GLOBAL FIELD ISOMORPHISMS: A CLASS FIELD THEORETICAL APPROACH

SUBMITTED BY
HARRY SMIT

IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF MATHEMATICAL SCIENCES

Department of Mathematics
Faculty of Science
Utrecht University

SUPERVISOR: Gunther Cornelissen
SECOND READER: Frits Beukers

June 2016

Harry Smit, BSc, 3870901: *Global field isomorphisms: a class field theoretical approach*

SUPERVISOR:
Gunther Cornelissen

SECOND READER:
Frits Beukers

UNIVERSITY:
Utrecht University

TIME FRAME:
October 2015 — June 2016

ABSTRACT

This master's thesis, *Global field isomorphisms: a class field theoretical approach*, was written by Harry Smit from October 2015 until June 2016. It is submitted to the Department of Mathematics at Utrecht University. The research was conducted under supervision of professor Gunther Cornelissen, and the second reader is professor Frits Beukers.

After an introduction into both local and global class field theory, we investigate two objects that uniquely determine the isomorphism type of a global field K, following an unpublished article of Cornelissen, Li, and Marcolli. Firstly, we use the maximal abelian Galois group to create a topological space X_K and subsequently a dynamical system by defining an action $I_K \curvearrowright X_K$ of the integral ideals I_K on X_K. Secondly, we combine the maximal abelian Galois group with the Dirichlet L-series. Both these objects can be described using only objects from within K itself. The original contributions in this thesis are the proof that X_K is a Hausdorff space and various improvements on the proofs given by Cornelissen, Li, and Marcolli.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the help and support of many individuals. I would like to extend my gratitude to all of them.

Foremost, I would like to thank my supervisor Gunther Cornelissen and second reader and mentor Frits Beukers.

Gunther Cornelissen has been a great supervisor throughout the duration of the thesis: even though he has an extremely busy schedule, he has always found the time to listen to my questions, remarks, and attempts at proofs. I have greatly enjoyed these last months under his supervision, and I would like to express my deepest gratitude for his efforts.

Frits Beukers has played a significant role in my development as a mathematician, especially in the years prior to my thesis. As the supervisor of my bachelor's thesis and mentor of my master's programme, I have always felt that he created a welcoming environment. I appreciate it that he took the time to be the second reader. Many thanks to him.

I would also like to thank Merlijn Staps, Daniël Kroes, and Pol van Hoften. Merlijn has helped me with my thesis presentation, which improved greatly thanks to him. With Daniël I had weekly meetings, in which he provided comments on my work, listened to my mathematical problems, and gave insight on the process of writing a thesis from his own experience. Pol and Daniël helped with the written part of the thesis: they improved sentences, removed unnecessary comments, and improved the overall structure of the proofs. All three have been very helpful, for which I would like to express my gratitude.

My family also deserves my appreciation. Both my parents, Ronald and Anne-Marie, and my sister, Nimuë, have been extremely supportive throughout my entire education, for which I would like to thank them.

John Voight was very helpful when I asked him some questions on topology, aside from being exceedingly friendly and quick to respond. Many thanks to him.

Lastly, I would like to thank André Miede for creating this LaTeX template bundle.

CONTENTS

1 INTRODUCTION

The main objects of study in this thesis are *global fields*: finite algebraic extensions of $\mathbb{Q}$ (which are known as *number fields*) or $\mathbb{F}_q(T)$ for some transcendental T and prime power q (known as *function fields*). They find their use in solving *Diophantine equations*: polynomial equations over $\mathbb{Z}$ or $\mathbb{F}_q[T]$ in one or more variables, where we are interested in the solutions that are defined over $\mathbb{Z}$ or $\mathbb{F}_q[T]$ respectively. One of the questions that arises from the study of global fields is the following:

Given two global fields, can we determine whether or not they are isomorphic (as fields)?

It is important to note that we assume no information other than the global fields themselves, hence we can only use information that we can obtain from objects within the global fields themselves, such as the ring of integers, prime ideals or the Dedekind zeta function.

The strategy we follow in this thesis is to determine objects associated to a global field that determines the isomorphism type of the underlying field. However, they still have the requirement that they can be described or at least approximated using objects within the field itself, as only objects with such a description will aid in determining whether two fields are isomorphic. We will therefore focus on partially answering the following question:

What objects associated to a global field uniquely determine the underlying field, yet can be described using only objects within the field?

Finding these objects has historically not been a simple task. For example, number fields with identical Dedekind zeta function are not necessary isomorphic ([Gas26]), even though this implies the existence of a norm-preserving bijection between the primes of the number fields. An example of an object that does contain sufficient information is the Galois group of a separable closure (this is known as the Neukirch–Uchida theorem, see [Iva13]), but it has the drawback that it is difficult to describe.

Our approach is to consider the *abelian* extensions of a field. The study of these extensions is called *class field theory*, whose main theorems allow us to describe the abelian extensions using the prime ideals and embeddings of the field via the *localisations* of the global field. Unfortunately, the Galois groups of the abelian extensions do not quite uniquely define the isomorphism type of the underlying field ([AS12]). We can, however, combine the abelian extensions with other describable objects such that the isomorphism type *is* uniquely determined, following a preprint by Cornelissen, Li, and Marcolli ([CLM16]). One such combination we consider is the abelian extensions with localisations to obtain a topological space on which the monoid of integral ideals acts. This creates a dynamical system, which we will prove to contain enough information. The second approach we take is combining the abelian extensions with the Dirichlet L-series, which will also prove to be sufficient.

Part I

PRELIMINARIES

2

TOPOLOGY

This introductory chapter starts with basic definitions and theorems in topology on Hausdorff and (locally) compact spaces. The second section deals with topological groups, which play a central role in the extension of the fundamental theorem of Galois theory to include infinite extensions (Theorem 3.2.6). In the final section we consider a construction of a topological space known as the restricted product.

2.1 HAUSDORFF AND COMPACT SPACES

We briefly state the definition of Hausdorff, compact, and locally compact spaces as we will encounter these quite often. We also prove some basic theorems.

2.1.1 HAUSDORFFNESS

Definition 2.1.1 (HAUSDORFF)**.** A topological space X is said to be Hausdorff if for every distinct $x, y \in X$ there exist opens $U \ni x$ and $V \ni y$ such that $U \cap V = \emptyset$. ◁

From this definition it follows that subspaces of Hausdorff spaces and products of Hausdorff spaces are Hausdorff themselves.

Proposition 2.1.2. A topological space X is Hausdorff precisely when $\Delta_X = \{(x, x) \in X \times X : x \in X\}$, the *diagonal of* X, is closed. ◁

Proof. Suppose X is Hausdorff. For any pair of elements $x, y \in X$ with $x \neq y$ there exist open neighbourhoods U of x and V of y such that $U \cap V = \emptyset$. Thus $U \times V$ is an open neighbourhood of $(x, y) \in X \times X$ that has empty intersection with Δ_X, implying that $(X \times X) - \Delta_X$ is open.

On the other hand, if $(X \times X) - \Delta_X$ is open, then for any $(x, y) \in (X \times X) - \Delta_X$ there exists an open $B \subseteq X \times X$ in the basis of open sets, i. e. of the form $U \times V$ with U and V open in X, containing (x, y), that does not intersect Δ_X. Hence U and V do not intersect, while $x \in U$ and $y \in V$, thus X is Hausdorff. ❐

Proposition 2.1.3. Let f be a continuous function from a topological space X to a Hausdorff space Y. Then the *graph* $G_f := \{(x, f(x)) \in X \times Y \mid x \in X\}$ is closed in $X \times Y$. ◁

Proof. Let $(x, y) \in (X \times Y) - G_f$. As Y is Hausdorff, there exist open neighbourhoods $U \ni y$, $V \ni f(x)$ such that their intersection is empty. Let $W = f^{-1}(V)$, which is open as f is continuous. We claim that the open neighbourhood $W \times U$ of (x, y) does not intersect G_f, proving that $(X \times Y) - G_f$ is open and subsequently that G_f is closed. Suppose $(z, f(z)) \in W \times U$. Then, as $z \in W$, we have $f(z) \in V$, hence $f(z) \in U \cap V = \emptyset$, a contradiction. We conclude that $(W \times U) \cap G_f = \emptyset$, and the result follows. ❐

Corollary 2.1.4. As a result of this this proposition, the graph map $g_f : X \to X \times Y$ is a closed map, as the image of g_f is closed and g_f restricts to a homeomorphism $X \to G_f$ (the inverse is given by projection to the first coordinate). ◁

2.1.2 COMPACT SPACES

Compact spaces play a central role in topology throughout this thesis, mainly in Chapter 4 on local fields. Especially the interaction between Hausdorffness and compactness will be used extensively.

Definition 2.1.5 (COMPACT). A topological space X is compact if for every open cover of X there exists a finite open subcover, i. e. for any index set I and open sets U_i for $i \in I$ such that $\bigcup_{i\in I} U_i = X$, there exists a finite subset J of I such that $\bigcup_{i\in J} U_i = X$. ◁

Proposition 2.1.6. Let X be a compact space and $C \subseteq X$ a closed subset. Then C is compact. ◁

Proof. Let $\{U_i : i \in I\}$ be an open cover of C. As C is closed, $X - C$ is open, hence $\{U_i : i \in I\} \cup \{X - C\}$ is an open cover of X. As X is compact, the cover can be reduced to a finite open cover. Removing $X - C$ from this cover gives a finite subcover of $\{U_i : i \in I\}$ of C. □

Lemma 2.1.7 (TUBE LEMMA). Let X be a space and Y a compact space. For each $x \in X$ and open $U \subseteq X \times Y$ such that $\{x\} \times Y \subseteq U$, there exists an open $V \subseteq X$ such that $x \in V$ and $V \times Y \subseteq U$. ◁

Proof. Let $x \in X$ and $U \subseteq X \times Y$ open such that $\{x\} \times Y \subseteq U$. For any $y \in Y$ there is an open neighbourhood of (x, y) of the form $A_y \times B_y$ contained in U, as U is open. Because $Y = \bigcup_{y\in Y} B_y$ is compact, there exist finitely many $y_1, \ldots, y_n$ such that $Y = \bigcup_{i=1}^n B_{y_i}$. Let $V = \bigcap_{i=1}^n A_{y_i}$, which is open as the intersection is finite. Moreover, we have $x \in A_{y_i}$ for all y_i, hence $x \in V$, and for any $v \in V$ and $1 \leq i \leq n$ we find that $v \in A_{y_i}$, hence $\{v\} \times B_{y_i} \subseteq U$, hence $\{v\} \times \bigcup_{i=1}^n B_{y_i} = \{v\} \times Y \subseteq U$, and we conclude that

$$\{x\} \times Y \subseteq V \times Y \subseteq U.$$

□

Corollary 2.1.8. Let X be a space and Y a compact space. Then the projection map $\pi : X \times Y \to X$ is closed. ◁

Proof. Let C be a closed subset of $X \times Y$. Suppose $x \notin \pi(C)$. We prove that there is an open neighbourhood of x that does not intersect $\pi(C)$. Then $\pi^{-1}(x) = \{x\} \times Y$ is disjoint from C, hence contained in the open set $(X \times Y) - C$. By application of the Tube Lemma, there is an open V such that $V \times Y$ is disjoint from C, hence V is disjoint from $\pi(C)$. Thus we have found an open neighbourhood of x that does not intersect $\pi(C)$, which completes the proof. □

Theorem 2.1.9 (TYCHONOFF). Let $\{X_i : i \in I\}$ be an indexed set of non-empty Hausdorff spaces. Then $X = \prod X_i$ is compact if and only if each X_i is compact. ◁

Proof. Theorem 5D of [Loo53]. □

Proposition 2.1.10. Suppose C is a compact subset of a Hausdorff space X. Then C is closed. ◁

Proof. We prove that any element $x \in X - C$ has an open neighbourhood that does not intersect C. For any $c \in C$, as X is Hausdorff, there exists an open neighbourhood $V(c)$ that does not contain x. Note that $\{V(c) \cap C : c \in C\}$ forms an open cover of C, and as C is compact, can be reduced to a finite subcover $\{V(c_1) \cap C, \ldots, V(c_n) \cap C\}$. For each $V(c_i)$, as again X is Hausdorff, there exists a $U_i(x)$ such that $U_i(x) \cap V(c_i) = \emptyset$.

Let $U = \bigcap_{i=1}^{n} U_i(x)$, then U is an open neighbourhood of x which does not intersect any of the $V(c_i)$. However, as they formed a cover of C, we have $U \cap C = \emptyset$, which concludes the proof. ❐

Proposition 2.1.11. Let $f : X \to Y$ be a continuous map to a Hausdorff space Y. If $C \subset X$ is compact, then $f(C)$ is compact. ◁

Proof. Suppose $C \subset X$ is compact and let $\{V_i : i \in I\}$ be an open cover of $f(C)$. Then $\{f^{-1}(V_i) : i \in I\}$ is an open cover of C as f is continuous (and C is mapped into $f(C)$). As C is compact, there exists a finite subcover $\{f^{-1}(V_1), \ldots, f^{-1}(V_n)\}$ of C. As C is mapped surjectively to $f(C)$, $f(f^{-1}(V_i)) = V_i$. Moreover, as $\{f^{-1}(V_1), \ldots, f^{-1}(V_n)\}$ covers C, we find that $\{f(f^{-1}(V_1)), \ldots, f(f^{-1}(V_n))\} = \{V_1, \ldots, V_n\}$ covers $f(C)$, hence $f(C)$ is compact. ❐

Like many properties of topological spaces, there exists a local variant of compactness, which is slightly weaker than compactness itself:

Definition 2.1.12 (LOCALLY COMPACT)**.** A topological space X is called locally compact if every point $x \in X$ has a compact neighbourhood (when equipped with the subspace topology). ◁

2.2 TOPOLOGICAL GROUPS

The majority of spaces that we will be working with in later chapters are examples of *topological groups*: groups equipped with a topology that respects the group operations. We define them here and prove some basic properties. The important result is Corollary 2.2.7, which will be applied on a certain topological space in Chapter 9.

Definition 2.2.1 (TOPOLOGICAL GROUP)**.** A group G equipped with a topology is called a *topological group* if the multiplication and inversion maps

$$G \times G \longrightarrow G \qquad G \longrightarrow G$$

$$(g, h) \longmapsto gh \qquad g \longmapsto g^{-1}.$$

are continuous.

We say that two topological groups G, G' are *isomorphic as topological groups* if there exists a map $f : G \to G'$ that is both an isomorphism of groups and a homeomorphism. ◁

Remark. The maps *left* and *right multiplication* with a certain element $\sigma \in G$ are homeomorphisms, as they are continuous and the inverse is multiplication with σ^{-1}. In particular, they are open and closed maps.

Remark. In Chapter 9 we will also use *topological monoids*: they are monoids equipped with a topology such that the multiplication map is continuous.

The subgroups of topological groups that are open or closed often play a central role. We have the following lemma:

Lemma 2.2.2. Let G be a topological group. Any open subgroup of G is closed. Moreover, any closed subgroup of finite index is open. ◁

Proof. Any subgroup H of G induces cosets σH, $\sigma \in G$. We have

$$H = G - \bigcup_{\sigma : \sigma H \neq H} \sigma H.$$

If H is open, σH is open for any $\sigma \in G$, hence H is closed. If H is closed, then all σH are closed. If H is then additionally of finite index, there exist only finitely many different cosets, hence $\bigcup_{\sigma : \sigma H \neq H} \sigma H$ is closed, thus H is open. ❐

2.2.1 CONTINUOUS GROUP ACTIONS

As the name suggests, continuous group actions are a certain type of *group action*, which we will define first:

Definition 2.2.3 (GROUP ACTION)**.** A *group action* of a group G on a set X is a map $\phi : G \times X \to X$ such that $\phi(e, x) = x$ and $\phi(g, \phi(h, x)) = \phi(gh, x)$ for all $g, h \in G$, $x \in X$. ◁

Note that there is no topology involved in group actions, neither on G, nor on X. Topologies play a role if we require the group action to be *continuous*:

Definition 2.2.4 (CONTINUOUS GROUP ACTION)**.** Let G be a topological group and X a topological space. A continuous group action of G on X is a group action of G on the set X such that

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

is continuous. ◁

Proposition 2.2.5. Let G act continuously on a topological space X. Then X/G is Hausdorff if and only if the image of the action map $\alpha : G \times X \to X \times X$ given by $(g, x) \mapsto (x, gx)$ is closed. ◁

Proof. We know that a topological space Y is Hausdorff precisely when the diagonal Δ_Y is closed in $Y \times Y$.

Let $\Delta = \Delta_{X/G}$. The projection map $\pi : X \to X/G$ is continuous, surjective, and open, hence the same holds for $\tau = \pi \times \pi : X \times X \to X/G \times X/G$. Consider

$$U := (X/G \times X/G) - \Delta,$$

which is open in $X/G \times X/G$ iff Δ is closed. Because τ is surjective, $\tau(\tau^{-1}(U)) = U$, and as τ is open and continuous, we find that $U = \tau(\tau^{-1}(U))$ is open precisely when $\tau^{-1}(U)$ is open. However,

$$\tau^{-1}(U) = \{(x, y) \in X \times X \mid \nexists\, g \in G \text{ such that } gx = y\} = (X \times X) - \mathrm{im}(\alpha),$$

hence we conclude that X/G is Hausdorff if and only if α has closed image. ❐

Proposition 2.2.6. If G is a compact group acting continuously on a Hausdorff space X, then the action map α is a closed map. ◁

Proof. We split the action map into two parts:

$$G \times X \longrightarrow G \times X \times X \longrightarrow X \times X$$

$$(g, x) \longmapsto (g, x, gx) \longmapsto (x, gx).$$

The first map is the graph of the continuous map $f : (g, x) \mapsto gx$, hence its image G_f is closed as X is Hausdorff, see Proposition 2.1.3. Moreover, the graph map of f is continuous and, by restricting its codomain to the image G_f, has a continuous inverse $G_f \to G \times X$ (projection onto the first two coordinates), thus the graph map is a homeomorphism onto its image. As the image G_f is closed, it follows that the graph map is a closed map. As the second map is a a projection map and G is compact, it is closed by Corollary 2.1.8. Hence the composition α is closed as well. ❐

Corollary 2.2.7. If G is a compact group acting continuously on a Hausdorff space X, then X/G is Hausdorff. ◂

Proof. The result follows from combining Proposition 2.2.5 and Proposition 2.2.6. ❐

2.3 RESTRICTED PRODUCTS

In this final section of the chapter we introduce a construction of a topological space known as a *restricted product*, which is necessary for the definition of adeles and ideles in Chapter 7.

Definition 2.3.1 (RESTRICTED PRODUCT)**.** Given an index set I and topological spaces X_i with open subsets $Y_i \subseteq X_i$ for all $i \in I$, the *restricted product*, denoted $\prod'_{i \in I}(X_i, Y_i)$, is a topological space that consists of all elements $x = (x_i)_{i \in I}$ in $\prod_{i \in I} X_i$ such that $x_i \in Y_i$ for all but finitely many $i \in I$.

A basis of the open sets of the topology on $\prod'_{i \in I}(X_i, Y_i)$ is given by sets of the form $\prod_{i \in I} U_i$, where U_i is open in X_i and $U_i = Y_i$ for almost all $i \in I$. ◂

This is a topology different than the topology on $\prod'(X_i, Y_i)$ as a subset of $\prod X_i$. The open set $\prod Y_i$ in the restricted product does not contain an open set in the standard basis of the direct product.

Example. Let $\{A_i : i \in I\}$, be a family of abelian groups equipped with the discrete topology. Then

$$\prod_{i \in I}{}'(A_i, \{1\}) = \bigoplus_{i \in I} A_i.$$

Proposition 2.3.2. Let S be a finite subset of I, and

$$X_S = \prod_{i \in S} X_i \times \prod_{i \notin S} Y_i.$$

Then X_S is open in X and the topology on X_S as a subset of X is the same as the topology on X_S as the direct product of the X_i and Y_i. ◂

Proof. X_S is part of the aforementioned basis of opens, hence open. A basis of open subsets of X_S are the sets that are a product of the Y_i for almost all $i \in I$ (as S is finite), which is exactly a basis of open subsets of the product topology of the X_i and Y_i. ❐

Proposition 2.3.3. Let X be a restricted product $\prod'_{i\in I}(X_i, Y_i)$. Suppose all X_i are locally compact and the Y_i are compact. Then X is locally compact. ◅

Proof. Note that the product of infinitely many locally compact spaces is in general not locally compact.

Let $S \subseteq I$ be any finite set. The product $\prod_{i\notin S} Y_i$ is compact by Theorem 2.1.9 and $\prod_{i\in S} X_i$ is locally compact as the product is finite. Hence the set X_S is locally compact. As we have $X = \bigcup_S X_S$, and the X_S are open in X, any open in X_S is open in X, thus any neighbourhood of a point in X_S is also a neighbourhood of that point in X. Because the X_S are locally compact, so is X. ❐

3

GALOIS THEORY

In Chapter 6 and 7 on class field theory, we will be working extensively with infinite Galois extensions. This chapter is an introduction to infinite Galois theory. We start by extending the fundamental theorem of Galois theory to infinite extensions with the use of topology, after which we investigate the structure of Galois groups of infinite extensions.

3.1 FINITE GALOIS THEORY

This section will be very short: the results of the theory of finite Galois extensions is summarised nicely in the fundamental theorem of Galois theory.

Theorem 3.1.1 (FUNDAMENTAL THEOREM OF GALOIS THEORY)**.** Let L/K a finite Galois extension. There exists a bijection

$$\{\text{finite extensions of } K\} \longleftrightarrow \{\text{subgroups of } \mathrm{Gal}(L/K)\}$$

that restricts to a bijection

$$\{\text{finite Galois extensions of } K\} \longleftrightarrow \{\text{normal subgroups of } \mathrm{Gal}(L/K)\}.$$

The bijections are given by $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$. ◁

We will not provide a proof here, as Theorem 3.2.6 is an extended version of this theorem, for which we will provide a proof.

Moreover, we will sometimes require the *primitive element theorem*:

Theorem 3.1.2 (PRIMITIVE ELEMENT THEOREM)**.** For every finite separable extension of fields L/K there exists an $\alpha \in L$ such that $L = K(\alpha)$. ◁

Proof. See [Gre11]. ❐

3.2 INFINITE GALOIS THEORY

The fundamental theorem of Galois theory in its current form does not hold for infinite extensions, of which we will see an example below. However, only a slight adaptation has to be made, which can be described beautifully with the help of a topology. Using this topology, we prove an extended version of the fundamental theorem of Galois theory, Theorem 3.2.6. This section follows a structure similar to that of Neukirch's Class Field Theory, [Neu86].

3.2.1 THE FUNDAMENTAL THEOREM

Aside from extensions of finite degree, many fields K has infinite algebraic extensions as well. One such extension is a *separable algebraic closure* K^s, containing all algebraic separable extensions of K. If K is a perfect field, then K^s is equal to the algebraic closure.

The extension K^s/K is Galois and the Galois group $\mathrm{Gal}(K^s/K)$ is known as the *absolute Galois group* of K. It is an interesting object of study as it describes all finite Galois extensions of K. A separable algebraic closure is unique up to isomorphism, which is why we will now fix a separable closure en refer to it as *the* separable closure and denote it by K^s. It is obtained by taking the composite of all finite algebraic separable extensions.

A slightly smaller, but still often an infinite extension of K, is the *maximal abelian extension* K^{ab} of K, contained in our separable closure. It contains all finite abelian extensions, i. e. finite Galois extensions with abelian Galois group. Not unlike the separable algebraic closure, it is constructed by taking the composite of all finite abelian extensions. The maximal abelian Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ will be the main object of study in Chapters 6 and 7.

Theorem 3.2.1. The composite of two Galois extensions is again Galois. ◁

Proof. Proposition 1.1 of [Smi04]. ❐

Theorem 3.2.2. Let L/K and M/K be finite abelian extensions. Then the composite $L \cdot M$ is again an abelian extension of K. ◁

Proof. By the primitive element theorem, Theorem 3.1.2, $L = K(\alpha)$ and $M = K(\beta)$, hence $L \cdot M = K(\alpha, \beta)$. Thus, any Galois element of $L \cdot M$ is determined uniquely by the image of α and β, so we obtain an homomorphism

$$\begin{aligned} \mathrm{Gal}(L \cdot M/K) &\to \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \sigma &\mapsto (\sigma\big|_L, \sigma\big|_M), \end{aligned}$$

which is injective because when $\sigma\big|_L = e$, then $\sigma(\alpha) = \alpha$ and when $\sigma\big|_M = e$, $\sigma(\beta) = \beta$, hence any σ in the kernel acts trivially on $K(\alpha, \beta) = L \cdot M$.

Thus $\mathrm{Gal}(L \cdot M/K)$ is a subgroup of the abelian group $\mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, and therefore abelian itself. ❐

An question is whether Theorem 3.1.1 still holds for infinite extensions. For this we consider the case where K is a finite field, e.g. $\mathbb{F}_p$ for some prime p.

Example. The field $\mathbb{F}_p$ is perfect (as it is finite), hence $\mathbb{F}_p^s$ is the algebraic closure $\overline{\mathbb{F}}_p$. All finite extensions of $\mathbb{F}_p$ are of the form $\mathbb{F}_{p^n}$, $n \in \mathbb{N}$. While we currently do not know the exact structure of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, it certainly contains the *Frobenius automorphism* ϕ defined by $\phi(x) = x^p$ for all $x \in \overline{\mathbb{F}}_p$. Consider the subgroup of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ generated by ϕ, i. e. the subgroup $\Phi = \{\phi^n : n \in \mathbb{Z}\}$. As ϕ only leaves the base field $\mathbb{F}_p$ fixed, the fixed field of Φ is $\mathbb{F}_p$. Hence, if the infinite equivalent of Theorem 3.1.1 were to hold, we should have $\Phi = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

To show that it does not, we construct an element of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ that does not lie in Φ. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of integers such that $a_n \equiv a_m \pmod m$ whenever $m \mid n$, but there exists no integer a such that $a \equiv a_n \pmod n$ for all $n \in \mathbb{N}$. An example of such a sequence can be created by letting $a_p = 1$ for all primes p, then $a_{p^n} = a_{p^{n-1}} + p^{n-1}$ for all $n \in \mathbb{N}$, and finally all other a_n are now fixed by the Chinese Remainder Theorem. Suppose there exists an $a \in \mathbb{Z}$ such that $a \equiv a_n \pmod n$. As $a_p \equiv 1 \pmod p$ for all primes p, we find that a must equal 1. However, $a_4 = 3$, which gives a contradiction. Hence no a such that $a \equiv a_{p^n} \pmod{p^n}$ for all $n \in \mathbb{N}$ exists.

Now let $\psi_n = \phi^{a_n}\big|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. A subfield of $\mathbb{F}_{p^n}$ is of the form $\mathbb{F}_{p^m}$ where $m \mid n$. As a result,

$$\psi_n\big|_{\mathbb{F}_{p^m}} = \phi^{a_n}\big|_{\mathbb{F}_{p^m}} = \phi^{a_m}\big|_{\mathbb{F}_{p^m}} = \psi_m,$$

as $a_n \equiv a_m \mod m$ and the order of $\phi|_{\mathbb{F}_{p^m}}$ is m.

As $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$, the ψ_n together form an automorphism ψ of $\overline{\mathbb{F}}_p$ (that leaves $\mathbb{F}_p$ fixed). However, $\psi \notin \Phi$, because $\psi = \phi^a$ for some $a \in \mathbb{Z}$ would imply that $\phi^a|_{\mathbb{F}_{p^n}} = \psi|_{\mathbb{F}_{p^n}} = \phi^{a_n}|_{\mathbb{F}_{p^n}}$ for all $n \in \mathbb{N}$, hence $a \equiv a_n \pmod n$ for all $n \in \mathbb{N}$, which contradicts the construction of $(a_n)_{n\in\mathbb{N}}$.

With this example we see that Theorem 3.1.1 does not hold for infinite extensions. However, not all hope is lost. In the upcoming we will derive a theorem that is highly similar to the theorem in the finite case, but requires some extra work. This effort will be put in via the use of a topology, which helps to mark all groups that still have a sense of Galois correspondence.

Definition 3.2.3 (KRULL TOPOLOGY)**.** Let L/K be a (possibly infinite) Galois extension. We equip $\mathrm{Gal}(L/K)$ with a topology, known as the *Krull topology*. For any $\sigma \in \mathrm{Gal}(L/K)$ we take the cosets $\sigma\mathrm{Gal}(L/E)$ as a basis of neighbourhoods of σ, where E/K runs through all finite Galois extensions of K contained in L. ◂

Proposition 3.2.4. $\mathrm{Gal}(L/K)$ is a topological group when equipped with the Krull topology. ◂

Proof. For the extent of this proof, denote by m the multiplication map and i the inverse map. To prove that these are continuous it suffices to check this on the given basis of open neighbourhoods.

First we prove that for any finite Galois extension E/K, the group $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. As E/K is a finite Galois extension, it is the splitting field of a polynomial $f \in K[X]$. Every element $\sigma \in \mathrm{Gal}(L/K)$ permutes the roots of the polynomial, hence $\sigma E = E$. As a result, for any $\tau \in \mathrm{Gal}(L/E)$ and $x \in E$ $\sigma^{-1}(\tau(\sigma(x))) = \sigma^{-1}(\sigma(x)) = x$, where $\tau(\sigma(x)) = \sigma(x)$ as $\sigma(x) \in E$. As a result, $\sigma^{-1}\tau\sigma$ is trivial on E, hence $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$, showing that $\mathrm{Gal}(L/E)$ is normal in $\mathrm{Gal}(L/K)$.

We turn to proving that the multiplication map is continuous. Let $\alpha \in \mathrm{Gal}(L/K)$ and E/K a finite Galois extension, from which we obtain a basic open neighbourhood $\alpha\mathrm{Gal}(L/E)$ of α. Take any $(\sigma, \tau) \in m^{-1}(\alpha\mathrm{Gal}(L/E))$, then $\alpha\mathrm{Gal}(L/E) = \sigma\tau\mathrm{Gal}(L/E)$ as $\alpha^{-1}\sigma\tau \in \mathrm{Gal}(L/E)$. Thus it now suffices to show that

$$\sigma\mathrm{Gal}(L/E)\tau\mathrm{Gal}(L/E) \subseteq \sigma\tau\mathrm{Gal}(L/E),$$

because then (σ, τ) has an open neighbourhood $\sigma\mathrm{Gal}(L/E) \times \tau\mathrm{Gal}(L/E)$ contained in $m^{-1}(\alpha\mathrm{Gal}(L/E))$, proving that $m^{-1}(\alpha\mathrm{Gal}(L/E))$ is open. As $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$, we obtain $\mathrm{Gal}(L/E)\tau = \tau\mathrm{Gal}(L/E)$, thus $\mathrm{Gal}(L/E)\tau\mathrm{Gal}(L/E) \subseteq \tau\mathrm{Gal}(L/E)$, and consequently $\sigma\mathrm{Gal}(L/E)\tau\mathrm{Gal}(L/E) \subseteq \sigma\tau\mathrm{Gal}(L/E)$.

All that remains is to show that the inverse map is continuous. Take an open basic neighbourhood $\alpha\mathrm{Gal}(L/E)$ of some $\alpha \in \mathrm{Gal}(L/K)$ and suppose $\sigma \in i^{-1}(\alpha\mathrm{Gal}(L/E))$. We will prove that $\sigma\mathrm{Gal}(L/E) \subseteq i^{-1}(\alpha\mathrm{Gal}(L/E))$, from which it follows that the set $i^{-1}(\alpha\mathrm{Gal}(L/E))$ is open. We have $i(\sigma\mathrm{Gal}(L/E)) = (\sigma\mathrm{Gal}(L/E))^{-1} = \mathrm{Gal}(L/E)^{-1}\sigma^{-1} = \mathrm{Gal}(L/E)\sigma^{-1}$ as $\mathrm{Gal}(L/E)$ is a group. Moreover, as it is a normal subgroup of $\mathrm{Gal}(L/K)$, we have $\mathrm{Gal}(L/E)\sigma^{-1} = \sigma^{-1}\mathrm{Gal}(L/E)$. Then, because $\sigma^{-1} = i(\sigma) \in \alpha\mathrm{Gal}(L/E)$,

we find that $i(\sigma\mathrm{Gal}(L/E)) = \sigma^{-1}\mathrm{Gal}(L/E) \subseteq \alpha\mathrm{Gal}(L/E)$, and we conclude that $\sigma\mathrm{Gal}(L/E) \subseteq i^{-1}(\alpha\mathrm{Gal}(L/E))$. ❐

Remark. For any Galois group of a finite Galois extension, the Krull topology is the discrete topology. Any topology that makes a finite group a topological group is the discrete topology.

From now on, whenever we mention a Galois group, we automatically assume that it is equipped with the Krull topology.

