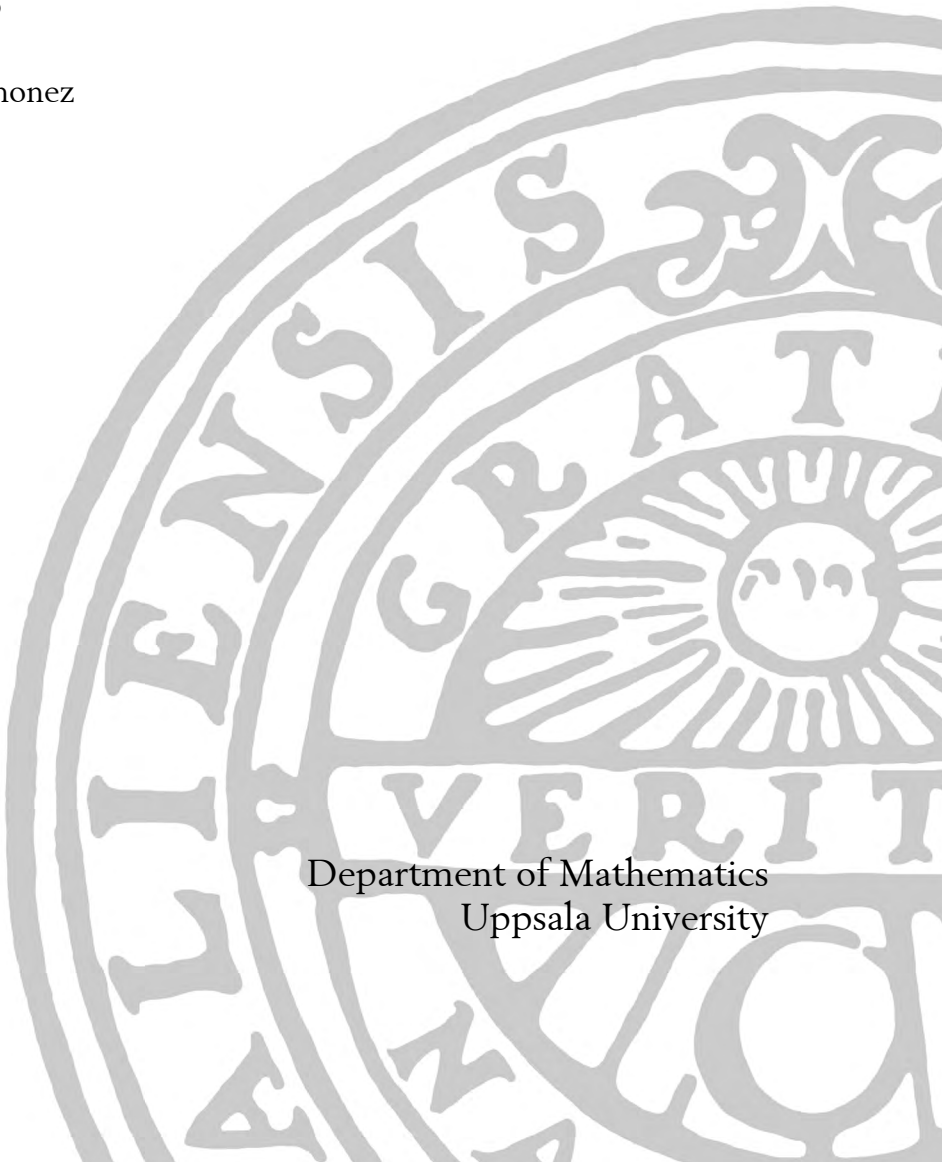
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2019:52

Profinite Groups and Infinite Galois Extensions

Jonatan Lindell

Examensarbete i matematik, 15 hp
Handledare: Martin Herschend
Examinator: Veronica Crispin Quinonez
November 2019



Department of Mathematics
Uppsala University

Abstract. In the 1930's Wolfgang Krull extended the fundamental theorem of Galois theory to infinite Galois extension via introducing a topology on the Galois group. This gave a correspondence between closed subgroups and intermediate fields. The aim of this thesis is to show that every Galois group is a profinite group, use this to prove the theorem of Krull and lastly as well show that every profinite group can be realised as a Galois group of a Galois extension.

Contents

1. Introduction

The modern version of Galois theory as the study of field extension and automorphism groups was first developed by Emil Artin from earlier work going back to several authors, including Everisté Galois [5]. One of the most important theorems, if not the most important theorem, of Galois theory is the fundamental theorem of finite Galois extension which gives a bijective correspondence between intermediate field extensions of a finite field extension and the subgroups of the Galois group of the extension. This is important as it allows us to use group-theoretical tools to study certain field extensions.

During the 1930's Krull extended the fundamental theorem of Galois theory to infinite Galois extension using topology. The aim of this thesis is to give a proof of the theorem that Krull proved and to give a connection between profinite groups and Galois groups. To do this we will give an introduction of Galois theory, starting from group theory and ring theory. We will then give a condensed introduction to topology as well as an introduction to topological groups. Followed by this we will give an introduction to profinite groups and give a characterisation of profinite groups. Lastly we will connect profinite groups to Galois groups and prove Krull's theorem.

We will assume basic knowledge of set theory. Both the introduction to topology and Galois theory we will be quite terse, so therefore it will be helpful to have some familiarity with basic topology and basic algebra, though not formally needed.

2. Conventions

Here we will quickly repeat some definitions from set theory to make sure that we are all on the same page. For this section we will basically follow [3].

We will denote that A is a subset of or equal to B by $A \subseteq B$. If A is a subset of B that is not equal to B we say that A then is a *proper subset* and denote this by $A \subsetneq B$.

Definition 2.0.1. Let A and B be two sets, then we define a *map* f between A and B to be a subset of $A \times B$ such that for all $a \in A$ there exists one pair (a, b) such that $(a, b) \in f$. We denote $(a, b) \in f$ by $f(a) = b$. If f is a map from A to B we write $f : A \to B$. We will use map, function and morphism interchangeably. If $f : A \to B$ and $g : B \to C$ are maps, then we define the composition of f with g as the set

$$\{(a, d) \in A \times C \mid \text{There exists } (a, b) \in f \text{ and } (c, d) \in g \text{ such that } b = c\}. \tag{1}$$

We denote the composition $g \circ f$.

We will use "$a \mapsto b$" to denote that a function maps a to b.

Definition 2.0.2. Let A and B be sets and let $f : A \to B$ be a map. Then

(a) f is *surjective* if for all $b \in B$ there exists a $a \in A$ such that $f(a) = b$;
(b) f is *injective* if for all $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, we have that $a_1 = a_2$.
(c) f is *bijective* if it is surjective and injective.

Definition 2.0.3. Let A be a set and let $f : A \to A$ be a map. Then we say that f is an *endomorphism*. If f is also bijective we say that f is an *automorphism*.

Proposition 2.0.4. *Let A and B be sets and let $f : A \to B$ be a bijective map. Then $g = \{(b, a) \mid (a, b) \in f\}$ is a map and $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$.*

Proof. It follows from that f is surjective that for every $b \in B$ there exists a pair $(b, a) \in g$. It also follows from that f is injective that there exists only one such pair for each $b \in B$. Thus g is a map. That $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$ follows from the definition of composition of maps. □

Definition 2.0.5. Let A and B be sets and let $f : A \to B$ be a bijective map. We then define the *inverse* of f to be the map define in the above proposition. We denote the inverse of f by f^{-1}.

Definition 2.0.6. Let A, B, C, D be sets and let $f : A \to C$ and let $g : B \to D$. Then we define the *product map* of f, g from $A \times B \to C \times D$ to be the map defined by $(a, b) \mapsto (f(a), g(b))$. We denote this map $f \times g$.

Definition 2.0.7. Let A and B be two sets, we say that A and B are *isomorphic* if there exists maps $f : A \to B$ and $g : B \to A$ such that $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$. We denote this $A \cong B$.

Proposition 2.0.8. *Let A and B be sets. Then $A \cong B$ if and only if there exists a bijective map $f : A \to B$.*

Proof. Assume that $A \cong B$. Then by definition there exists $f : A \to B$, $g : B \to A$ such that $g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$. We aim to show that f is bijective. Firstly f is surjective as if $b \in B$, then for $a = g(b)$, we get that $f(a) = b$ as $f \circ g = \mathsf{id}_B$. Secondly f is injective as if $f(a_1) = f(a_2)$ then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$ as $g \circ f = \mathsf{id}_A$. Thus f is bijective. Conversely assume f is bijective. Then the result follows by Proposition 2.0.4. □

Definition 2.0.9. A commutative diagram is a collection of objects and morphisms such that for any path (morphism seen as directed edges) between any two objects the compositions of the morphisms in the respective paths are equal.

This is much easier understood by seeing an example.

Example 2.0.10. Let $A = \mathbb{N}$, $B = \mathbb{Z}$, $C = \mathbb{R}$ and $D = \mathbb{C}$. Let f be function defined by $x \mapsto x^2$, g the function defined by $x \mapsto x^3$, h the function defined by $x \mapsto x^6$ and j the function defined by $x \mapsto x$. We say that the following diagram commutes as $g \circ f = j \circ h$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{j} & D \end{array}$$

3. Groups and Rings

Here we will give a short introduction to basic group and ring theory. The proofs and exposition will follow Chapters I, II and III in [4].

3.1. Group Theory.

Definition 3.1.1. A *group* is a set G together with a map $\cdot : G \times G \to G$, called multiplication, such that the following condition are fulfilled.

(a) There exists a element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$. We call such an element the identity element. This element is unique.
(b) For all $a, b, c \in G$, we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(c) For all $a \in G$ there exists a element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. We call a^{-1} the inverse element of a.

We often denote a group by only its underlying set. We will also often write ab instead of $a \cdot b$.

One geometric way to think about a group is that is describe the symmetries of an object. For example if we take the set of all reflective and rotational symmetries of triangle we get a group. We define the operation on this group as composition of these operation.

Example 3.1.2. Here are some examples of groups.

(a) The set $\mathbb{Z}$ with the operation $\cdot$ defined as addition.

(b) The set $\mathbb{Q} \setminus \{0\}$ with the operation $\cdot$ defined as usual multiplication.
(c) The set $\mathbb{R} \setminus \{0\}$ with the operation defined likewise.
(d) The set of $n \times n$ invertible matrices, with operation being matrix multiplication.

Here are two examples of things that are not groups.

(a) The set $\mathbb{Z}$ with the operation being defined as usual multiplication.
(b) The set of $n \times n$ matrices with the operation being defined as matrix multiplication.

Definition 3.1.3. Let $(G, \cdot)$ be a group. If for all $a, b \in G$, $a \cdot b = b \cdot a$ holds, then we say that the group is *abelian* (after Niels Henrik Abel) and we often denote $\cdot$ by $+$ and the identity by 0 instead.

Definition 3.1.4. A *subgroup* of a group G is a non-empty subset $H \subseteq G$ such that H is closed under multiplication and inverses. We denote this by $H \leq G$.

We say that a subgroup is trivial if it only consists of the identity element.

The following proposition is often easier and quicker to use than the definition.

Proposition 3.1.5. *Let G be a group, and $H \subseteq G$ be a subset of G. Then H is a subgroup of G if and only if for all $a, b \in H$ it holds that $ab^{-1} \in H$ and $H \neq \emptyset$.*

Proof. Assume that H is a subgroup of G. Then H is by definition closed under inverse and thus for all $a \in H$, $a^{-1} \in H$. Therefore we have that, as H is closed under products, that for all $a, b \in H$, $ab^{-1} \in H$. By definition H is also non-empty. Conversely assume that for all $a, b \in H$ that $ab^{-1} \in H$. Then we have that $e \in H$ as $aa^{-1} = e$ and by assumption $aa^{-1} \in H$. Therefore we also have that $a^{-1} \in H$ for all $a \in H$ by assumption as $a^{-1} = ea^{-1}$. Therefore it remains to show that H is closed under products, but this follows as $ab = a(b^{-1})^{-1}$ for all $a, b \in H$. □

The following definition we will need for two important concepts, normal subgroups and quotient groups.

Definition 3.1.6. Let G be a group and let H be a subgroup. We then define

(a) a *left-coset* of H to be the set $aH = \{ah \mid h \in H\}$ for some $a \in G$;
(b) a *right-coset* of H to be the set $Ha = \{ha \mid h \in H\}$ for some $a \in G$.

Now we can define what we mean by a normal subgroup.

Definition 3.1.7. Let G be a group and let $N \leq G$ be a subgroup. We then say that N is *normal* if for all $g \in G$, $gN = Ng$. We denote this by $N \trianglelefteq G$.

Note that if a group is abelian then every subgroup is normal. We also have the following proposition regarding normal subgroups.

Proposition 3.1.8. *Let G be a group and let H be a subgroup G. Then H is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.*

Proof. Note that $gNg^{-1} \subseteq N$ for all $g \in G$ is equivalent to that $g^{-1}Ng \subseteq N$ for all $g \in G$. We first prove the if direction. Assume that $gNg^{-1} \subseteq N$ for all $g \in G$. Then let $gn \in gN$, then $gng^{-1} = n'$ for some $n' \in N$, thus $gn = n'g$ and therefore $gn \in Ng$. Conversely let $ng \in Ng$ then $g^{-1}ng = n'$ for some $n' \in N$, therefore $ng = gn'$ and thus $ng \in gN$. Therefore $gN = Ng$ for all $g \in G$. We now prove the only if direction. Assume that $gN = Ng$ for all $g \in G$. Then let $gng^{-1} \in gNg^{-1}$. Then $gn = n'g$ for some $n' \in N$ and thus $gng^{-1} = n' \in N$. Therefore $gNg^{-1} \subseteq N$ for all $g \in G$. □

Next we will define what a morphism of groups is.

Definition 3.1.9. Let G and H be two groups. A *group morphism* $f : G \to H$ is map such that for all $a, b \in G$, $f(ab) = f(a)f(b)$.

The following properties of group morphisms are easily verified.

Lemma 3.1.10. *Let $f : G \to H$ be a group morphism. Then the following is true.*

(a) $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$.
(b) $f(e_G) = e_H$.

Next we define two important subsets connected to morphisms.

Definition 3.1.11. Let G and H be groups, and let $f : G \to H$ be a group morphism.

(a) The kernel of a morphism is the set of elements that gets map to the identity element. We denote this by $\mathsf{ker}(f) = \{g \in G \mid f(g) = e_H\}$.
(b) The image of a morphism is the set of elements that lie in the set $f(G)$. We denote this by Let $\mathsf{im}(f) = \{h \in H \mid \text{There exists a } g \in G \text{ such that } f(g) = h\}$.

Note that a morphism is surjective if and only if the image of the morphism is the whole group. Note also that a morphism is injective if and only if the kernel is trivial.

Proposition 3.1.12. *Let G and H be groups, and let $f : G \to H$ be a group morphism. Then the following is true.*

(a) $\mathsf{ker}(f)$ *is a normal subgroup of* G.
(b) $\mathsf{im}(f)$ *is subgroup of* H.

Proof. We begin by proving (a). We start by showing that $\mathsf{ker}(f)$ is a subgroup. By Proposition 3.1.5 we only need to show that $\mathsf{ker}(f)$ is nonempty and that for all $a, b \in \mathsf{ker}(f)$ we have that $ab^{-1} \in \mathsf{ker}(f)$. That the kernel is nonempty follows by Lemma 3.1.10 as $f(e_G) = e_H$. Now let $a, b \in \mathsf{ker}(f)$. Then, by Lemma 3.1.10, we have that $f(ab^{-1}) = f(a)f(b)^{-1} = e \cdot e^{-1} = e$. Therefore, as $a, b \in \mathsf{ker}(f)$ were arbitrary, it follows that $\mathsf{ker}(F)$ is a subgroup of G. To show that $\mathsf{ker}(f)$ is normal we will use Proposition 3.1.8. Let $g \in G$ and $n \in \mathsf{ker}(f)$ be arbitrary. Then $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = f(g)ef(g)^{-1} = e$ and thus it follows that $gng^{-1} \in \mathsf{ker}(f)$ for all $g \in G$ and all $n \in \mathsf{ker}(f)$. Therefore $\mathsf{ker}(f)$ is normal.

We now prove (b). That $\mathsf{im}(f)$ is nonempty follows directly from the definition. Let $a, b \in \mathsf{im}(f)$, then there exists $a', b' \in G$ such that $a = f(a')$ and $b = f(b')$. Note that $ab^{-1} \in \mathsf{im}(f)$ as $a'b'^{-1} \in G$ and $f(a'b'^{-1}) = f(a')f(b')^{-1} = ab^{-1}$. Therefore $\mathsf{im}(f)$ is a subgroup of H. □

Next we define a concept that we will need briefly for the Galois theory in later sections.

Definition 3.1.13. Let G be a group and let H_1 and H_2 be subgroups of G. We then say that H_1 is conjugate to H_2 if there exists an element $g \in G$ such that $gH_1g^{-1} = H_2$.

Note that normal subgroups only have one conjugate, itself.

Proposition 3.1.14. *Let G be a group and let H be a subgroup of G. Then the number of right cosets of H are equal to the number of left cosets of H.*

For a proof see Proposition 3.12 in Chapter I, section 3 of [4].

Thus by knowing this, we know that it doesn't matter if we choose the left or right cosets for the following definition.

Definition 3.1.15. Let G be a group and let H be a subgroup. The *index* of H is the number of left cosets.

We can now finally define what a quotient group is.

Proposition 3.1.16. *Let G be an group and let N be a normal subgroup. Then we define G/N to be the set of all left-cosets $G/N = \{aN \mid a \in G\}$ and endow it with the operation defined as follows, $aN \cdot bN = abN$. Then G/N is a group.*

For a proof of this see Proposition 4.7 in Chapter I, section 4 of [4].

Definition 3.1.17. We call G/N, defined as above, the *quotient group* of G by N.

One way to think about quotient group is that we take away everything that we don't want, so to speak, i.e. that lying in N. Note that $xN = yN$ if and only if $y^{-1}x \in N$. Therefore we could also have define the quotient group via the equivalence relation $x \sim y$ if $y^{-1}x \in N$.

The following two theorems were first proved by Emmy Noether in 1927 for modules [9]. Especially the first theorem here we will be very important and often used for the rest of thesis.

Theorem 3.1.18 (First isomorphism theorem)**.** *Let $f : G \to H$ be a group morphism, then there exists a isomorphism $\tilde{f} : G/\mathsf{ker}(f) \to \mathsf{im}(f)$ defined by $a\mathsf{ker}(f) \mapsto f(a)$. In particular if f is surjective then $G/\mathsf{ker}(f) \cong H$.*

Proof. We first prove that $\tilde{f}$ is well defined. Note that $a\mathsf{ker}(f) = b\mathsf{ker}(f)$ is equivalent to that $ab^{-1} \in \mathsf{ker}(f)$. Let $a\mathsf{ker}(f) = a'\mathsf{ker}(f)$, then $f(aa'^{-1}) = e_H$ which implies that $f(a) = f(a')$. Hence $\tilde{f}$ is well defined. Next we prove that $\tilde{f}$ is group morphism. Let $a\mathsf{ker}(f), b\mathsf{ker}(f) \in G/\mathsf{ker}(f)$, then $\tilde{f}((ab)\mathsf{ker}(f)) = f(ab) = f(a)f(b) = \tilde{f}(a\mathsf{ker}(f)) + \tilde{f}(b\mathsf{ker}(f))$. By definition we have that $\tilde{f}$ is surjective, thus we only need to prove injectivity. Assume that $f(a) = f(b)$ then this implies that $f(ab^{-1}) = e_H$. Therefore $ab^{-1} \in \mathsf{ker}(f)$ and thus $a\mathsf{ker}(f) = b\mathsf{ker}(f)$. □

Next we prove the second isomorphism, which says that in some cases we can treat quotients as usual division.

Theorem 3.1.19 (Third isomophism theorem)**.** *Let G be a group and let H be a normal subgroup, and let N be a normal subgroup of H. Then H/N is a normal subgroup of G/N and $(G/N)/(H/N) \cong (G/H)$.*

Proof. Let $aN \in H/N$ then $gNaNg^{-1}N = gag^{-1}N \in H/N$. Therefore by Proposition 3.1.8 H/N is a normal subgroup of G/N. Define $f : G/N \mapsto G/H$ by $aN \mapsto aH$. To see that it well defined note that if $ab^{-1} \in N$ then $ab^{-1} \in H$ as $N \subseteq H$. Next we show that f is a group morphism. We have that $f((ab)N) = (ab)H = abH = f(a)f(b)$. Thus f is a group morphism. Note that $\mathsf{ker}(f) = \{aN \in G/N \mid a \in H\} = H/N$ and that f is surjective. Therefore we get by Theorem 3.1.18 that $(G/N)/(H/N) \cong (G/H)$. □

3.2. **Ring Theory.** Now we will give some basic results in ring theory.

Definition 3.2.1. A *ring* is a three tuple $(R, +, \cdot)$ of a set R, an operation $+ : R \times R \to R$ and a operation $\cdot : R \times R \to R$ such that $(R, +)$ is abelian group, with the identity element denoted by 0, and such that the following condition are fulfilled.

(a) For all $a, b, c \in R$, we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(b) There exists a element $1 \in R$, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
(c) For all $a, b, c \in R$, we have that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
(d) For all $a, b, c \in R$, we have that $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

We will, as with groups, often denote a ring only by its underlying set. We will also often write ab instead of $a \cdot b$. We call the operation $+$ addition and the operation $\cdot$ multiplication. The identity of element of $+$ and $\cdot$ is called the additive, respectively multiplicative, identity element. We say that a ring is commutative if $ab = ba$ for all $a, b \in R$.

Example 3.2.2. Here we give some examples of rings.

(a) $(\mathbb{Z}, +, \cdot)$ with addition and multiplication defined as usual is a ring.
(b) $(\mathbb{Q}, +, \cdot)$ with addition and multiplication defined likewise.
(c) The set of all $n \times n$ matrices with addition and multiplication defined as usual is a ring.

We will from now on assume that all rings are commutative. We next define what a subring is.

