Profinite Groups

Juan Moreno Poncela

Master's thesis
2023:E63

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

Centrum Scientiarum Mathematicarum

Abstract

This thesis provides a comprehensive study of profinite groups, which are fascinating mathematical objects that have attracted significant interest in modern algebraic research. Profinite groups are infinite generalizations of finite groups and share many similarities with them. They are endowed with a topology that makes them compact and totally disconnected, which is the foundation from which we draw conclusions on their structure. In this thesis, we introduce the basic concepts of profinite groups and their relationship with finite groups. We then generalize Lagrange's theorem and the Sylow theorems to profinite groups, which are crucial for understanding their structure and subgroups. We also provide a generalization of the Fundamental Theorem of Galois Theory to profinite groups, which has important implications for the study of number theory and algebraic geometry. We conclude with examples of infinite Galois groups, including the Galois group of the algebraic closure of finite fields, and some infinite Galois extensions of the rational numbers, which illustrate the power of profinite groups in studying the structure of infinite Galois groups.

Popular Scientific Summary

This thesis provides a comprehensive study of a special kind of topological groups. Topological groups are sets with a notion of "closeness" defined by their topological structure, and with a binary operation between the elements in the set (an operation that takes two elements in the set to a new element in the set) that satisfies a compatibility condition that makes the binary operation map "close" elements to "close" elements. These concepts serve as a bridge between fields of study in mathematics such as topology and geometry, and are used to describe and analyze physical systems in quantum mechanics and particle physics, being key to understanding continuous symmetries.

Profinite groups are a special type of possibly infinite abstract topological groups. These groups are constructed from collections of finite groups in such a way that many of the properties related to the finite groups in a collection are inherited by their profinite group. This construction is called an inverse limit, which is a mathematical structure that allows us to "glue" together the finite groups to form a possibly infinite group.

Due to this relationship between finite groups and profinite groups many theorems relating finite groups can be extended to profinite groups. One such theorem —and the motivation from which profinite groups arose— is the Fundamental Theorem of Galois Theory, an extremely powerful result that establishes a deep connection between group theory and field theory.

In this thesis we explore all of these concepts and topics in hopes of gaining a better understanding of these mathematical structures. We study profinite groups as inverse limits of finite groups; as topological groups with specific properties, namely compactness and total disconnectedness; and as Galois groups, the object of study of Galois Theory.

Contents

Index of Notation

$\leq$	subgroup
$\leq_o$	open subgroup
$\leq_c$	closed subgroup
$\leq_{co}$	clopen subgroup
$\subseteq_o$	open subset
$\subseteq_c$	closed subset
$\subseteq_{co}$	clopen subset
U_x	open neighbourhood of x
$\mid$	divides/ such that
$\mathrm{lcm}\{n_i\}_{i\in I}$	least common multiple of $\{n_i\}_{i\in I}$
$\gcd\{n_i\}_{i\in I}$	greatest common divisor of $\{n_i\}_{i\in I}$
$(x_i)_{i\in I}$	sequence of elements indexed by I
$(x_i)_1^n$	sequence of elements indexed by $\{i,\ldots,n\}$
$\{x_i\}_{i\in I}$	collection of elements indexed by I
Id_S	identity map of S
$\cong$	isomorphic
$\ker(\alpha)$	kernel of α
$\alpha(S)$	image of S under α
$S \setminus T$	set S minus T
S^c	complement of S
$\overline{S}$	closure of S
S^{-1}	set of inverses of S
$F^\times$	multiplicative group of F
F^G	fixed field of F with respect to G
G_s	stabilizer of $s \in S$ with respect to G
Gs	orbit of $s \in S$ with respect to G
K^{alg}	algebraic closure of K
G/N	quotient group of N over G
F/K	field extension F of K
$K(S)$	field extension of K generated by S
$K[S]$	polynomial ring of K with variables in S
∂p	degree of $p(t)$
$[G:H]$	index of H in G
e_G	identity element of G
$\varprojlim G_n$	inverse limit of G_n
$\mathrm{Gal}(F/K)$	Galois group of F/K
$\mathbb{N}_\infty$	extended natural numbers $\mathbb{N} \cup \{\infty\}$
$n\mathbb{Z}$	integer multiples of n
$\mathbb{Z}_n$	integers modulo n
$\mathbb{Z}_{\hat{p}}$	p-adic integers
$\hat{\mathbb{Z}}$	profinite completion of the integers
$\mathbb{F}_{p^n}$	finite field of order p^n
C_n	cyclic group of order n
ζ_n	primitive nth root of unity
Ω	set of all primitive roots of unity

Introduction

Profinite groups are incredible mathematical objects that are of great interest in modern algebraic research. They are in essence generalizations of finite groups that can be infinite and behave in many ways like finite groups do. As such, these groups are particularly useful for extending theorems on finite groups to the infinite realm. Profinite groups are groups endowed with a topology that makes them compact and totally disconnected. As will be shown in this thesis these very strong properties are the foundation from which we will draw conclusions on the structure of the groups. In this thesis the main focus will be on the generalization of finite group theorems and specifically on the Fundamental Theorem of Galois Theory, but profinite groups are also intimately connected with number theory, algebraic geometry, homology theory and representation theory, and have found applications in many areas of mathematics and theoretical physics.

The emergence of the theory of profinite groups is tightly connected to the advancement of topological groups and the exploration of infinite Galois theory. This field traces its roots to the 1920s, when the mathematician Wolfgang Krull formulated what is now recognized as the Krull topology, which we will later see is crucial to understanding infinite Galois groups as profinite groups. The first thorough examination of profinite groups was presented in Jean-Pierre Serre's book 'Cohomologie Galoisienne' in 1964. Although Michel Lazard, Claude Chevalley and Kurt Hirsch laid the groundwork for this area of study, Serre was the first to introduce the term and systematically develop the theory of profinite groups. Many papers and books have been written on this topic, but the most comprehensive introductory literature are the books titled 'Profinite Groups' written by Luis Ribes and Pavel Zalesskii, and John S. Wilson, the two main sources of information for this thesis.

This thesis provides a comprehensive study of profinite groups and their properties. We assume the reader has a solid understanding of finite Galois theory, as well as key concepts from basic group theory and algebraic structures. To aid the reader in their understanding, we reference the books 'Fields and Galois Theory' by John M. Howie and 'Algebra' by Serge Lang, both of which provide excellent sources of information on the prerequisites for this thesis. Additionally, the first appendix includes a list of important lemmas and theorems that are expected to be familiar to the reader.

The thesis is structured into three sections. The first section lays the foundations for topological groups and inverse limits, building up to the definition of profinite groups and introducing some of the key concepts and ideas that will

help us understand their relationship to finite groups.

In the second section we generalize Lagrange's Theorem, the Sylow Theorems and the Fundamental Theorem of Galois Theory to the profinite group setting. For the proof of the generalized versions of Lagrange's Theorem and the Sylow Theorems we introduce a new notion of index of profinite groups that relies on the idea of using supernatural numbers to represent different infinities. On the other hand, the subsection on the generalization of the Fundamental Theorem of Galois Theory helps us understand the relationship between infinite profinite groups and infinite Galois groups.

Finally, we present a short lemma original to the thesis and we provide some examples of infinite Galois groups over the rationals that serve to illustrate the power of the said lemma in studying the structure of infinite Galois groups.

1 Profinite Groups

1.1 Inverse Limits

The notions of an inverse system and an inverse limit can be broadly defined for any category. However, in the context of this project, we will limit our definitions to the category of topological groups with continuous group homomorphisms.

For this purpose we will start by first defining topological groups and their behaviour both as topological spaces and as groups. This will serve as a foundation for our subsequent discussion on inverse systems and inverse limits.

Definition 1.1.1 (Topological Group)**.** A topological group G is a set that is both a topological space and a group, satisfying that the group operation and the inversion maps are continuous, i.e. $B : (x, y) \mapsto xy$ and $i : x \mapsto x^{-1}$ are continuous.

Example 1.1.2. An example of a topological group is any group G under the discrete topology. To show that this is indeed a topological group we must prove that this topology is compatible with the group structure, i.e. the maps B and i are continuous under this topology. This is clearly true for any group under the discrete topology since i^{-1} maps subsets of G to subsets of G and every subset in the discrete topology is open, and B^{-1} maps subsets of G to the product of subsets of G, i.e. open sets in the product topology of discrete spaces. These topological groups are sometimes called discrete groups.

It is worth noting that not all topologies are compatible with every group structure. However, the discrete topology is an exception to this rule. As we will explore further, discrete groups are in fact the building blocks from which profinite groups are constructed.

Example 1.1.3. Another not so trivial example of a topological group would be the group $\mathbb{Q} \times \mathbb{Q}$, where $\mathbb{Q}$ represents the additive group on the rational numbers together with the Euclidean topology. The product of groups induces a new group in which the binary operation is given by the componentwise addition of elements. Again, to prove compatibility of the topology we must show that B and i are continuous. The map i is clearly continuous since it is continuous componentwise because it maps open intervals in $\mathbb{Q}$ to symmetric intervals around 0 in $\mathbb{Q}$, which are clearly open. On the other hand, the map B is continuous because $B((x_1, y_1), (x_2, y_2)) = (x_1 + x_2, y_1 + y_2) = (\mathcal{B}(x_1, x_2), \mathcal{B}(y_1, y_2))$ where the map $\mathcal{B} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is defined by $\mathcal{B} : (x, y) \mapsto x + y$, i.e. B is a product of continuous functions ($\mathcal{B}$ is continuous because the addition of coordinates on the Euclidean plane $\mathbb{R}^2$ is continuous, and the restriction of a continuous function to a subspace is continuous).

The topological and group structure on a topological group G give rise to a series of interesting properties on the subsets and subgroups of G.

Lemma 1.1.4. *[5, Lemma 0.3.1] Given a topological group G the following hold:*

(a) *If $H \subseteq_o G$ (respectively $\subseteq_c$) $\implies Hg, gH \subseteq_o G$ (respectively $\subseteq_c$) $\forall g \in G$.*

(b) *If $H \leq_o G \implies H \leq_c G$.*

(c) *If $H \leq_c G$ and $[G : H] < \infty \implies H \leq_o G$.*

(d) *If $H \leq_o G$ and G* is compact *$\implies [G : H] < \infty$.*

(e) *If $H \leq G$ and $S \subseteq_o G$ such that $\emptyset \neq S \subseteq H \implies H \leq_o G$.*

(f) *The group G* is Hausdorff *$\iff \{e\} \subseteq_c G$.*

(g) *If $H \leq G \implies \overline{H} \leq G$.*

Proof. (a) The maps $\alpha : x \mapsto xg$ and $\beta : x \mapsto gx$ are continuous since they are a composition of continuous maps, $\mathrm{Id}_G : x \mapsto x$ (the identity) and $c_g : x \mapsto g$ (a constant map), and the continuous map $B : (x, y) \mapsto xy$. Indeed $\alpha(x) = B(\mathrm{Id}_G(x), c_g(x))$ and similarly for $\beta(x)$. Moreover, using the same argument, we see that the maps $\alpha^{-1} : x \mapsto xg^{-1}$ and the map $\beta^{-1} : x \mapsto g^{-1}x$ are also continuous and they are inverses to α and β respectively, so these are homeomorphisms, and so they are open and closed maps.

(b) If $H \leq_o G$ then by (a) $Hg \subseteq_o G$, which implies that $\bigcup_{g \notin H} Hg$ is open. Furthermore, by Lemma A.0.9 the following equality holds $\bigcup_{g \notin H} Hg = H^c$, therefore the subgroup H is closed in G.

(c) If $[G : H] < \infty$ then the number of distinct right cosets is finite, therefore the union $\bigcup_{g \notin H} Hg$ is a finite union of cosets by Lemma A.0.9. Now, by (a) we have that H being closed in G implies that $Hg \subseteq_c G$ for all $g \in G$, so the set $H^c = \bigcup_{g \notin H} Hg$ is a union of finitely many closed cosets, meaning that the set H^c is closed, i.e. $H \leq_o G$.

(d) Since $G = \bigcup_{g \in C} Hg$, where C is a set with a representative from each coset of G, is a disjoint union by Lemma A.0.9, if G is compact and $H \leq_o G$ then $\bigcup_{g \in C} Hg$ is an open cover, so there is a finite subcover, i.e. there are finitely many distinct right cosets of H, so $[G : H] < \infty$.

(e) Since S is open, by (a) the set Sh is open $\forall h \in H$, and since $H = \bigcup_{h \in H} Sh$ then the subgroup H is open.

(f) ($\Rightarrow$) If G is Hausdorff, then $\{g\} \subseteq_c G \ \ \forall g \in G$ by Lemma B.0.1, so $\{e\} \subseteq_c G$.
($\Leftarrow$) Let $\{e\} \subseteq_c G$ and take $x, y \in G$ such that $x \neq y$ we want to prove that there exist disjoint open neighbourhoods of x and y. First we notice that the map $\phi : (x, y) \mapsto xy^{-1}$ is continuous since it is the composition of two continuous maps ($\phi(x, y) = B(x, i(y))$), so $\phi^{-1}(G \setminus \{e\})$ is open (since $\{e\}$ is closed). Furthermore, clearly $(x, y) \in \phi^{-1}(G \setminus \{e\})$, so, by the way open sets are constructed in the product topology, $\exists\, U_x$ and U_y such that $U_x \times U_y \subseteq \phi^{-1}(G \setminus \{e\})$. Finally, to prove that $U_x \cap U_y = \emptyset$ we assume the contrary, therefore $\exists\, p \in U_x \cap U_y$, i.e. $(p, p) \in U_x \times U_y \subseteq \phi^{-1}(G \setminus \{e\})$, but $\phi(p, p) = e$, so $(p, p) \notin \phi^{-1}(G \setminus \{e\})$, which is a contradiction.

(g) For any $x, y \in \overline{H}$ if $x^{-1} \notin \overline{H}$ then there is a $U_{x^{-1}}$ such that $U_{x^{-1}} \cap H = \emptyset$, but the inversion map i in a topological group is continuous by definition, thus the set $i(U_{x^{-1}})$ is an open neighbourhood of x and $i(U_{x^{-1}}) \cap H = i(U_{x^{-1}}) \cap i(H) = i(U_{x^{-1}} \cap H) = \emptyset$, which is a contradiction to the fact that $x \in \overline{H}$. Similarly, if $xy \notin \overline{H}$ then there would be an open neighbourhood U_{xy} such that $U_{xy} \cap H = \emptyset$, but, by the continuity of the group operation map B and the construction of the product space, we know there exist open neighbourhoods U_x and U_y such that $U_x \times U_y \subseteq B^{-1}(U_{xy})$. Since $x, y \in \overline{H}$ we have $(U_x \times U_y) \cap (H \times H) \neq \emptyset$, meaning that $B((U_x \times U_y) \cap (H \times H)) \neq \emptyset$, but $B((U_x \times U_y) \cap (H \times H)) \subseteq B(U_x \times U_y) \cap B(H \times H) \subseteq U_{xy} \cap H = \emptyset$, which is a contradiction. □

Lemma 1.1.5. *[5, Lemmas 0.1.1(c) and 0.3.2] Given $U \subseteq_o G$ where G is a compact and totally disconnected topological group and $e \in U$ there exists a normal subgroup $N \trianglelefteq_o G$ such that $N \subseteq U$.*

Proof. Using Lemma B.0.5 we know that $\forall y \in G$ with $y \neq e$ there is a subset F_y that is clopen such that $e \in F_y$ and $y \notin F_y$. We first prove that there is a set F clopen in U. Clearly $G = U \cup (\bigcup_{y \neq e} (G \setminus F_y))$. By compactness of G there is a finite subcover $G = U \cup (\bigcup_1^n (G \setminus F_{y_i}))$ and so $e \in F = \bigcap_1^n F_{y_i} \subseteq U$ where the set F is clearly clopen.

Finally, we prove that $\exists N \trianglelefteq_o G$ with $N \subseteq F$. Since the group operation map, $B : G \times G \to G$, is continuous by Definition 1.1.1, and because of the way the product space is constructed $\exists V_e, W_e \subseteq_o G$ such that $(e, e) \in V_e \times W_e$

and $B(V_e, W_e) = V_e W_e \subseteq F$. Then the set $S = V_e \cap W_e$ is such that $S \subseteq_o G$, $e \in S$ and $S = S\{e\} \subseteq SS \subseteq V_e W_e \subseteq F$. If we now denote $T = S \cap S^{-1}$ where $S^{-1} := \{g \in G \mid g^{-1} \in S\}$, clearly T is open in G since the set S^{-1} is open by the continuity of $i : G \to G$ given in Definition 1.1.1. Moreover, $T = T^{-1}$ and $e \in T$. For all $x \in F$ we have $F \subseteq \bigcup\limits_{x \in F} Sx$ is an open cover and F is compact since it is closed, so $F \subseteq \bigcup_1^k Sx_i$ is a finite subcover so we have $SF \subseteq \bigcup_1^k SSx_i \subseteq \bigcup_1^k Fx_i \subseteq F$, meaning that $TF \subseteq F$, which by induction gives us that $T^n \subseteq F \ \forall n \in \mathbb{N}$ and so the set $H = \bigcup_1^\infty T^n \subseteq F$ and it is open since it is a union of sets of the form Ty, which by Lemma 1.1.4 are open because the set T is. Furthermore, H is a subgroup since $e \in H$ because $e \in S$, and for any two elements $h, g \in H$ we must have $h \in T^n$ and $g \in T^m$ for some $n, m \in \mathbb{N}$, meaning that $h = t_1 \cdots t_n$ for some $t_i \in T$, which implies that $h^{-1} = t_n^{-1} \cdots t_1^{-1} \in T^n \subseteq H$, and $hg \in T^{n+m} \subseteq H$. Finally, from Lemma 1.1.4 H is of finite index, so the group $N = \bigcap\limits_{g \in G} gHg^{-1}$ is an intersection of finitely many open sets, so it is open and clearly $N \subseteq F$ since $N = \bigcap\limits_{g \in G} gHg^{-1} \subseteq eHe^{-1} = H \subseteq F$. The subgroup N is in fact normal since $\forall g \in G$ and $\forall n \in N$ we have $gng^{-1} \in g(\bigcap\limits_{h \in G} hHh^{-1})g^{-1} = \bigcap\limits_{h \in G} ghHh^{-1}g^{-1} \subseteq N$. □

Having established the concept of a topological group and the impact of its topological and group structure compatibility on the properties of its subgroups and open subsets, we can now introduce the notion of inverse limits of inverse systems of topological groups.

