universität wien

MASTERARBEIT | MASTER'S THESIS

Titel | Title

On the Centre of the Absolute Galois Group of a Global Field

verfasst von | submitted by

Laura Chalabi BSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 821
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von | Supervisor:	Mag. Dr. Harald Grobner Privatdoz.

Abstract (Deutsch)

In dieser Arbeit wird bewiesen, dass das Zentrum der absoluten Galoisgruppe eines globalen Körpers trivial ist. Da die absolute Galoisgruppe im Allgemeinen eine unendliche Gruppe ist, wird dazu anfangs die Galoistheorie von unendlichen Körpererweiterungen eingeführt. Danach werden die Grundlagen der Bewertungstheorie behandelt, insbesondere Erweiterungen von Bewertungen von einem Grundkörper in einen Erweiterungskörper. Solche Erweiterungen werden mithilfe einer Untergruppe der Galoisgruppe beschrieben, die man Zerlegungsgruppe nennt. Schließlich wird die Trivialität des Zentrums der absoluten Galoisgruppe eines globalen Körpers mithilfe von Eigenschaften der Zerlegungsgruppe bewiesen.

Abstract (English)

In this thesis, it is proved that the absolute Galois group of a global field has trivial centre. This is done by means of the decomposition group, a subgroup of the absolute Galois group. In order to define it, valuations are introduced, and their extensions to algebraic field extensions are studied. Since the absolute Galois group is an infinite group, the thesis starts with a chapter devoted to the Galois correspondence in infinite Galois extensions.

Contents

1 Introduction

Since the 19^{th} century, Galois theory provides a link between field theory and group theory. It is nowadays indispensable in algebraic number theory, and in fact, its applications to modern mathematics transcend classical number theory vastly. The study of number theory has advanced rapidly in the past decades and it owes this development partly to the application of concepts in algebraic geometry and algebraic topology to problems in classical number theory - and vice versa.

One of these concepts is the Galois group of a field extension, specifically a certain type of field extension, namely the extension of a field by its separable closure. The separable closure $\overline{K}$ of a field K is defined as its maximal separable extension in the algebraic closure of K. The Galois group of such a field extension is called the absolute Galois group of K. The interesting questions arise in those cases when this group is infinite.

The absolute Galois group of the rational numbers $\mathbb{Q}$, for instance, is uncountable and far from being completely understood. The group is studied by means of its representations and possible links to algebraic geometry. A description of this group could provide huge insights into questions in algebraic geometry and topology, because it contains information about solutions of polynomials with rational coefficients.

In general, the absolute Galois group of a global field[1] is a complicated object. The goal of this thesis is to provide a little bit of insight into its structure by proving that the centre of the absolute Galois group of a global field is always trivial. This result validates the reasonable assumption that there are no extraordinary field extensions of global fields, which have Galois automorphisms that commute with all other Galois automorphisms.

Since the absolute Galois group of a global field is in general infinite, the first step in proving that its centre is trivial is defining the Galois theory of infinite field extensions. We recall that, in finite Galois extensions, there is a one-to-one correspondence between intermediate Galois extensions and subgroups of the Galois group. In infinite Galois extensions, this correspondence ceases to exist. Indeed, there are more subgroups of the Galois group than there are intermediate Galois extensions. The correspondence can be salvaged, however, by imposing a topology on the Galois group and restricting one's attention to *closed* subgroups of the Galois group. This is done in Chapter 2.

[1] A global field is a certain type of field that arises either as an algebraic number field or as a function field over a finite field. This will properly be defined in Section 3.4.

In Chapter 3, we introduce the theory of valuations. A valuation is a map on a field that provides a notion of the size of an element of that field. For example, the degree of a pole or the multiplicity of a zero of a function, as well as the degree of divisibility of an integer by a prime number can be generalised using valuations. Our main goal is to extend a valuation of a field K to a valuation of an algebraic field extension L of K. Specifically, we want L to be the separable closure $\overline{K}$. To do so, we first restrict to a specific kind of valued field before generalising the result to a more general class of fields. In Section 3.4, we then see that there is a natural analogy between valuations and prime ideals, and that we can switch between the two points of view. Finally, Section 3.5 explains how to change from a global situation to a local one, and vice versa. This provides a general way of extending valuations of a base field to an algebraic field extension.

Chapter 4 brings us back to Galois extensions, by introducing the decomposition group. The decomposition group is a subgroup of the Galois group and is attached to an extension of a valuation of a field K to an extension field L. In light of Section 3.4, it can be defined with regard to valuations, as well as to ideals. We also see that it has functorial properties that link it to the local situation introduced in Section 3.5.

Finally, in Chapter 5, we can prove that the centre of the absolute Galois group of a global field is trivial. This is done by linking the splitting fields of polynomials to prime ideals of the ring of integers of their coefficient field and by then using properties of the decomposition group. In the very last section, we then state the famous theorem of Neukirch and Uchida, the proof of which uses the fact that the absolute Galois group has trivial centre.

This thesis is by no means a complete introduction to infinite Galois theory or valuation theory. Especially valuation theory has more depths and applications than what is touched upon here. The results stated here, some of them without proof, are only those that are later used to prove the triviality of the centre of the absolute Galois group. For a more complete account of valuation theory, I recommend reading Chapter II of [7]. Moreover, an introduction to how Galois theory can be used to approach problems in algebraic geometry and algebraic topology can be found in [8].

Lastly, I would like to express my profound gratitude to my supervisor Harald Grobner, for his continuous support and encouragement. I could not have wished for a better supervisor. Also, thank you to the psychological counseling service for students, and to my friends and family, who have helped me through this long and difficult time. Specifically, I would like to thank Anna Gütl and Felix Sefzig, for years of invaluable help, unwavering support, and heartfelt friendship.

2 Infinite Galois Theory

In Galois theory, there is a one-to-one correspondence between the intermediate Galois extensions of a *finite* Galois extension, and the subgroups of its Galois group. In this section, we see that such a correspondence fails when considering infinite Galois extensions. To tackle this problem, we then introduce a topology on the Galois group and prove an analogue correspondence for infinite Galois extensions, which is restricted to only closed subgroups.

2.1 Field Theory

We begin with a short recap of the necessary concepts of field and Galois theory. Unless otherwise noted, this subsection follows §I.1 of [1].

Definition. Let K be a field. A **field extension** of K is a pair (L, ε) consisting of a field L and a (necessarily injective) ring morphism $\varepsilon : K \to L$, i.e. a field L containing a subfield isomorphic to K. The extension is denoted by L/K.

For two field extensions (L_1, ε_1) and (L_2, ε_2) of K, we define a **morphism** $\iota : (L_1, \varepsilon_1) \to (L_2, \varepsilon_2)$ **of field extensions** as a ring morphism $u : L_1 \to L_2$ such that $u \circ \varepsilon_1 = \varepsilon_2$. The morphism ι is also called a K**-embedding** of L_1 into L_2.

A bijective morphism of field extensions is an **isomorphism** of field extensions and the isomorphism ι is called a K**-isomorphism** of L_1 onto L_2.

K is usually identified with its image $\varepsilon(K)$ and considered as a subfield of L. Therefore, we will henceforth simply write K instead of $\varepsilon(K)$.

Definition. Let L/K be a field extension. The dimension of L as a K-vector space is called the **degree** of L/K and is denoted by $[L : K]$.

Definition. If L/K is a field extension and $A \subseteq L$ is a subset, then we denote by $K[A]$ the **subring of** L **generated by** A over K, i.e. the smallest subring of L containing A and K.

Similarly, $K(A)$ denotes the **subextension of** L **generated by** A over K, i.e. the smallest subfield of L containing A and K.

If $A = \{\alpha_1, \ldots, \alpha_n\}$, then $K[A]$ is denoted by $K[\alpha_1, \ldots, \alpha_n]$ and $K(A)$ is denoted by $K(\alpha_1, \ldots, \alpha_n)$.

Definition. If L/K is a field extension and L_1, L_2 are two subfields of L both containing K, then the **composite** of L_1 and L_2 is the subfield generated by $L_1 \cup L_2$ and is denoted by $L_1 L_2$.

Definition. If L/K is a field extension and $\alpha \in L$, then we say that an *element* α is **algebraic** over K if there exists a non-zero polynomial $P \in K[x]$ such that $P(\alpha) = 0$. Conversely, an *element* α is called **transcendental** if such a non-zero

polynomial does not exist. A *field extension* L/K is **algebraic** if every element of L is algebraic over K and **transcendental** if there exists an element in L that is transcendental over K.

Let L/K be a field extension and $\alpha \in L$. Then $I_\alpha = \{P \in K[x] | P(\alpha) = 0\}$ is an ideal of $K[x]$ and is non-zero if and only if α is algebraic over K. In this case, there exists a unique monic irreducible polynomial $\mu_{\alpha,K}$ such that $I_\alpha =< \mu_{\alpha,K} >$. This polynomial is called the **minimal polynomial of α over K**.

Proposition 2.1. *Let L/K be a field extension. An element $\alpha \in L$ is algebraic over K if and only if $K(\alpha)/K$ has finite degree. In this case, $1, \alpha, \ldots, \alpha^{d-1}$, where $d = \deg(\mu_{\alpha,K})$ form a K-basis of $K(\alpha)$. In particular, $[K(\alpha) : K] = \deg(\mu_{\alpha,K})$.*

These results and their proofs can be found in [5], Proposition I.1.15 and Corollary I.1.22.

Definition. A field K is said to be **algebraically closed** if every non-constant polynomial with coefficients in K has a root in K. An algebraic field extension K^{alg}/K such that K^{alg} is algebraically closed is called an **algebraic closure** of K.

Every field has an algebraic closure and it is unique up to isomorphism ([4], Theorem V.3.6).

Definition. Let K^{alg} be a fixed algebraic closure of a field K. We say that a *polynomial* $f \in K[x]$ is **separable** if it has no multiple roots in K^{alg}. In a field extension L/K, an *element* $x \in L$ is called **separable** over K if x is algebraic over K and its minimal polynomial over K is separable. An *extension* L/K is **separable** if every element of L is separable over K.

Remark. One can show that the composite of two separable extensions is separable (Proposition IV.5.11 in [3]) and that the extension $K(\alpha_1, \ldots, \alpha_n)/K$ is separable if and only if all $\alpha_1, \ldots, \alpha_n$ are separable elements over K (Proposition IV.5.6 in [3]).

Definition. The **separable closure** $\overline{K}$ of K in K^{alg} is the maximal separable extension of K in K^{alg}, i.e. the maximal subfield of K^{alg} such that $\overline{K}/K$ is a separable extension. It consists of all elements in K^{alg} which are separable over K.

Finite field extensions are algebraic but the converse is not true in general. There are algebraic extensions of infinite degree.

Example. The field of algebraic numbers

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a \text{ is algebraic over } \mathbb{Q}\}$$

is an infinite algebraic extension of the rational numbers $\mathbb{Q}$ ([5], Corollary I.1.22 and the discussion after it). Since it is a subfield of the field of complex numbers $\mathbb{C}$, and $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra, Proposition 13.31 in [2] implies that $\overline{\mathbb{Q}}$ is algebraically closed. Recall that the rational numbers $\mathbb{Q}$ form a perfect field and that this is defined as a field of which every algebraic extension is separable ([5], Definition I.4.11 and Example I.4.12). Therefore, the field $\overline{\mathbb{Q}}$ serves as the algebraic as well as the separable closure of $\mathbb{Q}$.

Definition. For two fields K_1 and K_2, a ring morphism $\iota : K_1 \to K_2$ between them and two corresponding field extensions L_1/K_1 and L_2/K_2, we call a ring morphism $\varphi : L_1 \to L_2$ an **extension** of ι if the following diagram commutes:

$$\begin{array}{ccc} L_1 & \xrightarrow{\varphi} & L_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow{\iota} & K_2 \end{array}$$

Notation. Let K_1, K_2 and ι be as in the definition above and let $P \in K_1[x]$, $P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$. Then we denote by $\iota(P)$ the element of $K_2[x]$ defined by $\iota(a_n)X^n + \ldots + \iota(a_0)$.

The following results are useful for describing Galois extensions.

Lemma 2.2. *Let K_1 and K_2 be two fields, L_1/K_1 a field extension, $\iota : K_1 \to K_2$ a ring morphism, and $\alpha \in L_1$. Then for every extension $\varphi : L_1 \to K_2^{alg}$ of ι, $\varphi(\alpha)$ is a root of $\iota(\mu_{\alpha,K_1})$.*

Proof. We can write $\mu_{\alpha,K_1} = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. Because φ is an extension of ι, we have by definition $\iota(\mu_{\alpha,K_1}) = X^n + \varphi(a_{n-1})X^{n-1} + \ldots + \varphi(a_0)$.

But φ is a ring morphism, so we get

$$\iota(\mu_{\alpha,K_1})(\varphi(\alpha)) = \varphi(\mu_{\alpha,K_1}(\alpha)) = \varphi(0) = 0,$$

which proves that $\varphi(\alpha)$ is a root of $\iota(\mu_{\alpha,K_1})$. □

Theorem 2.3. ***(Isomorphism Extension Theorem)*** *Let K_1, K_2 be two fields and let $\iota : K_1 \to K_2$ be a field isomorphism. Let $S_1 = \{f_i(x)\}$ be an arbitrarily large set of polynomials over K_1, and let $S_2 = \{\iota(f_i)\}$ be the corresponding set over K_2. Let L_1 be a splitting field for S_1 over K_1, and let L_2 be a splitting field for S_2 over K_2. Then there exists an extended isomorphism $\varphi : L_1 \to L_2$ such*

that $\varphi|_{K_1} = \iota$. *Moreover, if* $\alpha \in L_1$ *and* α' *is a root of* $\iota(\mu_{\alpha,K_1})$, *then* φ *can be chosen so that* $\varphi(\alpha) = \alpha'$.

The proof of the Isomorphism Extension Theorem can be found in [5], Theorem I.3.20.

The following proposition is a direct consequence of the Isomorphism Extension Theorem, Theorem 2.3, because the algebraic closure of a field is the splitting field of all irreducible polynomials over that field.

Proposition 2.4. *Let* K_1, K_2 *be two fields,* $\iota : K_1 \to K_2$ *a ring morphism,* $\alpha \in K_1^{alg}$ *and let* β *be a root of* $\iota(\mu_{\alpha,K_1})$ *in* K_2^{alg}. *Then there exists a unique extension* $\varphi : K_1(\alpha) \to K_2^{alg}$ *of* ι *such that* $\varphi(\alpha) = \beta$. *In particular, there is a bijection between the set of extensions of* ι *and the set of roots of* $\iota(\mu_{\alpha,K_1})$.

The next theorem follows immediately from Proposition 2.4 by applying the proposition inductively.

Theorem 2.5. *Let* K *be a field,* L/K *an algebraic field extension,* M *an algebraically closed field, and let* $\tau : K \to M$ *be a ring morphism. Then there exists a ring morphism* $\sigma : L \to M$ *such that* $\sigma|_K = \tau$, *i.e. there exists an extension* $\sigma : L \to M$ *of* τ.

Corollary 2.6. *Let* K_1 *and* K_2 *be two fields and let* $\iota : K_1 \to K_2$ *be a ring morphism. Then there exists an extension* $\varphi : \overline{K_1} \to \overline{K_2}$ *of* ι *to the separable closures.*

Proof. Let τ be the composition of ι with the inclusion $K_2 \subseteq K_2^{alg}$. Theorem 2.5 implies that there exists an extension $\varphi : \overline{K_1} \to K_2^{alg}$ such that $\varphi|_{K_1} = \tau$. To prove that φ is the desired extension between separable closures, we must show that $\varphi(\overline{K_1}) \subseteq \overline{K_2}$.

Take $\alpha \in \overline{K_1}$, so that μ_{α,K_1} has n distinct roots in K_1^{alg} and denote them by $\alpha = \alpha_1, \ldots, \alpha_n$. Now define $P = \tau(\mu_{\alpha,K_1})$. Since for all i, we have $\mu_{\alpha,K_1} = \mu_{\alpha_i,K_1}$, we know by Lemma 2.2 that $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ are roots of P, but P and μ_{α,K_1} have the same degree and φ is injective, so P must be separable. Since $\varphi(\alpha)$ is a root of P, P must be divisible by $\mu_{\varphi(\alpha),K_2}$. This implies that $\mu_{\varphi(\alpha),K_2}$ has no multiple roots and, thus, $\varphi(\alpha)$ is separable over K_2, which means that $\varphi(\overline{K_1}) \subseteq \overline{K_2}$, as claimed. □

2.2 Galois Extensions

After having seen some general results on field extensions, we now turn to the Galois case. The primary source for this subsection is §I.2 in [1]. We recall:

Definition. A field extension L/K (contained in K^{alg}) is said to be **normal** if, for every K-linear embedding $\sigma : L \to K^{alg}$, we have $\sigma(L) = L$, i.e. σ is a K-automorphism of L.