Definition 3.2.3. Let $(R, +, \cdot)$ be a ring. A *subring* $(A, +, \cdot)$ of R is subset $A \subseteq R$ such that following conditions are fulfilled.

(a) $(A, +)$ is subgroup of $(R, +)$.
(b) $(A, +, \cdot)$ is closed under multiplication and it contains the multiplicative identity element 1.

Example 3.2.4. For example $(\mathbb{Q}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$.

Now we define the corresponding notation of normal subgroups but for rings.

Definition 3.2.5. Let R be a ring and let $I \subseteq R$ be a subset. We call I an *ideal* if $(I, +)$ is a subgroup of $(R, +)$ and $rI \subseteq I$ for all $r \in R$. We say that an ideal is *proper* if $I \subsetneq R$.

We define what a ring morphism is.

Definition 3.2.6. Let R, S be rings and let $\varphi : R \to S$. We then say that $\varphi : R \to S$ is a ring morphism the following condition are fulfilled.

(a) The map $\varphi : (R, +) \to (S, +)$ is a group morphism.
(b) For all $r_1, r_2 \in R$, $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$.
(c) $\varphi(1_R) = 1_S$.

Likewise as we define the kernel and image of a group morphism we can define the kernel and image of a ring morphism.

Definition 3.2.7. Let R and S be rings and let $\varphi : R \to S$ be a ring morphism. Then we define

(a) the *kernel* of φ to be the set $\mathsf{ker}(\varphi) = \{r \in R \mid \varphi(r) = 0\}$;
(b) the *image* of φ to be the set $\mathsf{im}(\varphi) = \{s \in S \mid \text{There exists a } r \in R \text{ such that } \varphi(r) = s\}$.

Proposition 3.2.8. *Let R and S be a rings and let $\varphi : R \to S$ be a ring morphism. Then*

(a) $\mathsf{ker}(\varphi)$ is an ideal of R;
(b) $\mathsf{im}(\varphi)$ is a subring of S.

Proof. We first prove that the kernel of R is an ideal. We know by Proposition 3.1.12 that $(\mathsf{ker}(\varphi), +)$ is a subgroup of $(R, +)$. Thus we only need to show that $r\mathsf{ker}(\varphi) \subseteq \mathsf{ker}(\varphi)$ for all $r \in R$. Note that $\varphi(ra) = \varphi(r) \cdot 0 = 0$ for all $a \in \mathsf{ker}(\varphi)$. Thus we have that $r\mathsf{ker}(\varphi) \subseteq \mathsf{ker}(\varphi)$.

Now we prove that $\mathsf{im}(\varphi)$ is a subring of S. We know by Proposition 3.1.12 that $(\mathsf{im}(\varphi), +)$ is a subgroup of $(S, +)$. Thus it remains to show that $1 \in \mathsf{im}(\varphi)$ and that if $a, b \in \mathsf{im}(\varphi)$ then $ab \in \mathsf{im}(\varphi)$. Firstly note that $1 \in \mathsf{im}(\varphi)$ as by definition $\varphi(1) = 1$. Next let $a, b \in \mathsf{im}(\varphi)$ then there exists $a', b' \in R$ such that $\varphi(a') = a$ and $\varphi(b') = b$. Thus $\varphi(a'b') = ab$ and therefore $ab \in \mathsf{im}(\varphi)$. □

Like we can quotient groups by normal subgroups, we can quotient rings by ideals.

Proposition 3.2.9. *Let R be a ring and let I be an ideal. Let S be the quotient group $(S, +)$ given by R/I, seeing I as a normal subgroup, with multiplication defined as $(a+I)(b+I) = ab+I$. Then S is a ring.*

For a proof of this see Proposition 3.3 in section 3 of Chapter III in [4].

Definition 3.2.10. Let R be a ring and let I be an ideal. We define the *quotient ring* of R by I to be the ring S in the above proposition. We denote this R/I.

Now we will prove the first isomorphism theorem for rings. Like the one for groups this will be very important for the rest of the thesis.

Theorem 3.2.11 (First Isomorphism Theorem)**.** *Let $\varphi : R \to S$ be a ring morphism. Then $R/\ker(\varphi) \cong \mathsf{im}(\varphi)$, with the isomorphism given by $a\ker(\varphi) \mapsto \varphi(a)$.*

Proof. We know by Theorem 3.1.18 that we have isomorphism $\tilde{f}$ of the underlying additive groups given by $a + \ker(\varphi) \mapsto \varphi(a)$. Thus if we can show that this is also a ring morphism we will be done. Let $a+\ker(\varphi), b+\ker(\varphi) \in R/\ker(\varphi)$, then $\tilde{f}((a+\ker(\varphi))(b+\ker(\varphi))) = \tilde{f}((ab)+\ker(\varphi)) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{f}(a+\ker(\varphi))\tilde{f}(b+\ker(\varphi))$. Thus it remains to show that $\tilde{f}(1+\ker(\varphi)) = 1$ but this is true as $\tilde{f}(1+\ker(\varphi)) = \varphi(1) = 1$. □

In the rest of this subsection we will describe several important properties and types of rings. We begin with one of the most basic (in the sense that it pops up often).

Definition 3.2.12. Let $R \neq \{0\}$ be a ring. Then we say that R is an *integral domain* if R for all $a, b \in R$ we have that $ab = 0$ implies that either $a = 0$ or $b = 0$.

Another way of phrasing this definition is that there aren't two non-zero element such that the product of these two elements are zero.

Example 3.2.13. We now give one example of a field that is not an integral domain and of one that is.

(a) Let $\mathbb{Z}/12\mathbb{Z}$ be the ring of all integers modulo 12. Then $6 \cdot 2 = 0 \bmod 12$ but $6 \neq 0$ and $2 \neq 0$. Therefore $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain.
(b) Let $\mathbb{Z}$ be the ring of all integers, then this is integral domain.

Next we define elements that have multiplicative inverses.

Definition 3.2.14. Let R be a ring and let $a \in R$. We then say that a is a *unit* if there exists an element $r \in R$ such that $ar = ra = 1$. We denote the set of all units of ring by R^*.

Next we generalise the notation of divisors, prime and irreducible from the natural numbers.

Definition 3.2.15. Let R be a integral domain. We say that an element $a \in R$ *divides* an element b if $b = ac$ for some $c \in R$. We denote this $a|b$. We say that a non-unit p is

(a) *prime* if $p|ab$ implies that $p|a$ or $p|b$ for all $a, b \in R$;
(b) *irreducible* if $p = ab$ implies that a or b is a unit for all $a, b \in R$.

Now we can generalise the notation of prime elements to ideals.

Definition 3.2.16. Let R be a ring and let $I \subset R$ be a proper ideal. We say that I is a *prime ideal* if for all $ab \in I$ implies that either $a \in I$ or $b \in I$.

Definition 3.2.17. Let R be a ring and let $I \subseteq R$ be an proper ideal. We say that I is a *maximal ideal* if there exists no proper ideal J such that $I \subsetneq J$.

We will now define two important types of rings, principal ideal domains and unique factorisation domains. Both of these properties generalise in some sense the properties of $\mathbb{Z}$. Principal ideal domains are rings where every ideal is generated by one element, and unique factorisation domains are rings where every element can be factorised uniquely into irreducible elements.

Definition 3.2.18. Let R be a ring and let I be an ideal of R. We say that I is a *principal ideal* if $I = Ra = \{ra \mid r \in R\}$ for some fixed $a \in R$. We then say that I is generated by a and denote this as $I = (a)$.

Definition 3.2.19. Let R be an integral domain. We say that R is a *principal ideal domain*, shortened *PID*, if every ideal of R is principal.

The following is an important property of PIDs.

Proposition 3.2.20. *Let R be a PID. Then every non-trivial prime ideal is a maximal ideal.*

For a proof of this see Proposition 8.3 in section 8 of Chapter III in [4].

Definition 3.2.21. Let R be an integral domain. We say that R is a *unique factorization domain*, shortened *UFD*, if every non-zero element can be written uniquely on the form $up_0^{k_0}p_1^{k_1}...p_n^{k_n}$, where u is a unit and $p_0, ..., p_n$ are irreducible elements of R and $k_i \in \mathbb{N}$. More precisely by uniquely we mean that if $up_0^{k_o}...p_n^{k_n} = vq_0^{l_0}...q_m^{l_m}$ then $n = m$ and up to reordering $Rp_i = Rq_i$ for all i.

The following proposition says that in a UFD there is no difference between being irreducible and being prime.

Proposition 3.2.22. *Let R be a UFD and let $a \in R$. Then a is irreducible if and only if a is prime.*

For a proof of this see Proposition 10.2 in section 10 of Chapter III in [4].

The following theorem allows us to in one direction connect the two concepts.

Theorem 3.2.23. *Every PID is a UFD.*

For a proof of this see Theorem 8.4 in section 8 of Chapter III in [4].

If we draw a diagram of the different types of rings we get the following.

Rings (not necessarily commutative) $\supseteq$ Commutative Rings $\supseteq$ Integral Domains $\supseteq$ UFDs $\supseteq$ PIDs

Next we generalise the notation of polynomials by letting the coefficients lie in an arbitrary ring, instead of just being real numbers as when one often first encounters them.

Proposition 3.2.24. *Let R be a ring. Let S be sets consisting of elements of the form $r_0 + r_1x + r_2x^2 + ... + r_nx^n$ where $r_0, ..., r_n \in R$, $n \in \mathbb{N}$ and x is an indeterminant. Define addition between the elements the following way*

$$(r_0 + ... + r_nx^n) + (s_0 + ... + s_mx^m) = q_0 + ... + q_kx^k$$

where $k = \mathsf{max}\{n, m\}$, $q_i = r_i + s_i$ and where we define $r_i = 0$ if $i > n$ and $s_i = 0$ if $i > m$. Define multiplication between the elements the following way

$$(r_0 + ... + r_nx^n)(s_0 + ... + s_mx^m) = q_0 + ... + q_kx^k$$

where $k = n + m$, $q_i = r_0s_i + r_1s_{i-1} + ... + r_{i-1}s_1 + r_is_0$ and where we define $r_i = 0$ if $i > n$ and $s_i = 0$ if $i > m$. Then this is a ring.

For a proof of this see Proposition 5.1 in section 5 of Chapter III in [4].

Definition 3.2.25. Let R be a ring. We define the *polynomial ring* of R to be the ring define in the above proposition. We denote this ring $R[x]$.

Proposition 3.2.26. *Let $\varphi : R \to S$ be a ring morphism, then this induces a ring morphism $f_\varphi : R[x] \to S[x]$ defined by $f_\varphi(a_nx^n + ... + a_0) = \varphi(a_n)x^n + ... + \varphi(a_0)$. If q is a polynomial in $R[x]$ then we denote the image of q under f_φ by q_φ.*

Proof. Let $a = a_0 + ... + a_n x^n, b = b_0 + ... + b_m x^m \in R[x]$ be given. Then

$$f_\varphi(a+b) = f_\varphi(q_0 + ... + q_k x^k) = \varphi(q_0) + ... + \varphi(q_k)x^k = f_\varphi(a) + f_\varphi(b)$$

where $k = \mathsf{max}\{n, m\}$, $q_i = a_i + b_i$ and where $a_i = 0$ if $i > n$ and $b_i = 0$ if $i > m$. Likewise

$$f_\varphi(ab) = f_\varphi(s_0 + ... + s_k x^k) = \varphi(s_0) + ... + \varphi(s_k)x^k = f_\varphi(a)f_\varphi(b)$$

where $k = n + m$, $s_i = a_0 b_i + a_1 b_{i-1} + ... + a_{i-1}b_1 + a_i b_0$ and where $a_i = 0$ if $i > n$ and $b_i = 0$ if $i > m$. Note that $f_\varphi(1) = \varphi(1) = 1$. Thus f_φ is ring morphism. □

Next we have the following important theorem.

Theorem 3.2.27. *Let R be a ring. If R is a UFD then $R[x]$ is a UFD.*

For a proof of this see Theorem 10.4 in section 10 of Chapter III in [4].

4. Field Theory

Here we will study field extensions, mainly to get to Galois extensions. The proofs and exposition of this section will mainly follow Chapter IV and V in [4].

Definition 4.0.1. A *field* is a ring $(F, +, \cdot)$ such that $F^* = F \setminus \{0\}$.

We usually (that is the rest of the thesis) denote a field only by its underlying set. Intuitively one can think of a field as a set where we can add, subtract, multiply and divide numbers as usual. Note that the definition assures that a field has at least two elements.

Example 4.0.2. The following examples are fields

(a) The set of rational numbers $\mathbb{Q}$, where multiplication is normal multiplication and addition is normal addition.
(b) The set of real numbers $\mathbb{R}$, defined likewise.
(c) The set of complex numbers $\mathbb{C}$, defined likewise.
(d) $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number.

Definition 4.0.3. The *characteristic* of a field F is the smallest $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$. If no such n exists we say that the characteristic is zero.

Now we have the following proposition regarding rings that we will need for later propositions.

Proposition 4.0.4. *Let R be a ring and let $I \subseteq R$ be an ideal.*

(a) I is a prime ideal if and only if R/I is an integral domain.
(b) I is a maximal ideal if and only if R/I is a field.

Proof. We begin by proving (a). Assume that I is a prime ideal. Let $a+I, b+I \in R/I$ and assume that $ab + I = 0 + I$. This is equivalent to that $ab \in I$. But this implies that either $a \in I$ or $b \in I$ as I is prime. Assume without loss of generality that $a \in I$. Then we get that $a + I = 0 + I$. As a and b were arbitrary it follows that R/I is a integral domain. Conversely assume that R/I is a integral domain. Let $ab \in I$, then $ab + I = 0 + I$ in R/I and thus as R/I is an integral either $a + I = 0 + I$ or $b + I = 0$. But this implies that either a or b lie in I. Therefore, as a and b were arbitrary it follows that I is a prime ideal.

Next we prove (b). Assume that I is a maximal ideal. Then we need to show that every element is unit except zero. Let $a \in R/I$ be a non-zero elemnt. Then $Ra + I$ is an ideal of R containing I. This implies that $Ra + I = R$ as I is maximal. Therefore there exists $r \in R$ and $i \in I$ such that $ra + i = 1$. This implies that $(ra + i) + I = (ra) + I = (r + I)(a + I) = 1 + I$ and therefore $a + I$ is unit. Thus we get that R/I is a field. Conversely assume that R/I is a field and that J is an

ideal such that $I \subsetneq J \subseteq R$. Then there exists $a \in J \setminus I$ and therefore $a + I$ is a non-zero element in R/I. This implies that there exists $b + I \in R/I$ such that $(ab) + I = 1 + I$. This is equivalent to that $(1 - ab) \in I$ which implies that $(1 - ab) \in J$. Note also that $ab \in J$ as J is an ideal of R. Therefore we get that $ab + (1 - ab) = 1 \in J$ and thus $J = R$. Therefore I is maximal. □

Note that every field is a PID as the only ideals of a field F are (0) and F. We also have the following proposition.

Proposition 4.0.5. *Let F be a field, then $F[x]$ is PID.*

For a proof of this see Proposition 5.12 in section 5 of Chapter III in [4].
The following proposition will be often used later.

Proposition 4.0.6. *Let F be a field and let $f \in F[x]$ be a irreducible polynomial. Then (f) is a maximal ideal, and thus $F[x]/(f)$ is a field.*

Proof. Firstly by Proposition 4.0.5 we know that $F[x]$ is a PID. We also have by Theorem 3.2.23 that $F[x]$ is a UFD. Therefore we can conclude by Proposition 3.2.22 (f) is also a non-trivial prime ideal. Lastly it follows by Proposition 3.2.20 that (f) is a maximal ideal. Then $F[x]/(f)$ is a field by Proposition 4.0.4. □

We will now define what a field morphism is.

Definition 4.0.7. Let F and E be fields, a *field morphism* is a map
$\varphi : F \longrightarrow E$ such that $\varphi(1) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(a + b) = \varphi(a) + \varphi(b)$.

Note that this is the same as the definition of a ring morphism except that the domain and codomain of the map are now fields.

Proposition 4.0.8. *Every field morphism is injective.*

Proof. Let $\varphi : F \longrightarrow E$ be a field morphism. Then since F is a field, the only ideals of F are (0) or F. As $\ker(\varphi)$ is an ideal we have that $\ker(\varphi) = (0)$ as otherwise $\varphi(1) = 0$, hence φ is injective. □

Now we come to one of the most basic definitions of the thesis, namely field extensions.

Definition 4.0.9. A field extension of a field F is an field E such that $F \subseteq E$. We denote this E/F. The dimension of the field extension is the dimension of E as an vector spaces over F. We denote this by $[E : F]$. We say that a field extension E/F is finite if $[E : F] < \infty$

Example 4.0.10. The following are examples of field extensions

(a) For any field F, F itself is an extension of F and $[F : F] = 1$.
(b) $\mathbb{C}$ is an extension of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.
(c) The dimension of an extension can also be infinite e.g $\mathbb{R}$ is an infinite extension of $\mathbb{Q}$.

Proposition 4.0.11. *Let E/F be a field extension and let L be an intermediate field extension, $F \subseteq L \subseteq E$. Then $[E : F] = [E : L][L : F]$.*

Proof. Let $(\alpha_i)_{i\in I}$ be a basis for L/F and let $(\beta_j)_{j\in J}$ be a basis for E/L. Then every element in E can be written as a linear combination of β_j's, where in turn each term can be written as a linear combination of α_i's. More concretely if $a \in E$ then we know that $a = \sum_{j\in J} a_j\beta_j$, $a_j \in L$ and $\beta_j \in E$. In turn $a_j = \sum_{i\in I} b_{ij}\alpha_i$, $b_{ij} \in F$ and $\alpha \in L$. Thus $a = \sum_{(i,j)\in I\times J} b_{ij}(\alpha_i\beta_j)$. Thus we want to show that $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ forms a basis for E over F. That it spans E we have already established, thus we only need to show that it is linear independent. Assume that $\sum_{(i,j)\in I\times J} a_{ij}(\alpha_i\beta_j) = 0$ then this is equivalent to that $\sum_{j\in J}(\sum_{i\in I} a_{ij}\alpha_i)\beta_j = 0$, which implies that $\sum_{i\in I} a_{ij}\alpha_i = 0$, as $(\beta)_{j\in J}$ is linearly independent, which in turn implies that $a_{ij} = 0$ as $(\alpha_i)_{i\in I}$ is linearly independent. Thus $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is a basis for E over F. Therefore we have that $[E : F] = |I \times J| = |I||J| = [E : L][L : F]$. □

Definition 4.0.12. Let E/F and E/L be a field extensions. A *F-morphism* $\varphi : E \to L$ is a field morphism such that $f_{|F} = \mathsf{id}_F$.

We will now define two ways of constructing new fields that will be used often.

Proposition 4.0.13. *Let E be a field extension of F, and let $S \subseteq E$ be a subset of E. Then $F[S]$, generated by $F \cup S$, is the ring of linear combinations of finite powers of elements of S with coefficients in F. The field $F(S)$, generated by $F \cup S$, is the field of $ab^{-1} \in E$, $b \neq 0$, where $a, b \in F[S]$.*

For a proof of this see Proposition 1.9 in section 1 of Chapter IV in [4].

We can likewise define this for polynomials.

Proposition 4.0.14. *Let F be a field. Then we define the set*

$$F(x) = \{\frac{p}{q} \mid p, q \in F[x] \text{ and } q \neq 0\}/\sim$$

where the equivalence relation is given by $\frac{p}{q} \sim \frac{p'}{q'}$ if $pq' = p'q$. Then this is field where addition is defined by $\frac{p}{q} + \frac{p'}{q'} = \frac{pq'+qp'}{qq'}$ and where multiplication is defined by $\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$.

For a proof of this see Proposition 4.10 in section 4 of Chapter III of [4].

Definition 4.0.15. Let E be a field extension F. We say that E is *finitely generated* when $E = F(\alpha_0, ..., \alpha_k)$, for some $\alpha_i \in E$. If $E = F(\alpha)$, for some $\alpha \in E$, we say that E is a *simple* extension of F.

Note that every finite extension is finitely generated. One important meta-method is that when we have a finite extension $F(\alpha_1, ..., \alpha_n)/F$ we can build a tower of simple extension

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq ... \subseteq F_{n-1} \subseteq F_n = F(\alpha_1, ..., \alpha_n)$$

where we define $F_i = F_{i-1}(\alpha_i)$. The following proposition is important as it allows us to connect the degree of a simple extension to degree of a polynomial.

Proposition 4.0.16. *Let F be a field and let E be a field extension of F. Let $\alpha \in E$.*

(a) If $f(\alpha) \neq 0$ for all $f \in F[x]$ and then $F(\alpha) \cong F(x)$ for an indeterminant x.
(b) If $f(\alpha) = 0$ for some $f \in F[x]$ and then there exists a unique irreducible monic polynomial $g \in F[x]$ such that $g(\alpha) = 0$. Then $F(\alpha) \cong F[x]/(g)$, the degree of the extension is the degree of g, and $1, \alpha, \alpha^2, ..., \alpha^{deg(g)-1}$ forms a basis for $F(\alpha)$ over F. We also have that for any polynomial h such that $h(\alpha) = 0$ it is the case that $g|h$.

We denote the unique irreducible monic polynomial of an algebraic element $\alpha \in E$ determined by (b) by $\mathsf{irr}(\alpha : F)$. For a proof of this see Proposition 2.2 in section 2 of Chapter IV in [4].

4.1. **Algebraic Extensions.** Now we generalise the concept of algebraic numbers to arbritrary field extensions.

Definition 4.1.1. Let F be a field and let E be an extension of F. We say that $\alpha \in E$ is *algebraic* over F if there exists a polynomial $f \in F[x]$ such that $f(\alpha) = 0$. An extension E of F is *algebraic* if each element in E is algebraic over F.

Proposition 4.1.2. *Every finite extension is algebraic.*

Proof. Let E/F be a finite extension and assume that $[E : F] = n$. Let $\alpha \in E \setminus F$ be an arbitrary element. Consider $\{1, \alpha, \alpha^2, ..., \alpha^n\}$. Since this set contains $n + 1$ vectors it follows that the set must be linearly dependent and thus $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$ for some $a_0, ..., a_n \in F$. Now define $f(x) = a_0 + ... + a_n x^n$, then $f(\alpha) = 0$ and thus α is algebraic over F. As α was arbitrary it now follows that E/F is an algebraic extension. □

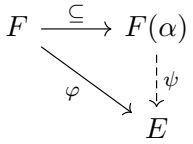
We now give some properties of algebraic extensions.