For this purpose we will first explain what is meant by an inverse system of topological groups and then proceed to provide a comprehensive example that illustrates the construction of this mathematical structure.

Definition 1.1.6 (Directed Poset)**.** A directed poset is a set I together with a binary relation $\leq$ satisfying the following:

(a) $i \leq i \qquad \forall i \in I.$

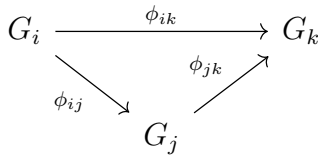
(b) $i \leq j$ and $j \leq k \implies i \leq k \qquad \forall i, j, k \in I.$

(c) $i \leq j$ and $j \leq i \implies i = j \qquad \forall i, j \in I.$

(d) $\forall i, j \in I \quad \exists\, k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 1.1.7 (Inverse System)**.** An inverse system is a collection $\{G_i\}_{i \in I}$ of topological groups indexed by a directed poset I with a collection of continuous group homomorphisms $\{\phi_{ij} : G_i \to G_j\}$ defined whenever $i \geq j$ such that

whenever $i \geq j \geq k$, the following diagram commutes



An inverse system is denoted $\{G_i, \phi_{ij}, I\}$. The maps ϕ_{ii} are just the identity maps on G_i.

Example 1.1.8. An example of an inverse system of topological groups is the system $\{\mathbb{Z}_n, \phi_{nm}, \mathbb{N}\}$ where $\mathbb{Z}_n$ represents the group of integers modulo n under addition with the discrete topology, $\mathbb{N}$ is a directed poset with respect to the divisibility relation $n \mid m$, and $\phi_{nm} : \mathbb{Z}_n \to \mathbb{Z}_m$ is given by $\phi_{nm} : [z]_n \mapsto [z]_m$ whenever $m \mid n$. The maps ϕ_{nm} are clearly continuous since they are maps between discrete spaces, and they are homomorphisms since

$$\begin{aligned}\phi_{nm}([x]_n + [y]_n) &= \phi_{nm}([x+y]_n) \\ &= [x+y]_m \\ &= [x]_m + [y]_m \\ &= \phi_{nm}([x]_n) + \phi_{nm}([y]_n)\end{aligned}$$

for any $x, y \in \mathbb{Z}$.

Building upon the concept of an inverse system, we can create yet another mathematical construct known as the inverse limit, which is a topological group that is a composition —via the continuous group homomorphisms— of the topological groups of an inverse system. This structure is in fact unique up to topological and group isomorphism.

Definition 1.1.9 (Compatible maps)**.** A family of compatible maps is a collection $\{\pi_i : H \to G_i\}_{i \in I}$ of continuous group homomorphisms from a topological group H to an inverse system $\{G_i, \phi_{ij}, I\}$, satisfying that $\phi_{ij}\pi_i = \pi_j$.

Definition 1.1.10 (Inverse Limit)**.** An inverse limit of an inverse system, say $\{G_i, \phi_{ij}, I\}$, is a topological group G together with compatible mappings $\{\pi_i\}$ satisfying the following universal property: given any other topological group H with compatible mappings $\{\psi_i\}$, there is a map $\theta : H \to G$ that is a unique continuous homomorphism satisfying $\pi_i\theta = \psi_i \ \forall i \in I$. The inverse limit is denoted by $\varprojlim G_i = G$. The compatible mappings are usually called projections.

Proposition 1.1.11. *[4, Proposition 1.1.1] Given an inverse system $\{G_i, \phi_{ij}, I\}$ the following hold:*

(a) *There is an inverse limit to the inverse system.*

(b) *The inverse limit is unique up to topological and group isomorphism.*

Proof. (a) Let $G := \{(g_i) \in \prod_{i\in I} G_i \mid \phi_{ij}(g_i) = g_j \text{ whenever } i \geq j\}$, then the set G is a subgroup of $\prod G_i$. This is because $(e) \in G$ and $(x_i)(y_i)^{-1} \in G$ for all $(x_i), (y_i) \in G$ since $\{\phi_{ij}\}$ are homomorphisms, meaning they map $e \mapsto e$ and they map $x_i y_i^{-1} \mapsto \phi_{ij}(x_i y_i^{-1}) = \phi_{ij}(x_i)\phi_{ij}(y_i)^{-1} = x_j y_j^{-1}$. Let $\{\pi_i : G \to G_i\}$ be given by $\pi_i : (g_i) \mapsto g_i$, then clearly $\{\pi_i\}$ are continuous homomorphisms since they are simply the canonical projections restricted to G, so they are compatible maps. Finally, assuming there is another topological group H with compatible maps $\{\psi_i\}$, the map $\theta : H \to \prod G_i$ given by $\theta : h \mapsto (\psi_i(h))$ is a continuous homomorphism since it is the product of continuous homomorphisms, and since $\{\psi_i\}$ are compatible maps, they satisfy $\phi_{ij}\psi_i = \psi_j$, so $\theta(H) \subseteq G$, i.e. $\theta : H \to G$. Note that the specific construction of θ implies it is induced by the compatible mappings $\{\psi_i\}$ and $\pi_i\theta : h \mapsto \psi_i(h)$, so $\pi_i\theta = \psi_i$, therefore all the conditions are satisfied and $G = \varprojlim G_i$.

(b) Say there are two inverse limits $\{G, \pi_i\}$ and $\{H, \psi_i\}$. From the definition of the inverse limit $\exists\, \theta : H \to G$ and $\exists\, \theta^{-1} : G \to H$ that are continuous homomorphisms satisfying $\pi_i\theta = \psi_i$ and $\psi_i\theta^{-1} = \pi_i$, so $\theta\theta^{-1} = \mathrm{Id}_G$ and $\theta^{-1}\theta = \mathrm{Id}_H$, meaning that θ is a bijective homeomorphism and homomorphism, i.e. a topological and group isomorphism. □

Example 1.1.12. The most trivial example of an inverse limit is that of a trivial inverse system, i.e. an inverse system of topological groups $\{G_i, \mathrm{Id}_G, I\}$ where $G_i = G$ for all $i \in I$. In this case the inverse limit is clearly just $\varprojlim G_i = G$ since the map $\theta : \varprojlim G_i \to G$ by $\theta : (g) \mapsto g$ is clearly a bijective homomorphism and a homeomorphism no matter the topology.

Example 1.1.13. Another example of a limit of an inverse system that can be finite is that of a stabilizing inverse system, i.e. a system $\{G_i, \phi_{ij}, I\}$ in which there is an $N \in I$ such that $G_i = G_N\ \forall i \geq N$ and $\phi_{ij} = \mathrm{Id}_{G_N}$ whenever $j \geq N$. Clearly, the inverse limit in this case is $\varprojlim G_i = G_N$ since $\theta : G_N \to \varprojlim G_i$ given by $\theta : g \to (\phi_{Nj}(g))$ is again a bijective homomorphism and a homeomorphism.

Example 1.1.14. Sometimes the inverse limit of a non-trivial inverse system can in fact be trivial. This is the case for the inverse system $\{G_n, \phi_{nm}, I\}$ where $G_n = n\mathbb{Z}$ for all $n \in \mathbb{N}$, i.e. G_n is the additive group $n\mathbb{Z}$ with the discrete topology, $\phi_{nm} : g \mapsto g$ whenever $m \mid n$, and I is the poset $\mathbb{N}$ with the binary relation '$\mid$'. Clearly, for any $(g_i) \in \varprojlim G_n$ we have $g_n = g_m$ whenever $m \mid n$, i.e. $g_m \in n\mathbb{Z}$. As a result, we see that for any $i \in \mathbb{N}$ we have $g_i \in ki\mathbb{Z}$ for any $k \in \mathbb{N}$, meaning that $g_i \in \bigcap_{k\in\mathbb{N}} ki\mathbb{Z} = \{0\}$, so the only possible element in this inverse limit is the identity element.

Example 1.1.15. A simple example of an infinite inverse limit would be that of the following inverse system $\{\prod_{i=1}^{n} G, \phi_{nm}, \mathbb{N}\}$, where $\prod_{i=1}^{n} G$ is just the product of a group G with the discrete topology n times, ϕ_{nm} are just the natural continuous surjective homomorphisms given by the projections $\phi_{nm}((x_1^{(n)}, \ldots, x_n^{(n)})) = (x_1^{(n)}, \ldots, x_m^{(n)})$ (where $(x_1^{(n)}, \ldots, x_n^{(n)}) \in \prod_{i=1}^{n} G$), and $\mathbb{N}$ is seen as a directed poset with respect to the relation $\leq$. Then the inverse limit is given by $\varprojlim \prod_{i=1}^{n} G \cong \prod_{i=1}^{\infty} G$. This is obvious, since the inverse limit is

$$\begin{aligned}\varprojlim \prod_{i=1}^{n} G =& \Big\{ \big((x_1^{(k)}, \ldots, x_k^{(k)})\big)_{k=1}^{\infty} \in \prod_{k=1}^{\infty} \prod_{i=1}^{k} G \mid \phi_{nm}((x_i^{(n)})_{i=1}^{n}) = (x_i^{(m)})_{i=1}^{m} \text{ when } n \geq m \Big\} \\ =& \Big\{ (x_i^{(k)}) \in \prod_{k=1}^{\infty} \prod_{i=1}^{k} G \mid (x_i^{(n)})_{i=1}^{m} = (x_i^{(m)})_{i=1}^{m} \text{ when } n \geq m \Big\} \\ \cong& \prod_{k=1}^{\infty} G.\end{aligned}$$

There are different approaches to gaining a better understanding of the inverse limit. While finding isomorphisms is one way to obtain information, we can also derive more general insights from the properties of the inverse system itself. The following lemmas provide us with further insights into the structure of the inverse limit that can be inferred from the structure of the inverse system.

Lemma 1.1.16. *[5, Proposition 1.1.5][4, Lemma 1.1.2, Propositions 1.1.3–1.1.4] Given an inverse limit $\varprojlim G_i = G$ of an inverse system $\{G_i, \phi_{ij}, I\}$ the following hold:*

(a) *If G_i is Hausdorff $\forall i \in I \implies G$ is Hausdorff.*

(b) *If G_i is totally disconnected $\forall i \in I \implies G$ is totally disconnected.*

(c) *If G_i is Hausdorff $\forall i \in I \implies G \leq_c \prod G_i$.*

(d) *If G_i is compact and Hausdorff $\forall i \in I \implies G$ is compact.*

(e) *If G_i is non-empty, compact and Hausdorff $\forall i \in I \implies G$ is non-empty.*

Proof. (a) The product of Hausdorff spaces is Hausdorff.

(b) The product of totally disconnected spaces is totally disconnected.

(c) Let $(g_i) \in (\prod G_i \setminus \varprojlim G_i)$ then $\exists\, r, s \in I$ such that $\phi_{rs}(g_r) \neq g_s$. Let $U_{r'} = U_{\phi_{rs}(g_r)} \subseteq G_s$ and $U_s = U_{g_s} \subseteq G_s$ be disjoint (this can be done due to Hausdorffness), and let $U_r = U_{g_r}$ be such that $\phi_{rs}(U_r) \subseteq U_{r'}$ (this can be done

due to the continuity of ϕ_{rs}). Then $\prod U_i$, where $U_i = G_i \quad \forall i \neq r, s$ is an open neighbourhood of (g_i) contained in $(\prod G_i \setminus \varprojlim G_i)$, so $\varprojlim G_i$ is closed.

(d) By Tychonoff's Theorem the product of compact spaces is compact, and from (c) G is closed, so it is a closed subgroup of a compact group, meaning it is compact.

(e) Defining $X_j \ \forall j \in I$ as subsets of $\prod G_i$ satisfying $\phi_{jk}(g_j) = g_k$ for all $k \leq j$, we see that $G = \bigcap X_j$. Furthermore, using the same argument as in (c) applied to each X_j we see that these are closed subsets, and by the axiom of choice they are non-empty, and since $X_j \subseteq X_{j'}$ when $j \geq j'$, they satisfy the finite intersection property (finite intersections are non-empty). Finally, since $\prod G_i$ is compact $\bigcap X_j$ is non-empty, otherwise the following would be an infinite open cover $\bigcup X_j^c$ which would have a finite subcover say $\bigcup_{j \in F} X_j^c = \prod G_i$, meaning that $\bigcap_{j \in F} X_j = \emptyset$, which contradicts the finite intersection property. □

It is worth highlighting an important result that pertains to the commutativity of inverse limits. As we will see, commutativity of a double inverse limit on a system of doubly-indexed topological groups is guaranteed whenever certain properties on the homomorphisms between the groups are satisfied. Furthermore, a doubly indexed inverse limit can be expressed as a double inverse limit.

Proposition 1.1.17. *[Author's work] Given a collection of topological groups $\{G_n^i\}_{n \in N}^{i \in I}$ with two indices and two sets of inverse systems on it, namely $\{G_n^i, \phi_{nm}^i, N\}$ for any fixed $i \in I$ and $\{G_n^i, \phi_n^{ij}, I\}$ for any fixed $n \in N$ such that $\phi_{nm}^j \phi_n^{ij} = \phi_m^{ij} \phi_{nm}^i$, the following inverse systems arrise: $\{\varprojlim_n G_n^i, \phi^{ij} = (\phi_n^{ij})_{n \in N}, I\}$, $\{\varprojlim_i G_n^i, \phi_{nm} = (\phi_{nm}^i)^{i \in I}, N\}$ and $\{G_n^i, \phi_{nm}^{ij} = \phi_m^{ij} \phi_{nm}^i, N \times I\}$. Furthermore, we have that the double inverse limits commute and are isomorphic to the inverse limit indexed by $N \times I$, i.e.*

$$\varprojlim_n \varprojlim_i G_n^i \cong \varprojlim_{(n,i)} G_n^i \cong \varprojlim_i \varprojlim_n G_n^i.$$

Proof. Using the description of the inverse limit given in Proposition 1.1.11(a), and by the commutativity of the lattice of topological groups we have that

$$\begin{aligned}
\varprojlim_n \varprojlim_i G_n^i &= \{(x_n^i) \in \prod_{n \in N} \varprojlim_i G_n^i \mid \phi_{nm}((x_n^i)^{i \in I}) = (x_m^i)^{i \in I}\} \\
&= \{(x_n^i) \in \prod_{n \in N} \prod_{i \in I} G_n^i \mid \phi_{nm}^i(x_n^i) = x_m^i \text{ and } \phi_n^{ij}(x_n^i) = (x_n^j)\} \\
&= \{(x_n^i) \in \prod_{n \in N} \prod_{i \in I} G_n^i \mid \phi_m^{ij} \phi_{nm}^i(x_n^i) = x_m^j\}
\end{aligned}$$

$$
\begin{aligned}
&= \varprojlim_{(n,i)} G_n^i \\
&\cong \{(x_n^i) \in \prod_{i\in I}\prod_{n\in N} G_n^i \mid \phi_m^{ij}\phi_{nm}^i(x_n^i) = x_m^j\} \\
&= \{(x_n^i) \in \prod_{i\in I} \varprojlim_{n} G_n^i \mid \phi^{ij}((x_n^i)_{n\in N}) = (x_n^j)_{n\in N}\} \\
&= \varprojlim_{i}\varprojlim_{n} G_n^i. \qquad \square
\end{aligned}
$$

The following proposition demonstrates that every inverse limit of an inverse system can be regarded as an inverse limit of a corresponding surjective inverse system. Therefore, whenever we consider an inverse limit, we can always view it in terms of a surjective inverse system.

Proposition 1.1.18. *(Inspired by [4, Corollary 1.1.8(a)]) The inverse limit $\{G, \pi_i\}$ of an inverse system $\{G_i, \phi_{ij}, I\}$ of topological groups is isomorphic to the inverse limit of a surjective inverse system, i.e. an inverse system with surjective mappings ϕ_{ij}.*

Proof. We claim that the surjective inverse system we are looking for is the one given by $\{\pi_i(G), \phi_{ij}|_{\pi_i(G)}, I\}$. First, we define the maps $\psi_i : G \to \pi_i(G)$ given by $\psi_i : (g_k) \mapsto \pi_i((g_k)) = g_i$, which are clearly well-defined compatible surjections, hence by the universal property of the inverse limit they induce a continuous homomorphism $\theta : G \to \varprojlim \pi_i(G)$ given by $\theta : (g_k) \mapsto (\psi_i((g_k)))$, which is clearly the identity map, so it is an isomorphism. Finally, we note that this is indeed a surjective inverse system since the mappings $\phi_{ij}|_{\pi_i(G)}$ satisfy $\phi_{ij}|_{\pi_i(G)}(\pi_i(G)) = \phi_{ij}(\pi_i(G)) = \pi_j(G)$ by the compatibility of the projections. $\square$

Just like we saw in the proposition above, we can have different inverse systems having the same inverse limit. It turns out that for certain inverse systems, more specifically those with compact Hausdorff topological groups, a similar kind of result can be obtained. By restricting —following certain restriction rules— the number of topological groups composing an inverse system we can find "reduced" inverse systems with the same inverse limit as our original inverse system. This reduction is what we will call finding a cofinal subsystem to an inverse system.

Definition 1.1.19 (Cofinal Subset)**.** A cofinal subset is a subset $I' \subseteq I$ of a directed poset that is also a directed poset and satisfies that $\forall i \in I$ there is an element $i' \in I'$ such that $i \leq i'$. Given an inverse system with poset I the subsystem with poset I' is called a cofinal subsystem.

Example 1.1.20. An example of a cofinal subset of $\mathbb{N}$ with the relation $\leq$ is the subset of all even natural numbers.

