Profinite Groups

Author: Chiara Sarti

Supervisor: Prof Fred Diamond

April 10, 2021



Abstract

In this thesis, I will give a self-contained exposition of profinite groups, from definition to key properties, focusing on their topology and generators, the generalisation of the Sylow Theorems and how they may be seen as group completions. Each section will present motivating examples most relevant to modern research in number theory, such as the p-adic integers $\mathbb{Z}_p$, the profinite integers $\hat{\mathbb{Z}}$, the Nottingham group $\mathcal{J}(\mathbb{F}_p)$ and infinite Galois groups. Since the construction of profinite groups relies on inverse limits, I will analyse them in detail, introducing the necessary category theoretical notions. I will explore at length the link between infinite Galois theory and profinite groups, generalising the Fundamental Theorem and proving the realisability of certain profinite groups as Galois groups.

Contents

1 Introduction **4**

2 Limits and Colimits **5**

2.0.1 Example: the Cantor set as an inverse limit . . . 9

2.0.2 Example: the infinite general linear group $GL_\infty(K)$ . . . 10

3 Topological Groups **11**

4 Profinite Groups **14**

4.1 Construction . . . 14

4.2 Properties as Topological Groups . . . 15

4.2.1 Example: the p-adic integers $\mathbb{Z}_p$ . . . 18

4.3 Profinite Completions . . . 22

4.3.1 Example: the profinite integers $\hat{\mathbb{Z}}$ . . . 24

4.4 Sylow's Theorems . . . 26

4.4.1 Example: $\mathbb{Z}_p$ as Sylow p-subgroup of $\hat{\mathbb{Z}}$ . . . 30

4.5 Generators and procyclic groups . . . 31

4.5.1 Example: the generators of $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ . . . 32

4.6 The Frattini Subgroup . . . 34

4.6.1 Example: the Nottingham group $\mathcal{J}(\mathbb{F}_p)$ . . . 36

5 Infinite Galois Theory **42**

5.1 Finite Galois Theory . . . 42

5.2 Galois Connections and Closures . . . 44

5.3 Constructing the Krull Topology . . . 47

5.4 The Infinite Fundamental Theorem . . . 51

5.5 Examples . . . 52

5.5.1 Example: $\mathbb{Z}_p$ as a Galois group over $\mathbb{Q}$ . . . 52

5.5.2 Example: $\hat{\mathbb{Z}}$ as a Galois group over $\mathbb{F}_p$ . . . 54

6 Conclusion **56**

Bibliography **60**

1 Introduction

The study of profinite groups has a rich history. The most well-known profinite group, the p-adic integers $\mathbb{Z}_p$, is considered to have been introduced at the end of the 19th century by K. Hensel, who established several important results about the p-adics, such as what we now call Hensel's (Lifting) Lemma. This area of research grew considerably in the first half of the 20th century, through the contributions of the likes of J. Kürschák, E. E. Kummer, H. Hasse and A. Ostrowski [KKM02].

Another thread in the history of profinite groups stems from the work of W. Krull on infinite Galois Theory. In order to generalise the Fundamental Theorem of Galois Theory to infinite extensions, he introduced a topology on infinite Galois groups and characterised them as compact, Hausdorff and totally disconnected. Since groups with these properties can be realised as Galois groups, they became known as *groups of Galois type*. Then, J. P. Serre's 1964 book "Cohomologie Galoisienne" [Ser97] popularised the term *profinite groups*, which reflected their structure of projective limits of finite groups.

However, the study of profinite groups is of interest beyond its Galois theory roots. They represent a large class of infinite groups for which many important results of finite groups hold. Profinite groups sit at the crossroads between elementary group theory and modern algebraic number theory. Hence, we will present here a self-contained discussion of this topic, aimed at introducing the reader to many techniques used in fields such as Iwasawa Theory or p-adic Lie Theory, assuming only knowledge of elementary group theory, topology, finite Galois theory and basic category theory.

The discussion is organised as follows: first, we introduce the category theoretical machinery necessary to define inverse limits. We will then move to introduce some minimal theory of topological groups, which will be essential throughout the rest of the discussion. The main chapter concerns profinite groups themselves, touching on their construction and basic topological properties, to profinite completions, the generalisation of the Sylow Theorems, topological generators and the Frattini subgroup. The final chapter will be dedicated to uncovering the link between profinite groups and infinite Galois Theory, providing an original take on the classical proof of the infinite Fundamental Theorem of Galois Theory. In the conclusion we will summarise the theory developed throughout this study, alongside prompts for future research. Each section will provide relevant examples to familiarise the reader with the theoretical notions introduced.

The main sources for this discussion are the following: for what concerns category theoretical concepts, our notation and most results are indebted to "Categories and Functors" by B. Pareigis [Par70], while the remaining results are split between the nLab project [nLa21] and "Categories for the Working Mathematician" by S. Mac Lane [ML78]. For profinite groups, the most important sources are, in no particular order, "Profinite Groups" by L. Ribes [RZ10], "Lectures in Profinite Topics in Group Theory" by B. Klopsch, et al. [KVSN11] and the lecture notes "Profinite Groups and Group Cohomology" by G. Wilkes [Wil], all of which are highly advised to the interested reader. Finally, for the Galois Theory chapter, "Fields and Galois Theory" by J. S. Milne [Mil20b] is our main source.