Proposition 4.1.3. *Assume that E/F is an algebraic extension, and let L be an intermediate field $F \subseteq L \subseteq E$. Then E/L and L/F are algebraic extensions if and only if E/F is an algebraic extension.*

Proof. First assume that E/F is algebraic and let $\alpha \in E$. Then there exists $f \in F[x]$ such that $f(\alpha) = 0$ and as $F[x] \subseteq L[x]$ we have that α is algebraic over L. Let $\beta \in L$ be given, then there exists $g \in F[x]$ such that $g(\beta) = 0$ as $L \subseteq E$. Thus β is algebraic over F.

Now conversely assume that E/L and L/F are algebraic extensions. Let $\alpha \in E$ be given. Then there exists a irreducible polynomial $f = a_0 + ... + a_n x^n \in L[x]$ such that $f(\alpha) = 0$. Then we have that α is algebraic over $K = F(a_0, ..., a_n)$. Therefore $K(\alpha)/K$ is an algebraic extension and $[K(\alpha) : F] = [K(\alpha) : K][K : F]$ by Proposition 4.0.11. By Proposition 4.0.16 we have that $[K(\alpha) : K] = \mathsf{deg}(f)$. Thus $[K(\alpha) : F]$ is finite. Hence by Proposition 4.1.2 we get that $K(\alpha)/F$ is algebraic and therefore α is algebraic over F. Thus, as α was arbitrary, E/F is algebraic. □

Proposition 4.1.4. *Let F and E be fields and let α be algebraic over F. Let $f = \mathsf{irr}(\alpha : F)$. If $\psi : F(\alpha) \to E$ is a field morphism and φ is a restriction of ψ to F, then $\psi(\alpha)$ is a root of f_φ in E. Conversely, for every field morphism $\varphi : F \to E$ and every root β of f_φ in E, there exists a unique field morphism $\psi : F(\alpha) \to E$ that extends φ and sends α to β.*



For a proof of this see Proposition 2.4 in section 2 of Chapter IV in [4].

Definition 4.1.5. Let F be a field, we then say that F is *algebraically closed* if it fulfills any of these following equivalent properties.

(a) The only algebraic extension of F is F itself.
(b) All irreducible polynomials are of degree 1.
(c) Every nonconstant polynomial in $F[x]$ has a root in F.

We now prove that these three properties actually are equivalent

Proof. We will start by proving that (a) implies (b). Let $p \in F[x]$ be an irreducible polynomial. Then $F[x]/(p)$ is an algebraic extension of F, since it is finite. By (a) the degree of the extension must be one and hence by Proposition 4.0.16 $\mathsf{deg}(p) = 1$.

We will now prove that (b) implies (c). Let $p \in F[x]$ be a polynomial of degree 1. Then $p(x) = ax+b$ for some $a, b \in F$ where $a \neq 0$. Then $(-b)a^{-1} \in F$ is a root of p. Therefore all polynomials of degree 1 has a root in F and since they are the only irreducible polynomials by (b), every non-constant polynomial has a root in F as $F[x]$ is a UFD.

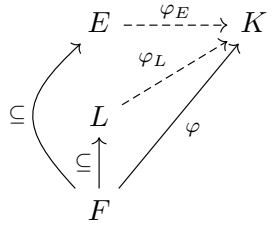
Finally we prove that (c) implies (a). Assume there exists an algebraic extension E/F other than F. Then $\alpha \in E$ is algebraic over F. Let $f = \mathsf{irr}(\alpha : F)$, then by (c) f must have a root $r \in F$. As f

is irreducible and monic it must be the case that $f = x - r$. Therefore, as $f(\alpha) = 0$, we have that $\alpha = r \in F$ and thus the only algebraic extension of F is F itself. □

The proof of the following theorem relies on Zorn's lemma. For proofs of the following theorems of this subsection see Theorem 4.2, Lemma 4.3 and Theorem 4.4 in section 4 of Chapter IV in [4, p. 166-168].

Theorem 4.1.6. *Every of morphism of a field F into an algebraically closed field K can be extended to a morphism from every algebraic extension of F.*

More visually the above theorem looks like this. Let $\varphi : F \to K$ be a field morphism and let E/F and L/F be algebraic field extensions.



This very powerful as we can in general not extend morphism to arbitrary extensions when we map into a field.

Lemma 4.1.7. *Every field F has an algebraic extension that contains a root of every nonconstant polynomial with coefficients in F.*

Theorem 4.1.8. *Every field F has an algebraic and algebraic closed field extension E that is unique up to F-isomorphism.*

Now we can define what we mean by the algebraic closure of a field.

Definition 4.1.9. The *algebraic closure* of a field F is an algebraic field extension E/F such that E is algebraically closed. We denote the algebraic closure of a field F by $\bar{F}$.

Next we will give some properties regarding morphism and algebraic closures. These properties will be very useful later for Galois extensions.

Proposition 4.1.10. *Every F-endomorphism of $\bar{F}$ is an F-automorphism.*

Proof. Let $\varphi : \bar{F} \to \bar{F}$ be an F-morphism. Then $\mathsf{im}(\varphi) \cong \bar{F}$ by Proposition 4.0.8. Therefore we have that $\mathsf{im}(\varphi)$ is algebraically closed. It then follows that $\mathsf{im}(\varphi) = \bar{F}$. Therefore it now follows that φ is an F-automorphism. □

Proposition 4.1.11. *If E/F is an algebraic extension, then every F-morphism $\varphi : E \to \bar{F}$ extends to a F-automorphism of $\bar{F}$.*

Proof. Let $\varphi : E \to \bar{F}$ be a F-morphism. Then by Theorem 4.1.6, φ can be extended to a F-morphism $\psi : \bar{F} \to \bar{F}$. Thus it now follows by Proposition 4.1.11 that ψ is a F-automorphism of $\bar{F}$. □

4.2. **Splitting Fields and Normal Extensions.** The exposition and proofs will follow Chapter V in [4].

Definition 4.2.1. Let E/F be a field extension and let $f \in F[x]$. We say that f *splits* in an extension E if $f = a\prod_{i\in I}(x - a_i)^{m_i}$, where $(x - a_i) \in E[x]$, $m_i \in \mathbb{N}$. We say that a field E is a *splitting field* of $f \in F[x]$ if f splits in E and E is generated by the roots of f. Likewise K/F is the splitting field of a set of polynomials $\{f_i \mid i \in I\}$ if every polynomials splits in K and K is generated by the roots of all the polynomials.

Lemma 4.2.2. *If E and L are splitting fields of a set $\mathcal{S} \subseteq F[x]$ over F, and $L \subseteq \bar{F}$, then for every F-morphism $\varphi : E \to \bar{F}$, $\varphi(E) = L$.*

For a proof of this see Lemma 1.1 in section 1 of Chapter V in [4].

Proposition 4.2.3. *Let F be a field. Then every set $\mathcal{S} \subseteq F[x]$ has a splitting field, and moreover all the splitting fields of $\mathcal{S}$ are F-isomorphic.*

For a proof of this see Proposition 1.2 in section 1 of Chapter V in [4].

Thus we now can speak of the splitting field of a set of polynomials (up to isomorphism). We now define what a normal extension is.

Definition 4.2.4. A field extension E/F is *normal* if it is the splitting field of a set polynomials $\mathcal{S} \subseteq F[x]$.

We now give some properties of normal extensions.

Proposition 4.2.5. *Let E/F be a field extension, then the following are equivalent.*

(a) E is the splitting field of a set of polynomials.
(b) For every F-morphism $\varphi : E \to \bar{F}$, satisfies that $\varphi(E) = E$.
(c) For every F-morphism $\varphi : E \to \bar{F}$, satisfies that $\varphi(E) \subseteq E$.
(d) For every F-automorphism $\varphi : \bar{F} \to \bar{F}$, satisfies that $\varphi(E) = E$.
(e) For every F-automorphism $\varphi : \bar{F} \to \bar{F}$, satisfies that $\varphi(E) \subseteq E$.
(f) Every irreducible polynomial $f \in F[x]$ with a root in E, splits in E

Proof. (a) $\Rightarrow$ (b):
This follows by Lemma 4.2.2.

(b) $\Rightarrow$ (c): This follows as if $\varphi(E) = E$ then by definition $\varphi(E) \subseteq E$.

(b) $\Rightarrow$ (d): Let $\varphi : \bar{F} \to \bar{F}$ be an F-automorphism, then $\varphi_{|E} : E \to \bar{F}$ is a F-morphism and by (b) $\varphi(E) = \varphi_{|E}(E) = E$.

(c) $\Rightarrow$ (e): Let $\varphi : \bar{F} \to \bar{F}$ be an F-automorphism, then $\varphi_{|E} : E \to \bar{F}$ is a F-morphism and by (b) $\varphi(E) = \varphi_{|E}(E) \subseteq E$.

(d) $\Rightarrow$ (e): This follows as if $\varphi(E) = E$ then per definition $\varphi(E) \subseteq E$.

(e) $\Rightarrow$ (f): Let $f \in F[x]$ be an arbitrary irreducible polynomial with a root $\alpha \in E$. For every root $\beta \in \bar{F}$ of f there exists, by Proposition 4.1.4, a F-morphism $\varphi : F(\alpha) \to \bar{F}$ that sends α to β. By Proposition 4.1.11, φ extends to a F-automorphism $\sigma : \bar{F} \to \bar{F}$. Thus, by (e), $\beta = \sigma(\alpha) \in E$. Therefore E contains every root of f and thus f splits in $E[x]$.

(f) $\Rightarrow$ (a): Let $\mathcal{S} = \{\mathsf{irr}(\alpha : F) \mid \alpha \in E\}$. Then every $f \in \mathcal{S}$ has a root in E and so therefore splits in E. Moreover E is generated by the roots of these polynomials and thus it is the splitting field of $\mathcal{S}$. □

Unfortunatley normality does not transfer as strongly to intermidiate field extension compared to algebraic extensions.

Proposition 4.2.6. *Let $F \subseteq L \subseteq E$ be field extensions, and assume that E/F is normal. Then E/L is normal.*

Proof. By definition E/F is normal if E is the splitting fields of set of polynomials $\mathcal{S} \subseteq F[x]$. As $\mathcal{S} \subseteq F[x] \subseteq L[x]$ we have that E/L is normal. □

We now generalise the concept of conjugates from $\mathbb{C}$ to arbitrary fields.

Definition 4.2.7. Let F be a field and let $a \in \bar{F}$. We then say that an element $b \in \bar{F}$ is a *conjugate* of a over F if $b = \varphi(a)$ for some F-automorphism $\varphi : \bar{F} \to \bar{F}$.

Definition 4.2.8. Let E/F be an algebraic extension and assume that $E \subseteq \bar{F}$. We then say that a field L is a *conjugate* of E if it is the image of E under a F-automorphism of $\bar{F}$.

Proposition 4.2.9. *Let F be a field and let $a \in \bar{F}$. Then the conjugates of a are the roots of $\mathsf{irr}(a : F)$ in $\bar{F}$.*

For a proof of this see Proposition 2.2 in section 2 in Chapter V in [4].

Proposition 4.2.10. *Let E/F be a algebraic extension and assume that $E \subseteq \bar{F}$. Then following properties are equivalent.*

(a) E/F is a normal extensions;
(b) For every element $\alpha \in E$, E contains all the conjugates of α over F.
(c) E has only itself as it conjugate.

Proof. This equivalence follows from Proposition 4.2.5. To see this more precisely, (b) follows from (f) in Proposition 4.2.5 by Proposition 4.2.9 as $\mathsf{irr}(\alpha : F)$ splits in E. Finally (c) follows by (d) in Proposition 4.2.5. □

4.3. **Separable Extension.** We will now define what a separable extension is and give some properties of said extensions.

Definition 4.3.1. A polynomial $p \in F[x]$ is *separable* if p can be factored in $\bar{F}[x]$ as

$$p = (x - a_0)(x - a_1)...(x - a_n) \tag{1}$$

where $a_i \neq a_j$ if $i \neq j$. Let E be an extension of F, we then say that $\alpha \in E$ is *separable* if it is algebraic over F and $\mathsf{irr}(\alpha : F)$ is separable. We say that an extension E/F is *separable* if every element of E is separable over F.

Alot of field extension are separable as the following proposition shows.

Proposition 4.3.2. *Let F be a field of characteristic zero and let E/F be an algebraic extension. Then E/F is separable.*

For a proof of this see Proposition 5.1 in section 5 of Chapter IV in [4].

Now we will define what the separability degree of an extension is.

Definition 4.3.3. The *separability degree* of an algebraic extension E/F is the number of F-morphism $\varphi : E \to \bar{F}$. We denote this $[E : F]_S$.

Proposition 4.3.4. *Let F be a field and let α be algebraic over F. Then $[F(\alpha) : F]_S$ is the number of distinct roots of $\mathsf{irr}(\alpha : F)$. Thus $[F(\alpha) : F]_S \leq [F(\alpha) : F]$.*

Proof. Let $f = \mathsf{irr}(\alpha : F)$ and let $\varphi : F(\alpha) \to \bar{F}$ be a F-morphism. As $f \in F[x]$ we have that $f_\varphi = f$ and therefore we get that $0 = f_\varphi(\varphi(\alpha)) = f(\varphi(\alpha))$. Thus for any $\varphi : F(\alpha) \to \bar{F}$, $\varphi(\alpha)$ is a root of f. Therefore we have that the number of F-automorphism $\varphi : F(\alpha) \to \bar{F}$ are equal to distinct roots of f as these maps are uniquely determined from where they send α. We have, by Proposition 4.0.16, that $[F(\alpha) : F] = \mathsf{deg}(f)$ and therefore we have that $[F(\alpha) : F]_S \leq [F(\alpha) : F]$. □

The following Corollary follows directly from the above proposition.

Corollary 4.3.5. *Let F be a field and let α be algebraic over F. Then $[F(\alpha):F]_S = [F(\alpha):F]$ if and only if $\mathsf{irr}(\alpha:F)$ is separable.*

Like with the dimension of an extension we can split up the separability degree.

Proposition 4.3.6. *If E/F is an algebraic extension and L is an intermediate field, then $[E:F]_S = [E:L]_S[L:F]_S$.*

For a proof of this see Proposition 5.3 in section 5 of Chapter IV in [4].

Proposition 4.3.7. *Let E/F be a finite extension. Then the following condition are equivalent.*

(a) E is separable over F.
(b) E is generated by finitely many separable elements.
(c) $[E:F]_S = [E:F]$.

Proof. (a) $\Rightarrow$ (b):
As E/F is finite extension, we know that $E = F(\alpha_1, ..., \alpha_n)$ for some $\alpha_1, ..., \alpha_n \in E$. Thus, as by (a) every element in E is separable, the results follows as therefore especially $\alpha_1, ..., \alpha_n$ are separable.

(b) $\Rightarrow$ (c):
By assumption $E = F(\alpha_1, ..., \alpha_n)$ for some separable $\alpha_0, ..., \alpha_n \in E$. Define the following intermediate fields, $E_0 = F$, $E_i = E_{i-1}(\alpha_i)$. Thus we have the following tower of fields $F = E_0 \subseteq E_1 \subseteq ... \subseteq E_{n-1} \subseteq E_n = E$. Let $f_i = \mathsf{irr}(\alpha_i : E_{i-1})$ and let $g_i = \mathsf{irr}(\alpha_i : F)$. We now by assumption that g_i is separable and as $F[x] \subseteq E_{i-1}[x]$ we must have that $f_i | g_i$. Therefore f_i is separable. Thus we get by repeated use of Proposition 4.3.6, Proposition 4.0.11 and Proposition 4.3.5

$$\begin{aligned}[E:F]_S &= [E_n : E_{n-1}]_S ... [E_1 : E_0]_S \\ &= [E_n : E_{n-1}] ... [E_1 : E_0] \\ &= [E:F]\end{aligned}$$

Thus we have proved (c).
(c) $\Rightarrow$ (a): Let $\alpha \in E$ be arbitrary. Then we have by assumption and by Proposition 4.3.6 and Proposition 4.0.11 that

$$\begin{aligned}[E:F(\alpha)]_S[F(\alpha):F]_S = [E:F]_S &= [E:F] \\ &= [E:F(\alpha)][F(\alpha):F]\end{aligned}$$

We also know that, by Proposition 4.3.4 $[F(\alpha):F]_S \leq [F(\alpha):F]$. We also have that $[E:F(\alpha)]_S \leq [E:F(\alpha)]$. To see this note firstly that E/F is algebraic by Proposition 4.1.2 and therefore $E = F(\beta_1, ..., \beta_n)$. Define $E_0 = F(\alpha)$ and $E_i = E_{i-1}(\beta_i)$. Then we have that $[E:F(\alpha)]_s = [E:E_{n-1}]_s ... [E_1 : F(\alpha)]_s$ which is less than or equal to $[E:E_{n-1}]...[E_1:F(\alpha)] = [E:F(\alpha)]$ by Propositio 4.3.4. Therefore $[E:F(\alpha)]_s \leq [E:F(\alpha)]$. Thus as E/F is a finite extension it must be the case that $[E:F(\alpha)]_S = [E:F(\alpha)]$ and that $[F(\alpha):F]_S = [F(\alpha):F]$. Therefore we have that α is separable by Proposition 4.3.4 and as $\alpha \in E$ was arbitrary E/F is a separable extension. $\square$

We now give some properties of separable extensions.

Proposition 4.3.8. *Let E/F be a separable extension and let L be an intermediate extension. Then E/L and L/F are separable extensions if and only if E/F is separable.*

Proof. First assume that E/F is algebraic and let $\alpha \in E$. Then α is separable over L as $F[x] \subseteq L[x]$. Thus E/L is separable. Let $\beta \in L$ be given then β is separable over F as $\beta \in E$ as $L \subseteq E$.

Conversely assume that E/L and L/F are separable extensions. Let $\alpha \in E$ is separable over L and $\mathsf{irr}(\alpha : L) = a_0 + ... + a_n x^n$. Then $K = F(a_0, ..., a_n)$ is separable over F as L/F is separable. Also

$K(\alpha)/K$ is also separable as α is separable over L. Define $K_0 = F$ and $K_i = K_{i-1}(a_{i-1})$, then we have the following tower of extensions

$$F = K_0 \subseteq K_1 \subseteq ... \subseteq K_{n-1} \subseteq K_n = K \subseteq K(\alpha).$$

Then we get by Proposition 4.3.6, Proposition 4.3.5 and Proposition 4.0.11 that

$$\begin{aligned}[K(\alpha) : F] &= [K(\alpha) : K][K : K_{n-1}]...[K_1 : F] \\ &= [K(\alpha) : K]_S[K : K_{n-1}]_S...[K_2 : K_1][K_1 : F]_S \\ &= [K(\alpha) : F]_S\end{aligned}$$

Therefore by Proposition 4.3.7 we get that $K(\alpha)/F$ is separable. Thus especially α is separable over F. Therefore, as α was arbitrary, we get that E/F is separable. □

Proposition 4.3.9. *Every finite separable extension is simple.*

For a proof of this see Proposition 5.12 in section 5 of Chapter IV in [4].

Proposition 4.3.10. *If E/F is separable and $\mathsf{irr}(\alpha : F)$ has degree at most n for every $\alpha \in E$, then E/F is simple and $[E : F] \leq n$.*

For a proof of this see Proposition 5.13 in section 5 of Chapter IV in [4].

4.4. **Galois Extensions.** We will now define what Galois extensions and Galois groups are. We will then connect subgroups and intermediate field extensions via the fundamental theorem of Galois extensions. The proofs and exposition of this section will mostly follow section 3 of Chapter V in [4].

Definition 4.4.1. An algebraic extension E of a field F is called a *Galois extension* of F if it is separable and normal.

This definition may not make it entirely intuitive why we study precisely these extensions. The following theorem gives a maybe more intuitive explanation why these extension are interesting.

Theorem 4.4.2. *Let E/F be a algebraic extension. Then E/F is a Galois extension if and only if every F-automorphism of E is the identity on and only on F.*

We will later show the backwards direction of the if and only if statement but for all whole proof see [1]. Note that a Galois extension in [1] is called a normal extension.

Given a Galois extension E/F we can study the group of F-automorphism.

Proposition 4.4.3. *Let E/F be a field extension, then the set of all F-automorphism forms a group with composition as the group operation.*

Proof. Let G denote the set of all F-automorphisms. First by definition composition of function are associative. We also have an identity element given by the $\mathsf{id}_E : E \to E$ as by definition for any $\sigma \in G$, we have that $\sigma \circ \mathsf{id}_E = \mathsf{id}_E \circ \sigma = \sigma$. Note that as every $\sigma \in G$ is bijective we have inverse given by $\sigma^{-1} \in G$. Therefore G forms a group. □

Definition 4.4.4. Let E/F be a Galois extension, then we define the *Galois group* to be the group of F-automorphisms. We denote this group by $\mathsf{Gal}(E/F)$ for a Galois extension E/F.

Proposition 4.4.5. *If E/F is a finite Galois extension, then $|\mathsf{Gal}(E/F)| = [E : F]$.*

Proof. As E/F is normal it follows by Proposition 4.2.5, that every F-morphism of E into $\bar{F}$ sends E onto E. Therefore, if we restricted such a map to E it is precisely an F-automorphism of E. Hence it follows that $|\mathsf{Gal}(E/F)| = [E : F]_S = [E : F]$ as E is also separable over F. □

Definition 4.4.6. Let G be a group of automorphism of a field F. We then defined the *fixed field* of G to be $\{a \in F \mid \sigma a = a \text{ for all } \sigma \in G\}$. We denote this by $\mathsf{Fix}_F(G)$.

We need to prove that this is also indeed a field.