A **Galois extension** is an algebraic field extension that is both separable and normal.

If the field extension L/K is Galois, we can define the **Galois group** $\mathrm{Gal}(L/K)$ of L/K as the group of all K-automorphisms of L/K:

$$\mathrm{Gal}(L/K) = \{\sigma : L \to L \text{ isomorphism} \mid \sigma(a) = a \text{ for all } a \in K\}.$$

Notation. Let L be a field and let $G \leq \mathrm{Aut}(L)$ be a subgroup of the automorphism group of L. We denote the subfield of L, consisting of those elements of L that are fixed by all automorphisms of G, by L^G:

$$L^G = \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in G\}.$$

Remark. Note that the above definition of a Galois extension does not assume the field extension to be finite.

Example. Let K be a field and $K^{alg} \neq K$ its algebraic closure. Let L be a field $K \subset L \subseteq K^{alg}$ such that $L = K(\alpha)$ for some $\alpha \in K^{alg} - K$ that satisfies $\alpha^2 \in K$. Then the quadratic extension L/K is Galois.

Example. Let $\alpha \in K^{alg}$ be separable over K, $\alpha = \alpha_1, \ldots, \alpha_n$ be the n distinct roots of $\mu_{\alpha,K}$ in K^{alg}, and $L = K(\alpha_1, \ldots, \alpha_n)$. Then L/K is a finite Galois extension.

To see why, note that the α_i's are all separable over K, because they all have the same minimal polynomial, and that, thus, $K(\alpha_1, \ldots, \alpha_n)/K$ is separable by the remark on page 4. Let now $\sigma : L \to K^{alg}$ be a K-embedding. Lemma 2.2 then implies that $\sigma(\alpha_i)$ is one of the α_j's, which makes it an element of L. Thus, $\sigma(L) \subseteq L$. As L is a finite-dimensional K-vector space and $\sigma : L \to L$ is K-linear and injective, σ must be bijective, which proves that L/K is Galois.

Lemma 2.7. *If L/K is a Galois extension, $\alpha \in L$ and $\alpha_1 = \alpha, \ldots, \alpha_n$ are the roots of $\mu_{\alpha,K}$ in K^{alg}, then $\alpha_i \in L$ for all $i \in \{1, \ldots, n\}$.*

Proof. By taking $K = K_1 = K_2$ in Proposition 2.4, we know that, for every $i \in \{1, \ldots, n\}$, there exists a unique K-embedding $\tau_i : K(\alpha) \to K^{alg}$ such that $\tau_i(\alpha) = \alpha_i$. Then by Theorem 2.5, for $K = K, L = L, M = K^{alg}$, each τ_i extends to a K-embedding $\sigma_i : L \to K^{alg}$. We have $\sigma_i(L) = L$ because L/K is a Galois extension. In particular, $\sigma_i(\alpha) = \tau_i(\alpha) = \alpha_i \in L$. □

Lemma 2.8. *If L/K is a Galois extension and $\alpha \in L$, then there exists a finite Galois subextension of L/K containing α.*

Proof. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of $\mu_{\alpha,K}$ in K^{alg}. Then, by the previous lemma, $K(\alpha_1, \ldots, \alpha_n) \subseteq L$. The above example then implies the result, since $K(\alpha_1, \ldots, \alpha_n)/K$ is a finite Galois extension containing α. □

The following lemma provides an important example of an infinite Galois extension. It is the Galois extension with which we will be concerned in the following chapters.

Lemma 2.9. *If $\overline{K}$ is the separable closure of a field K in a fixed algebraic closure of K, then the extension $\overline{K}/K$ is Galois.*

Proof. First, note that $\overline{K}/K$ is separable by definition. Let $\sigma : \overline{K} \to K^{alg}$ be a K-linear embedding. We need to show that $\sigma(\overline{K}) = \overline{K}$. For the first inclusion $\sigma(\overline{K}) \subseteq \overline{K}$, take $x \in \overline{K}$. By the previous lemma, there exists a finite Galois subextension L/K of $\overline{K}/K$ containing x. Then, $\sigma|_L : L \to K^{alg}$ is a K-embedding of L into K^{alg} and $\sigma(x) \in L$ because L/K is a Galois extension. In particular, $\sigma(x)$ is separable, because L/K is. Thus, $\sigma(\overline{K}) \subseteq \overline{K}$. For the other inclusion, let $x' \in \overline{K}$ and L'/K be a finite Galois subextension containing x'. Because L'/K is Galois, $\sigma|_{L'}$ is a K-automorphism of L'. Thus, there exists $x \in L' \subseteq \overline{K}$ such that $\sigma|_{L'}(x) = x'$. Hence, $x' = \sigma|_{L'}(x) = \sigma(x)$, which implies $\overline{K} \subseteq \sigma(\overline{K})$ and thus $\sigma(\overline{K}) = \overline{K}$. □

Definition. Let K be a field and $\overline{K}$ its separable closure. The Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ of the Galois extension $\overline{K}/K$ is called the **absolute Galois group** of the field K.

Example. As mentioned before, if $K = \mathbb{Q}$, then $\overline{K} = K^{alg}$, so $G_{\mathbb{Q}}$ can also be written as $\mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q})$.

2.3 The Galois Correspondence

As in the case of finite Galois extensions, we would like to characterise the intermediate field extensions of an arbitrary Galois extension L/K by considering the subgroups of the Galois group of L/K. Unfortunately, we cannot simply adopt the correspondence for finite Galois extensions one-to-one to infinite Galois extensions, as the following example shows:

Example. [1] Let $L = \mathbb{Q}(\sqrt{p}, p \text{ prime})$, i.e. L is constructed by adjoining the square roots of all prime numbers. Then $L/\mathbb{Q}$ is a Galois extension, because it is a limit of quadratic extensions. For a fixed prime number p, let σ_p be the unique element of $\mathrm{Gal}(L/\mathbb{Q})$ that maps $\sqrt{p}$ to $-\sqrt{p}$ and fixes $\sqrt{p'}$ if $p' \neq p$.

The $\sigma_p's$ generate a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, which we will denote by H. Then H does not contain the element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, which maps $\sqrt{p}$ to $-\sqrt{p}$ for *all* prime numbers p. Thus, H is a proper subgroup of $\mathrm{Gal}(L/\mathbb{Q})$.

However, $L^H = L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$.

To see why, note that any element $x \in L$ is contained in some subfield M of the form $M = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$. Then $M/\mathbb{Q}$ is a finite Galois extension. Now assume that $x \in L^H$. By definition of H, $\sigma_{p_1}, \ldots, \sigma_{p_r} \in H$. At the same time, the $\sigma_{p_1}, \ldots, \sigma_{p_r}$ generate $\mathrm{Gal}(M/\mathbb{Q})$. Thus, classical Galois theory implies that $x \in \mathbb{Q}$.

The above example shows that, when considering infinite extensions, two distinct subgroups can fix the same field. Thus, there can be more subgroups of the Galois group than there are Galois subextensions of the Galois extension. This means that we have to restrict ourselves to only certain subgroups when trying to find a correspondence. This is done by defining a topology on the Galois group. It then turns out that there is a Galois correspondence for *closed* subgroups only. The rest of this section follows §17 of [5].

Let L/K be an arbitrary Galois extension. For simplicity, we introduce the following notation:

$$G = \mathrm{Gal}(L/K)$$
$$\mathcal{M} = \{M \mid K \subseteq M \subseteq L, [M : K] < \infty \text{ and } M/K \text{ is Galois } \}$$
$$\mathcal{H} = \{H < G \mid H = \mathrm{Gal}(L/M) \text{ for some } M \in \mathcal{M}\}$$

We will frequently use the following results, which can be found, together with their proofs, in [5], Proposition I.3.28.

Proposition 2.10. *Let F be an algebraic field extension of a field K. Then the following statements are equivalent:*

(i). The field F is normal over K.

(ii). For an algebraic closure F^{alg} of F and a K-morphism $\tau : F \to F^{alg}$, we have $\tau(F) = F$.

(iii). Let $K \subseteq M \subseteq F \subseteq L$ be fields and let $\tau : M \to L$ be a K-morphism. Then $\tau(M) \subseteq F$ and there exists $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma|_M = \tau$.

(iv). Let $P \in K[x]$ be irreducible. If P has a root in N, then P splits over N.

Lemma 2.11. *Let $M \in \mathcal{M}$ and set $H = \mathrm{Gal}(L/M)$, i.e. $H \in \mathcal{H}$. Then $M = L^H$.*

Moreover, H is normal in G and $G/H \simeq \mathrm{Gal}(M/K)$. Thus, we have $|G/H| = |\mathrm{Gal}(M/K)| = [M : K] < \infty$.

Proof. Since L/K is a Galois extension, L is normal and separable over K, so it must also be normal and separable over the field M. Thus, L/M is a Galois

extension, which implies that $M = L^H$. One can show (and it is usually shown in the proof of the Fundamental Theorem of Finite Galois Theory) that the map $\tau : G \to \mathrm{Gal}(M/K)$ given by $\sigma \mapsto \sigma|_M$ is a group homomorphism with kernel $\mathrm{Gal}(L/M) = H$. Thus, H is normal in G. Then by the third part of Proposition 2.10, τ is surjective, which implies that $G/H \simeq \mathrm{Gal}(M/K)$ as groups. □

Lemma 2.12. *The intersection of all the $H \in \mathcal{H}$ is trivial, i.e. $\bigcap_{H\in\mathcal{H}} H = \{1\}$. Moreover, $\bigcap_{H\in\mathcal{H}} \sigma H = \{\sigma\}$ for all $\sigma \in G$.*

Proof. Let $\tau \in \bigcap_{H\in\mathcal{H}} H$ and let $\alpha \in L$. By Lemma 2.8, there exists an $M \in \mathcal{M}$ such that $\alpha \in M$. Now set $H = \mathrm{Gal}(L/M) \in \mathcal{H}$. Then the automorphism τ fixes M because $\tau \in H$. Thus, $\tau(\alpha) = \alpha$ and $\tau = \mathrm{id}$.

Now let $\tau \in \sigma H$ for all H. Then $\sigma^{-1}\tau \in H$ for all H. By the first statement, $\sigma^{-1}\tau = \mathrm{id}$. Thus, $\tau = \sigma$, which implies $\bigcap_{H\in\mathcal{H}} \sigma H = \{\sigma\}$. □

Lemma 2.13. *If $H_1, H_2 \in \mathcal{H}$, then $H_1 \cap H_2 \in \mathcal{H}$.*

Proof. Let $H_1 = \mathrm{Gal}(L/M_1)$ and $H_2 = \mathrm{Gal}(L/M_2)$ for $M_1, M_2 \in \mathcal{M}$. Each M_i is a finite Galois extension of K, so the composite M_1M_2 is also a finite Galois extension of K. Hence, $M_1M_2 \in \mathcal{M}$.

Now note that $\sigma \in H_1 \cap H_2$ if and only if $\sigma|_{M_1} = \mathrm{id}$ and $\sigma|_{M_2} = \mathrm{id}$, and this holds if and only if $M_1 \in \{a \in L \mid \sigma(a) = a\}$ and $M_2 \in \{a \in L \mid \sigma(a) = a\}$, if and only if $M_1M_2 \in \{a \in L \mid \sigma(a) = a\}$. The last condition is equivalent to $\sigma \in \mathrm{Gal}(L/M_1M_2)$. Hence, $H_1 \cap H_2 = \mathrm{Gal}(L/M_1M_2) \in \mathcal{H}$. □

We can now define a topology on the Galois group G.

Definition. We define the **Krull topology** on the Galois group G by defining a subset X of G to be open if either $X = \varnothing$ or $X = \bigcup_i \sigma_i H_i$ for some $\sigma_i \in G$ and $H_i \in \mathcal{H}$.

It is clear from the definition that G and $\varnothing$ are open sets and that the union of open sets is open. To prove that the topology is well-defined, it remains to show that the intersection of two open sets is open. To this end, let $H_1, H_2 \in \mathcal{H}$ and $\tau_1, \tau_2 \in G$. If $\sigma \in \tau_1H_1 \cap \tau_2H_2$, then $\tau_1H_1 \cap \tau_2H_2 = \sigma H_1 \cap \sigma H_2 = \sigma(H_1 \cap H_2)$, and $\sigma(H_1 \cap H_2)$ is open because $H_1 \cap H_2 \in \mathcal{H}$ by Lemma 2.13.

Remark. The set $\{\sigma H \mid \sigma \in G, H \in \mathcal{H}\}$ is a basis for the Krull topology because each non-empty open set of G is a union of left translations of subgroups of $\mathcal{H}$.

If $H \in \mathcal{H}$, then $|G : H| < \infty$, so $G - \sigma H$ is a union of finitely many left translations of H. Thus, σH is both open and closed. This means that the Krull topology has a basis of clopen sets, which is uncommon in familiar topologies on $\mathbb{R}$ or $\mathbb{C}$.

Theorem 2.14. *As a topological space under the Krull topology, G is Hausdorff, compact and totally disconnected.*

Proof. Let X be a subset of G, $\sigma, \tau \in X$ and let σH be an open neighbourhood of σ not containing τ. Such a neighbourhood exists because of Lemma 2.12. Then $\sigma H \cap X$ and $(G - \sigma H) \cap X$ are two disjoint non-empty open sets in X, but $X = (\sigma H \cap X) \cup ((G - \sigma H) \cap X)$, so X is not connected. Since X was an arbitrary subset containing more than one point, G must be totally disconnected.

To see that G is Hausdorff, let $\sigma \in G$. By Lemma 2.12, $\{\sigma\} = \bigcap_H \sigma H$. If $\tau \neq \sigma$, then there exists an $H \in \mathcal{H}$ such that $\tau \notin \sigma H$. Each σH is an open neighbourhood of σ, but, by the remark above, also closed. Therefore, σH and $G - \sigma H$ are disjoint open sets with $\sigma \in \sigma H$ and $\tau \in G - \sigma H$, which implies that G is Hausdorff.

We now show that G is compact. In doing so, we will also indirectly prove that G can be constructed from finite Galois groups.

Let P be the direct product of finite groups G/H, i.e. $P = \prod_{H \in \mathcal{H}} G/H$. We make P into a topological space by giving each G/H the discrete topology and then P the product topology. Each G/H is both Hausdorff and compact, so P is Hausdorff and, by the Tychonoff theorem, also compact. There is a natural group homomorphism $f : G \to P$ mapping $\sigma \mapsto (\sigma H)_{H \in \mathcal{H}}$. We want to show that f is a homeomorphism from G to the image of f and that this image is a closed subset of P. This will prove that $\mathrm{im}(f)$ is compact, since P is compact and Hausdorff. Since G is homeomorphic to $\mathrm{im}(f)$, it will follow that G is also compact.

Let now f be as above. The kernel of f consists of those $\sigma \in G$ such that $\sigma H = H$ for all $H \in \mathcal{H}$. Thus, if $\sigma \in \ker(f)$, then $\sigma \in \bigcap_{H \in \mathcal{H}} H$. But by Lemma 2.12, we have that $\bigcap_{H \in \mathcal{H}} H = \{1\}$. Hence, f is injective.

Let $\pi_H : P \to G/H$ be the projection onto the H-component. Then $\pi_H(f(\sigma)) = \sigma H$ for all $\sigma \in G$. For any $\tau \in G$, the singleton sets τH form a basis for the discrete topology on G/H. Thus, by definition of the product topology, every open set in P is a union of a finite intersection of sets of the form $\pi_H^{-1}(\tau H)$ for various $\tau \in G$ and $H \in \mathcal{H}$. To prove that f is continuous, it suffices to show that $f^{-1}(\pi_H^{-1}(\tau H))$ is open for any τH. But this preimage is just τH, which is open. Thus, f is continuous. Moreover, $f(\tau H) = \pi_H^{-1}(\tau H) \cap \mathrm{im}(f)$ is open in $\mathrm{im}(f)$, so f^{-1} is continuous as well. We have thus proved that f is a homeomorphism from G to $\mathrm{im}(f)$.