2 Limits and Colimits

We begin our discussion by introducing the theoretical machinery that will allow us to construct profinite groups, namely, inverse limits. Although the inverse limit procedure may be understood entirely from an algebraic point of view, as it originated historically, we will present it, in a more modern fashion, as a special case of the notion of limit in category theory. We will assume the reader is familiar with basic concept from category theory, such as categories, functors and the duality principle. A primer on these concepts can be found in the Appendix, or references such as "Categories and Functors" by B. Pareigis [Par70] or "Categories for the Working Mathematician" by S. Mac Lane [ML78].

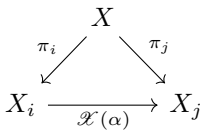
This section is organised as follows: we will first define limits and colimits in arbitrary categories, establishing uniqueness and presenting familiar examples. We will then introduce directed posets as index categories for limits and thus introduce inverse and direct limits. Since working explicitly with limits of functors for the rest of the discussion is too verbose, we will look at the alternative formalism of inverse and direct systems. We will conclude the section by presenting examples of inverse and direct limits.

Let us move to define limits. We first introduce the notion of a diagram:

Definition 2.1. Let $\mathscr{I}, \mathscr{C}$ be categories. If $\mathscr{I}$ is a small category[1], we call a functor $\mathscr{X} : \mathscr{I} \to \mathscr{C}$ a **diagram of shape** $\mathscr{I}$. In which case, for each $i \in \mathrm{Obj}\mathscr{I}$, we denote $X_i = \mathscr{X}(i)$.

From diagrams we define cones, as selected objects and morphisms in the target category of a diagram:

Definition 2.2. Let $\mathscr{I}, \mathscr{C}$ be categories and $\mathscr{X}$ a diagram of shape $\mathscr{I}$ in $\mathscr{C}$. A **cone** on $\mathscr{X}$ is an object $X \in \mathrm{Obj}\mathscr{C}$ together with morphisms $\pi_i : X \to X_i$ for each $i \in \mathrm{Obj}\mathscr{I}$, such that for any $\alpha : i \to j$ in $\mathscr{I}$, we have $\mathscr{X}(\alpha) \circ \pi_i = \pi_j$, i.e. the following diagram commutes:

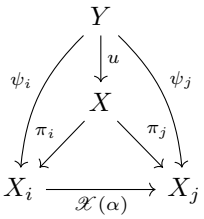


If (X, π_i) is a cone, we call the morphisms π_i **projections**. Finally, limits are universal cones, or cones such that every other cone factors though them.

Definition 2.3. Let $\mathscr{I}, \mathscr{C}$ be categories and (X, π_i) be a cone on the diagram $\mathscr{X}$. A **limit** of the diagram $\mathscr{X}$ is a cone (X, π_i) such that for any other cone (Y, ψ_i) there is a unique morphism $u : Y \to X$

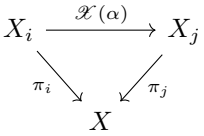
[1] A category is small if its class of objects and morphisms are sets, instead of proper classes. For an example of a category that is not small, consider the category of sets **Set**, whose class of objects cannot be a set by Russell's Paradox.

such that for all $i \in \mathrm{Obj}\mathscr{I}$, we have $\pi_i \circ u = \psi_i$, i.e. the following diagram commutes:

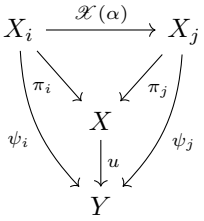


To cones and limits correspond the dual notions of cocones and colimits:

Definition 2.4. Let $\mathscr{I}, \mathscr{C}$ be categories and $\mathscr{X}$ a diagram of shape $\mathscr{I}$ in $\mathscr{C}$. A **cocone** on $\mathscr{X}$ is an object $X \in \mathrm{Obj}\mathscr{C}$ together with morphisms $\pi_i : X_i \to X$ for each $i \in \mathrm{Obj}\mathscr{I}$, such that for any $\alpha : i \to j$ in $\mathscr{I}$, we have $\pi_i = \pi_j \circ \mathscr{X}(\alpha)$, i.e. the following diagram commutes:



Definition 2.5. Let $\mathscr{I}, \mathscr{C}$ be categories and (X, π_i) be a cone on the diagram $\mathscr{X}$. A **colimit** of the diagram $\mathscr{X}$ is a cocone (X, π_i) such that for any other cocone (Y, ψ_i) there is a unique morphism $u : Y \to X$ such that for all $i \in \mathrm{Obj}\mathscr{I}$, we have $u \circ \pi_i = \psi_i$, i.e. the following diagram commutes:



When the morphisms are obvious, we will sometimes elide them and improperly refer to the object as a limit. Having introduces several new notions, it is important to pause and consider the usual questions of existence and uniqueness of these objects. While existence of limits and colimits depends on the category, strong uniqueness holds in all categories:

Proposition 2.6. Limits and colimits, when they exist, are unique up an isomorphism which commutes with the projections.

Proof. See Proposition 1.1.18 in Chapter 1 of "Profinite Groups and Group Cohomology" by G. Wilkes [Wil]. □

In the most trivial and familiar example, let $\mathscr{J}$ be a small discrete category of two or more objects and $\mathscr{C}$ a category with (co)products. Then a (co)limit of any diagram of shape $\mathscr{X} : \mathscr{J} \to \mathscr{C}$ is a (co)product of the family of objects $\{X_i\}_{i \in \mathrm{Obj}\mathscr{J}}$, by the very definition of (co)products. Recall that in the category

of sets **Set**, coproducts are the disjoint unions.