Proof. Firstly by definition every field automorphism must fix 1 so therefore $1 \in \mathsf{Fix}_F(G)$. Let $a, b \in \mathsf{Fix}_F(G)$, then by the definition of a group morphism and Lemma 3.1.10 we have that

(a) $\sigma(ab) = \sigma(a)\sigma(b) = ab$ for all $\sigma \in G$, hence $ab \in \mathsf{Fix}_F(G)$;
(b) $\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$ for all $\sigma \in G$, hence $a + b \in \mathsf{Fix}_F(G)$;
(c) $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$ for all $\sigma \in G$, hence $a^{-1} \in \mathsf{Fix}_F(G)$;
(d) $\sigma(-a) = -\sigma(a) = -a$ for all $\sigma \in G$, hence $-a \in \mathsf{Fix}_F(G)$.

Therefore $\mathsf{Fix}_F(G)$ forms a field. □

Proposition 4.4.7. *If G is a finite group of automorphism of a field E then E is a finite Galois extension of $F = \mathsf{Fix}_E(G)$ and $\mathsf{Gal}(E/F) = G$.*

Proof. We will begin by showing that E is algebraic over F. Let $\alpha \in E$ be an arbitrary element. Then, as G is finite, $G\alpha = \{\beta \in E \mid \sigma\alpha = \beta \text{ for some } \sigma \in G\} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, where $n \leq |G|$ and $\alpha_1, ..., \alpha_n \in E$ are distinct elements. Note that we must have that one of the α_i is equal to α as G is a group and therefore contains the identity automorphism. Without loss of generality we will assume that $\alpha_1 = \alpha$. We now define the polynomial $f_\alpha(X) = (\alpha_1 - X)(\alpha_2 - X)...(\alpha_n - X) \in E[X]$. Then $f_\alpha(\alpha) = 0$ and f_α is separable. Moreover, every $\sigma \in G$ permutes $\alpha_1, ..., \alpha_n$ and therefore $(f_\alpha)_\sigma = f_\alpha$. Thus $f_\alpha \in F[X]$. It now follows that α is algebraic over F and as $\mathsf{irr}(\alpha : F)$ must divide f_α, α is also separable. Thus E is an algebraic and separable extension of F as α was arbitrary. We also see that E is a splitting field of the polynomials $f_\alpha \in F[X]$ for all $\alpha \in E$, hence it also normal over F. We therefore conclude that E/F is a Galois extension.

By Proposition 4.3.10 it follows that $[E : F] \leq |G|$ as E/F is a finite extension. We also have by Proposition 4.4.5 that $|\mathsf{Gal}(E/F)| = [E : F] \leq |G|$. But every $\sigma \in G$ is an F-automorphism of E, so $G \subseteq \mathsf{Gal}(E/F)$. Therefore we conclude that $\mathsf{Gal}(E/F) = G$. □

Proposition 4.4.8. *If E/F is a Galois extension, then the fixed field of $\mathsf{Gal}(E/F)$ is precisely F.*

Proof. Let $G = \mathsf{Gal}(E/F)$ and let $L = \mathsf{Fix}_E(G)$. Then $F \subseteq L$. Let $\alpha \in L$, now we want to show that $\alpha \in F$. There exists an algebraic closure of F such that $E \subseteq \bar{F}$. Every F-morphism $\varphi : F(\alpha) \to \bar{F}$ extends to a F-automorphism of $\bar{F}$. As E/F is also a normal extension, we can restrict φ to a F-automorphism ψ of E. Hence $\varphi(\alpha) = \psi(\alpha) = \alpha$, as $\alpha \in L = \mathsf{Fix}_E(G)$. By definition φ is the inclusion morphism of $F(\alpha)$ into $\bar{F}$. Thus $[F(\alpha) : F]_S = 1$. Therefore, since $F(\alpha) \subseteq E$ is separable over F, this implies that $F(\alpha) = F$, by Proposition 4.3.4. Therefore we conclude that $\alpha \in F$ and thus that $F = L$. □

We can now finally prove the fundamental theorem of finite Galois extensions.

Theorem 4.4.9. *Let E/F be a finite Galois extension and let $G = \mathsf{Gal}(E/F)$. Let $\mathcal{F}(E/F) = \{L \mid L \text{ is a field and } F \subseteq L \subseteq E\}$ and let $\mathcal{S}(G) = \{H \mid H \leq G\}$. We then have a bijection between $\mathcal{F}(E/F)$ and $\mathcal{S}(G)$ via the map*

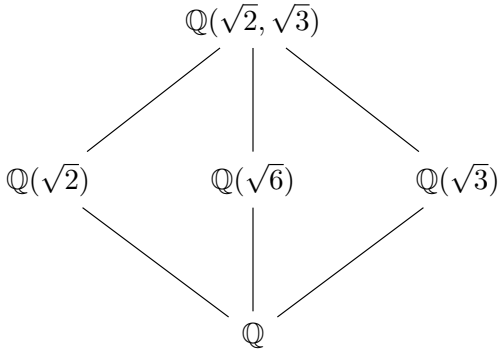
$$\begin{aligned} \Phi : \mathcal{F}(E/F) &\to \mathcal{S}(G) \\ L &\mapsto \mathsf{Gal}(E/L) \end{aligned}$$

and the map

$$\begin{aligned} \Gamma : \mathcal{S}(G) &\to \mathcal{F}(E/F) \\ H &\mapsto \mathsf{Fix}_E(H) \end{aligned}$$

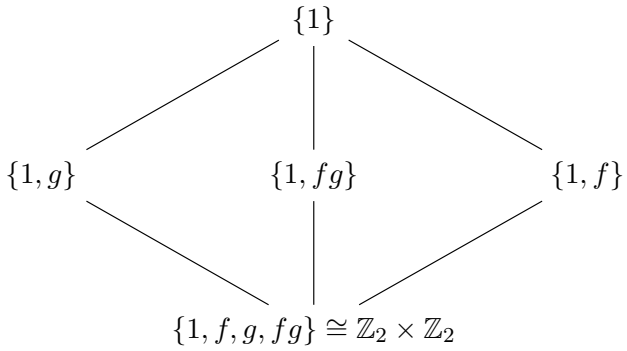
Proof. To show this we need to show that $\Phi \circ \Gamma = \mathsf{id}_{\mathcal{S}(G)}$ and that $\Gamma \circ \Phi = \mathsf{id}_{\mathcal{F}(E/F)}$. Let H be a subgroup of G and let $\mathsf{Fix}_E(G) = L$. Then it follows by Proposition 4.4.7 that $G = \mathsf{Gal}(E/F)$ and thus it follows that $\Phi \circ \Gamma = id_{\mathcal{S}(G)}$. Likewise let L be an intermediate field then it follows that $\Gamma(\Phi(L)) = L$ by Proposition 4.4.8. □

Example 4.4.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is finite Galois extensions. Then the Galois group $\mathsf{Gal}((\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is generated by the $\mathbb{Q}$-automorphism $f : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ given by $f(\sqrt{2}) = -\sqrt{2}$, $f(\sqrt{3}) = \sqrt{3}$ and the $\mathbb{Q}$-automorphism $g : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ given by $g(\sqrt{3}) = -\sqrt{3}$, $g(\sqrt{2}) = \sqrt{2}$. We then get the following lattice diagram for $\mathcal{F}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.



(2)

Respectively the following lattice diagram for $\mathcal{S}(\mathsf{Gal}(E/F))$.



(3)

We now prove some properties of finite Galois extensions.

Proposition 4.4.11. *Let E/F be a finite Galois extension and let $E \subseteq \bar{F}$. Let L_1 and L_2 be two intermediate fields and let $G_1 = \mathsf{Gal}(E/L_1)$ and $G_2 = \mathsf{Gal}(E/L_2)$. Then L_1 and L_2 are conjugate if and only if G_1 and G_2 are conjugate.*

For a proof see Proposition 3.10, part (4), in section 3 of Chapter V in [4].

Proposition 4.4.12. *Let E/F be a finite Galois extension, let $G = \mathsf{Gal}(E/F)$ and assume that $E \subseteq \bar{F}$. Then an intermediate field extension $F \subseteq L \subseteq E$ is normal over F if and only if $\mathsf{Gal}(E/L)$ is normal subgroup of $\mathsf{Gal}(E/F)$. Moreover if L is normal $\mathsf{Gal}(L/F) \cong \mathsf{Gal}(E/F)/\mathsf{Gal}(E/L)$.*

Proof. Note that it follows from Proposition 4.4.11 and Proposition 4.2.10 that L is normal if and only if G is normal. Thus it remains to show that $\mathsf{Gal}(L/F) \cong \mathsf{Gal}(E/F)/\mathsf{Gal}(E/L)$. Now we assume that L is normal. Then for each element $\sigma \in \mathsf{Gal}(E/F)$ we have a well define restriction $\sigma_{|L} \in \mathsf{Gal}(L/F)$. We therefore define a morphism $\sigma : \mathsf{Gal}(E/F) \to \mathsf{Gal}(L/F)$ by $\sigma \mapsto \sigma_{|L}$. This is surjective as by Proposition 4.1.11 every F-endomorphism of L can be seen as a F-morphism from L to $\bar{F}$ and can therefore be extended to a F-automorphism of $\bar{F}$. Furthermore note that $\mathsf{ker}(\varphi) = \mathsf{Gal}(E/L)$. Thus it follows by Theorem 3.1.18 that $\mathsf{Gal}(L/F) \cong \mathsf{Gal}(E/F)/\mathsf{Gal}(E/L)$. □

A question that one now might be wondering about is what happens if we take away the condition of the Galois extension being finite in the main theorem. The problem we will see in later examples is that we get too many subgroups, i.e subgroups of the Galois group that have the same fixed field, thus losing our lovely bijection in the fundamental theorem. The strategy, as we will see in the sections following, is to restrict which subgroups we take and then hopefully attain a bijection in the infinite case. What Krull found out in the 1930's is that the key is to introduce a topology.

5. Topological Spaces and Topological Groups

5.1. **Basic Topology.** Here will recall the basic definitions of topology as well as some results that we will need later. The proofs and exposition will basically follow [8].

A topology on a set allows us in an abstract way to "measure" how close two points are. Thus, as we can "measure" closeness, we get a better grasp over infinite things, as we can say if something approaches something else.

Definition 5.1.1. A *topological space* is a 2-tuple $(X, \mathcal{T})$, where X is set and $\mathcal{T} \subseteq P(X)$ is subset of the power set of X, that fulfills the following conditions

(a) $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$.
(b) If $(A_i)_{i\in I}$ is a collection of sets, each in $\mathcal{T}$, then $\bigcup_{i\in I} A_i \in \mathcal{T}$.
(c) If $(A_i)_{i\in I}$ is a finite collection of sets, each in $\mathcal{T}$, then $\bigcap_{i\in I} A_i \in \mathcal{T}$.

The sets in $\mathcal{T}$ are called open sets. We say that $\mathcal{T}$ defines a topology on X or that X is endowed with the topology given by $\mathcal{T}$. We say that a subset $V \subseteq X$ is closed if $X \setminus V \in \mathcal{T}$. We denote that an subset U is open in a topological space X by $U \subseteq_{op} X$ and that U is closed by $U \subseteq_{cl} X$.

Note that we are allowed to take the union of any number of open sets, even a uncountable number, whilst we are only allowed to take the intersection of a finite number of open sets. We will often (almost always) denote a topological space only by its underlying set.

Example 5.1.2. We will now give a couple of examples and non-examples of topological spaces.

(a) Let $X = \{a, b, c\}$ and let $\mathcal{T} = \{X, \{a, b\}, \{a\}, \{b\}, \emptyset\}$. Then $(X, \mathcal{T})$ is a topological space.
(b) Let X be as above and let $\mathcal{T} = \{X, \{a, b\}, \{a\}, \{c\}, \emptyset\}$. Then $(X, \mathcal{T})$ is not a topological space as for example $\{c\} \cup \{a\} \notin \mathcal{T}$.
(c) Let $X = \mathbb{N}$. Let $\mathcal{T} = \{M \subseteq \mathbb{N} \mid \mathbb{N} \setminus M \text{ is finite or } M = \emptyset\}$. Then $(X, \mathcal{T})$ is a topological space.

Definition 5.1.3. Let X be any set. Then we define the *trivial topology* as the topology given by $\mathcal{T} = \{X, \emptyset\}$ and the *discrete topology* on X as the topology given by letting every set be open.

Definition 5.1.4. Let $(X, \mathcal{T})$ be a topological space and let $A \subseteq X$. We then define the *subset topology* on A as the topology given by $\mathcal{T}' = \{A \cap U \mid U \in \mathcal{T}\}$.

We now define what the structure preserving maps between topological space are.

Definition 5.1.5. Let X and Y be topological spaces. We say that a map $f : X \to Y$ is *continuous* if the preimage of every open set is open.

Example 5.1.6. We will now give a couple of examples of continuous maps.

(a) Let $X = \{a, b, c\}$, let $\mathcal{T}_1 = \{X, \{a, b\}, \{a\}, \{b\}, \emptyset\}$ and $\mathcal{T}_2 = \{X, \{b, c\}, \{b\}, \{c\}, \emptyset\}$. Let $f = \mathsf{id}_X$ and let g be the function defined by $a \mapsto b$, $b \mapsto c$ and $c \mapsto a$. Then $f : (X, \mathcal{T}_1) \to (X, \mathcal{T}_1)$ is continuous but $f : (X, \mathcal{T}_1) \to (X, \mathcal{T}_2)$ is not continuous. Likewise $g : (X, \mathcal{T}_1) \to (X, \mathcal{T}_2)$ is continuous but $g : (X, \mathcal{T}_1) \to (X, \mathcal{T}_1)$ is not continuous.
(b) Let X be any set endowed with the discrete topology and let Y be any topological space. Then any function $f : X \to Y$ is continuous.

(c) Let X and Y be any topological spaces. Fix a $y_0 \in Y$ and let $f : X \to Y$ be the map defined by $x \mapsto y_0$. Then f is continuous.

Note from the examples above that the underlying topology is very important as to whether a map is continuous as a map can be continuous or not depending on the the underlying topology.

Proposition 5.1.7. *Let $f : X \to Y$ be a map. Then f is continuous if and only if the preimage of closed sets are closed.*

Proof. First we assume that f is continuous. Let $U \subseteq Y$ be a closed set. Then $Y \setminus U$ is an open set. Therefore we get that $f^{-1}(Y \setminus U) = f^{-1}(Y) \setminus f^{-1}(U) = X \setminus f^{-1}(U)$ is open. This in turn implies that $f^{-1}(U)$ is closed. Conversely assume that the preimage of a closed set is closed and let $U \subseteq Y$ be an open set. Then $Y \setminus U$ is a closed set and therefore $f^{-1}(Y \setminus U) = f^{-1}(Y) \setminus f^{-1}(U) = X \setminus f^{-1}(U)$ is an closed set. This in turn implies that $f^{-1}(U)$ is an open set. □

Proposition 5.1.8. *Let X, Y and Z be topological spaces and let $f : X \to Y$ and $g : Y \to Z$ be continuous maps. Then $g \circ f$ is a continuous map.*

Proof. Let U be an open set in Z. Then $(g \circ f)^{-1}(U) = f^{-1}(g^{-1}(U))$ is an open set as $g^{-1}(U)$ is an open set by continuity of g and therefore $f^{-1}(g^{-1}(U))$ is an open set by continuity of f. Thus $g \circ f$ is continuous. □

Definition 5.1.9. Let X and Y be topological spaces. We say that X and Y are *homeomorphic* if there exists continuous maps $f : X \to Y$ and $g : Y \to X$ such that $g \circ f = \mathsf{id}_X$ and $f \circ g = \mathsf{id}_Y$.

Definition 5.1.10. Let X be a topological space and let $A \subseteq X$ be a set of points. We say that a subset $N \subseteq X$ is a *neighbourhood* of A if there exists an open set V such that $A \subseteq V \subseteq N$.

Proposition 5.1.11. *A set is a neighbourhood of each of its points if and only if it is open.*

Proof. Assume that $N \subseteq X$ is a set that is a neighbourhood of all of its points. Then by definition for every $x \in N$ there exists a $V_x \subseteq N$ such that V_x is open. Thus we have that $N = \bigcup_{x \in N} V_x$ which is open. Therefore N is an open set. Conversely assume that N is open, then by definition N is a neighbourhood of all of points. □

We now give an alternative definition of continuity in terms of neighbourhoods.

Proposition 5.1.12. *Let X and Y be topological spaces. Then a map $f : X \to Y$ is continuous if and only if at every point $x \in X$ and for every neighbourhood U of $f(x)$ there is a neighbourhood of V of x such that $f(V) \subseteq U$.*

For a proof see Theorem I (Chapter I, 2.1) in [2].

In this next proposition we will see that we can define a unique topology on a set by a suitable collection of subsets for each point.

Proposition 5.1.13. *Let X be a set and assume that for every point $x \in X$ we have a collection of sets $\mathcal{B}(x)$ of subsets of X fulfilling the following properties.*

(a) If $B \in \mathcal{B}(x)$ and $B \subseteq Y \subseteq X$ then $Y \in \mathcal{B}(x)$.
(b) Let $(B_i)_{i \in I}$ be a finite collection of sets in $\mathcal{B}(x)$. Then $\bigcap_{i \in I} B_i \in \mathcal{B}(x)$.
(c) For every element $B \in \mathcal{B}(x)$, $x \in B$.
(d) Let $B \in \mathcal{B}(x)$. Then there exists a $C \in \mathcal{B}(x)$ such that $B \in \mathcal{B}(y)$ for all $y \in C$.

Then there exists a unique topology on X such that for all $x \in X$, $\mathcal{B}(x)$ is precisely the set of all neighbourhoods of x.

Proof. Let $\mathcal{T}$ be set consisting of all subset $A \subseteq X$ which satisfies that $A \in \mathcal{B}(x)$ for all $x \in A$. $A \in \mathcal{B}(x)$. We now aim to show that $(X, \mathcal{T})$ is a topological space. By Proposition 5.1.11 it follows that this topology, if it exists, is unique. Now we need to show that this is indeed a topology. Note that (a) gives us that $X \in \mathcal{B}(x)$. Vacuously it also holds that $\emptyset \in \mathcal{B}(x)$. Thus $X, \emptyset \in \mathcal{T}$. Secondly let $(C_i)_{i\in I}$ be an arbitrary collection of sets in $\mathcal{T}$. Then from (a) it follows that $\bigcup_{i\in I} C_i \in \mathcal{T}$. Likewise it follows from (b) that for any finite collection $(C_j)_{j\in J}$, we have that $\bigcap_{j\in J} C_j \in \mathcal{T}$. Thus we have now proven that $\mathcal{T}$ indeed defines a topology on X.

Lastly it remains to show that $\mathcal{B}(x)$ is the set of all neighbourhoods of x for all $x \in X$. Fix an arbitrary $x \in X$ and let $\mathcal{D}(x)$ be the set of all neighbourhoods of x in the topology defined by $\mathcal{T}$. We aim to show that $\mathcal{B}(x) = \mathcal{D}(x)$. We begin by showing that $\mathcal{D}(x) \subseteq \mathcal{B}(x)$. Let $D \in \mathcal{D}(x)$ be given. Then D contains a set $A \subseteq D$, $x \in A$, such that for all $y \in A$, $A \in \mathcal{B}(y)$. Thus by (a) it follows that $D \in \mathcal{B}(x)$. Conversely let $B \in \mathcal{B}(x)$ be given. Define C to be set of points $y \in X$ for which $B \in \mathcal{B}(y)$. If we can show that $x \in C$, $C \subseteq B$ and that $C \in \mathcal{T}$ we are done. Firstly $x \in C$ as $B \in \mathcal{B}(x)$. Let $c \in C$, then $B \in \mathcal{B}(c)$ and therefore by (c) $c \in B$, thus $C \subseteq B$. To show that $C \in \mathcal{T}$ we will show that for all $c \in C$, $C \in \mathcal{B}(c)$. Let $c \in C$ be arbitrary, then $B \in \mathcal{B}(c)$. By (d) there exists a set $W \in \mathcal{B}(x)$ such that for all $w \in W$, $B \in \mathcal{B}(w)$. Now $W \subseteq C$ and thus it follows from (a) that $C \in \mathcal{B}(x)$. □

Definition 5.1.14. A *fundamental system of neighbourhoods* of a point x in a topological space X is a collection of neighbourhoods $\mathcal{N}$ of x such that for any neighbourhood V of x there is a neighbourhood $W \in \mathcal{N}$ such that $W \subset V$.

We now define what a connected set is.

Definition 5.1.15. Let X be a topological space and let $A \subseteq X$. We say that A is *connected* if it cannot be written as the union of two disjoint non-empty closed subsets of A. Otherwise we say that A is *disconnected*.

This definition is equivalent to the one where we say that A is disconnected if it can be written as a union of two disjoint non-empty *open* subsets.

Definition 5.1.16. Let X be a topological space and let $x \in X$ be a point. The *connected component* of x is the largest subset $A \subseteq X$ containing x such that it is connected.

Definition 5.1.17. Let X be a topological space. We then say that X is *totally disconnected* if all the connected components are singletons.

We will now define what is means for topological spaces to be compact. To do this we first need to define what an open cover is.

Definition 5.1.18. An *open cover* of a topological set X is collection of open sets U_i such that $\bigcup_{i\in I} U_i = X$. A subcover of an open cover $(U_i)_{i\in I}$ of a topological space X is a collection $(U_j)_{j\in J}$, where $J \subseteq I$, such that $(U_j)_{j\in J}$ is a open cover of X. If J is finite then we say that the subcover is finite. An open cover of a subset $Y \subseteq X$ is a collection $(U_i)_{i\in I}$ such that $Y \subseteq \bigcup_{i\in I} U_i$.

Definition 5.1.19. A topological space X or a subspace $Y \subseteq X$ is *compact* if every open cover has a finite subcover.

The importance of compactness is that it allows us to care only about a finite number of sets.

Example 5.1.20. We will now give some examples and non-examples of compact topological spaces.

(a) Let X be any finite set and endow X with any topology. Then X is compact.
(b) Let X be any set endowed with the trivial topology. Then X is compact.

(c) Let X be a infinite set and endow it with the discrete topology. Then X is not compact as for example if we take the covering consisting of all single point sets, it has no finite subcover.

Now we will see that continuous maps preserve connectness and compactness.