The last step of the proof is showing that $\mathrm{im}(f)$ is closed in P. We will identify G/H with the isomorphic group $\mathrm{Gal}(M_H/K)$, where $M_H = L^H$. This isomorphism is from Lemma 2.11 and amounts to identifying τH with the restriction $\tau|_{M_H}$. With this identification, the element $\pi_H(\rho)$ is an automorphism

of M_H for $\rho \in P$. Note that we have $\pi_H(f(\tau)) = \tau|_{M_H}$. Let

$$C := \{\rho \in P \mid \text{for each } H_1, H_2 \in \mathcal{H},\ \pi_{H_1}(\rho)|_{M_{H_1} \cap M_{H_2}} = \pi_{H_2}(\rho)|_{M_{H_1} \cap M_{H_2}}\}.$$

We claim that $C = \mathrm{im}(f)$.

We know that $\mathrm{im}(f) \subseteq C$ since $\pi_H(f(\tau))|_{M_H} = \tau|_{M_H}$ for any $\tau \in G$.

For the reverse inclusion, let $\rho \in C$. We define $\tau : L \to L$ as follows: For $a \in L$, pick any $M_H \in \mathcal{M}$, which is possible by Lemma 2.8, and define $\tau(a) = \pi_H(\rho)(a)$. This is a well-defined map because $\rho \in C$. To show that τ is a ring homomorphism, let $a, b \in L$, let $M_H \in \mathcal{M}$ with $a, b \in M_H$. Then $\tau|_{M_H} = \pi_H(\rho)$ is a ring homomorphism, so $\tau(a+b) = \tau(a) + \tau(b)$ and $\tau(ab) = \tau(a)\tau(b)$. Moreover, τ is a bijection because we can construct τ^{-1} from ρ^{-1}. Clearly, τ fixes the field K, so $\tau \in G$. Now we have $f(\tau) = \rho$ because $\tau|_{M_H} = \pi_H(\rho)$. Thus, $C = \mathrm{im}(f)$.

It remains to show that C is closed in P. Take any $\rho \in P$ with $\rho \notin C$. Then there are $H_1, H_2 \in \mathcal{H}$ with $\pi_{H_1}(\rho)|_{M_{H_1} \cap M_{H_2}} \neq \pi_{H_2}(\rho)|_{M_{H_1} \cap M_{H_2}}$. Hence, $\pi_{H_1}^{-1}(\pi_{H_1}(\rho)) \cap \pi_{H_2}^{-1}(\pi_{H_2}(\rho))$ is an open subset of P which contains ρ and is disjoint from C. Therefore, $P - C$ is open, and thus, $C = \mathrm{im}(f)$ is closed, which finishes the proof. □

The last step we need to extend the Fundamental Theorem of Finite Galois Theory to arbitrary Galois extensions is the following theorem:

Theorem 2.15. *Let H be a subgroup of G, let $H' = \mathrm{Gal}(L/L^H)$, and let $\overline{H}$ be the closure of H in the topology of G. Then $H' = \overline{H}$.*

Proof. Clearly, $H \subseteq H'$, so it suffices to show that H' is closed and that $H' \subseteq \overline{H}$.

We first prove that H' is closed. Let $\sigma \in G - H$. Then there is $\alpha \in L^H$ such that $\sigma(\alpha) \neq \alpha$. Take an $M \in \mathcal{M}$ with $\alpha \in M$ and let $\Gamma = \mathrm{Gal}(L/M) \in \mathcal{H}$. Then, for all $\tau \in \Gamma$, we have $\tau(\alpha) = \alpha$, so $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$. Thus, $\sigma\Gamma$ is an open neighbourhood of σ disjoint from H', which implies that $G - H'$ is open. Hence, H' is closed.

To show that $H' \subseteq \overline{H}$, we first set $M = L^H$. Let $\sigma \in H'$ and $\Gamma \in \mathcal{H}$. Let $F = L^\Gamma \in \mathcal{M}$ and let $H_0 = \{\rho|_F \mid \rho \in H\}$. Then H_0 is a subgroup of the finite group $\mathrm{Gal}(F/K)$. Note that $L^{H_0} = L^H \cap F = M \cap F$, so the Fundamental Theorem of Finite Galois Theory shows that $H_0 = \mathrm{Gal}(F/(F \cap M))$. Since $\sigma \in H'$, we have $\sigma|_M = \mathrm{id}$, so $\sigma|_F \in H_0$. Thus, there exists $\rho \in H$ with $\rho|_F = \sigma|_F$. Hence, $\sigma^{-1}\rho \in \mathrm{Gal}(L/F) = \Gamma$, so $\rho \in \sigma\Gamma \cap H$. This proves that every basic open neighbourhood $\sigma\Gamma$ of $\sigma \in H'$ intersects H, so $\sigma \in \overline{H}$. Therefore, $H' \subseteq \overline{H}$ and we are done. □

We can now finally state and prove the Fundamental Theorem of Infinite Galois Theory.

Theorem 2.16. ***(The Fundamental Theorem of Infinite Galois Theory)*** *Let L be a Galois extension of K, and let $G = \mathrm{Gal}(L/K)$. Then, under the Krull topology on G, there exist inclusion-reversing one-to-one correspondences between the following sets:*

*(i). The set of subfields M with $K \subseteq M \subseteq L$ and the set of **closed** subgroups H of G.*

*(ii). The set of subfields M with $K \subseteq M \subseteq L$ such that $[M : K] < \infty$ and the set of **open** subgroups H of G. In this case, $|G : H| = [M : K]$.*

*(iii). The set of subfields M with $K \subseteq M \subseteq L$ such that M/K is a **Galois** extension and the set of **normal** subgroups H of G.*

In all cases, the correspondence is given by

$$M \mapsto \mathrm{Gal}(L/M)$$
$$L^H \hookleftarrow H.$$

Moreover, if H is a normal subgroup of G, then we have a group isomorphism

$$\mathrm{Gal}(L^H/K) \cong G/H.$$

If G/H is endowed with the quotient topology, this isomorphism is also a homeomorphism.

Proof. Let M be a subfield of L containing K. Then L is normal and separable over M, so L is Galois over M. Thus, $M = L^{\mathrm{Gal}(L/M)}$. For a subgroup H of G, we know by Theorem 2.15 that $H = \mathrm{Gal}(L/L^H)$ if and only if H is closed in G. The maps $M \mapsto \mathrm{Gal}(L/M)$ and $H \mapsto L^H$ then give an inclusion-reversing one-to-one correspondence between the set of intermediate fields of L/K and the set of closed subgroups of G.

For the second statement, let M be an intermediate field of L/K, and let $H = \mathrm{Gal}(L/M)$. Suppose that $|G : H| < \infty$. Then $G - H$ is a finite union of left-twists of H, and each of these is closed, because H is closed. Thus, $G - H$ is closed, so H is open. Now suppose that H is open. Then H contains some basic neighbourhood of the identity map, so we have $\Gamma \subseteq H$ for some $\Gamma \in \mathcal{H}$. Thus, $M \subseteq L^\Gamma$, so $[M : K] < \infty$. Finally, suppose that $[M : K] < \infty$ and choose $F \in \mathcal{M}$ with $M \subseteq F$, which is possible by Lemma 2.8. Let $\Gamma = \mathrm{Gal}(L/F)$. Then $\Gamma \subseteq H$ because $M \subseteq F$, so $|G : H| \leq |G : \Gamma| < \infty$. We have hence shown that $|G : H| < \infty$, if and only if $[M : K] < \infty$, if and only if H is open. To prove that $|G : H| = [M : K]$, note that by Lemma 2.11, there is an isomorphism $G/\Gamma \cong \mathrm{Gal}(F/K)$ via the map $\sigma\Gamma \mapsto \sigma|_F$, with Γ and F as before. Thus,

H/Γ maps to $\{\rho|_F \mid \rho \in H\}$, which is a subgroup of $\mathrm{Gal}(F/K)$ with fixed field $M \cap F = M$. By the Fundamental Theorem of Finite Galois Theory, we know that the order of this group is $[F : M]$, Therefore,

$$|G : H| = |G/\Gamma : H/\Gamma| = \frac{|G/\Gamma|}{|H/\Gamma|} = \frac{[F : K]}{[F : M]} = [M : K].$$

For the statements about normality, we continue to assume that $H = \mathrm{Gal}(L/M)$. Suppose that H is a normal subgroup of G. Let $\alpha \in M$ and let $\mu_{\alpha,K}$ be the minimal polynomial of α over K. If $\beta \in L$ is a root of f, then by the Isomorphism Extension Theorem, Theorem 2.3, there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$. We claim that $\beta \in M$. To see why, take $\tau \in H$. Then $\tau(\beta) = \sigma(\sigma^{-1}\tau\sigma(\alpha)) = \sigma(\alpha) = \beta$. The second equality holds because H is normal in G. Hence, $\beta \in L^H = M$, so $\mu_{\alpha,K}$ splits over M. Therefore, M is normal over K. Moreover, M/K is separable, so M is also separable over K. Thus, M is Galois over k.

Conversely, assume that M/K is a Galois extension. Then by Proposition 2.10, the map $\theta : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ defined as $\sigma \mapsto \sigma|_M$ is a well-defined group homomorphism. Its kernel is $\mathrm{Gal}(L/M) = H$, so H is normal in G. Also, θ is surjective by the Isomorphism Extension Theorem, Theorem 2.3. Hence, $G/H \cong \mathrm{Gal}(M/K)$, which just means $G/H \cong \mathrm{Gal}(L^H/K)$, as desired.

It remains to show that this isomorphism is also a homeomorphism, i.e. that the natural map $\varphi : G/H \to \mathrm{Gal}(M/K)$ is a homeomorphism, if H is normal in G. A basic open subset of $\mathrm{Gal}(M/K)$ is of the form $\rho\,\mathrm{Gal}(M/F)$ for an extension F that is contained in M and is finite Galois over K. Let $\Gamma = \mathrm{Gal}(L/F) \in \mathcal{H}$. Then $\theta^{-1}(\mathrm{Gal}(M/F)) = \Gamma$, where θ is as before and induces φ. Thus, $\theta^{-1}(\rho\,\mathrm{Gal}(M/F)) = \tau\Gamma$ for any $\tau \in G$ such that $\tau|_M = \rho$. Since $\tau\Gamma$ is open in G, θ is continuous. Moreover, the image of a compact set under a continuous map is compact, and any compact subset of a Hausdorff space is closed. By Theorem 2.14, we know that G is compact and $\mathrm{Gal}(M/K)$ is Hausdorff, so θ maps closed sets to closed sets, i.e. θ is a closed map. Since φ is induced from θ, φ is then also a continuous and closed map when G/H is induced with the quotient topology. Hence, φ is a homeomorphism, which finishes the proof. □

Example. If L/K is a Galois extension with $[L : K] < \infty$, then the Krull topology on $\mathrm{Gal}(L/K)$ is the discrete topology, meaning that every subgroup of $\mathrm{Gal}(L/K)$ is closed. Thus, Theorem 2.16 reduces to the Fundamental Theorem of Finite Galois Theory.

3 Valuations

Valuations are a useful tool to give meaning to the notion of "size" of an element of a field. In our cases, this notion is of either a number theoretical or of a complex analytical manner. Valuations make fields into metric spaces, which can then be embedded into fields that are complete with respect to the metric defined by the valuation. Such a notion of size in a base field K can even be extended to an algebraic field extension L/K. We will examine when and how it is possible to do so. We will also see that there is a natural link between valuations and prime ideals, which will prove useful in later chapters.

The primary source for this chapter is §II of [7].

3.1 Definition and First Properties

Definition. Let K be a field. A (multiplicative) **valuation** of K is a function $|\ |: K \to \mathbb{R}$ such that:

(i). $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,

(ii). $|xy| = |x||y|$,

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

The last condition is called the triangle inequality.

In the following, we will assume the valuations to be non-trivial, i.e. we exclude the trivial valuation, which satisfies $|x| = 1$ for all $x \neq 0$.

We make the field K into a metric space, and thus into a topological space, by defining the distance between two points $x, y \in K$ by $d(x, y) = |x - y|$.

Definition. Two valuations of K are said to be **equivalent** if they induce the same topology on K.

The following two propositions provide more practical ways of defining equivalent valuations:

Proposition 3.1. *Two valuations $|\ |_1$ and $|\ |_2$ on a field K are equivalent if and only if they satisfy the implication:*

$$|x|_1 < 1 \implies |x|_2 < 1, \tag{3.1}$$

Proof. The proposition derives from the fact that for an arbitrary valuation $|\ |$ on K, the inequality $|x| < 1$ is equivalent to the condition that the sequence $(x^n)_{n\in\mathbb{N}}$ converges to 0 in the topology defined by $|\ |$. This means that two equivalent valuations $|\ |_1$ and $|\ |_2$ must satisfy the implication (3.1), since they

define the same topology on K. Conversely, if two valuations satisfy (3.1), then they define the same topology on K, so they are equivalent. □

Proposition 3.2. *Two valuations $|\ |_1$ and $|\ |_2$ on K are equivalent if and only if there exists an $s \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.*

Proof. If $|\ |_1 = |\ |_2^s$ with $s \in \mathbb{R}_{>0}$, then $|\ |_1$ and $|\ |_2$ clearly induce the same topology on K.

For the converse, we use condition (3.1) from Proposition 3.1. Let $y \in K$ be a fixed element satisfying $|y|_1 > 1$. Then for an $x \in K, x \neq 0$, we have $|x|_1 = |y|_1^\alpha$ for some $\alpha \in \mathbb{R}$. Let $\{\frac{m_i}{n_i}\}_{i\in\mathbb{N}}$ be a sequence of rational numbers, with $n_i > 0$ for all i, which converges to α from above. Then $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, which implies

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1 \implies \left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1.$$

Then $|x|_2 \leq |y|_2^{m_i/n_i}$, so $|x|_2 \leq |y|_2^\alpha$. One can then repeat the same strategy using 3.1 with a sequence $\{\frac{m_i}{n_i}\}_{i\in\mathbb{N}}$ which converges to α from below, yielding $|x|_2 \geq |y|_2^\alpha$. Hence, $|x|_2 = |y|_2^\alpha$. Therefore, for all non-zero $x \in K$, we have

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s.$$

Hence, $|x|_1 = |x|_2^s$. Since $|y|_1 > 1$ implies $|y|_2 > 1$, we conclude that $s > 0$. □

We can now state and prove the useful Approximation Theorem for valuations.

Theorem 3.3. ***(Approximation Theorem)*** *Let K be a field and let $|\ |_1$ and $|\ |_2$ be inequivalent valuations of K, and fix $a_1, a_2 \in K$. Then for every $\varepsilon > 0$, there exists $x \in K$ such that*

$$|x - a_1|_1 < \varepsilon \text{ and } |x - a_2|_2 < \varepsilon.$$

Proof. Note that the assumption that $|\ |_1$ and $|\ |_2$ are inequivalent implies, by Proposition 3.1, that there exists $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_2 \geq 1$. Similarly, there exists $\beta \in K$ such that $|\beta|_2 < 1$ and $|\beta|_1 \geq 1$. Then the sequence $\{t_m = \frac{\alpha^m}{1+\alpha^m}\}_{m\in\mathbb{N}}$ converges to 1 with respect to $|\ |_2$ and to 0 with respect to $|\ |_1$. Similarly, the sequence $\{s_m = \frac{\beta^m}{1+\beta^m}\}_{m\in\mathbb{N}}$ converges to 1 with respect to $|\ |_1$ and to 0 with respect to $|\ |_2$. Then $x = a_1 s_m + a_2 t_m$ satisfies the desired statement of the theorem.

□

Definition. A valuation $|\ |$ is said to be **non-archimedean** if $|n|$ stays bounded, for all $n \in \mathbb{N}$. The valuation is called **archimedean** otherwise.

Proposition 3.4. *A valuation $|\ |$ of a field K is non-archimedean if and only if it satisfies the* ***strong triangle inequality***

$$|x+y| \leq \max\{|x|, |y|\}.$$

Proof. If $|\ |$ satisfies the strong triangle inequality, then $|n| = |1 + \cdots + 1| \leq 1$.