To make the jump from limits to inverse limits, and dually from colimits to direct limits, we must restrict ourselves to a particular type of index category. To this end, consider the definition of partially ordered sets:

Definition 2.7. Let I be a set and $\leq$ a binary relation on I. We say $(I, \leq)$ is a **partially ordered set**, or **poset**, if I is non-empty and $\leq$ is

1. Reflexive: $\forall i \in I,\ i \leq i$,
2. Transitive: $\forall i, j, k \in I,\ i \leq j \wedge j \leq k \implies i \leq k$,
3. Antisymmetric: $\forall i, j \in I,\ i \leq j \wedge j \leq i \implies i = j$.

Posets may be viewed as special categories characterised by having at most a single morphism between objects:

Definition 2.8. Let $(I, \leq)$ be a poset. We define the **poset category** $\mathscr{I}$ by

1. $\mathrm{Obj}_{\mathscr{I}} := I$,
2. For all $i \leq j$, $\mathrm{Mor}_{\mathscr{I}}(i, j) := \{j \to i\}$,
3. For all $i \not\leq j$, $\mathrm{Mor}_{\mathscr{I}}(i, j) := \emptyset$.

Note that we will sometimes abuse notation and write $(I, \leq)$ for a poset category, since one may always be converted into the other. We distinguish a particular type of poset:

Definition 2.9. Let $(I, \leq)$ be a poset. We say $(I, \leq)$ is **upward-directed**, or simply **directed**, if for every $i, j \in I$, there exists a $k \in I$ such that $i \leq k$ and $j \leq k$.

Inverse limits are limits whose index category is a directed poset, and similarly for directed limits and colimit. Formally, we have:

Definition 2.10. Let $\mathscr{C}$ be a category and $\mathscr{X}$ a diagram of shape $\mathscr{I}$, a directed poset category. We say a limit of $\mathscr{X}$ is an **inverse limit** and denote its object $\varprojlim_{i \in I} X_i$ if $\mathscr{X}$ is covariant. Dually, we say a colimit of $\mathscr{X}$ is a **direct limit** and denote its object $\varinjlim_{i \in I} X_i$ if $\mathscr{X}$ is contravariant.

We can avoid specifying the diagram every time by relying on an alternative formalism:

Definition 2.11. Let $\mathscr{C}$ be a category and $(I, \leq)$ a directed poset. Let (X_i) be a family of objects and $(\phi_{ij} : X_j \to X_i)_{i \leq j}$ of morphisms in $\mathscr{C}$ indexed by I. We say $(X_i, \phi_{ij}, I, \leq)$ is an **inverse system** if there exists a diagram $\mathscr{X}$ of shape $(I, \leq)$ such that for all $i, j \in I$, $\mathscr{X}(i) = X_i$ and $\mathscr{X}(j \to i) = \phi_{ij}$[2].

[2] $\mathscr{X}$ being covariant is ensured by the $\mathscr{X}(j \to i) = \phi_{ij}$

Dually, if the morphisms run $(\phi_{ij} : X_i \to X_j)_{i \leq j}$, we say $(X_i, \phi_{ij}, I, \leq)$ is a **direct system**.

We will write (X_i, ϕ_{ij}), (X_i, I) or even (X_i) for an inverse or direct system $(X_i, \phi_{ij}, I, \leq)$ if the index set or the morphisms are clear from the context, and say that the inverse system is **surjective** if its morphisms are. We will also refer to an inverse limit of the diagram as an inverse limit of the inverse system and similarly for direct system. In this case, we can omit the diagram since the requirements in Definition 2.11 uniquely determine the functor.

Proposition 2.12. Let $\mathscr{C}$ be a category, (X_i) be a family of objects and $(\phi_{ij} : X_j \to X_i)_{i \leq j}$ of morphisms in $\mathscr{C}$ indexed by $(I, \leq)$, a directed poset. Then $(X_i, \phi_{ij}, I, \leq)$ is an inverse system if and only if

1. For all $i \leq j \leq k$, $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$,
2. For all $i \in I$, $\phi_{ii} = 1_{X_i}$.

Proof. Assume $(X_i, \phi_{ij}, I, \leq)$ is an inverse system and let $\mathscr{X}$ be the covariant functor defined in 2.11. Since functors preserve identities $\mathscr{X}(i \to i) = \phi_{ii} = 1_{X_i}$. Moreover, since $(I, \leq)$ is transitive, $\phi_{ij} \circ \phi_{jk} = \mathscr{X}(j \to i) \circ \mathscr{X}(k \to j) = \mathscr{X}(k \to i) = \phi_{ik}$.

Conversely, assume (1) and (2) hold for (X_i) and (ϕ_{ij}). Then we can define the mapping $\mathscr{X} : (I, \leq) \to \mathscr{C}$ by $i, j \in I$, $\mathscr{X}(i) = X_i$ and $\mathscr{X}(j \to i) = \phi_{ij}$. By (1), $\mathscr{X}(i \to i) = \phi_{ii} = 1_{X_i}$, so $\mathscr{X}$ carries identities. By (2), $\mathscr{X}(j \to i) \circ \mathscr{X}(k \to j) = \phi_{ij} \circ \phi_{jk} = \phi_{ik} = \mathscr{X}(k \to i)$, so $\mathscr{X}$ carries compositions. Hence $\mathscr{X}$ is a functor and $(X_i, \phi_{ij}, I, \leq)$ is an inverse system. □

The dual theorem exists for direct systems, where condition (1) becomes $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$.