Proposition 5.1.21. *Let $f : X \to Y$ be a continuous map of topological spaces. Then the following holds.*

(a) For all compact subsets $A \subseteq X$, it holds that $f(A)$ is compact.
(b) For all connected subsets $A \subseteq X$, it holds that $f(A)$ is connected.

Proof. We begin by proving (a). Let $A \subseteq X$ be a compact subset and let $\{U_i\}_{i\in I}$ be an arbitrary open cover of $f(A)$. Then $\{f^{-1}(U_i)\}_{i\in I}$ is an open cover of A. Then by compactness of A there exists a finite index set $J \subseteq I$ such that $\{f^{-1}(U_i)\}_{i\in J}$ is a open cover of A. Then $\{U_i\}_{i\in J}$ is a finite open subcover of $f(A)$. Therefore, as $\{U_i\}_{i\in I}$ was arbitrary, A is compact.

We now prove (b). Let $A \subseteq X$ be connected and assume towards a contradiction that $f(A)$ is not connected. Then by definition $f(A) = U \cup V$ for two disjoint non-empty closed subset $U, V \subseteq Y$. But then $A = f^{-1}(f(A)) = f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$. By Proposition 5.1.7 we have that $f^{-1}(U)$ and $f^{-1}(V)$ are closed. Therefore we get that A is not connected. This is a contradiction as we assume that A is connected. Therefore it must be the case that $f(A)$ is connected. □

We will now define what a basis and a subbasis of a topology is.

Definition 5.1.22. Let $(X, \mathcal{T})$ be a topological space. A subset of subsets $\mathcal{B} \subseteq P(X)$ is called *a basis* if the following condition are fulfilled.

(a) $\bigcup_{B\in\mathcal{B}} B = X$;
(b) Let $B_1, B_2 \in \mathcal{B}$ be two arbitrary basis elements. Then for every $x \in B_1 \cap B_2$ there exists a $B_3 \in \mathcal{B}$ such that $x \in B_3 \subseteq B_1 \cap B_2$.

Given a basis $\mathcal{B}$ we say that the topology generated by $\mathcal{B}$ is the smallest topology containing $\mathcal{B}$.

Example 5.1.23. We now give a example of a basis and a topology generated by a basis.

(a) For example if we yet again take our three point space $X = \{a, b, c\}$ and endow it with the following topology $\mathcal{T} = \{X, \{a, b\}, \{a\}, \{b\}, \emptyset\}$. Then $\mathcal{B} = \{\{a\}, \{b\}, \{c\}, \emptyset\}$ forms a basis for $(X, \mathcal{T})$.
(b) The standard topology on $\mathbb{R}^n$ is the topology generated, as a basis, by $\mathcal{B} = \{B(x, r) \mid x \in X \text{ and } r \in \mathbb{R}_{\geq 0}\}$, where $B(x, r)$ is the open ball centered at x with radius r.

We also have the following proposition.

Proposition 5.1.24. *Let X be a topological space and let $\mathcal{B}$ be a basis then every open set $U \subseteq X$ can be written as a union of basis elements.*

For a proof of this see Lemma 13.1 in section 13, Chapter 2 in [8]. Note though that the expression of open subsets as union of basis elements is in general not unique.

Definition 5.1.25. Let $(X, \mathcal{T})$ be a topological space. A subset of open subsets $\mathcal{S} \subseteq P(X)$ is called *a subbasis* of $\mathcal{T}$ if $\mathcal{T}$ is the smallest topology containing $\mathcal{S}$. We say that a topology $\mathcal{T}$ is generated as a subbasis by a collection of subsets $\mathcal{S} \subseteq P(X)$ if $\mathcal{S}$ is a subbasis of $\mathcal{T}$.

Definition 5.1.26. Let $(X_i)_{i\in I}$ be a collection of topological sets. Let $p_i : \prod_{i\in I} X_i \to X_i$ be the canonical projection, that is $(x_i)_{i\in I} \mapsto x_i$. The *product topology* is the topology generated as a subbasis by $p_i^{-1}(U_i)$, where U_i is an open subset of X_i. Stated differently this is the weakest topology that makes the projection maps continuous.

We now prove a nice property of the product of topological spaces endowed with the product topology.

Proposition 5.1.27. *Let $(X_i)_{i\in I}$ be a collection of topological space and let $\prod_{i\in I} X_i$ be endowed with the product topology. Let B a topological space. Then a map $f : B \to \prod_{i\in I} X_i$ is continuous if and only if $h_i = p_i \circ f : B \to X_i$ is continuous for all $i \in I$.*

Proof. We have the following commutative diagram for all $i \in I$.

$$\begin{array}{ccc} B & \xrightarrow{f} & \prod_{i\in I} X_i \\ & \searrow^{h_i} & \downarrow{\scriptstyle p_i} \\ & & X_i \end{array}$$

We know by the definition of the product topology that $p_i : \prod_{i\in I} X_i \to X_i$ is continuous for all $i \in I$. The only if part follows directly from Proposition 5.1.8. Conversely assume that h_i is continuous for all $i \in I$. Let $U \subseteq \prod_{i\in I} X_i$ be an open subset. Then, by the definition of the product topology, $U = \bigcup_{l\in L}((\prod_{i\notin J_l} X_i) \times (\prod_{j\in J_l} U_{lj}))$, for some finite index set $J_l \subseteq I$, where $U_{lj} \subseteq_{op} X_j$ for all $j \in J_l$ for all $l \in L$. Thus we get that $f^{-1}(U) = \bigcup_{l\in L}(\bigcap_{j\in J_l} h_j^{-1}(U_{lj}))$ which is open in B as each h_j is continuous and as J_l is finite for all $l \in L$. Therefore f is a continuous function. □

This could also been shown in a interesting way if we instead define products of topological spaces by the universal property of products.

Proposition 5.1.28. *Let X be a topological space and let $\mathcal{C}$ be a collection of open subsets of X. Assume for any open set $U \subseteq X$ it holds that for all $x \in U$ there exists a $C \in \mathcal{C}$ such that $x \in C \subseteq U$. Then $\mathcal{C}$ is a basis for the topology on X.*

Definition 5.1.29. A topological space X is called *Hausdorff* if for every two distinct points $x, y \in X$ there exists open neighbourhoods U and V of x and y respectively such that $U \cap V = \emptyset$.

Example 5.1.30. Yet again we take our favorite three point set $X = \{a, b, c\}$ and the following two topologies: $\mathcal{T}_1$ as the discrete topology and $\mathcal{T}_2 = \{X, \{a, b\}, \{a\}, \{b\}, \emptyset\}$. Then $(X, \mathcal{T}_1)$ is Hausdorff, whilst $(X, \mathcal{T}_2)$ is not Hausdorff as one cannot separate e.g. c and a as the only open set containing c is X.

Definition 5.1.31. A topological space is called *normal* if for every pair of closed disjoint subsets $U, V \subseteq X$ there exists open disjoint sets U' and V' containing U and V respectively.

The following properties of compact and Hausdorff spaces will be important.

Proposition 5.1.32. *Let X be a compact and Hausdorff topological space. Then X is normal.*

For a proof of this see Theorem 32.3 in Section 32, Chapter 4 of [8].

First we have that compact subsets of Hausdorff spaces are closed.

Proposition 5.1.33. *Let X be a Hausdorff topological space. If $C \subseteq X$ is a compact then C is closed in X.*

Proof. Let $Y = X \setminus C$ and fix $y \in Y$, then for all $x \in X$ there exists open disjoint sets U_x and V_x containing x and y respectively. Then $(U_x)_{x\in C}$ is a an open cover of C, thus there exists a finite subcover $(U_x)_{x\in C'}$ for some finite subset $C' \subseteq C$. Then $V = \bigcap_{x\in C'} V_x$ is an open set containing y contained in Y, and thus C is closed. □

Secondly we have that closed sets of compact spaces are compact.

Proposition 5.1.34. *Let X be a compact topological space. If $C \subseteq X$ is a closed subset of X then C is compact.*

Proof. As C is a closed set we get that $X \setminus C$ is open. Let $\{U_i\}_{i\in I}$ be any open cover of C. Then $\{X \setminus C\} \cup \{U_i\}_{i\in I}$ is an open cover of X. Therefore as X is compact there exists a finite subcover $\{X \setminus C\} \cup \{U_j\}_{j\in J}$ of X for some finite index set $J \subseteq I$. Then we get that $\{U_j\}_{j\in J}$ is an open cover of C. Therefore, as $\{U_i\}_{i\in I}$ was arbitrary, it follows that C is compact. □

The following proposition will be useful for when we want to prove that two spaces are homeomorphic.

Proposition 5.1.35. *If $f : X \to Y$ is continuous and bijective map and X is compact and Y is Hausdorff, then f is a homeomorphism.*

Proof. We will prove this via Proposition 5.1.7. Let U be a closed subset of X then by Proposition 5.1.34, U is compact. Then as the image of compact sets are compact we get that $f(U)$ is compact. Then by Proposition 5.1.33 we get that $f(U)$ is closed. Thus f^{-1} is continuous by Proposition 5.1.7 and therefore f is an homeomorphism. □

5.2. **Topological Groups.** Before we begin studying profinite groups we will need some basic results about topological groups. The proofs and exposition will follow Chapter III in [2]. Before we introduced a topology on a set, but now we instead let the underlying set be a group.

Definition 5.2.1. A *topological group* is a triple $(G, \cdot, \mathcal{T})$ where $(G, \cdot)$ is a group and $(G, \mathcal{T})$ is a topological space such that

(i) The map $G \times G \to G$ define by $(a, b) \mapsto ab$ is continuous.
(ii) The map $G \to G$ defined by $a \mapsto a^{-1}$ is continuous.

We then say that the group structure and the topology are compatible on G. We will often, as with groups and topological spaces, denote a topological group only by its underlying set.

Example 5.2.2. Here are some examples of topological groups

(a) The additive group $(\mathbb{R}^n, +)$ is a topological group with the standard topology.
(b) Endow $\mathbb{C}$ with the standard topology generated by as a basis by all the open balls $B_r(z)$, $z \in \mathbb{C}$ and $r \in \mathbb{R}$. Let $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$, that is the unit circle around the origin. Note that $\mathbb{T}$ forms a group under multiplication. If we endow $\mathbb{T}$ with the subspace topology given by the standard topology on $\mathbb{C}$ we get that $\mathbb{T}$ is a topological group.

We also have following useful proposition for proving that something is a topological group.

Proposition 5.2.3. *Let G be a group and let $(G, \mathcal{T})$ be a topological space. Then G is a topological group if and only if the map $(x, y) \mapsto xy^{-1}$ is continuous.*

Proof. Assume that G is topological group, then it follows that $(x, y) \mapsto xy^{-1}$ is continuous as it the map $(\mathsf{id}_G \times (x \mapsto x^{-1}))$ composed with $(x, y) \mapsto xy$. Conversely assume that $(x, y) \mapsto xy^{-1}$ is continuous. Then it follows that the map $x \mapsto x^{-1}$ is continuous as it is given by the maps $x \mapsto (e, x) \mapsto ex^{-1} = x^{-1}$. By pre-composing $(x, y) \mapsto xy^{-1}$ with $(\mathsf{id}_G \times (x \mapsto x^{-1}))$ we get that $(x, y) \mapsto xy$ is continuous. □

Definition 5.2.4. Let $W \subseteq G$. Then we say that W is *symmetric* if $W^{-1} = W$.

Proposition 5.2.5. *Let $a, b \in G$. Then the following maps $G \to G$ given by $x \mapsto ax$, $x \mapsto xa$, and $x \mapsto axb$ respectively are homeomorphisms.*

Proof. From the first condition it follows that the morphism $x \mapsto ax$ and $x \mapsto xa$ are continuous for any fixed $a, b \in G$ as $x \mapsto ax$ and $x \mapsto xa$ is equivalent to $x \mapsto (a, x) \mapsto ax$ and $x \mapsto (x, a) \mapsto xa$ respectively. It also follows that $x \mapsto axb$ is continuous as it is the composition of the two maps $x \mapsto ax$ and $x \mapsto xb$. Note that especially $x \mapsto a^{-1}x$, $x \mapsto xa^{-1}$ and $x \mapsto a^{-1}xb^{-1}$ are also continuous. Thus the maps $x \mapsto ax$, $x \mapsto xa$, and $x \mapsto axb$ for some fixed $a, b \in G$ are homeomorphism from G to G. □

Corollary 5.2.6. *Let $U \subseteq G$ be an open neighbourhood of $e \in G$. Then it follows that Ua and aU are open neighbourhoods of a for all $a \in G$. Likewise if V is a open neighbourhood of $a \in G$ then $a^{-1}V$ and Va^{-1} are open neighbourhoods of $e \in G$.*

Proof. This follows from Proposition 5.2.5 as Ua is the image of U under the homeomorphism $x \mapsto xa$, thus open. Likewise it follows that aU is a open neighbourhood of x as it is the image of U under the homeomorphism $x \mapsto ax$. Now if V is an open neighbourhood of a it follows that $a^{-1}V$ and Va^{-1} are open neighbourhoods of e as they are the image of V under the maps $x \mapsto a^{-1}x$ and $x \mapsto xa^{-1}$ respectively. □

We therefore have a one to one correspondence between the open neighbourhoods of a point and the open neighbourhoods of the identity element. Thus it is enough to know what the open neighbourhoods around the identity are to know what the open neighbourhoods around any point are. For the next proposition we will need to know what a filter is.

Definition 5.2.7. A *filter* on a set X is a non-empty subset $\mathscr{F}$ of the power set of X such that the following properties are fulfilled:

(a) If $F \subseteq A \subseteq X$ and $F \in \mathscr{F}$, then $A \in \mathscr{F}$.
(b) If $(A_i)_{i \in I} \subseteq \mathscr{F}$ is a finite collection of subsets of $\mathscr{F}$ then $\bigcap_{i \in I} A_i \in \mathscr{F}$.
(c) The empty set is not in $\mathscr{F}$.

We will now also define what a filter base is.

Proposition 5.2.8. *Let $\mathscr{B}$ be a set of subset of a set X. Then*

$$\mathscr{F} = \{A \subseteq X \mid B \subseteq A \text{ for some } B \in \mathscr{B}\}$$

is a filter if the following condition are fulfilled.

(a) Let $A, B \in \mathscr{B}$. Then $A \cap B \in \mathscr{B}$.
(b) The empty set in not contained in $\mathscr{B}$ and $\mathscr{B} \neq \emptyset$.

Proof. The first condition for begin a filter is fulfilled by $\mathscr{F}$ by definition. By induction using (a) the second condition for begin a filter is fulfilled by $\mathscr{F}$. Lastly the last condition for begin a filter is fulfilled by $\mathscr{F}$ via (b). □

Definition 5.2.9. A set of subset fulfilling the condition in the above proposition is called a *filter base* of $\mathscr{F}$.

Example 5.2.10. If X is topological space, then the collection of all neighbourhoods of a point $x \in X$ is a filter. We call this filter the *neighbourhood filter* of x. In this case a basis for $\mathscr{F}$ is the set of all open sets containing x.

We can now state the next proposition which says that if we have a filter on a group fulfilling certain condition then this filter induces a compatible topology on this group where the filter is precisely the neighbourhood filter of e.

Proposition 5.2.11. *Let G be a group and let $\mathscr{F}$ be a filter fulfilling the following properties:*

(a) Let $U \in \mathscr{F}$, then there exists a $V \in \mathscr{F}$ such that $V \cdot V \subseteq U$
(b) Let $U \in \mathscr{F}$, then $U^{-1} \in \mathscr{F}$.

(c) For all $a \in G$ and all $V \in \mathscr{F}$, we have that $aVa^{-1} \in \mathscr{F}$.

Then there is a unique topology compatible with the group structure on G such that $\mathscr{F}$ is the neighbourhood filter of e. Moreover in this topology the neighbourhood filter of a point $a \in G$ is the same as the filters $a\mathscr{F}$ and $\mathscr{F}a$. The equivalent properties needed to be fulfilled for a filter base $\mathscr{B}$ are the following.

(a) For any $U \in \mathscr{B}$ there exists a $V \in \mathscr{B}$ such that $V \cdot V \subseteq U$.
(b) For any $U \in \mathscr{B}$ there exists a $V \in \mathscr{B}$ such that $V^{-1} \subseteq U$.
(c) For any $a \in G$ and any $U \in \mathscr{B}$, there exists a $V \in \mathscr{B}$ such that $V \subseteq aVa^{-1} \subseteq U$.

Proof. To show this we will firstly show that $\mathscr{F}$ defines a topology, via Proposition 5.1.13. Secondly we will show that this topology is compatible with the group structure on G. Let $\mathcal{B}(x) = x\mathscr{F}$. Now the collection of all $\mathcal{B}(x)$ fulfills the first condition and the second condition of Proposition 5.1.13 as $\mathscr{F}$ is a filter. Thus it remains to show that the collection of $\mathcal{B}(x)$ fulfills the third and fourth condition. To show that $\mathcal{B}(x)$ fulfills the third condition for all $x \in X$ we will show that for any $U \in \mathscr{F}$ there exists a $V \in \mathscr{F}$ such that $V \cdot V^{-1} \subseteq U$ as this implies that the result holds for all $\mathcal{B}(x)$. Let $U \in \mathscr{F}$. Firstly by (a) there exists a $W \in \mathscr{F}$ such that $W \cdot W \subseteq U$. By (b) we also have that $W^{-1} \in \mathscr{F}$, hence as $\mathscr{F}$ is a filter $W \cap W^{-1} \in \mathscr{F}$. Thus there exists a $V \in \mathscr{F}$ such that $V \subseteq W \cap W^{-1}$. Thus $V^{-1} \subseteq W$ and therefore $V \cdot V^{-1} \subseteq W \cdot W \subseteq U$. By this it now follows that every $U \in \mathscr{F}$ contains e. Therefore third condition of Proposition 5.1.13 is fulfilled. We now show that fourth condition is fulfilled. Let $V \in \mathscr{F}$ be arbitrary set and let $W \in \mathscr{F}$ be a set such that $W \cdot W \subseteq V$, which exists by (a). Then for any $x \in aW$ we have that $xW \subseteq aW \cdot W \subseteq aV$, thus aV is in the filter $x\mathscr{F} = \mathcal{B}(x)$.

Now we need to show that this topology given by Proposition 5.1.13 is compatible with the group structure on G. To show this we will show that the map $(x, y) \mapsto xy^{-1}$ is continuous. We denote this map f. Let $a, b \in G$ be two arbitrary points and let U be an arbitrary neighbourhood of e, then $ab^{-1}U$ is a neighbourhood of ab^{-1}. We want to show that there exists a neighbourhood U' of (a, b) such that for all $(x, y) \in U'$, $xy^{-1} \in ab^{-1}U$. Let $V = bUb^{-1}$, then V is a neighbourhood of e by (c). By (a) and (b) we know that there exists a neighbourhood W of e such that $W \cdot W^{-1} \subseteq V$. Let $U' = aW \times bW$, then U' is a neighbourhood of (a, b). Let $(x, y) \in U'$, then $x = au$ and $y = av$, where $u, v \in W$. Then $xy^{-1} \in ab^{-1}U$ if $(ab^{-1})^{-1}xy^{-1} \in U$. This is equivalent to that $uv^{-1} \in bUb^{-1}$ as $(ab)^{-1}xy^{-1} = b^{-1}uv^{-1}b$. But this is true as we choose $W \cdot W^{-1} \subseteq V = bUb^{-1}$. Thus $(x, y) \mapsto xy^{-1}$ is continuous by Proposition 5.1.12. Therefore finally by Proposition 5.2.3 G is a topological group. □

So now given a group G we can get a compatible topological structure on G by finding a suitable filter or filter base.

6. Inverse Limits

6.1. **Inverse limits of sets.** We will start by looking at inverse limits of sets, which we will later generalise to inverse limits of topological spaces and finally to topological groups, which we will need later to define what a profinite group is. First we will define what we take the inverse limit of and also give two definitions of the inverse limit. The proofs and exposition will follow Chapter 1.1 about inverse limits in [10].

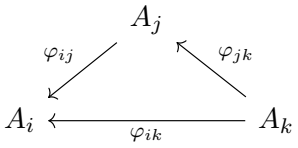
Definition 6.1.1. An *directed partially ordered* set (or a *directed poset*) is a tuple $(I, \leq)$ such that the following conditions are fulfilled

(a) $i \leq i$ for all $i \in I$.
(b) If $i \leq j$ and $j \leq i$ then $i = j$.
(c) If $i \leq j$ and $j \leq k$ then $i \leq k$.

(d) For all $i, j \in I$ there exists a $k \in I$ such that $i \leq k$ and $j \leq k$.

We will say poset instead of partially ordered set and we will often denote a directed poset only by its underlying set.

Definition 6.1.2. An *inverse system* over an directed partially ordered set I is a double (A_i, φ_{ij}), where the A_i's are sets and $\varphi_{ij} : A_j \to A_i$, $\varphi_{ii} = \mathsf{id}_{A_i}$ are maps between the sets, such that the following diagram commutes for any $i \leq j \leq k$



Now there are so to say two definitions of the inverse limit of an inverse system, one is more concrete, whilst one is the more abstract definition. We will first give the concrete definition and after that give the abstract definition. Then finally we will prove that the concrete definition is indeed a inverse limit in the abstract sense.

Definition 6.1.3. Let (A_i, φ_{ij}) be an inverse system over a directed poset I. The *inverse limit* $A = \varprojlim A_i$ of (A_i, φ_{ij}) is the following subset of the set $\prod_{i \in I} A_i$,

$$\varprojlim A_i = \{a \in \prod_{i \in I} A_i \mid a_i = \varphi_{ij}(a_j) \text{ for all } i \leq j \text{ in } I\}.$$

Note that we will only use $\varprojlim A_i$ to refer to the set above and not to the inverse limit in the abstract sense.

Informally one can of think of this construction kind of like when construction the real numbers one "completes" the rational numbers by taking all Cauchy sequences of rational numbers.