Lemma 1.1.21. *[4, Lemma 1.1.9] Given an inverse system $\{G_i, \phi_{ij}, I\}$ of compact Hausdorff topological groups, and a cofinal subsystem $\{G_i, \phi_{ij}, I'\}$, we have that $\varprojlim G_i \cong \varprojlim G_{i'}$ (topological and group isomorphism).*

Proof. Define $\psi_i : \varprojlim G_{i'} \to G_i$ as $\psi_i = \phi_{i'i}\pi_{i'}$, where $\pi_{i'}$ are the projections of $\varprojlim G_{i'}$. Then, since $\{\psi_i\}$ are well-defined and compatible, by the universal property of the inverse limit and from Proposition 1.1.11, these maps induce a continuous homomorphism $\theta : \varprojlim G_{i'} \to \varprojlim G_i$ by $\theta : (g_{i'}) \mapsto (\psi_i((g_{i'})))$, which we claim is a bijection. To prove injectivity, let $(x_{i'}), (y_{i'}) \in \varprojlim G_{i'}$ such that $\theta((x_{i'})) = \theta((y_{i'}))$ then $\forall i \in I$

$$\psi_i((x_{i'})) = \psi_i((y_{i'})) \implies \phi_{i'i}\pi_{i'}((x_{i'})) = \phi_{i'i}\pi_{i'}((y_{i'})) \implies x_i = y_i$$

i.e. $(x_{i'}) = (y_{i'})$. Now, for surjectivity we take an arbitrary $(y_i) \in \varprojlim G_i$ and see that the element $(x_{i'}) \in \varprojlim G_{i'}$ satisfying $x_{i'} = y_{i'}$ $\forall i' \in I'$ is such that

$$\theta((x_{i'})) = (\psi_i((x_{i'}))) = (\phi_{i'i}\pi_{i'}((x_{i'}))) = (\phi_{i'i}(x_{i'})) = (\phi_{i'i}(y_{i'})) = (y_i).$$

Since θ is a bijective homomorphism it is a group isomorphism, so all that is left to prove is that it is a topological isomorphism, i.e. a homeomorphism. Since the G_i are compact and Hausdorff, by Lemma 1.1.16(a),(d) the domain and codomain of θ are compact Hausdorff, meaning that θ is a closed map (because a closed subset of a compact space is compact and continuous maps map compact sets to compact sets, so the image of a closed subset is compact), and every compact subset in a Hausdorff space is closed, meaning that θ sends closed sets to closed sets, which is equivalent to its inverse being continuous, thus θ is indeed a homeomorphism. □

The lemma mentioned above, which allows for reduction of inverse systems, will prove to be particularly valuable in our forthcoming discussions of profinite groups. Since profinite groups are instances of inverse limits of compact Hausdorff inverse systems, we can utilize this lemma to obtain more explicit expressions for certain profinite groups that we will be investigating. Moreover, these compact and Hausdorff properties of the inverse systems composing profinite groups allow us to draw conclusions regarding the surjectivity of the projections when the continuous homomorphisms between the topological groups are surjective.

Proposition 1.1.22. *[4, Proposition 1.1.10] Given a non-empty compact Hausdorff inverse system $\{G_i, \phi_{ij}, I\}$ where ϕ_{ij} are surjective maps, the projections of the inverse limit $\{\varprojlim G_i, \pi_i\}$ are also surjective.*

Proof. For any $k \in I$ and any $g \in G_k$, following the proof of Lemma 1.1.16(e) with the sets X_j defined as $X_j := \{(g_i) \in \prod G_i \mid g_j \in \phi_{jk}^{-1}(g) \text{ and } g_i = \phi_{ji}(g_j)\ \forall i \leq j\}$ (which we know are non-empty by the use of Zorn's Lemma and the fact that ϕ_{jk} are surjective) we arrive at the conclusion that $\bigcap_{j\in I} X_j \neq \emptyset$, and clearly $\bigcap_{j\in I} X_j \subseteq \varprojlim G_i$, so for any $(g_i) \in \bigcap_{j\in I} X_j$ we have $(g_i) \in \varprojlim G_i$ and $\pi_k((g_i)) = g$. □

1.2 Profinite Groups

In the following section we will explore the concept of profinite groups to better understand the properties associated with them that make them so useful for generalizing finite group theory to the infinite case.

Definition 1.2.1 (Profinite Group)**.** A profinite group is a topological group that is the inverse limit of a surjective inverse system of finite discrete topological groups.

Given Proposition 1.1.18 the surjectivity condition on the construction of a profinite group may be disregarded, but it is included in the definition here because this is the way it is usually presented in the literature.

Example 1.2.2. We have already seen the construction of a profinite group given in Example 1.1.15.

Example 1.2.3. The p-adic integers $\mathbb{Z}_{\hat{p}}$ are an important and useful example of profinite groups. Given the inverse system $\{\mathbb{Z}_{p^n}, \phi_{nm}, \mathbb{N}\}$ where $\mathbb{Z}_{p^n}$ are simply the additive groups of integers modulo p^n with the discrete topology, the maps ϕ_{nm} are given by the natural surjective homomorphisms $\phi_{nm} : [z]_{p^n} \mapsto [z]_{p^m}$ whenever $n \geq m$ and the directed poset $\mathbb{N}$ is given by the relation $\leq$. Then, following the construction presented in Proposition 1.1.11(a) we see that the inverse limit is given by

$$\varprojlim \mathbb{Z}_{p^n} := \{(z_i) \in \prod_{1}^{\infty} \mathbb{Z}_{p^n} \mid z_i \equiv z_j \pmod{p^i} \text{ whenever } i \leq j\},$$

which is precisely the definition of the p-adic integers, i.e. $\mathbb{Z}_{\hat{p}} = \varprojlim \mathbb{Z}_{p^n}$.

Example 1.2.4. A typical example of a profinite group is also the inverse limit of the inverse system $\{\mathbb{Z}_n, \phi_{nm}, \mathbb{N}\}$ where $\mathbb{Z}_n$ are the additive groups of integers modulo n and ϕ_{nm} are the natural surjective homomorphisms given by $\phi_{nm} : [z]_n \mapsto [[z]_n]_m$ whenever $m \mid n$. This group is sometimes called the profinite completion of the integers and it is denoted $\hat{\mathbb{Z}}$. We can then show that this group is in fact isomorphic to $\prod_{p \text{ prime}} \mathbb{Z}_{\hat{p}}$. By the Chinese Remainder Theorem (see Theorem A.0.1), given a number $n \in \mathbb{N}$ and its factor decomposition $n = p_1^{k_{p_1}(n)} \cdots p_r^{k_{p_r}(n)}$ we can construct an isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_{p_1}(n)}} \times \cdots \times \mathbb{Z}_{p_r^{k_{p_r}(n)}} = \prod_{\substack{p \text{ prime} \\ p \mid n}} \mathbb{Z}_{p^{k_p(n)}}.$$

As a result we have that

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n \cong \varprojlim_n \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(n)}},$$

which we can see is the inverse limit of a cofinal subsystem of the system of groups

$$\left\{ \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(m)}} \right\}_{(n,m) \in N \times M}.$$

With this we can reexpress the inverse limit as a double inverse limit (using Proposition 1.1.17 and Lemma 1.1.21)

$$\varprojlim_n \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(n)}} \cong \varprojlim_{(n,m)} \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(m)}} \cong \varprojlim_m \varprojlim_n \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(m)}}.$$

Then, using Proposition 1.1.17 and Example 1.1.15 we get that

$$\varprojlim_m \varprojlim_n \prod_{\substack{p \text{ prime} \\ p|n}} \mathbb{Z}_{p^{k_p(m)}} \cong \varprojlim_n \prod_{\substack{p \text{ prime} \\ p|n}} \varprojlim_m \mathbb{Z}_{p^{k_p(m)}} \cong \prod_{p \text{ prime}} \varprojlim \mathbb{Z}_{p^{k_p(n)}}.$$

Finally, the inverse limit $\varprojlim \mathbb{Z}_{p^n}$ is isomorphic to $\varprojlim \mathbb{Z}_{p^{k_p(n)}}$ by Lemma 1.1.21 since it is the inverse limit of a cofinal subsystem, so

$$\prod_{p \text{ prime}} \varprojlim \mathbb{Z}_{p^{k_p(n)}} \cong \prod_{p \text{ prime}} \varprojlim \mathbb{Z}_{p^n} = \prod_{p \text{ prime}} \mathbb{Z}_{\hat{p}},$$

meaning that the profinite completion of the integers $\hat{\mathbb{Z}}$ is isomorphic to $\prod_{p \text{ prime}} \mathbb{Z}_{\hat{p}}$.

Example 1.2.5. The subset of the set of integers modulo n, i.e. $\mathbb{Z}_n$, comprised of those elements coprime to n can be seen as a multiplicative group. This group is called the group of units of the integers modulo n (ring theoretical name that expresses the idea of this being a subset of elements with multiplicative inverses), denoted $\mathbb{Z}_n^\times$. From this idea we may construct the multiplicative group of the p-adic integers as a profinite group from the inverse system $\{\mathbb{Z}_{p^n}^\times, \phi_{nm}, \mathbb{N}\}$, where ϕ_{nm} are defined as restrictions of the maps in the example above (these are still clear homomorphisms under multiplication and they are well defined between the sets of units because under these maps coprimes of n in $\mathbb{Z}_{p^n}$ are mapped to coprimes of m in $\mathbb{Z}_{p^m}$ whenever $m \leq n$). As a result, we have that $\varprojlim \mathbb{Z}_{p^n}^\times = \mathbb{Z}_{\hat{p}}^\times$.

We can also define profinite groups in terms of some of their topological and group properties. In fact, it turns out that these properties that fully characterize profinite groups are not as restrictive as one might intuitively think.

Lemma 1.2.6. *[5, Corollary 1.2.4] Let G be a topological group. The following are equivalent:*

(a) *The group G is a profinite group.*

(b) *The group G is isomorphic to some $H \leq_c \prod G_i$, where $\{G_i\}$ are finite discrete topological groups.*

(c) *The group G is compact and $\bigcap_{N \trianglelefteq_o G} N = \{e\}$.*

(d) *The group G is compact and totally disconnected.*

Proof. (a)⇒(b) This follows from Lemma 1.1.16(c).

(b)⇒(c) Compactness comes from the fact that G is isomorphic to a closed subset of the compact space $\prod G_i$, i.e. it is isomorphic to a compact set. Now, denoting by $K_i := \ker(\pi_i)$ the kernel of π_i (where $\pi_i : \prod G_n \to G_i$ are the canonical projections) we can construct the sets $N_i = K_i \cap G$. Clearly K_i are open in $\prod G_i$ since the canonical projections are continuous, and so N_i are open in the subspace topology of G. Finally, $\forall g \in G$ we have $gN_ig^{-1} \in K_i$ since $\pi_i(gN_ig^{-1}) = \pi_i(g)e\pi_i(g)^{-1} = e$ and $gN_ig^{-1} \in G$ therefore we have that $gN_ig^{-1} \in N_i$, so $N_i \trianglelefteq_o G$, and $\bigcap K_i = \{e\}$, so $\bigcap N_i = \{e\}$, meaning that $\bigcap_{N \trianglelefteq_o G} N = \{e\}$.

(c)⇒(a) Let $I := \{N \mid N \trianglelefteq_o G\}$ and let $N_i = i \in I$, then by Lemma 1.1.4(d) G/N_i are finite $\forall i \in I$. Given the partial ordering on I by $i \leq j \iff N_i \geq N_j$, the following surjective continuous homomorphisms can be constructed $\phi_{ij} : N_ig \mapsto N_jN_ig$ whenever $i \geq j$, so $\{G/N_i, \phi_{ij}, I\}$ is a surjective inverse system of finite groups which we can endow with the discrete topology. Finally, we prove the existence of an isomorphism of topological groups between G and the inverse limit of said inverse system. We construct the following compatible maps $\psi_i : G \to G/N_i$ by $\psi_i : g \mapsto N_ig$, and then by the universal property of the inverse limit these maps induce a continuous homomorphism $\theta : G \to \varprojlim G/N_i$ by $\theta(g) = (\psi_i(g))$. Now we claim $\ker(\theta) = \bigcap N_i$, which is true since

$$g \in \ker(\theta) \iff Ng = N \quad \forall N \in I \iff g \in \bigcap N_i$$

so $\ker(\theta) = \{e\}$, i.e. θ is injective since it is a homomorphism with trivial kernel. It is also surjective since it is induced by clearly surjective mappings, so it is a bijection, hence, just like in the proof of Lemma 1.1.21, the map θ is an isomorphism of topological groups, so G is a profinite group.

(a)⇒(d) This follows from Lemma 1.1.16(a),(b).

(d)⇒(c) We will first prove that for any closed subset $C \subseteq_c G$ we have that $C = \bigcap_{N \trianglelefteq_o G} NC$. If $x \notin C$ then $x \in C^c$ open, so $C^c x^{-1}$ is an open set by Lemma 1.1.4(a) and it clearly contains e, meaning that we can apply Lemma 1.1.5, so $\exists N \trianglelefteq_o G$ such that $N \subseteq C^c x^{-1}$, so $Nx \subseteq C^c$ therefore $Nx \cap C = \emptyset$, i.e. the element $x \notin NC$. As a result we gather that $\bigcap_{N \trianglelefteq_o G} NC \subseteq C$ and the other inclusion comes from the fact that C being closed implies it is its own closure, i.e. it is the intersection of all closed sets containing it, and NC is closed $\forall N \trianglelefteq_o G$ because it is open $NC = \bigcup_{c \in C} Nc$ by Lemma 1.1.4(a),(b). Finally, since G is compact and totally disconnected, using Lemma B.0.5 we see that for any $g \in G$ the set $(G \setminus \{g\}) = \bigcup_{h \in (G \setminus \{g\})} U_h$ —where U_h are clopen sets not containing g— is a union of open sets, meaning that $\{g\}$ is closed, therefore $\{e\} = \bigcap_{N \trianglelefteq_o G} N$. □

Corollary 1.2.7. *[4, Proposition 2.2.1] The inverse limit of an inverse system of profinite groups is a profinite group.*

Proof. This follows from the lemma above together with Lemma 1.1.16. □

Corollary 1.2.8. *A subgroup of a profinite group is closed if and only if it is a profinite group.*

Proof. (⇒) Follows from the above lemma and the fact that closed subgroups in compact spaces are compact.
(⇐) By the lemma above given a profinite group G with a subgroup H that is also a profinite group we have that both are compact totally disconnected spaces. Now, using Lemma B.0.5 we see that for any $x \in H^c$ there is an open cover $\bigcup_{h \in H} F_h$ of H composed of clopen sets F_h satisfying that $h \in F_h$ and $x \notin F_h$. By the compactness of H there must be a finite subcover $H \subseteq F = \bigcup_1^n F_i$. As a result, F is a closed subset of G —since it is the finite union of clopen sets—, and $x \in F^c \subseteq H^c$, meaning that for any point $x \in H^c$ we can find an open neighbourhood of x contained in H^c, i.e. H^c is open and so H must be closed. □

Profinite groups possess a remarkable attribute in that they can never be countably infinite. This distinguishing feature arises directly from their topological properties as compact totally disconnected spaces.

Proposition 1.2.9. *[4, Proposition 2.3.1] Every profinite group is either finite or uncountable.*

Proof. Assume G is infinite, we will first show that $G \neq \bigcup_1^\infty C_i$ where C_i are non-empty closed sets with empty interior. We search for a contradiction to the statement $G = \bigcup_1^\infty C_i$. Then $D_i = (G \setminus C_i)$ are dense open subsets. Then taking U_0 to be any non-empty open subset, clearly $U_0 \cap D_1$ is a non-empty open set, so by the same argument as in the first part of the proof in Lemma 1.1.5, there exists $U_1 \subseteq U_0 \cap D_1$ that is clopen and non-empty. But then, $U_1 \cap D_2$ is an open non-empty subset, so we can find $U_2 \subseteq U_1 \cap D_2$ that is clopen. By continuing this process we get a descending chain of clopen sets $U_0 \supseteq U_1 \supseteq U_2 \supseteq \cdots$. Clearly these sets U_i have the finite intersection property, and since G is compact we have $\bigcap U_i \neq \emptyset$, but on the other hand $\bigcap U_i \subseteq \bigcap D_i \subseteq (G \setminus \bigcup C_i) = \emptyset$, which is a contradiction, so $G \neq \bigcup_1^\infty C_i$.
Finally, since G is a profinite group, by Lemma 1.2.6(d) we know it is compact and totally disconnected, so using Lemma B.0.5 we see that for any $g \in G$ the set $(G \setminus \{g\}) = \bigcup_{h \in (G \setminus \{g\})} U_h$ —where U_h are clopen sets not containing g— is a union of open sets, meaning that $\{g\}$ is closed. As a result we see that if G were countable then $G = \bigcup_1^\infty \{g_i\}$ where $\{g_i\}$ are non-empty closed sets with empty interior, which is a contradiction, thus G is uncountable. □

2 Lagrange, Sylow and Galois Theorems

2.1 Index and Order of Profinite Groups

The notion of index of finite groups as the number of distinct right cosets of a subgroup becomes too limiting if we only allow said numbers to be finite ones, especially when considering infinite profinite groups. In order to circumvent this problem a —not necessarily finite— notion of the index is introduced, and for that the concept of supernatural numbers is utilized.

Definition 2.1.1 (Supernatural Numbers)**.** A supernatural number is a number n that is the formal product of all primes to a non-negative (possibly infinite) power, i.e.

$$n = \prod_{p \text{ prime}} p^{n(p)} \qquad \text{where } n(p) \in \mathbb{N}_\infty \ .$$

Example 2.1.2. An example of a supernatural number is any natural number. This is trivially true since natural numbers can be decomposed into prime factors. The importance of supernatural numbers comes when distinguishing the factors of different types of infinity. The supernatural number 2^∞ is clearly not divisible by the supernatural number 3^∞, since they do not share any common factors, but both numbers are infinite ones in the sense that they are an infinite power of a natural number. This distinction is what we will later use to distinguish profinite groups of infinite order that are constructed from finite groups of prime power orders.

Under this definition the least common multiple of supernatural numbers is defined as follows.