We must stress that inverse limits are a special type of limits, not colimits, and direct limits of colimits, not limits. The reasons behind this questionable nomenclature are, as typical, of historical nature: algebraic definitions preceded the categorical ones. In existing literature, this situation is further complicated by two factors: firstly, although most authors [Wil98, RZ10, KVSN11, Wil] require the $\mathscr{I}$ category to be a directed poset, some require it to be just a poset [Bou95] or just a directed preordered[3] set [ML78, nLa21]. Secondly, when authors require directed sets, they disagree on whether they should be upward-directed [ML78, Wil98, RZ10, KVSN11] or downward-directed [Wil, nLa21], depending on how they define the direction of arrows in the index categories. To make the matter worse, some authors call the poset categories for directed sets *filtered* categories [ML78], while others call them *cofiltered* categories [MLM94].

For the purposes of this discussion, we chose to take inverse limits as limits on upward-directed posets, as in [Wil98, RZ10, KVSN11], to guarantee consistency with Definition 2.8. This matters little for examples presented, as they will generally be based on either lattices[4] or even totally ordered sets, which will work

[3] In this context, a preordered set is a poset without the antisymmetric property, i.e. there can be two $i, j \in I$ such that $i \leq j$ and $j \leq i$ but $i \neq j$.

[4] A lattice is a poset which is admits all finite meets and joins, or finite products and coproducts [nLa21]

with any formulation.

We will now work towards making the abstract notions we just defined more familiar. Firstly, we note that inverse and direct limits are unique in a very strong sense, as they are special cases of limits and colimits so Proposition 2.6 applies. This means that we can look for useful canonical representations of such objects which simplify our treatment. These will not exist in all categories, but fortunately they do in the categories that most interest us, like **Set**, **Grp**, **Top** and **TopGrp**.

Proposition 2.13. Let $\mathscr{C}$ be a concrete[5] category with arbitrary products. Any inverse limit of an inverse system (X_i, ϕ_{ij}, I) is isomorphic to

$$\left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \,\middle|\, \forall i,j \in I,\ i \leq j \implies \phi_{ij}(x_j) = x_i \right\}.$$

Proof. Let (X_i, ϕ_{ij}, I) be an inverse system and $X \subset \prod_i X_i$ the object defined in the statement. For each $j \in I$, let $\pi_j((x_i)_i) = x_j$ be the X restriction of the projection maps from $\prod_i X_i$. Let (Y, ψ_i) be another cone over the diagram $(I, \leq) \to \mathscr{C}$. Then since $\mathscr{C}$ has arbitrary products, we can construct the morphism

$$u : Y \ni y \mapsto (\psi_i(y))_{i\in I} \in X,$$

which clearly satisfies the properties in Definition 2.3. Hence X is a limit and by Proposition 2.6, it is isomorphic to any other limit. □

Dually, we have:

Proposition 2.14. Let $\mathscr{C}$ be a concrete category with arbitrary coproducts. Any direct limit of a direct system (X_i, ϕ_{ij}, I) is isomorphic to

$$\coprod_{i\in I} X_i \Big/ \sim,$$

where the equivalence relationship $\sim$ is given by $X_i \ni x_i \sim x_j \in X_j$ if and only if there exists some $k \in I$ such that $i, j \leq k$ and $\phi_{ik}(x_i) = \phi_{jk}(x_j)$.

2.0.1 Example: the Cantor set as an inverse limit

We will now provide a reference example of the inverse limit construction for a familiar object: the Cantor set, commonly referred to as Cantor's middle thirds set. It is usually represented as a subspace of the interval $[0, 1] \subseteq \mathbb{R}$ and constructed from the following sequence of sets: starting from the interval $[0, 1]$, we iteratively remove the middle third, obtaining $C_1 = [0, 1]$, $C_2 = [0, \frac{1}{3}] \cap [\frac{2}{3}, 1]$, $C_3 = [0, \frac{1}{9}] \cap [\frac{2}{9}, \frac{3}{9}] \cap [\frac{6}{9}, \frac{7}{9}] \cap [\frac{8}{9}, 1]$, etc [Sch97, Pg. 453]. The Cantor set is then the intersection $C := \bigcap_{n\in\mathbb{N}} C_n$ of the entire sequence of sets, equipped with the subspace topology.

There is an alternative way to view the Cantor set as the space of infinite binary sequences, equipped

[5] A concrete category is a category equipped with a faithful functor into **Set** [nLa21]. Informally, concrete categories are categories whose objects are sets with additional structure.

with product topology. Denote $\mathbf{2}^n$ the space $\{0,1\}^n$, equipped with the product topology, and consider the truncation maps:

$$\phi_{nm} : \mathbf{2}^m \ni (b_1, b_2, \ldots, b_n, \ldots, b_m) \mapsto (b_1, b_2, \ldots, b_n) \in \mathbf{2}^n,$$

for $n \leq m$[6]. By Proposition 2.12, $(\mathbf{2}^n, \phi_{nm}, \mathbb{N})$ is an inverse system. We identify its inverse limit with

$$\varprojlim_{n\in\mathbb{N}} \mathbf{2}^n = \left\{ (\mathbf{b}_n) \in \prod_{n\in\mathbb{N}} \mathbf{2}^n \;\middle|\; n \leq m \implies \phi_{nm}(\mathbf{b}_m) = \mathbf{b}_n \right\} \cong \mathbf{2}^{\mathbb{N}},$$

where $\mathbf{2}^{\mathbb{N}}$ is the countable product of $\{0,1\}$. It can be shown that this space is homeomorphic to the middle-third space C we constructed before[7]. Hence, starting from any finite binary string $\mathbf{b}_n$, we choose chains of compatible preimages $\mathbf{b}_m \in \phi_{nm}^{-1}(\{\mathbf{b}_n\})$, which build an infinite object. In this topology, how close two elements are is determined by how long their common prefix or initial substring of digits is. Thus, by leveraging inverse limits it is possible to glue together local structures into a global one. This will turn out to be incredibly powerful when group operations will be introduced.