Conversely, let $|n| < N$ for all $n \in \mathbb{N}$, and let $x, y \in K$ with $|x| \geq |y|$. Then $|x|^\nu |y|^{n-\nu} \leq |x|^n$ for $\nu \geq 0$, and thus,

$$|x+y|^n \leq \sum_{\nu=0}^{n} \left| \binom{n}{\nu} \right| |x|^\nu |y|^{n-\nu} \leq N(n+1)|x|^n,$$

which implies

$$|x+y| \leq N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n} \max\{|x|, |y|\}.$$

Hence, letting $n \to \infty$, we get $|x+y| \leq \max\{|x|, |y|\}$. □

Definition. Let $|\ |$ be a non-archimedean valuation of a field K. Define a function $\nu : K \to \mathbb{R} \cup \{\infty\}$ by setting

$$\nu(x) = -\log|x| \text{ for } x \neq 0, \text{ and } \nu(0) = \infty$$

Then ν satisfies the following properties:

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

(ii). $\nu(xy) = \nu(x) + \nu(y)$,

(iii). $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

We fix the following conventions for elements $a \in \mathbb{R}$ and the symbol ∞:

$$a + \infty = \infty \ , \ \infty + \infty = \infty.$$

Such a function ν on K is called an **exponential valuation** of K. Again, we only include non-trivial functions, i.e. not $\nu(x) = 0$ for $x \neq 0$, $\nu(0) = \infty$.

Two exponential valuations ν_1 and ν_2 of K are called **equivalent** if there exists $s \in \mathbb{R}_{>0}$ such that $\nu_1 = s\nu_2$.

The valuation $|\ |$ from our previous definition can be recovered from a non-archimedean exponential valuation ν by setting $|x| = q^{-\nu(x)}$, for a fixed real number $q > 1$.

The valuation $|\ |$ is called the associated **multiplicative valuation** or **absolute value**. Equivalent exponential valuations correspond to equivalent multiplicative valuations.

Example. Let $p \in \mathbb{Z}$ be a prime number and $a = \frac{b}{c} \in \mathbb{Q} - \{0\}$. We extract from b and c the highest possible power m of p, such that

$$a = p^m \frac{b'}{c'} \text{ for } \gcd(b'c', p) = 1.$$

Then we can define the **p-adic absolute value** $|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}$ of $\mathbb{Q}$ by

$$|a|_p = \frac{1}{p^m}.$$

The associated **p-adic exponential valuation** $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ of $\mathbb{Q}$ is then defined as

$$\nu_p(a) = m \quad \text{and, formally,} \quad \nu_p(0) = \infty.$$

It is easily checked that these are indeed multiplicative, resp. exponential valuations.

For every prime number $p \in \mathbb{Z}$, the valuation $|\ |_p$ is non-archimedean. The usual absolute value on $\mathbb{R}$, denoted here by $|\ |_\infty$, is the only archimedean valuation on $\mathbb{Q}$. In fact, it is shown in Proposition II.3.7 in [7] that every valuation on $\mathbb{Q}$ is equivalent to either $|\ |_p$ or $|\ |_\infty$.

Example. Let k be a finite field and $k(t)$ the field of rational functions over k. Then the non-zero prime ideals $\mathfrak{p}$ of the polynomial ring $k[t]$ are given by monic irreducible polynomials $p(t) \in k[t]$. In analogy to the p-adic absolute value, we can, for any such $\mathfrak{p}$, define an absolute value $|\ |_\mathfrak{p} : k(t) \to \mathbb{R}$ on the rational function field $k(t)$ as follows:

Let $f(t) = \frac{g(t)}{h(t)}$, for $g(t), h(t) \in k[t]$ be a non-zero rational function. Extract from $g(t)$ and $h(t)$ the highest possible power of the irreducible polynomial $p(t)$ such that

$$f(t) = p(t)^m \frac{\tilde{g}(t)}{\tilde{h}(t)}, \text{ for } \gcd(\tilde{g}\tilde{h}, p) = 1.$$

Then set

$$\nu_\mathfrak{p}(f) = m \text{ and } |f|_\mathfrak{p} = q_\mathfrak{p}^{-\nu_\mathfrak{p}(f)}.$$

Here, $q_\mathfrak{p}$ is defined by $q_\mathfrak{p} = q^{d_\mathfrak{p}}$, $d_\mathfrak{p}$ is the degree of the residue class field[2] of $\mathfrak{p}$ over k and q is a fixed real number > 1. Moreover, set $\nu_\mathfrak{p}(0) = \infty$ and $|0|_\mathfrak{p} = 0$. Then $\nu_\mathfrak{p}$ and $|\ |_\mathfrak{p}$ satisfy the defining properties of exponential resp. multiplicative valuations.

If $\mathfrak{p} = (t - a)$ for $a \in k$, then the valuation $\nu_\mathfrak{p}(f)$ is the order of the zero, resp. pole, of the function $f = f(t)$ at $t = a$.

The function field $k(t)$ also has one more exponential valuation, which is

[2] Residue class fields are defined on page 20.

defined as

$$\nu_\infty : k(t) - \{0\} \longrightarrow \mathbb{Z} \cup \{\infty\} : f = \frac{g}{h} \longmapsto \deg(h) - \deg(g).$$

This valuation describes the order of the zero, resp. pole, of $f(\frac{1}{t})$ at the point $t = 0$, i.e. the order of the zero, resp. pole, of $f(t)$ at the point at infinity. It is associated to the prime ideal $\mathfrak{p} = (\frac{1}{t})$ of the ring $k[\frac{1}{t}] \subseteq k(t)$. Setting $|f|_\infty = q^{-\nu_\infty(f)}$ gives the corresponding multiplicative valuation.

The following proposition follows immediately from the defining properties of a (non-archimedean) exponential valuation ν:

Proposition 3.5. *The set*

$$\mathcal{O}_\nu = \{x \in K \mid \nu(x) \geq 0\} = \{x \in K \mid |x| \leq 1\}$$

is a ring with group of units

$$\mathcal{O}_\nu^* = \{x \in K \mid \nu(x) = 0\} = \{x \in K \mid |x| = 1\}$$

and (unique) maximal ideal

$$\mathfrak{m} = \{x \in K \mid \nu(x) > 0\} = \{x \in K \mid |x| < 1\}.$$

Note that this proposition is only true if $|\ |$ is a non-archimedean valuation. In fact, $\mathcal{O}_\nu$ is not even a ring if $|\ |$ is archimedean. More so, with our definition of an exponential valuation ν, we cannot even define ν from a multiplicative valuation $|\ |$ if $|\ |$ is archimedean.

The ring $\mathcal{O}_\nu$ is an integral domain with K as its field of fractions and with the property that, for every $x \in K$, either $x \in \mathcal{O}_\nu$ or $x^{-1} \in \mathcal{O}_\nu$. This is an important class of rings:

Definition. An integral domain $\mathcal{O}$ for which every element x in its field of fractions K satisfies either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ is called a **valuation ring**.

Lemma 3.6. *Valuation rings are local rings.*

Proof. Let $\mathcal{O}$ be a valuation ring. We will show that if $x, y \in \mathcal{O}$ are non-units, then their sum $x + y$ is not a unit.

If either $x = 0$ or $y = 0$, then their sum is a non-unit by assumption. So let $x \neq 0$ and $y \neq 0$. Let $xy^{-1} \in \mathcal{O}$ and suppose there exists $u \in \mathcal{O}$ such that $u(x + y) = 1$. Then

$$y^{-1} = u(x + y)y^{-1} = u(xy^{-1} + 1) \in \mathcal{O},$$

which contradicts the assumption that y is not a unit. Hence, the sum of two non-units is a non-unit, which makes $\mathcal{O}$ into a local ring. □

Being a local ring, a valuation ring $\mathcal{O}$ has a unique maximal ideal $\mathfrak{m}$, which is given by

$$\mathfrak{m} = \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}.$$

Definition. Let $\mathcal{O}$ be a valuation ring with unique maximal ideal $\mathfrak{m}$. Then the field $\mathcal{O}/\mathfrak{m}$ is called the **residue class field** of $\mathcal{O}$.

Lemma 3.7. *Valuation rings are integrally closed.*

Proof. Let $\mathcal{O}$ be a valuation ring and let $x \in K$ be integral over $\mathcal{O}$. Then there is an equation $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathcal{O}$. If $x \notin \mathcal{O}$, then $x^{-1} \in \mathcal{O}$ by definition, but this implies the contradiction $x = -a_1 - a_2 x^{-1} - \cdots - a_n (x^{-1})^{n-1} \in \mathcal{O}$. So $x \in \mathcal{O}$. □

Definition. We call an exponential valuation ν of a field K **discrete** if it admits a smallest positive value s. In this case, we have $\nu(K^*) = s\mathbb{Z}$, i.e. the value group $\nu(K^*)$ is discrete. A discrete exponential valuation ν is called **normalised** if $s = 1$.

We can always normalise a discrete exponential valuation ν by dividing by s. This does not change the invariants $\mathcal{O}_\nu, \mathcal{O}_\nu^*, \mathfrak{m}$.

Definition. For a normalised exponential valuation ν of a field K, we call an element π in its valuation ring $\mathcal{O}_\nu$ a **prime element** if $\nu(\pi) = 1$.

Every element $x \in K^*$ can be respresented uniquely as $x = u\pi^m$, where $m \in \mathbb{Z}$ and $u \in \mathcal{O}_\nu^*$. This is because for $\nu(x) = m$, we have $\nu(x\pi^{-m}) = 0$, so $u = x\pi^{-m} \in \mathcal{O}_\nu^*$.

3.2 Completions

After having introduced multiplicative and exponential valuations on a field, we can now turn to the question of how to (topologically) complete the field with respect to the metric induced by a valuation. Let $(K, |\ |)$ be a valued field, archimedean or non-archimedean. We want to construct a field $(\hat{K}, |\ |)$ from $(K, |\ |)$, which is not only complete with respect to the valuation $|\ |$, but also has the property that K is dense $\hat{K}$. The field $\hat{K}$ will then be called the **completion** of K. It is constructed as follows:

Let R be the ring of all Cauchy sequences of $(K, |\ |)$ and consider the ideal $\mathfrak{m}$ of R consisting of all nullsequences with respect to $|\ |$. It can be shown that

$\mathfrak{m}$ is maximal ([3], Theorem VI.4.1). The field

$$\hat{K} = R/\mathfrak{m}.$$

is then the set of equivalence classes of Cauchy sequences. The field K is embedded into $\hat{K}$ by the natural injective map

$$i : K \longrightarrow \hat{K} : \ a \longmapsto (a, a, a, \ldots),$$

i.e. $a \in K$ is mapped to the class of the constant Cauchy sequence $(a, a, a, \ldots)$. The field operations on the equivalence classes of Cauchy sequences in $\hat{K}$ are induced by the continuous field operations on K and are therefore well-defined.

We extend the valuation $|\ |$ from K to $\hat{K}$ by defining a valuation on $\hat{K}$ by

$$|(a_n)_{n\in\mathbb{N}}| = \lim_{n\to\infty} |a_n|.$$

Since $||a_n| - |a_m|| \leq |a_n - a_m|$ implies that $|a_n|$ is a Cauchy sequence of real numbers, this limit exists. One can then prove (it is done in [3], Theorem VI.4.1) that $\hat{K}$ is complete with respect to the extended valuation and that every $a \in \hat{K}$ is a limit of a sequence $(a_n)_{n\in\mathbb{N}}$ in K. Note that by construction, K is dense in $\hat{K}$. Finally:

Lemma 3.8. *[10] The completion $(\hat{K}, |\ |)$, which has just been constructed, is unique up to a unique isomorphism fixing K.*

Proof. Let $a \in \hat{K}$ and $(a_n)_{n\in\mathbb{N}}$ a sequence in $\hat{K}$ such that $a = \lim_{n\to\infty} a_n$. Let $\sigma : \hat{K} \to \hat{K}$ be a continuous automorphism fixing K. Since σ is continuous, there exists δ with $0 < \delta < \frac{1}{n}$ such that if $a_n \in \hat{K}$ satisfies $|a - a_n| < \delta$, then $|\sigma(a) - \sigma(a_n)| < \frac{1}{n}$. But K is dense in $\hat{K}$, so we can choose the a_n to be inside K. Then, as σ fixes K, we have $\sigma(a_n) = a_n$. This implies $|\sigma(a) - a_n| < \frac{1}{n}$, so $\sigma(a) = \lim_{n\to\infty} a_n = a$. Hence, there are no non-trivial continuous automorphisms $\hat{K} \to \hat{K}$ that fix K. This implies the statement of the lemma.

□

The most common examples of complete valued fields are $\mathbb{R}$ and $\mathbb{C}$, which are both complete with respect to an archimedean valuation. Surprisingly, it turns out that these are the only two fields (up to isomorphism) for which this is the case:

Theorem 3.9. ***(Ostrowski)*** *For every field K which is complete with respect to an archimedean valuation $|\ |$, there exists an isomorphism σ from K onto either $\mathbb{R}$ or $\mathbb{C}$ which satisfies $|a| = |\sigma a|^s$ for all $a \in K$, for a fixed $s \in (0, 1]$.*

Theorem 3.9 is stated and proved in [7], Theorem II.4.2. Note that in the theorem, the valuation on the left side of the equation is in K, while the valuation on the right side is in either $\mathbb{R}$ or $\mathbb{C}$.

By Ostrowski's theorem, archimedean valuations on complete valued fields serve more of an analytic than an arithmetic interest. Therefore, we will from now on focus on non-archimedean valuations. For practical purposes, we will mostly be considering exponential valuations ν instead of multiplicative valuations $|\ |$.

So let ν be a non-archimedean exponential valuation on a field K. We want to continue ν to an exponential valuation $\hat{\nu}$ of the completion $\hat{K}$.

Proposition 3.10. *Let K be a valued field and let ν be a non-archimedean exponential valuation on K. Then there exists an exponential valuation $\hat{\nu}$ on the completion $\hat{K}$ that extends ν.*

Proof. We will construct the extended valuation ν as follows: Let $a_n \in K$ and $a = \lim_{n\to\infty} a_n \in \hat{K}$. Set

$$\hat{\nu}(a) = \lim_{n\to\infty} \nu(a_n). \tag{3.2}$$

To argue why this definition of $\hat{\nu}$ is well-defined, we need to prove that the sequence $\nu(a_n)$ becomes stationary at some point (if $a \neq 0$). Indeed, for $n \geq n_0$, we have $\hat{\nu}(a - a_n) > \hat{\nu}(a)$, so by the strong triangle inequality,

$$\nu(a_n) = \hat{\nu}(a_n - a + a) = \min\{\hat{\nu}(a_n - a), \hat{\nu}(a)\} = \hat{\nu}(a).$$

Hence, $\nu(K^*) = \hat{\nu}(\hat{K}^*)$. □

Definition. Let K be a field with non-archimedean exponential valuation ν and completion $\hat{K}$. We call the extended valuation $\hat{\nu}$ from (3.2) the **continuation** of ν.

By construction, if ν is discrete and normalised, then so is the extension $\hat{\nu}$.

Proposition 3.11. *Let $\mathcal{O}_\nu \subseteq K$ be the valuation ring of a non-archimedean exponential valuation ν with maximal ideal $\mathfrak{m}$, and let $\hat{\mathcal{O}}_\nu \subseteq \hat{K}$ be the valuation ring of the continuation $\hat{\nu}$ with maximal ideal $\hat{\mathfrak{m}}$. Then*

$$\hat{\mathcal{O}}_\nu/\hat{\mathfrak{m}} \cong \mathcal{O}_\nu/\mathfrak{m}.$$

Moreover, if ν is discrete, then

$$\hat{\mathcal{O}}_\nu/\hat{\mathfrak{m}}^n \cong \mathcal{O}_\nu/\mathfrak{m}^n \quad \textit{for} \quad n \geq 1.$$

Proof. The proof is analogue to the proof of the special case $(\mathbb{Q}, \nu_p)$ in Proposition II.2.4 in [7]. □

The following proposition generalises the p-adic expansion to arbitrary discrete valuations ν of a field K. It tells us what the elements in the completion $\hat{K}$ of K look like concretely.

Proposition 3.12. *Let K be a field endowed with a discrete non-archimedean valuation ν and let $\mathcal{O}_\nu$ be its valuation ring with maximal ideal $\mathfrak{m}$. Let $R \subseteq \mathcal{O}_\nu$ be a system of representatives for the residue class field $\kappa = \mathcal{O}_\nu/\mathfrak{m}$ such that $0 \in R$. Let $\pi \in \mathcal{O}_\nu$ be a prime element. Then every $x \neq 0$ in the completion $\hat{K}$ of K can be uniquely represented as a convergent series:*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots).$$

Here, $a_i \in R, a_0 \neq 0$ and $m \in \mathbb{Z}$.