Definition 2.1.3 (Least Common Multiple)**.** Given a set of supernatural numbers $\{n_i\}_{i\in I}$ the least common multiple is

$$\operatorname{lcm}\{n_i\}_{i\in I} = \prod_{p \text{ prime}} p^{n(p)} \qquad \text{where } n(p) = \max_{i\in I}\{n_i(p)\} \ .$$

Example 2.1.4. The least common multiple of the two supernatural numbers $n = 2^{56}11^{20}101^3$ and $m = 3^\infty 7^2 11^2$ is $\operatorname{lcm}\{n, m\} = 2^{56}3^\infty 7^2 11^{20}101^3$.

Now we are ready to introduce the idea of the index and order of a profinite group.

Definition 2.1.5 (Index)**.** The index of a closed subgroup H of a profinite group G is $(G : H) = \operatorname{lcm}\{[G : U] \mid H \leq U \leq_o G\}$.

Remark 2.1.6. Clearly this is a well-defined expression since it is induced by the notion of index of finite groups. Notice that $[G : U]$ is finite by Lemma 1.1.4(d). Furthermore, $\operatorname{lcm}\{[G : U] \mid H \leq U \leq_o G\} = \operatorname{lcm}\{[G : NH] \mid N \trianglelefteq_o G\}$ since by Lemma 1.1.5 for any $U \leq_o G$ such that $H \leq U$, there exists $N \trianglelefteq_o G$ such that $NH \leq U$, meaning that $[G : U] \mid [G : NH]$.

Example 2.1.7. The subgroup $H = \prod_1^n \{e\} \times \prod_n^\infty C_2$ of the profinite group $G = \prod_1^\infty C_2$ given as in Example 1.1.15 is clearly an open subgroup in its product topology since it is a product with only finitely many open strict subgroups of the group C_2, so $(G : H) = [G : H]$ and the number of distinct right cosets of H is exactly 2^n since there are 2^n distinct elements in $\prod_1^n C_2$, therefore $(G : H) = 2^n$.

With the new definition of index, we can now express the infinite index of the identity element of an infinite profinite group in terms of supernatural numbers.

Example 2.1.8. Taking our infinite profinite group to be $G = \prod_1^\infty C_2$ as in Example 1.1.15, and since from Example 2.1.7 we know that the chain of open subgroups $U_n = \prod_1^n \{e\} \times \prod_n^\infty C_2$ satisfying that $U_n \supseteq U_{n+1}$ and $U_n \supset \{e\}$ for all $n \in \mathbb{N}$ is such that $[G : U_n] = 2^n$, we have that

$$[G : \{e\}] = \operatorname{lcm}\{[G : U] \mid \{e\} \leq U \leq_o G\} = \lim_{n\to\infty} [G : U_n] = \lim_{n\to\infty} 2^n = 2^\infty.$$

Proposition 2.1.9. *[4, Proposition 2.3.2] Given $H \leq_c G$ where G is a profinite group, then $(G : H) < \infty$ if and only if $H \leq_o G$.*

Proof. ($\Leftarrow$) If H is an open subgroup of G then

$$(G : H) = \operatorname{lcm}\{[G : U] \mid H \leq U \leq_o G\} = [G : H],$$

and by Lemma 1.1.4(d) we have that $[G : H] < \infty$, so $(G : H) < \infty$.

($\Rightarrow$) If the index is finite, i.e. $(G : H) < \infty$, then, since by Remark 2.1.6 we have $(G : H) = \operatorname{lcm}\{[G : NH] \mid N \trianglelefteq_o G\}$ and for any two $N, M \trianglelefteq_o G$ we have that $N \cap M \trianglelefteq_o G$ then;

$$(G : H) = \operatorname{lcm}\{[G : N_iH] \mid N_i \trianglelefteq_o G,\ N_{i+1} \leq N_i\} < \infty.$$

As a result, we see that there is a $k \in \mathbb{N}$ such that $N_i = N_{i+1}\ \forall i > k$, so $\bigcap N_iH$ is a finite intersection of open sets, and using the same argument as in Lemma 1.2.6 proof (d)$\Rightarrow$(c) we see that $H = \bigcap N_iH$, so $H \leq_o G$. □

Corollary 2.1.10. *The index of a closed subgroup of a profinite group is finite if and only if it has finitely many distinct cosets.*

Proof. Follows from the proposition above together with Lemma 1.1.4. □

Remark 2.1.11. From this corollary we see that this new notion of index aligns —in the finite case— with the idea of the index of a subgroup as the number of distinct cosets of the subgroup, so from this point forward we shall denote both notions of index by $[G : H]$. It is also important to point out that the restriction in the definition of the index that makes the subgroup necessarily closed is indeed essential to this alignment of concepts since it is required for the proof of Proposition 2.1.9.

Following this new definition of index a natural definition of order of a group arises as well.

Definition 2.1.12 (Order)**.** The order of a profinite group G is $|G| = [G : \{e\}]$.

Example 2.1.13. As shown in Example 2.1.8, the profinite group $G = \prod_1^\infty C_2$ is a group of order $|G| = 2^\infty$.

2.2 Lagrange and Sylow Theorems for Profinite Groups

In this section we will use the tools and concepts developed up to this point to generalize Lagrange's Theorem and the Sylow Theorems to profinite groups, which, as we know, will be a generalization beyond the classical finite constitution of these theorems.

Theorem 2.2.1 (Lagrange's Theorem for Profinite Groups.)**.** *[5, Proposition 2.1.2] Given $K \leq_c H \leq_c G$ where G is a profinite group then*

$$[G : K] = [G : H]\,[H : K]\,.$$

Proof. First we notice that for any $S \leq G$ and any $N \trianglelefteq_o G$, the set NS is open in G because $NS = \bigcup_{s\in S} Ns$ and $Ns \subseteq_o G$ by Lemma 1.1.4(a). As a result, by Lemma 1.1.4(d), we have that $[G : NK] < \infty$ so we can use Lagrange's Theorem for Finite Groups (see Theorem A.0.2) to see that

$$[G : NK] = [G : NH]\,[NH : NK] = [G : NH]\,[H : (N \cap H)K] \qquad (*)$$

(here the second equality is satisfied by the use of the First Isomorphism Theorem (see Theorem A.0.3) on the homomorphism $H \to NH/NK$ given by $h \mapsto hNK$ which has $\ker = H \cap NK$).
Then we see that, by Remark 2.1.6, we have

$$\begin{aligned}[G : H]\,[H : K] &= \operatorname{lcm}\{[G : NH] \mid N \trianglelefteq_o G\}\operatorname{lcm}\{[H : NK] \mid N \trianglelefteq_o H\} \\ &= \operatorname{lcm}\{[G : N_1H]\,[H : N_2K] \mid N_1 \trianglelefteq_o G,\ N_2 \trianglelefteq_o H\}.\end{aligned}$$

As a result, since in $(*)$ the subgroup $(N \cap H)$ is a normal open subgroup in H, we immediately get

$$[G : K] = \text{lcm}\{[G : NK] \mid N \trianglelefteq_o G\} = \text{lcm}\{[G : NH]\,[H : (N \cap H)K] \mid N \trianglelefteq_o G\}$$

divides

$$\text{lcm}\{[G : N_1H]\,[H : N_2K] \mid N_1 \trianglelefteq_o G,\ N_2 \trianglelefteq_o H\} = [G : H]\,[H : K]\,.$$

Now, if $N_1 \trianglelefteq_o G$ and $N_2 \trianglelefteq_o H$ then N_2 is the intersection of H and an open subset of G, so using Lemma 1.1.5 $\exists M \trianglelefteq_o G$ such that $(M \cap H) \leq N_2$. Finally, letting $N = M \cap N_1$ and using $(*)$ we get that $[G : N_1H]\,[H : N_2K]$ divides $[G : NH]\,[H : (N \cap H)K] = [G : NK]$, which implies that

$$[G : H]\,[H : K] = \text{lcm}\{[G : N_1H]\,[H : N_2K] \mid N_1 \trianglelefteq_o G,\ N_2 \trianglelefteq_o H\}$$

divides

$$\text{lcm}\{[G : NH]\,[H : (N \cap H)K] \mid N \trianglelefteq_o G\} = [G : K]\,,$$

meaning that $[G : H]\,[H : K] = [G : K]$. □

Now that we have an equivalent theorem to Lagrange's concerning profinite groups we can tackle the idea of extending the Sylow Theorems to profinite groups as well. For this purpose we shall start by defining pro-p subgroups and p-Sylow subgroups.

Definition 2.2.2 (Pro-p Subgroup)**.** A pro-p subgroup is a closed subgroup H of a profinite group G whose order $|H|$ is a power of p.

Lemma 2.2.3. *[5, Comment pg 35, Proposition 1.2.1] The following are equivalent:*

(a) *The group G is a pro-p subgroup of a profinite group.*

(b) *The quotient G/N has p-power order for every $N \trianglelefteq_o G$.*

(c) *The group G is the inverse limit of an inverse system of finite groups of order a power of p.*

Proof. (a)⇔(b) We have $|G| = [G : \{e\}] = \text{lcm}\{[G : N] \mid N \trianglelefteq_o G\} = p^{n(p)}$ for some $n(p) \in \mathbb{N}_\infty \iff [G : N] = p^{n_N}$ for some $n_N \in \mathbb{N}$, $\forall N \trianglelefteq_o G$.

(a)⇒(c) The group G being a pro-p subgroup implies it is a closed subgroup of a profinite group, and so, by Corollary 1.2.8, it is a profinite group. Finally, following the same construction of an inverse system as in Lemma 1.2.6, proof of (c)⇒(a), we see that G is an inverse limit to the inverse system of finite groups

$\{G/N \mid N \trianglelefteq_o G\}$, which by (b) are of p-power order.

(c)⇒(b) Since G is an inverse limit of an inverse system of finite groups of p-power order, say $\{G_i\}_{i\in I}$, it must have projection mappings say $\{\pi_i\}$. Then we notice that since $\{e_{G_i}\} \leq_c G_i$ (under the discrete topology every subset is clopen) and $\{\pi_i\}$ are continuous homomorphism, we have $\ker(\pi_i) \trianglelefteq_c G$ (normality comes from the fact that the kernel of a homomorphism is always a normal subgroup) and by the First Isomorphism Theorem (see Theorem A.0.3) $G/\ker(\pi_i) \cong \pi_i(G) \leq G_i$, hence $[G : \ker(\pi_i)] < \infty$, therefore by Lemma 1.1.4(c) we have that $\ker(\pi_i) \trianglelefteq_o G$.

We now claim that, given any $N \trianglelefteq_o G$, $\exists\, k \in I$ such that $\ker(\pi_k) \leq N$. To prove this claim we start by noticing that $\bigcap_{i\in I} \ker(\pi_i) = e$, this is true since for any $g \neq e$, expressing the element as a sequence $g = (g_i) \in \prod G_i$, we see that there must be some $n \in I$ such that $g_n \neq e \in G_n$, which implies that $(g_i) \notin \ker(\pi_n)$, meaning that $g \notin \bigcap_{i\in I} \ker(\pi_i)$. Then N^c is compact since it is a closed subset of a compact set (here G is compact by Lemma 1.1.16) and $\bigcup_{i\in I} \ker(\pi_i)^c$ is an open cover of it since $e = \bigcap_{i\in I} \ker(\pi_i) \subseteq N$, meaning that there exists a finite subcover $\bigcup_{i\in F} \ker(\pi_i)^c$ for some $F \subseteq I$ with $|F| < \infty$ such that $\bigcap_{i\in F} \ker(\pi_i) \subseteq N$. Since I is a directed poset there must be some $k \in I$ such that $k \geq i$ for all $i \in F$ and since $\ker(\pi_i) \leq \ker(\pi_j)$ whenever $i \geq j$, we must have $\ker(\pi_k) \leq \bigcap_{i\in F} \ker(\pi_i) \leq N$. As a result, using Lagrange, we get that

$$|G/N| = \frac{|G/\ker(\pi_k)|}{|N/\ker(\pi_k)|} \;\Big|\; \frac{|G_k|}{|N/\ker(\pi_k)|}$$

hence $|G/N|$ is a divisor of a p-power, so it is a p-power itself. □

Example 2.2.4. An easy example of a pro-p group is the profinite group given in Example 2.1.8. This group is indeed a pro-2 group since it is the inverse limit of an inverse system of finite groups of order 2^n.

Example 2.2.5. Another example we have seen of pro-p groups are the groups of p-adic integers $\mathbb{Z}_{\hat{p}}$ since, as seen in Example 1.2.3, they are constructed from finite groups of order p^n.

Definition 2.2.6 (p-Sylow Subgroup)**.** A p-Sylow subgroup is a closed subgroup $H \leq G$ of a profinite group G that is a maximal pro-p subgroup in the sense that $[G : H]$ is coprime to p.

Example 2.2.7. The subgroup $(\mathbb{Z}_{\hat{q}} \times \prod_{\substack{p \text{ prime} \\ p\neq q}} \{e_{\mathbb{Z}_{\hat{p}}}\})$ (where $e_{\mathbb{Z}_{\hat{p}}}$ is the identity in the group $\mathbb{Z}_{\hat{p}}$) of the group $\hat{\mathbb{Z}}$ given in Example 1.2.4 is a p-Sylow subgroup.

It is important to note that both pro-p subgroups and p-Sylow subgroups could still have infinite order, as demonstrated in the preceding example. Based on our definition of supernatural numbers, as well as the definitions of index and order that follow, these subgroups may potentially have orders that are infinite powers of p.

Before proving the Sylow Theorems for profinite groups we need to introduce a lemma concerning the index of intersections of chains of closed subgoups.

Lemma 2.2.8. *[5, Lemma 2.1.3] Given a family of closed subgroups $\{H_j\}_{j\in J}$ of a profinite group G that is a descending directed poset with respect to inclusion, the following holds*

$$\left[G : \bigcap H_j\right] = \operatorname{lcm}\{[G : H_j]\}_{j\in J}.$$

Proof. Clearly, by Lagrange $\operatorname{lcm}\{[G : H_j]\}_{j\in J}$ divides $[G : \bigcap H_j]$. Now, given U such that $\bigcap H_j \leq U \leq_o G$, it is true that $\bigcup H_j^c$ is an open cover for U^c which is clearly compact since it is a closed subgroup in a compact space (here G is compact by Lemma 1.2.6), meaning that there is a finite subset $F \subseteq J$ such that $\bigcup\limits_{j\in F} H_j^c$ is a finite subcover for U^c, which implies that $\bigcap\limits_{j\in F} H_j \leq U$. Finally, since $\{H_j\}_{j\in J}$ is a directed poset there is some $k \in J$ such that $H_k \leq H_j$ for all $j \in F$, i.e. $H_k \leq U$, so $[G : U] \mid [G : H_k]$, meaning that $[G : \bigcap H_j] = \operatorname{lcm}\{[G : U] \mid \bigcap H_j \leq U \leq_o G\}$ divides $\operatorname{lcm}\{[G : H_j]\}_{j\in J}$. □

The subsequent theorem will present and establish the two generalizations of the Sylow Theorems - the existence theorem and the conjugate theorem.

Theorem 2.2.9 (Sylow Theorems for Profinite Groups)**.** *[5, Proposition 2.2.2][4, Corollary 2.3.6] Given a profinite group G and a prime p the following hold:*

(a) *The group G has p-Sylow subgroups.*

(b) *The p-Sylow subgroups of G are conjugate to each other.*

Proof. (a) We first note that the set I of all subgroups of G of index coprime to p is a non-empty (since $G \in I$) poset with the inclusion relation. Now, by Lemma 2.2.8 we see that any chain of subgroups in I, i.e. any totally ordered (and thus directed) subset of I, say $\{H_j\}_{j\in J}$ satisfies that $\bigcap H_j \in I$, i.e. has a lower bound, so using Zorn's Lemma (see Theorem A.0.7) there must be a minimal element in I say P. The index $[G : P]$ is coprime to p, so proving that the set P is a pro-p group is enough to prove that P is a p-Sylow subgroup. Assume for a contradiction that P is not a pro-p group, then by Lemma 2.2.3 there exists some $N \trianglelefteq_o G$ such that $|P/N|$ is not a power of p. But, by the First Sylow Theorem

for Finite Groups (see Theorem A.0.5) there is a p-Sylow subgroup $Q/N < P/N$. Finally, Q is closed since it is the union of finitely many closed cosets of N by Lemma 1.1.4(b),(a), so we can use Lagrange's Theorem on the index of Q and see that $[G:Q] = [G:P]\,[P:Q]$, meaning that $[G:Q]$ is coprime to p, which contradicts the minimality of P, so P must be a pro-p group.