Proposition 3.2.5. Let L/K be a Galois extension. The Galois group $\mathrm{Gal}(L/K)$ is Hausdorff and compact. ◅

Proof. We start with Hausdorffness. Suppose $\sigma \neq \tau \in \mathrm{Gal}(L/K)$. Then there exists some element $\alpha \in L$ such that $\sigma(\alpha) \neq \tau(\alpha)$, hence for E equal to the Galois closure of $K(\alpha)$ we have that $\sigma\big|_E \neq \tau\big|_E$. Moreover, E is a finite extension of K as α is algebraic. Hence we have the open neighbourhoods $\sigma\mathrm{Gal}(E/K)$ and $\tau\mathrm{Gal}(E/K)$ that are unequal cosets and therefore disjoint. We conclude that $\mathrm{Gal}(L/K)$ is Hausdorff.

Showing compactness is slightly more difficult. Consider the homomorphism

$$\begin{aligned} \iota : \mathrm{Gal}(L/K) &\to \prod_{E/K \text{ finite},\, E\subseteq L} \mathrm{Gal}(E/K) \\ \sigma &\mapsto \prod_E \sigma\big|_E \end{aligned}$$

Note that $\prod_{E/K \text{ finite},\, E\subseteq L} \mathrm{Gal}(E/K)$ is a compact space by Theorem 2.1.9. It is injective by the reasoning used to prove Hausdorffness; if $\sigma \neq \tau \in \mathrm{Gal}(L/K)$, then there exists a finite Galois extension E/K such that $\sigma\big|_E \neq \tau\big|_E$. As the $\mathrm{Gal}(E/K)$ are equipped with the discrete topology, the collection of sets

$$\left\{ U_F = \prod_{E\neq F} \mathrm{Gal}(E/K) \times \{\overline{\sigma}\} : F/E \text{ finite Galois, } \overline{\sigma} \in \mathrm{Gal}(F/K) \right\}$$

forms a subbasis of open neighbourhoods of $\prod_E \mathrm{Gal}(E/K)$. Let σ be any element in the pre-image of $\{\sigma\}$ under the projection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$. We have

$$\tau \in \iota^{-1}(U_F) \iff \tau\big|_F = \sigma\big|_F \iff \tau \in \sigma\mathrm{Gal}(L/F),$$

hence $\iota^{-1}(U_F) = \sigma\mathrm{Gal}(L/F)$. As $\sigma\mathrm{Gal}(L/F)$ is open, ι is continuous. Moreover,

$$\begin{aligned} \prod_E \tau_E \in \iota(\sigma\mathrm{Gal}(L/F)) &\iff \prod_E \tau_E \in \iota(\mathrm{Gal}(L/K)) \text{ and } \tau_F = \sigma\big|_F = \overline{\sigma} \\ &\iff \prod_E \tau_E \in \iota(\mathrm{Gal}(L/K)) \text{ and } \prod_E \tau_E \in U_F, \end{aligned}$$

hence $\iota(\sigma\mathrm{Gal}(L/F)) = \iota(\mathrm{Gal}(L/K)) \cap U_F$, making $\iota : \mathrm{Gal}(L/K) \to \iota(\mathrm{Gal}(L/K))$ an open map. Hence $\iota : \mathrm{Gal}(L/K) \to \iota(\mathrm{Gal}(L/K))$ is an homeomorphism. To show that $\mathrm{Gal}(L/K)$ is compact, it now suffices to show that $\iota(\mathrm{Gal}(L/K))$ is closed in $\prod_E \mathrm{Gal}(E/K)$.

Consider for every pair of extensions F, F' with $L/F'/F/K$ and F'/K finite the following set:

$$M_{F'/F} = \left\{ \prod_E \sigma_E \in \prod_E \mathrm{Gal}(E/K) : \sigma_{F'}\big|_F = \sigma_F \right\}$$

Enumerate the elements of $\mathrm{Gal}(F/K)$ by $\sigma_1, \ldots, \sigma_n$. For every σ_i, there is a subset Σ_i of $\mathrm{Gal}(F'/K)$ that contains the extensions of σ_i to F'/K, i. e. all $\tau \in \mathrm{Gal}(F'/K)$ such that $\tau\big|_F = \sigma_i$. As a result,

$$M_{F'/F} = \bigcup_{i=1}^{n} \left(\prod_{E \neq F,F'} \mathrm{Gal}(E/K) \times \Sigma_i \times \{\sigma_i\} \right),$$

which is a finite union of closed sets (recall that the finite groups have the discrete topology), hence $M_{F'/F}$ is closed.

Certainly we have $\iota(\mathrm{Gal}(L/K)) \subseteq M_{F'/F}$ for all pairs F, F'. Moreover, if $\prod_E \sigma_E \in M_{F'/F}$ for all F, F', then the σ_E together create a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\big|_E = \sigma_E$ for all E. Hence

$$\iota(\mathrm{Gal}(L/K)) = \bigcap_{F,F' \colon L/F'/F/K} M_{F'/F}.$$

We conclude that $\iota(\mathrm{Gal}(L/K))$ is closed in $\prod_E \mathrm{Gal}(E/K)$, thus it is compact, and we conclude that $\mathrm{Gal}(L/K)$ is compact itself. ❐

This proposition is invaluable for the reformulation of the fundamental theorem of Galois theory to include infinite extensions. The Krull topology does all the work, as made explicit by the next theorem:

Theorem 3.2.6 (FUNDAMENTAL THEOREM OF GALOIS THEORY (EXTENDED))**.** Let L/K be a Galois extension. The map $E \mapsto \mathrm{Gal}(L/E)$ is a bijection between

$$\{\text{subextensions } E \text{ of } L/K\} \longleftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(L/K)\}$$

that restricts to a bijection

$$\{\text{finite subextensions } E \text{ of } L/K\} \longleftrightarrow \{\text{open subgroups of } \mathrm{Gal}(L/K)\}. \quad \blacktriangleleft$$

Proof. The fact that the open subgroups form a subset of the closed subgroups has been proven in Lemma 2.2.2. There we also find a connection between open subgroups and finiteness.

Let E/K be a finite subextension of L/K and let F be its Galois closure (which is a finite subextension as well). Then $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/K)$. Moreover, it is open as any $\sigma \in \mathrm{Gal}(L/E)$ has the open neighbourhood $\sigma\mathrm{Gal}(L/F)$. By Lemma 2.2.2, it is also closed.

Consider any subextension E/K and let A_E be the set of all finite subextensions of E. For any $F \in A_E$ we have $\mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/F)$, and if $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\big|_F = e$ for all $F \in A_E$, then $\sigma\big|_E = e$ (this follows as for any $\alpha \in E$ we have $K(\alpha) \in A_E$). Hence

$$\mathrm{Gal}(L/E) = \bigcap_{F \in A_E} \mathrm{Gal}(L/F),$$

and as all $\mathrm{Gal}(L/F)$ are closed, $\mathrm{Gal}(L/E)$ is closed.

We have now proven that $E \mapsto \mathrm{Gal}(L/E)$ is a map with the correct domain and codomain.

Note that by definition, E is the fixed field of $\mathrm{Gal}(L/E)$. As a result, $E \mapsto \mathrm{Gal}(L/E)$ must be injective, as it has an inverse. It is left to prove that $E \mapsto \mathrm{Gal}(L/E)$ is surjective (for both bijections), i. e. that for a open/closed subgroup H we have $H = \mathrm{Gal}(L/L^H)$, where L^H is the fixed field of H.

Let H be a closed subgroup of $\mathrm{Gal}(L/K)$ and consider the fixed field L^H. As every element in H leaves L^H fixed, we have $H \subseteq \mathrm{Gal}(L/L^H)$. To show the other inclusion

we will prove that any $\sigma \in \mathrm{Gal}(L/L^H)$ lies in the closure of H, hence in H itself as it is closed. It suffices to prove that for any finite subextension E/L^H of L/L^H the intersection of H and $\sigma\mathrm{Gal}(L/E)$ is nonempty, as the $\sigma\mathrm{Gal}(L/E)$ form a basis of open neighbourhoods of σ in $\mathrm{Gal}(L/L^H)$. Consider the restriction map $H \to \mathrm{Gal}(E/L^H)$ given by $\tau \mapsto \tau\big|_E$. Its image has fixed field L^H as H has fixed field L^H, hence by Theorem 3.1.1 its image is $\mathrm{Gal}(E/L^H)$. We can therefore find a $\tau \in H$ such that $\tau\big|_E = \sigma\big|_E$, i. e. $\tau \in H \cap \sigma\mathrm{Gal}(L/E)$. As mentioned, we may now conclude that $H = \mathrm{Gal}(L/L^H)$.

Now let H be an open subgroup. It is then also closed, hence equal to $\mathrm{Gal}(L/L^H)$. The union of all cosets of H is $\mathrm{Gal}(L/K)$, the cosets are all disjoint, and these cosets are open as H is open. Hence the cosets form a disjoint open covering of $\mathrm{Gal}(L/K)$. From Proposition 3.2.5 we know that $\mathrm{Gal}(L/K)$ is compact, hence only finitely many different cosets exist. Thus $H = \mathrm{Gal}(L/L^H)$ must be of finite index in $\mathrm{Gal}(L/K)$, hence L^H/K is a finite extension. ❐

Remark. Suppose H is a normal closed subgroup of $\mathrm{Gal}(L/K)$. Then the fixed field L^H is a Galois extension of K, and $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H) = \mathrm{Gal}(L^H/K)$.

Proposition 3.2.7. Let L/K be a Galois extension, I an index set and $\{N_i : i \in I\}$ a collection of closed normal subgroups of $\mathrm{Gal}(L/K)$ with corresponding extensions $\{K_i : i \in I\}$. The extension corresponding to $\bigcap_{i\in I} N_i$ is Galois and contains the composite of all K_i. ◅

Proof. As the intersection of normal subgroups is normal, the extension K_I corresponding to $\bigcap_{i\in I} N_i$ is Galois. As K_i is the fixed field of N_i for all $i \in I$, K_i is fixed by $\bigcap_{i\in I} N_i$ as well. Therefore $K_i \subset K_I$ for all I. Because the composite is defined as the smallest extension containing all K_i, we see that K_I contains the composite of all K_i. ❐

3.2.2 PROFINITE GROUPS

Now that we have regained the fundamental theorem, this section will be devoted to gaining more insight into the Galois groups of infinite extensions.

We reconsider the example of finite fields in Section 3.2.1. Every finite extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ has a Galois group of order n generated by the Frobenius automorphism $\phi_n = \phi\big|_{\mathbb{F}_{p^n}}$. Hence any element $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ restricted to $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is of the form $\phi_n^{a_n}$ for some $1 \le a_n \le n$, which can be seen as an element in $\mathbb{Z}/n\mathbb{Z}$. Moreover, as $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$, ψ is uniquely determined by these a_n. Thus we obtain an injective group homomorphism from $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ to $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$, sending ψ to $(a_n)_{n\in\mathbb{N}}$. However, this homomorphism is not surjective, as we cannot choose ψ freely on all extensions $\mathbb{F}_{p^n}/\mathbb{F}_p$: e.g, once we have determined $\psi\big|_{\mathbb{F}_{p^2}}$, only two options for $\psi\big|_{\mathbb{F}_{p^4}}$ remain: the $\phi_4^{a_4}$ such that $a_4 \equiv a_2 \pmod 2$. Hence the image of the homomorphism lies inside

$$\left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} : a_n \equiv a_m \pmod m \ \forall\, m \mid n \right\}.$$

Moreover, in the example we saw that elements in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ could be constructed from such sequences, hence we conclude that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} : a_n \equiv a_m \pmod{m} \ \forall\ m \mid n \right\}.$$

We have seen in Proposition 3.2.5 that all Galois groups are Hausdorff and compact. As every finite extension is contained in a finite Galois extension, we can reduce the current basis of open neighbourhoods of the Krull topology to subsets of the form $\sigma\mathrm{Gal}(L/F)$, where F/K is a finite Galois extension. As mentioned in the remark below the proof of Theorem 3.2.6, these are exactly the open normal subgroups. Hence $\mathrm{Gal}(L/K)$ has the property that it has a basis of e that is given by the normal subgroups. With this in mind we define a certain type of topological group:

Definition 3.2.8 (PROFINITE GROUP)**.** A *profinite group* is a topological groups that is Hausdorff, compact, and has a basis of open neighbourhoods of e consisting of normal subgroups. ◁

This definition may seem unexciting, but the requirements are in fact quite strong so that we can characterise all profinite groups. The will look very similar to the explicit form of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ that we derived earlier.

3.2.3 INVERSE SYSTEMS

To fully understand the strength of profinite groups, we must first generalise the group that we have seen in the case of finite field extensions:

$$\left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} : a_m \equiv a_n \pmod{m} \ \forall\ m \mid n \right\}.$$

Intuitively it consists of sequences whose coordinates match somehow. This will be made more explicit in the definition of an *inverse system* (of groups), Definition 3.2.11.

Definition 3.2.9 (PARTIAL ORDER)**.** A partial order on a set P (often called a *poset*) is a binary relation $\leq$ such that for all $a, b, c \in P$ we have

- $a \leq a$ ($\leq$ is *reflexive*);
- if $a \leq b$ and $b \leq a$, then $a = b$ ($\leq$ is *antisymmetric*);
- if $a \leq b$ and $b \leq c$, then $a \leq c$ ($\leq$ is *transitive*). ◁

Definition 3.2.10 (DIRECTED POSET)**.** A poset $(I, \leq)$ is called directed if it has the property that for any $a, b \in I$ there exists a $c \in I$ such that $a \leq c$ and $b \leq c$. ◁

Now to the interesting definition; that of an *inverse system*.

Definition 3.2.11 (INVERSE SYSTEM OF GROUPS)**.** Let I be a directed poset such that for every $i \in I$ we have a group σ_i along with morphisms $f_{ij} : \sigma_j \to \sigma_i$ for all $i, j \in I$ with $i \leq j$, with the following properties:

- f_{ii} is the identity on σ_i for all $i \in I$;
- $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$.

Then $((\sigma_i)_{i\in I}, (f_{ij})_{i\leq j})$ is called an *inverse system of groups*. The *inverse limit* of this inverse system is defined as

$$\varprojlim_{i\in I} \sigma_i = \left\{ (\sigma_i)_{i\in I} \in \prod_{i\in I} \sigma_i : f_{ij}(\sigma_j) = \sigma_i \ \forall\ i \leq j \right\}. \qquad \blacktriangleleft$$

Remark. If the G_i are topological groups and the f_{ij} continuous homomorphisms, then $\varprojlim_{i\in I} G_i$ can be made a topological group as well through the inclusion into $\prod_{i\in I} G_i$. Equivalently, it is equipped with the smallest topology such that the projections

$$\varprojlim_{i\in I} G_i \to G_i$$

are continuous.

Example. In the extensions of a finite field we have seen our first inverse system: let $G_n = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$ and let $\leq$ be a partial order on $\mathbb{N}$ such that $m \leq n$ if $m \mid n$. The functions $f_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are given by $a \mapsto a \pmod m$. Hence we now have a more concise notation:

$$\varprojlim_{n\in\mathbb{N}} G_n = \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} : a_n \equiv a_m \pmod m \ \forall\ m \mid n \right\}.$$

Lemma 3.2.12. Let $G = \varprojlim_{i\in I} G_i$. If all G_i are Hausdorff, then so is G and G is a closed subset of $\prod_{i\in I} G_i$. If additionally the G_i are compact, then G is compact. $\blacktriangleleft$

Proof. The proof is actually quite similar to the proof of Proposition 3.2.5 (which is more than a coincidence). Note that

$$G = \bigcap_{j\leq k} \left\{ \prod_{i\in I} \sigma_i \in \prod_{i\in I} G_i : f_{jk}(\sigma_k) = \sigma_j \right\}$$

hence it suffices to show that $C_{jk} = \{\prod_{i\in I} \sigma_i \in \prod_{i\in I} G_i : f_{jk}(\sigma_k) = \sigma_j\}$ is closed for any pair j, k with $j \leq k$.

Consider the composite f of continuous homomorphisms:

$$\prod_{i\in I} G_i \longrightarrow G_j \times G_k \xrightarrow{\mathrm{id}\times f_{jk}} G_j \times G_j$$

$$\prod_{i\in I} \sigma_i \longmapsto (\sigma_j, \sigma_k) \longmapsto (\sigma_j, f_{jk}(\sigma_k)).$$

The image of C_{jk} under f is contained in Δ_{G_j}. Moreover, any element $\prod_{i\in I} \sigma_i \in \prod_{i\in I} G_i$ that maps into Δ_{G_j} abides $f_{jk}(\sigma_k) = \sigma_j$, hence lies in C_{jk}. Therefore we have $C_{jk} = f^{-1}(\Delta_{G_j})$. As G_j is Hausdorff, Δ_{G_j} is closed, thus C_{jk} is closed.

We may now conclude that G is a closed subset of $\prod_{i\in I} G_i$. As the G_i are Hausdorff, $\prod_{i\in I} G_i$ is Hausdorff as well, hence G is Hausdorff. If the G_i are compact, then by Theorem 2.1.9 $\prod_{i\in I} G_i$ is compact, which makes G a closed subset of a compact space, thus compact itself. $\square$

3.2.4 PROFINITE GROUPS (CONTINUED)

We have already seen the definition of a profinite group. In this section we prove an equivalent definition that connects profinite groups and inverse limits.

Proposition 3.2.13. If G is a profinite group and N runs through the open normal subgroups of G, then

$$G \cong \varprojlim_N G/N.$$

Conversely, if $\{(G_i)_{i\in I}, (f_{ij})_{i\leq j}\}$ is an inverse system of finite groups, then $G = \varprojlim_{i\in I} G_i$ is a profinite group. ◂

Proof. Let G be a profinite group and let $\{N_i : i \in I\}$ be the family of open normal subsets. From Lemma 2.2.2, we know that every N_i is of finite index in G. We make I into a poset by $i \leq j$ if $N_i \supset N_j$. The maps $f_{ij} : G_j \to G_i$ are projections. The G_i are all finite (thus topological) groups, and the composite of two projections f_{jk} and f_{ij} is indeed f_{ik}. Hence the groups $(G_i)_{i\in I}$ along with the maps $(f_{ij})_{i\leq j}$ form an inverse system of topological groups. We also have a homomorphism

$$\begin{aligned} f : G &\to \varprojlim_{i\in I} G_i \\ \sigma &\mapsto \prod_{i\in I} \sigma_i, \end{aligned}$$

where $\sigma_i = \sigma \pmod{N_i}$. We will prove that this is an isomorphism and homeomorphism, which means that we should prove that it is bijective, continuous and an open map.

We start with continuity. The G_i are finite, hence equipped with the discrete topology. Let $U_S = \prod_{i\notin S} G_i \times \prod_{i\in S} \{e_{G_i}\}$. Then

$$\{U_S : S \text{ finite subset of } I\}$$

forms a basis of open neighbourhoods of $e \in \prod_{i\in I} G_i$. Furthermore, $f^{-1}(U_S \cap \varprojlim_{i\in I} G_i)$ consists precisely of all $\sigma \in G$ such that $\sigma \pmod{N_i} = e$ for all $i \in S$, which means that $\sigma \in N_i$ for all $i \in S$. Hence $f^{-1}(U_S \cap \varprojlim_{i\in I} G_i) = \bigcap_{i\in S} N_i$, which is open.

Similarly, for $\Sigma = \prod_{i\in I} \sigma_i \in \varprojlim_{i\in I} G_i$ the opens $\Sigma(U_S \cap \varprojlim_{i\in I} G_i)$ form a basis of open neighbourhoods. We have $f^{-1}(\Sigma(U_S \cap \varprojlim_{i\in I} G_i)) = \bigcap_{i\in S} \overline{\sigma}_i N_i$, where $\overline{\sigma}_i$ is a lift of σ_i from G_i to G. Because multiplication is a homeomorphism, this is an intersection of open sets and therefore open. As a result, f is continuous.

The kernel of f is given exactly by $f^{-1}(e) = f^{-1}(U_I) = f^{-1}(U_I \cap \varprojlim_{i\in I} G_i) = \bigcap_{i\in I} N_i$. As G is Hausdorff (as it is profinite), for any element $\sigma \in G$ there exists an element N of the basis of open neighbourhoods of $e \in G$ such that $\sigma \notin N$. As a basis of open neighbourhoods is given by $\{N_i : i \in I\}$, we have $\bigcap_{i\in I} N_i = \{e\}$, thus f is injective.

G is compact and f is continuous, hence $f(G)$ is closed. Hence, to prove f is surjective, it suffices to prove $f(G)$ is dense in $\varprojlim_{i\in I} G_i$. Let $\Sigma \in \varprojlim_{i\in I} G_i$. As mentioned, the $\Sigma(U_S \cap \varprojlim_{i\in I} G_i)$ form an open basis of neighbourhoods of Σ. Let $N_S = \bigcap_{i\in S} N_i$, which is

an intersection of normal subgroups, hence normal itself. We obtain a surjective projection map $G \to {}^{G}/_{N_S}$, hence there is some $\sigma \in G$ such that its image under $G \to {}^{G}/_{N_S}$ is Σ_S, hence $\sigma \equiv \Sigma_i \pmod{N_i}$ for all $i \in S$. As a result, $f(\sigma) \in \Sigma(U_S \cap \varprojlim_{i \in I} G_i)$. Thus $f(G)$ is dense in $\varprojlim_{i \in I} G_i$, which suffices for surjectivity.

Finally, G is compact, thus a closed subset of G is mapped to a closed subset of $\varprojlim_{i \in I} G_i$, which makes f a closed map. As f is surjective, f is an open map. We conclude that f is both an isomorphism and a homeomorphism, hence $G \cong \varprojlim_{i \in I} G_i$ as topological groups.

Now let $\{(G_i)_{i \in I}, (f_{ij})_{i \leq j}\}$ be an inverse system of finite groups. The G_i are finite and equipped with the discrete topology, thus Hausdorff and compact. By Lemma 3.2.12 G is compact and Hausdorff as well. Finally, the normal subgroup $\{e_{G_i}\}$ is open in G_i, hence the normal subgroups $U_S \cap G$, where again

$$U_S = \prod_{i \notin S} G_i \times \prod_{i \in S} \{e_{G_i}\}$$

for S a finite subset of I, form a basis of open neighbourhoods of $e \in G$. We conclude that G is a profinite group. ❐

Equipped with the Krull topology, Galois groups are examples of profinite groups. Let L/K be a Galois extension. We have seen in Proposition 3.2.5 that $\mathrm{Gal}(L/K)$ is Hausdorff and compact, and by definition a basis of open neighbourhoods of e are given by $\mathrm{Gal}(L/E)$, where E runs over the finite Galois subextensions of L/K, which are all open normal subgroups. As a result,

$$\mathrm{Gal}(L/K) \cong \varprojlim_{E/K \text{ finite Galois}} {}^{\mathrm{Gal}(L/K)}/_{\mathrm{Gal}(L/E)} \cong \varprojlim_{E/K \text{ finite Galois}} \mathrm{Gal}(E/K).$$

Example. To return to the finite fields, we see that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{n \in \mathbb{N}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

which is what we have seen before.

4

LOCAL FIELDS

Local fields are a special type of fields that come equipped with an absolute value and consequently a topology, which some additional properties, namely *completeness* with regard to this absolute value and a *finite residue field*, which will be defined in Definition 4.1.7. The reason we study local fields is because every global field has associated local fields known as *completions*, which will prove useful for studying the extensions of the global field.

This chapter will only deal with the definition of local fields and basic theory, namely Hensel's Lemma and Teichmuller representatives. In the final section we investigate the topology on these local fields and prove compactness and/or Hausdorffness of object associated to a local field.

We will continue working with local fields in Chapter 6, where we study the extensions of local fields.

One final remark before we begin: if R is a ring, we denote by R^* its group of invertible elements, and by $R^\times = R - \{0\}$ its multiplicative monoid.

4.1 DEFINITION OF A LOCAL FIELD

In order to define a local field, we require the notion of a *valuation*, *completeness* and a *residue field*. We define all these formally, and we complete this section with a pair of explicit examples.

We begin with K a general field, and, once local fields are defined, K will usually be a local field. To start off, we state a pair of definitions that estimate the size of the elements of a field and establish a connection between the two.

Definition 4.1.1 (ABSOLUTE VALUE). An *absolute value* on a field K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ with the following properties:

A. $|x| = 0 \iff x = 0$;

B. $|xy| = |x||y| \ \forall\ x, y \in K$;

C. $|x + y| \leq |x| + |y| \ \forall\ x, y \in K$.

We differentiate between two types of absolute values: if, in addition to the three properties above, $|\cdot|$ also abides

$$|x + y| \leq \max(|x|, |y|) \ \forall\ x, y \in K,$$

we say that the absolute value is *nonarchimedean*. Otherwise, the absolute value is said to be *archimedean*. Note that this condition is stronger than the third property of an absolute value. ◂

Definition 4.1.2 (VALUATION). A *valuation* v on K is a map $K \to \mathbb{R} \cup \{\infty\}$ such that:

A. $v(x) = \infty \iff x = 0$;

B. v is an additive homomorphism, i. e. $v(xy) = v(x) + v(y)$ for all $x, y \in K^\times$;

C. $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K^\times$.

If the image of the valuation is isomorphic to $\mathbb{Z} \cup \infty$ (i. e. of the form $s\mathbb{Z} \cup \{\infty\}$ for some $s \in \mathbb{R}_{>0}$), the valuation is said to be *discrete*. Furthermore, we say that v is *normalised* if the image of v is $\mathbb{Z} \cup \{\infty\}$. Note that all valuations can be normalised by dividing by s. ◁

Every valuation induces an absolute value by $|\cdot|_v : K \to \mathbb{R}_{\geq 0}$ by $|x|_v := C^{-v(x)}$ for a fixed $C > 1$ (where we use the convention $C^{-\infty} = 0$). This absolute value is always nonarchimedean as $v(x+y) \geq \min(v(x), v(y)) \iff |x+y| \leq \max(|x|, |y|)$. In turn, nonarchimedean absolute values induce valuations.

Definition 4.1.3 (TOPOLOGY INDUCED BY ABSOLUTE VALUE)**.** Any absolute value induces a *topology* $\mathcal{T}_v$ on K created from the basis of open balls $B_{x,\epsilon} := \{y \in K : |x-y|_v < \epsilon\}$. ◁

Remark. This topology does not depend on the choice of C. In general, whenever two absolute values (or two valuations inducing absolute values) induce the same topology, we call the absolute values (or valuations) *equivalent*. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent precisely when $|x|_1 \leq 1$ if and only if $|x|_2 \leq 1$, which is the case precisely when $|\cdot|_1^e = |\cdot|_2$ for some exponent e, see Lemma 1.10 of [Bro13]. If the absolute values are nonarchimedean with associated valuations v_1 and v_2, then v_1 and v_2 are equivalent if and only if $e \cdot v_1 = v_2$.

Example. Suppose we are given a number field K with ring of integers R. For any prime ideal $\mathfrak{p}$, we can define a valuation, denoted $v_\mathfrak{p}$ by $v_\mathfrak{p}(a) = \max\{n \in \mathbb{N} : a \in \mathfrak{p}^n\}$ for $a \in R$. Because we have $|x| \leq 1 \iff |x^{-1}| \geq 1$ for $x \in K^\times$ we find that $K = \mathrm{Frac}(R)$, thus we can extend this valuation $v_\mathfrak{p}$ to the entirety of K. Moreover, the real and complex embeddings provide archimedean absolute values.

Definition 4.1.4 (RING OF INTEGERS)**.** For a field K and nonarchimedean absolute value $|\cdot|$, the *ring of integers* $\mathcal{O}_K$ (abbreviated as $\mathcal{O}$ when unambiguous) is defined as the ring $\mathcal{O}_K = \{x \in K : |x| \leq 1\}$. In $\mathcal{O}_K$ we have the ideal $\mathfrak{m} = \{x \in K : |x| < 1\}$. ◁

Indeed $\mathcal{O}_K$ is a ring as for $x, y \in \mathcal{O}_K$ we have $|x+y| \leq \max(|x|, |y|) = 1$ and $|x||y| = |x||y| \leq 1$, so that $x+y, xy \in \mathcal{O}_K$. Moreover, $|0| = 0$ and $|1| = 1$, thus they both lie in $\mathcal{O}_K$, making $\mathcal{O}_K$ a ring. We find that $\mathfrak{m}$ is an ideal for similar reasons. Because $|x^{-1}| = 1/|x|$ for all $x \in K^\times$, we see that $\mathcal{O}_K^* = \{x \in K : |x| = 1\}$. As a result, $\mathfrak{m} = \mathcal{O}_K - \mathcal{O}_K^*$, hence $\mathfrak{m}$ is the unique maximal ideal in $\mathcal{O}_K$.

Remark. If the absolute value has corresponding valuation v, the ring of integers is sometimes denoted as $\mathcal{O}_{K,v}$ or $\mathcal{O}_v$. The condition $|x| \leq 1$ rewrites to $v(x) \geq 0$ and $|x| = 1$ to $v(x) = 0$.

Lemma 4.1.5. Suppose K is equipped with a nonarchimedian absolute value $|\cdot|$ with corresponding valuation v. The maximal ideal $\mathfrak{m}$ is principal precisely when v is discrete. ◁

Proof. Suppose $\mathfrak{m}$ is principal, say $\mathfrak{m} = (\pi)$, then any element $x \in K$ can be written as $x = u \cdot \pi^n$, $u \in \mathcal{O}_K^*$, $n \in \mathbb{Z}$. We have $|x| = |u||\pi^n| = |\pi|^n$, hence $v(x) = nv(\pi)$. Therefore the image of v is $v(\pi)\mathbb{Z} \cup \{\infty\}$, making v discrete.

If, on the other hand, v is a discrete valuation, then we can normalise v and we obtain some element $\pi \in \mathfrak{m}$ with $v(\pi) = 1$. As $\mathcal{O}_K^* = \{x \in K : v(x) = 0\}$, every element $a \in K^\times$ can be written in the form $a = u \cdot \pi^n$, where $u \in \mathcal{O}_K^*$ and $n = v(a) \in \mathbb{Z}$ (u lies in $\mathcal{O}_K^*$ because $v(u) = v(a/\pi^n) = v(a) - v(\pi^n) = 0$). Hence $a \in \mathfrak{m}$ precisely when $\pi \mid a$, or $\mathfrak{m} = (\pi)$. ❐

As mentioned in the proof, if $\mathfrak{m} = (\pi)$, then every element in the ring of integers can be written as a unit times an integer power of π. Many proofs in the rest of the section rely on this.

Remark. Two valuations v_1 and v_2 on K are equivalent precisely when $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$. This follows immediately as $\mathcal{O}_v := \{x \in K : |x|_v \leq 1\}$.

Definition 4.1.6 (UNIFORMISER)**.** Let K be a field with a normalised valuation v. A *uniformiser*, or *prime element*, π of K is an element $\pi \in K$ with $v(\pi) = 1$. ◁

Uniformisers are unique up to multiplication with elements in $\mathcal{O}_K^*$.

Definition 4.1.7 (RESIDUE FIELD)**.** The quotient $k = \mathcal{O}/\mathfrak{m}$ is called the *residue field* of K. ◁

The last notion we need for defining local fields is that of completeness.

Definition 4.1.8 (COMPLETENESS)**.** A field K with absolute value $|\cdot|$ is said to be *complete* if every Cauchy sequence with respect to the absolute value admits a limit in K. ◁

Definition 4.1.9 (COMPLETION)**.** Given a field K with absolute value $|\cdot|$, the *completion* $\overline{K}$ of K with respect to $|\cdot|$ consists of all limits of Cauchy sequences in K. We can write this down explicitly by defining an equivalence relation $\sim$ on the Cauchy sequences in K given by $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ precisely when $|x_n - y_n| \to 0$ for $n \to \infty$. $\overline{K}$ can be explicitly written as

$$\overline{K} = \{(x_n)_{n\in\mathbb{N}} \text{ Cauchy in } K\}/\sim.$$ ◁

Remark. If the absolute value is nonarchimedean with corresponding valuation v, we sometimes write K_v for $\overline{K}$.

Proposition 4.1.10. Given a field K and a discrete valuation v on K, we can uniquely extend v to $\overline{K}$. ◁

Proof. See Chapter II, paragraph 10 of [CF67]. ❐

At this point we have enough preparation to define a local field.

Definition 4.1.11 (LOCAL FIELD)**.** A *local field* K is a field complete with respect to a discrete valuation v and a finite residue field. ◁

Remark. The term local field is sometimes also used for fields complete with respect to any absolute value, not just nonarchimedean ones. If this is the case, what we call local fields will be referred to as *nonarchimedean local fields*.

Remark. An equivalent definition of a local field is a field K with valuation v that is locally compact with respect to the topology T_v. For a proof of this equivalence, see Proposition II.1.1 of [Ser95].