2.0.2 Example: the infinite general linear group $GL_\infty(K)$

After having introduced the Cantor set as an example of an inverse limit, we will present the construction of the infinite general linear group $GL_\infty(K)$ as an example of a direct limit. To build this group of infinite invertible matrices, let K be a field and for each $n \in \mathbb{N}$, consider the multiplicative group $GL_n(K)$ of invertible n by n matrices with coefficients in K. Each $GL_n(K)$ be embedded in $GL_{n+1}(K)$ by the inclusion

$$\phi_{n,n+1} : GL_n(K) \ni M \mapsto \left[\begin{array}{c|c} M & 0 \\ \hline 0 & 1 \end{array}\right] \in GL_{n+1}(K),$$

which augments each matrix with an extra row and column of zeros, except for a one in the corner [nLa21, "Stable General Linear Group"]. This map can be applied inductively to obtain inclusions $\phi_{nm} : GL_n(K) \to GL_m(K)$ for any $n \leq m$. By the dual of Proposition 2.12, $(GL_n(K), \phi_{nm}, \mathbb{N})$ is a direct system with a direct limit

$$\varinjlim_{n\in\mathbb{N}} GL_n(K) = \bigsqcup_{n\in\mathbb{N}} GL_n(K) \Big/ \sim \; = GL_\infty(K),$$

where for any $n \leq m$, $GL_n(K) \ni M_n \sim M_m \in GL_m(K)$ if and only if $\phi_{nm}(M_n) = M_m$, i.e. if by augmenting the smaller matrix by ones, the two can be made equal. For example, in the disjoint union there are all the n by n identity matrices, which the equivalence relationship $\sim$ makes one. We call $GL_\infty(K)$ the infinite general linear group or the stable general linear group. As the name suggests, it carries a group structure, which is analysed in depth in "The Structure of the Infinite General Linear Group" by A. Rosenberg [Ros58].

[6] The notation for this example is inspired by [Mos]

[7] To get an intuition of why this is true, consider the base-3 representation $\sum_{k=0}^{\infty} \alpha_k 3^{-k}$ with $\alpha_k \in \{0,1,2\}$ of the elements of $C \subset [0,1]$. It is easy to show that C is exactly the subset of $[0,1]$ with no 1s in their base-3 representation, i.e. $\alpha_k \in \{0,2\}$. Thus their base-3 expansion may be described as an infinite binary sequence.

3 Topological Groups

This chapter will be dedicated to introducing the notion of topological groups. The study of these objects, although an immense area of research on its own, is related to our discussion of profinite groups by its necessity to deduce most meaningful results. In general, inferring properties of infinite groups without any additional structure is an incredibly hard task. The difference is as stark as trying to study $(\mathbb{R}, +)$ as a discrete topological space, versus studying it when equipped with the usual topology. Introducing a topological structure on a group can often yield significant insight into its algebraic structure. Let us move from the definition:

Definition 3.1. Let G be a group, equipped with a topology. We say G is a **topological group** if the maps

$$m : G \times G \ni (g, h) \mapsto gh \in G,$$
$$s : G \ni g \mapsto g^{-1} \in G,$$

are continuous[8].

We also need to specify a notion of equivalence for topological groups which is stronger than isomorphism or homeomorphism alone:

Definition 3.2. Let G and H be topological groups. We say G and H are **topologically isomorphic** or **isomorphic as topological groups** if there exists a bijective function $\phi : G \to H$ which is both a homeomorphism and an isomorphism of groups.

As the reader can expect, we are interested in taking inverse limits of such objects. For the purpose of this discussion we will think of topological groups as objects in their own category **TopGrp**, where the morphisms are continuous group homomorphisms [nLa21, "TopGrp"]. In this category, the product of a family of topological groups is given by the product group equipped with the product topology.

It is important to note that every group can be made into a topological group by equipping it with the discrete topology, hence we may view **Grp** as a subcategory of **TopGrp**. Since the discrete topology carries no additional useful information about the structure of the group in question, we call these groups **abstract**. We will prove a few useful results about topological groups that we will regularly use in future chapters. We start by considering the consequences which the group structure has on the topological structure:

Proposition 3.3. Let G be a topological group. Then G is **translation-invariant**, i.e. for every $g \in G$, $U \subseteq G$ the following are equivalent:

1. U is open,

[8] In the case of the map m, it has be continuous with respect of the product topology on $G \times G$

2. gU is open,

3. Ug is open.

Moreover, U is open if and only if U^{-1} is open.