(b) We shall prove this by proving that every pro-p subgroup $T \leq G$ is a subgroup of a conjugate of a p-Sylow subgroup $P \leq G$, i.e. $T \leq gPg^{-1}$ for some element $g \in G$. First, take any $N \trianglelefteq_o G$, then $(N \cap P) \trianglelefteq_o P$ and $NP/N \cong P/(N \cap P)$ by the Second Isomorphism Theorem for groups (see Theorem A.0.4), so using Lagrange's Theorem $|P/(N \cap P)||N \cap P| = |P|$, meaning that $|NP/N| \mid |P|$, i.e. NP/N is a pro-p subgroup, and by the same argument NT/N is a pro-p subgroup too. Furthermore, from Remark 2.1.6 we see that $[G:NP] \mid [G:P]$ and by Lagrange's Theorem

$$[G:NP] = \frac{[G:N]}{[NP:N]} = \frac{|G/N|}{|NP/N|} = [G/N : NP/N]$$

so $[G/N : NP/N]$ is coprime to p, meaning that NP/N is a p-Sylow subgroup of G/N. Now, using the Second Sylow Theorem for Finite Groups (see Theorem A.0.6) (we know these groups are finite because the quotient group G/N is finite by Lemma 1.1.4(d)) we see that the following set is non-empty

$$R(N) := \bigcup \Big\{ gN \in \frac{G}{N} \mid (gN)^{-1} \frac{NT}{N}(gN) \leq \frac{NP}{N} \Big\} = \{ g \in G \mid g^{-1}NTg \leq NP \}$$

and it is closed since it is the union of closed cosets of N by Lemma 1.1.4(a). Moreover, for $M \leq N$, $R(M) \subseteq R(N)$ because given the natural surjective homomorphism $\phi : G/M \to G/N$ given by $\phi : gM \mapsto gN$ for any $g \in R(M)$ we have $(gM)^{-1}\frac{MT}{M}(gM) \leq \frac{MP}{M}$ and so

$$(gN)^{-1}\frac{NT}{N}(gN) = \phi\Big((gM)^{-1}\frac{MT}{M}(gM)\Big) \leq \phi\Big(\frac{MP}{M}\Big) = \frac{NP}{N},$$

meaning that $g \in R(N)$. As a result we have that $\{R(N)\}_{N \trianglelefteq_o G}$ has the finite intersection property because

$$R(N_i) \cap \cdots \cap R(N_k) \supseteq R(N_1 \cap \cdots \cap N_k) \neq \emptyset$$

which, by compactness of G implies that $\bigcap\limits_{N \trianglelefteq_o G} R(N) \neq \emptyset$, so there is an element $g \in G$ such that $g^{-1}NTg \leq NP$ for all $N \trianglelefteq_o G$. But then $g^{-1}Tg \leq g^{-1}NTg$, meaning that $g^{-1}Tg \leq \bigcap\limits_{N \trianglelefteq_o G} NP$ and using the same argument as in Lemma 1.2.6 proof (d)⇒(c) we see that $\bigcap\limits_{N \trianglelefteq_o G} NP = P$, so $g^{-1}Tg \leq P$ as required. □

2.3 Galois Theory on Profinite Groups

As we have seen throughout the previous section, the topology on the profinite groups is key to generalizing some of the most fundamental theorems on finite groups to profinite groups. As such, in this section we will study the topology of profinite groups this time looking at it from the perspective of Galois Theory. We will construct Galois groups of infinite extensions as inverse limits of finite Galois groups and we will reconstruct the Galois correspondence for these infinite extensions generalizing the Fundamental Theorem of Galois Theory to these profinite groups. Finally, we will show that, in fact, every profinite group can be expressed as a Galois group, thus making Galois groups and profinite groups one and the same.

We will start by first defining the field extensions on which the Galois correspondence can be drawn, i.e. Galois extensions, and the corresponding Galois groups.

Definition 2.3.1 (Galois Extension)**.** A Galois extension is a field extension F/K that is normal and separable (see Definitions A.0.13, A.0.15), i.e. the number of distinct roots of any irreducible polynomial $k \in K[t]$ in F is either 0 or exactly the degree of k.

Example 2.3.2. A very simple example of a Galois extension is the extension $\mathbb{Q}(i)/\mathbb{Q}$. This extension is normal since it is the splitting field of the polynomial $t^2+1 \in \mathbb{Q}[t]$ and it is separable since it is an extension of a field of characteristic 0 [1, Theorem 7.22].

Example 2.3.3. Another more interesting example of a Galois extension is the algebraic closure of any finite field $\mathbb{F}$ denoted $\mathbb{F}^{\text{alg}}/\mathbb{F}$, where the algebraic closure is the extension of all algebraic elements over $\mathbb{F}$. This extension is clearly normal since it is the splitting field of all the irreducible polynomials over $\mathbb{F}[t]$ and it is separable because it is an algebraic extension over a finite field [1, Theorem 7.25].

Example 2.3.4. An example of another infinite Galois extension is that of the compositum of all nth cyclotomic extensions over $\mathbb{Q}$, i.e. the extension $\mathbb{Q}(\zeta_1, \zeta_2, \ldots)$ of all nth primitive roots of unity ζ_n. This extension, that we will denote by $\mathbb{Q}(\Omega)$, is clearly a normal extension since it is the splitting field of all the polynomials $t^n - 1 \in \mathbb{Q}[t]$, and again it is separable because it is an extension of a field of characteristic 0.

Definition 2.3.5 (Galois Group)**.** The Galois group of a Galois extension F/K is the group of all automorphisms of F that fix K, i.e. K-automorphisms of F. It is usually denoted $\text{Gal}(F/K)$.

Example 2.3.6. The Galois extension given in Example 2.3.2 is a finite extension since it is a simple algebraic extension, and since it is a splitting field for the polynomial $t^2 + 1 \in \mathbb{Q}[t]$, by [1, Theorem 7.9], every element in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is such that it permutes the roots of $t^2 + 1$. Clearly there are only two possible permutations $i \mapsto i$ and $i \mapsto -i$, and the elements of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ are fully characterized by these two permutations —meaning that these are the only two elements in the group—, so $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$.

As previously mentioned, establishing a correspondence between subgroups of a Galois group and intermediate field extensions of the Galois extension necessitates introducing a topological structure on the Galois group when dealing with infinite extensions. The name of the specific topology required is the Krull topology.

Definition 2.3.7 (Krull Topology)**.** The Krull topology on the Galois group of a Galois extension F/K is the topology on which

$$\mathcal{F} := \{\mathrm{Gal}(F/L) \mid L/K \text{ is a finite Galois extension}\}$$

forms a base of open neighbourhoods of $e \in \mathrm{Gal}(F/K)$.

Remark 2.3.8. Notice that the definition above indeed describes a topology on $\mathrm{Gal}(F/K)$ compatible with its group structure. Since the maps B and i from Definition 1.1.1 are continuous, which we know because the inverse images of the open sets in $\mathcal{F}$, $B^{-1}(\mathrm{Gal}(F/L)) = \mathrm{Gal}(F/L) \times \mathrm{Gal}(F/L)$ and $i^{-1}(\mathrm{Gal}(F/L)) = \mathrm{Gal}(F/L)$ (where L/K is a finite Galois extension), are clearly open sets in their respective topologies, the Krull topology is indeed compatible. Furthermore, any base of neighbourhoods around the identity fully defines a topology on a group since the left and right translation maps ($x \mapsto gx$ and $x \mapsto xg$ respectively) are topological isomorphisms, meaning that a base of neighbourhoods of e automatically describes a base of neighbourhoods of g for any element g in the group, i.e. a basis for a compatible topology is fully characterized by any base of neighbourhoods of e.

Remark 2.3.9. It is also noteworthy to point out that the Krull topology on a finite Galois group, $\mathrm{Gal}(F/K)$, is just the discrete topology. This is true because we have that $\{e\} = \mathrm{Gal}(F/F) \leq_o \mathrm{Gal}(F/K) \iff F/K$ is a finite Galois extension, and by finite Galois theory F/K is a finite Galois extension when $\mathrm{Gal}(F/K)$ is a finite Galois group.

As it turns out, Galois groups with the Krull topology can be expressed as inverse limits of inverse systems of finite Galois groups with the discrete topology, meaning that this newly defined topology is the same as the subspace topology of the inverse limit with respect to the product topology of the finite Galois groups composing the inverse system.

Lemma 2.3.10. *[5, Lemma 3.1.1] Every Galois group* $\mathrm{Gal}(F/K)$ *with the Krull topology is isomorphic to a profinite group.*

Proof. Letting $I := \{L_i \mid L_i/K \text{ is a finite Galois extension and } L_i \subseteq F\}$ with the binary relation $i \leq j \iff L_i \subseteq L_j$ we see that this forms a directed poset on the finite groups $\{\mathrm{Gal}(L_i/K)\}_{i\in I}$. Furthermore, we can construct the following continuous surjective homomorphisms $\phi_{ij} : \mathrm{Gal}(L_i/K) \to \mathrm{Gal}(L_j/K)$ by $\phi_{ij} : \sigma \mapsto \sigma|_{L_j}$ whenever $i \geq j$ (surjectivity comes from the fact that isomorphisms of fields can be extended to isomorphisms of extensions when the said extensions are finite splitting fields, see [1, Theorem 5.3]), so we have a surjective inverse system of finite groups given by $\{\mathrm{Gal}(L_i/K), \phi_{ij}, I\}$ (it is important to note that by Proposition 1.1.22, the projections of the inverse limit of this inverse system are also surjective). We now claim that the inverse limit of the said inverse system is isomorphic as a topological group to $\mathrm{Gal}(F/K)$ under the Krull topology. The maps $\psi_i : \mathrm{Gal}(F/K) \to \mathrm{Gal}(L_i/K)$ by $\psi_i : \sigma \mapsto \sigma|_{L_i}$ form a family of compatible mappings (continuity comes from the fact that the base of open neighbourhoods of $e \in \mathrm{Gal}(L_i/K)$ under the discrete topology is just $\{e\}$, and

$$\psi_i^{-1}(\{e\}) = \{\sigma \in \mathrm{Gal}(F/K) \mid \sigma|_{L_i} \in \{e\} \subseteq \mathrm{Gal}(L_i/K)\} = \mathrm{Gal}(F/L_i),$$

which is clearly an element in the base of neighbourhoods of $e \in \mathrm{Gal}(F/K)$ under the Krull topology), therefore by the universal property of the inverse limit there is a continuous homomorphism $\theta : \mathrm{Gal}(F/K) \to \varprojlim \mathrm{Gal}(L_i/K)$ given by $\theta : \sigma \mapsto (\psi_i(\sigma))$. Finally, given $\theta^{-1} : \varprojlim \mathrm{Gal}(L_i/K) \to \mathrm{Gal}(F/K)$ by $\theta^{-1} : (\sigma_i) \mapsto \alpha$ where $\alpha(x) = \sigma_i(x)$ whenever $x \in L_i \in I$, the map θ^{-1} is clearly an inverse map to θ and it is also continuous since given an element of the base of open neighbourhoods of $e \in \mathrm{Gal}(F/K)$ described in Definition 2.3.7, say $H = \mathrm{Gal}(F/L)$, then we have that

$$\theta(H) = \{(\sigma|_{L_i}) \in \varprojlim \mathrm{Gal}(L_i/K) \mid \sigma_L = \mathrm{Id}_L\} = \pi_L^{-1}(\{e_{\mathrm{Gal}(L/K)}\})$$

where $e_{\mathrm{Gal}(L/K)}$ is the identity in $\mathrm{Gal}(L/K)$ and π_L is the projection of the inverse limit to $\mathrm{Gal}(L/K)$, i.e. $\theta(H)$ is open in $\varprojlim \mathrm{Gal}(L_i/K)$ since the projection π_L is continuous, meaning that θ is a topological isomorphism. □

Corollary 2.3.11. *Infinite countable subgroups of a Galois group are never closed.*

Proof. This follows from the above lemma together with Corollary 1.2.8 and Proposition 1.2.9. □

With Lemma 2.3.10 we are now ready to construct some explicit examples of infinite Galois groups. As demonstrated in the proof of the lemma, if we can explicitly describe the Galois groups of every finite intermediate Galois extension

—or a cofinal subset of these with respect to inclusion— of an infinite Galois extension then we can describe the infinite Galois group as an inverse limit of these finite groups.

Example 2.3.12. In the case of Example 2.3.3, the Galois group $\mathrm{Gal}(\mathbb{F}^{\mathrm{alg}}/\mathbb{F})$ turns out to be isomorphic to the profinite completion of the integers $\hat{\mathbb{Z}}$ given in Example 1.2.4. This can be easily seen by first understanding what the finite intermediate Galois extensions are. It can be proven, as given in [1, Theorem 6.2], that every finite field is of prime power order and that finite fields of same order are isomorphic to each other. As a result, without loss of generality, we may assume that $\mathbb{F} = \mathbb{F}_{p^n}$ where $\mathbb{F}_{p^n}$ is a finite field of order p^n. Then, for any finite field extension $F/\mathbb{F}_{p^n}$ with $[F : \mathbb{F}_{p^n}] = k$, we have $F \cong (\mathbb{F}_{p^n})^k \cong \mathbb{F}_{p^{nk}}$. Moreover, we know that for any m such that $n \mid m$, the extension $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is normal since by [1, Theorem 6.2] $\mathbb{F}_{p^m}$ is a splitting field for the polynomial $t^{p^m} - t \in \mathbb{F}_p[t]$. Finally, as shown in [1, Theorem 6.3], the group $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ is cyclic, so using finite Galois theory we see that $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) \cong C_{m/n} \cong \mathbb{Z}_{m/n}$ and so, using Lemma 1.1.21 and following the construction of the Galois group given in the proof of Lemma 2.3.10 we get the following description of the infinite Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}^{\mathrm{alg}}/\mathbb{F}_{p^n}) \cong \varprojlim \mathbb{Z}_n = \hat{\mathbb{Z}}$.

One final result is needed for the proof of the Fundamental Theorem. This result helps us prove the surjectivity of the natural map between the Galois group of an extension and the Galois group of an intermediate extension when the extensions are possibly infinite.

Lemma 2.3.13. *[Author's work] Given a Galois extension F/K and an intermediate Galois extension M/K, for any element $\sigma \in \mathrm{Gal}(M/K)$ there is some element $\tau \in \mathrm{Gal}(F/K)$ such that $\tau|_M = \sigma$.*

Proof. Using the isomorphism from Lemma 2.3.10 the result is proved if we can find some element $(\tau_i) \in \varprojlim \mathrm{Gal}(L_i/K)$ such that $\tau_i = \sigma|_{L_i}$ whenever $L_i \subseteq M$ (every element in M is in some finite Galois extension $L_i \subseteq M$). Clearly, any element in the set $\bigcap_{\substack{L_i \subseteq M \\ L_i \in \mathcal{F}}} \pi_i^{-1}(\{\sigma|_{L_i}\})$ (where $\mathcal{F}$ is the set of finite intermediate Galois extensions of F/K, and π_n are the projections from $\varprojlim \mathrm{Gal}(L_i/K)$ to $\mathrm{Gal}(L_n/K)$) satisfies this condition, thus showing that this set is non-empty is enough to prove the result. Indeed this set is non-empty since it is an intersection of closed sets with the finite intersection property in a compact space. The sets $\pi_i^{-1}(\{\sigma|_{L_i}\})$ are closed by the continuity of the projections. The finite intersection property comes from the fact that any finite intersection $\bigcap_{L_i \in \{L_i\}_1^n} \pi_i^{-1}(\{\sigma|_{L_i}\})$ contains the set $\pi_{(L_i)_1^n}^{-1}(\{\sigma|_{(L_i)_1^n}\})$ where $(L_i)_1^n$ is the compositum of the extensions $\{L_i\}_1^n$ and

$\pi_{(L_i)_1^n}$ is the projection to $\mathrm{Gal}((L_i)_1^n/K)$, which is clearly non-empty by the surjectivity of $\pi_{(L_i)_1^n}$ (this containment holds because $\pi_i^{-1}(\{\sigma|_{L_i}\}) \subseteq \pi_j^{-1}(\{\sigma|_{L_j}\})$ whenever $L_i \supseteq L_j$). Finally, compactness comes from Lemma 1.2.6. □

At last, we have reached the point where we can prove the Fundamental Theorem of Galois Theory for profinite groups. However, this generalization of the finite theorem comes with an important caveat. Specifically, the correspondence between subgroups of the Galois group and the intermediate fields of the Galois extension is not a bijective correspondence with all subgroups, but rather only with those that are closed. This naturally makes sense, since, as we saw in Corollary 1.2.8, the correspondence is with the subgroups that can also be expressed as inverse limits of inverse systems of finite Galois groups.

Theorem 2.3.14 (FTGT for Infinite Extensions)**.** *[4, Theorem 2.11.3][5, Theorem 3.2.1] Given a Galois extension F/K the map $\Phi : \mathtt{F} \to \mathbb{G}$ given by $\Phi : M \mapsto \mathrm{Gal}(F/M)$ where*

$$\mathtt{F} := \{M \subseteq F \mid M \text{ is an intermediate field extension}\}\ ;\ \mathbb{G} := \{H \leq_c \mathrm{Gal}(F/K)\}$$

is an inclusion reversing bijection.

Proof. First we note that this map is indeed well defined since for any $M \in \mathtt{F}$, the group $\mathrm{Gal}(F/M)$ is a profinite group by Lemma 2.3.10 and so, using Corollary 1.2.8, we see that this is indeed a closed subgroup of $G = \mathrm{Gal}(F/K)$.

In order to show Φ is a bijection we will show that $\Psi : \mathbb{G} \to \mathtt{F}$ given by $\Psi : H \mapsto F^H$ where $F^H := \{x \in F \mid \sigma(x) = x,\ \forall \sigma \in H\}$ (F^H is called the fixed field of H) is an inverse to Φ.

We claim that $\Psi\Phi(M) = F^{\mathrm{Gal}(F/M)} = M$. Clearly $F^{\mathrm{Gal}(F/M)} \supseteq M$ by definition of $F^{\mathrm{Gal}(F/M)}$. Now, $\forall x \in F^{\mathrm{Gal}(F/M)}$ we claim that the minimal polynomial m of x over M is of degree 1, i.e. $x \in M$. If $\partial m > 1$ then $\exists y \in F \setminus M$ such that $y \neq x$ and $m(y) = 0$, but then $M(x) \cong M(y)$ (using [1, Corollary 3.24] an isomorphism of fields that fixes M and sends $x \mapsto y$ can be constructed). Then, given the splitting field of m say S_m we have that the isomorphism $M(x) \cong M(y)$ can be extended to an M-automorphism of S_m say $\sigma \in \mathrm{Gal}(S_m/M)$ (using [1, Theorem 5.3]), that sends $x \mapsto y$. Then, using Lemma 2.3.13 we see that σ can be extended to an element of $\mathrm{Gal}(F/M)$, say τ, such that $\tau(x) = y$, meaning that $x \notin F^{\mathrm{Gal}(F/M)}$, which is a contradiction.