Proof. Let $\hat{\mathcal{O}}_\nu$ be the valuation ring of the continued valuation $\hat{\nu}$ and let $x = u\pi^m$ with $u \in \hat{\mathcal{O}}_\nu^*$. By the previous proposition, we have $\hat{\mathcal{O}}_\nu/\hat{\mathfrak{m}} \cong \mathcal{O}_\nu/\mathfrak{m}$, so the class $u \bmod \hat{\mathfrak{m}}$ has a unique representative $a_0 \in R, a_0 \neq 0$. Thus, $u = a_0 + \pi b_1$, for some $b_1 \in \hat{\mathcal{O}}_\nu$. By induction, assume that we have found $a_0, \ldots, a_{n-1} \in R$ such that

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \pi^n b_n,$$

for some $b_n \in \hat{\mathcal{O}}_\nu$, and that this equation determines the a_i uniquely. Then the representative $a_n \in R$ of $b_n \bmod \pi\hat{\mathcal{O}}_\nu \in \hat{\mathcal{O}}_\nu/\hat{\mathfrak{m}} \cong \mathcal{O}_\nu/\mathfrak{m}$ is also uniquely determined by u. We have $b_n = a_n + \pi b_{n+1}$, for some $b_{n+1} \in \hat{\mathcal{O}}_\nu$. Therefore,

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + \pi^{n+1}b_{n+1}.$$

Continuing in this way, we find an infinite series $\sum_{i=0}^{\infty} a_i\pi^i$ that is uniquely determined by u. Since the remainder term $\pi^{n+1}b_{n+1}$ tends to 0, the series converges to u. □

Example. We want to apply Proposition 3.12 to the field of rational numbers $\mathbb{Q}$ and the p-adic valuation ν_p with its completion $\mathbb{Q}_p$. Taking the numbers $0, 1, \ldots, p-1$ as a system of representatives R for the residue class field $\mathbb{Z}/p\mathbb{Z}$ of the valuation, the proposition gives back the usual series representation of p-adic numbers:

$$x = p^m(a_0 + a_1p + a_2p^2 + \cdots),$$

where $0 \leq a_i < p$, $a_0 \neq 0$ and $m \in \mathbb{Z}$.

Example. Consider now the field of rational functions $k(t)$ over a finite field k. Recall from Section 3.1 that to every prime ideal $\mathfrak{p}$ of $k[t]$, we can associate a $\mathfrak{p}$-adic valuation $\nu_\mathfrak{p}$. Now take as a system of representatives R the field of coefficients k. Then by Proposition 3.12, the completion is the field of formal

power series $k((x)), x = t - a$, consisting of all formal Laurent series

$$f(t) = (t-a)^m(a_0 + a_1(t-a) + a_2(t - a^2 + \cdots)),$$

with $a_i \in k$ and $m \in \mathbb{Z}$.

We want to study algebraic field extensions L/K of complete valued fields K. To this end, we need to find a classification of the factorisation of algebraic equations over complete valued fields. For this, the following lemma, the proof of which we refer to [7], Lemma II.4.6, is crucial.

Lemma 3.13. ***(Hensel's Lemma)*** *Let K be a field which is complete with respect to a non-archimedean valuation $|\ |$ and let $\mathcal{O}_{|\ |}$ be the corresponding valuation ring with maximal ideal $\mathfrak{m}$ and residue class field $\kappa = \mathcal{O}_{|\ |}/\mathfrak{m}$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{O}_{|\ |}[x]$ be a primitive polynomial, i.e. $f(x) \not\equiv 0 \bmod \mathfrak{m}$.*[3]

If there is a factorisation modulo $\mathfrak{m}$

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \bmod \mathfrak{m}$$

of $f(x)$ into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$, then $f(x)$ also factorises as

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}_{|\ |}[x]$ such that $\deg(g) = \deg(\overline{g})$ and

$$g(x) \equiv \overline{g}(x) \bmod \mathfrak{m} \text{ and } h(x) \equiv \overline{h}(x) \bmod \mathfrak{m}.$$

Example. Consider the polynomial $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$, which splits into distinct linear factors over the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. After applying Lemma 3.13 repeatedly, we see that it also splits into linear factors over $\mathbb{Z}_p$. This implies that the field $\mathbb{Q}_p$ of p-adic numbers contains the $(p-1)$-th roots of unity, and these, together with 0, form a system of representatives for the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$. This system of representatives is closed under multiplication.

Example. In Hensel's Lemma 3.13, the condition on the factors to be relatively prime is necessary. For example, the polynomial $x^p - 1 \in \mathbb{Z}_p[x]$ factors as $x^p - 1 = (x-1)^p \bmod p$. These factors are not relatively prime. If Hensel's Lemma held nevertheless, the factorisation would also be true in $\mathbb{Q}_p$, which is clearly not true.

The proof of the following important theorem is lengthy and can be found in [7], Theorem II.4.8.

[3] This condition is equivalent to saying $|f| = \max\{|a_0|, \ldots, |a_n|\} = 1$.

Theorem 3.14. *Let K be a field which is complete with respect to the valuation $|\ |$. Then there is a unique extended valuation of $|\ |$ to a valuation of any given algebraic extension L/K. If L/K has finite degree n, then L is again complete and the extended valuation is given by*

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}.$$[4]

Theorem 3.14 implies that an exponential valuation ν on K associated with $|\ |$ extends uniquely to L as well. If L/K is finite of degree n, then the extended exponential valuation ω is given by

$$\omega(\alpha) = \frac{1}{n}\nu(N_{L/K}(\alpha)).$$

Recall that the (infinite) field extension we are interested in is the extension of a global field by its separable closure. This extension is algebraic, but the global field is not necessarily complete. Thus, we need a generalisation of Theorem 3.14, that allows us to find extensions of valuations of fields that are not necessarily complete. This brings us to henselian fields.

3.3 Henselian Fields

We want to relax the conditions of Hensel's Lemma 3.13 to not require completeness of the non-archimedean valued field. This is indeed possible because it turns out that Hensel's Lemma 3.13 holds for a wider class of non-archimedean valued fields, as the following example shows:

Example. Let (K, ν) be a non-archimedean valued field, $(\hat{K}, \hat{\nu})$ its completion, and let $\mathcal{O}_\nu$, resp. $\hat{\mathcal{O}}_\nu$, be the valuation rings of K, resp. $\hat{K}$. Then, if $\overline{K}$ denotes the separable closure of K in $\hat{K}$, we have $K \subseteq \overline{K} \subseteq \hat{K}$. Let $\overline{\mathcal{O}}_\nu$ denote the valuation ring of $\overline{K}$, with maximal ideal $\overline{\mathfrak{m}}$. Then $\overline{\mathcal{O}}_\nu$ is associated to the restriction of $\hat{\nu}$ to $\overline{K}$ and satisfies $\mathcal{O}_\nu \subseteq \overline{\mathcal{O}}_\nu \subseteq \hat{\mathcal{O}}_\nu$.

$\overline{K}$ is not complete (otherwise it would have to be equal to $\hat{K}$). Yet, Hensel's Lemma, Lemma 3.13, holds in the ring $\overline{\mathcal{O}}_\nu$ as well as in the ring $\hat{\mathcal{O}}_\nu$. Indeed, Proposition 3.11 implies $\mathcal{O}_\nu/\mathfrak{m} \cong \overline{\mathcal{O}}_\nu/\overline{\mathfrak{m}} \cong \hat{\mathcal{O}}_\nu/\hat{\mathfrak{m}}$. Thus, if a primitive polynomial $f(x) \in \overline{\mathcal{O}}_\nu[x]$ splits over $\overline{\mathcal{O}}_\nu/\overline{\mathfrak{m}}$ into relatively prime factors $\overline{g}(x), \overline{h}(x)$, then Hensel's Lemma, Lemma 3.13, gives a factorisation $f(x) = g(x)h(x)$ in $\hat{\mathcal{O}}_\nu$ such that $g \equiv \overline{g} \bmod \hat{\mathfrak{m}}, h \equiv \overline{h} \bmod \hat{\mathfrak{m}}, \deg(g) = \deg(\overline{g})$. But the highest coefficient of g can be chosen to be in $\overline{\mathcal{O}}_\nu^*$, so because the coefficients of f, and thus also those of g and h, are algebraic over K, this factorsation already takes place over $\overline{\mathcal{O}}_\nu$.

[4] Here, $N_{L/K}(\alpha)$ denotes the norm of the extension, i.e. the determinant of the endomorphism $L \to L : x \mapsto \alpha x$. If L/K is a Galois extension, then the norm is equal to the product of all the Galois conjugates of α, i.e. $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$.

Definition. Let (K, ν) be a non-archimedean valued field and $(\hat{K}, \hat{\nu})$ its completion. Then the valued field $\overline{K}$ is defined as the separable closure of K in $\hat{K}$ and is called the **henselisation** of K with respect to ν.

The henselisation has all the relevant algebraic properties of the completion $\hat{K}$, but is itself an algebraic extension of K and can thus be obtained in a purely alegbraic manner without the analytic construction of the completion. This allows taking the henselisation of an infinite algebraic extension L/K within the category of algebraic extensions.

Definition. A non-archimedean valued field (K, ν) is called **henselian** if its valuation ring $\mathcal{O}_\nu$ satisfies Hensel's Lemma, Lemma 3.13. The valuation ν or the valuation ring $\mathcal{O}_\nu$ are then also called henselian.

The following theorem is proved similarly to its analogue for complete fields, Theorem 3.14.

Theorem 3.15. *Let K be a henselian field with respect to a valuation $|\ |$. Then $|\ |$ can be extended uniquely to any given algebraic extension L/K. If the extension L/K has finite degree n, the extended valuation is given by*

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}.$$

In any case, the valuation ring of the extended valuation is equal to the integral closure of the valuation ring of K in L.

Remarkably, the converse of Theorem 3.15 is also true, i.e. unique extendability also characterises henselian fields. The proof of this uses the concept of a Newton polygon, which will not be dealt with here. The interested reader can find the proof in [7], Theorem II.6.6.

Theorem 3.16. *Let $(K, |\ |)$ be a non-archimedean valued field. Then K is henselian if and only if the valuation $|\ |$ extends uniquely to any algebraic extension.*

Let K be henselian with respect to a non-archimedean exponential valuation ν and let L/K be a finite field extension of degree n. As in the case of complete valued fields, exponential valuations of henselian fields also extend uniquely to exponential valuations of the field extension. The extended valuation ω of L is given by

$$\omega(\alpha) = \frac{1}{n}\nu(N_{L/K}(\alpha)).$$

This follows from Theorem 3.15 by taking the logarithm.

The value groups of ν and ω then satisfy $\nu(K^*) \subseteq \omega(L^*)$, and the residue class fields κ, resp. λ, of ν, resp. ω, satisfy $\kappa \subseteq \lambda$.

Definition. The group index $e = e(\omega/\nu) = (\omega(L^*) : \nu(K^*))$ is called the **ramification index** of the extension L/K. The degree $f = f(\omega/\nu) = [\lambda : \kappa]$ is called the **inertia degree**.

The ramification index and the inertia degree of an algebraic field extension L/K provide a useful tool for describing the extension of valuations in the field extension. Their most important properties are summarised in the next proposition, which is stated and proved in [7], Proposition II.6.8.

Proposition 3.17. *The ramification index e and the inertia degree f of a finite field extension L/K satisfy $[L : K] \geq ef$. Moreover, if the valuation ν of K is discrete and L/K is a separable extension, then the* ***fundamental identity*** *$[L : K] = ef$ holds.*

3.4 Valuations and Ideals

We have seen in the examples in Section 3.1 that we can associate valuations to the prime ideals of $\mathbb{Z}$ and of the polynomial ring $k[t]$ of a finite field. In fact, every prime ideal of the ring of integers of a field, can be associated to a valuation of that field. This enables us to switch between a valuation-theoretic perspective and an ideal-theoretic perspective. To see how, we first need to clarify what those terms mean in each particular setting. We begin by distinguishing **global** and **local** fields:

Definition. Let p be a prime number and $n \in \mathbb{N}$. We denote by $\mathbb{F}_q(t)$ the field of rational functions in one variable over the finite field with $q = p^n$ elements. A **function field** is a finite extension of $\mathbb{F}_q(t)$. An **algebraic number field** is a finite extension of the field of rational numbers $\mathbb{Q}$. A **global field** is a field that is either a function field, or an algebraic number field.

Definition. In contrast, **local fields** are finite extensions of either the field of p-adic numbers $\mathbb{Q}_p$ or of the field $\mathbb{F}_p((t))$ of formal Laurent series over a finite field $\mathbb{F}_p$. Equivalently, by Proposition II.5.2 in [7], a local field is a field which is complete with respect to a discrete non-archimedean valuation and has a finite residue class field.

Remark. We have already seen examples of how local fields arise as completions of valued fields with respect to discrete non-archimedean valuations. Recall the examples after Proposition 3.12.

Definition. (page 164 in [9]) Let K be a global field and let $\{\nu_i\}_i$ be the class of all non-archimedean valuations of K with respective valuation rings $\mathcal{O}_{\nu_i}$. Then

we define the **ring of integers** $\mathcal{O}_K$ of K as the intersection of all the valuation rings $\mathcal{O}_{\nu_i}$:

$$\mathcal{O}_K = \bigcap_i \mathcal{O}_{\nu_i}.$$

Proposition 3.18. *(Proposition 4-35 in [9]) If K is a global field, then its ring of integers $\mathcal{O}_K$ satisfies the following properties:*

(i). The ring $\mathcal{O}_K$ is a Dedekind domain. This means that it is an integrally closed (in its field of fractions) Noetherian domain with the property that every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

(ii). If the field K is a number field, i.e. has characteristic zero, then the ring $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. If K is a function field, i.e. has positive characteristic, then $\mathcal{O}_K$ is the integral closure of $\mathbb{F}_{p^n}[t]$ in K, for a prime number p.

Let K be a global field with a non-archimedean valuation ν. Since global fields have several different non-archimedean valuations (otherwise, they would be local), the ring of integers $\mathcal{O}_K$ of K and the valuation ring $\mathcal{O}_\nu$ satisfy

$$\mathcal{O}_K \subsetneq \mathcal{O}_\nu.$$

Example. Consider the field of rational numbers $\mathbb{Q}$ with the p-adic valuation, where p is a prime number. The valuation ring $\mathcal{O}_p$ is given by $\mathcal{O}_p = \{\frac{a}{n} \mid a, n \in \mathbb{Z}, p \nmid n\}$, which is also the localisation $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. By intersecting all valuation rings,

$$\bigcap_{p \text{ prime number}} \mathcal{O}_p = \bigcap_{p \text{ prime number}} \mathbb{Z}_{(p)} = \mathbb{Z},$$

we retrieve the ring of integers $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ of $\mathbb{Q}$, and see that $\mathcal{O}_\mathbb{Q} \subsetneq \mathcal{O}_p$.

In contrast:

Definition. Let K be a local field, i.e. K is complete with respect to a discrete exponential valuation ν. Then the **ring of integers** $\mathcal{O}_K$ of K is a local ring and is defined as the valuation ring $\mathcal{O}_\nu$ of ν, which we introduced on page 19.

Example. The local field $\mathbb{Q}_p$ of p-adic rationals is the completion of $\mathbb{Q}$ with respect to the p-adic valuation $|\ |_p$ induced by a prime number p. The ring of integers of $\mathbb{Q}_p$, which is also its valuation ring, is the ring of p-adic integers $\mathbb{Z}_p$. This ring is also the completion of the localisation $\mathbb{Z}_{(p)}$ from the previous example with respect to $|\ |_p$.

The ring of integers of a local field is a discrete valuation ring and hence, also a Dedekind domain. Being a local ring, it has only one non-trivial prime

ideal, which is also maximal, so many statements about the prime ideals of the ring of integers of a global field are trivially true for local fields. This is why the main part of this thesis is restricted to global fields.

Definition. Let K be a global field. We call a prime ideal of its ring of integers $\mathcal{O}_K$ a **prime of the field** K.

Example. (§I.14 in [7])Let p be a prime number, $n \in \mathbb{N}$ and $q = p^n$. The ring of integers of the function field $\mathbb{F}_q(t)$ is equal to the polynomial ring $\mathbb{F}_q[t]$. This is a principal ideal domain, hence also a Dedekind domain, where each nontrivial prime ideal is generated by a monic irreducible polynomial $p(t) \in \mathbb{F}_q[t]$.

Example. The ring of integers of the field $\mathbb{Q}$ is the integer ring $\mathbb{Z}$, which has prime ideals generated by prime numbers. Similarly, consider the algebraic number field $\mathbb{Q}(i)$ of Gaussian rationals. Its ring of integers is the ring of Gaussian integers $\mathbb{Z}[i]$. In this ring, the prime ideals are again generated by the prime elements. However, a prime element π of $\mathbb{Z}[i]$ is only given as either one of the following elements ([7], Theorem I.1.4):

(i). $\pi = 1 + i$,

(ii). $\pi = a + bi$, where $a^2 + b^2 = p$, $p \equiv 1 \bmod 4$, $a > |b| > 0$ and p is a prime number of $\mathbb{Z}$,

(iii). $\pi = p$, $p \equiv 3 \bmod 4$, where p is again a prime number of $\mathbb{Z}$.