Proof. This follows by apply the left and right multiplication by g homeomorphisms and the inversion homeomorphism. □

A critical consequence of this Proposition is the homogeneity property of topological groups:

Definition 3.4. Let X be a topological space and $\mathrm{Homeo}(X)$ be the set of homeomorphisms $X \to X$. We say X is a **homogeneous space under** $S \subseteq \mathrm{Homeo}(X)$, or simply that X is **homogeneous**, if for all $x, y \in X$, there exists an $f \in S$ such that $f(x) = y$.

Let $g, h \in G$ and consider the left multiplication homeomorphism $x \mapsto hg^{-1}x$, which takes g to h. Clearly, this shows that any topological group is homogeneous. Hence the topology of these groups can be entirely specified by an open base around the identity.

Definition 3.5. Let X be a topological space. A **neighbourhood base** for a point x is a set of neighbourhoods $\mathcal{N}$ of x such that each open set U containing x contains an $N \in \mathcal{N}$.

Open neighbourhood bases will play an important role in characterising the topology of profinite groups, and in particular in the proof of the infinite Fundamental Theorem of Galois Theory. In this regard, the following lemma allows us to reconstruct a topology from a neighbourhood base:

Lemma 3.6. Let G be a topological group and $\mathcal{N}$ an neighbourhood base for the identity e of G. Then

1. For all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subseteq N_1 \cap N_2$,

2. For all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N'N' \subseteq N$,

3. For all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N' \subseteq N^{-1}$,

4. For all $N \in \mathcal{N}$ and all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $N' \subseteq gNg^{-1}$,

5. For all $g \in G$, $\{gN \mid N \in \mathcal{N}\}$ is neighbourhood base for g.

Conversely, if G is a group and $\mathcal{N}$ is a non-empty set of subsets of G satisfying (1,2,3,4), then there is a unique topology on G for which (5) holds.

Proof. See Proposition 7.2 in Chapter 7 of "Field and Galois Theory" by J. S. Milne [Mil20b]. □

We will conclude this chapter by introducing three results regarding the relationship between open and closed subgroups in topological groups. These will be critical to proving many properties of profinite

groups. The first Proposition relates open subgroups to closed subgroups:

Proposition 3.7. Let G be a topological group. Every open subgroup is closed.

Proof. Let H be an open subgroup of G. By homogeneity, any coset gH is open. Thus

$$Y = \bigcup_{g \in G \setminus H} gH$$

is also open. From elementary group theory, $H = G \setminus Y$, so H is closed. □

The second Proposition relates closed subgroups of finite index subgroups to open subgroups:

Proposition 3.8. Let G be a topological group and H a subgroup. If H is closed and of finite index, H is open.

Proof. Let $n = [G : H]$. Since H is of finite index, there exists $e = g_1, g_2, \ldots, g_n \in G$ such that

$$G = \bigsqcup_{i=1}^{n} g_i H.$$

Consider $\phi_i : g \mapsto g_i^{-1} g$. Clearly, ϕ_i is continuous and $g_i H = \phi_i^{-1}(H)$, hence $g_i H$ is closed. Thus the finite union

$$K = \bigsqcup_{i=2}^{n} g_i H$$

is closed and $H = G \setminus K$ is open. □

The third Proposition applies only to compact topological groups and relates open subgroups, which we have already shown to be closed, to finite index subgroups. We omit the proof for brevity.

Proposition 3.9. Let G be a compact topological group and H a subgroup. If H is open, H is of finite index.

Proof. See Proposition 1.4 in Chapter 1 of "Fourier Analysis on Number Fields" by D. Ramakrishnan, et al. [RV99]. □

4 Profinite Groups

This chapter will tie together the theory developed in the previous chapters regarding inverse limits and topological groups to finally introduce the notion of profinite groups. We will organise our discussion as follows: we will first define profinite groups and establish their basic properties as topological groups. Then we will present profinite completions, which assign to each group a corresponding profinite group in which it can be embedded. The rest of the chapter is dedicated to topics relating to the order of a profinite group and its generators. There we will present the profinite equivalent of Sylow's Theorems, the classification of procyclic groups and the Frattini subgroups, which will allow us to characterise the generators of profinite groups. Each section will present examples relevant to the theory introduced.

4.1 Construction

Let us move to define profinite groups:

Definition 4.1. A **profinite group** is an inverse limit of an inverse system of finite groups.

In this definition, the finite groups are to be taken as topological spaces with discrete topology and the transition maps as continuous group homomorphisms, i.e. as objects and morphisms in **TopGrp**. We can similarly define profinite rings, modules and other algebraic objects, or pro-p, pronilpotent and prosolvable groups. By Proposition 2.13, since **TopGrp** is a category with arbitrary products, for any inverse system of finite groups (G_i, ϕ_{ij}, I), there is a canonical representative in the equivalence class of inverse limits up to topological isomorphism, i.e.

$$\varprojlim_{i\in I} G_i = \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; \forall i,j \in I,\ i \leq j \implies \phi_{ij}(g_j) = g_i \right\}.$$

We will generally deal with profinite groups as written in this form. It follows that the group multiplication operation is inherited from the product group. Hence we can easily show that profinite groups are indeed groups:

Proposition 4.2. Non-empty profinite groups are groups.

