrak{m}}$ induces an isomorphism $A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \cong \mathrm{Gal}(L/K)$, and hence, by Theorem 4.8, we also have

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \cong A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \cong \mathrm{Gal}(L/K).$$

We want this isomorphism to be the map induced by the Artin map on idèles. In other words, we want to define the Artin map $\theta_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ such that the induced map $\theta_{L/K} : \mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K)$ coincides with the following composition of maps:

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \xrightarrow{\bar{\iota}_K^{-1}} U_\mathfrak{m}/\mathrm{Ker}\ \overline{\tau}_K \xrightarrow{\overline{\tau}_K} A_\mathfrak{m}/(H^0_\mathfrak{m} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \xrightarrow{\psi_{L/K,\mathfrak{m}}} \mathrm{Gal}(L/K)$$

After defining the Artin map on idèles we will show in Lemma 4.11 that this is indeed the case. Stating Artin Reciprocity Law on idèles; that is, the isomorphism

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \cong \mathrm{Gal}(L/K)$$

induced by the Artin map for idèles, will then be a consequence of Lemma 4.11 and Theorem 4.8.

Definition 4.9. Let L/K be a finite abelian extension and $\mathfrak{m}$ be its defining modulus. The *Artin map* on idèles is defined in two steps:

1. First, define

$$\theta_{L/K} : U_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$
$$(a_w)_w \mapsto \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$$

   where the product is taken over the finite primes only and we write $a_w = a_{\mathfrak{p}}$ if w corresponds to a prime ideal $\mathfrak{p}$.

2. For $(a_v)_v \in \mathbb{I}_K$ there is $k \in K^\times, (b_w)_w \in U_{\mathfrak{m}}$ such that $(a_v)_v = k(b_w)_w$ by Lemma 4.6. Define

$$\theta_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$
$$\theta_{L/K}((a_v)_v) = \theta_{L/K}((b_w)_w).$$

Remark. The well-definedness of the Artin map on idèles consists of the following parts:

(a) The Artin symbols are well-defined since all $\mathfrak{p}$'s for which $\mathfrak{p} \nmid \mathfrak{m}_0$ are unramified.

(b) The product $\prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$ is finite because all but finitely many coordinates of $(a_v)_v$ lie in $\mathcal{O}_v^\times$ and for such coordinates corresponding to finite places we have $\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}) = 0$.

(c) $\theta_{L/K}((a_v)_v)$ does not depend on the choice of $(b_w)_w \in U_{\mathfrak{m}}$. Suppose that $(a_v)_v = k(b_w)_w = l(c_w)_w$ with $k, l \in K^\times, (b_w)_w, (c_w)_w \in U_{\mathfrak{m}}$. We need to show that $\theta_{L/K}((b_w)_w) = \theta_{L/K}((c_w)_w)$. Indeed, we have $\theta_{L/K}((b_w)_w(c_w)_w^{-1}) = \theta_{L/K}(k^{-1}l)$ where $k^{-1}l \in K^\times \cap U_{\mathfrak{m}}$. However, $\tau_K(K^\times) = P_K$ and so $\tau_K(K^\times \cap U_{\mathfrak{m}})$ consists of principal fractional ideals which are congruent to 1 modulo $\mathfrak{m}$. Since $\mathfrak{m}$ is a defining modulus, the image of $\tau_K(K^\times \cap U_{\mathfrak{m}})$ under the Artin map for ideals is trivial.

(d) $\theta_{L/K}((a_v)_v)$ does not depend on the choice of a defining modulus. It can be shown that if $\mathfrak{m}_1, \mathfrak{m}_2$ are two defining moduli then $U_{\mathfrak{m}_1} \cap U_{\mathfrak{m}_2} = U_{\mathfrak{n}}$ where $\mathfrak{n}$ is the least common multiple of $\mathfrak{m}_1, \mathfrak{m}_2$ and $\mathfrak{n}$ is again a defining modulus.