Remark. As K is complete with respect to the absolute value, so are $\mathcal{O}$ and $\mathcal{O}^\times$.

Before we continue with spewing properties of local fields, we consider an important pair of examples:

- The *field of p-adic numbers* $\mathbb{Q}_p$ for a certain prime number p is obtained by completing $\mathbb{Q}$ with respect to the discrete valuation v_p, where $v_p(a/b)$ is defined by the unique integer $n \in \mathbb{Z}$ such that $a/b = p^n c/d$, where $\gcd(c,d) = 1$, $p \nmid cd$. Alternatively, one might view the elements of $\mathbb{Q}_p$ as power series $\sum_{i=k}^{\infty} a_i p^i$, where k is some integer and $a_i \in \{0, \dots, p-1\}$, $a_k \neq 0$. $\mathbb{Q}$ is embedded into $\mathbb{Q}_p$ as the elements whose power series stop, i. e. are of the form $\sum_{i=k}^{n} a_i p^i$. The ring of p-adic integers, $\mathbb{Z}_p$, contains the elements that are of the form $\sum_{i=0}^{\infty} a_i p^i$. A uniformiser is p, hence the maximal ideal is (p). The residue field is $\mathbb{Z}/p\mathbb{Z}$. Alternatively, one could define the p-adic integers $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^k\mathbb{Z}$, where the limit is taken over all k, and subsequently $\mathbb{Q}_p := \operatorname{Frac}(\mathbb{Z}_p)$.
- The field of *formal Laurent series* $k((T))$ over a finite field k is given by power series $\sum_{i=n}^{\infty} a_i T^i$, where n is some integer and $a_i \in k$, $a_n \neq 0$. The valuation is given by $v\left(\sum_{i=n}^{\infty} a_i T^i\right) = n$. The ring of integers is $k[[T]]$. A uniformiser is T, hence the maximal ideal is (T) and the residue field is k.

4.2 PROPERTIES OF LOCAL FIELDS

Now that we have a feeling of what local fields are, we investigate two important techniques for using the residue field: the former allows us to find linear factors of polynomials over a local field by finding roots in the residue field, while the latter provides a technique of embedding a residue field into its local field. The structure and idea of the proofs are from [Rie06].

4.2.1 HENSEL'S LEMMA

Hensel's Lemma allows for finding roots of polynomials over a local fields using the roots of the reduced polynomial over the residue field.

Lemma 4.2.1 (HENSEL'S LEMMA)**.** Let K be a local field and let $f \in \mathcal{O}[X]$ be a polynomial. Suppose we have $a_0 \in \mathcal{O}$ such that $|f(a_0)| < |f'(a_0)|^2$. Then there exists a unique $a \in \mathcal{O}$ such that

$$|a - a_0| \leq \left| \frac{f(a_0)}{f'(a_0)} \right| \text{ and } f(a) = 0. \qquad \blacktriangleleft$$

In the above form, Hensel's Lemma is an analogue of Newton's approximation method.

Proof. If $f(a_0) = 0$, then we are done, hence assume $f(a_0) \neq 0$. We construct a Cauchy sequence of approximate roots of $f(X)$, starting with a_0. As we are dealing with local fields, the Cauchy sequence will have a limit lying in K.

Using Newton's binomium, expand $f(X+Y)$:

$$f(X+Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \dots.$$

We have $f_i \in \mathcal{O}[X]$ and $f_1 = f'$. Define $b_0 \in K$ such that that $f(a_0) + f'(a_0)b_0 = 0$ (it is unequal to zero). Note that because $f'(a_0) \in \mathcal{O}$, we have $v(f'(a_0)) \geq 0$ and consequently $v(f(a_0)) > 2v(f'(a_0)) \geq v(f'(a_0))$ (the first inequality is our assumption). It follows that $v(b_0) > 0$, hence $b_0 \in \mathcal{O}$. We have

$$f(a_0 + b_0) = f(a_0) + f'(a_0)b_0 + f_2(a_0)b_0^2 + \cdots = f_2(a_0)b_0^2 + \ldots,$$

thus

$$\begin{aligned}
v(f(a_0 + b_0)) &= v(f_2(a_0)b_0^2 + \ldots) \\
&\geq \min_{i>1} v(f_i(a_0)b_0^i) && \text{(property of a valuation)} \\
&\geq \min_{i>1} i \cdot v(b_0) && (v(f_i(a_0)) \geq 0 \text{ as } f_i(a_0) \in \mathcal{O}) \\
&= 2v(b_0) \\
&= 2v(f(a_0)) - 2v(f'(a_0)) && \text{(definition of } b_0) \\
&> v(f(a_0)). && \text{(assumption)}
\end{aligned}$$

Similarly, we have, writing $f'(X + Y) = f'(X) + g_1(X)Y + g_2(X)Y^2 + \ldots$ (all g_i lie in $\mathcal{O}[X]$),

$$\begin{aligned}
v(f'(a_0 + b_0) - f'(a_0)) &= v(g_1(a_0)b_0 + g_2(a_0)b_0^2 + \ldots) \\
&\geq v(b_0) \\
&= v(f(a_0)) - v(f'(a_0)) \\
&> v(f'(a_0)).
\end{aligned}$$

This implies that $f'(a_0 + b_0)$ and $f'(a_0)$ must have the same valuation.

Let $a_1 = a_0 + b_0$. We have found the following inequalities and equality:

A. $v(f(a_1)) > v(f(a_0))$;

B. $v(f'(a_1)) = v(f'(a_0))$;

C. $v(a_1 - a_0) = v(f(a_0)) - v(f'(a_0))$.

By A. and B. we have $v(f(a_1)) > v(f(a_0)) > 2v(f'(a_0)) = 2v(f'(a_1))$, which allows us to repeat the same construction to obtain $a_2, a_3, \ldots$ (which ends if $f(a_n) = 0$ for some n). In this way we obtain a sequence $(a_n)_{n\in\mathbb{N}}$ with the following properties for all $n \in \mathbb{N}$.

A. $v(f(a_{n+1})) > v(f(a_n))$;

B. $v(f'(a_{n+1})) = v(f'(a_n))$;

C. $v(a_{n+1} - a_n) = v(f(a_n)) - v(f'(a_n))$.

We see that $v(f(a_n))$ is strictly increasing, hence $v(f(a_n)) \to \infty$ as $n \to \infty$. Furthermore, C. tells us that $v(a_{n+1} - a_n) \to \infty$ as $n \to \infty$, as $v(f(a_n))$ is strictly increasing and $-v(f'(a_n))$ is non-decreasing. It follows that, for $m > n$, $v(a_m - a_n) \geq \min_{j\in[n+1,m]} v(a_m - a_{m-1}) \to \infty$ for $m, n \to \infty$. We conclude that $a_0, a_1, a_2, \ldots$ is a Cauchy sequence, and we obtain a limit a. As $v(a_n) \geq 0$ for all n, we have $v(a) \geq 0$, hence $a \in \mathcal{O}$. Lastly, $v(f(a)) = \infty$, hence $f(a) = 0$.

We will not prove unicity here. The idea behind the proof is that if we have a root b with the same properties, then assuming that $v(b-a)$ is finite leads to a contradiction using only methods that were used to find the root a.

❐

Corollary 4.2.2. Given a polynomial $\overline{p}(x) \in k[x]$ with a simple root $a \in k$ and a lift, $p(x) \in \mathcal{O}[x]$ of $\overline{p}(x)$, i. e. the coefficients of $p \pmod{\mathfrak{m}}$ are the coefficients of $\overline{p}$, there exists a unique root $\alpha \in \mathcal{O}$ of $p(x)$ such that $\alpha \equiv a \pmod{\mathfrak{m}}$. ◁

4.2.2 TEICHMÜLLER REPRESENTATIVES

Naturally, the quotient map $\mathcal{O} \to \mathcal{O}/\mathfrak{m} = k$ is a surjection, but it fails to be injective. This section is devoted to showing that we can choose representatives in $\mathcal{O}$ of every equivalence class in $\mathcal{O}/\mathfrak{m}$ such that the map which sends the equivalence class to its representative is multiplicative. For this, we begin with the definition of a section, which is a partial inverse.

Definition 4.2.3 (SECTION)**.** Given two morphisms $f : X \to Y$ and $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ we call g a *section* of f. The map f is called a *retraction* of g. ◁

Remark. The section of a quotient map is sometimes known as a *transversal*.

Definition 4.2.4 (TEICHMÜLLER REPRESENTATIVE)**.** Let K be a local field with residue field k and suppose ω is a multiplicative section of the quotient map. Then we call $\omega(a)$ a *Teichmüller representative* of $a \in k$. ◁

Proposition 4.2.5. A multiplicative section of the quotient map exists. Moreover, it is unique. ◁

This proposition has a lengthy proof. We start with a lemma and introduce a new concept called *ancient* elements. We will use the standard setting: we assume that we have a local field K, ring of integers $\mathcal{O}$ and a residue field k that has q elements, where q is a power of p.

Lemma 4.2.6. Let $a, b \in \mathcal{O}$. Suppose $a \equiv b \pmod{\mathfrak{m}^n}$ for some $n \in \mathbb{N}$. Then $a^p \equiv b^p \pmod{\mathfrak{m}^{n+1}}$. ◁

Proof. First note that multiplication by p annihiliates k (i. e. $p\alpha = 0$ for $\alpha \in k$), hence $p\mathcal{O} \subseteq \mathfrak{m}$. For any $a, b \in \mathcal{O}$ we have

$$a^p - b^p = (a-b)\left(\sum_{k=0}^{p-1} a^k b^{p-1-k}\right).$$

By assumption $a - b \equiv 0 \pmod{\mathfrak{m}^n}$. Moreover,

$$\sum_{k=0}^{p-1} a^k b^{p-1-k} \equiv \sum_{k=0}^{p-1} a^{p-1} \equiv pa^{p-1} \equiv 0 \pmod{\mathfrak{m}},$$

hence $a^p \equiv b^p \pmod{\mathfrak{m}^{n+1}}$. ❐

Definition 4.2.7 (n-ANCIENT)**.** Let $a \in \mathcal{O}$ and $n \in \mathbb{N}$. We call a *n-ancient* if for all $m \in \mathbb{N}_0$ there exists a $b \in \mathcal{O}$ such that $b^{n^m} = a$, i. e. a is an $n^{m\text{th}}$ power for all $m \in \mathbb{N}$. ◁

Proof (PROPOSITION 4.2.5). Denote the quotient map by $\bar{\cdot}$. The proof is split into three parts:

A. For every element $\alpha \in k$ there is a unique q-ancient element $a \in \mathcal{O}$ such that $\overline{a} = \alpha$.

B. The map $\omega : k \to \mathcal{O}$ that sends α to a is a multiplicative section of the quotient map.

C. ω is the unique multiplicative section of the quotient map.

The proofs themselves are fairly straightforward.

A. Let $\alpha \in k = {}^{\mathcal{O}}/_{\mathfrak{m}}$. We begin by proving existence. If $\alpha = 0$, then we have the obvious lift 0, which is also q-ancient. Suppose $\alpha \neq 0$. Take any lift $a \in \mathcal{O}$ of α. This a must lie in $\mathcal{O}^*$ as $\mathfrak{m}$ is annihilated by the quotient map and $\mathcal{O}^* = \mathcal{O} - \mathfrak{m}$. Define $A := \lim_{n\to\infty} a^{q^n}$. As k has q elements, $a^q \equiv a \pmod{\mathfrak{m}}$. Lemma 4.2.6 then dictates that $a^{q^{n+1}} \equiv a^{q^n} \pmod{\mathfrak{m}^{n+1}}$. This implies that, for $m > n$, $a^{q^m} \equiv a^{q^n} \pmod{\mathfrak{m}^{n+1}}$, hence $\left(a^{q^n}\right)_{n\in\mathbb{N}_0}$ is a Cauchy sequence, implying $A \in \mathcal{O}^*$. As $a^{q^n} \equiv a \pmod{\mathfrak{m}}$ for all $n \in \mathbb{N}_0$, we have $\overline{A} = \alpha$ and by construction $A^{q^n} = A$, thus A is q-ancient.

Suppose we have two q-ancient elements a and b such that $\overline{a} = \overline{b}$, or $a \equiv b \pmod{\mathfrak{m}}$. For any $s \in \mathbb{N}_0$, we have a_s and b_s such that $a = a_s^{q^s}$ and $b = b_s^{q^s}$. As noted before, $a_s^{q^s} \equiv a_s \pmod{\mathfrak{m}}$ and $b_s^{q^s} \equiv b_s \pmod{\mathfrak{m}}$, hence $a_s \equiv b_s \pmod{\mathfrak{m}}$. As a result of Lemma 4.2.6 we have $a = a_s^{q^s} \equiv b_s^{q^s} = b \pmod{\mathfrak{m}^{s+1}}$. It follows that $v(a-b) \geq s$ for all $s \in \mathbb{N}$, thus $v(a-b) = \infty$ and consequently $a = b$.

For any $\alpha \in k$, denote by $\omega(\alpha)$ the unique lift to $\mathcal{O}$ that is a q-ancient element. We have seen that $\overline{\omega(\alpha)} = \alpha$. It immediately follows that ω is injective.

B. As $0, 1 \in \mathcal{O}$ are trivially q-ancient, we have $\omega(0) = 0$ and $\omega(1) = 1$. Furthermore, $\omega(\alpha) = \lim\limits_{n\to\infty} a^{q^n}$ and $\omega(\beta) = \lim\limits_{n\to\infty} b^{q^n}$, hence $\omega(\alpha)\omega(\beta) = \lim\limits_{n\to\infty} (ab)^{q^n}$. However, ab is a lift of $\alpha\beta$, hence $\omega(\alpha\beta) = \lim\limits_{n\to\infty} (ab)^{q^n}$. It follows that $\omega(\alpha\beta) = \omega(\alpha)\omega(\beta)$.

C. Suppose we have a multiplicative section ω' of the quotient map. Let $\alpha \in k$ and note that $\alpha^q = \alpha$. We have $\omega'(\alpha) = \omega'\left(\alpha^{q^n}\right) = \omega'\left(\alpha\right)^{q^n}$ for any $n \in \mathbb{N}_0$, hence $\omega'(\alpha)$ is q-ancient. Furthermore, as ω' is a section, $\overline{\omega'(\alpha)} = \alpha$. However, we just proved that there is a unique q-ancient element in the equivalence class α, namely $\omega(\alpha)$. We conclude that $\omega'(\alpha) = \omega(\alpha)$ for all $\alpha \in k$, hence $\omega' = \omega$. ❐

As an application of the Teichmüller representatives, we conclude this section with a lemma that gives an interesting isomorphism:

Lemma 4.2.8. Let K be a local field with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$ and residue field k. Then $\mathcal{O}^* \xrightarrow{\sim} k^\times \times (1+\mathfrak{m})$. ◁

Proof. Consider the homomorphism $a \mapsto (\overline{a}, {}^{a}/_{\omega(\overline{a})})$. As $a \notin \mathfrak{m}$, we have $\omega(\overline{a}) \in \mathcal{O}^*$, hence this is a well-defined homomorphism. We prove that it is in fact an isomorphism.

Suppose $a, b \in \mathcal{O}^*$ that map to the same element, i. e. $\overline{a} = \overline{b}$ and ${}^{a}/_{\omega(\overline{a})} = {}^{b}/_{\omega(\overline{b})}$. The former implies $\omega(\overline{a}) = \omega(\overline{b})$, which, combined with the latter, gives $a = b$.

If we have an element $(\alpha, a) \in k^\times \times (1+\mathfrak{m})$, then $a \cdot \omega(\alpha) \mapsto (\alpha, a)$ as $a \equiv 1 \pmod{\mathfrak{m}}$, thus $\overline{a \cdot \omega(\alpha)} = \overline{\omega(\alpha)} = \alpha$.

This shows that the homomorphism is also bijective, hence it is an isomorphism. ❐

Remark. It is also possible to define the homomorphism as $a \mapsto (\overline{a}, \omega(\overline{a})/_a)$.

4.3 THE TOPOLOGY ON LOCAL FIELDS

For the remainder of the section, let K be a local field with ring of integers $\mathcal{O}$ and discrete absolute value $|\cdot|$. As mentioned in Definition 4.1.3, the topology on K (and subsequently on $\mathcal{O}$ as it is equipped with the subspace topology) is induced by the open balls $B_{x,r} = \{y \in K : |x - y| < r\}$.

Lemma 4.3.1. All closed balls, i. e. $\{y \in K : |x - y| \leq r\}$ for some $x \in K$ and $r > 0$, are open. ◁

Proof. Because $|\cdot|$ is discrete, its image is $C^{-s\mathbb{Z}} \cup \{0\}$, which only has the accumulation point 0, hence there exists an $\epsilon > 0$ such that $(r, r+\epsilon)$ has empty intersection with the image. It follows that $\{y \in K : |x - y| \leq r\} = \{y \in K : |x - y| < r + \epsilon\}$, which is open. ❐

The ring of integers $\mathcal{O}$, equipped with the subspace topology from K, in particular has some special properties.

Corollary 4.3.2. The ring $\mathcal{O}$ is open and closed in K, as $\mathcal{O} = \{x \in K : |x| \leq 1\}$. $\mathcal{O}^*$ is open as $\mathcal{O} = \{x \in K : |x| < 1\}$. Thirdly, the ideal $\pi\mathcal{O}$ is closed as $\pi\mathcal{O} = \mathcal{O} \cap (\mathcal{O}^*)^c$, which is the intersection of two closed subsets. ◁

Proposition 4.3.3. The (additive group of the) ring of integers $\mathcal{O}$ is a compact and Hausdorff topological group. ◁

Proof. This proof is used as the proof of Lemma 3.8 in [Bro13]. All properties follows from the fact that a basis of open neighbourhoods of $a \in \mathcal{O}$ is given by $a + \pi^n\mathcal{O}$, $n \in \mathbb{N}$. Suppose $x + y \in a + \pi^n\mathcal{O}$. Then also $(x + \pi^n\mathcal{O}) + (y + \pi^n\mathcal{O}) \subseteq a + \pi^n\mathcal{O}$, hence the addition map $\mathcal{O} \times \mathcal{O} \to \mathcal{O}$ is continuous. The inverse image of $a + \pi^n\mathcal{O}$ under inversion is precisely $-a + \pi^n\mathcal{O}$, hence inversion is continuous as well, making $\mathcal{O}$ a topological group.

For any $a, b \in \mathcal{O}$ with $a \neq b$ there is some n such that $a \not\equiv b \pmod{\pi^n\mathcal{O}}$, hence $(a + \pi^n\mathcal{O}) \cap (b + \pi^n\mathcal{O}) = \emptyset$ and we obtain that $\mathcal{O}$ is Hausdorff.

Now suppose there is some open covering $\{U_i : i \in I\}$ of $\mathcal{O}$ that can not be reduced to a finite covering. Let $A_1 \subseteq \mathcal{O}$ be a set of representatives of all equivalence classes in $\mathcal{O}/_{\pi\mathcal{O}} = k$. Then $\mathcal{O}$ is covered by open sets of the form $x + \pi\mathcal{O}$, $x \in A_1$. As k is finite, this is a finite covering. As $\{U_i : i \in I\}$ could not be reduced to a finite covering, it follows that there exists an $x_0 \in A_1$ such that the cover $\{U_i : i \in I\}$ can not be reduced to a finite cover of $x_0 + \pi\mathcal{O}$. Repeating this gives an x_1 such that $\{U_i : i \in I\}$ can not be reduced to a finite cover of $x_0 + x_1\pi + \pi^2\mathcal{O}$. We obtain a sequence of elements $x_0, x_0 + x_1\pi, x_0 + x_1\pi + x_2\pi^2, \ldots$ such that $x_0 + \cdots + x_{n-1}\pi^{n-1} + \pi^n\mathcal{O}$ can not be covered by finitely many U_i, $i \in I$. As $\mathcal{O}$ is complete and this sequence is a Cauchy sequence, it follows that it has a limit $x = x_0 + x_1\pi + x_2\pi^2 + \cdots \in \mathcal{O}$. There exists a $j \in I$ such that $x \in U_j$. Because U_j is open, it contains for some $n \in \mathbb{N}$ the open set $x + \pi^n\mathcal{O}$ (as these open sets form the basis). However, $x + \pi^n\mathcal{O} = x_0 + \cdots + x_{n-1}\pi^{n-1} + \pi^n\mathcal{O}$, which is now covered by only U_j, which is a contradiction. We conclude that $\mathcal{O}$ is compact. ❐

Corollary 4.3.4. The field K is locally compact, as any $x \in K$ has the compact open neighbourhood $x + \mathcal{O}$. ◁

If we consider the basis of open neighbourhoods of $0 \in \mathcal{O}$, namely the sets $\pi^n\mathcal{O}$, we note that they are subgroups of $\mathcal{O}$. Moreover, as $\mathcal{O}$ is abelian, they are even normal subgroups. Combining this with Proposition 4.3.3 leads to the following lemma.

Lemma 4.3.5. The topological group $\mathcal{O}$ is a profinite group. ◂

Corollary 4.3.6. There is an isomorphism of topological groups

$$\mathcal{O} \cong \varprojlim_{n\in\mathbb{N}} \mathcal{O}/\pi^n\mathcal{O}. \qquad \blacktriangleleft$$

As a result, any element $x \in \mathcal{O}$ has a unique representation as a sequence $(a_0, a_1, \dots) \in \varprojlim_{n\in\mathbb{N}} \mathcal{O}/\pi^n\mathcal{O}$. Note that $a_n \equiv a_m \pmod{\pi^m\mathcal{O}}$ for all $n \geq m$. Let $A_n \subseteq \mathcal{O}$ be a set of representative of the equivalence classes of $\mathcal{O}/\pi^n\mathcal{O}$. We can inductively create a sequence $x_0, x_1, \dots, x_i \in A_i$ such that $(a_0, a_1, a_2, \dots) = (x_0 \pmod{\pi\mathcal{O}}, x_0 + x_1\pi \pmod{\pi^2\mathcal{O}}, x_0 + x_1\pi + x_2\pi^2 \pmod{\pi^3\mathcal{O}}, \dots)$. The limit of this sequence is precisely x, hence we can write $x = \sum_{n\in\mathbb{Z}_{\geq 0}} x_i\pi^i$.

The subset $\mathcal{O}^*$ of $\mathcal{O}$ is in general not equipped with the subspace topology; if R is a ring and a topological group for addition, then the inverse map $^{-1} : R^* \to R^*$ may fail to be continuous in the subspace topology, which means that R^* is not a topological group. The topology on multiplicative group R^* is given by the subspace topology obtained by embedding R^* into $R \times R$ via $u \mapsto (u, u^{-1})$. With this, the inverse map is continuous, and the composition $R^* \to R \times R \to R$ given by $u \mapsto (u, u^{-1}) \mapsto u$ is a continuous injection $R^* \to R$ with image $R^* \subseteq R$, hence this topology on R^* is finer than the subspace topology from R. An example of such a ring R is the *adele ring*, which we will encounter in Section 7.4.2.

Going off on a bit of a tangent, this construction is similar to a possible proof that $\mathbb{A}^1 - \{0\}$ is a variety: $\mathbb{A}^1 - \{0\}$ is not the zero set of a polynomial in a single variable (i. e. if we embed $\mathbb{A}^1 - \{0\}$ into $\mathbb{A}^1$ we do not obtain the desired result), while embedding it into $\mathbb{A}^2$ via $u \mapsto (u, u^{-1})$ makes it the zero set of the polynomial $xy - 1$, hence $\mathbb{A}^1 - \{0\}$ is a variety.

Let us return to the matters at hand: the properties of $\mathcal{O}^*$.

Proposition 4.3.7. The topological group $\mathcal{O}^*$ is compact and Hausdorff. ◂

Proof. As $\mathcal{O}$ is compact and Hausdorff, so is $\mathcal{O} \times \mathcal{O}$. It follows that $\mathcal{O}^*$ is Hausdorff as well. Consider

$$(\mathcal{O} \times \mathcal{O}) - \mathcal{O}^* = \{(x, y) \in \mathcal{O} \times \mathcal{O} : xy \neq 1\}.$$

For any (x, y) in this set we have $xy \neq 1$, hence for some $n \in \mathbb{N}$ we have $xy \not\equiv 1 \pmod{\pi^n\mathcal{O}}$. Then, for any $x' \in x + \pi^n\mathcal{O}$ and $y' \in x + \pi^n\mathcal{O}$ we have $x'y' \not\equiv 1 \pmod{\pi^n\mathcal{O}}$, thus $x'y' \neq 1$. As a result, $(x + \pi^n\mathcal{O}) \times (y + \pi^n\mathcal{O}) \subseteq (\mathcal{O} \times \mathcal{O}) - \mathcal{O}^*$, hence $(\mathcal{O} \times \mathcal{O}) - \mathcal{O}^*$ is open, thus $\mathcal{O}^*$ is closed. A closed subset of a compact space is compact, hence $\mathcal{O}^*$ is compact. ❐

We end with one last remark on $\mathcal{O}^*$: as $\mathcal{O} \cong \varprojlim_{n\in\mathbb{N}} \mathcal{O}/\pi^n\mathcal{O}$, we have

$$\mathcal{O}^* \cong \varprojlim_{n\in\mathbb{N}} (\mathcal{O}/\pi^n\mathcal{O})^*.$$

Part II

CLASS FIELD THEORY

5

INTRODUCTION

In class field theory, the abelian extensions of a field are studied, i. e. the Galois extensions with abelian galois group. Abelian extensions are somewhat easier to comprehend for a number of reasons, e.g. because all subgroups of an abelian group are normal. It follows from the Galois correspondence that the closed/open subgroups of the Galois group all correspond to Galois subextensions. The objective is to describe $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ using only objects within the field K itself.

"The object of class field theory is to show how the abelian extensions of an algebraic number field K can be determined by objects drawn from our knowledge of K itself; or, if one prefers to present things in dialectic terms, how a field contains within itself the elements of its own transcending."
— Chevalley, 1940 (translated)

The main theorem is Theorem 7.4.8, which approximates the structure of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the use of a map called the *global Artin map*. The approach we take here will be using *completions*: local fields associated to a prime ideal or embedding of a global field. The extensions of a global field can be described via extensions of these completions. The first chapter will therefore deal with *local class field theory*: the study of abelian extensions of local fields. In this chapter we construct the *local Artin map*, which approximates the structure of the maximal abelian Galois group of a local field. Subsequently, we connect extensions of global fields with extensions of their completions, so that we can use the local Artin maps of the completions to form the global Artin map.

In the next two chapters, whenever we talk about an extension, we will assume that this extension is both algebraic and separable.

6

LOCAL CLASS FIELD THEORY

We continue the study of local fields from Chapter 4 by investigating the extensions of local fields. The main theorem of this chapter is Theorem 6.4.2. It states the existence of the *local Artin map*, which connects the subgroups of the units of a local field with the finite abelian extensions of the field.

6.1 EXTENSIONS OF LOCAL FIELDS

As mentioned, we will assume all extensions to be algebraic and separable. Moreover, for every field we fix an algebraic closure. An extension is therefore Galois precisely when it is normal. Any finite extension L/K that fails to be normal is contained in a finite Galois extension (that lies in the fixed algebraic closure) called the *Galois closure* of L. It is defined as the smallest field containing L that is Galois over K. It is constructed using the primitive element theorem: L can be written as $K(\alpha)$ for some element α algebraic over K, then the Galois closure of L is the splitting field of α over K. As L is a finite extension, the Galois closure is a finite as well.

In the upcoming paragraphs, let L/K be an extension of degree n, where K is a local field with valuation v (and absolute value $|\cdot|$), ring of integers $\mathcal{O}$, residue field k. The first question is whether L is a local field with a valuation v_L that extends v. We will state theorems in the next paragraph that show that this is indeed the case if L/K is finite and that the valuation v_L is obtained very naturally.

In fact, the valuation is unique. To prove this, we borrow a fact from linear algebra, which will be useful as L is an n-dimensional vector space over K.

Proposition 6.1.1. Let K be a field, complete with respect to an absolute value $|\cdot|$. If V is a finite-dimensional vector space over K, then any two norms on V are equivalent and V is complete with respect to any norm. ◁

Proof. Theorem 0.1 of [Zho11]. □

Corollary 6.1.2. Any two extensions of the absolute value of $|\cdot|$ on K to L are equal. ◁

Proof. By considering L as a finite-dimensional vector space over K, the absolute values on L can be seen as norms, which must be equivalent. However, they agree on K, hence they must be equal. □

Define $\mathcal{O}_L$ as the integral closure of $\mathcal{O}_K$ in L. Note that $\mathcal{O}_K$ is a Dedekind domain. We prove that $\mathcal{O}_L$ is a Dedekind domain as well.

Proposition 6.1.3. Let R be a Dedekind domain, $K = \mathrm{Frac}(R)$ and L/K a finite extension. Then the integral closure of R in L is again a Dedekind domain. ◁

Proof. Theorem 4 of [Mor14]. □

As Dedekind domains have unique prime factorisation, the unique prime ideal $\pi\mathcal{O}_K$ of K factors uniquely in $\mathcal{O}_L$, say $\pi\mathcal{O}_L = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Note that $r \geq 1$ as $\pi\mathcal{O}_L \neq L$. Each

of those prime ideals induces a valuation $v_{\mathfrak{p}_i}$ and absolute value $|\cdot|_{\mathfrak{p}_i}$, and because for any $i \neq j$ there exists an element $a \in \mathcal{O}_L$ such that $a \in \mathfrak{p}_i$, $a \notin \mathfrak{p}_j$, the valuations (and absolute values) are not equivalent. However, they are all extensions of (a valuation equivalent to) v, hence, using Lemma 6.1.2, we find that $r \leq 1$. We conclude that there exists only a single prime lying over $\pi\mathcal{O}_L$, so we have $\pi\mathcal{O}_L = \mathfrak{p}^e$. As a result, L has a single prime ideal $\mathfrak{p}$. It is therefore also the unique maximal ideal, hence it consists of all non-units.

The valuation v_L is the valuation induced by $\mathfrak{p}$. We can make the valuation v_L explicit using the following theorem:

Theorem 6.1.4. Suppose L is a finite extension of a local field K of degree n. Denote by $\sigma_1, \ldots, \sigma_n$ the n distinct embeddings of L into its Galois closure over K. The valuations v and $|\cdot|$ on K can be extended uniquely to v_L and $|\cdot|_L$ on L by

$$v_L(x) = \frac{1}{n} v(N_{L/K}(x)) \text{ and } |x|_L = \sqrt[n]{|N_{L/K}(x)|},$$

where $N_{L/K}$ is the *norm map* given by $N_{L/K}(x) = \prod_i \sigma_i(x)$. ◁

Proof. Theorem 3.2 of [Sch12]. □

As was the case with $\mathcal{O}_K$, we have $\mathcal{O}_L^* = \{x \in \mathcal{O}_L : |x|_L = 1\}$, hence $\mathfrak{p} = \{x \in \mathcal{O}_L : |x|_L < 1\}$. However, as v is a discrete valuation, so is v_L, thus by Lemma 4.1.5, $\mathfrak{p}$ is principal, say $\mathfrak{p} = \pi_L\mathcal{O}_L$, which is a uniformiser of L. As $\mathfrak{p}^e = \pi\mathcal{O}_L$, we find that $v_L(\pi_L) = \frac{1}{e}$. This e is called the *ramification index*. The extension L/K is called *unramified* if $e = 1$ and ramified otherwise. If $e = n$, the extension is said to be *totally ramified*. Define $k_L = \mathcal{O}_L/\pi_L\mathcal{O}_L$.

Proposition 6.1.5. The extension k_L/k is finite. If we let f be the degree of this extension, then $ef = [L : K]$. ◁

Proof. Theorem 3.5(a) of [Sch12]. □

These results combined show that L is itself a local field.

A result of the previous theorems is that valuation interacts nicely with the Galois group of a Galois extension of local fields:

Corollary 6.1.6. The elements of the Galois groups of L/K preserve valuation. As a direct consequence, for any $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma\mathcal{O}_L^* = \mathcal{O}_L^*$ and $\sigma\mathfrak{m}_L = \mathfrak{m}_L$. ◁

Proof. For any $\alpha \in L$ and $\sigma \in \mathrm{Gal}(L/K)$ we have $N_{L/K}(\alpha) = \prod_{\tau \in \mathrm{Gal}(L/K)} \tau\alpha = \prod_{\tau \in \mathrm{Gal}(L/K)} \tau\sigma\alpha = N_{L/K}(\sigma\alpha)$ as multiplication with σ (from the right as well as the left) is a bijection of $\mathrm{Gal}(L/K)$, thus also $v_L(\alpha) = v_L(\sigma\alpha)$. □

6.2 UNRAMIFIED EXTENSIONS

In this section we consider the finite unramified extensions of a local field K, i. e. the extensions with ramification index equal to 1. It is possible to characterise all unramified finite Galois extensions, as explained by the lemmata below. We begin with a lemma that associates the finite unramified Galois extensions with the induced extension of residue fields.