Proof. Let G be a non-empty inverse limit of an inverse system of finite groups (G_i, ϕ_{ij}, I). Associativity follows from the product group operation. To prove multiplication is closed, we need to show that for $(g_i)_{i\in I}(h_i)_{i\in I} \in G$, we have $(g_i) \circ (h_i) = (g_i \circ h_i) \in G$. Since each ϕ_{ij} is a homomorphism, we have

$$\phi_{ij}(g_j \circ h_j) = \phi_{ij}(g_j) \circ \phi_{ij}(h_j) = g_i \circ h_i,$$

as desired. Similarly, it is easy to see that the identity element (e_i) is in G and that for all $(g_i) \in G$, the inverse $(g_i)^{-1}$ is given by $(g_i^{-1}) \in G$. □

We are yet to show that such non-empty profinite groups actually exist, or whether they are common at all. We will take care of this in the next section, where we will introduce the profinite topology.

4.2 Properties as Topological Groups

This section is dedicated to the properties of profinite groups as topological groups[9]. From the structure of $\varprojlim_{i\in I} G_i$ suggested by Proposition 2.13, we have a natural topology for profinite groups:

Definition 4.3. Let $(G_i)_{i\in I}$ be an inverse system of finite groups. Endow each G_i with a discrete topology and $\prod_i G_i$ with the product topology. The **profinite topology** on $\varprojlim G_i \subseteq \prod G_i$ is the subspace topology.

However, we still haven't proved that these objects aren't all degenerate. We establish this critical result now:

Proposition 4.4. Let (X_i, ϕ_{ii}, I) be an inverse system of non-empty finite sets, equipped with the discrete topology. Then $\varprojlim X_I$ is non-empty.

Proof. If we equip each X_i with the discrete topology, by Tychonoff's Theorem $\prod_i X_i$ is compact and since $\varprojlim_{i\in I} X_i$ can be written as the intersection of closed sets, it is also compact. Let $J_k \subseteq I$ be any finite subset and let

$$Y_{J_k} = \varprojlim_{i\in J_k} X_i = \left\{ (x_i) \in \prod_{i\in J_k} \,\middle|\, i \leq j \implies \phi_{ij}(x_j) = x_i \right\}.$$

It is easy to see that Y_{J_k} is closed in $\prod_{i\in I} X_i$ and

$$Y_{J_1} \cap Y_{J_2} \cap \cdots \cap Y_{J_n} \supseteq Y_{J_1 \cup J_2 \cup \cdots \cup J_n}.$$

We wish to prove now that each Y_{J_k} is non-empty. Since I is directed and J_k is finite, we can find some $i_0 \in J_k$ such that for all $i \in J_k$ we have $i \leq i_0$. Choose some $x_{i_0} \in X_{i_0}$ and set $x_i = \phi_{i,i_0}(x_{i_0})$ for all $i \in J_k$. By choosing $x_i \in X_i$ arbitrarily for $i \in I \setminus J_k$ we can construct an element in Y_{J_k}.

Hence, Y_{J_k} are non-empty and we can apply the Finite Intersection Property to conclude that the intersection over all such partitions of I is non-empty. Since this intersection is exactly $\varprojlim_{i\in I} X_i$, we have proved the claim [Wil, Prop. 1.2.14]. □

Hence, since each group contains at least the identity element, every inverse limit of inverse systems of finite groups will be non-empty and thus a valid group, as we established previously. As for their order, it can be shown that profinite groups are either finite or uncountable. Thus, we now have a group structure and a topological structure for profinite groups, but not evidence that the two structures are compatible, i.e. that profinite groups are topological groups. This result, albeit critical, is rather immediate:

[9] This section will largely follow Section 1.2 of "Profinite Groups and Group Cohomology" by G. Wilkes [Wil]

Theorem 4.5. Profinite groups are topological groups when endowed with the profinite topology.

Proof. Let G be a profinite group and $m : G \times G \to G$, $s : G \to G$ the multiplication and inversion maps. Consider the subbase of G given by $U_{i,g} = \pi_i^{-1}(\{g_i\})$ for $i \in I$ and $(g_i) \in G$. Then we have $s^{-1}(U_{i,g}) = U_{i,g^{-1}}$ and

$$m^{-1}(U_{i,g}) = \bigcup_{h \in G} U_{i,h} \times U_{i,h^{-1}g},$$

which is open in $G \times G$. Hence s and m are continuous and G is a topological group [Wil, Prop. 1.2.19]. □

Since we have established that profinite groups are indeed topological groups, we can move to better characterise their structure. A remarkable property of profinite groups is that the topology arising from the inverse limit of finite groups is, in a way, rather unique among topological groups. Let us make this precise:

Theorem 4.6. A profinite group is compact, Hasudorff and totally disconnected.

Proof. Let G_i be an inverse system of finite groups with inverse limit G. As we've seen in Proposition 4.4, G is compact by Tychonoff's Theorem.

To prove G is Hausdorff, we consider distinct $g, h \in G$, i.e. there exists some $i \in I$ such that $\pi_i(g) \neq \pi_i(h)$. Then since G_i is Hausdorff we can find open sets $U, V \subseteq G_i$ such that $\pi_i(g) \in U$, $\pi_i(h) \in V$ and $U \cap V = \emptyset$. Since $\pi_i^{-1}(U), \pi_i^{-1}(V)$ are open in G, it is Hausdorff.

To prove G is totally disconnected, we again consider distinct $g, h \in G$ such that $\pi_i(g) \neq \pi_i(h)$. Since G_i is totally disconnected, we can find a clopen set $U \subset G_i$ such that $\pi_i(g) \in U$ and $\pi_i(h) \notin U$. Since $\pi_i^{-1}(U)$ is clopen in G, it is totally disconnected [RZ10, Prop. 1.1.3]. □

The converse also holds, although we will not prove it.