Lemma 4.10. *Let L/K be a finite abelian extension. Then $K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L) \subset \mathrm{Ker}(\theta_{L/K})$. Thus, $\theta_{L/K}$ can be extended to $\theta_{L/K} : \mathbb{I}_K/K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L) \to \mathrm{Gal}(L/K)$.*

Proof. **(1)** We show $K^\times \subset \mathrm{Ker}(\theta_{L/K})$. Let $\mathfrak{m}$ be a defining modulus for L/K and $k \in K^\times$. Clearly, $1 \in U_{\mathfrak{m}}$ and $k = k \cdot 1$ where k on the left-hand side is considered to be an element of $\mathbb{I}_K$ and k on the right-hand side is just a scalar from $K^\times$. By definition of Artin map, we can write

$$\theta_{L/K}(k) = \theta_{L/K}(1) = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(1)} = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(\frac{L/K}{\mathfrak{p}}\right)^{0} = 1,$$

meaning $k \in \mathrm{Ker}(\theta_{L/K})$.

(2) By proof of [9, Chapter V, Prop. 5.2] the following diagram commutes:

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{\theta_{L/L}} & \mathrm{Gal}(L/L) \\ \big\downarrow{\scriptstyle \mathcal{N}_{L/K}} & & \big\downarrow \\ \mathbb{I}_K & \xrightarrow{\theta_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

This implies $\mathcal{N}_{L/K}(\mathbb{I}_L) \subset \mathrm{Ker}(\theta_{L/K})$ and completes the proof. □

Lemma 4.11. *Let L/K be a finite abelian extension and let $\mathfrak{m}$ be a defining modulus of L/K. Then the Artin map $\theta_{L/K}$ coincides with the compositions of maps $\psi_{L/K,\mathfrak{m}} \circ \overline{\tau}_K \circ \overline{\iota}_K^{-1}$ on $\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L))$.*

Proof. It will be all clear after writing down what both maps do. Take $(a_v)_v \in \mathbb{I}_K$ and consider its image under the projection map $\overline{(a_v)}_v \in \mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L))$. Then

$$\theta_{L/K}(\overline{(a_v)}_v) = \theta_{L/K}((a_v)_v) = \theta_{L/K}((b_w)_w) = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(b_{\mathfrak{p}})}$$

where $(b_w)_w$ is any element of $U_{\mathfrak{m}}$ such that $(a_v)_v(b_w)_w^{-1} \in K^\times$.

On the other hand, we have

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \xrightarrow{\overline{\iota}_K^{-1}} U_{\mathfrak{m}}/\mathrm{Ker}(\overline{\tau}_K) \xrightarrow{\overline{\tau}_K} A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}})) \xrightarrow{\psi_{L/K,\mathfrak{m}}} G$$

$$\overline{(a_v)}_v \quad \mapsto \quad \overline{(c_w)}_w \quad \mapsto \quad \overline{\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(c_{\mathfrak{p}})}} \quad \mapsto \quad \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(c_{\mathfrak{p}})}$$

where

- $(c_w)_w \in U_{\mathfrak{m}}$ is any element of $U_{\mathfrak{m}}$ such that $(a_v)_v(c_w)_w^{-1} \in K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)$ and $\overline{(c_w)}_w$ denotes its image in $U_{\mathfrak{m}}/\mathrm{Ker}(\overline{\tau}_K)$,
- $\overline{\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(c_{\mathfrak{p}})}}$ is the image of $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(c_{\mathfrak{p}})}$ in $A_{\mathfrak{m}}/(H^0_{\mathfrak{m}} \cdot \mathcal{N}_{L/K}(A_{L,\mathfrak{m}}))$.

But now, from the well-definedness of $\psi_{L/K,\mathfrak{m}} \circ \overline{\tau}_K \circ \overline{\iota}_K^{-1}$, for $(b_w)_w \in U_{\mathfrak{m}}$ such that $(a_v)_v(b_w)_w^{-1} \in K^\times \subset K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)$ and $(c_w)_w \in U_{\mathfrak{m}}$ such that $(a_v)_v(c_w)_w^{-1} \in K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)$ it must hold that $\prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(b_{\mathfrak{p}})} = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(c_{\mathfrak{p}})}$. □

Theorem 4.12 (Artin Reciprocity Law for idèles)**.** *Let L/K be a finite abelian extension and let $\mathfrak{m}$ be a defining modulus of L/K. Then the Artin map $\theta_{L/K}$ induces an isomorphism*

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \cong \mathrm{Gal}(L/K).$$

Proof. From Theorem 4.8 and the discussion below it, the isomorphism is induced by $\psi_{L/K,\mathfrak{m}} \circ \overline{\tau}_K \circ \overline{\iota}_K^{-1}$. By Lemma 4.11, this map coincides with the Artin map on $\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L))$. □