Lemma 6.2.1. Let L/K be a finite Galois extension of local fields and let k_L be the residue field of L. If L/K is unramified, there exists an isomorphism $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(k_L/k)$. Moreover, the inverse is true as well; if $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$, then L/K is unramified. ◂

Proof. By the primitive element theorem, we can write $k_L = k[a]$, and let $\overline{f}(X) \in k[X]$ be the minimal polynomial of a. Finite fields are perfect, hence k_L/k is a separable extension, i. e. $\overline{f}$ does not have any double roots. We can lift $\overline{f}$ to a polynomial $f(X) \in K[X]$. Using Hensel's Lemma we know that there is a unique $\alpha \in L$ that is a root of f and $\overline{\alpha} = a$. However, L/K is Galois, hence the extension is normal, thus f must split completely in L. Returning to k_L, as $\overline{f}$ did not have any double roots, $\overline{f}$ splits completely in k_L. Thus k_L/k is normal and consequently Galois.

Corollary 6.1.6 states that any element σ of $\mathrm{Gal}(L/K)$ leaves $\mathcal{O}_L$ and $\mathfrak{m}_L$ intact, hence σ induces a field automorphism $\overline{\sigma} : \mathcal{O}_L/\mathfrak{m}_L \to \mathcal{O}_L/\mathfrak{m}_L$, which is in turn an element of $\mathrm{Gal}(k_L/k)$. As $\overline{\sigma} \cdot \overline{\tau} = \overline{\sigma \cdot \tau}$, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ given by $\sigma \mapsto \overline{\sigma}$ is a homomorphism.

If L/K is unramified, we have $[L : K] = [\mathcal{O}_L : \mathcal{O}] = [\mathcal{O}_L/(\pi) : \mathcal{O}/(\pi)] = [k_L : k]$. This implies that L is the splitting field of f, i. e. $L = K(\alpha)$. The elements of σ send α to another root of f, and no two different elements in $\mathrm{Gal}(L/K)$ will send α to the same root. All roots of $\overline{f}$ are distinct as k_L/k is separable, thus the elements of $\mathrm{Gal}(k_L/k)$ will send $a = \overline{\alpha}$ to the other roots of $\overline{f}$. Similarly, no two different elements in $\mathrm{Gal}(k_L/k)$ will send a to the same root of $\overline{f}$. By Hensel's Lemma, for every root a of $\overline{f}$ there is precisely one root of f that is mapped to a under the quotient map, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is injective and surjective, hence an isomorphism.

Suppose, on the other hand, we have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$. This implies $[L : K] = \#\mathrm{Gal}(L/K) = \#\mathrm{Gal}(k_L/k) = [k_L : k]$, and thus

$$[\mathcal{O}_L/\pi\mathcal{O}_L : \mathcal{O}/\pi\mathcal{O}] = [\mathcal{O}_L : \mathcal{O}] = [L : K] = [k_L : k] = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}/\mathfrak{m}].$$

As $\pi\mathcal{O} = \mathfrak{m}$ and $\mathcal{O}_L$ has at most one ideal of each index, we see that $\pi\mathcal{O}_L = \mathfrak{m}_L$, proving that L/K is unramified. ❐

Corollary 6.2.2. As all extensions of finite fields are cyclic, we see that unramified finite Galois extensions of local fields have cyclic Galois group. ◂

Another result of the proof is that we have a homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$. This homomorphism is surjective by Hensel's Lemma: an automorphism of the extension k_L/k is determined by a permutation of the roots of the polynomial of the extension, which we can lift to roots of the polynomial of L/K, where we can follow the same permutation. This results in the following proposition.

Proposition 6.2.3. There exists a surjective homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$. If we denote the kernel of this sequence by $I(L/K)$ (sometimes abbreviated to I), we obtain an exact sequence

$$1 \longrightarrow I(L/K) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(k_L/k) \longrightarrow 1. \quad \blacktriangleleft \tag{1}$$

Explicitly, we can write

$$I(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma x \equiv x \pmod{\mathfrak{m}_L} \ \forall\, x \in L\},$$

and $\#I(L/K) = e$.

Proof. An element σ of $\mathrm{Gal}(L/K)$ is trivial in $\mathrm{Gal}(k_L/k)$ precisely when σ leaves all elements fixed mod $\mathfrak{m}_L$, hence the explicit form of $I(L/K)$ follows.

As $n = \#\mathrm{Gal}(L/K)$, $f = \mathrm{Gal}(k_L/k)$, and $ef = n$ (Proposition 6.1.5), we find that $I(L/K)$ contains e elements. ❐

Corollary 6.2.4. If L/K is an unramified extension of local fields, then there exists a unique automorphism $\mathrm{Frob}_{L/K}$ that maps to the Frobenius generator of the finite field extension k_L/k. This automorphism will be called the *Frobenius element of* L/K. ◁

Proposition 6.2.5. Let L/K and M/K be two extensions of K. If L/K is unramified, then LM/M is unramified. ◁

Proof. Chapter II, Section 7, Proposition 7.2 of [NS99]. ❐

Corollary 6.2.6. The composite of two unramified extensions is again unramified. ◁

Proof. Call the extensions L/K and M/K. By the previous proposition, we have that LM/M is unramified. As M/K is unramified, we have an unramified tower of extensions $LM/M/K$, hence LM/K is unramified. ❐

Lemma 6.2.7. For a local field K and a positive integer n, there exists a unique unramified Galois extension L of degree n over K. It has a Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$. ◁

Proof. Suppose the residue field k of K has q elements, where q is some power of p. The extensions of k are given by $\mathbb{F}_{q^n}$ (the unique extension of degree n), obtained by adjoining the roots of $X^{q^n} - X$ to k. Let $\overline{f}(x) \in k[x]$ be the minimal polynomial for $\mathbb{F}_{q^n}/k$ and lift this to $f(x) \in K[x]$. As $f(x)$ is irreducible mod $\mathfrak{m}$, it is an irreducible polynomial. Let L be the splitting field of f (over K). As the roots of $\overline{f}$ are all distinct (the extension $\mathbb{F}_{q^n}/k$ is separable as k is perfect), the roots of f in L are all distinct as well. As L is defined as the splitting field of f, L/K is Galois. Moreover, both f and $\overline{f}$ have the same degree, hence L/K and $\mathbb{F}_{q^n}/k$ are extension of the same degree. As $\bar{f}$ is the minimal polynomial for $\mathbb{F}_{q^n}/K$, we obtain $\mathbb{F}_{q^n} \subseteq k_L$, thus we find $[k_L : k] \geq [\mathbb{F}_{q^n} : k] = [L : K]$. However, we have already shown that $[L : K] \geq [k_L : k]$, hence we find $[L : K] = [k_L : k]$. Using the proof of Lemma 6.2.1, we find that L/K is unramified. Moreover, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k) = \mathbb{Z}/n\mathbb{Z}$. Hence we have created an unramified Galois extension L/K of degree n.

To show that this is unique, suppose we have a different unramified Galois extension M/K of degree n. Let $E := M \cap L$. By assumption, $E \neq M, L$. The extensions L/E and M/E are unramified as well, thus both have a cyclic Galois group, both of the same order unequal to 1. Moreover, LM/E is an unramified extension by Corollary 6.2.6. However, As $L \cap M = E$, we have $\mathrm{Gal}(LM/E) = \mathrm{Gal}(L/E) \times \mathrm{Gal}(M/E)$, which is not cyclic as $\mathrm{Gal}(L/E)$ and $\mathrm{Gal}(M/E)$ are cyclic of the same order. This contradicts the fact that $\mathrm{Gal}(LM/E)$ is unramified; the unramified Galois extension of K of degree n is thus unique. ❐

Let K_n stand for the unique unramified Galois extension of K of degree n. As the compositum of two unramified extensions is again unramified, it makes sense to take the composite of all unramified Galois extensions of a local field K: denote this by K^{ur}. It is known as the *maximal unramified extension*. Using Lemma 6.2.7, we see that $\mathrm{Gal}(K^{\mathrm{ur}}/K) = \varprojlim \mathrm{Gal}(K_n/K) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$. Interestingly enough, this is independent of K.

This concludes the section on unramified extensions; we know what the unramified Galois extensions of a local field look like, and we have found the Galois group of the maximal unramified extension.

6.3 TOTALLY RAMIFIED EXTENSIONS

Recall that an extension L/K of degree n is called totally ramified if the extension of the valuation of K to L has image $\frac{1}{n}\mathbb{Z} \cup \{\infty\}$. Alternatively, one might state that the prime elements π resp. π_L of K resp. L abide $\pi = u\pi^n$ for some $u \in \mathcal{O}^*$, i. e. $\mathfrak{m} = (\pi) = (\pi_L)^n = \mathfrak{m}_L^n$. Interestingly, we have $[k_L : k] = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}/\mathfrak{m}] = \frac{1}{n}[\mathcal{O}_L/\mathfrak{m} : \mathcal{O}/\mathfrak{m}] = \frac{1}{n}[\mathcal{O}_L : \mathcal{O}] = \frac{1}{n}[L : K] = 1$, so we see that the residue field has not grown at all! This is in sharp contrast with the unramified extensions, where we had $[k_L : k] = [L : K]$.

Unfortunately, totally ramified extensions are not as easily characterised as unramified extensions. First of all, the compositum of the totally ramified extensions need not be totally ramified. We illustrate this with a small example below. Furthermore, the extensions are often based on polynomials that depend on the choice of uniformiser, creating many different totally ramified extensions.

Example. We start with an example where the composite of two totally ramified extensions is not totally ramified. Consider the local field $\mathbb{Q}_p$ with uniformiser p. Let q be a nonsquare modulo p and the extensions $\mathbb{Q}_p[\sqrt{p}]$ and $\mathbb{Q}_p[\sqrt{pq}]$ (these extensions are different as q is a nonsquare). These are both extensions of degree 2, and in the fields the ideal (p) factorises as $(\sqrt{p})^2$ resp. $(\sqrt{pq})^2 = (pq) = (p)$, thus both extensions are totally ramified. However, the composite $\mathbb{Q}_p[\sqrt{p}, \sqrt{pq}] = \mathbb{Q}_p[\sqrt{p}, \sqrt{q}]$ is not totally ramified as it contains the subfield $\mathbb{Q}_p[\sqrt{q}]$, which is an unramified extension of $\mathbb{Q}_p$ as the maximal ideal (p) remains inert.

However, not all hope is lost; there is still a great deal of structure to be found in totally ramified extensions. For this, we start with the notion of an *Eisenstein polynomial*:

Definition 6.3.1 (EISENSTEIN POLYNOMIAL)**.** A polynomial $a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}[x]$ is *Eisenstein* if $v(a_0) = 0$, $v(a_i) \geq 1$ for all $1 \leq i < n$ and $v(a_n) = 1$. ◁

Proposition 6.3.2. Any Eisenstein polynomial is irreducible. ◁

Proof. Suppose an Eisenstein polynomial $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ is not irreducible and write $f(x) = g(x)h(x)$, where both $g(x) = g_0x^a + \cdots + g_a$ and $h(x) = h_0x^b + \cdots + h_b$ are polynomials in $\mathcal{O}[x]$. We can expand the product:

$$\begin{aligned} g(x)h(x) &= (g_0x^a + \cdots + g_a)(h_0x^b + \cdots + h_b) \\ &= g_0h_0x^{a+b} + \cdots + (g_{a-1}h_b + g_ah_{b-1})x + f_ag_b. \end{aligned}$$

As $v(g_ah_b) = v(a_n) = 1$, we have either $v(g_a) = 0$ and $v(h_b) = 1$ or $v(g_a) = 1$ and $v(h_b) = 0$. Without loss of generality, assume the former. As $v(g_{a-1}h_b + g_ah_{b-1}) = v(a_{n-1}) \geq 1$ and $v(g_a) = 1$, $v(h_b) = 0$, we must have $v(g_{a-1}) \geq 1$. Proceeding with the coefficient of x^2, we find $v(g_{a-2}h_b + g_{a-1}h_{b-1} + g_ah_{b-2}) \geq 1$, hence $v(g_{a-2}) \geq 1$. By repetition of this argument we see that $v(g_i) \geq 1$ for all $0 \leq i \leq a$, contradicting the fact that $v(g_0h_0) = v(a_0) = 0$. Thus any Eisenstein polynomial is irreducible. ❐

As a corollary, the Eisenstein polynomials are suitable as polynomials for extensions of K. In fact, they play a much bigger role, clarified by the following theorem:

Theorem 6.3.3. An extension L/K of local fields is totally ramified precisely when $L = K(\alpha)$, with α a root of an Eisenstein polynomial. ◁

Proof. Theorem 2.4 of [Cai10]. ❐

Corollary 6.3.4. There exists a totally ramified extension of K of degree n for any $n \geq 1$. ◁

Proof. The polynomial $X^n - \pi$ is Eisenstein for any uniformiser π of K. □

As mentioned, the composite of two totally ramified extensions is not necessarily totally ramified. As a result, we cannot create a "maximal totally ramified extension" in the same manner we did for unramified extensions. It is, however, still possible to create a tower of totally ramified extensions (of which the composite is totally ramified), which itself does not contain all totally ramified extensions, but once combined with K^{ur}, it will contain every totally ramified extension. To construct this tower we need the so-called Lubin-Tate formal group laws, about which we will only state the most important results.

In the following sections, we will heavily use the polynomial $f(X) = X^q + \pi X$ for a fixed uniformiser π. Note that $f(X)/X$ is an Eisenstein polynomial.

Theorem 6.3.5 (Lubin-Tate formal group law)**.** There exists a unique power series $F_f \in \mathcal{O}[[X, Y]]$ such that $F_f(X, Y) \equiv X + Y \mod \deg 2$, $F_f(X, Y) = F_f(Y, X)$ and $f \circ F_f = F_f \circ f$ called the *commutative formal group law*. ◁

Proposition 6.3.6. For every $a \in \mathcal{O}$, there exists a unique $[a] \in \mathcal{O}[[X]]$ such that $[a] \equiv aX \pmod{\deg 2}$ and $[a] \circ f = f \circ [a]$. ◁

Proof. Lemma 4.2 of [Rieo6]. □

Here mod deg 2 means that we only consider linear and constant terms. An important remark is that $[\pi] = f$. The notation $X +_{F_f} Y := F_f(X, Y)$ is often used. Let $\mathfrak{m}^s = \{\alpha \in K^s \mid |\alpha| < 1\}$, where the absolute value of α in K^s is the absolute value of α in $K(\alpha)$. With the Lubin-Tate formal group law, we can adhere an $\mathcal{O}$-module structure to $\mathfrak{m}^s$ using $+_{F_f}$ and $a \cdot \alpha = [a](\alpha)$. Call the resulting $\mathcal{O}$-module Λ. Consider the submodules $\Lambda_n := \operatorname{Ann}(\pi^n) = \{\alpha \in \Lambda : \pi^n \cdot \alpha = 0\}$ for any $n \in \mathbb{N}$ and note that $\pi^n \cdot \alpha = 0$ precisely when $f^n(\alpha) = 0$, where $f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}}$. It is immediate that Λ_{n-1} is a submodule of Λ_n for any n. As f is a polynomial, f^n has finitely many roots, thus Λ_n has a finite number of elements. Because $\mathcal{O}$ has only ideals of the form (π^m), it is a principal ideal domain. By the structure theorem for finitely generated modules we have

$$\Lambda_n \cong \mathcal{O}/(\pi^{d_1}) \times \cdots \times \mathcal{O}/(\pi^{d_m}),$$

where the d_i are positive integers. In the separable closure, f has q distinct roots. However, as we have seen, $f(X)/X$ is Eisenstein, thus the roots all have positive valuation. Hence all the roots of f lie in Λ. As a result, Λ_1 has $q = \#\mathcal{O}/(\pi)$ elements, and the structure theorem guarantees $\Lambda_1 \cong \mathcal{O}/(\pi)$.

For the other Λ_n, we prove that there exists an exact sequence

$$0 \longrightarrow \Lambda_1 \longrightarrow \Lambda_n \xrightarrow{\pi} \Lambda_{n-1} \longrightarrow 0,$$

where $\Lambda_1 \to \Lambda_n$ is inclusion and $\pi : \Lambda \to \Lambda$ is given by multiplication with π. We want to prove that this map is surjective, i. e. for all $\alpha \in \Lambda$ there is a $\beta \in \Lambda$ with $f(\beta) = \alpha$. The polynomial $f(X) - \alpha$ has q different roots in Λ, and their product is $\pm\alpha$, which has positive valuation, hence all roots must have positive valuation, thus they lie in Λ. So not only is π surjective, it is even a q-to-1 map. As $\alpha \in \Lambda_n \Leftrightarrow f^n(\alpha) = 0$,

we can restrict π to a homomorphism $\pi : \Lambda_n \to \Lambda_{n-1}$. Moreover, we claim that $\pi^{-1}(\Lambda_{n-1}) = \Lambda_n$. Suppose $\alpha \in \Lambda_{n-1}$ and let $\beta \in \Lambda$ such that $f(\beta) = \alpha$. As $\alpha \in \Lambda_{n-1}$, we have $f^n(\beta) = f^{n-1}(\alpha) = 0$, hence $\beta \in \Lambda_n$. Hence the restriction $\pi : \Lambda_n \to \Lambda_{n-1}$ is a surjective q-to-1 map. Moreover, it is clear that $\ker(\pi) = \mathrm{Ann}(\pi) = \Lambda_1$.

Using the exact sequence, combined with the fact that $\#\Lambda_1 = q$, we inductively find $\#\Lambda_n = q^n$. Assume as an induction hypothesis that $\Lambda_i \cong \mathcal{O}/(\pi^i)$ for all $1 \leq i \leq n$ (this holds for the base case $n = 1$). Using the structure theorem, we have either $\Lambda_{n+1} \cong \mathcal{O}/(\pi^n) \times \mathcal{O}/(\pi)$ or $\Lambda_{n+1} \cong \mathcal{O}/(\pi^{n+1})$ as it must contain $\Lambda_n \cong \mathcal{O}/(\pi^n)$. As Λ_{n+1} is not annihilated bu π^n by construction, but $\mathcal{O}/(\pi^n) \times \mathcal{O}/(\pi)$ is, we find $\Lambda_{n+1} \cong \mathcal{O}/(\pi^{n+1})$. As a result, we have $\mathrm{Aut}(\Lambda_n) = (\mathcal{O}/(\pi^n))^*$.

Define $K_{\pi,n} := K[\Lambda_n]$. We obtain a tower of extensions $K \subseteq K[\Lambda_1] \subseteq \cdots \subseteq K[\Lambda_n] \subseteq \ldots$.

Proposition 6.3.7. For any n, $K_{\pi,n}$ is a totally ramified extension of degree $(q-1)q^{n-1}$ with Galois group isomorphic to $(\mathcal{O}/(\pi^n))^*$. ◂

Proof. We create intermediate extensions between K and $K_{\pi,n}$ to show the desired results.

Let α_1 be any nonzero root of f. As $f(X)/X$ is Eisenstein, $K[\alpha_1]/K$ is totally ramified of degree $q-1$. Then consider the polynomial $X^q + \pi X - \alpha_1 \in \mathcal{O}_{K[\alpha_1]}[X]$. As mentioned in the proof of Theorem 6.3.3, α_1 is a uniformiser of $K[\alpha_1]$, hence $X^q + \pi X - \alpha_1$ is an Eisenstein polynomial in $\mathcal{O}_{K[\alpha_1]}[X]$. Take any root α_2 and we obtain an extension $K[\alpha_1, \alpha_2]/K[\alpha_1]$, which is totally ramified of degree q. We have $K[\alpha_1, \alpha_2] = K[\alpha_2]$ as $\alpha_1 = \alpha_2^q + \pi\alpha_2$. We can repeat this process to obtain $\alpha_1, \ldots, \alpha_n$, where α_i is a root of $f(X) - \alpha_{i-1}$, or $f(\alpha_i) = \alpha_{i-1}$. Note that as α_1 is a root of f unequal to zero, α_i is a root of f^i, but not of f^{i-1}.

As $K \subseteq K[\alpha_1] \subseteq \cdots \subseteq K[\alpha_n]$ is a tower obtained by adhering a root of an Eisenstein polynomial to the previous extension. It follows from Theorem 6.3.3 that all extensions are totally ramified, and $[K[\alpha_1] : K] = q-1$, while $[K[\alpha_i] : K[\alpha_{i-1}]] = q$ for $i > 1$. Hence $K[\alpha_n]/K$ is a totally ramified extension of degree $(q-1)q^{n-1}$.

As mentioned, α_n is a root of f^n, hence $K[\alpha_n] \subseteq K_{\pi,n}$. The elements of the Galois group of $K_{\pi,n}$ permute the elements of Λ_n. As the Galois elements commute with polynomials, i. e. $\sigma(g(\alpha)) = g(\sigma(\alpha))$, they commute with power series as well, thus the elements of the Galois group act as $\mathcal{O}$-module isomorphisms on Λ_n. As a result, $\mathrm{Gal}(K[\Lambda_n]/K)$ is (isomorphic to) a subgroup of $\mathrm{Aut}(\Lambda_n) \cong (\mathcal{O}/(\pi^n))^*$, which has order $(q-1)q^{n-1}$. Hence $\#\mathrm{Gal}(K[\Lambda_n]/K) \leq (q-1)q^{n-1}$, thus $[K_{\pi,n} : K] \leq (q-1)q^{n-1}$. However, we have seen that $K[\alpha_n] \subseteq K_{\pi,n}$, and $K[\alpha_n]/K$ is an extension of degree $(q-1)q^{n-1}$. We conclude that $K[\alpha_n] = K_{\pi,n}$, thus $K_{\pi,n}$ is a totally ramified extension of degree $(q-1)q^{n-1}$. Furthermore, $\mathrm{Gal}(K[\Lambda_n]/K)$ is isomorphic to the entire group $\mathrm{Aut}(\Lambda_n)$, thus $\mathrm{Gal}(K[\Lambda_n]/K) \cong (\mathcal{O}/(\pi^n))^*$. ❐

Let $K_\pi := \bigcup_n K_{\pi,n}$. As $K_{\pi,n} \subseteq K_{\pi,n+1}$ and $K_{\pi,n}$ is totally ramified for all n with Galois group $(\mathcal{O}/(\pi^n))^*$, we have $\mathrm{Gal}(K_\pi/K) \cong \varprojlim \mathrm{Gal}(K_{\pi,n}/K) \cong \varprojlim (\mathcal{O}/(\pi^n))^* \cong \mathcal{O}^*$. The extension K_π is still dependent on the choice of uniformiser π.

6.4 THE MAXIMAL ABELIAN EXTENSION

This final section states the central theorem of local class field theory (Theorem 6.4.2): the existence of the local Artin map, which creates a connection between the subgroups of $K^\times$ and the finite abelian extensions of K. Our starting point is Lemma 6.4.1,

we uses the previous sections to help structure the Galois group of the maximal abelian extension K^{ab}, which is the composite of all finite abelian extensions.

6.4.1 CONSTRUCTION OF THE MAXIMAL ABELIAN EXTENSION

So far we have explored the unramified extensions, from which we obtained a composite of all unramified extensions K^{ur}, and the totally ramified extensions, from which we obtained a union of a tower of extensions K_π. They combine nicely in the following lemma:

Lemma 6.4.1. For any choice of uniformiser π we have $K^{\text{ab}} = K^{\text{ur}} \cdot K_\pi$. As a result, $\text{Gal}(K^{\text{ab}}/K) \cong \text{Gal}(K^{\text{ur}}/K) \times \text{Gal}(K_\pi/K) \cong \hat{\mathbb{Z}} \times \mathcal{O}^*$. ◁

Proof. Section 6.1 of [Rieo6]. □

We make two important remarks about this lemma: firstly, even though K_π is dependent on the choice of π, K^{ab} is not. Secondly, as $K^\times \cong \mathbb{Z} \times \mathcal{O}^*$ (recall that every element can be written uniquely as $u \times \pi^n$, $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$) it seems that there may exist a map $K^\times \to \text{Gal}(K^{\text{ab}}/K)$, using an embedding $\mathbb{Z} \to \hat{\mathbb{Z}}$ and an automorphism of $\mathcal{O}^*$. It turns out that this is indeed the case.

6.4.2 THE LOCAL ARTIN MAP

In this final section we will state the main theorem of local class field theory: the existence and unicity of a group homomorphism $K^\times \to \text{Gal}(K^{\text{ab}}/K)$ that contains all information on the Galois groups of finite abelian extensions of K.

The full theorem is as follows:

Theorem 6.4.2. Let K be a local field with uniformiser π. There exists a unique continuous group homomorphism $\phi : K^\times \to \text{Gal}(K^{\text{ab}}/K)$ known as the *local Artin map* such that

1. we have induced isomorphisms $K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K)$ via $a \mapsto \phi(a)\big|_L$ for any finite extension L/K;
2. the restriction of $\phi(\pi)$ to a finite unramified extension L of K for any uniformiser π is the Frobenius automorphism of L/K, i. e. $\phi(\pi)\big|_L = \text{Frob}_{L/K}$.

Moreover, any open subgroup of $K^\times$ of finite index is of the form $N_{L/K}(L^\times)$ for some finite abelian extension L of K. ◁

Proof. Theorem 5.1 of [Rieo6]. □

We can describe the map using the decompositions of the previous sections (see page 21 of [Rieo6]):

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\ 1 & \longrightarrow & \text{Gal}(K^{\text{ab}}/K^{\text{ur}}) & \longrightarrow & \text{Gal}(K^{\text{ab}}/K) & \longrightarrow & \text{Gal}(K^{\text{ur}}/K) & \longrightarrow & 1. \end{array}$$

The map $\mathcal{O}^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K)$ is an isomorphism, given by sending $u \in \mathcal{O}^*$ to the automorphism $[u^{-1}]_f$, where again $f = X^q + \pi X$. The map $\mathbb{Z} \to \mathrm{Gal}(K^{\mathrm{ur}}/K)$ sends n to Frob^n, where

$$\mathrm{Frob} = \prod_{\substack{L/K \\ \text{finite abelian}}} (\mathrm{Frob}_{L/K}) \in \varprojlim_{\substack{L/K \\ \text{finite abelian}}} \mathrm{Gal}(L/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K),$$

the *universal Frobenius*.

By descending to a finite abelian extension L/K and using the exact sequence from Proposition 6.2.3 we can extend the diagram above to include a third row:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ur}}/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I(L/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k) & \longrightarrow & 1.
\end{array}$$

As all finite extensions of finite fields are generated by the Frobenius, that induced map $\mathbb{Z} \to \mathrm{Gal}(k_L/k)$ is surjective. As the map $\mathcal{O}^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})$ is an isomorphism and $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \to I(L/K)$ is surjective, the composite $\mathcal{O}^* \to I(L/K)$ is surjective as well for any finite abelian extension L/K.

7

GLOBAL CLASS FIELD THEORY

As in the chapter on local fields, *global class field theory* studies the finite abelian extensions of a global field. The first sections are mostly definitions and basic theorems, so that in Section 7.4 we can state the central result of global class field theory, Theorem 7.4.8. It states the existence of a map that approximates the maximal abelian Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and is called the *global reciprocity map* or *global Artin map*. This map comes to life by making a connection between global field extensions and local field extensions, Theorem 7.4.2, after which we can rely on the local reciprocity map to define this global reciprocity map.

7.1 COUNTING EXTENSIONS OF GLOBAL FIELDS

This short section is devoted to showing that global fields have countably many extensions.

Lemma 7.1.1. Suppose S is a countable set. Then the polynomial ring $S[X]$ is countable as well. ◁

Proof. Let $S_n[X]$ be the polynomials of degree n. Then we have a bijection $S_n[X] \to S^{n+1}$ via

$$\sum_{i=0}^{n} s_i X^i \mapsto (s_0, s_1, \ldots, s_n).$$

As S is countable, S^{n+1} is countable, hence $S_n[X]$ is countable. Because we have $S[X] = \bigcup_{n\in\mathbb{N}} S_n[X]$, which is a countable union of countable sets, we find that $S[X]$ is countable as well. ❐

Theorem 7.1.2. Any global field K has countably many finite extensions. ◁

Proof. A global field is either a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(T)$ for some prime power q and transcendent element T. Any finite extension of K is therefore either a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_q(T)$. Certainly $\mathbb{Q}$ is countable, and by Lemma 7.1.1 we find that $\mathbb{F}_q(T)$ is countable as well.

Let F be either $\mathbb{Q}$ or $\mathbb{F}_q(T)$. The finite extensions of F are obtained by adding a root of a polynomial in $F[X]$ to F. By Lemma 7.1.1 only countable many such polynomials exist, and each of those polynomials has a finite number of roots, hence there are countably many roots of polynomials over F. Thus F has countably many finite extensions, and it follows that K has countably many finite extensions as well. ❐

7.2 SPLITTING BEHAVIOUR OF PRIMES

We prove that for any Galois extension it is possible to define certain subgroups of the Galois group that separate the types of behaviour that the primes can display, namely splitting, ramification, and staying inert.

We start with an important theorem on the behaviour of prime ideals in finite extensions, taken from J.S. Milne's Algebraic Number Theory, [Mil14].

Theorem 7.2.1. Let L/K be an extension of global fields of degree n. Let $\mathfrak{p}$ be a prime ideal (or equivalently a finite prime) of K and $\mathfrak{q}_1, \dots, \mathfrak{q}_g$ the primes of L dividing $\mathfrak{p}$, and write e_i respectively f_i for the ramification index respectively residue class degree. Then

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

If additionally L/K is Galois, then all e_i and f_i are equal, which will be named e and f respectively, (so we have $efg = n$) and $\mathrm{Gal}(L/K)$ acts transitively on the prime ideals of L dividing $\mathfrak{p}$. ◁

Proof. Theorem 3.34 of [Mil14]. □

7.2.1 DECOMPOSITION AND INERTIA GROUPS

Fix a finite extension L/K of degree n and let $G = \mathrm{Gal}(L/K)$. We define a pair of groups associated to G, namely the *decomposition* and *inertia group*. Using the groups we can split the extension L/K into a tower of extensions $L/L^I/L^D/K$, where in every extension the primes over a certain prime of K exhibit only a single type of behaviour: in L^D/K, they split completely, in L^I/L^D, they are completely inert, while in L/L^I, they are totally ramified.

Definition 7.2.2 (DECOMPOSITION GROUP)**.** Let L/K be an extension of global fields with Galois group G. Let $\mathfrak{p}$ be a finite prime of K and $\mathfrak{q}$ a (finite) prime of L lying over $\mathfrak{p}$. Define the *decomposition group of* $\mathfrak{q}$, $G_\mathfrak{q}$, as

$$G_\mathfrak{q} = \{\sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q}\}.$$ ◁

The decomposition group will help establish a connection between Galois extensions of global fields and their localisations.

Lemma 7.2.3. The decomposition groups $D_\mathfrak{q}$ corresponding to primes $\mathfrak{q}$ of L lying over the same prime $\mathfrak{p}$ of K are conjugate in G. ◁

Proof. For any $\sigma, \tau \in G$, as they are field automorphisms, we have $(\tau\sigma\tau^{-1})(\mathfrak{q}) = \mathfrak{q}$ precisely when $\sigma(\tau^{-1}(\mathfrak{q})) = \tau^{-1}(\mathfrak{q})$. Hence $\tau\sigma\tau^{-1} \in D_\mathfrak{q}$ if and only if $\sigma \in D_{\tau^{-1}(\mathfrak{q})}$ and therefore $\tau^{-1} D_\mathfrak{q} \tau = D_{\tau^{-1}(\mathfrak{q})}$. By Theorem 7.2.1, G acts transitively on the set of primes dividing $\mathfrak{p}$, and therefore we obtain that the decomposition groups are indeed conjugate in G. □

Corollary 7.2.4. From the Orbit-Stabiliser Theorem we deduce that $[G : D_\mathfrak{q}] = g$, the number of primes in L dividing $\mathfrak{p}$, for any $\mathfrak{q}$ dividing $\mathfrak{p}$. ◁

Theorem 7.2.5. For readability, write $D = D_\mathfrak{q}$. The *fixed field* L^D of D, defined by

$$L^D = \{a \in L : \sigma a = a \text{ for all } \sigma \in D\},$$

is the smallest subfield $E \subseteq L$ such that $g(L/E) = 1$. ◁

Proof. We have $\mathrm{Gal}(L/L^D) \simeq D$ and $\mathfrak{q} \cap L^D$ is a prime of L^D. Theorem 7.2.1 states that D acts transitively on the primes lying over $\mathfrak{q} \cap L^D$. However, by definition D leaves $\mathfrak{q}$ invariant, thus $\mathfrak{q}$ must be the only prime in L dividing $\mathfrak{q} \cap L^D$. Thus $g(L/L^D) = 1$.