Recall that in Dedekind domains, each non-zero proper ideal factors into a product of prime ideals. We will use this property to construct a valuation from a prime ideal.

Remark. We have already seen in an example in Section 3.1 how to construct a valuation from a prime ideal in the concrete example of a polynomial ring. As we know from the above example, a polynomial ring can be thought of as the ring of integers of a function field. We thus have a classification of the primes of function fields and their associated valuations.

The following construction follows page 165 in [7]. Let $\mathcal{O}_K$ be a Dedekind domain and K its fraction field. For instance, K could be a global field and $\mathcal{O}_K$ could be its ring of integers as defined above. Then we can associate to every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ the $\mathfrak{p}$-adic valuation $\nu_\mathfrak{p}$, defined by

$$\nu_\mathfrak{p}(a) = v_\mathfrak{p} \text{ , where } (a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}$$

for $a \in \mathcal{O}_K$. The valuation ring of $\nu_\mathfrak{p}$ is then the localisation of $\mathcal{O}_K$ at $\mathfrak{p}$. In the case where, for example, $K = \mathbb{Q}$, we retrieve the usual p-adic valuation that was introduced in Section 3.1.

Let now L/K be a finite field extension and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be prime ideals of $\mathcal{O}_L$ such that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

is the prime decomposition of $\mathfrak{p}$ in L. We often write $\mathfrak{p}$ instead of $\mathfrak{p}\mathcal{O}_L$ and say that the $\mathfrak{P}_i$ **lie over** $\mathfrak{p}$. This means that $\mathfrak{p} = \mathfrak{P}_\mathfrak{i} \cap \mathcal{O}_K$.

Then the valuations

$$\omega_i = \tfrac{1}{e_i}\nu_{\mathfrak{P}_i}, \text{ where } i = 1, \ldots, r,$$

are precisely the extensions of $\nu_\mathfrak{p}$ to L. The e_i are then the corresponding ramification indices and the $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ the inertia degrees. In this setting, the ideal $\mathfrak{p}$ is called **indecomposable** if $r = 1$, meaning that there is only one prime ideal of L lying over $\mathfrak{p}$ (page 49 in [7]).

Let L/K now be an infinite algebraic field extension, $\mathfrak{p}$ a prime of K, $\mathcal{O}_K$ the ring of integers of K and $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$, i.e. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. In order to find an expression for the valuation associated to $\mathfrak{P}$, which should also be the extension of the valuation associated to $\mathfrak{p}$, take $a \in \mathcal{O}_L$. Then there is an intermediate field M, such that M/K is finite and $a \in M$. If then $\mathcal{O}_M$ is the ring of integers of M, we can define an extension of the valuation $\nu_\mathfrak{p}$ to L as the valuation $\omega_{\mathfrak{P}\cap\mathcal{O}_M}(a)$ in the same way as before.

We claim that this valuation is independent of the choice of M. Indeed, if M' is a different intermediate field such that M'/K is finite and $a \in M'$, then there is a field M'' that contains both M and M' and extends K finitely. The prime ideal $\mathfrak{P}'' = \mathfrak{P} \cap \mathcal{O}_{M''}$ then lies over both $\mathfrak{P} \cap \mathcal{O}_M$ and $\mathfrak{P} \cap \mathcal{O}_{M'}$. Hence, $\omega_{\mathfrak{P}''}$ extends $\omega_{\mathfrak{P}\cap\mathcal{O}_{M'}}$ and $\omega_{\mathfrak{P}\cap\mathcal{O}_M}$. Thus, evaluated at $a \in \mathcal{O}_L$, we have $\omega_{\mathfrak{P}\cap\mathcal{O}_M}(a) = \omega_{\mathfrak{P}''}(a) = \omega_{\mathfrak{P}\cap\mathcal{O}_{M'}}(a)$. Therefore, the valuation $\omega_{\mathfrak{P}\cap\mathcal{O}_M}$ is independent of the choice of M.

The independence of M implies directly that the valuation $\omega_{\mathfrak{P}\cap\mathcal{O}_M}$ indeed defines a valuation on L, which by construction extends the one associated to $\mathfrak{p}$.

Hence, we see that, for global fields, we can always obtain a valuation from a prime ideal, and that a prime ideal being extended to a prime ideal lying over it in a field extension is analogous to extending a valuation to a valuation of the field extension. We will make use of this in later sections.

For a global field K, our main interest will lie in the extension $\overline{K}/K$, where

$\overline{K}$ denotes the separable closure of K. This field extension is Galois by Lemma 2.9 and it is, crucially, infinite. In infinite extensions, the above classification of an extended valuation is only useful if a concrete prime lying over a prime of the base field is known. It does not, however, give any information about how many extensions there are and what these extensions look like. Therefore, we need to study how valuations extend to algebraic extensions in general.

3.5 Arbitrary Extensions of Valuations

We have seen that henselian valuations extend uniquely to algebraic extensions. Now, we will examine how a valuation ν of a field K extends to an algebraic extension in general. Before diving into it, we fix some notation:

Notation. Let ν be a (non-archimedean) exponential valuation of a field K.

Let $|\ |_\nu$ be the corresponding multiplicative valuation.

Let K_ν denote the completion of K with respect to ν.

For every valuation ν of K, let K_ν^{alg} be the algebraic closure of K_ν.

We denote the canonical extension of ν to K_ν by ν again and the unique extension of this latter valuation to K_ν^{alg} by $\overline{\nu}$.

Let L/K be any algebraic extension. For instance, K could be a global field and L its separable closure $\overline{K}$. We choose a K-embedding $\tau : L \to K_\nu^{alg}$ and obtain an extension

$$\omega = \overline{\nu} \circ \tau$$

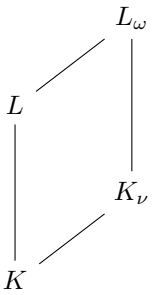
of the valuation ν to L, by restricting $\overline{\nu}$ to $\tau(L)$.

This can be translated to multiplicative valuations as follows: If ν, resp. $\overline{\nu}$, correspond to the absolute values $|\ |_\nu$, resp. $|\ |_{\overline{\nu}}$, on K, K_ν, resp. K_ν^{alg}, and $|\ |_{\overline{\nu}}$ extends the absolute value $|\ |_\nu$ of K_ν, then we obtain the absolute value $|x|_\omega = |\tau x|_{\overline{\nu}}$ on L.

The map $\tau : L \to K_\nu^{alg}$ is continuous with respect to this valuation and extends uniquely to a continuous K-embedding

$$\tau : L_\omega \to K_\nu^{alg}.$$

Here, if the extension L/K is infinite, L_ω does not denote the completion of L with respect to ω, but instead the union $L_\omega = \bigcup_i L_{i\omega}$ of the completions $L_{i\omega}$ of all finite subextensions L_i/K of L/K. This union is called the **localisation** of L with respect to ω. We have the following field diagram:



The valuation ω extends canonically from L to L_ω, and this extension is exactly the unique extension of the valuation ν from K_ν to the extension L_ω/K_ν. We have $L_\omega = LK_\nu$. Indeed, if L/K is finite, then Theorem 3.14 says that the field $LK_\nu \subseteq L_\omega$ is complete, contains the field L and is thus its completion. If L_ω/K_ν is finite, then, again by Theorem 3.14, we have $|x|_\omega = \sqrt[n]{|N_{L_\omega/K_\nu}(x)|_\nu}$.

The diagram shows that we can pass from a global extension L/K to a local extension L_ω/K_ν, which is called the **local-to-global principle**.

We have seen that for every K-embedding $\tau : L \to K_\nu^{alg}$, we can get an extension $\omega = \overline{\nu} \circ \tau$ of ν to L. Now we consider for every automorphism $\sigma \in \mathrm{Gal}(K_\nu^{alg}/K_\nu)$ of K_ν^{alg} over K_ν, the composite

$$L \xrightarrow{\tau} K_\nu^{alg} \xrightarrow{\sigma} K_\nu^{alg}$$

and obtain a new K-embedding $\tau' = \sigma \circ \tau$ of L. We say that it is **conjugate to** τ **over** K_ν. The following theorem, which is stated and proved in [7], Theorem II.8.1, describes the possible extensions of ν to L completely:

Theorem 3.19. ***(Extension Theorem)*** *Let L/K be an algebraic field extension and ν a valuation of K. Then:*

(i). Every extension ω of the valuation ν is a composite $\omega = \overline{\nu} \circ \tau$ for some K-embedding $\tau : L \to K_\nu^{alg}$.

(ii). Two extensions $\overline{\nu} \circ \tau$ and $\overline{\nu} \circ \tau'$ are equal if and only if τ and τ' are conjugate over K_ν.

The extension theorem gives us a recipe of how to find all extensions of a valuation ν by means of the extension of ν to the algebraic closure K_ν^{alg} of the completion K_ν. There is a concrete version of Theorem 3.19 for extensions given by algebraic equations.

Theorem 3.20. *Let $f(x) \in K[x]$ be an irreducible polynomial with root α and let $f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$ be its decomposition into irreducible factors over*

the completion K_ν. If $L = K(\alpha)$, then the valuations $\omega_1, \ldots, \omega_r$ extending ν to L correspond one-to-one to the irreducible factors $f_1, \ldots, f_r$.

Proof sketch. The K-embeddings $\tau : L \to K_\nu^{alg}$ are given by the roots β of $f(x)$ which lie in K_ν^{alg}, i.e.

$$\tau : L \to K_\nu^{alg}, \ \tau(\alpha) = \beta.$$

The embeddings τ and τ' are conjugate over K_ν if and only if the roots $\tau(\alpha)$ and $\tau'(\alpha)$ are conjugate over K_ν, i.e. if they are both roots of the same irreducible factor f_i. We can then apply Theorem 3.19 and get the statement of Theorem 3.20. □

The extended valuation ω_i can then explicitly be obtained from the irreducible factor f_i in the following way: Let $\alpha_i \in K_\nu^{alg}$ be a root of f_i and let

$$\tau_i : L \to K_\nu^{alg} : \alpha \mapsto \alpha_i$$

be the corresponding K-embedding of L into K_ν^{alg}. Then

$$\omega_i = \overline{\nu} \circ \tau_i,$$

and τ_i extends to an isomorphism

$$\tau_i : L_{\omega_i} \xrightarrow{\sim} K_\nu(\alpha_i)$$

on the completion L_{ω_i} of L with respect to ω_i.

As in the henselian case, we can define for any non-archimedean valuation ν, the **ramification index** of an extension ω/ν by $e_\omega = (\omega(L^*) : \nu(K^*))$ and the **inertia degree** by $f_\omega = [\lambda_\omega : \kappa]$, where λ_ω, resp. κ, is the residue class field of ω, resp. ν. As before, we then obtain the **fundamental identity of valuation theory** (Proposition II.8.5 in [7]):

Proposition 3.21. *Let ν be a discrete non-archimedean valuation and L/K a separable field extension. Then $\sum_{\omega/\nu} e_\omega f_\omega = [L : K]$.*

4 The Decomposition Group

The decomposition group is a subgroup of the Galois group that describes the splitting of prime ideals in Galois extensions. This point of view can be generalised to extensions of a valuation ν of a field K in a Galois extension L/K. This requires fixing a specific extension ω of ν and defining the decomposition group of this specific ω in the Galois group of L/K. From Section 3.5, we know that this puts us in a local situation, and we will see that there is an isomorphism between the decomposition group of an extended valuation ω in $\mathrm{Gal}(L/K)$ and the Galois group $\mathrm{Gal}(L_\omega/K_\nu)$ of the local fields localised at ω, resp. completing K with respect to ν.

This chapter follows §II.9 in [7].

4.1 First Definitions

Fix a (possibly infinite) Galois extension L/K with Galois group $G = \mathrm{Gal}(L/K)$. For instance, K could be a global field and L could be its separable closure $\overline{K}$. Recall that this extension is Galois by Lemma 2.9. Let ν be a non-archimedean valuation of K and ω an extension to L. For every $\sigma \in G$, the valuation $\omega \circ \sigma$ is also an extension of ν. In other words, the group G acts on the set of extensions ω/ν:

Proposition 4.1. *The Galois group G acts transitively on the set of extensions ω/ν. This means that any two extensions of ν are conjugate by G.*

Proof. Let ω and ω' be two extensions of ν to L. Suppose ω and ω' are not conjugate, i.e. the sets $\{\omega \circ \sigma \mid \sigma \in G\}$ and $\{\omega' \circ \sigma \mid \sigma \in G\}$ are disjoint. If L/K is finite, then by the Approximation Theorem, Theorem 3.3, there exists $x \in L$ such that

$$|\sigma x|_\omega < 1 \quad \text{and} \quad |\sigma x|_{\omega'} > 1$$

for all $\sigma \in G$. Then the norm $N = N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$ satisfies $|N|_\nu = \prod_\sigma |\sigma x|_\omega < 1$ and at the same time $|N|_\nu = \prod_\sigma |\sigma x|_{\omega'} > 1$, which is a contradiction.

So suppose that L/K is infinite. For every finite Galois subextension M/K, consider the set $X_M = \{\sigma \in G \mid \omega \circ \sigma|_M = \omega'|_M\}$. From the finite case, we know that these sets are non-empty for all finite subextensions M/K. The sets are also closed in the Krull topology since, if $\sigma \in G - X_M$, then the whole open neighbourhood $\sigma\,\mathrm{Gal}(L/M)$ is in the complement of X_M. If $\bigcap_M X_M = \varnothing$, then the complements of the X_M form an open cover of G. Since G is compact, there is a finite subcover of G, so we have $\bigcap_{i=1}^r X_{M_i} = \varnothing$ for finitely many M_i. But $\bigcap_{i=1}^r X_{M_i} = X_{M_1 \cdots M_r}$, a contradiction. Hence, $\bigcap_M X_M \neq \varnothing$ and ω and ω' are conjugate. □

Definition. For any Galois extension L/K and a valuation ν of K, we define the **decomposition group** of the extension ω of ν to L as the subgroup

$$G_\omega = G_\omega(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \omega \circ \sigma = \omega\}.$$

In light of Section 3.4, the decomposition group can also be defined from an ideal-theoretic viewpoint. Let L/K be a Galois extension, let $\mathcal{O}_K$ be the ring of integers of K, and let $\mathfrak{p}$ be a prime of K, as defined in Section 3.4. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L. Then $\mathcal{O}_L$ is the ring of integers of L. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Note that the valuation induced by $\mathfrak{P}$ is the extended valuation to the valuation induced by $\mathfrak{p}$ by the construction from Section 3.4. We can then define the decomposition group of a prime ideal:

Definition. If L/K is a field extension, $\mathfrak{p}$ is a prime of K and $\mathfrak{P}$ is a prime of L lying over $\mathfrak{p}$, then the **decomposition group** of $\mathfrak{P}$ over K is defined as

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

Definition. Let L/K be a Galois extension, ν a valuation of K and ω an extension of ν to L. The fixed field of the decomposition group G_ω is

$$Z_\omega = Z_\omega(L/K) = \{x \in L \mid \sigma x = x \text{ for all } \sigma \in G_\omega\}.$$

It is called the **decomposition field** of ω over K.

For a prime $\mathfrak{P}$ of L lying over a prime $\mathfrak{p}$ of K, we define the **decomposition field** of $\mathfrak{P}$ over K as

$$Z_\mathfrak{P} = Z_\mathfrak{P}(L/K) = \{x \in L \mid \sigma x = x \text{ for all } \sigma \in G_\mathfrak{P}\}.$$

Proposition 4.2. *In the same valuation-theoretic setting as in the above definition, let ω_Z be the restriction of ω to the decomposition field Z_ω. Then ω_Z extends uniquely to L.*

Proof. Note that an arbitrary extension ω' of ω_Z to L must be conjugate to ω over Z_ω, i.e. $\omega' = \omega \circ \sigma$, for some $\sigma \in \mathrm{Gal}(L/Z_\omega) = G_\omega(L/K)$. Thus, $\omega' = \omega$. □

The following proposition describes an important topological property of the decomposition group. Recall from Section 2.3 that the basis of the Krull topology on the Galois group $\mathrm{Gal}(L/K)$ is:

$$\{\sigma\,\mathrm{Gal}(L/M) \mid \sigma \in \mathrm{Gal}(L/K), M/K \text{ a finite Galois subextension of } L/K\}.$$

Proposition 4.3. *The decomposition group*

$$G_\omega = G_\omega(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \omega \circ \sigma = \omega\}$$

is closed in the Krull topology.