Example 6.1.4. The simplest example is the case where one has the inverse system over an directed poset I consisting of sets $(X_i, \subseteq)$ looking as $X_0 \supseteq X_1 \supseteq ... \supseteq X_i \supseteq X_{i+1} \supseteq ...$, where the maps are all inclusions. Then we get that $\varprojlim X_i = \bigcap_{i \in I} X_i$. So in some sense inverse limits are like generalised intersections. The inverse limit can be seen as the smallest object we can "glue" together from the objects that we take the inverse limit of.

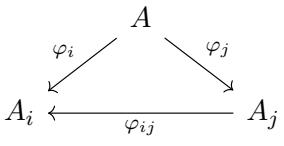
Example 6.1.5. Given any set A we can always define the constant inverse system (A, id_A) over an arbitrary directed poset I consisting only of A's and identity maps between them for any index set I. For example if we take I to be equal to $\mathbb{N}$ it looks like this (a bit misleading in general as the A's need not lie in a straight line for a arbitrary index set I)

$$A \xleftarrow[\mathsf{id}_A]{} A \xleftarrow[\mathsf{id}_A]{} A \xleftarrow[\mathsf{id}_A]{} A \xleftarrow[\mathsf{id}_A]{} A \xleftarrow[\mathsf{id}_A]{} ...$$

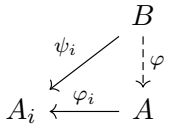
In these cases we simply get that $\varprojlim A = A$.

We will now give the more abstract definition of an inverse limit. This kind of construction is generally not the first imagined. Instead this is the definition we get if translate properties of objects into properties of morphism and objects.

Definition 6.1.6. Let (A_i, φ_{ij}) be an inverse system over an directed poset I. We say that (A, φ_i), where $\varphi_i : A \to A_i$, is a *cone* over (A_i, φ_{ij}) if the following diagram commutes for all $i \leq j$



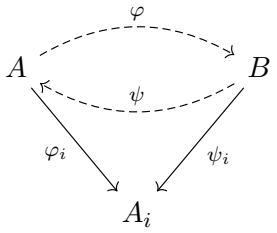
Definition 6.1.7. Let (A_i, φ_{ij}) be an inverse system and let (A, φ_i) be a cone over (A_i, φ_{ij}). We say (A, φ_i) is the *inverse limit* of the inverse system if the following universal property is fulfilled. If (B, ψ_i) is any cone over (A_i, φ_{ij}), then there exist a unique morphism $\varphi : B \to A$ such that the following diagram commutes for all $i \in I$



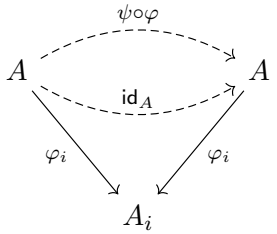
We will now prove that the inverse limit is unique up to isomorphism, and thus we can speak of *the* inverse limit (up to isomorphism).

Proposition 6.1.8. *Let (A_i, φ_{ij}) be an inverse system over a directed poset I. If (A, φ_i) and (B, ψ_i) are inverse limits of the inverse system then $A \cong B$.*

Proof. By the universal property of inverse limits we have the following commutative diagram for all $i \in I$.



This in turn gives us the following commutative diagram.



By the universal property the morphism from A to A must be unique and hence $\psi \circ \varphi = \mathsf{id}_A$. By the same method we get that $\varphi \circ \psi = \mathsf{id}_B$. Therefore $A \cong B$. □

The proof strategy here is the same as when in general proving that objects define by universal properties are isomorphic, for example fibre products, free groups etc. The important thing that creates the isomorphism here is that the induced morphism is unique.

We now show that "concrete" definition actually is an inverse limit in the sense of the abstract definition.

Proposition 6.1.9. *Let (A_i, φ_{ij}) be an inverse system. Then $A = \varprojlim A_i = \{a \in \prod_{i \in I} A_i \mid a_i = \varphi_{ij}(a_j)$ for all $i \leq j$ in $I\}$ is the inverse limit of (A_i, φ_{ij}).*

Proof. Let $\varphi_i : A \to A_i$ be the projection onto the ith coordinate. Then (A, φ_i) is a cone over (A_i, φ_{ij}) by definition of A. Thus we now only need to show that A fulfills the universal property. Let (B, ψ_i) be any other cone over (A_i, φ_{ij}). We then define the map $\varphi : B \to A$ to be the map given by $b \mapsto (\psi_i(b))_{i \in I}$. Then $\psi_i = \varphi_i \circ \varphi$ for all $i \in I$. To show that this map is unique let

$\psi : B \to A$ be another map such that $\psi_i = \varphi_i \circ \psi$. Then $\varphi_i \circ \psi = \varphi_i \circ \varphi$ for all $i \in I$. This implies that $\psi = \varphi$ as each φ_i's are projections onto the ith coordinate respectively. □

We now define what a morphism between two inverse systems over the same directed poset is.

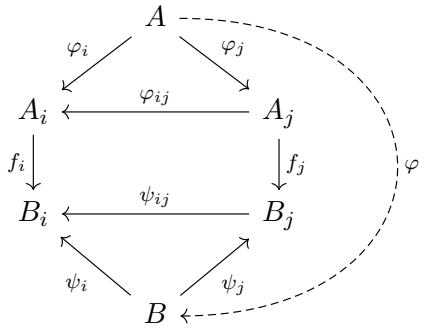
Definition 6.1.10. Let (A_i, φ_{ij}) and (B_i, ψ_{ij}) be inverse systems of sets over the same directed poset I. A *morphism* $f : (A_i, \varphi_{ij}) \to (B_i, \psi_{ij})$ is a set of functions $f_i : A_i \to B_i$ such that the following diagram commutes for all $i \leq j$

$$\begin{array}{ccc} A_i & \xleftarrow{\varphi_{ij}} & A_j \\ {\scriptstyle f_i}\downarrow & & \downarrow{\scriptstyle f_j} \\ B_i & \xleftarrow[\psi_{ij}]{} & B_J \end{array}$$

We call the f_i the component morphism of f. Given (A_i, φ_{ij}), (B_i, ψ_{ij}) and (C_i, θ_{ij}) and morphisms $f : (A_i, \varphi_{ij}) \to (B_i, \psi_{ij})$ and $g : (B_i, \psi_{ij}) \to (C_i, \theta_{ij})$ we define the composition $g \circ f$ as the composition of their component morphism, that is $g_i \circ f_i$.

We will now see that we can construct the inverse limit of a morphism as well.

Definition 6.1.11. Let (A_i, φ_{ij}) and (B_i, ψ_{ij}) be inverse system over a directed poset I and let $f : (A_i, \varphi_{ij}) \to (B_i, \psi_{ij})$ be a morphism of inverse systems. Let A and B be the respective inverse limits. We then define $\varprojlim f : A \to B$ to be the morphism given by the universal property of inverse limits. To be more precise, $(A, f_i \circ \varphi_i)$ is a cone over (B_i, ψ_{ij}), thus by the universal property of inverse limits we obtain a map $\varphi : A \to B$. We define $\varprojlim f$ to be precisely this φ.



Example 6.1.12. Let (A_i, φ_{ij}) and (B_i, ψ_{ij}) be two inverse system over a directed poset I and let $f : (A_i, \varphi_{ij}) \to (B_i, \psi_{ij})$ be a morphism. Then the induced map from $\varprojlim A_i \to \varprojlim B_i$ is the map given by $(x_i)_{i \in I} \mapsto (f_i(x_i))_{i \in I}$. Therefore we easily see that in the concrete case that if the f_i's are all injective then the induced map is injective. Furthermore as all inverse limits are unique up to isomorphism this holds for all induced morphisms between two inverse limits where the component maps are injective.

6.2. **Profinite Spaces.** We will now extend our definition of inverse limit for topological spaces. The general setup is still the same, though now we replace sets with topological spaces and functions with continuous functions.

Definition 6.2.1. Let (A_i, φ_{ij}) be an inverse system over a directed poset I, where all A_i's are topological space and φ_{ij} is a continuous map for all $i \leq j$. Then we endow $\varprojlim A_i$ with the subspace topology given by the product topology on $\prod_{i \in I} A_i$.

For the abstract definition we now require that there must exists a unique continuous map φ. Thus all the proposition and proofs hold if we replace sets by topological spaces and maps by continuous

maps except we need to show that the map given in the proof of Proposition 6.1.9 is continuous. We now restate and proof the Proposition for topological spaces.

Proposition 6.2.2. *Let (A_i, φ_{ij}) be an inverse system of topological spaces over a directed poset I. Then $A = \varprojlim A_i = \{a \in \prod_{i\in I} A_i \mid a_i = \varphi_{ij}(a_j) \text{ for all } i \leq j \text{ in } I\}$ is the inverse limit of (A_i, φ_{ij}).*

Proof. Let (B, ψ_i) be any other compatible topological space. Then define the map $f : B \to A$ to be the map given by $b \mapsto (\psi_i(b))_{i\in I}$. Now we only need to show that f is continuous as the rest follows by the proof of Proposition 6.1.9. Let V be an open set in A, then

$$V = A \cap \left(\bigcup_{l\in L} \left(\prod_{i\notin J_l} A_i \times \prod_{j\in J_l} U_{lj} \right) \right)$$

where $J_l \subseteq I$ is a finite subset for all $l \in L$ and $U_{lj} \subseteq A_j$ is open for all $j \in J$ and all $l \in L$. Then

$$f^{-1}(V) = B \cap \left(\bigcup_{l\in L} \left(\bigcap_{j\in J_l} \psi_j^{-1}(U_{lj}) \right) \right)$$

which is open in B as J_l is finite for all $l \in L$ and each $\psi_j^{-1}(U_{lj})$ is open as each ψ_j is continuous. Thus f is a continuous function. □

For this section we only prove all results for the concrete inverse limit, $\varprojlim A_i$, but as the inverse limit is unique up to isomorphism this implies that the results hold in general.

Proposition 6.2.3. *Let (A_i, φ_{ij}) be an inverse system of Hausdorff topological spaces over a directed poset I. Then $\varprojlim A_i$ is closed subset of $\prod_{i\in I} A_i$.*

Proof. To prove this we will show that $\prod_{i\in I} A_i \setminus \varprojlim A_i$ is an open set. Let $B = \prod_{i\in I} A_i \setminus \varprojlim A_i$ and let $(a_i)_{i\in I} \in B$. Then there exists i, j such that $i < j$ but $\varphi_{ij}(a_j) \neq a_i$. As A_i is Hausdorff there exists open neighbourhoods U and V of $\varphi_{ij}(a_j)$ and a_i such that $U \cap V = \emptyset$. Let U' be an open neighbourhood of a_j in A_j such that $\varphi_{ij}(U') \subseteq U$. Such a neighbourhood exists as we can for example pick $U' = \varphi_{ij}^{-1}(U)$. Consider the open set $W = \prod_{k\in I} V_i$ where $V_i = V$, $V_j = U'$ and $V_k = X_k$ for all $k \neq i, j$. Assume (towards a contradiction) that there exists a $b_j \in U'$ such that $\varphi_{ij}(b_j) = b_i \in V$. Then this would contradict that $U \cap V = \emptyset$ and therefore W is an open set containing $(a_i)_{i\in I}$ contained in B. Thus B is open and therefore $\varprojlim A_i$ is closed. □

To prove this next proposition we will need Tychnoff's theorem. Unfortunately we won't be able to prove it here, so therefore we will have to take it as a black box. For a proof of Tychnoff's theorem see for example Chapter 5 in [8].

Theorem 6.2.4 (Tychnoff's theorem)**.** *Let $(A_i)_{i\in I}$ be a collection of compact spaces, then $\prod_{i\in I} A_i$ is a compact space.*

We will now see how some topological properties transfer to the inverse limit from the inverse system.

Proposition 6.2.5. *Let (A_i, φ_{ij}) be an inverse system over a directed poset I. Then if every A_i is compact, Hausdorff and totally disconnected then the inverse limit $\varprojlim_{i\in I} A_i$ is compact, Hausdorff and totally disconnected.*

Proof. Let $A = \varprojlim A_i$. By Tychnoff's theorem we get that $\prod_{i\in I} A_i$ is compact as each A_i is compact. This in turn implies that $\varprojlim A_i$ is compact by Proposition 5.1.34, as by Proposition 6.2.3 $\varprojlim A_i$ is a closed subset of $\prod_{i\in I} A_i$. Now we show that A is Hausdorff. It is enough to show that $\prod_{i\in I} A_i$ is Hausdorff as then the induced subspace topology will be Hausdorff as well. Let

$(x_i)_{i\in I} \neq (y_i)_{i\in I}$ be two distinct points in $\prod_{i\in A_i}$. Then there exists a $j \in I$ such that $x_j \neq y_j$. Then, as A_j is Hausdorff, there exists open disjoint neighbourhoods $U_j, V_j \subseteq A_i$ of x_j and y_j respectively. Then $U = p_i^{-1}(U_i)$ and $V = p_i^{-1}(V_i)$ are open disjoint neighbourhoods of $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ respectively such that $U \cap V = \emptyset$. Therefore $\prod_{i\in I} A_i$ is Hausdorff. It now follows that A is Hausdorff as A is endowed with the subset topology. Lastly we will show that A is totally disconnected. It is again enough to show that $\prod_{i\in I} A_i$ is totally disconnected. Assume (towards a contradiction) that $\prod_{i\in I} A_i$ is not totally disconnected. Then there exists a connected subset $U \subseteq \prod_{i\in I} A_i$ such that U contains two distinct points $(a_i)_{i\in I}, (b_i)_{i\in I} \in U$. Since the points are distinct there exists a $j \in I$, such that $a_j \neq b_j$. Since p_j is a continuous function $p_j(U)$ is a connected subset by Proposition 5.1.21 of A_j, but $p_j(U)$ is not a singleton as $p_j(a), p_j(b) \in p_j(U)$, which contradicts that A_j is totally disconnected. Thus $\prod_{i\in I} A_i$ is totally disconnected and thus A is totally disconnected. □

Before we can prove that the inverse limit of a system of non-empty, compact and Hausdorff spaces indeed is non-empty we need a equivalent condition to compactness for topological spaces. We say that a family of topological subspaces has the *finite intersection property* if the intersection of a finite number of topological spaces from the family is nonempty.

Lemma 6.2.6. *A topological space is compact if and only if each family of closed sets which has the finite intersection property have a nonempty intersection.*

Proof. Note that for any family of closed subset $\{A_i\}_{i\in I}$ of X the following holds $X \setminus \bigcup\{A_i\}_{i\in I} = \bigcap\{X \setminus A_i\}_{i\in I}$. Therefore $\{A_i\}_{i\in I}$ is a cover if and only if $\bigcap\{X \setminus A_i\}_{i\in I}$ is empty. We first prove the forward direction. Assume that X is compact. Then assume, for contradiction, that there exists a closed family of subset $\{B_j\}_{j\in J}$ with the finite intersection property that has a empty intersection. Then it follows that $\{X \setminus B_j \mid {}_{j\in J}\}$ is an open cover of X that has no finite subcover. Thus contradicting that X is compact and therefore no such family can exists. Conversely assume that every closed family which has the finite intersection property has a non-empty intersection. Let $\{U_i\}_{i\in I}$ be an open cover of X. If $\{U_i\}_{i\in I}$ has no finite subcover, then $\{X \setminus U_i\}_{i\in I}$ is a family of closed subset with the finite intersection property that contradicts the assumption, thus $\{U_i\}_{i\in I}$ must have a finite subcover. As $\{U_i\}_{i\in I}$ was an arbitrary open cover X is compact. □

Proposition 6.2.7. *Let (A_i, φ_{ij}) be an inverse system of non-empty, compact and Hausdorff topological spaces over a directed poset I. Then $A = \varprojlim A_i$ is nonempty.*

Proof. For each $j \in I$, define the subsets Y_j of $\prod_{i\in I} A_i$ to be set of all $(a_i)_{i\in I}$ such that $\varphi_{kj}(a_j) = a_k$ for all $j \geq k$. We now show that each Y_j is non empty and closed subset of $\prod_{i\in I} A_i$. That each Y_j is non-empty subset follows from the axiom choice. To see this let $I' = \{i \in I \mid i \not\leq j\}$. Then for each $(b)_{i\in I'} \in \prod_{i\in I'} A_i$ can be extend to an element of Y_j via the morphism φ_{kj}. It is therefore enough to show that $\prod_{i\in I'} A_i$ is nonempty but this follows from the axiom of choice as each A_i is nonempty. We now show that each Y_j is a closed subset by showing that $(\prod_{i\in I} A_i) \setminus Y_j$ is an open subset. Let $a \in (\prod_{i\in I} A_i) \setminus Y_j$, then there exists a $j \leq k$ such that $\varphi_{jk}(a_k) \neq a_j$. Thus as A_j is Hausdorff there exists disjoint open subsets U and V of $\varphi_{jk}(a_k)$ and a_j respectively. Let $U' \subseteq A_k$ be an open subset such that $\varphi_{jk}(U') \subseteq U$. Now define $W = \prod_{i\in I} V_i$, where $V_j = U'$, $V_k = V$ and $V_i = A_i$ for all $i \neq j, k$. Then W is an open subset disjoint from Y_j, thus $(\prod_{i\in I} Y_i) \setminus Y_j$ is open, and therefore Y_j is closed. Note that $\{Y_j\}_{j\in I}$ has the finite intersection property, as if $j \leq j'$ then $Y_{j'} \subseteq Y_j$ as I is a directed poset. By Lemma 6.2.6 it now follows that $\bigcap\{Y_j\}_{j\in I}$ is non empty as $\prod_{j\in I} A_i$ is compact. Finally $\bigcap\{Y_j\}_{j\in I} = \varprojlim A_i$, and thus the result follows. □

Proposition 6.2.8. *Let $f : (A_i, \varphi_{ij}) \to (B_i, \psi_{ij})$ be a morphism of inverse systems of non-empty, compact and Hausdorff topological spaces over a directed poset I. If each component f_i is surjective then $\varprojlim f_i : \varprojlim A_i \to \varprojlim B_i$ is surjective.*

Proof. Let $A = \varprojlim A_i$ and $B = \varprojlim B_i$ be the inverse limit of (A_i, φ_{ij}) and (B_i, ψ_{ij}) respectively. Now let $(b_i) \in B$ be a fixed arbitrary element. Define $\tilde{A}_i = f_i^{-1}(b_i)$. Then since b_i is closed in B_i each $\tilde{A}_i$ is closed, and thus compact as each A_i is compact. Note that it holds for $\varphi_{ij}(\tilde{A}_j) \subseteq \tilde{A}_i$ for all $i, j \in I$ such that $i \leq j$. To show this more precisely, let $a \in \varphi_{ji}(\tilde{A}_j)$. We know by the definition of a morphism that $f_i \circ \varphi_{ij} = \psi_{ij} \circ f_j$. Therefore if $a' \in \tilde{A}_j$ we have that $f_i(\varphi_{ij}(a')) = \psi_{ij}(f_j(a')) = \psi_{ij}(b_j) = b_i$. Hence it is the case that $f_i(a) = b_i$ for any $a \in \varphi_{ij}(\tilde{A}_j)$ and therefore $\varphi_{ij}(\tilde{A}_j) \subseteq \tilde{A}_i$. Thus $(\tilde{A}_i, \varphi_{ij})$ form a inverse system of non-empty, compact and Hausdorff topological spaces over I. By Proposition 6.2.7 it follows that $\tilde{A} = \varprojlim \tilde{A}_i$ is nonempty. Let $(\tilde{a}_i) \in \tilde{A}$, then $f((\tilde{a}_i)_{i \in I}) = (b_i)_{i \in I}$, and therefore f is surjective as $\tilde{A} \subseteq A$ and as $b_i \in B$ was arbitrary. □

Corollary 6.2.9. *Let (A_i, φ_{ij}) be a inverse system of compact Hausdorff topological spaces over a directed poset I and let X be a compact Hausdorff topological space. Let (X, ψ_i) be a cone over (A_i, φ_{ij}). If ψ_i is surjective for all $i \in I$ then the induced map $f : X \to \varprojlim A_i$ is surjective.*

Proof. We can "view" X as the constant inverse system (X, id_X) over I, that is consider the constant inverse system defined by X. Then ψ_i's define a morphism from the constant inverse system of X to (A_i, φ_{ij}). Thus, as each ψ_i is surjective, the induced map $f : X \to \varprojlim A_i$ is surjective by Proposition 6.2.8. □

Lemma 6.2.10. *Let X be a compact Hausdorff topological space and let $x \in X$ be a point. Then the connected component of C of x is the intersection of all clopen (close and open) sets containing x.*

Proof. Let $U = \bigcap_{i \in I} U_i$, where each U_i is a clopen set containing x. Then $C \subseteq U_i$ as otherwise C wouldn't be connected and therefore $C \subseteq U$. If we now can prove that U is connected we will have $C = U$ as by definition the connected component of a point is the maximal connected set containing that point. Assume $U = V \cup W$, where V and W are disjoint closed subsets of X. We now will show that either V or W is empty. As X is compact and Hausdorff, X is normal by 5.1.32, therefore there exists disjoint open sets V' and W' containing V and W respectively. Note that $(X \setminus (V' \cup W')) \cap (\bigcap_{i \in I} U_i) = \emptyset$, which is equivalent to that $(V' \cup W') \cup (\bigcup_{i \in I}(X \setminus U_i)) = X$. Therefore it now follows, by compactness of X, that there exists a finite index set $I' \subseteq I$ such that $(V' \cup W') \cup (\bigcup_{i \in I'}(X \setminus U_i)) = X$, which is equivalent to that $(X \setminus (V' \cup W')) \cap (\bigcap_{i \in I'} U_i) = \emptyset$. Let $A = \bigcap_{i \in I'} U_t$, and note that A is a clopen neighbourhood of x as I' is finite. Thus $x \in (A \cap V') \cup (A \cap W') = A$. Say, without loss of generality, that $x \in (A \cap V')$. We know that $A \cap V'$ is open, but it is also closed as $A \cap V' = (X \setminus A \cap W') \cap A$, which is closed. Therefore $U \subseteq A \cap V' \subseteq V'$. Then $U \cap W \subseteq U \cap W' = \emptyset$ and thus $W = \emptyset$. Therefore we conclude that U is connected and therefore it follows that $C = U$. □

Definition 6.2.11. A topological space X is called a *profinite space* if it is homeomorphic to the inverse limit of finite topological spaces endowed with the discrete topology.