Conversely, if $E \subseteq L$ is such that $\mathfrak{q}$ is the only prime lying over $\mathfrak{q} \cap E$, then $\mathrm{Gal}(E/L)$ certainly fixes $\mathfrak{q}$, hence $\mathrm{Gal}(E/L) \subseteq D_\mathfrak{q}$, or $L^D \subseteq E$. □

The proposition effectively states that when going from L^D to L, the primes above $\mathfrak{p}$ do not split, but stay inert or ramify (or some combination). We can strengthen this somewhat by showing that when going from K to L^D, $\mathfrak{p}$ splits completely. Please be aware that L^D/K need not be Galois. (For this D would need to be a normal subgroup. This is a bit of foreshadowing, we will later consider abelian extensions and L^D/K will then be Galois.)

Proposition 7.2.6. We have $e(L/L^D) = e(L/K)(= e)$ and $f(L/L^D) = f(L/K)(= f)$. As a result, the prime $\mathfrak{p}$ only ramifies and/or stays inert when going from L^D to L, not from K to L^D, where it only splits (completely). ◂

Proof. We have $\#D = {}^{\#G}/_{[G:D]} = {}^{efg}/_{g} = ef$. Recall $g(L/L^D) = 1$, hence

$$e(L/L^D)f(L/L^D) = [L : L^D] = \#D = ef.$$

However, L^D is a subextension of L/K, hence $e(L/L^D) \leq e$ and $f(L/L^D) \leq f$, and we may conclude the proposed. ❐

Corollary 7.2.7. L^D is the largest field in which $\mathfrak{p}$ splits completely. ◂

Denote by $\mathbb{F}_\mathfrak{p} = {}^{\mathcal{O}_K}/_{\mathfrak{p}}$ and $\mathbb{F}_\mathfrak{q} = {}^{\mathcal{O}_L}/_{\mathfrak{q}}$ the residue fields of $\mathfrak{p}$ in K and $\mathfrak{q}$ in L, respectively. The finite field extension $\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$ is of degree f and has a cyclic Galois group generated by the *Frobenius automorphism* $\mathrm{Frob}_\mathfrak{q}$.

Any Galois element σ of L/K abides $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. If additionally $\sigma(\mathfrak{q}) = \mathfrak{q}$, i. e. $\sigma \in D_\mathfrak{q}$, then σ induces a field automorphism of $\mathbb{F}_\mathfrak{q} = {}^{\mathcal{O}_L}/_{\mathfrak{q}}$. We obtain a reduction homomorphism $D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$.

Lemma 7.2.8. The homomorphism $D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is surjective. ◂

Proof. By the primitive element theorem, we have an $\bar{a} \in \mathbb{F}_\mathfrak{q}$ such that $\mathbb{F}_\mathfrak{q} = \mathbb{F}_\mathfrak{p}(\bar{a})$. We can lift $\bar{a}$ to an element a of $\mathcal{O}_K \subseteq \mathcal{O}_{L^D}$. Let $P = \prod_{\sigma \in D_\mathfrak{q}}(x - \sigma(a)) \in L^D[x]$ be the characteristic polynomial of a over L^D. Returning to the residue fields, $\bar{P} = \prod_{\sigma \in D_\mathfrak{q}}(x - \sigma(\bar{a}))$ is a polynomial in the polynomial ring of the residue field of the prime $\mathfrak{q} \cap L^D$. Theorem 7.2.6 states that the residue field of $\mathfrak{q}$ does not grow when going from K to L^D (as $f(L^D/K) = 1$), thus $\bar{P} \in \mathbb{F}_\mathfrak{p}[x]$. Moreover, $\bar{a}$ is a root of $\bar{P}$. However, as $\bar{P} \in \mathbb{F}_\mathfrak{p}[x]$, the minimal polynomial of $\bar{a}$ divides $\bar{P}$, i. e. all Galois conjugates of $\bar{a}$ must also be roots of $\bar{P}$. In particular, $\mathrm{Frob}_\mathfrak{q}(a)$ is such a root, and is therefore of the form $\sigma(\hat{a})$, implying that $\mathrm{Frob}_\mathfrak{q}$ is in the image of $D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. As $\mathrm{Frob}_\mathfrak{q}$ is the generator of $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$, this suffices to prove the lemma. ❐

Definition 7.2.9 (INERTIA GROUP)**.** The *inertia group* is defined as the kernel of the homomorphism $D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. We obtain an exact sequence

$$1 \longrightarrow I_\mathfrak{q} \longrightarrow D_\mathfrak{q} \longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) \longrightarrow 1. \quad \blacktriangleleft \tag{2}$$

This implicit definition of an inertia group can be made more explicit:

Proposition 7.2.10. We have $\#I_\mathfrak{q} = e$ and

$$I_\mathfrak{q} = \{\sigma \in G : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in \mathcal{O}_L\}. \quad \blacktriangleleft$$

Proof. The first assertion follows from the exact sequence as $\#D_\mathfrak{q} = ef$ and $[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] = f$. Secondly, the elements in the kernel of $D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ are precisely those that abide $\sigma a \equiv a \pmod{\mathfrak{q}}$ for all $a \in \mathcal{O}_L$, hence

$$I_\mathfrak{q} = \{\sigma \in D_\mathfrak{q} : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in \mathcal{O}_L\}.$$

Suppose $\sigma \notin D_\mathfrak{q}$. Then $\sigma^{-1} \notin D_\mathfrak{q}$, hence $\sigma^{-1}(\mathfrak{q}) \neq \mathfrak{q}$. However, both are prime ideals, hence (using, for example, the Chinese Remainder Theorem) we can find some $a \in \mathcal{O}_L$ that lies in $\mathfrak{q}$, but not in $\sigma^{-1}(\mathfrak{q})$. Hence we have $a \in \mathfrak{q}$, while $a \notin \sigma(\mathfrak{q})$, hence $\sigma(a) \not\equiv a \pmod{\mathfrak{q}}$. We conclude that

$$\begin{aligned} I_\mathfrak{q} &= \{\sigma \in D_\mathfrak{q} : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in \mathcal{O}_L\} \\ &= \{\sigma \in G \ \ : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in \mathcal{O}_L\}. \end{aligned}$$

∎

Corollary 7.2.11. The prime $\mathfrak{p}$ of K is unramified in L/K precisely when the inertia groups $I_\mathfrak{q}$ are trivial. ◁

We have a similar fixed field theorem as we had for the decomposition group:

Theorem 7.2.12. Write $I = I_\mathfrak{q}$. Then L^I is the largest subfield of L in which $\mathfrak{p}$ is unramified. ◁

Proof. Consider the prime $\mathfrak{q} \cap L^I$ of L^I. As we have seen in Theorem 7.2.5, $g(L/L^D) = 1$, hence $g(L/L^I) = 1$ and we obtain that $\mathfrak{q}$ is the only prime dividing $\mathfrak{q} \cap L^I$. As the Galois group $\mathrm{Gal}(L/L^I)$ is precisely the inertia group, we see from the exact sequence (2) that the Galois group of the extension $\mathbb{F}_\mathfrak{q}/\mathbb{F}_{\mathfrak{q}\cap L^I}$ is trivial, hence $\mathbb{F}_\mathfrak{q} = \mathbb{F}_{\mathfrak{q}\cap L^I}$. This implies that $f(L/L^I) = 1$. As $[L : L^I] = \#I = e$, we conclude that $e(L/L^I) = e(L/L^I)f(L/L^I)g(L/L^I) = [L : L^I] = e$. In turn, this implies $e(L^I/K) = 1$.

Now suppose we have a field $K \subseteq E \subseteq L$ and the prime $\mathfrak{q} \cap E$. The inertia group of $\mathfrak{q}$ over E, denoted I_E, is equal to

$$I_E = \{\sigma \in \mathrm{Gal}(L/E) : \sigma a \equiv a \pmod{\mathfrak{q}} \text{ for all } a \in \mathcal{O}_L\} = I \cap \mathrm{Gal}(L/E).$$

It follows that $L^{I_E} = L^I \cdot E$.

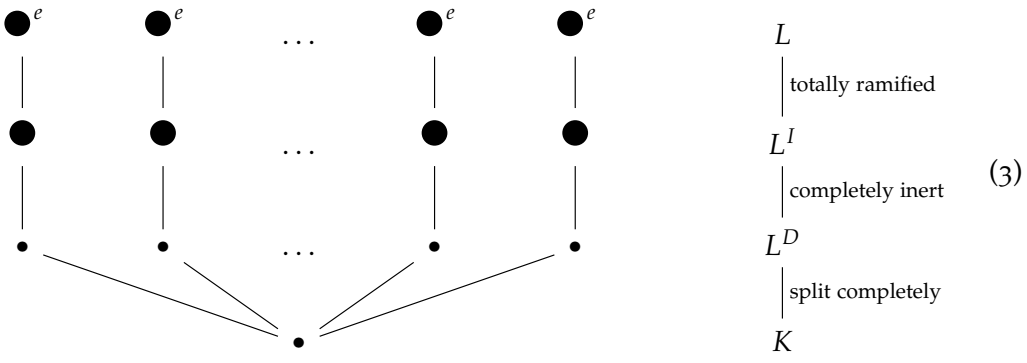
Suppose that $\mathfrak{p}$ is unramified in E. Then $e(L/L^{I_E}) = {}^{e(L/K)}/_{e(L^{I_E}/K)} = {}^{e}/_{1} = e$ (here $e(L/L^{I_E})$ is the ramification index of $\mathfrak{q} \cap E$ in L). The ramification index of $\mathfrak{q} \cap E$ in L is equal to the index of the inertia field L^{I_E} in L (we have seen this in Proposition 7.2.10). Hence

$$[L : L^I \cdot E] = [L : L^{I_E}] = e(L/L^{I_E}) = e = [L : L^I],$$

and we conclude that $E \subseteq L^I$. This proves the theorem. ∎

Corollary 7.2.13. Suppose we have two finite unramified extensions L_1/K, L_2/K. Suppose they both lie in some finite Galois extension L/K. Then they lie in $\bigcap L^{I_\mathfrak{q}}$ for all primes in L, hence the compositum $L_1 \cdot L_2$ does as well. Thus $L_1 \cdot L_2$ is unramified. ◁

We can summarise the theorems in the following diagram:



(3)

Every black dot represents a prime, and the size of the dot symbolises the size of the residue field. The credits for this picture and many proofs in this section go to William Stein, [Ste04].

7.2.2 THE FROBENIUS ELEMENT

If the prime $\mathfrak{p}$ is unramified in L/K, the inertia groups are trivial, as we have seen in Corollary 7.2.11. Hence, fixing a prime $\mathfrak{q}$ of L dividing $\mathfrak{p}$, we obtain the exact sequence

$$1 \longrightarrow 1 \longrightarrow D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1, \tag{4}$$

i. e. an isomorphism $D_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. Thus there is a unique element in $D_{\mathfrak{q}}$ that maps to the Frobenius element of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ (the generator that raises every element to the power $\#\mathbb{F}_{\mathfrak{p}}$). Denote this element by $(\mathfrak{q}, L/K)$ (this is the notation used in [Mil14].)

Proposition 7.2.14. The set of Frobenius elements $\{(\mathfrak{q}, L/K) : \mathfrak{q} \mid \mathfrak{p}\}$ form a conjugacy class, denoted $(\mathfrak{p}, L/K)$. ◁

Proof. From Lemma 7.2.3 we know that the decomposition groups are conjugate. Let $\tau \in G$ be such that $\tau D_{\mathfrak{q}_1} \tau^{-1} = D_{\mathfrak{q}_2}$. We can construct the following diagram:

$$\begin{array}{ccc} D_{\mathfrak{q}_1} & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}_1}/\mathbb{F}_{\mathfrak{p}}) \\ \downarrow{\scriptstyle \tau \circ \cdot \circ \tau^{-1}} & & \downarrow{\scriptstyle id} \\ D_{\mathfrak{q}_2} & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}_2}/\mathbb{F}_{\mathfrak{p}}). \end{array}$$

The arrow on the right is an isomorphism as all residue class degrees are equal, hence $\mathbb{F}_{\mathfrak{q}_1} \simeq \mathbb{F}_{\mathfrak{q}_2}$. Moreover, the diagram commutes as the Galois group of the finite field extension is abelian. Hence we may conclude that $\tau(\mathfrak{q}_1, L/K)\tau^{-1} = (\mathfrak{q}_2, L/K)$. ❐

Proposition 7.2.15. Let $M/L/K$ be a tower of finite Galois extensions. Choose a prime $\mathfrak{p}$ of K, a prime $\mathfrak{q}$ dividing $\mathfrak{p}$, and a prime $\mathfrak{r}$ dividing $\mathfrak{q}$. Assume that $\mathfrak{r}$ is unramified over $\mathfrak{p}$. Then

$$(\mathfrak{r}, M/K)^{f(\mathfrak{q}/\mathfrak{p})} = (\mathfrak{r}, M/L). \qquad \triangleleft$$

Moreover, $(\mathfrak{r}, M/K)\big|_L = (\mathfrak{q}, L/K)$.

Proof. The Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{r}}/\mathbb{F}_{\mathfrak{p}})$ is given by $\alpha \mapsto \alpha^{\#\mathbb{F}_{\mathfrak{p}}}$, while for $\mathrm{Gal}(\mathbb{F}_{\mathfrak{r}}/\mathbb{F}_{\mathfrak{q}})$ we have $\alpha \mapsto \alpha^{\#\mathbb{F}_{\mathfrak{q}}}$. By definition, $[\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] = f(\mathfrak{q}/\mathfrak{p})$. The second part follows as the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{r}}/\mathbb{F}_{\mathfrak{p}})$ restricts to the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. ❐

7.3 ABELIAN EXTENSIONS

When considering abelian extensions of a global field, the engine of the decomposition and inertia groups runs a bit more smoothly. This happens because every subgroup of an abelian group is normal. As a result, the theorems of the previous section can be strengthened.

Suppose L/K is a finite abelian extension. Let $\mathfrak{p}$ be a prime ideal of K, with $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ the primes of L dividing $\mathfrak{p}$.

Lemma 7.3.1. The decomposition groups $D_{\mathfrak{q}_i}$ are all equal. ◁

Proof. We know that the decomposition groups are conjugate by Lemma 7.2.3. As the decomposition groups are normal subgroups, which means the are fixed under conjugation, they must all be equal. ❐

Hence we can write $D_{\mathfrak{p}} = D_{\mathfrak{q}_i}$ and we obtain an exact sequence

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

In abelian groups, all conjugacy classes consist of a single element. In particular, $(\mathfrak{p}, L/K)$ is just a single element, hence there exists an element, denoted $\mathrm{Frob}_{\mathfrak{p}}(L/K)$, that acts as the Frobenius element for all primes dividing $\mathfrak{p}$ at the same time.

7.3.1 FINITE ABELIAN EXTENSIONS

A final important method of approaching finite abelian extensions comes from the fundamental theorem of finite abelian groups:

Theorem 7.3.2 (FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS)**.** Let G be a finite abelian group. There exist finite cyclic groups $A_1, \ldots, A_n$ such that $G \cong \bigoplus_{i=1}^{n} A_i$. ◁

Proof. Theorem 6.9 of [Rot99]. ❐

Now suppose we have a finite abelian extension L/K with Galois group G and, using the aforementioned fundamental theorem, we can write $G \cong \bigoplus_{i=1}^{n} A_i$. For any $1 \leq i \leq n$, let $B_i = \bigoplus_{j \neq i} A_j$ be a subgroup of G. As G is abelian, B_i is a normal subgroup of G, hence L^{B_i} is a Galois subextension of L/K. Its Galois group is isomorphic to $G/B_i \cong A_i$, hence L^{B_i} is a finite cyclic extension of K.

Consider the composite $L^{B_1} \cdot \ldots \cdot L^{B_n}$. It is a Galois subextension of L/K, hence there is some (normal) subgroup H of G that has this composite as fixed field. As $L^{B_i} \subseteq L^{B_1} \cdot \ldots \cdot L^{B_n}$, we have $H \subseteq B_i$ for all i, hence

$$H \subseteq \bigcap_{i=1}^{n} B_i = \{e\}.$$

However, this implies $L^H = L$, thus $L^{B_1} \cdot \ldots \cdot L^{B_n} = L$. We summarise this in the following lemma:

Lemma 7.3.3. Let L/K be a finite abelian extension. There exist finite cyclic subextensions $L_1, \ldots, L_n$ such that $L_1 \cdot \ldots \cdot L_n = L$. ◁

Because all extensions we consider are algebraic, this extends to abelian extensions in general. Any abelian extensions is the composite of finite abelian extensions, and for each of these extensions we find the finite cyclic subextensions. As the composite of the (possibly infinitely many) finite cyclic extensions contains all the finite abelian extensions, it contains the original abelian extension as well. Hence we can restate the lemma, this time dropping the finiteness condition:

Lemma 7.3.4. Let L/K be an abelian extension. There exists an index set I and finite cyclic subextensions L_i for every $i \in I$ such that the composite of all L_i equals L. ◁

7.4 GLOBAL CLASS FIELD THEORY USING LOCAL CLASS FIELD THEORY

This approach to global class field theory essentially borrows all theorems from local class field theory; we stated the beautiful central theorem of local class field theory in Theorem 6.4.2. In order to do this, we need to associate local fields to a global field, which is done using *completions*, which we have defined before, see Definition 4.1.9.

7.4.1 COMPLETIONS

In this section we will create a connection between extensions of a global field and the extensions of a localisation of this field and relate the Galois groups of both extensions. In order to create localisations, we require absolute values, whose equivalence classes are called *primes*.

Definition 7.4.1 (PRIME)**.** Given a global field K, a prime of K is an equivalence class of nontrivial valuations on K. ◁

The primes of K can be split into three sets:

- the finite primes: these correspond one-to-one with nonzero prime ideals in $\mathcal{O}_K$;
- the real primes: these correspond one-to-one with real embeddings $K \hookrightarrow \mathbb{R}$;
- the complex primes: these correspond one-to-one with (conjugate) pairs of complex embeddings $K \hookrightarrow \mathbb{C}$.

The real and complex primes together are known as the *infinite primes* or *primes at infinity*. A global field always has primes at infinity, while a function field only has finite primes. Just like the prime ideals of $\mathcal{O}_K$ factor into prime ideals of $\mathcal{O}_L$ for an extension L/K, i. e. finite primes of K factor into finite primes of L, the real and complex primes of K factor into real and complex primes of L. A real prime of K is said to *split completely* in L/K if every prime of L lying over this prime is real. If this is not the case, we say that the prime of K *ramifies*.

Example. Consider the extension $\mathbb{Q}[i]/\mathbb{Q}$. $\mathbb{Q}$ only has one real prime, the one corresponding to the trivial embedding, and no complex primes. $\mathbb{Q}[i]$ has no real primes, and one complex prime, corresponding to the pair of complex embeddings given by the identity and complex conjugation. This prime lies above the real prime in $\mathbb{Q}$, so we see that the real prime of $\mathbb{Q}$ ramifies in $\mathbb{Q}[i]$.

Remark. Let K be a number field and let v be a prime of K. If v is a real prime, then K_v is isomorphic to $\mathbb{R}$. If v is a complex prime, then K_v is isomorphic to $\mathbb{C}$. Finally, if v is a finite prime, K_v is a local field.

Example. Suppose $K = \mathbb{Q}$ and let v_p be the prime associated to the prime ideal (p). Then $K_{v_p} = \mathbb{Q}_p$.

Let K be a global field along with a prime v. Suppose we have a Galois extension L/K and a completion K_v of K. In the extension L there are primes $w_1, \ldots, w_g$ lying above v. Choosing any w of these primes, we obtain a localisation L_w of L. Then L_w is an extension of K_v.

Theorem 7.4.2. Let L/K be a finite extension of global fields, $\mathfrak{p}$ a finite prime in K and $\mathfrak{q}$ a prime in L dividing $\mathfrak{p}$. The exact sequences in Proposition 6.2.3 and Definition 7.2.9 are isomorphic, i. e. there exist isomorphisms $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) \xrightarrow{\sim} D_\mathfrak{q}(L/K)$, $I \xrightarrow{\sim} I_q$, and $\mathrm{Gal}(k_L/k) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I & \longrightarrow & \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(k_{L_\mathfrak{q}}/k_{K_\mathfrak{p}}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I_\mathfrak{q}(L/K) & \longrightarrow & D_\mathfrak{q}(L/K) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) & \longrightarrow & 1 \end{array}$$

commutes. ◁

Proof. Propostition 9.6 of [NS99].

The intuitive proof is as follows: any element of $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ leaves K fixed, and as L/K is Galois, any element of $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ can be seen as an element of $\mathrm{Gal}(L/K)$. As any element of $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ must leave $\mathfrak{q}$ fixed, it lies in $D_\mathfrak{q}(L/K)$. Now that these sets are the same, I and $I_\mathfrak{q}(L/K)$ also consist of precisely the same elements by their explicit forms from Propostion 6.2.3 and Proposition 7.2.10. From the exact sequences we obtain the final isomorphism. ❐

Corollary 7.4.3. For a finite abelian extension L/K, the extension $L_\mathfrak{q}/K_\mathfrak{p}$ is abelian as well, as its Galois group is a subgroup of $\mathrm{Gal}(L/K)$. ◁

7.4.2 ADELES, IDELES AND THE IDELE CLASS GROUP

In the previous section we created a connection between the extensions of global fields and their completions, and we would like to combine this with the stellar result from local class field theory, Theorem 6.4.2. The first attempt would be as follows: does there exist a continuous homomorphism $\prod_{v \text{ place}} K_v^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that for all places v of K the following diagram commutes?

$$\begin{array}{ccc} K_v^\times & \longrightarrow & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ \prod_{v \text{ place}} K_v^\times & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array} \tag{5}$$

The answer, unfortunately, is no. An indication of why this might be the case is that while $K_v^\times$, $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ are all locally compact (the latter two spaces are even compact), while $\prod_{v \text{ place}} K_v^\times$ (abbreviated as $\prod K_v^\times$) is might not be, as an infinite product of locally compact spaces is in general not locally compact. Informally, the space $\prod K_v^\times$ can be thought of as being too large, see also page 11 of [Mil13].

With this in mind we define a subspace of $\prod K_v^\times$ called the *idele class group*. We also define an additive version known as the *adele ring*, which seems similar, but is significantly different as a topological space. One last remark before the definition: if v is not a finite place, then it corresponds to either a real embedding or a pair of complex embeddings, and K_v is isomorphic to $\mathbb{R}$ respectively $\mathbb{C}$. In this case we define $\mathcal{O}_v = K_v$.

Definition 7.4.4 (ADELES, IDELES). Let K be a global field. The adele ring $\mathbb{A}_K$ is defined as

$$\mathbb{A}_K = \prod_{v \text{ place}}{}'(K_v, \mathcal{O}_v) = \{(x_v)_v \in \prod K_v : x_v \in \mathcal{O}_v \text{ for all but finitely many } v\},$$

with addition and multiplication defined componentwise. The ideles $\mathbb{A}_K^*$ are defined as

$$\mathbb{A}_K^* = \prod_{v \text{ place}}{}'(K_v^\times, \mathcal{O}_v^*) = \{(x_v)_v \in \prod K_v^\times : x_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

This construction is an example of a *restricted product*, which was defined in Definition 2.3.1. ◁

Remark. The idele group is sometimes denoted by $\mathbb{I}_K$.

We will often not require the infinite places, and with that in mind we define the *finite* adeles and ideles:

Definition 7.4.5. Let K be a global field. The finite adele ring $\mathbb{A}_{K,f}$ is defined as

$$\begin{aligned}\mathbb{A}_{K,f} &= \prod_{\substack{\mathfrak{p} \\ \text{fin. prime}}}{}'(K_\mathfrak{p}, \mathcal{O}_\mathfrak{p}) \\ &= \{(x_\mathfrak{p})_\mathfrak{p} \in \prod K_\mathfrak{p} : x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} \text{ for all but finitely many prime ideals } \mathfrak{p}\}.\end{aligned}$$

and the finite ideles $\mathbb{A}_{K,f}^*$ as

$$\begin{aligned}\mathbb{A}_{K,f}^* &= \prod_{\substack{\mathfrak{p} \\ \text{fin. prime}}}{}'(K_\mathfrak{p}^\times, \mathcal{O}_\mathfrak{p}^*) \\ &= \{(x_\mathfrak{p})_\mathfrak{p} \in \prod K_\mathfrak{p}^\times : x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^* \text{ for all but finitely many prime ideals } \mathfrak{p}\}.\end{aligned}$$ ◁

Lemma 7.4.6. Both $\mathbb{A}_K$ and $\mathbb{A}_K^*$ are locally compact. ◁

Proof. As all K_v and $K_v^\times$ are locally compact, while all $\mathcal{O}_v$ and $\mathcal{O}_v^*$ are compact, both the adeles and ideles are locally compact by Proposition 2.3.3. ❐

Remark. The topology on $\mathbb{A}_K^*$ is finer than the subspace topology obtained from $\mathbb{A}_K^* \subseteq \mathbb{A}_K$. To illustrate this, enumerate the primes of K by $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ and let $a_1, a_2, \ldots$ be the sequence in $\mathbb{A}_K^*$ defined by $(a_i)_{\mathfrak{p}_i} = \pi_i$ and $(a_i)_\mathfrak{p} = 1$ for all other $\mathfrak{p}$.

In $\mathbb{A}_K^*$, the sequence $a_1, a_2, \ldots$ does not converge to 1, as 1 has the open neighbourhood $\prod_{\mathfrak{p} \text{ prime}} \widehat{\mathcal{O}}_K^*$ by Definition 2.3.1 of a restricted product.

In $\mathbb{A}_K$, a basis of open neighbourhoods is given by sets of the form

$$\prod_{i \in S}(1 + \pi_i^{n_i}\mathcal{O}_{\mathfrak{p}_i}) \times \prod_{i \notin S}(1 + \mathcal{O}_{\mathfrak{p}_i})$$

where $S \subseteq \mathbb{N}$ is finite and $n_i \in \mathbb{N}$. However, every a_i with $i > \max_{s \in S} s$ lies in this open set. As S is finite, this maximum is well-defined, and we see that the sequence converges to 1.

The credits for this example go to user29743 of StackExchange, see [Sta12].

We can generalise the proof that the above sequence converges in the topology of the adeles to the following lemma:

Lemma 7.4.7. Suppose for every prime $\mathfrak{p}$ of K we are given a sequence $x_{\mathfrak{p},i} \in \mathcal{O}_\mathfrak{p}$ that converges to an element $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$. Then $\prod x_{\mathfrak{p},i}$ converges to $\prod x_\mathfrak{p}$ in the adele topology. ◁

Proof. The proof is very similar to the argument given in the remark above: again enumerate the primes of K by $\mathfrak{p}_1, \mathfrak{p}_2, \dots$ and let $P_{\mathfrak{p}_i} : \mathbb{A}_K \to K_{\mathfrak{p}_i}$ be the projection map to the coordinate corresponding to $\mathfrak{p}_i$. A basis of open neighbourhoods of $\prod x_{\mathfrak{p}_i}$ is given by sets of the form:

$$\prod_{i \in S} (1 + \pi_i^{n_i} \mathcal{O}_{\mathfrak{p}_i}) \times \prod_{i \notin S} (x_v + \mathcal{O}_{\mathfrak{p}_i}) = \prod_{i \in S} (1 + \pi_i^{n_i} \mathcal{O}_{\mathfrak{p}_i}) \times \prod_{i \notin S} \mathcal{O}_{\mathfrak{p}_i}$$

where $S \subseteq \mathbb{N}$ is finite and $n_i \in \mathbb{N}$. Fix such a set S and an open U_S in the aforementioned basis. Let s be the maximal element in S. As $x_{\mathfrak{p}_i,1}, x_{\mathfrak{p}_i,2}, \dots$ converges to $x_{\mathfrak{p}_i}$ for all $i \in \mathbb{N}$, there exists an integer $a_{\mathfrak{p}_i}$ for every prime $\mathfrak{p}_i$ such that $x_{\mathfrak{p}_i,j} \in P_{\mathfrak{p}_i}(U_S)$ for all $j \geq a_{\mathfrak{p}_i}$, as $P_{\mathfrak{p}_i}(U_S)$ is an open neighbourhood of $x_{\mathfrak{p}_i}$. Let $a = \max_{i \leq s} a_{\mathfrak{p}_i}$. Then for all $i \in S$ and $j \geq a$, we have $x_{\mathfrak{p}_i,j} \in P_{\mathfrak{p}_i}(U_S)$, hence $\prod x_{\mathfrak{p}_i,j} \in U_S$ for all $j \geq a$, implying that $\prod x_{\mathfrak{p}_i,j}$ converges to $\prod x_{\mathfrak{p}_i}$. ❐

The idele class group is the substitute of $\prod K_v^\times$ in Diagram 5, as explained in the following theorem:

Theorem 7.4.8. There exists a continuous homomorphism $\mathrm{rec}_K : \mathbb{A}_K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ known as the *global Artin map* or *global reciprocity map* such that the following diagram commutes for all places v:

$$\begin{array}{ccc} K_v^\times & \longrightarrow & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^* & \xrightarrow{\mathrm{rec}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K). \end{array} \tag{6}$$

◁

We can embed $K^\times$ into $\mathbb{A}_K^*$ diagonally: every element of $\mathcal{O}$ except zero is divisible by finitely many primes, hence $K^\times = \mathrm{Frac}(\mathcal{O}) - \{0\}$ indeed lies in the restricted product.

Proposition 7.4.9. $K^\times$ lies in the kernel of rec_K. ◁

Proof. Theorem 5.3(a) of [Mil13]. ❐

This allows us to substitute $\mathbb{A}_K^*/K^\times$ for $\mathbb{A}_K^*$ in Diagram 6. This quotient is called the *idele class group* and often denoted C_K. This idele class group plays a role similar to $K_v^\times$ in local class field theory, as made precise by the following theorem:

Theorem 7.4.10. For any finite abelian extension L/K we have a norm map $N_{L/K} : C_L \to C_K$ induced from the norm map $\mathbb{A}_L^* \to \mathbb{A}_K^*$. The following diagram commutes:

$$\begin{array}{ccc} C_K & \xrightarrow{\mathrm{rec}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow \\ C_K/N_{L/K}(C_L) & \xrightarrow{\mathrm{rec}_{L/K}} & \mathrm{Gal}(L/K), \end{array}$$

where $\mathrm{rec}_{L/K}$ is an isomorphism such that $\mathrm{rec}_{L/K}(1, \dots, 1, \pi_v, 1, \dots) = (\mathfrak{p}_v, L/K)$ for every prime unramified in L/K. Moreover, all open subgroups of finite index of C_K are of the form $N_{L/K}(C_L)$ for some finite abelian extension L/K. ◁

Proof. Theorem 5.3(b) of [Mil13]. ❐

The image of the subgroup $\mathcal{O}_\mathfrak{p}^* \subset K_\mathfrak{p}^\times$ for $\mathfrak{p}$ a prime ideal in the bottom right of Diagram 6 is particularly interesting: one of the results of Theorem 6.4.2 was that for a finite abelian extension $L_\mathfrak{q}/K_\mathfrak{p}$, the reciprocity map induced a surjective map $\mathcal{O}_\mathfrak{p}^* \to I(L_\mathfrak{q}/K_\mathfrak{p})$. By Theorem 7.4.2 and because L/K is abelian, $I(L_\mathfrak{q}/K_\mathfrak{p})$ is mapped (isomorphically) to $I_\mathfrak{p}(L/K)$ under the map $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$, which is induced from $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Hence $\mathcal{O}_\mathfrak{p}^*$ is mapped surjectively to $I_\mathfrak{p}(L/K)$ for every finite abelian extension L/K. The image of $\mathcal{O}_\mathfrak{p}^*$ in the bottom right of Diagram 6 is denoted $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$, even though this is a slight abuse of notation. The following lemma summarises this:

Lemma 7.4.11. For every finite abelian extension L/K the image of $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ under $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ is the inertia subgroup $I_\mathfrak{p}(L/K)$. ◁

Part III

A DYNAMICAL SYSTEM AND ITS RELATION TO L-SERIES: AN APPLICATION OF CLASS FIELD THEORY

8

INTRODUCTION

In this final part we study an as of yet unpublished paper by Cornelissen, Li, and Marcolli, [CLM16]. It mainly deals with proving the equivalence of a number of statements regarding two global fields K and L that are sufficient for a field isomorphism $K \cong L$. In the first chapter, we construct a certain topological monoid X_K (and X_L) which contains sufficient information on the underlying field as part of a dynamical system $I_K \curvearrowright X_K$ to determine the isomorphism type. In the second section, we supply a partial proof of the equivalence of some properties of this dynamical system. In the second chapter, we provide a brief introduction to the Dirichlet L-series, which, combined with the maximal abelian Galois group, also contain sufficient information on the underlying field. We finish by showing how these statements lead to a field isomorphism.