Next, we claim that $\Phi\Psi(H) = \mathrm{Gal}(F/F^H) = H$. Clearly, we have that $\mathrm{Gal}(F/F^H) \geq H$ by the definition of F^H. To prove $\mathrm{Gal}(F/F^H) = H$ we will show that H is dense in $\mathrm{Gal}(F/F^H)$, i.e. for any $\tau \in \mathrm{Gal}(F/F^H)$ any element

in the base of open neighbourhood of τ, say $\tau\mathrm{Gal}(F/L)$ where L/F^H is a finite Galois extension, is such that $\tau\mathrm{Gal}(F/L) \cap H \neq \emptyset$. Since $\forall\sigma \in H$ we have $\sigma(L) = L$ (given any normal extension L/F^H and any $\tau \in \mathrm{Gal}(F/F^H)$ for any $x \in L$ with minimal polynomial $m \in F^H[t]$ we have that $m(\tau(x)) = \tau(m(x)) = 0$, i.e. $\tau(x)$ is a root of m, so $\tau(x) \in L$, i.e. $\tau(L) \subseteq L$, and since τ is a bijection $\tau(L) = L$), this clearly implies that $S = \{\sigma|_L \mid \sigma \in H\} \leq \mathrm{Gal}(L/F^H)$. We claim that $S = \mathrm{Gal}(L/F^H)$, which —by finite Galois theory— we know is true if and only if $L^S = F^H$. Since $S \leq \mathrm{Gal}(L/F^H)$ we obviously have $F^H \subseteq L^S \subseteq L$ and for every $x \in L^S = \{x \in L \mid \sigma|_L(x) = x,\ \forall\sigma \in H\}$ we have $x \in L \subseteq F$ and $\sigma(x) = x\ \forall\sigma \in H$, thus $x \in F^H$, meaning that $L^S \subseteq F^H$. As a result $\tau|_L \in \mathrm{Gal}(L/F^H) = S = \{\sigma|_L \mid \sigma \in H\}$, meaning that there is $\sigma \in H$ such that $\sigma|_L = \tau|_L$, i.e. $\tau^{-1}\sigma \in \mathrm{Gal}(F/L)$, so $\sigma \in \tau\mathrm{Gal}(F/L) \cap H$, hence $\mathrm{Gal}(F/F^H) = \overline{H} = H$. □

Corollary 2.3.15. *A closed subgroup H of a Galois group $\mathrm{Gal}(F/K)$ is of the form $H = \mathrm{Gal}(F/F^H)$.*

Proof. By the above theorem since $H = \Phi\Phi^{-1}(H) = \mathrm{Gal}(F/F^H)$. □

Proposition 2.3.16. *[3, Proposition 7.12] For any subgroup of a Galois group $H \leq \mathrm{Gal}(F/K)$ we have that $\overline{H} = \mathrm{Gal}(F/F^H)$.*

Proof. First we notice that $H \leq \mathrm{Gal}(F/F^H)$ by the definition of the fixed field and $\mathrm{Gal}(F/F^H)$ is closed since it is isomorphic to a profinite group by Lemma 2.3.10, meaning it is closed by Corollary 1.2.8. As a result $\overline{H} \subseteq \mathrm{Gal}(F/F^H)$. Now, since the set $\overline{H}$ is a closed subgroup by Lemma 1.1.4(g) and by Corollary 2.3.15 we know that $\overline{H} = \mathrm{Gal}(F/F^{\overline{H}})$ and since $F^H \supseteq F^{\overline{H}}$ we have $\mathrm{Gal}(F/F^H) \leq \mathrm{Gal}(F/F^{\overline{H}})$, and so $\overline{H} \leq \mathrm{Gal}(F/F^H) \leq \overline{H}$, meaning that $\overline{H} = \mathrm{Gal}(F/F^H)$. □

Lemma 2.3.17 (FTGT for Normal Extensions)**.** *[4, Theorem 2.11.3][5, Proposition 3.2.2] Given an intermediate field extension M of F/K, the extension M/K is normal if and only if $\Phi(M) \trianglelefteq \mathrm{Gal}(F/K)$. Furthermore, if $\Phi(M) \trianglelefteq \mathrm{Gal}(F/K)$ then $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(F/K)/\Phi(M)$.*

Proof. To prove this we will first show that M/K is normal iff $\tau(M) = M$ for all $\tau \in \mathrm{Gal}(F/K)$. Given any $\tau \in \mathrm{Gal}(F/K)$ and any $x \in M$ with minimal polynomial $m \in K[t]$ we have that $m(\tau(x)) = \tau(m(x)) = 0$, i.e. τ permutes the roots of m, so if the extension M/K is normal then $\tau(x)$ is a root of m, so $\tau(x) \in M$, i.e. $\tau(M) \subseteq M$, and since τ is a bijection $\tau(M) = M$. On the other hand, if for any $\tau \in \mathrm{Gal}(F/K)$ we have that $\tau(M) = M$ then for any $x \in M$ with minimal polynomial $m \in K[t]$ such that $\partial m > 1$, given any other root y of m such that $y \neq x$ we can construct an element of $\mathrm{Gal}(F/K)$ (following the same procedure as in paragraph 3 in the proof of Theorem 2.3.14), say σ, that satisfies

that $\sigma(x) = y$, but then, from the assumption $\sigma(M) = M$, so $y \in M$, meaning that M/K is normal.

Now, clearly, if M/K is a normal extension then for any $\tau \in \mathrm{Gal}(F/K)$ we have that $\tau(M) = M$, so given $\sigma \in \Phi(M) = \mathrm{Gal}(F/M)$ we have that $\tau^{-1}\sigma\tau \in \Phi(M)$, i.e. the subgroup $\Phi(M)$ is normal. Moreover, if $\Phi(M) \trianglelefteq \mathrm{Gal}(F/K)$ then for any $\tau \in \mathrm{Gal}(F/K)$ we have that $\tau^{-1}\sigma\tau \in \mathrm{Gal}(F/M)$ $\forall \sigma \in \mathrm{Gal}(F/M)$. So, if for some $x \in M$ we have $\tau(x) \notin M$ then $\exists \alpha \in \Phi(M)$ such that $\alpha(\tau(x)) \neq \tau(x)$ (otherwise $\tau(x) \in F^{\Phi(M)}$, $\tau(x) \notin M$, which contradicts $M = \Phi^{-1}\Phi(M) = F^{\Phi(M)}$), meaning that $\tau^{-1}\alpha\tau(x) \neq x$, i.e. $\tau^{-1}\alpha\tau|_M \neq \mathrm{Id}_M$, which contradicts the fact that the element $\tau^{-1}\alpha\tau \in \mathrm{Gal}(F/M)$, so $\tau(x) \in M$, i.e. $\tau(M) = M$. Therefore, M/K must be a normal extension.

Finally, if $\Phi(M) \trianglelefteq \mathrm{Gal}(F/K)$ then by the above $\tau(M) = M$ $\forall \tau \in \mathrm{Gal}(F/K)$, so the map $\lambda : \mathrm{Gal}(F/K) \to \mathrm{Gal}(M/K)$ by $\lambda : \sigma \mapsto \sigma|_M$ is a well-defined surjective homomorphism, and $\ker(\lambda) = \mathrm{Gal}(F/M) = \Phi(M)$, so using the First Isomorphism Theorem (see Theorem A.0.3) we get that $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(F/K)/\Phi(M)$. □

As we mentioned at the beginning of this section, every profinite group can in fact be expressed as the Galois group of some extension. The following proof will show a way of constructing such a Galois extension, but, as we will see, this construction does not allow us to freely choose the base field of the extension. It turns out that expressing finite groups as Galois groups of an extension of a given base field is an ongoing problem mathematicians have been working on for centuries. The so called Inverse Galois Problem, devised in the 19th century, that asks whether every finite group can be expressed as a Galois group of a Galois extension over the base field $\mathbb{Q}$ is an open question yet to be answered.

Lemma 2.3.18. *[5, Theorem 3.3.2][4, Theorem 2.11.5] Every profinite group is a Galois group.*

Proof. To prove this we will show that for any profinite group G we can construct a Galois field extension such that the Galois group of the said field extension is precisely G. In order to do this we will first start by taking an arbitrary field K and denote by $F := K(T)$ the compositum of the field extensions of K with the transcendentals in T, where $T = \bigcup_{N \trianglelefteq_o G} G/N$. Now, G acts on T in a natural way $G \times T \to T$ by $(g, hN) \mapsto ghN$. This action permutes the elements of T, so G can be seen as a set of K-automorphisms on F, and in fact this set of automorphisms is a subgroup of $\mathrm{Aut}_K(F)$. Finally, we claim that F/F^G is a Galois extension and that $\mathrm{Gal}(F/F^G) = G$.

To prove that F/F^G is a Galois extension we take an arbitrary element $f \in F$. Now, letting $G_f := \{g \in G \mid g(f) = f\}$, i.e. the stabilizer of f, then, since the element f can be expressed as an element in the K-vector space $F = K(T)$, it can be expressed as a finite linear combination of elements in T, say $\{t_i\}_1^n$, where $t_i \in G/N_i$ for all $i \in I = \{1, \ldots, n\}$, given any $g \in \bigcap_1^n N_i$ we have that $g(t_i) = t_i$ for all elements $i \in I$, so $g(f) = f$, i.e. $g \in G_f$, meaning that $\bigcap_1^n N_i \subseteq G_f$ and $\bigcap_1^n N_i$ is open since it is a finite intersection of open sets, so by Lemma 1.1.4(e) we have that $G_f \leq_o G$. Now, since G_f is open, by Lemma 1.1.4(d) we gather that $[G : G_f] < \infty$, so the orbit of f, $Gf := \{g(f) \in F \mid g \in G\}$, is finite by the Orbit-Stabilizer Theorem (see Theorem A.0.8). Finally, we will prove that f is algebraic over F^G and that it is separable and then we will show that F/F^G is normal. Since $|Gf| < \infty$ we may assume, without loss of generality, that $Gf = \{f_i\}_1^r$ for some $f_i \in F$ where $f_1 = f$, and we may construct the polynomial

$$p(x) = \prod_1^r (x - f_i) = u_r x^r + \cdots + u_1 x + u_0$$

where $\{u_i\}_1^r$ lie in a splitting field of p. Then p is such that for any $g \in G$ we have

$$\begin{aligned} g(p(x)) =& g(\prod_1^r (x - f_i)) = \prod_1^r g(x - f_i) \\ =& \prod_1^r (g(x) - g(f_i)) = \prod_1^r (g(x) - f_i) = p(g(x)), \end{aligned}$$

so the coefficients of p must be in F^G (otherwise if $u_i \notin F^G$ for some $i \in \{0, \ldots, r\}$ then $\exists g \in G$ such that $g(u_i) \neq u_i$, so $g(p(x)) \neq p(g(x))$), i.e. $p(x) \in F^G[x]$, so f is algebraic over F^G. Now, since p has non-repeated roots, the minimal polynomial of f is separable over F^G, i.e. F/F^G is separable. Moreover, the extension $F^G(\{f_i\}_1^r)/F^G$ is a normal extension (this is because it is a splitting field of p over F^G) and clearly F is the compositum of all such extensions $\forall f \in F$, so F is the compositum of normal extensions over F^G, meaning that it is a normal extension over F^G (the compositum of splitting fields of polynomials is a splitting field for the union of the polynomials). As a result F/F^G is a normal and separable extension and therefore a Galois extension.

Now, to prove that $\mathrm{Gal}(F/F^G) = G$ we notice that if $G \leq_c \mathrm{Gal}(F/F^G)$ then, by the FTGT for Infinite Extensions, $G = \Phi\Phi^{-1}(G) = \mathrm{Gal}(F/F^G)$, so all we need to prove is that G is closed in $\mathrm{Gal}(F/F^G)$. First we claim that the inclusion mapping $\alpha : G \to \mathrm{Gal}(F/F^G)$ is continuous. We will prove this by showing that the inverse image of any element in the base of open neighbourhoods of $e \in \mathrm{Gal}(F/F^G)$ is open in G. Any element in the base of open neighbourhoods of

e in the Krull topology is of the form $\mathrm{Gal}(F/M)$ where M/F^G is a finite Galois extension. Since M/F^G is normal and finite, it is a splitting field for a polynomial with roots $\{a_i\}_1^s \subseteq F$, so we may write M as $M = F^G(\{a_i\}_1^s)$. Then, for any $g \in \bigcap_1^s G_{a_i}$, $g(M) = \mathrm{Id}_M$, i.e. $g \in \Phi(M) = \mathrm{Gal}(F/M)$ and $g \in G$, so $g \in G \cap \mathrm{Gal}(F/M)$, hence $\bigcap_1^s G_{a_i} \subseteq G \cap \mathrm{Gal}(F/M)$ and since $\bigcap_1^s G_{a_i}$ is a finite intersection of open sets in G, by Lemma 1.1.4(e) we have that the set $G \cap \mathrm{Gal}(F/M)$ is open in G, proving that α is continuous. Now that we have that α is continuous it is straightforward to see that, since G is compact $\alpha(G)$ is compact and so it is a compact subset in a Hausdorff space $\mathrm{Gal}(F/F^G)$ (where $\mathrm{Gal}(F/F^G)$ is Hausdorff because it is a profinite group by Lemma 2.3.10 and profinite groups are Hausdorff by Lemma 1.1.16(a)), so $\alpha(G) = G$ is closed in $\mathrm{Gal}(F/F^G)$. □

3 Examples of Infinite Galois Groups over $\mathbb{Q}$

In this section we will explore two examples of Galois groups of infinite Galois extensions over the base field $\mathbb{Q}$ and an example that illustrates the existence of subgroups of infinite Galois groups that are closed but not open under the Krull topology. In order to construct these examples the following lemma by the author will be utilized.

Lemma 3.0.1. *[Author's work] Given a Galois extension $K_{\mathcal{F}}/K$ where $K_{\mathcal{F}}$ is a splitting field for a countable family of polynomials $\mathcal{F} = \{p_i\}_{i\in\mathbb{N}}$ in $K[t]$ we have that*

$$\mathrm{Gal}(K_{\mathcal{F}}/K) \cong \varprojlim \mathrm{Gal}(K_n/K)$$

where K_n is a splitting field for the polynomials $\{p_i\}_1^n$ over K.

Proof. From Lemma 2.3.10 we know that $\mathrm{Gal}(K_{\mathcal{F}}/K) \cong \varprojlim \mathrm{Gal}(M/K)$ where M/K are intermediate finite Galois extensions. We claim that the subcollection of extensions $\{K_n\}_{n\in\mathbb{N}}$ forms a cofinal subsystem of the inverse system of intermediate finite Galois extensions. To prove this all we need to show is that for any M in the inverse system there is some $n \in \mathbb{N}$ such that $M \subseteq K_n$. Since the extension M/K is a finite Galois extension it can be expressed as $M = K(a_1, \ldots, a_r)$ for some $a_i \in K_{\mathcal{F}}$. Now, since $K_{\mathcal{F}} = K(R_{\mathcal{F}})$ where $R_{\mathcal{F}}$ is the set of roots of the polynomials in $\mathcal{F}$ and $K(R_{\mathcal{F}})$ can be seen as a vector space over the field K with a basis $\{e_l\}_{l\in L} \subseteq R_{\mathcal{F}}$ where L is just an indexing set, we may express the elements a_i in terms of finitely many basis elements. As a result we see that $M \subseteq K(\{e_l\}_{l\in L_M})$ for some finite subset $L_M \subseteq L$. Finally, M is now clearly seen to be contained in a splitting field of some finite subfamily of $\mathcal{F}$, which in turn must be contained in some K_n for large enough n, so $\{K_n\}_{n\in\mathbb{N}}$ does indeed form a cofinal subsystem, which by Lemma 1.1.21 proves that $\mathrm{Gal}(K_{\mathcal{F}}/K) \cong \varprojlim \mathrm{Gal}(K_n/K)$. □

The following propositions will also help us construct our first example. Note that the isomorphism in the first proposition is just a group isomorphism, not necessarily a topological isomorphism.

Proposition 3.0.2. *[5, Exercise 3.4 1a)] Given a Galois extension N/K and another extension M/K (not necessarily Galois) the extension NM/M, where NM is the compositum of both extensions, is a Galois extension. Furthermore, there is a group isomorphism* $\mathrm{Gal}(NM/M) \cong \mathrm{Gal}(N/(N \cap M))$.

Proof. As we saw in the proof of Lemma 2.3.17, any intermediate extension L/T of the Galois extension T^{alg}/T is normal iff $\sigma(L) = L$ for all $\sigma \in \mathrm{Gal}(T^{\mathrm{alg}}/T)$. Now, since for any $\alpha \in \mathrm{Gal}(M^{\mathrm{alg}}/M)$ we have $\alpha(NM) = \alpha(N)\alpha(M)$ and the extension N/K being normal implies that $\alpha \in \mathrm{Gal}(M^{\mathrm{alg}}/M) \subseteq \mathrm{Gal}(K^{\mathrm{alg}}/K)$ (here the containment is satisfied by Lemma B.0.3) is such that $\alpha(N) = N$,

so $\alpha(NM) = \alpha(N)\alpha(M) = N\mathrm{Id}_M(M) = NM$, meaning that the extension NM/M is normal. To prove separability we see that, since the extension N/K is separable, meaning that every element of N is separable over the field K, which implies that every element of N is separable over M since $M \supseteq K$, and $MN = M(N)$, for any $S \subseteq N$ such that $|S| < \infty$ the elements of S are separable over M, so every finite intermediate extension of MN/M is separable, meaning that the extension $M(N)/M$ is separable.

Finally, to prove the existence of the isomorphism we notice that the map $\alpha : \mathrm{Gal}(NM/M) \to \mathrm{Gal}(N/N \cap M)$ given by the restriction $\alpha : \sigma \mapsto \sigma|_N$ is a clear homomorphism of groups. Moreover, the map $\beta : \mathrm{Gal}(N/N\cap M) \to \mathrm{Gal}(NM/M)$ given by $\beta : \sigma \mapsto \phi$ where for any $x \in NM$ (x can be expressed in terms of a basis $\{n_i\}_{i\in I} \subseteq N$ of the vector space $M(N)$ over the field M as a finite sum $x = \sum m_i n_i$) the automorphism ϕ is given by $\phi(x) = \sum m_i \sigma(n_i)$, is a clear inverse to α, meaning that it is a bijective homomorphism, and so a group isomorphism. □

Proposition 3.0.3. *[5, Exercise 3.4 1b)] Given two Galois extensions N/K and M/K the extension $NM/(N \cap M)$, where NM is the compositum of both extensions, is a Galois extension. Furthermore, there is a group and topological isomorphism* $\mathrm{Gal}(NM/(N \cap M)) \cong \mathrm{Gal}(N/(N \cap M)) \times \mathrm{Gal}(M/(N \cap M))$.