We say that an equivalence relation R on a topological space X is open if for each $x \in X$, xR is an open subset of X. Note that if an equivalence relation R is open then it is also closed as each equivalence class is the complement of the union of the other (equivalence classes form a partition of a set).

Theorem 6.2.12. *Let X be a topological space. Then following conditions are equivalent.*

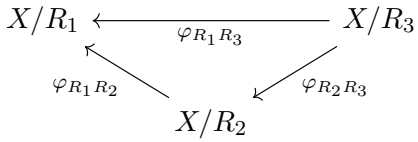
(a) X is a profinite space;
(b) X is compact, Hausdorff and totally disconnected;
(c) X is compact, Hausdorff and admits a base of clopen sets for its topology.

Proof. First we begin by proving that $(a) \Rightarrow (b)$. We note that the discrete topology on finite spaces is compact, Hausdorff and totally disconnected. Thus it follows by Proposition 6.2.5 that

X is compact, Hausdorff and totally disconnected.

We now prove that $(b) \Rightarrow (c)$. By Proposition 5.1.28 the result follows if we can prove that given any open subset U of X, there exists a clopen set C such that $x \in C \subseteq U$ for all $x \in U$. Let U be any open subset of X and let $x \in U$ be an arbitrary point. Let $C = \bigcap_{t \in T} C_t$ be the intersection of all clopen neighbourhoods of x. By Lemma 6.2.10 it follows that $\bigcap_{t \in T} C_t = \{x\}$. As $X \setminus U$ is closed set disjoint from C it follows by compactness of X that there exists a finite subset T' of T such that $(X \setminus U) \cap (\bigcap_{t \in T'} C_t) = \emptyset$ as this is equivalent to that $U \cup (\bigcup_{t \in T} (X \setminus U_t)) = X$ has a finite subcover. Thus $\bigcap_{t \in T'} C_t$ is a clopen set containing x that is contained in U.

We finally prove that $(c) \Rightarrow (a)$. Let $\mathcal{R}$ denote the collection of all open equivalence classes on X. Note that X/R will be a finite and discrete topological space for any $R \in \mathcal{R}$ as X is compact. Define a order $\leq$ on $\mathcal{R}$ by that $R_1 \leq R_2$ if for all $x \in X$, $xR_2 \subseteq xR_1$. One easily sees that $(\mathcal{R}, \leq)$ is partially ordered set. To see that it is also directed note that for any $R_1, R_2 \in \mathcal{R}$, it holds that $R_1, R_2 \leq R_1 \cap R_2$. If $R_1 \leq R_2$ we can define the map $\varphi_{R_1 R_2} : X/R_2 \to X/R_1$ given by $\varphi_{R_1 R_2}(xR_2) = xR_1$ for all $x \in X$. Note that if $R_1 \leq R_2 \leq R_3$ the following diagram commutes.



Therefore we get that $(X/R, \varphi_{RR'})$ forms an inverse system of topological spaces over $\mathcal{R}$. Thus we can define $Y = \varprojlim_{R \in \mathcal{R}} X/R$. We want to show that $X \cong Y$. We first define the map $f_R : X \to X/R$ by $f_R(x) = xR$. Next define $f : X \to Y$ to be the map $\varprojlim f_R$. By Corollary 6.2.9 it follows that f is surjective as each f_R is, thus we only need to show that f is injective as then f will be an isomorphism as X is compact. Let $x, y \in X$ be two distinct points. Then there exists a clopen set U containing x but not y as X is Hausdorff and admits a base of clopen sets for its topology. Now consider the open equivalence relation R_U given by the partition $X - U$ and U. Then $f_{R_U}(x) \neq f_{R_U}(y)$, thus $f(x) \neq f(y)$ as $f_R = f \circ \varphi_R$. Therefore f is injective and thus bijective. □

7. Profinite Groups and Galois Extensions

In this section we will first define what a profinite group is and give a characterisation of profinite groups as well as some basic properties. Then we will show that every Galois group is a profinite group and that every profinite group can be seen as a Galois group. The proofs and exposition will follow Chapter 2 in [10].

7.1. **Profinite Groups.**

Before we can define what a profinite group is we need to extend our definition of inverse limits to topological groups. To do this we just replace the topological spaces by topological groups and the continuous maps by continuous morphisms. All the proofs in the previous section hold for topological groups except we need to show that the concrete definition is also an inverse limit for topological groups. We now restate Proposition 6.2.2 in terms of topological groups.

Proposition 7.1.1. *Let (A_i, φ_{ij}) be an inverse system of topological groups. Then $A = \varprojlim A_i = \{a \in \prod_{i \in I} A_i \mid a_i = \varphi_{ij}(a_j)$ for all $i \leq j$ in $I\}$ is the inverse limit of (A_i, φ_{ij}).*

Proof. Let $(B, \psi_i)_{i\in I}$ be a compatible topological group. Define $\varphi : B \to A$ to be the map given by $b \mapsto (\psi_i(b))_{i\in I}$. We now only need to show that φ is a morphism as the rest follows from Proposition 6.2.2. Let $b_1, b_2 \in B$, then $\varphi(b_1b_2) = (\psi_i(b_1b_2))_{i\in I} = (\psi_i(b_1)\psi_i(b_2))_{i\in I} = (\psi_i(b_1))_{i\in I}(\psi_i(b_2))_{i\in I} = \varphi(b_1)\varphi(b_2)$. Therefore φ is a group morphism. □

Definition 7.1.2. A *profinite group* is a topological group that is the inverse limit of an inverse system of finite groups endowed with the discrete topology.

Thus especially as a topological space a profinite group is a profinite space. The name profinite comes from projectively finite in the sense that under the canonical projections a profinite group is finite. Though note that a profinite group in general is not itself necassarily finite.

Example 7.1.3. Here we give some examples of profinite groups.

(a) Let G be a finite group endowed with the discrete topology. Then G is profinite as it is the inverse limit of the constant inverse system of G itself. Hence every finite group is profinite.
(b) Let $\mathbb{Z}_p$ be the set of all p-adic integers. Then it is a profinite group as $\mathbb{Z}_p \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$.[1]

Proposition 7.1.4. *Let $G = \varprojlim G_i$ be a profinite group, and let $p_i : G \to G_i$ be the projections onto the ith coordinate. Then $\mathcal{S} = \{\ker(p_i) \mid p_i : G \to G_i\}$ forms a fundamental system of neighbourhoods around the identity element in G.*

Proof. Let $\mathcal{C}$ be collection of elements on the following form

$$\left(\prod_{i\neq i_0,\dots,i_n} G_i\right) \times \{1\}_{i_0} \times \dots \times \{1\}_{i_n}$$

where $i_1, \dots, i_n \in I$ are arbitrary and $i_0 \in I$ is a element such that $i_0 \geq i_1, \dots, i_n$. We will now prove that this is a fundamental system of neighbourhoods around 1 in $\prod_{i\in I} G_i$. Let $V \subseteq \prod_{i\in I} G_i$ be an neighbourhood of 1. Then V contains an open set of the form $(\prod_{i\neq j_1,\dots,j_n} G_i) \times U_{j_1} \times \dots \times U_{j_n}$. Now let $U = (\prod_{i\neq j_0,\dots,j_n} G_i) \times \{1\}_{j_0} \times \dots \times \{1\}_{j_n}$ with $j_0 \in I$ being a element such that $j_0 \geq j_1, \dots, j_n$ (this exists as I is directed). Then $U \subseteq V$ and $U \in \mathcal{C}$. Thus $\mathcal{C}$ is a fundamental system of open neighbourhoods around 1. Now we note that $\mathcal{D} = \{G \cap C \mid C \in \mathcal{C}\}$ forms a fundamental system of open neighbourhoods around 1 in G as G is equipped with the subspace topology. We now also note that $\mathcal{D}$ is the collection of elements of the following form

$$G \cap \left(\prod_{i\neq i_0} G_i \times \{1\}_{i_0}\right)$$

as $G \cap \left(\prod_{i\neq i_0,\dots,i_n} G_i \times \{1\}_{i_0} \times \dots \times \{1\}_{i_n}\right) = G \cap \left(\prod_{i\neq i_0} G_i \times \{1\}_{i_0}\right)$. We then see that $\ker(p_i) = G \cap \prod_{i\neq i_0} G_i \times \{1\}_{i_0}$ and thus $\mathcal{D} = \mathcal{S}$. Therefore we conclude that $\mathcal{S}$ forms a fundamental system of neighbourhoods around 1 in G. □

The following proposition is a very useful.

Proposition 7.1.5. *Let G be a compact topological group and let $H \leq G$ be a subgroup. Then H is open if and only if it is of finite index and closed.*

Proof. Assume that H is open. Then we first show that it is of finite index. Note that the cosets of H is an open cover G and therefore, as G is compact, there must be a finite number of cosets. Thus H is of finite index. That H is closed follows from the fact that $G \setminus H$ will be open as

[1] In fact $\mathbb{Z}_p$ can be given the structure of a profinite ring and one can take the definition of the p-adic integers as the ring constructed by this inverse limit.

$G \setminus H = \bigcup_{gH \neq H} gH$ as gH is open for all $g \in G$ by Proposition 5.2.5. Conversely assume that H is a closed subgroup of finite index. Let $G' \subseteq G$ be the index set of the left cosets. Then by Proposition 5.2.5 we get that $g'H$ is closed for all $g' \in G'$. Therefore $N = \bigcup_{g' \neq e} g'H$ is closed. Then finally H is open as $H = G \setminus N$. □

Before we can prove the following theorem we need the following useful lemma.

Lemma 7.1.6. *Let G be a compact topological group and let $H \leq G$ be a open subgroup. Then the core of H, defined as $\mathsf{core}(H) = \bigcap_{g \in G} gHg^{-1}$, is an open subgroup.*

Proof. This follows from Proposition 7.1.5 as H is open which implies that H has finite index. Let $G' \subseteq G$ be an index set for the cosets of H. Note that $gHg^{-1} = hHh^{-1}$ if g and h lie in the same coset. Therefore we get that $\mathsf{core}(H) = \bigcap_{g \in G'} gHg^{-1}$ is open as gHg^{-1} is open for all $g \in G'$ by Proposition 5.2.5 and since G' is finite. □

We will now give a characterisation of profinite groups analog to Theorem 6.2.12.

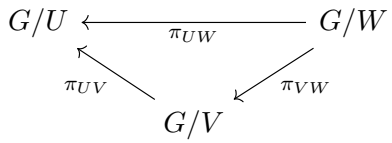
Theorem 7.1.7. *The following condition on a topological group G are equivalent.*

(a) G is a profinite group
(b) G is compact, Hausdorff and totally disconnected.
(c) G is compact, Hausdorff and the identity element 1 of G admits a fundamental system $\mathcal{S}$ of open subgroups U satisfying $\bigcap_{U \in \mathcal{S}} U = \{1\}$ and $U \trianglelefteq G$ with G/U finite.
(d) The identity element 1 of G admits a fundamental system $\mathcal{S}$ of open neighbourhoods U satisfying $U \trianglelefteq G$ for all $U \in \mathcal{S}$, with G/U being finite, and $G = \varprojlim_{U \in \mathcal{S}} G/U$.

Proof. (a) ⇒ (b):
It follows directly from Theorem 6.2.12 that G is compact, Hausdorff and totally disconnected.

(b) ⇒ (c):
By assumption we already have that G is compact and Hausdorff. We know by Theorem 6.2.12 that G admits a basis of clopen sets $\mathcal{C}$. Thus, we have a fundamental system of clopen sets around each point and therefore especially around 1. Denote this fundamental system around 1 by $\mathcal{V}$. By Lemma 6.2.10, as G is totally disconnected, we know that $\bigcap_{V \in \mathcal{V}} V = \{1\}$. If we can show that each $V \in \mathcal{V}$ contains a open normal subgroup $N \trianglelefteq G$, then the collection of all these normal subgroups would form the desired fundamental system. Therefore let $V \in \mathcal{V}$ be arbitrary. For this proof we will let X^n denote the following set $X^n = \{x_1 ... x_n \mid x_1, ..., x_n \in X\}$. As G is compact and V is a clopen subset of G we get that V is compact as closed subsets of compact Hausdorff spaces are compact. Set $F = (G \setminus V) \cap V^2$. Then V^2 is compact as V is compact, which implies that V^2 is closed. We therefore get that F is closed and therefore compact. Let $x \in V$ then $x \in G \setminus F$. Then, by continuity of multiplication and as $G \setminus F$ is open there exists open neighbourhoods $V_x, S_x \subseteq V$ of x and 1 respectively such that $V_x S_x \subseteq G \setminus F$. Then the $\{V_x \mid x \in V\}$ form an open cover of V, thus as V is compact there must exist an finite subcover $\{V_{x_i} \mid i = 1, ..., n\}$. Let $S_{x_1}, ..., S_{x_n}$ be the respective neighbourhoods of 1 and let $S = \bigcap_{i=1,...,n} S_{x_i}$. Set $W = S \cap S^{-1}$. Then we have that W is a symmetric neighbourhood of 1, $W \subseteq V$. Let $x \in VW$, then $x \in V_{x_j} S$ for some $x_j \in \{x_1, ..., x_n\}$. Then $x \in G \setminus F$ as $x \in V_{x_j} S = V_{x_j} S_{x_1} \cap ... \cap V_{x_j} S_{x_n}$ implies that $x \in V_{x_j} S_{x_j} \subseteq G \setminus F$. Therefore $VW \subseteq G \setminus F$. This implies that $VW \subseteq V$ as $VW \subseteq V^2$. We therefore also have that $VW^2 \subseteq VW \subseteq V$, thus $VW^n \subseteq V$ for all $n \in \mathbb{N}$. Therefore also $W^n \subseteq V$ as $1 \in V$ and $VW^n \subseteq V$ for all $n \in \mathbb{N}$. Let $R = \bigcup_{n \in \mathbb{N}} W_n$, then R is an open subgroup of G contained in V as W is open and symmetric. Thus by Lemma 7.1.6 the core of R, $R_G = \bigcap_{x \in G} (xRx^{-1})$ is an open normal subgroup of G. Finally observe that $R_G \leq R \subseteq VR \subseteq \bigcup_{i \in \mathbb{N}} VW^n \subseteq V$. That G/R_G is finite follows from (b) as G is assumed to be compact and the cosets of R_G will be a open covering of G.

(c) $\Rightarrow$ (d):
Let $\mathcal{U}$ be an fundamental system as the one described in (c). We will define a directed partial order on $\mathcal{U}$. Define $U \leq V$ if $V \subseteq U$. This is a directed as if U, V are two neighbourhoods of 1, $U \cap V$ is a neighbourhood of 1 and $U, V \leq U \cap V$. If $U \leq V$ we can define the following morphism $\pi_{UV} : G/V \to G/U$ by $gV \mapsto gU$. This is well defined as $V \subseteq U$. We then get that if $U \leq V \leq W$ that the following diagram commutes.



We therefore have the inverse system $(G/U, \pi_{UV})$ over $\mathcal{U}$. Note that $\pi_U : G \to G/U$ is compatible with the inverse system, thus we get a induced morphism $f : G \to \varprojlim_{U \in \mathcal{U}} G/U$. As G and $\varprojlim_{U \in \mathcal{U}} G/U$ are compact and Hausdorff we get by Proposition 6.2.8 that f is surjective. We want to show that f is a homeomorphism. As G is compact and $\varprojlim_{U \in \mathcal{U}} G/U$ is Hausdorff it follows by Proposition 5.1.35 that we only need to show that f is injective. Let $x \in G$ and assume that $f(x) = 1$. Then $x \in U$ for all $U \in \mathcal{U}$. Thus, as $\bigcap_{U \in \mathcal{U}} U = \{1\}$, $x = 1$. Therefore $\mathsf{ker}(f) = \{1\}$, and thus f is injective.

(d) $\Rightarrow$ (a):
This follows from the definition of a profinite group as for each $U \in \mathcal{S}$, G/U is finite. □

7.2. **Profinite Groups as Galois groups.** Before we can start to define the Krull topology on the Galois group, we need the following proposition regarding Galois extensions.

Proposition 7.2.1. *Let E/F be a Galois extension, and let $\mathsf{Int}(E/F) = \{L_i \mid E \subseteq L_i \subseteq E$, L_i/F finite Galois extension$\}$ denote the set of finite intermediate Galois extensions. Let $G = \mathsf{Gal}(E/F)$, $U_i = \mathsf{Gal}(E/L_i)$ and let $G_i = \mathsf{Gal}(L_i/F)$. Then the following is true:*

(a) $E = \bigcup_{i \in I} L_i$;
(b) $U_i \leq G_i$ and $G/U_i \cong G_i$ is finite for every $i \in I$;
(c) If $i, j \in I$, then there exists a $k \in I$ such that $U_k \leq U_i \cap U_j$;
(d) $\bigcap_{i \in I} U_i = \{1\}$.

Proof.

(a) Firstly we have that $\bigcup_{i \in I} L_i \subseteq E$. Let $\alpha \in E$, then $F(\alpha)/F$ is a finite Galois extension containing α and therefore $\alpha \in \bigcup_{i \in I} L_i$. Thus $E = \bigcup_{i \in I} L_i$.

(b) U_i is just precisely the following set $\{\sigma \in G \mid \sigma_{|L_i} = \mathsf{id}_{L_i}\}$ and thus it is a subgroup of G. Let $f : G \to G_i$ be the map defined by $\sigma \mapsto \sigma_{|L_i}$, this is well defined as L_i is normal. Then one sees that $G/U_i \cong G_i$ by the first isomorphism theorem, as $\mathsf{ker}(f) = U_i$. That G_i is finite for every $i \in I$ follows from Proposition 4.4.5.

(c) Let U_i, U_j be given and let L_i, L_j be the corresponding intermediate field extensions. Then as they are finite and normal, L_i and L_j is the splitting field of polynomials f_i and f_j respectively. Let L be the splitting field of $f_i f_j$. Then L is a finite intermediate Galois extension and thus $L = L_k$ for some $k \in I$. Furthermore $L_i, L_j \subseteq L_k$, thus we get that $U_k \subseteq U_i, U_j$ and thus $U_k \subseteq U_i \cap U_j$.

(d) Let $\sigma \in \bigcap_{i \in I} U_i$ and let $\alpha \in E$. Then $F(\alpha)/F$ is a finite Galois extension and hence $\mathsf{Gal}(E/F(\alpha))$ is equal U_t for some $t \in I$. Thus it follows that $\sigma(\alpha) = \alpha$. Therefore, as α was arbitrary, $\sigma = \mathsf{id}_E$ and thus $\bigcap_{i \in I} U_i = \{1\}$.

□

Now we can finally define what the Krull topology is. There are several ways to define this topology but we will define it using a filter base.

Proposition 7.2.2. *Let E/F be a Galois extension and let $\mathsf{Int}(E/F)$ be the set of finite intermediate Galois extensions $F \subseteq L_i \subseteq E$. Let $G = \mathsf{Gal}(E/F)$, let $U_i = \mathsf{Gal}(E/L_i)$. Then there exists a unique topology such that $\mathcal{U} = \{U_i \mid i \in I\}$ is a filter base for the neighbourhood filter of the identity element e in G. Moreover if E/F is a finite Galois extension then the topology induced is the discrete topology.*

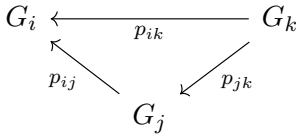
Proof. To show this we will show that $\mathcal{U}$ fulfills the assumptions in Proposition 5.2.11. We will begin by showing that $\mathcal{U}$ is a filter base. Let $U_i, U_j \in \mathcal{U}$ then by Proposition 7.2.1 it follows that there exists a $U_k \in \mathcal{U}$ such that $U_k \subseteq U_i \cap U_j$. The second condition is fulfilled as taken any element $\alpha \in E$, $F(\alpha)$ will be a finite Galois extension of F. Thus we have shown that $\mathcal{U}$ is filter base. Now it remains to show that it fulfills the condition in Proposition 5.2.11. The first and second condition is fulfilled as all the U_i are groups. The third condition follows from (b) in Proposition 7.2.1 as the kernel of an morphism is a normal subgroup. Thus we can now conclude that there exists a unique topology such that $\mathcal{U} = \{U_i \mid i \in I\}$ is a filter base for the neighbourhood filter of the identity element e in G. Now we assume that E/F is finite. To show that the topology is trivial we will show that every subset containing the identity automorphism is in the filter generated by $\mathcal{U}$. Let W be a subset of G containing the identity automorphism. Since E/F is finite, $\mathsf{Gal}(E/E) = \{\mathsf{id}_E\} \in \mathcal{U}$ and as $\mathsf{Gal}(E/E) \subseteq W$ it follows that W is in the filter generated by $\mathcal{U}$. Thus in this case the topology induced is the discrete topology. □

Definition 7.2.3. Let E/F be a Galois extension and let $G = \mathsf{Gal}(E/F)$. The *Krull topology* on G is topology induced on G by Proposition 7.2.2.

Now we finally arrive at one of the main theorems of this thesis.

Theorem 7.2.4. *Let E be a Galois extension of a field F and let $\mathsf{Int}(E/F)$ denote the set of all intermediate fields $F \subseteq L_i \subseteq E$ such that L_i/F is a finite Galois extension. Let I be the index set of $\mathsf{Int}(E/F)$. Then the Galois group $G = \mathsf{Gal}(E/F)$ endowed with the Krull topology is a profinite group. Moreover $G \cong \varprojlim_{L_i \in \mathsf{Int}(E/F)} \mathsf{Gal}(L_i/F)$.*

Proof. Let $\mathsf{Int}(E/F)$ be defined as in the assumption and let I be the associated index set. We will now define a partial order $\leq$ on I. Let $i \leq j$ if $L_i \subseteq L_j$. Plainly $\leq$ is a partial order. Furthermore it is a directed partial order by the following argument. Let $i, j \in I$, then the associated field extension L_i, L_j are finite and normal, and thus the splitting field of polynomials f_i and f_j respectively. Let L be the splitting field of $f_i f_j$, then L is a finite Galois extension of F and thus $L = L_k$ for some $k \in I$. We have that $L_i, L_j \subseteq L_k$ and therefore $i, j \leq k$. Thus $(I, \leq)$ is a directed poset. Let $G_i = \mathsf{Gal}(L_i/F)$. Then if $i \leq j$ we have a well defined map $p_{ij} : G_j \to G_i$ defined by $\sigma \mapsto \sigma_{|L_i}$, which is well defined as each extension is normal. Note also that the following diagram commutes for all $i \leq j \leq k$.