There will be quite a lot of notation, hence we provide an overview of the notation used in the following chapters of objects that were defined previously:

Sign	Description
K (or L)	A global field
$\mathcal{O}_K$	The ring of integers (of K)
I_K	The integral ideals
$\mathcal{P}_K$	The prime ideals
$K_\mathfrak{p}$	The completion of K with respect to $\lvert\cdot\rvert_\mathfrak{p}$
G_K^{ab}	The Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$
$\mathbb{A}_K$	The adele ring, Definition 7.4.4
$\mathbb{A}_{K,f}$	The finite adele ring, Definition 7.4.5
$\mathbb{A}_K^*$	The ideles, or invertable adeles
$\mathbb{A}_{K,f}^*$	The finite ideles

9 A DYNAMICAL SYSTEM

The first section is devoted to creating a dynamical system $I_K \circlearrowright X_K$, i. e. a monoid action on X_K by the integral ideals I_K, where X_K is a topological monoid that contains within it both information on the maximal abelian Galois group and the (finite) adeles. The two important theorems are Theorem 9.1.2 and Theorem 9.1.5, which combined allow us to prove properties of X_K by considering the integral ideals only.

The second section uses these properties to prove that if for two number fields K and L the topological spaces X_K and X_L are homeomorphic and the actions $I_K \circlearrowright X_K$ and $I_L \circlearrowright X_L$ are equivariant under this homeomorphism, then K and L are isomorphic.

9.1 CONSTRUCTION OF THE DYNAMICAL SYSTEM

Let K be a global field. We use the following abbreviations:

- $\widehat{\mathcal{O}}_K$ for $\prod_{v \text{ finite place}} \mathcal{O}_K \subset \mathbb{A}_{K,f}$, the *finite integral adeles*;
- $\widehat{\mathcal{O}}_K^*$ for $\prod_{v \text{ finite place}} \mathcal{O}_K^* \subset \mathbb{A}_{K,f}^*$, the *finite integral ideles*.

From the viewpoint of $\widehat{\mathcal{O}}_K^*$ we have already seen the following maps:

$$\begin{array}{ccccccc} \widehat{\mathcal{O}}_K^* & \hookrightarrow & \mathbb{A}_{K,f}^* & \hookrightarrow & \mathbb{A}_K^* & \xrightarrow{\text{rec}_K} & G_K^{\text{ab}} \\ \downarrow & & & & & & \\ \widehat{\mathcal{O}}_K & & & & & & \end{array}$$

which gives us a group action $\widehat{\mathcal{O}}_K^* \circlearrowright (G_K^{\text{ab}} \times \widehat{\mathcal{O}}_K)$ given by $u \cdot (\sigma, x) = (\text{rec}_K(u)^{-1}\sigma, ux)$. We obtain a topological quotient space $X_K = (G_K^{\text{ab}} \times \widehat{\mathcal{O}}_K)/\widehat{\mathcal{O}}_K^*$. Note that all arrows in the above diagram are continuous: the inclusion of $\widehat{\mathcal{O}}_K^*$ into $\widehat{\mathcal{O}}_K$ is continuous as the topology on $\widehat{\mathcal{O}}_K^*$ is finer than the subspace topology obtained from $\widehat{\mathcal{O}}_K$.

Recall from Section 3.2.2 that the topological group G_K^{ab} is a profinite group, and it is isomorphic to $\varprojlim_{L/K \text{ finite, abelian}} \text{Gal}(L/K)$, thus compact and Hausdorff. The topological group $\widehat{\mathcal{O}}_K$ is compact and Hausdorff as well, as it is the product of the profinite groups $\mathcal{O}_{K_v} = \varprojlim_{n \in \mathbb{N}} \mathcal{O}_{K_v}/\pi_v^n \mathcal{O}_{K_v}$ as stated by Lemma 4.3.5. As a result, $G_K^{\text{ab}} \times \widehat{\mathcal{O}}_K$ is both Hausdorff and compact.

Theorem 9.1.1. The group action $\widehat{\mathcal{O}}_K^* \circlearrowright (G_K^{\text{ab}} \times \widehat{\mathcal{O}}_K)$ is continuous. ◂

Proof. The multiplication map $\widehat{\mathcal{O}}_K^* \times G_K^{\text{ab}} \to G_K^{\text{ab}}$ is given by $(u, \sigma) \mapsto \text{rec}_K(u)^{-1}\sigma$. Hence it factors as follows:

$$\widehat{\mathcal{O}}_K^* \times G_K^{\text{ab}} \longrightarrow G_K^{\text{ab}} \times G_K^{\text{ab}} \longrightarrow G_K^{\text{ab}} \times G_K^{\text{ab}} \longrightarrow G_K^{\text{ab}}$$

$$(u, \sigma) \longmapsto (\text{rec}_K(u), \sigma) \longmapsto (\text{rec}_K(u)^{-1}, \sigma) \longmapsto \text{rec}_K(u)^{-1}\sigma.$$

As the Artin reciprocity map is continuous by construction, the first map is continuous. As G_K^{ab} is a topological group, inversion respectively multiplication is continuous, thus the second respectively third map is continuous.

The topology on $\mathbb{A}_K^*$ is obtained by the inclusion of $\mathbb{A}_K^*$ into $\mathbb{A}_K \times \mathbb{A}_K$ via $u \mapsto (u, u^{-1})$, thus on $\widehat{\mathcal{O}}_K^*$ by embedding it into $\widehat{\mathcal{O}}_K \times \widehat{\mathcal{O}}_K$. The multiplication map $\widehat{\mathcal{O}}_K^* \times \widehat{\mathcal{O}}_K \to \widehat{\mathcal{O}}_K$ is therefore constructed with the following continuous maps:

$$\widehat{\mathcal{O}}_K^* \times \widehat{\mathcal{O}}_K \longrightarrow \widehat{\mathcal{O}}_K \times \widehat{\mathcal{O}}_K \times \widehat{\mathcal{O}}_K \longrightarrow \widehat{\mathcal{O}}_K \times \widehat{\mathcal{O}}_K \longrightarrow \widehat{\mathcal{O}}_K$$

$$(u, x) \longmapsto (u, u^{-1}, x) \longmapsto (u, x) \longmapsto ux.$$

Hence the multiplication map is continuous itself.

We finish the proof by combining these two results:

$$\widehat{\mathcal{O}}_K^* \times G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K \longrightarrow (\widehat{\mathcal{O}}_K^* \times G_K^{\mathrm{ab}}) \times (\widehat{\mathcal{O}}_K^* \times \widehat{\mathcal{O}}_K) \longrightarrow G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K$$

$$(u, \sigma, x) \longmapsto (u, \sigma, u, x) \longmapsto (\mathrm{rec}_K(u)^{-1}\sigma, ux).$$

The first map is an embedding, hence continuous. The second is the combination of the two continuous maps we mentioned before. Hence the group action $\widehat{\mathcal{O}}_K^* \circlearrowright (G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K)$ is continuous. ❐

Theorem 9.1.2. X_K is Hausdorff. ◅

Proof. Proposition 4.3.7 states that $\mathcal{O}_\mathfrak{p}^*$ is compact for any prime $\mathfrak{p}$ of K. Hence $\widehat{\mathcal{O}}_K^* = \prod_{\mathfrak{p} \text{ finite place}} \mathcal{O}_\mathfrak{p}^*$ is also compact by Theorem 2.1.9. Moreover, $G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K$ is Hausdorff. This means that the action $\widehat{\mathcal{O}}_K^* \circlearrowright (G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K)$ meets the requirements of Corollary 2.2.7, hence the quotient X_K is Hausdorff. ❐

Definition 9.1.3 (SPLIT)**.** An integral ideal of K has a unique factorisation into prime ideals of K. Hence, by fixing uniformisers $\pi_\mathfrak{p}$ for every completion at a finite prime $\mathfrak{p}$, we obtain a split $s_K : I_K \to \mathbb{A}_{K,f}^*$ that is a monoid homomorphism such that $s_K(\mathfrak{m}) = (x_\mathfrak{p})_\mathfrak{p}$, where

$$x_\mathfrak{p} = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid \mathfrak{m}; \\ \pi_\mathfrak{p}^a & \text{if } \mathfrak{p}^a \| \mathfrak{m}. \end{cases}$$ ◅

As we only consider integral ideals, a will always be non-negative, hence the image of s_K lies in $\widehat{\mathcal{O}}_K$. Hence the split provides monoid homomorphisms $I_K \to \mathbb{A}_{K,f}^*$ and $I_K \to \widehat{\mathcal{O}}_K$, resulting in a map $I_K \to X_K$, which does not depend on the choice of uniformiser in the definition of s_K as uniformisers differ only by a unit, and as a consequence we obtain an action $I_K \circlearrowright X_K$ given by

$$\mathfrak{m} \cdot [\sigma, x] = [\mathrm{rec}_K(s_K(\mathfrak{m}))^{-1}\sigma, s_K(\mathfrak{m})x].$$

As I_K is a monoid, $I_K \circlearrowright X_K$ is a dynamical system. We will not delve into dynamical systems theory, but we will borrow some terms such as *orbit-equivalence* and *conjugacy* (to be defined later) that allow for easier notation. We continue with a theorem that will be useful for proving properties of this dynamical system, for which we need a lemma first:

Lemma 9.1.4. Given a cofinite subset S of $\mathcal{P}_K$, let $\langle S\rangle^+$ be the submonoid of I_K generated by S. Then the group generated by $K^\times$ and $s_K(\langle S\rangle^+)$ is dense in $\mathbb{A}_K^*$. ◂

Proof. This is a consequence of strong approximation, Theorem 7.12 of [PRR93], which states that $K^\times$ is dense in a subset of $\mathbb{A}_K^*$ defined by

$$\mathbb{A}_{K,S}^* = \{\prod_{\mathfrak{v}} x_v : x_v = 1 \text{ for all } v \in S\}.$$

Hence the group generated by $K^\times$ and $s_K(\langle S\rangle^+)$ is dense in $\mathbb{A}_K^*$. ❐

Theorem 9.1.5. I_K is a dense subset of X_K. ◂

Proof. Enumerate the primes in $\mathcal{P}_K$ by $\mathfrak{p}_1, \mathfrak{p}_2, \dots$. We begin by showing that the set of equivalence classes of $G_K^{\mathrm{ab}} \times \bigcup_{\mathfrak{m}} s_K(\mathfrak{m}) \subseteq G_K^{\mathrm{ab}} \times \widehat{\mathcal{O}}_K$, denoted $\left[G_K^{\mathrm{ab}} \times \bigcup_{\mathfrak{m}} s_K(\mathfrak{m})\right]$, is dense in X_K. Take any element in X_K with standard representative (σ, x), i. e. for all $\mathfrak{p} \in \mathcal{P}_K$ we have either $x_\mathfrak{p} = \pi_\mathfrak{p}^{v_\mathfrak{p}}$ for some $v_\mathfrak{p} \in \mathbb{Z}_{\geq 0}$ or $x_\mathfrak{p} = 0$. Define

$$\mathfrak{m}_j = \mathfrak{p}_1^{w_{1,j}} \mathfrak{p}_2^{w_{2,j}} \dots \mathfrak{p}_j^{w_{j,j}},$$

where for $1 \leq i \leq j$ we have

$$w_{i,j} = \begin{cases} j & \text{if } x_{\mathfrak{p}_i} = 0; \\ v_{\mathfrak{p}_i} & \text{if } x_{\mathfrak{p}_i} = \pi_{\mathfrak{p}_i}^{v_{\mathfrak{p}_i}}. \end{cases}$$

For all j and $i \leq j$, we have that $|x_{\mathfrak{p}_i} - s_K(\mathfrak{m}_j)_{\mathfrak{p}_i}|_{\mathfrak{p}_i}$ is either zero or $(N(\mathfrak{p}_i))^{-j}$, where $N(\mathfrak{p}_i)$ denotes the norm of $\mathfrak{p}_i$, i. e. the size of the residue field of $\mathfrak{p}_i$. Using Lemma 7.4.7, this implies that $s_K(\mathfrak{m}_j)_{j\in\mathbb{N}}$ has limit x, hence $[\sigma, x]$ is the limit of $([\sigma, s_K(\mathfrak{m}_j)])_{j\in\mathbb{N}}$. We conclude that $\left[G_K^{\mathrm{ab}} \times \bigcup_{\mathfrak{m}} s_K(\mathfrak{m})\right]$ is dense in X_K.

We proceed by proving that $\left[G_K^{\mathrm{ab}} \times \bigcup_{\mathfrak{m}} s_K(\mathfrak{m})\right]$ is in the closure of I_K in X_K. Take any element $[\sigma, s_K(\mathfrak{m})]$ in $\left[G_K^{\mathrm{ab}} \times \bigcup_{\mathfrak{m}} s_K(\mathfrak{m})\right]$. Define $\mathcal{P}(\mathfrak{m}) = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \mid \mathfrak{m}\}$ and $T = \mathcal{P}_K - \mathcal{P}(\mathfrak{m})$. Enumerate the primes in T by $\mathfrak{q}_1, \mathfrak{q}_2, \dots$ and let $T_i = T - \{\mathfrak{q}_1, \dots, \mathfrak{q}_i\}$. By Lemma 9.1.4, $\mathrm{rec}_K(s_K(\langle T_i\rangle^+))$ is dense in G_K^{ab}. Hence for every i there exists a sequence $\mathrm{rec}_K(s_K(\mathfrak{n}_{i,1})), \mathrm{rec}_K(s_K(\mathfrak{n}_{i,2})), \dots$ in $\mathrm{rec}_K(s_K(\langle T_i\rangle^+))$ converging to $\tau = \sigma^{-1}\mathrm{rec}_K(s_K(\mathfrak{m}))$.

By Theorem 7.1.2, K has countably many finite extensions, hence σ has a countable basis of open neighbourhoods, as a basis is given by open neighbourhoods of the form $\sigma\mathrm{Gal}(K^{\mathrm{ab}}/L)$, where L/K is a finite Galois extension.

We can therefore choose $U_1, U_2, \dots$ to be a countable basis of open neighbourhoods of σ such that $U_i \supset U_{i+1}$ for all $i \in \mathbb{N}$. For example, this can be done by enumerating the finite extensions of K by $L_1, L_2, \dots$ and letting $U_i = \bigcap_{1\leq j\leq i} \sigma\mathrm{Gal}(K^{\mathrm{ab}}/L_j)$, which is a finite union of opens. The U_i form a basis as for every open in the old basis $\sigma\mathrm{Gal}(K^{\mathrm{ab}}/L_j)$ we have $U_j \subseteq \sigma\mathrm{Gal}(K^{\mathrm{ab}}/L_j)$.

As the sequence $\mathrm{rec}_K(s_K(\mathfrak{n}_{i,1})), \mathrm{rec}_K(s_K(\mathfrak{n}_{i,2})), \dots$ converges to τ, there exists some $j_i \in \mathbb{N}$ such that $\mathrm{rec}_K(s_K(\mathfrak{n}_{i,j_i})) \in U_i$. By finding a j_i for each $i \in \mathbb{N}$, we obtain a sequence $\mathrm{rec}_K(s_K(\mathfrak{n}_{1,j_1})), \mathrm{rec}_K(s_K(\mathfrak{n}_{2,j_2})), \dots$ that converges to τ. Moreover, we have $s_K(\mathfrak{n}_{i,j_i})_{\mathfrak{p}_k} = 1$ for $1 \leq k \leq i$. Hence in the adele topology, $s_K(\mathfrak{n}_{i,j_i})$ converges to $1 = (1, 1, \dots)$ by Lemma 7.4.7. It follows that

$$[\mathrm{rec}_K(s_K(\mathfrak{n}_{i,j_i}))^{-1}, s_K(\mathfrak{n}_{i,j_i})] \to [\tau, 1]$$

as $i \to \infty$. Because rec_K and s_K are multiplicative, we find

$$[\mathrm{rec}_K(s_K(\mathfrak{n}_{i,j_i} \cdot \mathfrak{m}))^{-1}, s_K(\mathfrak{n}_{i,j_i} \cdot \mathfrak{m})] \to [\tau \cdot \mathrm{rec}_K(s_K(\mathfrak{m}))^{-1}, s_K(\mathfrak{m})] = [\sigma, s_K(\mathfrak{m})].$$

We conclude that I_K is dense in X_K. ❐

Remark. The sequence $s_K(\mathfrak{n}_{i,j_i})$ does not converge to $(1, 1, \dots)$ in the idele topology. This would be absurd as the reciprocity map $\mathrm{rec}_K : \mathbb{A}_K^* \to G_K^{\mathrm{ab}}$ is continuous, which would imply that

$$e = \mathrm{rec}_K(1) = \mathrm{rec}_K\left(\lim_{i\to\infty} s_K(\mathfrak{n}_{i,j_i})\right) = \lim_{i\to\infty} \mathrm{rec}_K(s_K(\mathfrak{n}_{i,j_i})) = \tau,$$

which is an immediate contradiction as $\tau = \sigma^{-1}\mathrm{rec}_K(s_K(\mathfrak{m}))$.

The combination of Theorem 9.1.2 and Theorem 9.1.5 is intuitively quite strong, as it is difficult for a set to be dense in a Hausdorff space, as every two points are separated by open sets. Formally, this combination allows properties of continuous maps on X_K to be proven only on I_K, which we will use extensively in the next section, where we prove some equivalent properties of a pair of dynamical systems $I_K \circlearrowright X_K$ and $I_L \circlearrowright X_L$.

9.2 EQUIVALENCES OF THE DYNAMICAL SYSTEM

The main focus of this section is (partially) proving Theorem 9.2.1, which provides some insight into the structure of X_K and helps proving the central property (property (iii) of Theorem 9.2.1), namely that we have an isomorphism of topological monoids $X_K \xrightarrow{\sim} X_L$ which restricts to a (norm-preserving) monoid isomorphism $I_K \xrightarrow{\sim} I_L$. In the next chapter, this will be proven equivalent to the existence of a isomorphism of topological groups $G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$ that respects the L-series (which will be defined later).

Theorem 9.2.1. Let K and L be two global fields. The following are equivalent:

(i) $I_K \circlearrowright X_K$ and $I_L \circlearrowright X_L$ are orbit-equivalent and norm-preserving, i. e. there exists a homeomorphism $\Phi : X_L \xrightarrow{\sim} X_K$ with $\Phi(I_K \cdot x) = I_L \cdot \Phi(x)$ for all $x \in X_K$. In addition, for every $\mathfrak{m} \in I_K$ and $x \in X_K$ there exists an $\mathfrak{n} \in I_L$ with $N(\mathfrak{m}) = N(\mathfrak{n})$ such that $\Phi(\mathfrak{m} \cdot x) = \mathfrak{n} \cdot \Phi(x)$.

(ii) $I_K \circlearrowright X_K$ and $I_L \circlearrowright X_L$ are conjugate and norm-preserving, i. e. there exist a homeomorphism $\Phi : X_L \xrightarrow{\sim} X_K$ and a norm-preserving monoid isomorphism $\phi : I_K \xrightarrow{\sim} I_L$ such that $\Phi(\mathfrak{m} \cdot x) = \phi(\mathfrak{m}) \cdot \Phi(x)$ for all $\mathfrak{m} \in I_K$ and $x \in X_K$.

(iii) There exists an isomorphism of topological monoids $\Phi : X_K \xrightarrow{\sim} X_L$ which restricts to a norm-preserving isomorphism $I_K \xrightarrow{\sim} I_L$. ◁

The implications (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) are somewhat straightforward.

Assume (iii). Then $\Phi(\mathfrak{m} \cdot x) = \Phi(\mathfrak{m}) \cdot \Phi(x)$ for all $\mathfrak{m} \in I_K$ and $x \in X_K$, thus we can take $\phi = \Phi\big|_{I_K}$, which shows (ii).

Assume (ii). Because $\phi(I_K) = I_L$ and ϕ is norm-preserving, we can choose $\mathfrak{n} = \phi(\mathfrak{m})$, hence (i) holds.

The other implications we will not prove completely, they are available in [CLM16]. However, we will address the general idea of the proofs, starting with (i) $\Longrightarrow$ (ii).

The start of the proof of this implication is the following proposition.

Proposition 9.2.2. Suppose (i) holds. Then $\Phi(1)$ is invertible in X_L. ◁

Proof. Assume that $\Phi(1) = [\tau, y]$ is not invertible. As G_K^{ab} is a group and the invertible elements in $\mathcal{O}_\mathfrak{p}$ are precisely those with valuation zero, there must be some prime $\mathfrak{q}$ of L such that $v_\mathfrak{q}(y_\mathfrak{q}) > 0$. Thus $\Phi(I_K \cdot 1) = I_L \cdot \Phi(1)$ is contained in the equivalence classes of $G_L^{\mathrm{ab}} \times \prod_{\mathfrak{q}' \neq \mathfrak{q}} \mathcal{O}_{\mathfrak{q}'} \times \pi\mathcal{O}_\mathfrak{q}$, which is closed in X_L as $G_K^{\mathrm{ab}} \times \prod_{\mathfrak{q}' \neq \mathfrak{q}} \mathcal{O}_{\mathfrak{q}'} \times \pi\mathcal{O}_\mathfrak{q}$ is closed in $G_L^{\mathrm{ab}} \times \widehat{\mathcal{O}}_L$ (see Corollary 4.3.2) and stable under the action of $\widehat{\mathcal{O}}_L^*$. However, as Φ is an isomorphism and I_K is dense in X_K (as we have seen in Theorem 9.1.5), we find that $\Phi(I_K \cdot 1) = I_L \cdot \Phi(1)$ is dense in X_L; a contradiction. Thus $\Phi(1)$ must be invertible. ❐

Corollary 9.2.3. For every $\mathfrak{m} \in I_K$ there exists a unique $\mathfrak{n} \in I_L$ such that $\Phi(\mathfrak{m} \cdot 1) = \mathfrak{n} \cdot \Phi(1)$. ◁

Proof. The existence of such an $\mathfrak{n}$ is guaranteed by the orbit-equivalence. If there are two such $\mathfrak{n}$, say $\mathfrak{n}_1$ and $\mathfrak{n}_2$, then $\mathfrak{n}_1 \cdot \Phi(1) = \mathfrak{n}_2 \cdot \Phi(1)$. As a result,

$$\mathfrak{n}_1 = \mathfrak{n}_1 \cdot 1_L = \mathfrak{n}_1 \cdot \Phi(1) \cdot \Phi(1)^{-1} = \mathfrak{n}_2 \cdot \Phi(1) \cdot \Phi(1)^{-1} = \mathfrak{n}_2 \cdot 1_L = \mathfrak{n}_2. \qquad ❐$$

This allows for the definition of a map $\phi : I_K \to I_L$, where $\Phi(\mathfrak{m} \cdot 1) = \phi(\mathfrak{m}) \cdot \Phi(1)$. As Φ is a homeomorphism, we obtain a full inverse of ϕ by considering Φ^{-1}, hence ϕ is a bijection.

The largest part of the remainder of the proof is to show that ϕ is a monoid isomorphism, which can be found in the proof of Proposition 5.1 of [CLM16]. As a result, we obtain for any $\mathfrak{m}, \mathfrak{n} \in I_K$ that

$$\Phi(\mathfrak{m} \cdot \mathfrak{n}) = \phi(\mathfrak{m} \cdot \mathfrak{n}) \cdot \Phi(1) = \phi(\mathfrak{m}) \cdot \phi(\mathfrak{n}) \cdot \Phi(1) = \phi(\mathfrak{m}) \cdot \Phi(\mathfrak{n}).$$

Recall from Theorem 9.1.5 that I_K is dense in X_K. Let $x \in X_K$ and let $\mathfrak{n}_1, \mathfrak{n}_2, \ldots$ be a sequence of ideals in I_K with limit x in X_K. Then $\mathfrak{m} \cdot \mathfrak{n}_i \to \mathfrak{m} \cdot x$. As Φ is a homeomorphism, it is continuous, thus sequentially continuous, from which it follows that $\Phi(\mathfrak{n}_i) \to \Phi(x)$ and $\Phi(\mathfrak{m} \cdot \mathfrak{n}_i) \to \Phi(\mathfrak{m} \cdot x)$. For any $i \in \mathbb{N}$ we have $\Phi(\mathfrak{m} \cdot \mathfrak{n}_i) = \phi(\mathfrak{m}) \cdot \Phi(\mathfrak{n}_i)$. The left hand side has limit $\Phi(\mathfrak{m} \cdot x)$ while the right hand side has limit $\phi(\mathfrak{m}) \cdot \Phi(x)$. As X_K is Hausdorff (Theorem 9.1.2), limits are unique, thus $\Phi(\mathfrak{m} \cdot x) = \phi(\mathfrak{m}) \cdot \Phi(x)$ for all $\mathfrak{m} \in I_K$ and $x \in X_K$, which proves (ii).

The implication (ii) $\Longrightarrow$ (iii) now follows quite easily. Let $\Psi : X_K \to X_L$ be the map given by $x \mapsto \Phi(x) \cdot \Phi(1)^{-1}$. As X_K is a topological monoid and Φ is a homeomorphism, Ψ is a homeomorphism as well. Furthermore, for any $\mathfrak{m}, \mathfrak{n} \in I_K$ we have

$$\begin{aligned}
\Psi(\mathfrak{m} \cdot \mathfrak{n}) &= \Phi(\mathfrak{m} \cdot \mathfrak{n}) \cdot \Phi(1)^{-1} \\
&= \phi(\mathfrak{m}) \cdot \phi(\mathfrak{n}) \cdot \Phi(1) \cdot \Phi(1)^{-1} \\
&= (\phi(\mathfrak{m}) \cdot \Phi(1) \cdot \Phi(1)^{-1}) \cdot (\phi(\mathfrak{n}) \cdot \Phi(1) \cdot \Phi(1)^{-1}) \\
&= \Psi(\mathfrak{m}) \cdot \Psi(\mathfrak{n}).
\end{aligned}$$

Again, I_K is dense in X_K, so using the same reasoning as before (where we use continuity of Ψ and the fact that X_K is Hausdorff), we find that $\Psi(x \cdot y) = \Psi(x) \cdot \Psi(y)$ for all $x, y \in X_K$. This means that Ψ is an isomorphism of topological monoids. Lastly,

$$\Psi(\mathfrak{m}) = \phi(\mathfrak{m}) \cdot \Phi(1) \cdot \Phi(1)^{-1} = \phi(\mathfrak{m}),$$

hence Ψ restricts to an isomorphism $I_K \xrightarrow{\sim} I_L$. This completes the proofs of the equivalences, as well as this chapter. We continue with Dirichlet L-series.

10 A RELATION WITH DIRICHLET L-SERIES

In a sense, L-series are a generalisation of the zeta function ζ_K associated to a global field, which is defined by

$$\zeta_K(s) = \sum_{\mathfrak{m} \in I_K} N(\mathfrak{m})^{-s},$$

where $N(\mathfrak{m})$ is the norm of $\mathfrak{m}$, i. e. the size of the residue field.

Informally, L-series are like the zeta function, but with a twist χ, called a character. L-series are of the form

$$L(\chi, s) = \sum_{\mathfrak{m} \in I_K} \chi(\mathfrak{m}) N(\mathfrak{m})^{-s}.$$

Just like the zeta function, L-series harbour within them information of the underlying field, but it is somewhat convoluted to extract this information. In the second section of this chapter, we will use these L-series to define a norm-preserving bijection between the prime ideals $\mathcal{P}_K$ of K and $\mathcal{P}_L$ of L.

A final warning before we begin: the following sections will use some notation for objects associated to either K or L that will not have the name of the global field in their notation. For example, we use $L(\chi, s)$ and not $L_K(\chi, s)$ to denote a Dirichlet L-series of K. We do make sure that the correct underlying field can be derived from the other objects, which is χ in the case of the given example.

10.1 CHARACTERS AND THEIR L-SERIES

In this section, we state and prove many propositions that connect characters and L-series with the prime ideals of the underlying field. The first section deals with the definition of objects associated to characters except for the L-series, which we define in Section 10.1.3. The middle section covers two methods of constructing characters, which will be essential for the proofs in Section 10.3.3.

10.1.1 DEFINITION OF CHARACTERS AND THEIR ASSOCIATED OBJECTS

Definition 10.1.1 (CHARACTER)**.** A character χ on G_K^{ab} is a multiplicative homomorphism $G_K^{\mathrm{ab}} \to \mathbb{C}^\times$ that is continuous when $\mathbb{C}^\times$ is equipped with the discrete topology. ◂

Example. One character that always exists is the *trivial character* defined by $\chi(\sigma) = 1$ for all $\sigma \in G_K^{\mathrm{ab}}$.

We can multiply characters χ_1, χ_2 by $(\chi_1\chi_2)(\sigma) = \chi_1(\sigma)\chi_2(\sigma)$. Any character χ has an inverse character χ^{-1} given by $\chi^{-1}(\sigma) = 1/\chi(\sigma)$. As the trivial character functions as the identity for this multiplication, we obtain a *character group*, often denoted $\widehat{G}_K^{\mathrm{ab}}$.

If we have an homomorphism $\phi : G_L^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$, any character χ on G_K^{ab} can be used to create a character $\chi \circ \phi$ on G_L^{ab}. In the following sections, we will encounter an isomorphism $\psi : G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$ where we will denote the corresponding isomorphism $\widehat{\psi} : \widehat{G}_K^{\mathrm{ab}} \to \widehat{G}_L^{\mathrm{ab}}$ given by $\widehat{\psi}(\chi) = \chi \circ \psi^{-1}$.

Definition 10.1.2 (KERNEL OF A CHARACTER)**.** For any character $\chi \in \widehat{G}_K^{\mathrm{ab}}$, define the *kernel* of χ by

$$\ker(\chi) = \{\sigma \in G_K^{\mathrm{ab}} : \chi(\sigma) = 1\}.$$

As χ is multiplicative, it is a subgroup of G_K^{ab}. ◁

The kernels of characters χ and $\widehat{\psi}(\chi)$ are closely related:

Proposition 10.1.3. Let $\chi \in \widehat{G}_K^{\mathrm{ab}}$ and $\psi : G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$ an isomorphism. Then $\ker(\widehat{\psi}(\chi)) = \psi(\ker(\chi))$. ◁

Proof. Let $\sigma \in \ker(\chi)$ and let $\tau = \psi(\sigma) \in \psi(\ker(\chi))$. Then $\widehat{\psi}(\chi)(\tau) = \chi(\psi^{-1}(\psi(\sigma))) = \chi(\sigma) = 1$, thus $\tau \in \ker(\widehat{\psi}(\chi))$.
Conversely, let $\tau \in \ker(\widehat{\psi}(\chi))$ and let $\sigma = \psi^{-1}(\tau)$. Then $\chi(\sigma) = \chi(\psi^{-1}(\tau)) = \widehat{\psi}(\tau) = 1$, thus $\sigma \in \ker(\chi)$, implying $\tau \in \psi(\ker(\chi))$. This proves the equality. ❐

As $\ker(\chi) = \chi^{-1}(1)$, it is open and closed in G_K^{ab}, thus by Theorem 3.2.6 we can associate the kernel to a finite extension of K, the fixed field of K^{ab} under $\ker(\chi)$, which we will denote by K_χ. It is a Galois extension as G_K^{ab} is abelian, hence $\ker(\chi)$ is a normal subgroup and K_χ/K is Galois. K_χ is called the *fixed field* of χ.

Because of the topology on G_K^{ab}, we obtain a simple, but interesting result:

Lemma 10.1.4. For any character $\chi \in \widehat{G}_K^{\mathrm{ab}}$ there exists some $n \in \mathbb{N}$ such that χ^n is the trivial character, i. e. $\chi(\sigma)^n = \chi(\sigma^n) = 1$ for all $\sigma \in G_K^{\mathrm{ab}}$. ◁

Proof. Let $n = \#\mathrm{Gal}(K_\chi/K)$. For any $\sigma \in G_K^{\mathrm{ab}}$ we have that $\left(\sigma|_{K_\chi}\right)^n = e_{K_\chi}$ by theory on finite groups. Therefore $\sigma^n \in \mathrm{Gal}(K^{\mathrm{ab}}/K_\chi)$, hence $\chi(\sigma)^n = 1$ for all $\sigma \in G_K^{\mathrm{ab}}$. ❐

Hence, for a character χ, we have that $\chi(\sigma)$ is an n^{th} root of unity for all $\sigma \in G_K^{\mathrm{ab}}$. This implies that there is a $d \mid n$ such that the image of σ is the group of d^{th} roots of unity. In particular, it is cyclic. As

$$\mathrm{im}(\chi) \cong {}^{G_K^{\mathrm{ab}}}\!/_{\ker(\chi)} \cong \mathrm{Gal}(K_\chi/K),$$

we find that K_χ/K is a cyclic extension.