Proof. As we saw in the proof of Lemma 2.3.17, any intermediate extension L/T of the Galois extension T^{alg}/T is normal iff $\sigma(L) = L$ for all $\sigma \in \mathrm{Gal}(T^{\mathrm{alg}}/T)$. Now, since for any $\alpha \in \mathrm{Gal}(K^{\mathrm{alg}}/K)$ we have $\alpha(NM) = \alpha(N)\alpha(M)$ and N/K, M/K being normal implies that $\alpha(N) = N$, and $\alpha(M) = M$, we gather that $\alpha(NM) = \alpha(N)\alpha(M) = NM$, meaning that NM/K is normal, which implies that $NM/(N\cap M)$ is normal. To prove separability we see that, since $N = K(N)$ and $M = K(M)$, we may express NM as $NM = K(N, M) = K(N \cup M)$. Furthermore, since N/K and M/K are separable over K, we have that for any subset $S \subseteq N \cup M$ such that $|S| < \infty$, the elements of S are separable over K, meaning that the extension NM/K is separable, which implies that $NM/(N \cap M)$ is separable.

Now, to show the existence of the isomorphism we see that the following map $\alpha : \mathrm{Gal}(NM/(N\cap M)) \to \mathrm{Gal}(N/(N\cap M)) \times \mathrm{Gal}(M/(N\cap M))$ given by the restrictions $\alpha : \sigma \mapsto (\sigma|_N, \sigma|_M)$ is a clear homomorphism. Moreover, we can construct a map $\beta : \mathrm{Gal}(N/(N \cap M)) \times \mathrm{Gal}(M/(N \cap M)) \to \mathrm{Gal}(NM/(N \cap M))$ given by $\beta : (\sigma, \tau) \mapsto \phi$ where for any $x \in NM = M(N)$ (x can be expressed in terms of a basis $\{n_i\}_{i\in I} \subseteq N$ of the vector space $M(N)$ over the field M as a finite sum $x = \sum m_i n_i$) $\phi(x) = \sum \sigma(m_i)\tau(n_i)$. The map β is a clear inverse to α, meaning that α is a bijective homomorphism, i.e. a group isomorphism.

The map α maps open sets to open sets. The openness of this map comes from the fact that given any element in the base of open neighbourhoods of $e \in \mathrm{Gal}(NM/(N \cap M))$, say $\mathrm{Gal}(NM/L)$ where $L/(N \cap M)$ is a finite Galois extension, we have that

$$\begin{aligned}\alpha(\mathrm{Gal}(NM/L)) =& \{(g|_N, g|_M) \mid g \in \mathrm{Gal}(NM/L)\} \\ =& \mathrm{Gal}(N/L) \times \mathrm{Gal}(M/L)\end{aligned}$$

(clearly $\{(g|_N, g|_M) \mid g \in \mathrm{Gal}(NM/L)\} \subseteq \mathrm{Gal}(N/L) \times \mathrm{Gal}(M/L)$, and, for any $(\sigma, \tau) \in \mathrm{Gal}(N/L) \times \mathrm{Gal}(M/L)$, the element $g \in \mathrm{Gal}(NM/L)$ given by $g(x) = \sum \sigma(m_i)\tau(n_i)$, where $x = \sum m_i n_i$ is the representation of the element $x \in NM$ in terms of a basis of the vector space NM, is such that $g|_N = \sigma$ and $g|_M = \tau$, so $\{(g|_N, g|_M) \mid g \in \mathrm{Gal}(NM/L)\} \supseteq \mathrm{Gal}(N/L) \times \mathrm{Gal}(M/L)$), and so elements in the base of open neighbourhoods of $e \in \mathrm{Gal}(NM/(N \cap M))$ are mapped to the product of elements in the open neighbourhoods of $e \in \mathrm{Gal}(N/(N \cap M))$ and $e \in \mathrm{Gal}(M/(N \cap M))$.

Finally, since α is an open map, β is continuous and $\mathrm{Gal}(NM/(N \cap M))$ is compact and Hausdorff by Lemma 2.3.10 and Lemma 1.2.6, and by the same reasoning $\mathrm{Gal}(N/(N \cap M)) \times \mathrm{Gal}(M/(N \cap M))$ is also compact and Hausdorff since it is a product of compact Hausdorff spaces, we have that β is a closed map (closed subsets in a compact space are compact and continuous maps map compact subsets to compact subsets, and compact subsets in a Hausdorff space are closed), i.e. α is continuous bijective map between compact Hausdorff spaces, so it is closed, and so β is a bijective homeomorphism, in other words a topological isomorphism. □

The following example is one that is normally found in the literature, but that is usually proved using the much more powerful Kronecker-Weber Theorem. This theorem asserts that every finite Galois extension of the rational numbers with abelian Galois group is a subfield of a cyclotomic extension. Unfortunately, the proof of this theorem falls outside the scope of what is contained in this thesis. We will instead use the lemma given at the beginning of this section, to keep this thesis as self-contained as possible.

Example 3.0.4. We will now find a more explicit representation of the Galois group of the extension given in Example 2.3.4. This Galois group can be shown to be $\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$. In order to show this we will make use of Lemma 3.0.1 and some results on cyclotomic extensions. We start by noticing that for any $n \in \mathbb{N}$ we have $\mathbb{Q}(\{\zeta_i\}_1^n) = \mathbb{Q}(\zeta_{\mathrm{lcm}\{1,\ldots,n\}})$ by Lemma B.0.4. Now, using Lemma 3.0.1, we see that

$$\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\{\zeta_i\}_1^n)/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathrm{lcm}\{1,\ldots,n\}})/\mathbb{Q}).$$

But $\{\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathrm{lcm}\{1,\dots,n\}})/\mathbb{Q})\}_{n\in\mathbb{N}}$ is clearly just a cofinal subsystem of the inverse system given by the family of topological groups $\{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\}_{n\in\mathbb{N}}$, so, using Lemma 1.1.21, we have

$$\varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathrm{lcm}\{1,\dots,n\}})/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Finally, by Lemma B.0.2 we know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$, meaning that $\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}) \cong \varprojlim \mathbb{Z}_n^\times = \hat{\mathbb{Z}}^\times$.

It is important, and not so trivial, to point out that not every subgroup of a Galois group is closed. This can be seen by looking at the example of the integers $\mathbb{Z}$, which are a countably infinite subgroup of the additive group $\mathbb{Z}_{\hat{p}}$, which is a Galois group by Lemma 2.3.18, therefore following Corollary 2.3.11 $\mathbb{Z}$ is not closed. This means that the Galois correspondence for infinite Galois extensions does not always correlate all the subgroups of a Galois group to all the intermediate extensions of its Galois extension the way the finite Galois correspondence does. Some information is indeed lost when studying the correspondence in the infinite case.

Example 3.0.5. The same way there are subgroups in a Galois group that are not closed there are also subgroups that are closed but not open, these are precisely the closed subgroups of infinite index (as shown by Lemma 1.1.4(c),(d)). One such example is the subgroup $\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}(\{\zeta_p\}_{p\in P})) \leq_c \mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q})$ (where P represents the set of prime numbers), which is closed by Corollary 1.2.8 and it is of infinite index since, by Lemma 2.3.17, its index is equal to $|\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P})/\mathbb{Q})|$, which we will see is an infinite group.

We will now try to find more explicit formulations for both these groups. We will start with the group $\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P})/\mathbb{Q})$. Using Lemma B.0.4 we see that given $P_n := \{p \in P \mid p \leq n\}$, we have $\mathbb{Q}(\zeta_q) \cap \mathbb{Q}(\{\zeta_p\}_{p\in(P_n\setminus\{q\})}) = \mathbb{Q}$ for any $q \in P_n$. This together with Proposition 3.0.3 and induction on the order of the subset P_n leads us to the isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P_n})/\mathbb{Q}) \cong \prod_{p\in P_n} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

Now, using Lemma 3.0.1, we see that

$$\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P})/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P_n})/\mathbb{Q}) \cong \varprojlim \prod_{p\in P_n} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}),$$

which, as shown in Example 1.1.15, gives

$$\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P})/\mathbb{Q}) \cong \prod_{p\in P} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

Finally, using Lemma B.0.2 we arrive at the isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\{\zeta_p\}_{p\in P})/\mathbb{Q}) \cong \prod_{p\in P} \mathbb{Z}_p^\times.$$

Now, for the group $\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}(\{\zeta_p\}_{p\in P}))$, using again Lemma 3.0.1 we see that

$$\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}(\{\zeta_p\}_{p\in P})) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\Omega_n)(\{\zeta_p\}_{p\in P})/\mathbb{Q}(\{\zeta_p\}_{p\in P}))$$

where $\Omega_n := \{\zeta_i \mid i \leq n\}$. Then, by Proposition 3.0.2 we know that this inverse limit is in fact isomorphic to $\varprojlim \mathrm{Gal}(\mathbb{Q}(\Omega_n)/\mathbb{Q}(\{\zeta_p\}_{p\in P_n}))$. Now, using Lemma B.0.4 with induction on $|\Omega_n|$ we see that

$$\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})(\{\zeta_p\}_{p\in P_n}) \cap \mathbb{Q}(\{\zeta_{p^k}\}_{\substack{p\in P_n\setminus\{q\}\\ k\in K_n(p)}})(\{\zeta_p\}_{p\in P_n}) = \mathbb{Q}(\{\zeta_p\}_{p\in P_n})$$

for any $q \in P_n$, where $K_n(p) := \{k \in \mathbb{N} \mid p^k \leq n\}$. With this we can now use Proposition 3.0.3 to find that

$$\begin{array}{c} \varprojlim \mathrm{Gal}(\mathbb{Q}(\Omega_n)/\mathbb{Q}(\{\zeta_p\}_{p\in P_n})) \\ \| \wr \\ \varprojlim \prod_{q\in P_n} \mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})(\{\zeta_p\}_{p\in P_n})/\mathbb{Q}(\{\zeta_p\}_{p\in P_n})). \end{array}$$

After this step we can use Proposition 3.0.2 one more time to get

$$\begin{array}{c} \varprojlim \prod_{q\in P_n} \mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})(\{\zeta_p\}_{p\in P_n})/\mathbb{Q}(\{\zeta_p\}_{p\in P_n})) \\ \| \wr \\ \varprojlim \prod_{q\in P_n} \mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})/\mathbb{Q}(\zeta_q)). \end{array}$$

Finally, we claim that

$$\mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})/\mathbb{Q}(\zeta_q)) \cong \{z \in \mathbb{Z}^\times_{q^{m_n(q)}} \mid z \equiv 1 \pmod q\}$$

where $m_n(q) = \max\{k \in K_n(q)\}$. This last claim is true since, using Galois theory, we know that this Galois group is a subgroup of the Galois group $\mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})/\mathbb{Q})$, which we know is isomorphic to $\mathbb{Z}^\times_{q^{m_n(q)}}$ by Lemma B.0.4 and Lemma B.0.2. Furthermore, $\mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k\in K_n(q)})/\mathbb{Q}(\zeta_q))$ is the subgroup whose automorphisms fix ζ_q. Since, as seen in the construction of the isomorphism in Lemma B.0.2, the automorphisms of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{q^{m_n(q)}})/\mathbb{Q})$ can

be given by $\zeta_{q^{m_n(q)}} \mapsto \zeta_{q^{m_n(q)}}^j$ for some $j \in \mathbb{Z}^\times_{q^{m_n(q)}}$, the automorphism of $j \in \mathbb{Z}^\times_{q^{m_n(q)}}$ is such that that $\zeta_q = \zeta_{q^m}^{q^{m-1}} \mapsto \zeta_{q^m}^{jq^{m-1}}$ (here for simplicity we use $m = m_n(q)$). As a result, we see that $\zeta_{q^m}^{q^{m-1}} = e^{\frac{2\pi i(q^{m-1}+kq^m}{q^m}}) = e^{\frac{2\pi ijq^{m-1}}{q^m}} = \zeta_{q^m}^{jq^{m-1}}$ if and only if

$$\begin{aligned} q^{m-1} + kq^m &= jq^{m-1} \\ 1 + kq &= j, \end{aligned}$$

i.e. the js such that $\zeta_q \mapsto \zeta_q$ are precisely those congruent to 1 (mod q). Finally, we have that

$$\varprojlim \prod_{q \in P_n} \mathrm{Gal}(\mathbb{Q}(\{\zeta_{q^k}\}_{k \in K_n(q)})/\mathbb{Q}(\zeta_q)) \cong \varprojlim \prod_{q \in P_n} \{z \in \mathbb{Z}^\times_{q^{m_n(q)}} \mid z \equiv 1 \pmod q\}$$

and, using Lemma 1.1.21 together with Proposition 1.1.17 (just like we did in Example 1.2.4), this can be expressed (in terms of an isomorphism) as a double inverse limit

$$\varprojlim_m \varprojlim_n \prod_{q \in P_n} \{z \in \mathbb{Z}^\times_{q^m} \mid z \equiv 1 \pmod q\},$$

which following Example 1.1.15 and Example 1.2.5 can be solved to give us

$$\varprojlim_m \varprojlim_n \prod_{q \in P_n} \{z \in \mathbb{Z}^\times_{q^m} \mid z \equiv 1 \pmod q\} \cong \prod_{q \in P} \{z \in \mathbb{Z}^\times_{\hat{q}} \mid z \equiv 1 \pmod q\},$$

so

$$\mathrm{Gal}(\mathbb{Q}(\Omega)/\mathbb{Q}(\{\zeta_p\}_{p \in P})) \cong \prod_{q \in P} \{(z_i) \in \mathbb{Z}^\times_{\hat{q}} \mid z_i \equiv 1 \pmod q\}.$$

As a result, by Lemma 2.3.17, we see that

$$\frac{\prod_{q \in P} \mathbb{Z}^\times_{\hat{q}}}{\prod_{q \in P} \{(z_i) \in \mathbb{Z}^\times_{\hat{q}} \mid z_i \equiv 1 \pmod q\}} \cong \prod_{q \in P} \mathbb{Z}^\times_q.$$

We will finish this thesis with a very original example that proves that the Galois group of an extension of the rationals that is a splitting field for all its polynomials of degree at most 2 is in fact the infinite product of groups of order 2.

Example 3.0.6. For this example we will denote by $\mathcal{F}$ the family of irreducible polynomials of degree 2 in $\mathbb{Q}[t]$ indexed by $\mathbb{N}$ (we can do this since $\mathbb{Q}[t]$ is a countable set), and by $\mathbb{Q}_\mathcal{F}$ the splitting field of all the polynomials in $\mathcal{F}$. We shall also denote by $\mathbb{Q}_n$ the splitting field of the polynomials $\{f_i\}_1^n$ where $\{f_i\}_{i \in \mathbb{N}} = \mathcal{F}$. Using Lemma 3.0.1 we know that $\mathrm{Gal}(\mathbb{Q}_\mathcal{F}/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}))$.

Now, $\mathbb{Q}_n = \mathbb{Q}(x_1, \ldots, x_r)$, where $\{x_i\}_1^r$ are the roots of the polynomials $\{f_i\}_1^n$, and the roots of these polynomials are given by the formula $\frac{-a_i \pm \sqrt{a_i^2 - 4b_i}}{2}$ for some $a_i, b_i \in \mathbb{Q}$, but $-a_i/2 \in \mathbb{Q}$ and $-\sqrt{a_i^2 - 4b_i}/2$ is just the additive inverse of $\sqrt{a_i^2 - 4b_i}/2$, so denoting by $d_i = a_i^2/4 - b_i$ the extension $\mathbb{Q}(\{x_i\}_1^r)$ can also be expressed as $\mathbb{Q}(\{\sqrt{d_i}\}_1^r)$. For any $d \in \mathbb{Q}$ we know that $\sqrt{d} = \sqrt{u}/\sqrt{v}$ for some $u, v \in \mathbb{Z}$, so we have that $\mathbb{Q}(\{\sqrt{d_i}\}_1^r) \subseteq \mathbb{Q}(\{\sqrt{u_i}\}_1^r, \{\sqrt{v_i}\}_1^r)$ for some $u_i, v_i \in \mathbb{Z}$. Finally, for any $z \in \mathbb{Z}$ we can decompose z into prime factors so that $z = (\pm)p_1^{k_1} \cdots p_s^{k_s}$ which allows us to express $\sqrt{z}$ as $\sqrt{z} = \sqrt{(\pm)p_1^{k_1} \cdots p_s^{k_s}}$. As a result we get that $\mathbb{Q}(\{\sqrt{u_i}\}_1^r, \{\sqrt{v_i}\}_1^r) \subseteq \mathbb{Q}(\{\sqrt{p}\}_{p \in Q})$ for some $Q \subseteq P \cup \{-1\}$ where P is the set of prime numbers and $|Q| < \infty$. Clearly $\mathbb{Q}(\{\sqrt{p}\}_{p \in Q}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_k})$ for large enough $k \in \mathbb{N}$ (where p_i are the indexed primes), so the collection of Galois groups $\{\mathrm{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q})\}_{k \in \mathbb{N}}$ forms a cofinal subsystem, meaning that, by Lemma 1.1.21, $\mathrm{Gal}(\mathbb{Q}_{\mathcal{F}}/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q})$.