Thus we now have that (G_i, p_{ij}) is an inverse system of finite topological groups over I if we endow each finite group with the discrete topology. We can now therefore take the inverse limit, $\varprojlim G_i$, of the system (G_i, p_{ij}). To show that G is a profinite group we will construct an isomorphism from G to $\varprojlim G_i$. Let $f : G \to \varprojlim G_i$ be the map defined by $\sigma \mapsto (\sigma_{|L_i})_{i \in I}$. Firstly note that this is a group morphism as $f(\sigma \circ \sigma') = ((\sigma \circ \sigma')_{|L_i})_{i \in I} = (\sigma_{|L_i})_{i \in I} \circ (\sigma'_{|L_i})_{i \in I} = f(\sigma) \circ f(\sigma')$. We will

now show that the map is bijective. To show that it is injective note that $\ker(f) = \bigcap_{i\in I} U_i$ where $U_i = \mathsf{Gal}(E/L_i)$. By Proposition 7.2.1 it follows that $\ker(f) = \{1\}$ and thus f is an injective map. To show surjectivity, let $(\sigma_i)_{i\in I} \in \varprojlim G_i$ be an arbitrary element. Let $\sigma \in G$ be the automorphism defined element wise as follows, $\sigma(a) = \sigma_i(a)$ if $a \in L_i$. This is well defined as if $a \in L_i$ and $a \in L_j$ then there exists L_k such that $L_i, L_j \subseteq L_k$ and therefore $\sigma_i(a) = \sigma_k(a) = \sigma_j(a)$. Then we have that $f(\sigma) = (\sigma_i(a))_{i\in I}$. Thus now we only have left to show that f is continuous and that f is an open mapping. To show that f is continuous we will show that $h_i = p_i \circ f : G \to G_i$ is continuous for all $i \in I$ as then f will be continuous by Proposition 5.1.27. Let V be an open subset of G_i and let $W = h_i^{-1}(V)$. To show that W is an open set, let σ be an arbitrary point in W, then σU_i for $U_i = \mathsf{Gal}(L_i/F)$ is an open neighbourhood of σ that is contained in W. This is true as if $\sigma' \in \sigma U_i$, then $\sigma'_{|_{L_i}} = (\sigma \circ \psi)_{|_{L_i}} = \sigma_{|_{L_i}} \circ \psi_{|_{L_i}} = \sigma_{|_{L_i}} \in V$. Thus h_i is continuous as V was an arbitrary open subset of G_i. Therefore as this holds for h_i for all $i \in I$ it follows that f is continuous. To see that f is an open mapping note let $U_i = \mathsf{Gal}(E/L_i)$ for some $L_i \in \mathsf{Int}(E/F)$. Note that $\sigma \in U_i$ if and only if $\sigma_{|L_i} = \mathsf{id}_{L_i}$. Therefore as f is bijective we have that $f(U_i) = \varprojlim G_i \cap ((\prod_{L_j \neq L_i} G_j) \times \{1\}_{L_i})$. As $((\prod_{L_j\neq L_i} G_j) \times \{1\}_{L_i})$ is open in $\prod_{i\in I} G_i$ we get that $f(U_i)$ is open in $\varprojlim G_i$. Therefore we conclude that f is an open mapping and thus it follows that f is an isomorphism of topological groups. Therefore $G \cong \varprojlim G_i$. □

Now we can prove a generalization of the fundamental theorem of finite Galois extensions.

Theorem 7.2.5. *Let E be a Galois extension of a field F, and let $G = \mathsf{Gal}(E/F)$ be the Galois group of the extension endowed with the Krull topology. Then the there exists a order reversing bijection between the set of closed subgroups of G, denoted $\mathcal{C}(G)$, and the intermediate extensions $F \subseteq L_i \subseteq E$, denoted $\mathcal{F}(E/F)$. given by the map*

$$\begin{aligned} \Phi : \mathcal{F}(E/F) &\to \mathcal{C}(G) \\ L &\mapsto \mathsf{Gal}(E/L) \end{aligned}$$

and the map

$$\begin{aligned} \Gamma : \mathcal{C}(G) &\to \mathcal{F}(E/F) \\ N &\mapsto \mathsf{Fix}_E(N) \end{aligned}$$

Proof. We will first show that Φ is well defined. Let $L \subseteq E$ be a intermediate field. Then we observe that $\Phi(L) = \mathsf{Gal}(E/L)$. We claim that the Krull topology on $\mathsf{Gal}(E/L)$ is the same as the topology induced from the Krull topology on $G = \mathsf{Gal}(E/F)$. To show this let $\mathscr{B}_1 = \{\mathsf{Gal}(E/L_i) \mid L_i/L \text{ finite and Galois}\}$ and $\mathscr{B}_2 = \{\mathsf{Gal}(E/F_i) \cap \mathsf{Gal}(E/L) \mid F_i/F \text{ finite and Galois}\}$. If we can show that $\mathscr{B}_1 = \mathscr{B}_2$ then the two topologies will be the same. Note that we have the following correspondence, if L'/L is finite Galois extension then $L' = L(\alpha_0, ..., \alpha_n)$ with $\alpha_i \in L'$ and then we have a corresponding extension $F(\alpha_0, ..., \alpha_n)$ which is finite and Galois over F. Likewise if F'/F is a finite Galois extension we have that $F' = F(\beta_0, ..., \beta_m)$ with $\beta_i \in F'$ and then we get a finite Galois extension $L(\beta_0, ..., \beta_m)$. Let $\mathsf{Gal}(E/L_i) \in \mathscr{B}_1$ be an arbitrary element. As L_i/L is finite we have that $L_i = L(\alpha_0, ..., \alpha_n)$. Now we get that $\mathsf{Gal}(E/L) \cap \mathsf{Gal}(E/F(\alpha_0, ..., \alpha_n)) = \mathsf{Gal}(E/L(\alpha_0, ..., \alpha_n))$ as both groups fix the same elements, thus we have that $\mathscr{B}_1 \subseteq \mathscr{B}_2$. Conversely let $\mathsf{Gal}(E/F_i) \cap \mathsf{Gal}(E/L) \in \mathscr{B}_2$ be an arbitrary element. Then we get that $F_i = F(\beta_0, ..., \beta_m)$ and therefore we have the corresponding finite Galois extension $L(\beta_0, ..., \beta_m)$. We then get that $\mathsf{Gal}(E/F(\beta_0, ..., \beta_m)) \cap \mathsf{Gal}(E/L) = \mathsf{Gal}(E/L(\beta_0, ..., \beta_m))$ as they fix the same elements. Thus $\mathscr{B}_2 \subseteq \mathscr{B}_1$ which implies that $\mathscr{B}_1 = \mathscr{B}_2$. Thus the two topologies are equal. Now it follows by Theorem 7.2.4 and Theorem 7.1.7 that $\mathsf{Gal}(E/L)$ is compact, and as G is Hausdorff, by Proposition 5.1.33 it follows that $\mathsf{Gal}(E/L)$ is a closed subgroup of G. Thus Φ is a well defined map.

First let prove that $(\Gamma \circ \Phi)(L) = L$ for all intermediate field extensions $F \subseteq L \subseteq E$. First note that $\Phi(L_i) = \mathsf{Gal}(E/L_i)$, and thus $L_i \subseteq \Gamma(\mathsf{Gal}(E/L_i))$. Now let $y \in \Gamma(\mathsf{Gal}(E/L_i))$, then as y is fixed by every automorphism in $\mathsf{Gal}(E/L_i)$ it follows that y has no conjugates and thus that $\mathsf{deg}(\mathsf{irr}(y : L_i)) = 1$. Thus we conclude that $y \in L_i$ and therefore $(\Gamma \circ \Phi)(L_i) = L_i$.

Conversely, now we want to show that $(\Phi \circ \Gamma)(N) = N$ for all closed subgroups N of G. Let $L = \Gamma(N)$. Then $(\Phi \circ \Gamma)(N) = \mathsf{Gal}(E/L) \supseteq N$. Now, as N is closed subgroup, it is enough to show that N is dense in $\mathsf{Gal}(E/L)$. To do this we will show that for any point $\sigma \in \mathsf{Gal}(E/L)$ and any neighbourhood of U of σ, $U \cap N \neq \emptyset$. Let $\sigma \in \mathsf{Gal}(E/L)$ be an arbitrary point and let U be a neighbourhood of σ. Then we can assume without loss of generality that $U = \sigma\mathsf{Gal}(E/K)$ for some finite intermediate Galois extension $L \subseteq K \subseteq E$. Now note that $\{\tau_{|K} \mid \tau \in N\}$ is a group of automorphism of K as K is normal. As K is finite Galois extension of L it now follows that $\{\tau_{|K} \mid \tau \in N\} = \mathsf{Gal}(K/L)$ by Theorem 4.4.9. Thus there exists a $\tau' \in N$ such that $\sigma_{|K} = \tau'_{|K}$, which implies that $\tau'_K \in \sigma\mathsf{Gal}(E/K)$. Therefore we finally conclude that $N \cap \sigma U \neq \emptyset$, and thus $N = \mathsf{Gal}(E/L)$.

□

We now generalise Proposition 4.4.12 to infinite Galois extensions.

Proposition 7.2.6. *Let E/F be a Galois extension and let L be an intermediate field extension. Assume that $E \subseteq \bar{F}$. Then L is a normal extension if and only if $\mathsf{Gal}(E/L)$ is normal subgroup of $\mathsf{Gal}(E/F)$. Moreover, in this case, $\mathsf{Gal}(L/F) \cong \mathsf{Gal}(E/F)/\mathsf{Gal}(E/L)$.*

Proof. Assume that L is a normal intermediate field extension. Let $\sigma \in g(L) = \mathsf{Gal}(E/L)$ be arbitrary and let $\tau \in \mathsf{Gal}(E/F)$. Then we have that $\tau\sigma\tau^{-1} \in \mathsf{Gal}(E/L)$. This is true as $\tau\sigma\tau^{-1}$ can be seen as a F-morphism into $\bar{F}$ and thus by Proposition 4.1.11 and by Proposition 4.2.5 $\tau\sigma\tau^{-1}(L) = L$ as L is normal. By the same normality argument $(\tau\sigma\tau^{-1})_{|L} = \tau_{|L}\sigma_{|L}\tau_{|L}^{-1} = \tau_{|L}\tau_{|L}^{-1} = \mathsf{id}_L$. Therefore $\tau\sigma\tau^{-1} \in \mathsf{Gal}(E/L)$. Conversely assume that $\mathsf{Gal}(E/L)$ is a normal subgroup of $\mathsf{Gal}(E/F)$ then we claim that $\tau(L) = L$ for all $\tau \in \mathsf{Gal}(E/F)$. To show this let $\sigma \in \mathsf{Gal}(E/L)$ then we have that $(\tau^{-1} \circ \sigma \circ \tau)(L) = L$ for all $\tau \in \mathsf{Gal}(E/F)$. This implies that $\sigma(\tau(L)) = \tau(L)$, which in turn implies that $\sigma_{|\tau(L)} = \mathsf{id}_{\tau(L)}$ for all $\tau \in \mathsf{Gal}(E/F)$ and all $\sigma \in \mathsf{Gal}(E/L)$. This implies that $\tau(L) \subseteq \mathsf{Fix}_E(\mathsf{Gal}(E/L)) = L$ for all $\tau \in \mathsf{Gal}(E/F)$. By the same argument we also have that $\tau^{-1}(L) \subseteq L$. This in turn gives us that $L = \tau(\tau^{-1}(L)) \subseteq \tau(L) \subseteq L$ which implies that $\tau(L) = L$ for all $\tau \in \mathsf{Gal}(E/F)$. This implies by Proposition 4.2.5 that L is a normal extension of F.

Assume now that L is normal field then we have a map from $\mathsf{Gal}(E/F) \to \mathsf{Gal}(L/F)$ given by $\sigma \mapsto \sigma_{|L}$, which is well defined as L is normal. Furthermore the kernel of this map is $\mathsf{Gal}(E/L)$ thus by Theorem 3.1.18 $\mathsf{Gal}(L/F) \cong \mathsf{Gal}(E/F)/\mathsf{Gal}(E/L)$. □

First we will give a nice property of open subgroups, which will be important later.

Proposition 7.2.7. *Let E/F be a Galois extension and let $G = \mathsf{Gal}(E/F)$ endowed with the Krull topology. Let H be a subgroup of G. Then H is open if and only if $H = \mathsf{Gal}(E/L)$ for some finite intermediate extension L.*

Proof. First assume that H is an open subgroup. Then, by definition, there exists a open group $U = \mathsf{Gal}(E/K)$, where K/F is a finite intermediate extension, such that $U \subseteq H$. Both H and U are also closed by Proposition 7.1.5. Let L be the fixed field of H. Then we get by Theorem 7.2.5 that $L \subseteq K$ as the bijection is order reversing. Therefore we have that L/F is a finite field extension as K/F is a finite field extension. Conversely assume that $H = \mathsf{Gal}(E/L)$ for some finite intermediate extension L. Then by the definition of the Krull topology H is open. □

Before we get to the example we need a small lemma.

Lemma 7.2.8. *Let G be a group and assume that $a^2 = e$ for all $a \in G$. Then we have that G is abelian.*

Proof. This is true as $(ab)^2 = e$ implies that $ba = ab$, by multiplication of a from the left and multiplication of b from right, for all $a, b \in G$. □

The following example is originally from [7], see also [4].

Example 7.2.9. We now give an example of a case where we need to restrict ourselves to the closed subgroups. In this example we will show that the Galois group has uncountably many subgroups whilst there only exist a countable amount of intermediate field extensions. Let $S = \{\sqrt{p} \mid p \text{ is prime and } p \geq 3\}$ and let $E = \mathbb{Q}(S)$. Then E is the splitting field of the following set of polynomials $S' = \{x^2 - p \mid p \text{ is prime and } p \geq 3\}$. Thus $E/\mathbb{Q}$ is a Galois extension. We now let $G = \mathsf{Gal}(E/\mathbb{Q})$.

We begin by studying G. Note that for any $\sqrt{p} \in S$, $\mathsf{irr}(\sqrt{p} : \mathbb{Q}) = x^2 - p$. Thus $\sqrt{p}$ has only two conjugates over $\mathbb{Q}$ and thus for all $\mathbb{Q}$-automorphism $\sigma \in \mathsf{Gal}(E/\mathbb{Q})$, $\sigma(\sqrt{p}) = \sqrt{p}$ or $\sigma(\sqrt{p}) = -\sqrt{p}$. Thus given any subset $A \subseteq S$ there exists a $\mathbb{Q}$-automorphism such that $\sigma(A) = -A$ and $\sigma(S \setminus A) = S \setminus A$. Therefore we get that the cardinality of G is the same as the cardinality of the power set of all primes, which is uncountable. Moreover note that for all $\sigma \in G$, $\sigma^2 = \mathsf{id}_G$. Then this implies that G is abelian by Lemma 7.2.8. Therefore we can now give G the structure of a vector space over $\mathbb{Z}_2$. Let $\mathcal{B}$ be a basis for G then $\mathcal{B}$ is uncountable as G is. Let $b \in \mathcal{B}$ be given, then let H_b be the group generated by $\mathcal{B} \setminus \{b\}$. Then H_b is a subgroup of index two as the only left cosets are H_b and $b + H_b$. Therefore G has uncountably many subgroups of finite index.

We now study $E/\mathbb{Q}$. First note that E is countable as a set as it is an algebraic extension of $\mathbb{Q}$. Note that $E/\mathbb{Q}$ also has a countable basis as vector space it follows that E only has countably many finite subspaces as a vector space over F. Thus we have that there are only countably many finite intermediate field extensions of $E/\mathbb{Q}$. Note that by Proposition 7.1.5 and Proposition 7.2.7 that G only has countably many closed subgroups, whilst it has uncountably many subgroups. Moreover, as state before, it even has uncountably many subgroups of finite index.

We will now see that the corresponds goes the other way, that is every profinite group can be realised as a Galois group of a Galois extension E/F.

Theorem 7.2.10. *Let G be a profinite group. Then there exists a Galois extension E/F such that $G = \mathsf{Gal}(E/F)$.*

Proof. Let $\{U_i \mid U_i \trianglelefteq G\}$ be the set of all open normal subgroups of G and let $T = \bigsqcup_{i \in I} G/U_i$ be the disjoint union of the quotient groups. Let F be any field[2] and let $E = F(T)$ seeing T as huge set of indeterminants. Now we see that we can let G act on T by the following, if $a, b \in G$ and $bU_i \in T$, then $a \cdot bU_i = (ab)U_i$. Thus now we can see that this gives G an action on E and therefore G can been seen as a group of automorphism on E. Now let $L = \mathsf{Fix}_E(G)$ be the field fixed by G. We now aim to show that $G = \mathsf{Gal}(E/L)$. To do this we must first show that E/L is a Galois extension. Let $\alpha \in E$ and define the following subgroup of G, $G_\alpha := \{a \in G \mid a(\alpha) = \alpha\}$. Let $A = \{t_j U_j \in G/U_j \mid j = 1, ..., n\}$ be the set of indeterminants that appear in α. Then $U = \bigcap_{j=1,...,n} U_j \subseteq G_\alpha$ as each $t_j U_j = u t_j U_j$ for any $u \in U_j$. This implies that G_α is open as each U_i is open and $G_\alpha = \bigcup_{h \in G_\alpha} hU$. Then as G_α is open it follows that it is of finite index by Proposition 7.1.5. Thus the orbit of α under G must be finite. Let $B = \{\alpha_0, ..., \alpha_m\}$ be the orbit of

[2] Choose your favorite!

α. We can assume without loss of generality that $\alpha_0 = \alpha$ as $1 \in G$. Then we define the following polynomial $f_\alpha(x) = \prod_{i=1,...,m}(\alpha_i - x)$. This polynomial is separable as all the roots are distinct. Note moreover that G maps the polynomial to itself, thus we have that $f_\alpha(x) \in L[x]$. Therefore $\alpha \in E$ is algebraic. Furthermore note that $L(\alpha_0, \alpha_1, ..., \alpha_m)/L$ is a normal extension extension as it is the splitting field of f. Thus we have that E is the union of all the splitting fields of each f_α for $\alpha \in E$. Hence E is a normal extension. Therefore we finally get that E/L is a Galois extensions.

Now it remains to show that the Galois group of E/L is equal to G. Let H be the Galois group of E/L. Then we have that $G \leq H$. We will first show that the inclusion map is continuous. Let U be a open subset of H. Then by Proposition 7.2.7 it follows that the fixed field of U is a field K such that K/L is finite. Therefore we have that $K = L(\alpha'_1, ..., \alpha'_s)$. We then have that $\bigcap_{i=1,...,s} G_{\alpha'_i} \subseteq G \cap U$. This in turn implies that $G \cap U$ is open as $G \cap U = \bigcup_{g \in G \cap U} g(\bigcap_{i=1,...,s} G_{\alpha'_i})$. Therefore we now have that the inclusion map is continuous. As H is closed we get that G is closed. This in turn implies, by Theorem 7.2.5, that $G = H$ as they fix the same elements. □

8. Further Generalization

The study of infinite Galois extension can be further generalized by studying the category of G-sets for a profinite group G and even more generally by Galois categories. More specifically let F be a field and let $G = \mathsf{Gal}(F_{\text{sep}}/F)$, where $F_{\text{sep}} = \{\alpha \in \bar{F} \mid \alpha \text{ is seperable}\}$ is the separable closure. Then there is an anti-equivalence between the category of free separable F-algebras and the category G-sets. For details of this, in the context of scheme theory for algebraic geometry, see for example section 2 and 3 of [6].

Acknowledgments

I wish to thank my advisor Martin Herschend for all his help, for answering all my questions and for all the helpful advices he has given me in general.

References

[1] Emil Artin. *Galois theory*. Edited and supplemented with a section on applications by Arthur N. Milgram. Second edition, with additions and revisions. Fifth reprinting. Notre Dame Mathematical Lectures, No. 2. University of Notre Dame Press, South Bend, Ind., 1959, pp. iii+82.

[2] Nicolas Bourbaki. *General topology: chapters 1-4*. Berlin: Springer, 1990.

[3] Daniel W. Cunningham. *Set theory*. Cambridge Mathematical Textbooks. A first course. Cambridge University Press, New York, 2016, pp. xii+250. ISBN: 978-1-107-12032-7.

[4] Pierre Antoine Grillet. *Abstract algebra*. Second. Vol. 242. Graduate Texts in Mathematics. Springer, New York, 2007, pp. xii+669. ISBN: 978-0-387-71567-4.

[5] B. Melvin Kiernan. "The development of Galois theory from Lagrange to Artin". In: *Arch. History Exact Sci.* 8.1-2 (1971), pp. 40–154. DOI: 10.1007/BF00327219. URL: https://doi.org/10.1007/BF00327219.

[6] Hendrik Willem Lenstra. *Galois Theory for Schemes*. https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf. Accessed: 2019-10-03.

[7] Paul J. McCarthy. *Algebraic extensions of fields*. Blaisdell Publishing Co. Ginn and Co. Waltham, Mass.-Toronto, Ont.-London, 1966, pp. ix+ 166.

[8] James R. Munkres. *Topology*. Second edition of [MR0464128]. Prentice Hall, Inc., Upper Saddle River, NJ, 2000, pp. xvi+537. ISBN: 0-13-181629-2.

[9] Emmy Noether. "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern". In: *Math. Ann.* 96.1 (1927), pp. 26–61. ISSN: 0025-5831. DOI: 10.1007/BF01209152. URL: https://doi.org/10.1007/BF01209152.

[10] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Second. Vol. 40. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin, 2010, pp. xvi+464. ISBN: 978-3-642-01641-7. DOI: 10.1007/978-3-642-01642-4. URL: https://doi.org/10.1007/978-3-642-01642-4.