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ be in the closure of G_ω, i.e. in every neighbourhood $\sigma\,\mathrm{Gal}(L/M)$, there is some element σ_M of G_ω, for any finite Galois subextension M/K of L/K. Since $\sigma_M \in \sigma\,\mathrm{Gal}(L/M)$, we have $\sigma_M|_M = \sigma|_M$. Moreover, $\sigma_M \in G_\omega$, so $\omega \circ \sigma_M = \omega$, and this implies that

$$\omega \circ \sigma|_M = \omega \circ \sigma_M|_M = \omega|_M.$$

But the field L is the union of all the M, so $\omega \circ \sigma = \omega$. Therefore, $\sigma \in G_\omega$ and G_ω is closed in $\mathrm{Gal}(L/K)$. □

4.2 Functorial Properties of the Decomposition Group

Let L/K and L'/K' be two Galois extensions and let τ be a homomorphism $\tau : L \to L'$ such that $\mathrm{im}(\tau|_K) \subseteq K'$. Typically, τ will be the inclusion. Then the following diagram commutes:

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\tau} & K' \end{array}$$

The homomorphism τ induces a homomorphism

$$\tau^* : \mathrm{Gal}(L'/K') \longrightarrow \mathrm{Gal}(L/K) : \ \sigma' \longmapsto \tau^{-1}\sigma'\tau.$$

Since L/K is a normal extension, $\tau(L)/\tau(K)$ must also be normal, so $\sigma'\tau(L) \subseteq \tau(L)$ and composing with τ^{-1} makes sense. Note that we are only applying τ^{-1} to something in the image of τ.

Proposition 4.4. *Let ω' be a valuation of L', $\nu' = \omega'|_{K'}$ and $\omega = \omega' \circ \tau$, $\nu = \omega|_K$. Then the homomorphism $\tau^* : \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$ induces a homomorphism*

$$G_{\omega'}(L'/K') \longrightarrow G_\omega(L/K).$$

Proof. Let $\sigma' \in G_{\omega'}(L'/K')$ and $\sigma = \tau^*(\sigma')$. Then for $x \in L$, we have

$$|x|_{\omega\circ\sigma} = |\sigma x|_\omega = |\tau^{-1}\sigma'\tau x|_\omega = |\sigma'\tau x|_{\omega'} = |\tau x|_{\omega'} = |x|_\omega.$$

Hence, $\sigma \in G_\omega(L/K)$. □

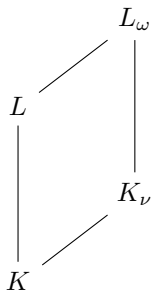
If the homomorphisms $\tau : L \to L'$ and $\tau : K \to K'$ are isomorphisms, then the above homomorphism is also an isomorphism. In particular, setting $K = K'$ and $L = L'$ gives:

Proposition 4.5. *Let L/K be a Galois extension, ν a valuation of K and ω its extension to L. Then the decomposition groups of conjugate valuations are conjugate, that is*

$$G_{\omega\circ\tau} = \tau^{-1} G_\omega \tau,$$

for all $\tau \in \mathrm{Gal}(L/K)$.

An important special case of Proposition 4.4 occurs in a situation that we introduced in Section 3.5. Let ω/ν be any extension of valuations of L/K. If L/K is infinite, then we consider the localisation L_ω, as discussed in Section 3.5. We have the following diagram:



In the local extension L_ω/K_ν, the extension of the valuation is unique. Since by Proposition 4.1, every $\sigma \in \mathrm{Gal}(L_\omega/K_\nu)$ maps extensions of ν to conjugate extensions of ν, this then means that $\omega \circ \sigma = \omega$. Hence, $\mathrm{Gal}(L_\omega/K_\nu) = G_\omega(L_\omega/K_\nu)$, so we denote the decomposition group simply by $\mathrm{Gal}(L_\omega/K_\nu)$. In this case, the homomorphism τ^* from Proposition 4.4 is the restriction map

$$\mathrm{Gal}(L_\omega/K_\nu) \longrightarrow \mathrm{Gal}(L/K) : \sigma \longmapsto \sigma|_L.$$

This gives rise to the following proposition:

Proposition 4.6. *Let L/K be a Galois extension, ν a valuation of K, ω an extension of ν to L, K_ν the completion of K with respect to ν and L_ω the localisation of L with respect to ω, as defined on page 31 in Section 3.5. Then the decomposition group of the global extension L/K is isomorphic to the Galois group of the local extension L_ω/K_ν:*

$$G_\omega(L/K) \cong \mathrm{Gal}(L_\omega/K_\nu) = G_\omega(L_\omega/K_\nu)$$

Before we can prove Proposition 4.6, we need the following Lemma:

Lemma 4.7. *The decomposition group $G_\omega(L/K)$ is composed precisely of all automorphisms $\sigma \in \mathrm{Gal}(L/K)$ which are continuous with respect to the valuation ω.*

Proof of Lemma 4.7. Note that all automorphisms $\sigma \in G_\omega(L/K)$ are necessarily continuous because $|\sigma x|_\omega = |x|_{\omega\circ\sigma} = |x|_\omega$, for $x \in L$.

Now let $\sigma \in \mathrm{Gal}(L/K)$ be continuous. For $x \in L$, we have that $|x|_\omega < 1$ implies that x^n and, hence, also σx^n are ω-nullsequences, i.e. $|\sigma x|_\omega < 1$. But $|\sigma x|_\omega = |x|_{\omega\circ\sigma}$. So we have:

$$|x|_\omega < 1 \implies |x|_{\omega\circ\sigma} < 1.$$

Thus, by Proposition 3.1, ω and $\omega \circ \sigma$ are equivalent. Since $\omega|_K = \omega \circ \sigma|_K$, they are in fact equal. Hence, $\sigma \in G_\omega(L/K)$. □

Proof of Proposition 4.6. We know by Proposition 4.4 that there is a homomorphism

$$G_\omega(L_\omega/K_\nu) \longrightarrow G_\omega(L/K)$$

Recall that L is dense in the localisation L_ω. Thus, every $\sigma \in G_\omega(L/K)$ extends uniquely to a continuous K_ν-automorphism $\hat{\sigma}$ of L_ω, i.e. $\hat{\sigma} \in \mathrm{Gal}(L_\omega/K_\nu)$. By Lemma 4.7, then $\hat{\sigma} \in G_\omega(L_\omega/K_\nu)$. □

Proposition 4.6 allows us to reduce problems concerning a single valuation ω of L to a local situation by identifying the decomposition group of L/K with respect to ω with the Galois group of L_ω/K_ν:

$$G_\omega(L/K) = \mathrm{Gal}(L_\omega/K_\nu).$$

The following example shows an application of this.

Example. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Then the Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ contains only two elements, the identity and complex conjugation. The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, and the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. As we know, the primes of $\mathbb{Q}$ are generated by prime numbers p. Recall from Section 3.4 that the primes of $\mathbb{Q}(i)$ are generated by either $1+i$, or $a+bi$, where $a^2+b^2 = p$, $a > |b| > 0$, $p \in \mathbb{Z}$ is prime and $p \equiv 1 \mod 4$, or by a prime number $p \in \mathbb{Z}$ that satisfies $p \equiv 3 \mod 4$.

(i). The prime ideal $2\mathbb{Z}$ of $\mathbb{Z}$ lies only under the prime ideal $(1+i)$ of $\mathbb{Z}[i]$ because $2 \equiv 0 \mod (1+i)$ and $i(1+i) = (-1)(1-i)$. Then $G_{(1+i)} = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ and by Proposition 4.6, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}_2(i)/\mathbb{Q}_2)$.

(ii). If $p \in \mathbb{Z}$ is prime such that $p \not\equiv 3 \mod 4$, then the ideal (p) of $\mathbb{Z}$ lies under the two distinct prime ideals $(a+bi)$ and $(a-bi)$ of $\mathbb{Z}[i]$, where $a^2+b^2 = p$

and $a > |b| > 0$. Then $G_{(1+i)} = G_{(1-i)} = \{1\}$. But by Proposition 4.6, this also means that $\mathrm{Gal}(\mathbb{Q}_p(i)/\mathbb{Q}_p) = \{1\}$, which implies that $i \in \mathbb{Q}_p$. To prove that this is indeed the case, it suffices to find a root of -1 in $\mathbb{F}_p$. Then the polynomial (x^2+1) splits into distinct linear factors in $\mathbb{F}_p[x]$ and by Hensel's Lemma 3.13, also in $\mathbb{Z}_p[x]$, so $i \in \mathbb{Q}_p$.

To find a root of -1 in $\mathbb{F}_p$, note that since $p \not\equiv 3 \mod 4$, we have $4|p-1$, which implies that there exists an element of $\mathbb{F}_p$ of order 4. This means that there exists $\alpha \in \mathbb{F}_p$ such that $\alpha^4 = 1$. Hence, $\alpha^2 = -1$.

(iii). The prime ideal of $\mathbb{Z}$ generated by a prime number $p \in \mathbb{Z}$ such that $p \equiv 3 \mod 4$ lies only under the prime ideal of $\mathbb{Z}[i]$ generated by that same prime number p. Then (p), as a prime of $\mathbb{Q}$, is indecomposable and $G_{(p)} = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. This is equal to $\mathrm{Gal}(\mathbb{Q}_p(i)/\mathbb{Q}_p)$ by Proposition 4.6.

We saw in Lemma 4.7 that the decomposition group $G_\omega = G_\omega(L/K)$ of a Galois extension L/K consists of precisely those automorphisms of $G = \mathrm{Gal}(L/K)$ that are continuous with respect to the extended valuation ω. Hence, the decomposition group gives a group-theoretic interpretation of the extension of ν to L. In fact, it also contains information about the number of extensions of ν to L:

Proposition 4.8. *Let L/K be a Galois extension, ν a valuation of K and ω an extension of ν to L. Then the set of all extensions of ν to L is in bijection with the quotient group $G_\omega\backslash G$.*

Proof. Denote by W_ν the set of extensions of ν to L. The group $G_\omega\backslash G$ consists of all right cosets $G_\omega\sigma$. By choosing a fixed extension ω, we obtain a bijection

$$G_\omega\backslash G \xrightarrow{\sim} W_\nu : G_\omega\sigma \longmapsto \omega\sigma.$$

□

Remark. In particular, Proposition 4.8 implies that if L/K is finite, then the cardinality of W_ν is equal to the group index $(G : G_\omega)$.

Applying Proposition 4.8 in the case of valuations induced by prime ideals, we get:

Corollary 4.9. *Let L/K be a Galois extension, $\mathfrak{p}$ a prime of K and $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$. Then $\mathfrak{p}$ is indecomposable in L if and only if the decomposition group $G_\mathfrak{P}$ is isomorphic to the Galois group $\mathrm{Gal}(L/K)$.*

5 The Centre of the Absolute Galois Group

5.1 The Main Result

In this section, we will finally be able to prove the main result of this thesis, namely that the absolute Galois group of a global field has trivial centre. This will be done by proving that the decomposition groups of distinct prime ideals intersect trivially. In order to be able to do this, we will first need to think about what we can say about the splitting fields of two polynomials with sufficiently small distance from each other. The following convenient lemma is a first step towards this goal.

Recall that Theorem 3.14 says, in particular, that any valuation of a complete valued field K extends uniquely to an algebraic closure of K.

This section follows the first part of §12.1 in [8].

Lemma 5.1. ***(Krasner's Lemma)*** *Let K be a complete field with respect to a non-archimedean valuation $|\ |_K$. Let K^{alg} be an algebraic closure of K, $\alpha \in K^{alg}$ and let $\alpha = \alpha_1, \ldots, \alpha_n$ be conjugates of α over K. We denote by $|\ |$ the unique extension of the valuation $|\ |_K$ to K^{alg}. If, for $\beta \in K^{alg}$ and $i = 2, \ldots, n$, we have*

$$|\alpha - \beta| < |\alpha - \alpha_i|,$$

then $K(\alpha) \subseteq K(\beta)$.

Proof. Consider the field extension $K(\alpha, \beta)/K(\beta)$ and let $L/K(\beta)$ be the minimal extension of $K(\alpha, \beta)/K(\beta)$ such that $L/K(\beta)$ is Galois [5] and let $\sigma \in \mathrm{Gal}(L/K(\beta))$. Then $\sigma(\beta - \alpha) = \beta - \sigma(\alpha)$. Since the extended valuation is unique, we have $|\sigma(x)| = |x|$ for all $x \in L$, by Proposition 4.1. Therefore,

$$|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha| < |\alpha_i - \alpha|,$$

for $i = 2, \ldots, n$. This implies

$$|\alpha - \sigma(\alpha)| = |\alpha - \beta + \beta - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\} < |\alpha - \alpha_i|$$

for $i = 2, \ldots, n$, because of Proposition 3.4. Hence, as by Lemma 2.2, $\sigma(\alpha) \in \{\alpha_1, \ldots, \alpha_n\}$, we get $\sigma(\alpha) = \alpha$, so $\alpha \in K(\beta)$. □

We can apply this to prove:

Lemma 5.2. *Let K be a field which is complete with respect to a valuation $|\ |$. Then for any separable polynomial $f = a_0 + a_1 x + \cdots + a_d x^d \in K[x]$, there exists*

[5] This is called the Galois closure of $K(\alpha, \beta)/K(\beta)$.

$\varepsilon > 0$ such that if $g = b_0 + b_1 x + \cdots + b_d x^d \in K[x]$ is any other polynomial satisfying

$$|f - g| := \max_{j=0,\ldots,d} |a_j - b_j| < \varepsilon,$$

then g and f have the same splitting field.

Proof. If $K = \mathbb{C}$, there is nothing to prove, by the Fundamental Theorem of Algebra. If $K = \mathbb{R}$ and f has d different roots in $\mathbb{R}$, then the same is true for every g sufficiently near to f, so f and g have the same splitting field. If $K = \mathbb{R}$ and f has a root in $\mathbb{C} - \mathbb{R}$, then every g sufficiently near to f also has such a root, by complex analysis. Therefore, by Ostrowski's Theorem, Theorem 3.9, we may assume that the valuation is non-archimedean.

Let g be near to f and α be a root of f in the separable closure $\overline{K}$ of K. Then $|g(\alpha)| = |(g - f)(\alpha)|$ is small. Denoting the roots of g by $\beta_1, \ldots, \beta_d$, we can write

$$g = c \prod_j (x - \beta_j)$$

and see that $|\alpha - \beta|$ is small for some root β of g. For g sufficiently near to f, we can, in particular, choose a root β of g such that

$$|\beta - \alpha| < |\alpha_i - \alpha|$$

for all other roots $\alpha_i \neq \alpha$ of f. Since these are all conjugates of α over K, we can apply Krasner's Lemma, Lemma 5.1, and get that $\alpha \in K(\beta)$. Hence, the splitting field of f is contained in the splitting field of g if g is sufficiently near to f.

Repeating the same argument for all roots $\alpha_1, \ldots, \alpha_d$ of f, we find for every i, a root $\beta_{j(i)}$ of g which is sufficiently near to α_i. Since f is separable, the roots $\alpha_1, \ldots, \alpha_d$ are pairwise different, so for g sufficiently near to f, there is a bijection $\alpha_i \leftrightarrow \beta_{j(i)}$ between the zero-sets of both polynomials, such that

$$|\beta_{j(i)} - \alpha_i| < |\beta_{j(i)} - \beta_j|,$$

for all i and all $j \neq j(i)$. Applying Krasner's Lemma, Lemma 5.1, again, we see that the splitting field of g is contained in that of f, provided that the distance between f and g is sufficiently small. □

Let K be a field with its separable closure $\overline{K}$. Recall from Lemma 2.9 that the extension $\overline{K}/K$ is Galois. The following proposition is crucial in classifying distinct decomposition groups.

Proposition 5.3. *Let K be a global field, $\overline{K}$ its separable closure and M a*

proper subfield of $\overline{K}$. Then M has at most one prime which is indecomposable in $\overline{K}$.

Proof. Suppose that M has two different primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ that are indecomposable in $\overline{K}$, meaning that in the extension $\overline{K}/M$, there is only one prime ideal of $\overline{K}$ lying over $\mathfrak{p}_1$ and only one prime ideal of $\overline{K}$ lying over $\mathfrak{p}_2$.