Recall the definition of $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ from Lemma 7.4.11. We use this to define the ramifying primes of a character:

Definition 10.1.5 (RAMIFICATION OF A CHARACTER)**.** Write

$$U(\chi) := \left\{\mathfrak{p} \in \mathcal{P}_K : \chi|_{\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)} = 1\right\},$$

the set of primes where χ is *unramified*. We say that χ ramifies at all other primes. ◁

A justification for the term *ramification* will be given in Proposition 10.1.7. For any prime $\mathfrak{p}$ in $U(\chi)$, the value $\chi(\mathfrak{p}) := \chi(\mathrm{rec}_K(s_K(\mathfrak{p})))$ is well-defined, as the uniformiser $\pi_\mathfrak{p}$ is unique up to multiplication with $\mathcal{O}_\mathfrak{p}^*$. This allows for the definition of a homomorphism $\chi : \langle U(\chi)\rangle \to \mathbb{C}^\times$ where $\chi(\mathfrak{m}) := \chi(\mathrm{rec}_K(s_K(\mathfrak{m})))$. For the sake of completeness, we set $\chi(\mathfrak{m}) = 0$ for all $\mathfrak{m} \in I_K - \langle U(\chi)\rangle$.

10.1.2 THE CONSTRUCTION OF CHARACTERS

We consider two ways of creating characters of G_K^{ab}: one using finite extensions, and one using the *Grunwald-Wang Theorem*.

Suppose we have a character $\chi \in \widehat{G}_K^{\mathrm{ab}}$. By Lemma 10.1.4, it is of finite order, say order n. Let K_χ be the fixed field of χ. We have $\mathrm{im}(\chi) \cong \mathrm{Gal}(K_\chi/K)$, hence χ is completely determined by its value on $\mathrm{Gal}(K_\chi/K)$.
Conversely, if we have some finite cyclic abelian extension L/K of degree n with generator σ_L, then we can create an injective character $\chi_{L/K} : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ via $\chi_{L/K}(\sigma_L) = \zeta_n$ (it is now uniquely determined as $\chi_{L/K}$ is multiplicative). We can extend this to a character on G_K^{ab} using the projection map $\pi_L : G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$, i. e. $\chi(\sigma) = \chi_{L/K}(\pi_L(\sigma))$. As $\ker(\chi_{L/K}) = \{e\}$, we have $\ker(\chi) = \pi_L^{-1}(\{e\}) = \mathrm{Gal}(K^{\mathrm{ab}}/L)$ and therefore $K_\chi = L$. Thus, for any finite cyclic abelian extension, we can find a character that has this extension as fixed field. Moreover, this character is uniquely determined by the values on the Galois group of the fixed field. We state this in a lemma.

Lemma 10.1.6. Let L/K be a finite cyclic abelian extension and $\pi_L : G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ the projection map. Then for every injective character $\overline{\chi}$ on $\mathrm{Gal}(L/K)$ there exists a unique character $\chi \in \widehat{G}_K^{\mathrm{ab}}$ such that $K_\chi = L$ and $\chi = \overline{\chi} \circ \pi_L$. ◂

We consider two applications of the construction of characters using this lemma. The first justifies the name *unramified* primes for the primes in $U(\chi)$, while the second shows the importance of $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$.

Proposition 10.1.7. Let $\chi \in \widehat{G}_K^{\mathrm{ab}}$. The primes unramified in K_χ are exactly the primes in $U(\chi)$. ◂

Proof. The Galois group of $\mathrm{Gal}(K_\chi/K)$ is cyclic and finite, say of order n. Write $\overline{\chi}$ for the (injective) character on $\mathrm{Gal}(K_\chi/K)$. Let σ_L be a generator of $\mathrm{Gal}(K_\chi/K))$. We have $\overline{\chi} = \zeta_n$.

Fix a prime $\mathfrak{p} \in K$. The inertia group $I_\mathfrak{p}(K_\chi/K)$ is a subgroup of the Galois group, hence generated by σ_χ^i for some i. $\overline{\chi}$ maps $I_\mathfrak{p}(K_\chi/K)$ to the group generated by ζ_n^i.

Under the projection map $\pi : G_K^{\mathrm{ab}} \to \mathrm{Gal}(K_\chi/K)$, the set $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ is mapped surjectively to $I_\mathfrak{p}(K_\chi/K)$ (see Lemma 7.4.11). As a result, we have

$$\chi(\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)) = \overline{\chi}(I_\mathfrak{p}(K_\chi/K)) = \langle \zeta_n^i \rangle.$$

We obtain

$$\chi(\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)) = \{1\} \iff i = n \iff I_\mathfrak{p}(K_\chi/K) = \langle \sigma_\chi^n \rangle = \{e\}.$$

As the first statement is equivalent to $\mathfrak{p} \in U(\chi)$ and the last statement is equivalent to $\mathfrak{p}$ unramified in K_χ/K, we find $\mathfrak{p} \in U(\chi) \iff \mathfrak{p}$ unramified in K_χ/K. ❐

Lemma 10.1.8. For any prime $\mathfrak{p}$ of K we have $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) = \bigcap_{\chi:\, \mathfrak{p} \in U(\chi)} \ker(\chi)$. ◂

Proof. For any character $\chi \in \widehat{G}_K^{\mathrm{ab}}$ with $\mathfrak{p} \in U(\chi)$, we have by definition $\chi\big|_{\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)} = 1$, thus $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) \subseteq \ker(\chi)$.

We have seen in Proposition 4.3.7 that $\mathcal{O}_\mathfrak{p}^*$ is compact. Moreover, G_K^{ab} is a Hausdorff space by Proposition 3.2.5 and rec_K is continuous by Theorem 7.4.8 (as is the inclusion $\mathcal{O}_\mathfrak{p}^* \subseteq \mathbb{A}_K^*$), hence by Proposition 2.1.11 $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ is compact and by Proposition 2.1.10

is it closed.

Using the Galois correspondence of Theorem 3.2.6 and using the fact that all subgroups of abelian groups are normal, we find that $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ corresponds to an abelian subextension of K^{ab}/K, which we will denote by $K^\mathfrak{p}/K$. Let $K^{\mathrm{ur}(\mathfrak{p})}$ be the maximal abelian extension unramified at $\mathfrak{p}$. We claim that $K^\mathfrak{p} \subseteq K^{\mathrm{ur}(\mathfrak{p})}$. Suppose this does not hold, i.e. $\mathfrak{p}$ ramifies in $K^\mathfrak{p}$. Lemma 7.4.11 states that the image of $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ in $\mathrm{Gal}(K^\mathfrak{p}/K)$ is exactly $I_\mathfrak{p}(K^\mathfrak{p}/K)$. However, as $\mathfrak{p}$ ramifies in $K^\mathfrak{p}$, $I_\mathfrak{p}(K^\mathfrak{p}/K)$ is not trivial. This implies that $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ does not leave $K^\mathfrak{p}$ fixed, which contradicts the fact that $K^\mathfrak{p}$ is the fixed field of $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$. We conclude that $K^\mathfrak{p} \subseteq K^{\mathrm{ur}(\mathfrak{p})}$.

By Lemma 7.3.4 there exists an index set I and finite cyclic extensions K_i/K for every $i \in I$ such that the composite of the K_i equals $K^{\mathrm{ur}(\mathfrak{p})}$. Using Lemma 10.1.6, we find characters χ_i for all $i \in I$ such that $\ker(\chi_i)$ has fixed field K_i. Moreover, $\ker(\chi_i) = \chi_i^{-1}(1)$ is closed as χ_i is continuous, hence $\cap_{i\in I} \ker(\chi_i)$ is a closed subgroup of G_K^{ab}. Let K_I be the abelian extension associated to $\bigcap_{i\in I} \ker(\chi_i)$. By Proposition 3.2.7, K_I contains the composite of all K_i, which is $K^{\mathrm{ur}(\mathfrak{p})}$. It follows that $K^{\mathrm{ur}(\mathfrak{p})} \subseteq K_I$.

Moreover, every K_i is a subextension of $K^{\mathrm{ur}(\mathfrak{p})}/K$, thus $\mathfrak{p}$ is unramified in K_i, which combined with Proposition 10.1.7 implies that $\mathfrak{p} \in U(\chi_i)$. As a result, $\bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi) \subseteq \bigcap_{i\in I} \ker(\chi_i)$. We know that $\ker(\chi)$ is closed for any $\chi \in \widehat{G}_K^{\mathrm{ab}}$, $\bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi)$ is a closed normal subgroup of G_K^{ab}, hence corresponds to some abelian extension which we will denote by $K^{U(\mathfrak{p})}$. As $\bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi) \subseteq \bigcap_{i\in I} \ker(\chi_i)$, we obtain that $K_I \subseteq K^{U(\mathfrak{p})}$.

Lastly, we have seen that $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) \subseteq \bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi)$, thus $K^{U(\mathfrak{p})} \subseteq K^\mathfrak{p}$.

We conclude that $K^\mathfrak{p} \subseteq K^{\mathrm{ur}(\mathfrak{p})} \subseteq K_I \subseteq K^{U(\mathfrak{p})} \subseteq K^\mathfrak{p}$, hence we have equality everywhere. The corresponding closed normal subgroups of G_K^{ab} are therefore all equal as well, and we conclude

$$\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}(\mathfrak{p})}) = \bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi). \qquad \square$$

The second method of character creation is a reformulation of a part of the Grunwald-Wang Theorem.

Theorem 10.1.9 (Grunwald-Wang, adapted)**.** Let S be a finite set of primes of K. For any $\mathfrak{p} \in S$, let $a_\mathfrak{p}$ be either zero or a root of unity. Then there exists a character $\chi \in \widehat{G}_K^{\mathrm{ab}}$ such that $\chi(\mathfrak{p}) = a_\mathfrak{p}$ for all $\mathfrak{p} \in S$. ◂

Proof. This is discussed between Theorem 4 and Theorem 5 in X.2 of [AT08], page 79–80. □

This is all we need to know about characters for the extent of this thesis. We continue with L-series.

10.1.3 DEFINITION AND PROPERTIES OF L-SERIES

Definition 10.1.10 (L-SERIES)**.** For a character $\chi \in \widehat{G}_K^{\mathrm{ab}}$, the associated L-series $L(\chi, s)$ is given by

$$L(\chi, s) = \prod_{\mathfrak{p} \in \mathcal{P}_K} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p} \in U(\chi)} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}},$$

where N is the norm function. It converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. ◁

If we expand this product, we obtain that

$$L(\chi, s) = \sum_{\mathfrak{m} \in \langle U(\chi) \rangle} \chi(\mathfrak{m}) N(\mathfrak{m})^{-s},$$

which uses the same method as proving that the Riemann zeta function is (formally) equal to the Euler product.

The remainder of chapter will be devoted entirely to partially proving the following theorem:

Theorem 10.1.11. Let K and L be two global fields. The following are equivalent:

(i) There exists an isomorphism of topological groups $\Phi : X_K \xrightarrow{\sim} X_L$ which restricts to a norm-preserving isomorphism $I_K \xrightarrow{\sim} I_L$.

(ii) There exists a norm-preserving monoid isomorphism $\phi : I_K \xrightarrow{\sim} I_L$, an isomorphism of topological groups $\psi : G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$, and splits $s_K : I_K \to \mathbb{A}_{K,f}^*$ and $s_L : I_L \to \mathbb{A}_{L,f}^*$ as in Definition 9.1.3 such that

$$\psi(\mathrm{rec}_K(\mathcal{O}_{\mathfrak{p}}^*)) = \mathrm{rec}_L(\mathcal{O}_{\phi(\mathfrak{p})}^*) \text{ for every prime } \mathfrak{p} \text{ of } K \text{ and} \tag{7}$$

$$\psi(\mathrm{rec}_K(s_K(\mathfrak{m}))) = \mathrm{rec}_L(s_L(\phi(\mathfrak{m}))) \text{ for every ideal } \mathfrak{m} \in I_K. \tag{8}$$

(iii) There exists an isomorphism of topological groups $\psi : G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$ such that $L(\chi, s) = L(\widehat{\psi}(\chi), s)$ for all $\chi \in G_K^{\mathrm{ab}}$. ◁

We have seen statement (i) before in Chapter 9. The proof that this is equivalent to statements (ii) and (iii) is somewhat lengthy and can be found in Section 7 of [CLM16]. We refer to the statement (ii) as *the existence of a reciprocity isomorphism*. The last statement ties in directly with what we have discussed in this chapter so far, and we will call this the *existence of an L-isomorphism*. The rest of this chapter will have a simple structure; in the first section we prove that the existence of a reciprocity isomorphism implies the existence of an L-isomorphism, while in the second section we prove that the existence of an L-isomorphism implies the existence of a reciprocity isomorphism.

10.2 RECIPROCITY ISOMORPHISM IMPLIES L-ISOMORPHISM

To prove the existence of an L-isomorphism from the reciprocity isomorphism we use a statement equivalent to the existence of a reciprocity isomorphism.

Proposition 10.2.1. The existence of a reciprocity isomorphism is equivalent to the following statement. There exists a norm-preserving monoid isomorphism $\phi : I_K \xrightarrow{\sim} I_L$ and an isomorphism of topological groups $\psi : G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$ with the following property: for every finite abelian extension $K_N = (K^{\mathrm{ab}})^N$ of K, N being some subgroup of G_K^{ab}, with associated finite abelian extension $L_{\psi(N)} = (L^{\mathrm{ab}})^{\psi(N)}$, the isomorphism ϕ restricts to a bijection

$$\{\text{primes } \mathfrak{p} \text{ unramified in } K_N/K\} \longleftrightarrow \{\text{primes } \mathfrak{q} = \phi(\mathfrak{p}) \text{ unramified in } L_{\psi(N)}/L\}.$$

Moreover, for every unramified prime $\mathfrak{p}$ of K_N/K,

$$\psi(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{Frob}_{\phi(\mathfrak{p})},$$

where we use ψ for the induced map $\mathrm{Gal}(K_N/K) \to \mathrm{Gal}(L_{\psi(N)}/L)$. ◁

Proof. Proposition 8.4 of [CLM16]. □

We will call this property the existence of a *finite reciprocity isomorphism.*

Proposition 10.2.2. Assume there exists a finite reciprocity isomorphism. Then we have $L(\chi, s) = L(\widehat{\psi}(\chi), s)$ for all $\chi \in \widehat{G}_K^{\mathrm{ab}}$. ◁

Proof. Let $\chi \in \widehat{G}_K^{\mathrm{ab}}$. We have

$$L(\chi, s) = \prod_{\mathfrak{p} \in U(\chi)} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}.$$

By Proposition 10.1.7, any prime $\mathfrak{p} \in U(\chi)$ is unramified in the fixed field K_χ. Denote by π the projection map $G_K^{\mathrm{ab}} \to \mathrm{Gal}(K_\chi/K)$ and by $\overline{\chi}$ the induced character on $\mathrm{Gal}(K_\chi/K)$. By Theorem 7.4.10, we have $\pi(\mathrm{rec}_K(s_K(\mathfrak{p}))) = \mathrm{Frob}_{\mathfrak{p}}(K_\chi/K)$ for any choice of split s_K. We shorten $\mathrm{Frob}_{\mathfrak{p}}(K_\chi/K)$ to $\mathrm{Frob}_{\mathfrak{p}}$. As $\chi(\mathfrak{p}) = \chi(\mathrm{rec}_K(s_K(\mathfrak{p})))$, we obtain

$$\chi(\mathfrak{p}) = \chi(\mathrm{rec}_K(s_K(\mathfrak{p}))) = \overline{\chi}(\pi(\mathrm{rec}_K(s_K(\mathfrak{p})))) = \overline{\chi}(\mathrm{Frob}_{\mathfrak{p}}),$$

and thus

$$L(\chi, s) = \prod_{\mathfrak{p} \in U(\chi)} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p} \in U(\chi)} \frac{1}{1 - \overline{\chi}(\mathrm{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s}}$$

From Proposition 10.1.3 we have $\ker(\widehat{\psi}(\chi)) = \psi(\ker(\chi))$, from which it follows that the fixed field of $\widehat{\psi}(\chi)$, denoted $L_{\widehat{\psi}(\chi)}$, is equal to $(L^{\mathrm{ab}})^{\psi(\ker(\chi))}$.

From the properties of the finite reciprocity isomorphism, we obtain a bijection

$$\{\text{primes } \mathfrak{p} \text{ unramified in } K_\chi/K\} \longleftrightarrow \{\text{primes } \mathfrak{q} = \phi(\mathfrak{p}) \text{ unramified in } L_{\widehat{\psi}(\chi)}/L\}.$$

From Proposition 10.1.7 it follows from this bijection (given by ϕ) that $\phi(U(\chi)) = U(\widehat{\psi}(\chi))$. Moreover, the finite reciprocity isomorphism implies that $N(\mathfrak{p}) = N(\mathfrak{q})$ and for $\mathfrak{p} \in U(\chi)$ we have $\psi(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{Frob}_{\mathfrak{q}}$, thus $\overline{\widehat{\psi}(\chi)}(\mathrm{Frob}_{\mathfrak{q}}) = \overline{\chi}(\mathrm{Frob}_{\mathfrak{p}})$. Therefore

$$\begin{aligned} L(\chi, s) &= \prod_{\mathfrak{p} \in U(\chi)} \frac{1}{1 - \overline{\chi}(\mathrm{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s}} \\ &= \prod_{\mathfrak{q} \in U(\widehat{\psi}(\chi))} \frac{1}{1 - \overline{\widehat{\psi}(\chi)}(\mathrm{Frob}_{\mathfrak{q}}) N(\mathfrak{q})^{-s}} \\ &= L(\widehat{\psi}(\chi), s). \end{aligned}$$

□

Corollary 10.2.3. The existence of an reciprocity isomorphism implies the existence of an L-isomorphism. ◁

10.3 L-ISOMORPHISM IMPLIES RECIPROCITY ISOMORPHISM

The existence of an L-isomorphism is meaningless if we have no information on the existence of characters, so we rely on the two methods of creating characters from Section 10.1.2. In order to construct a reciprocity isomorphism, we begin by proving that a sufficient condition for the existence of a reciprocity isomorphism is the existence of a bijection ϕ such that the following diagrams commute:

$$\begin{array}{ccc} \widehat{G}_K^{\mathrm{ab}} & \xrightarrow{U} & \mathcal{P}_K \\ {\scriptstyle\widehat{\psi}}\downarrow & & \downarrow{\scriptstyle\phi} \\ \widehat{G}_L^{\mathrm{ab}} & \xrightarrow{U} & \mathcal{P}_L \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathcal{P}_K & \xrightarrow{\chi} & \mathbb{C}. \\ {\scriptstyle\phi}\downarrow & \nearrow_{\widehat{\psi}(\chi)} & \\ \mathcal{P}_L & & \end{array}$$

After proving this in Theorem 10.3.1, we continue with the construction of such a ϕ. We will do this inductively: we create partial bijections between the primes of a certain norm, which combined form the desired bijection ϕ.

Theorem 10.3.1. Suppose we are supplied with an L-isomorphism and let $\phi : \mathcal{P}_K \to \mathcal{P}_L$ be a bijection such that the previous diagrams commute, i. e.

$$\begin{aligned} \phi(U(\chi)) &= U(\widehat{\psi}(\chi)) \text{ for all } \chi \in G_K^{\mathrm{ab}}; \text{ and} \\ \chi(\mathfrak{p}) &= \widehat{\psi}(\chi)(\phi(\mathfrak{p})) \text{ for all } \chi \in G_K^{\mathrm{ab}}, \mathfrak{p} \in U(\chi). \end{aligned}$$

Then there exists a reciprocity isomorphism. ◂

Proof. If we extend ϕ multiplicatively to I_K, we obtain a monoid isomorphism $I_K \xrightarrow{\sim} I_L$. The isomorphism of the topological groups G_K^{ab} and G_L^{ab} is obtained from the L-isomorphism.

Using Lemma 10.1.8 and the fact that ψ is an isomorphism, we find that

$$\psi(\mathrm{rec}_K(\mathcal{O}_{\mathfrak{p}}^*)) = \psi\left(\bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \ker(\chi)\right) = \bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \psi\left(\ker(\chi)\right).$$

By Proposition 10.1.3, $\psi\left(\ker(\chi)\right) = \ker(\widehat{\psi}(\chi))$ and $\phi(U(\chi)) = U(\widehat{\psi}(\chi))$ for all χ, and it follows that

$$\bigcap_{\chi:\, \mathfrak{p}\in U(\chi)} \psi\left(\ker(\chi)\right) = \bigcap_{\widehat{\psi}(\chi):\, \phi(\mathfrak{p})\in U(\chi)} \ker(\widehat{\psi}(\chi)).$$

As $\widehat{\psi}$ is an isomorphism, we take the intersection over all characters on G_L^{ab} with $\phi(\mathfrak{p})$ unramified, hence by Lemma 10.1.8 we obtain

$$\bigcap_{\widehat{\psi}(\chi):\, \phi(\mathfrak{p})\in U(\chi)} \ker(\widehat{\psi}(\chi)) = \mathrm{rec}_L(\mathcal{O}_{\phi(\mathfrak{p})}^*).$$

For any prime $\mathfrak{p} \in \mathcal{P}_K$, the second condition of ϕ states that for all characters χ with $\mathfrak{p} \in U(\chi)$ we have $\chi(\mathfrak{p}) = \widehat{\psi}(\chi)(\phi(\mathfrak{p}))$. Using only definitions, we find

$$\chi(\mathfrak{p}) = \chi(\mathrm{rec}_K(s_K(\mathfrak{p}))) \text{ and } \widehat{\psi}(\chi)(\phi(\mathfrak{p})) = \chi(\psi^{-1}(\mathrm{rec}_L(s_L(\phi(\mathfrak{p}))))),$$

thus

$$\mathrm{rec}_K(s_K(\mathfrak{p})) \equiv \psi^{-1}(\mathrm{rec}_L(s_L(\phi(\mathfrak{p})))) \pmod{\ker(\chi)}.$$

As this holds for all χ with $\mathfrak{p} \in U(\chi)$ and $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) = \bigcap_{\mathfrak{p}\in U(\chi)} \ker(\chi)$, we find

$$\mathrm{rec}_K(s_K(\mathfrak{p})) \equiv \psi^{-1}(\mathrm{rec}_L(s_L(\phi(\mathfrak{p})))) \pmod{\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)}.$$

However, we can modify the split s_K with elements in $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ freely, as the only condition was that $s_K(\mathfrak{p}) = (1,\dots,1,\pi_\mathfrak{p},1,\dots)$ and uniformisers are unique up to units. Hence it is possible to alter s_K (for every prime independently) such that

$$\mathrm{rec}_K(s_K(\mathfrak{p})) = \psi^{-1}(\mathrm{rec}_L(s_L(\phi(\mathfrak{p})))),$$

or equivalently

$$\psi(\mathrm{rec}_K(s_K(\mathfrak{p}))) = \mathrm{rec}_L(s_L(\phi(\mathfrak{p}))),$$

for all $\mathfrak{p} \in \mathcal{P}_K$. As all maps are multiplicative, the same equality holds for ideals $\mathfrak{m} \in I_K$ and therefore we have fulfilled all conditions for the reciprocity isomorphism. ❐

To construct this ϕ, we inductively create bijections ϕ_N between the primes of K and the primes of L of a certain norm N. Global fields only have finitely many primes of a given norm. With this in mind, we can create characters using Theorem 10.1.9 that have specific values on the primes of norm N, which will aid us in finding a bijection ϕ_N. Therefore, we introduce notation in order to deal with the primes one norm at a time. For any set S of ideals of K we define the following subsets:

$$\begin{aligned} S_N &= \{\mathfrak{m} \in S : N(\mathfrak{m}) = N\} \\ S_{\geq N} &= \{\mathfrak{m} \in S : N(\mathfrak{m}) \geq N\} \\ S_{<N} &= \{\mathfrak{m} \in S : N(\mathfrak{m}) < N\}. \end{aligned}$$

However, if the set of ideals has a subscript already, e.g. I_K, we use superscript for N, $\geq N$, and $< N$, e.g. $I_K^{<N}$.

Suppose for a given $N \in \mathbb{N}$ we are supplied with bijections $\phi_M : \mathcal{P}_K^M \to \mathcal{P}_L^M$ such that $\phi_M(U_M(\chi)) = U_M(\widehat{\psi}(\chi))$ and $\chi(\mathfrak{p}) = \widehat{\psi}(\chi)(\phi_M(\mathfrak{p}))$ for all $\chi \in G_K^{\mathrm{ab}}$, $\mathfrak{p} \in U_M(\chi)$ and all $M < N$. Let $\phi_{<N}$ be the bijection $\mathcal{P}_K^{<N} \to \mathcal{P}_L^{<N}$ given by $\phi_{<N}\big|_{\mathcal{P}_K^M} = \phi_M$ for all $M < N$. Thus $\phi_{<N}$ has the following properties:

$$\begin{aligned} &\phi_{<N}(U_{<N}(\chi)) = U_{<N}(\widehat{\psi}(\chi)) \text{ for all } \chi \in G_K^{\mathrm{ab}}; \text{ and} \\ &\chi(\mathfrak{p}) = \widehat{\psi}(\chi)(\phi_{<N}(\mathfrak{p})) \text{ for all } \chi \in G_K^{\mathrm{ab}}, \mathfrak{p} \in U_{<N}(\chi). \end{aligned}$$

We will refer to these as the properties of $\phi_{<N}$.

We have a trivial induction basis: there exist no primes of norm 1, hence for $N \leq 2$ the statement is empty (and therefore true).

This completes the induction hypothesis.

10.3.1 INFORMATION OBTAINED FROM L-SERIES

We are left with proving the induction step, which will be quite lengthy. The idea behind creating the bijection ϕ_N is as follows: we create a special type characters on both G_K^{ab} and G_L^{ab} that are associated to a prime of K resp L of norm N. We then establish a connection between those characters via the isomorphism $\widehat{\psi}$, which also connects the primes of K and L of norm N. This connection will prove to be a bijection.

We begin by extracting information on the primes of norm N from the L-series, with Corollary 10.3.4 as main result. In order to do this, we split the L-series into two

products; one over primes with norm below N and one over primes with norm at least N so that we can use the induction hypothesis.

Set

$$L_{<N}(\chi, s) = \prod_{\mathfrak{p} \in U_{<N}(\chi)} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1},$$
$$L_{\geq N}(\chi, s) = \prod_{\mathfrak{p} \in U_{\geq N}(\chi)} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

Proposition 10.3.2. We have $L_{<N}(\chi, s) = L_{<N}(\widehat{\psi}(\chi), s)$. ◁

Proof. We make use of the bijection $\phi_{<N} : \mathcal{P}^{<N}(K) \to \mathcal{P}^{<N}(L)$. By construction, $\phi_{<N}\big|_M$ is a bijection $\mathcal{P}_K^M \to \mathcal{P}_L^M$, hence $\phi_{<N}$ is norm-preserving. It follows from the properties of $\phi_{<N}$ (used for the third equality) that

$$\begin{aligned} L_{<N}(\chi, s) &= \prod_{\mathfrak{p} \in U_{<N}(\chi)} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1} \\ &= \prod_{\mathfrak{p} \in U_{<N}(\chi)} (1 - \widehat{\psi}(\chi)(\phi_{<N}(\mathfrak{p})) N(\phi_{<N}(\mathfrak{p}))^{-s})^{-1} \\ &= \prod_{\mathfrak{q} \in U_{<N}(\widehat{\psi}(\chi))} (1 - \widehat{\psi}(\chi)(\mathfrak{q}) N(\mathfrak{q})^{-s})^{-1} \\ &= L_{<N}(\widehat{\psi}(\chi), s). \end{aligned}$$ ❐

Corollary 10.3.3. We also have $L_{\geq N}(\chi, s) = L_{\geq N}(\widehat{\psi}(\chi), s)$. ◁

Proof. This follows as $L(\chi, s) = L(\widehat{\psi}(\chi), s)$ and $L(\chi, s) = L_{<N}(\chi, s) L_{\geq N}(\chi, s)$, as we have

$$\begin{aligned} L_{<N}(\chi, s) L_{\geq N}(\chi, s) &= L(\chi, s) \\ &= L(\widehat{\psi}(\chi), s) \\ &= L_{<N}(\widehat{\psi}(\chi), s) L_{\geq N}(\widehat{\psi}(\chi), s) \\ &= L_{<N}(\chi, s) L_{\geq N}(\widehat{\psi}(\chi), s) \end{aligned}$$

Hence $L_{\geq N}(\chi, s) = L_{\geq N}(\widehat{\psi}(\chi), s)$. ❐

Corollary 10.3.4. For any character $\chi \in \widehat{G}_K^{\mathrm{ab}}$ the equation

$$\sum_{\mathfrak{p} \in \mathcal{P}_K^N} \chi(\mathfrak{p}) = \sum_{\mathfrak{p} \in \mathcal{P}_L^N} \widehat{\psi}(\chi)(\mathfrak{p})$$

holds. ◁

Proof. As with $L(\chi, s)$, we can write $L_{\geq N}(\chi, s)$ in additive form

$$L_{\geq N}(\chi, s) = \sum_{\mathfrak{m} \in \langle U^{\geq N}(\chi) \rangle} \chi(\mathfrak{m}) N(\mathfrak{m})^{-s}.$$

If we now group all ideals of a certain norm, we obtain

$$L_{\geq N}(\chi, s) = \sum_{M \geq N} \left(\sum_{\mathfrak{m} \in \langle U^{\geq N}(\chi) \rangle \cap I_K^N} \chi(\mathfrak{m}) \right) M^{-s}.$$

Dividing on both sides by N^{-s} gives

$$\frac{L_{\geq N}(\chi,s)}{N^{-s}} = \left(\sum_{\mathfrak{m}\in\langle U^{\geq N}(\chi)\rangle\cap I_K^N}\chi(\mathfrak{m})\right) + \sum_{M>N}\left(\sum_{\mathfrak{m}\in\langle U^{\geq N}(\chi)\rangle\cap I_K^N}\chi(\mathfrak{m})\right)\frac{M^{-s}}{N^{-s}}.$$

As $\chi(\mathfrak{p})$ is zero at all primes where χ ramifies, we have

$$\sum_{\mathfrak{m}\in\langle U^{\geq N}(\chi)\rangle\cap I_K^N}\chi(\mathfrak{m}) = \sum_{\mathfrak{m}\in\langle \mathcal{P}_K^{\geq N}\rangle\cap I_K^N}\chi(\mathfrak{m}).$$

However, norms are multiplicative, hence any non-prime in $\langle\mathcal{P}_K^{\geq N}\rangle$ has norm at least N^2. As there exist no primes of norm 1 we may assume that $N^2 > N$ and therefore $\langle\mathcal{P}_K^{\geq N}\rangle\cap I_K^N$ contains only prime ideals (of norm N). Moreover, it contains all prime ideals of norm N, hence $\langle\mathcal{P}_K^{\geq N}\rangle\cap I_K^N = \mathcal{P}_K^N$.

If we let $s\to\infty$ we obtain

$$\lim_{s\to\infty}\frac{L_{\geq N}(\chi,s)}{N^{-s}} = \sum_{\mathfrak{m}\in\langle U^{\geq N}(\chi)\rangle\cap I_K^N}\chi(\mathfrak{m}) = \sum_{\mathfrak{m}\in\mathcal{P}_K^N}\chi(\mathfrak{p}).$$

From Corollary 10.3.3 we know that $L_{\geq N}(\chi,s) = L_{\geq N}(\widehat{\psi}(\chi),s)$. It follows that

$$\sum_{\mathfrak{p}\in\mathcal{P}_K^N}\chi(\mathfrak{p}) = \sum_{\mathfrak{p}\in\mathcal{P}_K^N}\widehat{\psi}(\chi)(\mathfrak{p}).$$

This concludes the proof. ❐

10.3.2 ASSOCIATING CERTAIN TYPES OF CHARACTERS

Now that we have Corollary 10.3.4 it is justified to further explore the types of characters we have. Two types of characters will be especially important: the characters that are 1 on all primes of norm N, and the characters that are 1 on all but one prime of norm N, and ramified on this last prime. By associating these type of characters on G_K^{ab} and G_L^{ab} in Lemma 10.3.10, we obtain an association of certain primes of K and L of norm N, and we will prove that this association is in fact a bijection in Lemma 10.3.13. We begin by introducing notation that is quite compact to allow for better readability.

Define for a character $\chi\in\widehat{G}_K^{\mathrm{ab}}$:

$$\mathcal{S}_N(\chi) = \sum_{\mathfrak{p}\in\mathcal{P}_K^N}\chi(\mathfrak{p}) = \sum_{\mathfrak{p}\in U_N(\chi)}\chi(\mathfrak{p}).$$

The second equality holds as χ is zero outside of $U_N(\chi)$.