All that is left to prove is that $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong \prod_0^n \mathbb{Z}_2$ and for this we will make use of Proposition 3.0.3. We first need to show that given a non-empty finite set $S = \{\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_n}\}$ the following holds $\mathbb{Q}(\sqrt{q}) \cap \mathbb{Q}(S \setminus \{\sqrt{q}\}) = \mathbb{Q}$ for any $\sqrt{q} \in S$. We will show this by induction on the order of S. First we see that for $|S| = 1$ this is trivially true since $\sqrt{q}$ is a root of the degree 2 polynomial $t^2 - q \in \mathbb{Q}[t]$, which is irreducible in $\mathbb{Q}[t]$ for any $q \in P \cup \{-1\}$ by the rational root test. Assuming the hypothesis holds for $|S_n| = n$, if for $|S_{n+1}| = n + 1$ we have that for some $\sqrt{q} \in S_{n+1}$ $\mathbb{Q}(\sqrt{q}) \cap \mathbb{Q}(S_{n+1} \setminus \{\sqrt{q}\}) \neq \mathbb{Q}$, then $\sqrt{q} \in \mathbb{Q}(S_{n+1} \setminus \{\sqrt{q}\}) = \mathbb{Q}(S_n \setminus \{\sqrt{p}\})(\sqrt{p})$ for some $\sqrt{p} \in S_n = S_{n+1} \setminus \{q\}$, which (by seeing $\mathbb{Q}(S_n \setminus \{\sqrt{p}\})(\sqrt{p})$ as a vector space over $\mathbb{Q}(S_n \setminus \{\sqrt{p}\})$) implies that $\sqrt{q} = a + b\sqrt{p}$ (since $\{1, \sqrt{p}\}$ is a basis for the mentioned vector space) for some $a, b \in \mathbb{Q}(S_n \setminus \{\sqrt{p}\})$, but then squaring we get that $q = a^2 + 2ab\sqrt{p} + b^2 p$, which implies that $\sqrt{p} \in \mathbb{Q}(S_n \setminus \{\sqrt{p}\})$, which is a contradiction to the induction hypothesis, so we must have that $\mathbb{Q}(\sqrt{q}) \cap \mathbb{Q}(S_{n+1} \setminus \{\sqrt{q}\}) = \mathbb{Q}$ for all $\sqrt{q} \in S_{n+1}$.

Finally we are ready to use Proposition 3.0.3 and so we see that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong \prod_{i=0}^{n} \mathrm{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q})$$

where $p_0 = -1$. Clearly $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}) \cong \mathbb{Z}_2$ since $\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}$ is a degree 2 extension, which from finite Galois theory we know implies that its Galois group is of order 2. As a result we get that $\mathrm{Gal}(\mathbb{Q}_{\mathcal{F}}/\mathbb{Q}) \cong \varprojlim \prod_0^n \mathbb{Z}_2$, which as seen in Example 1.1.15 proves that $\mathrm{Gal}(\mathbb{Q}_{\mathcal{F}}/\mathbb{Q}) \cong \prod_0^\infty \mathbb{Z}_2$.

Appendix A Background Knowledge

Theorem A.0.1 (Chinese Remainder Theorem)**.** *Given a set of numbers* $\{n_i\}_1^s$ *coprime to each other and a set of integers* $\{a_i\}_1^s$*, the system of congruences given by*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_s \pmod{n_s} \end{aligned}$$

has a unique solution congruent modulo $n_1 n_2 \cdots n_s$*.*

Theorem A.0.2 (Lagrange's Theorem for Finite Groups)**.** *Given a finite group* G *and a subgroup* $H \leq G$ *the following holds*

$$|G| = [G : H]\,|H|.$$

Theorem A.0.3 (First Isomorphism Theorem)**.** *Given a homomorphism* $\alpha : G \to H$ *between groups then* $G/\ker(\alpha) \cong \alpha(G)$*.*

Theorem A.0.4 (Second Isomorphism Theorem)**.** *Given a group* G *and subgroups* $H \leq G$ *and* $N \trianglelefteq G$ *then* $(HN)/N \cong H/(H \cap N)$*.*

Theorem A.0.5 (First Sylow Theorem)**.** *Given a finite group* G *and a prime* p *such that* $p \mid |G|$ *there is a Sylow* p*-subgroup.*

Theorem A.0.6 (Second Sylow Theorem)**.** *Given a finite group* G *and a prime* p *all the Sylow* p*-subgroups of* G *are conjugate to each other.*

Theorem A.0.7 (Zorn's Lemma)**.** *Given a poset in which every chain of ordered elements has an upper (respectively lower) bound, there is a maximal (respectively minimal) element in the set.*

Theorem A.0.8 (Orbit Stabilizer Theorem)**.** *Given a finite group* G *acting on a set* S *the following holds*

$$|G| = |Gs| \times |G_s|$$

where Gs *represents the orbit of* s *and* G_s *represents the stabilizer of* s *for some* $s \in S$*.*

Lemma A.0.9. *Given a group* G *and a subgroup* $H \leq G$ *the set of right (or left) cosets of* H *form a set of equivalence classes.*

Definition A.0.10 (Totally disconnected)**.** A totally disconnected topological space is a space in which the only connected subsets are the singletons.

Definition A.0.11 (Splitting field)**.** A splitting field of a family of polynomials $\mathcal{F} \subseteq K[t]$ is an extension L/K such that every polynomial in $\mathcal{F}$ splits into linear factors in L and L is minimal in the sense that no proper subfield of L satisfies the first condition.

Remark A.0.12. [2, pg 236] A splitting field L/F of a family of polynomials $\mathcal{F} \subseteq K[t]$ is always of the form $L = K(R_{\mathcal{F}})$ where $R_{\mathcal{F}}$ is the set of roots of the polynomials in $\mathcal{F}$.

Proof. Clearly, the polynomials in $\mathcal{F}$ split over $K(R_{\mathcal{F}})$, and since $K(R_{\mathcal{F}})$ is the field generated by the roots of the polynomials in $\mathcal{F}$ it is the smallest field containing all those roots, so the minimality condition is satisfied. □

Definition A.0.13 (Normal extension)**.** A normal extension F/K is an algebraic extension that satisfies that every irreducible polynomial in $K[t]$ with a root in F splits over F.

Remark A.0.14. [2, Theorem V.3.3] A normal extension F/K is a splitting field of a family of polynomials in $K[t]$.

Proof. If F/K is normal then for every $x \in F$ the minimal polynomial of x, say $m_x \in K[t]$, is such that it splits over F, so the splitting field $K(R_{m_x})$ is contained in F (here R_{m_x} represents the set of roots of m_x). As a result we have that $F = (K(R_{m_x}))_{x \in F} = K(\bigcup_{x \in F} R_{m_x})$ (here $(K(R_{m_x}))_{x \in F}$ represents the compositum of the extensions $\{K(R_{m_x})\}_{x \in F}$)), i.e. F is a splitting field for the minimal polynomials of its elements.
If F/K is a splitting field for a family of polynomials $\mathcal{F}$ then $F = K(R_{\mathcal{F}})$. Now, for any irreducible polynomial $p \in K[t]$ with a root x in F, p must be a multiple of the minimal polynomial of x, so it must have the same roots. Now, since $x \in F$ we must have $x \in K(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in R_{\mathcal{F}}$, and $K(a_1, \ldots, a_n) \subseteq K(R_T)$ where T is a set of n polynomials in $\mathcal{F}$ each with some a_i as a root. Finally, $K(R_T) \subseteq K(R_{\mathcal{F}})$ is a finite splitting field, so, as seen in [1, Theorem 7.13], it is normal meaning that the minimal polynomial x splits over it, and so p does too. □

Definition A.0.15 (Separable extension)**.** A separable extension F/K is an extension in which the minimal polynomial of every element in F over K has no multiple roots.

Remark A.0.16. [2, pg 241] An infinite separable extension F/K is an extension satisfying that any finite intermediate extension is separable.

Proof. If F/K is separable then given any intermediate extension M and any $x \in M$ we have that $x \in F$, so the minimal polynomial of x has no multiple roots, meaning that M/K is separable.
Now, if every finite intermediate extension of F/K is separable, then given some $x \in F$ we have $x \in K(x)$, which is a finite extension, thus the mininmal polynomial of x has no multiple roots by the separability of $K(x)$ $\square$

Appendix B Additional Information

Lemma B.0.1. *If G is a Hausdorff topological group then $\{g\} \leq_c G \ \forall g \in G$.*

Proof. Take an arbitrary element $g \in G$ then $(G \setminus \{g\}) = \bigcup_{h \in (G \setminus \{g\})} \{h\}$. Now, by Hausdorffness we can find $\{U_h\}_{h \in (G \setminus \{g\})}$ such that $U_h \cap U_g = \emptyset \ \forall h \in (G \setminus \{g\})$, therefore $(G \setminus \{g\}) = \bigcup_{h \in (G \setminus \{g\})} U_h$, i.e. $(G \setminus \{g\})$ is equal to a union of open sets, so it is open hence $\{g\}$ must be closed. □

Lemma B.0.2. *[1, Theorem 8.13] The Galois group of any cyclotomic extension $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has order $\varphi(n)$ (this is Euler's totient function counting the number of integers smaller than n relatively prime to n) and is isomorphic to $\mathbb{Z}_n^\times$.*

Proof. The map $\theta : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}_n^\times$ given by $\theta : \sigma \mapsto \alpha$ where α is the power of ζ_n to which σ sends ζ_n is a well-defined injective homomorphism. Now we claim that $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |\mathbb{Z}_n^\times|$, i.e. θ is surjective. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a simple algebraic extension, it must have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \partial(m_{\zeta_n})$ where m_{ζ_n} is the minimal polynomial of ζ_n over $\mathbb{Q}$. We now want to prove that for any prime number $p \leq n$ that does not divide n the element ζ_n^p (which is also a primitive nth root of unity) is a root of m_{ζ_n}, i.e. since any primitive nth root of unity is a succession of prime powers of ζ_n with primes $\leq n$ not dividing n, every primitive nth root of unity is a root of m_{ζ_n}, meaning that $\partial(m_{\zeta_n}) \geq \varphi(n)$. We will show this by assuming the contrary, that ζ_n^p is not a root of m_{ζ_n}. Then, since ζ_n^p is a root of $t^n - 1$, it must be a root of some polynomial $f \in \mathbb{Q}[t]$ such that $t^n - 1 = m_{\zeta_n} f$. As a result, ζ_n is a root of the polynomial $f(t^p)$, so $m_{\zeta_n}(t) \mid f(t^p)$. Now, since $a^p \equiv a \pmod p$ and $f, m_{\zeta_n} \in \mathbb{Z}[t]$ by Gauss Lemma, using the notation $\overline{g}$ to represent the reduction of any polynomial $g \in \mathbb{Z}[t]$ modulo p, using multinomial decomposition we would see that $\overline{f(t^p)} = \overline{f(t)}^p$, so $\overline{m_{\zeta_n}} \mid \overline{f(t)}^p$, meaning that $\overline{m_{\zeta_n}}$ and $\overline{f(t)}$ have a common factor, contradicting the fact that $\overline{m_{\zeta_n}}\,\overline{f(t)} = \overline{t^n - 1}$ has no multiple roots (which is obvious since we know that the roots of this polynomial in $\mathbb{C}[t]$ are precisely the elements $e^{2\pi i m/n}$ for $m \in \{1, \ldots, n\}$). Finally, since $\partial(m_{\zeta_n}) \geq \varphi(n)$ we have that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geq \varphi(n)$, but from finite Galois theory we know that the degree of the extension is the order of its Galois group, so $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \geq \varphi(n)$. Furthermore, $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$, so $|\mathbb{Z}_n^\times| = \varphi(n)$, meaning that θ is surjective and so it is a topological and group isomorphism (if we consider the domain and codomain as Discrete topological spaces). □

Lemma B.0.3. *Given an algebraic extension M/K the algebraic closures of both fields satisfy $M^{\mathrm{alg}} = K^{\mathrm{alg}}$.*

Proof. Clearly $M^{\text{alg}} \supseteq K^{\text{alg}}$, so all we need to prove is that $M^{\text{alg}} \subseteq K^{\text{alg}}$. For any $x \in M^{\text{alg}}$ there is a polynomial $p_x \in M[t]$ such that $p_x(x) = 0$ where $p_x(t) = a_n t^n + \cdots + a_1 t + a_0$ for some $a_i \in M$. Then $p_x \in K(\{a_i\}_0^n)[t]$, so $[K(\{a_i\}_0^n)(x) : K(\{a_i\}_0^n)] \leq \partial p_x$ and clearly $[K(\{a_i\}_0^n) : K] \leq n$, so using Lagrange's Theorem we clearly have that $[K(\{a_i\}_0^n)(x) : K] < \infty$, which implies (as shown in [1, Theorem 3.12]) that $K(\{a_i\}_0^n)(x)/K$ is an algebraic extension, meaning that $x \in K^{\text{alg}}$. □

Lemma B.0.4. *Given two numbers $n, m \in \mathbb{N}$ with $\gcd(n, m) = d$ and $\operatorname{lcm}(n, m) = f$ the nth and mth cyclotomic extensions satify*

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_f)$$

and

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d).$$

Proof. To prove the first equality we first notice that since $\zeta_f^{f/n} = e^{2\pi i(f/n)/f} = e^{2\pi i/n} = \zeta_n$ we have $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_f)$ and similarly for ζ_m, meaning that $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_f)$. Now, since $mn = df$ and we can find $a, b \in \mathbb{N}$ such that $an + bm = d$, dividing the left side by mn and the right side by df we get that $a/m + b/n = 1/f$, meaning that $\zeta_m^a \zeta_n^b = e^{2\pi i a/m} e^{2\pi i b/n} = e^{2\pi i/f} = \zeta_f$, i.e. $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) \supseteq \mathbb{Q}(\zeta_f)$, and so $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_f)$.

For the second inequality we can clearly see that $\zeta_d = \zeta_n^{n/d} = \zeta_m^{m/d}$, meaning that $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$. Now, since Euler's totient function can be given as $\varphi(x) = \prod p_i^{k_i - 1}(p_i - 1)$ where p_i are the prime factors of x and k_i are the powers of the prime factors, i.e. $x = \prod p_i^{k_i}$, we see that $\gcd(\varphi(n), \varphi(m)) = \varphi(\gcd(n, m))$, and using Lemma B.0.2 together with Lagrange's theorem we see that $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) : \mathbb{Q}]$ must divide $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ and $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, meaning that $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) : \mathbb{Q}] \mid \varphi(d) = [\mathbb{Q}(\zeta_d) : \mathbb{Q}]$, but we saw that $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$, so we must have $\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$. □

Lemma B.0.5. *[5, Lemma 0.1.1] In a compact totally disconnected space X given two points $x, y \in X$ with $x \neq y$ there exists a clopen set U_x containing x but not y.*

Proof. First we need to define the following relation: $\forall a, b \in X$ we say $a \sim b$ iff $\nexists U_a, U_b$ such that $U_a \cap U_b = \emptyset$ and $U_a \cup U_b = X$. This relation is in fact an equivalence relation since $\forall a \in X$ we clearly have $a \sim a$, and for any $a, b \in X$ such that $a \sim b$ clearly $b \sim a$, and furthermore, if we have $a \sim b$ and $b \sim c$ for some $a, b, c \in X$ then $a \sim c$ since if there was some disjoint U_a, U_c such that $U_a \cup U_c = X$ then either $b \in U_a$ which contradicts $b \sim c$ or $b \in U_c$ which contradicts $a \sim b$. As a result we see that this relation forms a set of equivalence

classes that we will call the quasicomponents. The quasicomponent Q_a of a point $a \in X$ is just the intersection of all the clopen sets in X containing a. This is true since $\forall x \in Q_a$ given any clopen set F containing a, the sets F and $(X \setminus F)$ form a separation of X, but since $x \sim a$ we must have $x \in F$, meaning that $x \in \bigcap F_i$ (the intersection of all clopen sets containing a), furthermore, $\forall x \in \bigcap F_i$ given a separation of X say U, V with $a \in U$, since U is clopen $x \in U$, meaning that x is in the same side of any separation of X as a, i.e. $x \in Q_a$.
Clearly, the connected component C_a (maximal connected set containing the point) of any point $a \in X$ is in its quasicomponent Q_a since for any $x \in C_a$ we must have $x \sim a$, i.e. $x \in Q_a$, otherwise there would exist disjoint U_x, U_a such that $U_x \cup U_a = X$, which would imply that $(C_a \cap U_x)$ and $(C_a \cap U_a)$ are two non-empty disjoint open (with respect to the subspace topology of C_a) subsets satisfying that $(C_a \cap U_x) \cup (C_a \cap U_a) = C_a$, which is a contradiction to the fact that C_a is connected. We now claim that in a compact topological space $C_a = Q_a$ for all $a \in X$. If we can prove that Q_a is connected for every $a \in X$ the claim will be satisfied. We will do this by assuming Q_a is not connected, i.e. there are open sets U and V such that $U \cup V \supseteq Q_a$ and $U \cap V = \emptyset$, then since X is compact and the set $(U \cup V)^c$ is closed it is a compact set. Furthermore, since $Q_a = \bigcap F_i \subseteq (U \cup V)$ (where F_i are the clopen sets containing a) we have $Q_a^c = \bigcup F_i^c \supseteq (U \cup V)^c$,i.e. $\bigcup F_i^c$ is an open cover of $(U \cup V)^c$, which by compactness implies there exists a finite subcover such that $\bigcup_1^n F_i^c \supseteq (U \cup V)^c$, meaning that $Q_a \subseteq F = \bigcap_1^n F_i \subseteq (U \cup V)$. Finally, F is clearly clopen and $\overline{U \cap F} \subseteq \overline{U} \cap \overline{F} = \overline{U} \cap ((U \cup V) \cap F) = (\overline{U} \cap (U \cup V)) \cap F = U \cap F$, meaning that $U \cap F$ is clopen. Now, without loss of generality we may assume $a \in U$, implying that $Q_a \subseteq U \cap F$, but then $V \cap Q_a \subseteq Q_a \subseteq U \cap F \subseteq U$, which by the disjointness of U and V implies that $V \cap Q_a = \emptyset$, proving that Q_a is connected, i.e. $Q_a = C_a$. As a result —and since the connected components in a totally disconnected space are the singletons—, given two points $x, y \in X$ with $x \neq y$ both points lie in different quasicomponents, meaning that there exists a separation of X say U_x, U_y in which U_x is clearly a clopen set containing x but not y. $\square$

References

[1] John M. Howie. *Fields and Galois Theory*. Springer, 2006.

[2] Serge Lang. *Algebra*. Springer, 3rd edition, 2002.

[3] James S. Milne. Fields and galois theory, 2022. URL `www.jmilne.org/math/`.

[4] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, 2000.

[5] John S. Wilson. *Profinite Groups*. Oxford University Press, 1998.

Master's Theses in Mathematical Sciences 2023:E63
ISSN 1404-6342

LUNFMA-3138-2023

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/