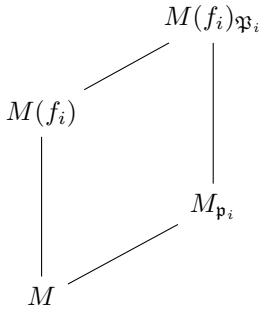
Let f_1 and f_2 be arbitrary separable polynomials in $M[x]$ of equal degree d and let $\varepsilon > 0$. We construct a new polynomial, for which we choose d coefficients, and apply the Approximation Theorem, Theorem 3.3, to two valuations in order to find a polynomial $f \in M[x]$ such that $|f - f_1|_{\mathfrak{p}_1} < \varepsilon$ and $|f - f_2|_{\mathfrak{p}_2} < \varepsilon$. Here, the distance between two polynomials is defined as in the statement of Lemma 5.2. Since Lemma 5.2 only holds for complete valued fields, we consider the completion $M_{\mathfrak{p}_i}$ of M with respect to the $\mathfrak{p}_i$-adic valuation on M, for $i = 1, 2$. The lemma then implies that, for ε sufficiently small, f and f_1 have the same splitting field over $M_{\mathfrak{p}_1}$, and f and f_2 have the same splitting field over $M_{\mathfrak{p}_2}$.

Let $i \in \{1, 2\}$ and let $M_{\mathfrak{p}_i}(f_i)$ denote the splitting field of f_i over the completion $M_{\mathfrak{p}_i}$. Analogously, let $M_{\mathfrak{p}_i}(f)$ denote the splitting field of f over $M_{\mathfrak{p}_i}$. Then, since $M_{\mathfrak{p}_i}(f_i) = M_{\mathfrak{p}_i}(f)$, the Galois groups satisfy

$$\mathrm{Gal}(M_{\mathfrak{p}_i}(f_i)/M_{\mathfrak{p}_i}) = \mathrm{Gal}(M_{\mathfrak{p}_i}(f)/M_{\mathfrak{p}_i}). \tag{5.1}$$

Note that these extensions are finite and Galois by an example in Chapter 2, page 7.

Let $M(f_i)$ denote the splitting field of f_i over M, let $\mathfrak{P}_i$ be a prime ideal of $M(f_i)$ lying over $\mathfrak{p}_i$ in $M(f_i)$ and let $M(f_i)_{\mathfrak{P}_i}$ denote the completion of $M(f_i)$ with respect to $\mathfrak{P}_i$. We have the following local-to-global situation:



Since $\mathfrak{p}_i$ is indecomposable in $\overline{K}$ by assumption, $\mathfrak{p}_i$ is also indecomposable in $M(f_i)$. Thus, $\mathfrak{P}_i$ is unique, so by Proposition 3.21, we have

$$[M(f_i)_{\mathfrak{P}_i} : M_{\mathfrak{p}_i}] = [M(f_i) : M].$$

This implies that the splitting field of f_i over $M_{\mathfrak{p}_i}$ is $M(f_i)_{\mathfrak{P}_i}$, i.e.

$$M_{\mathfrak{p}_i}(f_i) = M(f_i)_{\mathfrak{P}_i}.$$

Analogously, one finds that $M_{\mathfrak{p}_i}(f) = M(f)_{\mathfrak{P}}$, where $\mathfrak{P}$ denotes a prime ideal of $M(f)$ lying over $\mathfrak{p}_i$ [6] and $M(f)_{\mathfrak{P}}$ denotes the completion of $M(f)$ with respect to $\mathfrak{P}$.

From Proposition 4.6, we know that the decomposition group $G_{\mathfrak{P}_i}$ satisfies

$$G_{\mathfrak{P}_i}(M(f_i)/M) = \mathrm{Gal}(M(f_i)_{\mathfrak{P}_i}/M_{\mathfrak{p}_i}).$$

Then, by (5.1), we have

$$G_{\mathfrak{P}_i}(M(f_i)/M) = G_{\mathfrak{P}}(M(f)/M).$$

But as $\mathfrak{p}_i$ is indecomposable in $\overline{K}$, Corollary 4.9 implies that the decomposition group $G_{\mathfrak{P}_i}(M(f_i)/M)$ is isomorphic to the whole Galois group $\mathrm{Gal}(M(f_i)/M)$. Analogously, $G_{\mathfrak{P}}(M(f)/M)$ is isomorphic to $\mathrm{Gal}(M(f)/M)$. Hence,

$$\mathrm{Gal}(M(f_i)/M) = \mathrm{Gal}(M(f)/M).$$

Then, by the Fundamental Theorem of Infinite Galois Theory, Theorem 2.16, it follows that $M(f_i) = M(f)$. In particular,

$$M(f_1) = M(f_2),$$

i.e. the splitting fields of f_1 and f_2 over M coincide.

We can then apply this result to any separable, irreducible polynomial f_1 and to an f_2 written as $f_2 = \prod_{i=1}^{d}(x - \alpha_i)$, where the α_i are pairwise different elements in M. Since f_1 is separable, it splits in $\overline{K}$, so the union of the splitting fields of all the possible f_1's is equal to $\overline{K}$. But f_2 has splitting field M, so $M = \overline{K}$. □

Example. Recall the example after Proposition 4.6, where we found that in the extension $\mathbb{Q}(i)/\mathbb{Q}$, there are two prime ideals of $\mathbb{Q}$, which are indecomposable in $\mathbb{Q}(i)$. Therefore, we see that the statement of Proposition 5.3 necessarily requires considering a prime ideal decomposition in the separable closure.

Remark. Note that Proposition 5.3 is trivially true for a local field because its ring of integers, which is also its valuation ring, is a discrete valuation domain, and thus has only one non-trivial prime ideal, which is also maximal.

[6] It is a slight abuse of notation to use the same symbol $\mathfrak{P}$ for a prime ideal lying over $\mathfrak{p}_1$ as well as over $\mathfrak{p}_2$. Yet, we will see that it is indeed the same prime ideal.

Corollary 5.4. *Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be distinct prime ideals of the separable closure $\overline{K}$ of a global field K. Then their decomposition groups have trivial intersection:*

$$G_{\mathfrak{P}_1} \cap G_{\mathfrak{P}_2} = \{1\}.$$

Proof. Consider the decomposition fields

$$Z_{\mathfrak{P}_1} = \{x \in \overline{K} \mid \sigma x = x \text{ for all } \sigma \in G_{\mathfrak{P}_1}\}$$

and

$$Z_{\mathfrak{P}_2} = \{x \in \overline{K} \mid \sigma x = x \text{ for all } \sigma \in G_{\mathfrak{P}_2}\}.$$

Let $\mathfrak{p}_1$ be a prime of $Z_{\mathfrak{P}_1}$ lying under $\mathfrak{P}_1$ and $\mathfrak{p}_2$ a prime of $Z_{\mathfrak{P}_2}$ lying under $\mathfrak{P}_2$. Recall that this means that $\mathfrak{p}_i = \mathfrak{P}_i \cap Z_{\mathfrak{P}_i}$, for $i \in \{1, 2\}$. By Proposition 4.1, for $i \in \{1, 2\}$, $G_{\mathfrak{P}_i}$ acts transitively on the extensions of $\mathfrak{p}_i$. But by definition of $G_{\mathfrak{P}_i}$, $G_{\mathfrak{P}_i}$ fixes $\mathfrak{P}_i$. Thus, $\mathfrak{P}_i$ is the only extension of $\mathfrak{p}_i$ to $\overline{K}$. Note that this extension is well-defined by Proposition 4.2. Hence, also $\mathfrak{p}_1 \neq \mathfrak{p}_2$, since otherwise $\mathfrak{P}_1 = \mathfrak{P}_2$.

Now assume that $G_{\mathfrak{P}_1} \cap G_{\mathfrak{P}_2} \neq \{1\}$. By Proposition 4.3, $G_{\mathfrak{P}_1} \cap G_{\mathfrak{P}_2}$ is a closed subgroup of $\mathrm{Gal}(\overline{K}/K)$, so by the Fundamental Theorem of Infinite Galois Theory, Theorem 2.16, we can consider the fixed field $M := \overline{k}^{G_{\mathfrak{P}_1} \cap G_{\mathfrak{P}_2}}$, which is a proper subfield of $\overline{K}$ by assumption and by Theorem 2.16 again. Then M has two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, which each have only one extension to $\overline{K}$. This is a contradiction to the previous proposition. □

Corollary 5.5. *Let $\mathfrak{P}$ be a prime ideal of $\overline{K}$. Then the decomposition group $G_{\mathfrak{P}}$ is its own normaliser in the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$.*

Proof. Let $N = N_{G_K}(G_{\mathfrak{P}}) = \{g \in G_k \mid G_{\mathfrak{P}}^g := gG_{\mathfrak{P}}g^{-1} = G_{\mathfrak{P}}\}$ denote the normaliser of $G_{\mathfrak{P}}$. Trivially, $G_{\mathfrak{P}} \subseteq N$. Note that

$$G_{g\mathfrak{P}} = \{\sigma \in G_K \mid \sigma g\mathfrak{P} = g\mathfrak{P}\} = \{\sigma \in G_K \mid g^{-1}\sigma g\mathfrak{P} = \mathfrak{P}\} = G_{\mathfrak{P}}^g.$$

Hence, if $g \in N$, then $G_{g\mathfrak{P}} = G_{\mathfrak{P}}$. Then, by the previous corollary, $g\mathfrak{P} = \mathfrak{P}$ (otherwise, the decomposition groups would have to intersect trivially), which implies $g \in G_{\mathfrak{P}}$, so $N \subseteq G_{\mathfrak{P}}$. □

Proposition 5.6. *Let K be a global field and let G_K denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K. Then the canonical homomorphism*

$$G_K \longrightarrow \mathrm{Aut}(G_K) : \sigma \longmapsto (g \mapsto \sigma g \sigma^{-1})$$

is injective.

Proof. Assume σ lies in the kernel. Then σ is such that $\sigma g \sigma^{-1} = g$ for all $g \in G_K$, so $\sigma X \sigma^{-1} = X$ for all subsets $X \subseteq G_K$. In particular, σ fixes the decomposition group $G_{\mathfrak{P}}$ of every prime $\mathfrak{P}$ of $\overline{k}$, i.e. $\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\mathfrak{P}}$. By Corollary 5.5, then $\sigma \in G_{\mathfrak{P}}$. By the same reasoning, $\sigma \in G_{\sigma\mathfrak{P}}$. Hence, $G_{\mathfrak{P}} \cap G_{\sigma\mathfrak{P}} \neq \{1\}$. But then Corollary 5.4 implies that $\sigma\mathfrak{P} = \mathfrak{P}$ for all prime ideals $\mathfrak{P}$ of $\overline{K}$. This means that $\sigma \in G_{\mathfrak{P}}$ for every prime $\mathfrak{P}$. But any two distinct decomposition groups must have trivial intersection. Otherwise, all prime ideals of $\overline{K}$ would be equal. Hence, σ is trivial. □

Corollary 5.7. *The absolute Galois group G_K of a global field K has trivial centre.*

Proof. The previous proposition says that the only element $\sigma \in G_K$ which satisfies $\sigma g \sigma^{-1} = g$ for all $g \in G_K$, i.e. $\sigma g = g\sigma$ for all $g \in G_K$, is the identity automorphism. This is equivalent to saying that G_K has trivial centre. □

Corollary 5.7 has interesting arithmetic implications. For, if the centre of G_K, for a global field K, *did* contain non-trivial elements, then this would mean that there are extraordinarily convenient Galois extensions of K in its separable closure $\overline{K}$, the Galois-automorphisms of which would commute with the Galois-automorphisms of *all* other extensions of K in $\overline{K}$. Corollary 5.7 tells us that such extensions do not exist.

Moreover, the triviality of the centre of G_K is an important step in the proof of the Neukirch-Uchida Theorem, which we will briefly treat in the next section.

5.2 Application to the Neukirch-Uchida Theorem

The Neukirch-Uchida Theorem is one of the most important results in anabelian geometry. This area is concerned with finding a way to recover an arithmetic variety from its étale fundamental group. The term "anabelian" here refers to groups with the property that all of their subgroups of finite index have trivial centre.

The Neukirch-Uchida Theorem states that it is indeed possible to characterise an algebraic number field K by its absolute Galois group G_K. To formulate the theorem precisely, we will first need to define profinite groups. The following definitions are taken from §I.2.4 in [1] and [6].

Definition. Let I be a directed poset and $(X_i)_{i \in I}$ a family of sets together with maps $\pi_{ij} : X_j \to X_i$, for $i, j \in I, i \leq j$, such that

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

(ii). for all $i, j, k \in I$, there is the relation $\pi_{ij} \circ \pi_{jk} = \pi_{ik}$.

Then $(X_i)_{i\in I}$ is called a **projective system**.

A projective system is called **surjective** if all π_{ij} are surjective.

Definition. Let $((X_i)_{i\in I}, (\pi_{ij}))$ be a projective system of sets. Then the **inverse limit** $\varprojlim_{i\in I} X_i$ is the subspace defined as

$$\varprojlim_{i\in I} X_i = \Big\{(x_i)_{i\in I} \in \prod_{i\in I} X_i \mid \pi_{ij}(x_j) = x_i \text{ for all } i \leq j\Big\}.$$

Definition. A topological group G is called **profinite** if it is isomorphic to an inverse limit of a surjective projective system of finite groups. It inherits the subspace topology from the product, while every finite group has the discrete topology.

In Proposition 11 in [6], it is shown that a topological group is profinite if and only if it is Hausdorff, compact and totally disconnected. Thus, by Theorem 2.14, the Galois group of an arbitrary Galois extension is a profinite group under the Krull topollogy. Hence, in particular, the absolute Galois group of an algebraic number field is a profinite group.

Let now G_1 and G_2 be profinite groups and let $\mathrm{Iso}(G_1, G_2)$ denote the set of isomorphisms between them. An automorphism is called an **inner automorphism** if it arises from conjugation with a fixed element ([4], page 91). So let the group of inner automorphisms of G_1, resp. G_2, be denoted by $\mathrm{Inn}(G_1)$, resp. $\mathrm{Inn}(G_2)$. The group $\mathrm{Inn}(G_2)$ acts on $\mathrm{Iso}(G_1, G_2)$ by the action $\sigma(\phi) = \sigma \circ \phi$. The quotient

$$\mathrm{OutIso}(G_1, G_2) := \mathrm{Iso}(G_1, G_2)/\,\mathrm{Inn}(G_2)$$

is then called the set of **outer isomorphisms** from G_1 to G_2.

The Neukirch-Uchida Theorem, as formulated in Corollary 12.2.2 in [8], then states:

Theorem 5.8. ***(Neukirch-Uchida)*** *Let K_1 and K_2 be algebraic number fields and let G_{K_1} and G_{K_2} be their respective absolute Galois groups. Then the natural map*

$$\mathrm{Iso}(K_2, K_1) \longrightarrow \mathrm{OutIso}(G_{K_1}, G_{K_2})$$

is an isomorphism.

This amounts to saying that every outer isomorphism between absolute Galois groups arises from a uniquely determined isomorphism between algebraic number fields.

The proof of the Neukirch-Uchida Theorem can be found in §12.2 of [8]. In the proof of the theorem, our main result, Corollary 5.7, is used to show uniqueness of the isomorphism between the algebraic number fields.

6 References

[1] Gregory Berhuy. *London mathematical society lecture note series: An introduction to Galois cohomology and its applications series number 377*. Cambridge University Press, Cambridge, England, September 2010.

[2] David S Dummit and Richard M Foote. *Abstract Algebra*. John Wiley & Sons, Nashville, TN, 3 edition, June 2003.

[3] Pierre Antoine Grillet. *Abstract Algebra*. Graduate Texts in Mathematics. Springer, New York, NY, 2 edition, July 2007.

[4] Thomas W Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer, Berlin, Germany, December 1996.

[5] Patrick J Morandi. *Field and Galois theory*. Graduate Texts in Mathematics. Springer, New York, NY, 1996 edition, July 1996.

[6] Abhijit Mudigonda. Profinite groups and infinite galois theory. Website. url: https://abhijit-mudigonda.github.io/math/infgalois.pdf.

[7] Jürgen Neukirch. *Algebraic number theory*. Grundlehren der mathematischen Wissenschaften. Springer, Berlin, Germany, December 2010.

[8] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer, 2015.

[9] Dinakar Ramakrishnan and Robert J Valenza. *Fourier analysis on number fields*. Graduate Texts in Mathematics. Springer, New York, NY, 1999 edition, December 1998.

[10] William Stein. A brief introduction to classical and adelic algebraic number theory. Website, May 2004. url: https://wstein.org/papers/ant/ant.pdf.