Lemma 10.3.5. For any $\chi\in\widehat{G}_K^{\mathrm{ab}}$ we have $\mathcal{S}_N(\chi) = \mathcal{S}_N(\widehat{\psi}(\chi))$. ◁

Proof. We have already proven this in Corollary 10.3.4. ❐

Corollary 10.3.6. For any $N\in\mathbb{N}$ we have $|\mathcal{P}_K^N| = |\mathcal{P}_L^N|$. ◁

Proof. If we let $\chi=\chi_0$, we get $\mathcal{S}_N(\chi_0) = \sum_{\mathfrak{p}\in\mathcal{P}_K^N}1 = |\mathcal{P}_K^N|$. As $\widehat{\psi}$ is an isomorphism, $\widehat{\psi}(\chi_0)$ is the trivial character in $\widehat{G}_L^{\mathrm{ab}}$ and therefore $\mathcal{S}_N(\widehat{\psi}(\chi)) = |\mathcal{P}_L^N|$. It follows that $|\mathcal{P}_K^N| = |\mathcal{P}_L^N|$. ❐

This corollary allows us to define $c_N = |\mathcal{P}_K^N| = |\mathcal{P}_L^N|$. Moreover, let

$$U_N(\chi) = \left\{\mathfrak{p} \in \mathcal{P}_K^N : \chi|_{\mathrm{rec}_K(\widehat{\mathcal{O}}_K^*)} = 1\right\} = \left\{\mathfrak{p} \in \mathcal{P}_K^N : \chi(\mathfrak{p}) \neq 0\right\}$$

and

$$V_N(\chi) = \left\{\mathfrak{p} \in \mathcal{P}_K^N : \chi(\mathfrak{p}) = 1\right\} \subseteq U_N(\chi).$$

Denote $u_N(\chi) = |U_N(\chi)|$ and $v_N(\chi) = |V_N(\chi)|$ (these are finite numbers as there exist only finitely many primes of a given norm). We prove that the following two sets of characters are respected by the isomorphism $\widehat{\psi}$:

$$\Delta_K^1 := \left\{\chi \in \widehat{G}_K^{\mathrm{ab}} : u_N(\chi) = v_N(\chi) = c_N\right\}$$
$$\Delta_K^3 := \left\{\chi \in \widehat{G}_K^{\mathrm{ab}} : u_N(\chi) = v_N(\chi) = c_N - 1\right\}.$$

The intuitive definition of these sets is equally important: the characters in Δ_K^1 are those that are 1 on all primes of norm N (hence do not ramify there) and Δ_K^3 consists of the characters that ramify at exactly one prime (of norm N), and are 1 on all other primes of norm N.

Remark. The reason we use Δ^1 and Δ^3 is because this is compatible with [CLM16], in which a set of characters Δ^2 is defined that is not used in our proof.

Lemma 10.3.7. For any character χ, we have $|\mathcal{S}_N(\chi)| \leq u_N(\chi)$. We have $\mathcal{S}_N(\chi) = u_N(\chi)$ precisely when $u_N(\chi) = v_N(\chi)$. ◂

Proof. As $|\chi(\mathfrak{p})| \leq 1$ for all $\mathfrak{p} \in U_N(\chi)$, we have $|\mathcal{S}_N(\chi)| \leq u_N(\chi)$. The equality $\mathcal{S}_N(\chi) = u_N(\chi)$ holds precisely when

$$\chi(\mathfrak{p}) = 1 \text{ for all } \mathfrak{p} \in U_N(\chi) \iff U_N(\chi) = V_N(\chi) \iff u_N(\chi) = v_N(\chi). \qquad \square$$

Lemma 10.3.8. We have $\chi \in \Delta_K^1$ precisely when $\mathcal{S}_N(\chi) = c_N$. ◂

Proof. As $u_N(\chi) \leq c_N$, we see from Lemma 10.3.7 that $\mathcal{S}_N(\chi) = c_N$ precisely when $u_N(\chi) = v_N(\chi) = c_N$, which is equivalent to $\chi \in \Delta_K^1$. $\square$

Corollary 10.3.9. The isomorphism $\widehat{\psi}$ respects Δ^1, i. e. $\widehat{\psi}(\Delta_K^1) = \Delta_L^1$. ◂

Proof. We have $\chi \in \Delta_K^1$ if and only if $\mathcal{S}_N(\chi) = c_N$ by the previous lemma, which happens precisely when $\mathcal{S}_N(\widehat{\psi}(\chi)) = c_N$ by Lemma 10.3.5, which in turn is equivalent to $\widehat{\psi}(\chi) \in \Delta_L^1$ by the previous lemma. $\square$

Lemma 10.3.10. We have $\widehat{\psi}(\Delta_K^3) = \Delta_L^3$. ◂

Proof. Let $\chi \in \Delta_K^3$, then by definition there is some $\mathfrak{p}_\chi \in \mathcal{P}_K^N$ such that $\chi(\mathfrak{p}_\chi) = 0$. Then

$$\mathcal{S}_N(\chi) = \sum_{\mathfrak{p} \in U_N(\chi)} \chi(\mathfrak{p}) = u_N(\chi) = c_N - 1,$$

as $u_n(\chi) = v_n(\chi) = c_N - 1$. Hence we also have $\mathcal{S}_N(\widehat{\psi}(\chi)) = c_N - 1$. We consider three possibilities:

- $u_N(\widehat{\psi}(\chi)) < c_N - 1$. Then $|\mathcal{S}_N(\widehat{\psi}(\chi))| \leq u_N(\widehat{\psi}(\chi)) = c_N - 1$ by Lemma 10.3.7, which is a contradiction.

- $u_N(\widehat{\psi}(\chi)) = c_N - 1$. Then, again by Lemma 10.3.7, we see that $\mathcal{S}_N(\widehat{\psi}(\chi)) = c_N - 1$ exactly when $u_N(\widehat{\psi}(\chi)) = v_N(\widehat{\psi}(\chi))$, and therefore $\widehat{\psi}(\chi) \in \Delta_L^3$.
- $u_N(\widehat{\psi}(\chi)) = c_N$. As $\mathcal{S}_N(\widehat{\psi}(\chi)) = c_N - 1$, we have $u_N(\widehat{\psi}(\chi)) > v_N(\widehat{\psi}(\chi))$ (again by Lemma 10.3.7). Let $m = u_N(\widehat{\psi}(\chi)) - v_N(\widehat{\psi}(\chi))$ (which is finite) and enumerate the primes in $U_N(\widehat{\psi}(\chi)) - V_N(\widehat{\psi}(\chi))$ by $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. Then $\widehat{\psi}(\chi)(\mathfrak{q}_i)$ is a root of unity, say $\widehat{\psi}(\chi)(\mathfrak{q}_i)^{d_i} = 1$. Let $d = \prod_{i=1}^m d_i$. Then $\widehat{\psi}(\chi^d)(\mathfrak{p}) = 1$ for all $\mathfrak{p} \in U_N(\chi) = \mathcal{P}_L^N$ and therefore $\widehat{\psi}(\chi^d) \in \Delta_L^1$. By Corollary 10.3.9 we find $\chi^d \in \Delta_K^1$. However, $\chi^d(\mathfrak{p}_\chi) = 0^d = 0$, which is a contradiction.

We conclude that $\widehat{\psi}(\chi) \in \Delta_L^3$, thus $\widehat{\psi}(\Delta_K^3) \subseteq \Delta_L^3$.

If we repeat this process, this time using the isomorphism $\widehat{\psi}^{-1}$ (so the roles of K and L are reversed), we obtain that $\widehat{\psi}^{-1}(\Delta_L^3) \subseteq \Delta_K^3$, hence $\Delta_L^3 \subseteq \widehat{\psi}(\Delta_K^3)$ (as $\widehat{\psi}$ is an isomorphism). We conclude that $\widehat{\psi}(\Delta_K^3) = \Delta_L^3$. ❐

Corollary 10.3.11. For every $\mathfrak{p} \in \mathcal{P}_K^N$ and $\chi \in \Delta_K^3$ with $U_N(\chi) = \mathcal{P}_K^N - \{\mathfrak{p}\}$, there exists a prime $\phi_N(\mathfrak{p}, \chi) \in \mathcal{P}_L^N$ with $U_N(\widehat{\psi}(\chi)) = \mathcal{P}_L^N - \{\phi_N(\mathfrak{p}, \chi)\}$. ◅

10.3.3 BIJECTION OF PRIMES OF NORM N

The notation in Corollary 10.3.11 already suggests that this association of (some of the) primes in $\mathcal{P}_K^N$ and $\mathcal{P}_L^N$ is the bijection we are looking for. This section will be devoted to proving all required properties of ϕ_N. As a direct result this completes the proof of the equivalence of the existence of an L-isomorphism and a reciprocity isomorphism.

Lemma 10.3.12. The prime $\phi_N(\mathfrak{p}, \chi)$ does not depend on χ. ◅

Proof. Take $\chi, \chi' \in \Delta_K^3$ such that $U_N(\chi) = U_N(\chi') = \mathcal{P}_K^N - \{\mathfrak{p}_\chi\}$. Then for any $\mathfrak{p} \in U_N(\chi)$ we have $(\chi \cdot \chi')(\mathfrak{p}) = \chi(\mathfrak{p})\chi'(\mathfrak{p}) = 1 \cdot 1 = 1$, while $(\chi \cdot \chi')(\mathfrak{p}_\chi) = \chi(\mathfrak{p}_\chi)\chi'(\mathfrak{p}_\chi) = 0 \cdot 0 = 0$, hence $\chi \cdot \chi' \in \Delta_K^3$. As a result, $\widehat{\psi}(\chi \cdot \chi') \in \Delta_L^3$, hence there is only a single prime $\mathfrak{q}$ such that $\widehat{\psi}(\chi \cdot \chi')(\mathfrak{q}) = 0$, as $u_N(\chi \cdot \chi') = c_N - 1$. However, $\widehat{\psi}(\chi \cdot \chi')(\phi_N(\mathfrak{p}, \chi)) = 0$ and $\widehat{\psi}(\chi \cdot \chi')(\phi_N(\mathfrak{p}, \chi')) = 0$ by Corollary 10.3.11. We conclude that $\phi_N(\mathfrak{p}, \chi) = \phi_N(\mathfrak{p}, \chi')$. ❐

We drop the χ from $\phi_N(\mathfrak{p}, \chi)$ and obtain a connection between some of the primes of $\mathcal{P}_K^N$ and $\mathcal{P}_L^N$.

Enumerate the primes in $\mathcal{P}_K^N$ by $\mathfrak{p}_1, \ldots, \mathfrak{p}_{c_N}$ and let $\chi_1, \ldots, \chi_{c_N}$ be characters such that $\chi_i(\mathfrak{p}_i) = 0$ and $\chi_i(\mathfrak{p}) = 1$ for all $\mathfrak{p} \in \mathcal{P}_K^N - \{\mathfrak{p}_i\}$. These characters exist by Theorem 10.1.9.

Lemma 10.3.13. ϕ_N is a bijection. ◅

Proof. As $|\mathcal{P}_K^N| = |\mathcal{P}_L^N|$, it suffices to prove that ϕ_N is injective. Suppose $\mathfrak{q}_i := \phi_N(\mathfrak{p}_i)$ and $\mathfrak{q}_j := \phi_N(\mathfrak{p}_j)$ are equal for some $1 \leq i < j \leq c_N$. We obtain that $\widehat{\psi}(\chi_i)(\mathfrak{q}) = \widehat{\psi}(\chi_j)(\mathfrak{q})$ for all $\mathfrak{q} \in \mathcal{P}_L^N$ (as they are both zero on $\mathfrak{q}_i = \mathfrak{q}_j$ and 1 otherwise).

The character $\chi_i \cdot \chi_j$ does not lie in Δ_K^3 as $(\chi_i \cdot \chi_j)(\mathfrak{p}_i) = (\chi_i \cdot \chi_j)(\mathfrak{p}_j) = 0$ and $i \neq j$. On the other hand, as $\widehat{\psi}(\chi_i)(\mathfrak{q}) = \widehat{\psi}(\chi_j)(\mathfrak{q})$ for all $\mathfrak{q} \in \mathcal{P}_L^N$ we have

$$\widehat{\psi}(\chi_i \cdot \chi_j)(\mathfrak{q}) = \widehat{\psi}(\chi_i)^2(\mathfrak{q}) = \begin{cases} 0 & \text{if } \mathfrak{q} = \mathfrak{q}_i; \\ 1 & \text{otherwise,} \end{cases}$$

hence $\widehat{\psi}(\chi_i \cdot \chi_j) \in \Delta_L^3$. This is in contradiction with $\widehat{\psi}(\Delta_K^3) = \Delta_L^3$ (Lemma 10.3.10) combined with the fact that $\widehat{\psi}$ is an isomorphism. ❐

Enumerate the primes in $\mathcal{P}_L^N$ by $\mathfrak{q}_1, \ldots, \mathfrak{q}_{c_N}$ such that $\mathfrak{q}_i = \phi_N(\mathfrak{p}_i)$.

Corollary 10.3.14. For every $\chi \in \widehat{G}_K^{\mathrm{ab}}$, we have $\phi_N(U_N(\chi)) = U_N(\widehat{\psi}(\chi))$. Moreover, $\chi(\mathfrak{p}) = \widehat{\psi}(\chi)(\phi_N(\mathfrak{p}))$. ◁

Proof. Suppose $\mathfrak{p}_j \in U_N(\chi)$, thus $\phi_N(\mathfrak{p}_j) \in \phi_N(U_N(\chi))$. We know that $\chi(\mathfrak{p}_j) \neq 0$, hence the character $\chi \prod_{i \neq j} \chi_i$ is zero at all primes in $\mathcal{P}_K^N$ except for the prime $\mathfrak{p}_j$, where it is equal to $\chi(\mathfrak{p}_j)$. Thus $\mathcal{S}_N(\chi \prod_{i \neq j} \chi_i) = \chi(\mathfrak{p}_j)$.

We know that $\widehat{\psi}(\chi_i)$ is 1 everywhere except at $\phi_N(\mathfrak{p}_i)$, where it is zero. Thus $\widehat{\psi}(\chi \prod_{i \neq j} \chi_i)$ is zero at all primes of the form $\phi_N(\mathfrak{p}_i)$, $i \neq j$. As ϕ_N is a bijection by Lemma 10.3.13, $\widehat{\psi}(\chi \prod_{i \neq j} \chi_i)$ is zero everywhere except possibly at $\phi_N(\mathfrak{p}_j)$. Moreover, Lemma 10.3.5 implies that

$$\widehat{\psi}(\chi \prod_{i \neq j} \chi_i)(\phi_N(\mathfrak{p}_j)) = \mathcal{S}_N(\widehat{\psi}(\chi \prod_{i \neq j} \chi_i)) = \mathcal{S}_N(\chi \prod_{i \neq j} \chi_i) = \chi(\mathfrak{p}_j).$$

As $\widehat{\psi}(\chi_i)(\phi_N(\mathfrak{p}_j)) = 1$ for all $i \neq j$, we find

$$\widehat{\psi}(\chi)(\phi_N(\mathfrak{p}_j)) = \widehat{\psi}(\chi \prod_{i \neq j} \chi_i)(\phi_N(\mathfrak{p}_j)) = \chi(\mathfrak{p}_j). \tag{9}$$

Hence $\widehat{\psi}(\chi)(\phi_N(\mathfrak{p}_j)) \neq 0$ and therefore $\phi_N(\mathfrak{p}_j) \in U_N(\widehat{\psi}(\chi))$. It follows that $\phi_N(U_N(\chi)) \subseteq U_N(\widehat{\psi}(\chi))$.

For the inverse inclusion, we repeat the process this time reversing the roles of K and L, using the isomorphism $\widehat{\psi}^{-1}$ and the bijection ϕ_N^{-1}. We obtain that for all $\mathfrak{q}_j \in U_N(\widehat{\psi}(\chi))$ we have $\phi_N^{-1}(\mathfrak{q}_j) \in U_N(\chi)$ (note $\widehat{\psi}^{-1}(\widehat{\psi}(\chi)) = \chi$). As a result, $U_N(\widehat{\psi}(\chi)) \subseteq \phi_N(U_N(\chi))$.

We conclude that $\phi_N(U_N(\chi)) = U_N(\widehat{\psi}(\chi))$.

The second assertion follows immediately: for any $\mathfrak{p} \notin U_N(\chi)$ we have $\phi_N(\mathfrak{p}) \notin U_N(\widehat{\psi}(\chi))$, and therefore $\chi(\mathfrak{p}) = 0 = \widehat{\psi}(\chi)(\phi_N(\mathfrak{p}))$. For $\mathfrak{p} \in U_N(\chi)$ we have seen in Equation 9 that $\chi(\mathfrak{p}) = \widehat{\psi}(\chi)(\phi_N(\mathfrak{p}))$. ❐

This completes the proof by induction; we obtain a bijection $\phi : \mathcal{P}_K \to \mathcal{P}_L$ with properties as required in Theorem 10.3.1, and as a result we have a reciprocity isomorphism.

11

GLOBAL FIELD ISOMORPHISMS

In this final chapter we study the methods used to obtain a field isomorphism from the equivalent statements we have seen before. The objective here is not to provide rigorous proofs, but to provide the general idea of how to obtain the desired isomorphism, which will work only for function fields. A proof for number fields was given by Bart de Smit in an unpublished article. We begin by combining all equivalent statements of Chapter 9 and 10 so that we can freely use all properties we have seen. With this we can derive an isomorphism $\mathbb{A}_{K,f}^* \xrightarrow{\sim} \mathbb{A}_{L,f}^*$, which for function fields restricts to an isomorphism $K^\times \xrightarrow{\sim} L^\times$. A theorem by Ushida and Hoshi states a sufficient condition for an isomorphism $K^\times \xrightarrow{\sim} L^\times$ to extend to an isomorphism $K \to L$, which holds for the isomorphism we find.

11.1 COMBINING THE EQUIVALENT STATEMENTS

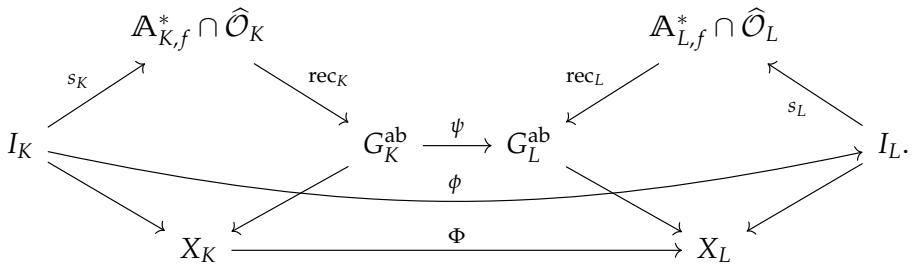
Suppose the equivalent statements hold. By combining Theorem 9.2.1, Theorem 10.1.11, and Proposition 10.2.1, we obtain the following maps:

A. an isomorphism of topological groups $\Phi : X_K \xrightarrow{\sim} X_L$ that restricts to a norm-preserving monoid isomorphism $\phi : I_K \xrightarrow{\sim} I_L$;

B. an isomorphism of topological groups $\psi : G_K^{\mathrm{ab}} \xrightarrow{\sim} G_L^{\mathrm{ab}}$ satisfying $\psi(\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)) = \mathrm{rec}_L(\mathcal{O}_{\phi(\mathfrak{p})}^*)$ for all $\mathfrak{p} \in \mathcal{P}_K$; and

C. splits $s_K : I_K \to \mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K$ and $s_L : I_L \to \mathbb{A}_{L,f}^* \cap \widehat{\mathcal{O}}_L$ such that $\psi(\mathrm{rec}_K(s_K(\mathfrak{m}))) = \mathrm{rec}_L(s_L(\phi(\mathfrak{m})))$ for all $\mathfrak{m} \in I_K$.

We can summarise this in a commutative diagram:



(10)

The first step will be to create an isomorphism $\Psi : \mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K \to \mathbb{A}_{L,f}^* \cap \widehat{\mathcal{O}}_L$. For this we change our perspective on $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K$:

Lemma 11.1.1. There exists a monoid isomorphism $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K \cong \widehat{\mathcal{O}}_K^* \times I_K$. ◂

Proof. Using the split s_K, we have a monoid homomorphism $\widehat{\mathcal{O}}_K^* \times I_K \to \mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K$ given by $(u, \mathfrak{m}) \mapsto u \cdot s_K(\mathfrak{m})$. We construct an inverse of this map.

Any element of $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K$ is of the form $\prod_{\mathfrak{p} \in \mathcal{P}_K} x_\mathfrak{p}$, where $x_\mathfrak{p}$ lies in $\mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p}$ and in $\mathcal{O}_\mathfrak{p}^*$ for all but finitely many $\mathfrak{p}$. Hence there exists a (smallest) finite subset $S \subseteq \mathcal{P}_K$

such that $x_\mathfrak{p} = u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^*$ if $\mathfrak{p} \notin S$ and $x_\mathfrak{p} = u_\mathfrak{p} \cdot \pi_\mathfrak{p}^{n_\mathfrak{p}}$ with $u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^*$ and $n_\mathfrak{p} \in \mathbb{N}_0$ if $\mathfrak{p} \in S$, where $\pi_\mathfrak{p}$ is a uniformiser chosen such that $s_K(\mathfrak{p}) = (1, \dots, 1, \pi_\mathfrak{p}, 1, \dots)$.

Combining the $u_\mathfrak{p}$ to $u = \prod_{\mathfrak{p} \in \mathcal{P}_K} u_\mathfrak{p}$, we obtain an element $u \in \widehat{\mathcal{O}}_K^*$. Moreover, we can send $\prod_{\mathfrak{p} \in S} \pi_\mathfrak{p}^{n_\mathfrak{p}}$ to the ideal $\prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_\mathfrak{p}}$, which is well-defined as S is finite. We obtain a monoid homomorphism $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K \to \widehat{\mathcal{O}}_K^* \times I_K$ given by

$$\prod_{\mathfrak{p} \in \mathcal{P}_K} x_\mathfrak{p} \mapsto \left(\prod_{\mathfrak{p} \in \mathcal{P}_K} u_\mathfrak{p}, \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_\mathfrak{p}} \right),$$

which is the inverse of $(u, \mathfrak{m}) \mapsto u \cdot s_K(\mathfrak{m})$. ❐

As we have seen in Theorem 6.4.2, under the local reciprocity map $\mathcal{O}_\mathfrak{p}^*$ is mapped isomorphically to $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}^{\mathrm{ur}})$, which is then mapped injectively to some subgroup of G_K^{ab} via the inclusion $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}) \hookrightarrow G_K^{\mathrm{ab}}$. As a result, $\mathcal{O}_\mathfrak{p}^*$ is isomorphic to $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$. We can use this to obtain the following result:

Proposition 11.1.2. For any $\mathfrak{p} \in \mathcal{P}_K$ we have $\mathcal{O}_\mathfrak{p}^* \cong \mathcal{O}_{\phi(\mathfrak{p})}^*$ and consequently $\widehat{\mathcal{O}}_K^* \cong \widehat{\mathcal{O}}_L^*$. ◂

Proof. As we have just mentioned, $\mathcal{O}_\mathfrak{p}^* \cong \mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*)$ and $\mathcal{O}_{\phi(\mathfrak{p})}^* \cong \mathrm{rec}_L(\mathcal{O}_{\phi(\mathfrak{p})}^*)$. Using the property of ψ (see part B. of the maps at the start of this section) we find $\mathrm{rec}_K(\mathcal{O}_\mathfrak{p}^*) \cong \mathrm{rec}_L(\mathcal{O}_{\phi(\mathfrak{p})}^*)$, which completes the proof. ❐

Corollary 11.1.3. We have $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K \cong \mathbb{A}_{L,f}^* \cap \widehat{\mathcal{O}}_L$. ◂

Proof. Using the monoid isomorphism $\phi : I_K \xrightarrow{\sim} I_L$ combined with Proposition 11.1.2 results in a monoid isomorphism $\widehat{\mathcal{O}}_K^* \times I_K \xrightarrow{\sim} \widehat{\mathcal{O}}_L^* \times I_L$. The result now follows from Lemma 11.1.1. ❐

Denote by Ψ the corresponding isomorphism. Using Lemma 7.9 of [CLM16], one can prove that this map fits nicely into Diagram 10, i. e. the following diagram commutes:

$$\begin{array}{ccc} \mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K & \xrightarrow{\Psi} & \mathbb{A}_{L,f}^* \cap \widehat{\mathcal{O}}_L \\ \downarrow{\scriptstyle \mathrm{rec}_K} & & \downarrow{\scriptstyle \mathrm{rec}_L} \\ G_K^{\mathrm{ab}} & \xrightarrow{\psi} & G_L^{\mathrm{ab}}. \end{array}$$

However, as the field of fractions of $\widehat{\mathcal{O}}_K$ is equal to $\prod_{\mathfrak{p} \in \mathcal{P}_K} K_\mathfrak{p}$, we find that the group of fractions of $\mathbb{A}_{K,f}^* \cap \widehat{\mathcal{O}}_K$ is equal to $\mathbb{A}_{K,f}^* \cap \prod_{\mathfrak{p} \in \mathcal{P}_K} K_\mathfrak{p} = \mathbb{A}_{K,f}^*$. Hence we can extend the previous diagram to the following commutative diagram:

$$\begin{array}{ccc} \mathbb{A}_{K,f}^* & \xrightarrow{\Psi} & \mathbb{A}_{L,f}^* \\ \downarrow{\scriptstyle \mathrm{rec}_K} & & \downarrow{\scriptstyle \mathrm{rec}_L} \\ G_K^{\mathrm{ab}} & \xrightarrow{\psi} & G_L^{\mathrm{ab}}. \end{array}$$

In particular, this gives us the following result:

Corollary 11.1.4. The kernels of rec_K and rec_L are isomorphic, i. e. $\Psi(\ker(\mathrm{rec}_K)) = \ker(\mathrm{rec}_L)$. ◂

Here we have to separate global function fields from number fields, as the reciprocity map has different kernels depending on the type of global field. If K and L are number fields, the kernel of rec_K and rec_L are difficult to describe, while if they are function fields, the kernels are $K^\times$ and $L^\times$ respectively, see Theorem 2.4 of [Poo12]. Hence, in the case of function fields, Corollary 11.1.4 can be reformulated:

Corollary 11.1.5. Suppose the equivalent statements hold for two global function fields K and L. Then $K^\times \cong L^\times$. ◁

Denote the isomorphism by Ψ. The question is now whether we can extend this isomorphism to a field isomorphism $L \cong K$ (by setting $0 \mapsto 0$). This turns out to be the case, provided that certain conditions hold.

Lemma 11.1.6 (Uchida & Hoshi)**.** Denote by $\Pi_\mathfrak{p} : \mathbb{A}_{K,f}^* \to K_\mathfrak{p}^\times$ the (surjective) projection map, and by $v_\mathfrak{p}$ the valuation on $K_\mathfrak{p}$. Suppose we have an isomorphism $\Psi : K^\times \xrightarrow{\sim} L^\times$. It can be extended to an isomorphism $K \xrightarrow{\sim} L$ if and only if there exists a bijection $\phi : \mathcal{P}_K \to \mathcal{P}_L$ such that for all $\mathfrak{p} \in \mathcal{P}_K$ we have

A. $\Psi(1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}) = 1 + \phi(\mathfrak{p})\mathcal{O}_{\phi(\mathfrak{p})}$; and

B. $v_{\phi(\mathfrak{p})} \circ \Pi_{\phi(\mathfrak{p})} = v_\mathfrak{p} \circ \Pi_\mathfrak{p} \circ \Psi$. ◁

Proof. The proof for function fields is a combination of Lemmas 8–11 of [Uch77], while the proof for number fields is Theorem D of [Hos14]. ❐

It turns out that these condition indeed hold for the Ψ that we have constructed. From this we obtain the following result:

Corollary 11.1.7. Suppose the equivalent statements hold for two global function fields K and L. Then $K \cong L$. ◁

Proof. Lemma 11.4 of [CLM16]. ❐

With these results we have proven that we have indeed found a two sets of objects associated to a global field K that determine K uniquely. Moreover, using class field theory, these objects are describable using only objects within K itself. This concludes the chapter and subsequently the thesis.

BIBLIOGRAPHY

[AS12] Athanasios Angelakis and Peter Stevenhagen. "Imaginary quadratic fields with isomorphic abelian Galois groups." In: *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium* (2012). DOI: 10.2140/obs.2013.1.21. eprint: arXiv:1209.6005.

[AT08] E. Artin and J.T. Tate. *Class Field Theory*. AMS Chelsea publishing. 2008.

[Bro13] Tim Browning. *Local Fields*. 2013. URL: https://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/local_fieldstcc.pdf.

[Cai10] Bryden R. Cais. *Local field extensions*. 2010. URL: http://math.arizona.edu/~cais/Prelim/LocalFieldExt.pdf.

[CF67] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, 1967.

[CLM16] Gunther Cornelissen, Xin Li, and Matilde Marcolli. *Class field theory and dynamical systems*. 2016.

[Gas26] Fritz Gassmann. "Bemerkungen zur vorstehenden Arbeit von Hurwitz: Uber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppen." In: *Mathematische Zeitschrift* 25 (1926), pp. 124–143.

[Gre11] Ralph Greenberg. *The primitive element theorem*. 2011. URL: https://www.math.washington.edu/~greenber/MATH404-PrimElem.pdf.

[Hos14] Yuichiro Hoshi. "On the Field-theoreticity of Homomorphisms Between the Multiplicative Groups of Number Fields." In: *Publ. RIMS Kyoto University* 50 (2014), pp. 269–285. URL: http://www.kurims.kyoto-u.ac.jp/~yuichiro/the_field-theoreticity_of_homomorphisms.pdf.

[Iva13] Alexander Ivanov. *On a generalization of the Neukirch-Uchida theorem*. 2013. eprint: arXiv:1309.3046.

[Loo53] Lynn H. Loomis. *An Introduction To Abstract Harmonic Analysis*. D. Van Nostrand Company Inc., 1953.

[Mil14] James S. Milne. *Algebraic Number Theory (v3.06)*. 2014, p. 164. URL: www.jmilne.org/math/.

[Mil13] J.S. Milne. *Class Field Theory (v4.02)*. 2013, pp. 281+viii. URL: www.jmilne.org/math/.

[Mor14] Patrick J. Morandi. *Dedekind Domains*. 2014. URL: https://www.math.nmsu.edu/~pmorandi/math601f01/DedekindDomains.pdf.

[Neu86] Jürgen Neukirch. *Class field theory*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1986. ISBN: 9783540152514. URL: https://books.google.nl/books?id=5%5C_vuAAAAMAAJ.

[NS99] Jürgen Neukirch and Norbert Schappacher. *Algebraic number theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1999. ISBN: 3-540-65399-6. URL: http://opac.inria.fr/record=b1094281.

[PRR93] V. Platonov, A. Rapinchuk, and R. Rowen. *Algebraic Groups and Number Theory*. Pure and Applied Mathematics. Elsevier Science, 1993. ISBN: 9780080874593. URL: https://books.google.nl/books?id=NpVdWdFq5YMC.

[Poo12] Bjorn Poonen. *A brief summary of the statements of class field theory*. 2012. URL: http://www-math.mit.edu/~poonen/papers/cft.pdfl.

[Rie06] Emily Riehl. *Lubin-Tate Formal Groups and Local Class Field Theory*. 2006. URL: http://www.math.jhu.edu/~eriehl/seniorthesis.pdf.

[Rot99] J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1999. ISBN: 9780387942858. URL: https://books.google.nl/books?id=lYrsiaHSHKcC.

[Sch12] Anthony J. Scholl. *Extensions of local fields*. 2012. URL: https://www.dpmms.cam.ac.uk/~ajs1005/ANT/notes_s3-4.pdf.

[Ser95] J.P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995. ISBN: 9780387904245. URL: https://books.google.nl/books?id=DAxlMdw%5C_QloC.

[Smi04] Tara L. Smith. *More On Galois Extensions*. 2004. URL: https://math.uc.edu/~tsmith/math612/moregalois.pdf.

[Sta12] StackExchange. *Why is the restricted direct product topology on the idele group stronger than the topology induced by the adele group?* 2012. URL: https://math.stackexchange.com/questions/145432/why-is-the-restricted-direct-product-topology-on-the-idele-group-stronger-than-t.

[Ste04] William Stein. *A brief introduction to Classical and Adelic Algebraic Number Theory*. 2004. URL: http://wstein.org/129/ant/html/node1.html.

[Uch77] Koji Uchida. "Isomorphisms of Galois Groups of Algebraic Function Fields." In: *Annals of Mathematics* 106.3 (1977), pp. 589–598. ISSN: 0003486X. URL: http://www.jstor.org/stable/1971069.

[Zho11] Yongcheng Zhou. *Equivalence of Norms in Finite Dimension*. 2011. URL: http://www.math.colostate.edu/~yzhou/course/math560_fall2011/norm_equiv.pdf.