Remark. The quotient $\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L))$ from Theorem 4.12 can be rewritten as follows:

$$\mathbb{I}_K/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)) \cong (\mathbb{I}_K/K^\times)/(K^\times \cdot \mathcal{N}_{L/K}(\mathbb{I}_L)/K^\times) \cong C_K/\mathcal{N}_{L/K}(C_L).$$

Let us finish with idèlic analogies to ray class groups $C_{\mathfrak{m}}$ which are isomorphic to $\mathrm{Gal}(K(\mathfrak{m})/K)$ and groups $I_{L/K,\mathfrak{m}} = \mathcal{N}_{L/K}(C_{L,\mathfrak{m}})$ which are isomorphic to $\mathrm{Gal}(K(\mathfrak{m})/L)$. We want to replace the ray class field $K(\mathfrak{m})$ by the maximal abelian extension of K denoted by K^{ab}. We submit a short summary of what can be found for example in [7, Section 8].

Let us denote the connected component of 1 in C_K by D_K. Then $\mathcal{N}_{L/K} : C_L \to C_K$ induces $\mathcal{N}_{L/K} : C_L/D_L \to C_K/D_K$ via $\mathcal{N}_{L/K}(aD_L) = \mathcal{N}_{L/K}(a)D_K \in C_K/D_K$ where $a \in C_L$. Then the desired isomorphisms (including the Artin Reciprocity Law) are:

1. $\mathrm{Gal}(L/K) \cong C_K/\mathcal{N}_{L/K}(C_L)$,
2. $\mathrm{Gal}(K^{ab}/K) \cong C_K/D_K$,
3. $\mathrm{Gal}(K^{ab}/L) \cong (C_K/D_K)/(C_K/\mathcal{N}_{L/K}(C_L)) \cong \mathcal{N}_{L/K}(C_L/D_L)$.

Bibliography

[1] John W. S. Cassels and Albrecht Fröhlich. *Algebraic number theory*. Thompson Book Company, Washington, D.C., 1967.

[2] Henry P.F. Swinnerton-Dyer. *A brief guide to algebraic number theory*. Cambridge University Press, Cambridge, 2001.

[3] Freydoon Shadidi. Class field theory.
https://www.math.mcgill.ca/darmon/courses/18-19/cft/refs/shahidi.pdf.

[4] James S. Milne. Algebraic number theory (v3.08), 2020.
URL: https://www.jmilne.org/math/CourseNotes/ANTc.pdf.

[5] Keith Conrad. Ideal factorization.
URL: https://kconrad. math. uconn. edu/blurbs/gradnumthy/idealfactor. pdf.

[6] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer, New York City, 1999.

[7] Dennis Garbanati. Class field theory summarized. *The Rocky Mountain Journal of Mathematics*, 11(2):195–225, 1981.

[8] David A. Cox. *Primes of the form x2+ ny2*. John Wiley & Sons Inc., New York, 1989.

[9] James S. Milne. Class field theory (v4.03), 2020.
URL: https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[10] Andrew V. Sutherland. Statement of the theorems of global class field theory.
URL: https://math.mit.edu/classes/18.785/2015fa/LectureNotes21.pdf.

[11] Andrew V. Sutherland. Global class field theory, the chebotarev density theorem.
URL: https://math.mit.edu/classes/18.785/2015fa/LectureNotes25.pdf.

5. Vocabulary

We submit translations of selected notions into Czech. It might not be possible to find Czech literature on this topic; however, it might help in spoken conversations or just entertain Czech readers. However, we advise to take the expressions with a grain of salt as we suggest our own translations for some terms.

ramify	větvit se
split	štěpit se
adèles	adely
idèles	idely
idèle class group	idelová třídová grupa
content map	obsahové zobrazení
defining modulus	definující modulus
Artin symbol	Artinův symbol
Artin map	Artinovo zobrazení
Hilbert class field	Hilbertovo třídové těleso
congruence subgroup	kongruenční podgrupa
ray modulo m	paprsek modulo m
ray class group	paprsková třídová grupa
ray class field	paprskové třídové těleso
congruence divisor class group	třídová grupa kongruenčních divisorů
conductor	průvodič
ideal map	ideálové zobrazení