Theorem 4.7. A topological group which compact, Hausdorff and totally disconnected is topologically isomorphic to a profinite group.

Proof. See Theorem 1.1.12 in Chapter 1 of "Profinite Groups" by L. Ribes [RZ10]. □

We have thus found an alternative characterisation of profinite groups, which does not rely on inverse limits. We will make use of this alternative definition when dealing with infinite Galois Theory.

The following two results which relate the global topology on the inverse limit to the topology on each projection. We will omit of the proof the second statement for brevity.

Proposition 4.8. Let H be a topological group and let $G = \varprojlim_{i\in I} G_i$ a profinite group with projections $\pi_i : G \to G_i$. A homomorphism $\psi : H \to G$ is continuous if and only if every composition $\psi_i = \pi_i \circ \psi : H \to G_i$ is continuous.

Proof. This follows from the definition of product topology on $\prod_i G_i \supseteq G$. □

Proposition 4.9. Let (X_i, ϕ_{ij}) be an inverse system of compact Hausdorff spaces with inverse limit X and projection mappings $\pi_i : X \to X_i$. If Y is a subspace of X, then $\varprojlim_{i\in I} \pi_i(Y) = \overline{Y}$ is the closure of Y.

Proof. See Corollary 1.1.8 in Chapter 1 of "Profinite Groups" L. Ribes [RZ10]. □

To aid our understanding of the profinite topology, we can look for a reference open neighbourhood basis. Luckily, there is one such basis that is particularly nice to work with:

Theorem 4.10. Let $(G_i)_{i\in I}$ be an inverse system of finite groups with inverse limit G. The open subgroups $U_i = \ker(\pi_i : G \to G_i)$ form an open neighbourhood basis of the identity consisting of normal subgroups, i.e. every open set $V \subseteq G$ containing the identity contains some U_i.

Proof. Consider the family of neighbours of the identity e in $\prod_i G_i$ of the form

$$\left(\prod_{i\neq i_1,\dots,i_k} G_i\right) \times \{e_{i_1}\}_{i_1} \times \cdots \times \{e_{i_k}\}_{i_k},$$

for any finite subset $i_1, \dots, i_k \subseteq I$, where $\{e_{i_1}\}_{i_1}$ denotes the subset of G_{i_1} containing the identity element. Since each G_i is discrete, it is easy to convince ourselves that this is indeed an open neighbourhood basis of the identity of $\prod_i G_i$. Consider now some $i_0 \in I$ such that $i_1, \dots, i_k \leq i_0$, which we can always find since I is directed. Then we have

$$G \cap \left[\left(\prod_{i\neq i_0} G_i\right) \times \{e_{i_0}\}_{i_0}\right] = G \cap \left[\left(\prod_{i\neq i_1,\dots,i_k} G_i\right) \times \{e_{i_1}\}_{i_1} \times \cdots \times \{e_{i_k}\}_{i_k}\right],$$

hence the family of open neighbours of the identity e of G of the form

$$G \cap \left[\left(\prod_{i\neq i_0} G_i\right) \times \{e_{i_0}\}_{i_0}\right] = \ker(\pi_{i_0} : G \to G_{i_0})$$

is a basis [RZ10, Lemma 2.1.1]. □

This neighbourhood basis of the identity can be generalised to the whole group by homogeneity:

Corollary 4.10.1. Let $(G_i)_{i\in I}$ be an inverse system of finite groups with inverse limit G and let $g = (g_i) \in G$. Then the open cosets $gU_i = \pi_i^{-1}(\{g_i\})$ form an open neighbourhood basis of g.

Moreover, a characterisation of dense subsets also follows from the previous Theorem:

Corollary 4.10.2. Let $(G_i)_{i\in I}$ be an inverse system of finite groups with inverse limit G. A subset $X \subseteq G$ is dense in G if and only if for all $i \in I$, we have $\pi_i(X) = \pi_i(G)$.

Proof. Assume X is not dense in G. Then we can find some non-empty open set U such that $X \cap U = \emptyset$. Without loss of generality, we can take U to be a basic open set of the form $\pi_i^{-1}(\{g_i\})$ for some $i \in I$ and $g_i \in G_i$, given that we can always shrink non-basic open sets. Since U is non-empty, $g_i \in \pi_i(G)$ and since $X \cap U = \emptyset$, we have $g_i \notin \pi_i(X)$, which proves $\pi_i(X) \neq \pi_i(G)$.

Assume now that X is dense in G. Then for every $g_i \in \pi_i(G)$, the open set $\pi_i^{-1}(\{g_i\})$ is non-empty and thus intersects with X. So $g_i \in \pi_i(X)$ and we have $\pi_i(G) \subseteq \pi_i(X)$, which proves $\pi_i(X) = \pi_i(G)$ [Wil, Cor. 1.2.30]. □

In studying a new class of topological groups, it is often useful to determine whether they are closed under products and quotients. For profinite groups, the following hold:

Proposition 4.11. Let G_i be a family of profinite groups indexed by some set I. Then the direct product $\prod_i G_i$ is a profinite group when equipped with the product topology.

Proof. Let $G = \prod_i G_i$. Since each G_i is profinite, G is compact, Hausdorff and totally disconnected. By Theorem 4.7, G is profinite [RZ10, Prop. 2.2.1]. □

Proposition 4.12. Let G be a profinite group and H a closed normal subgroup of G. Then G/H is a profinite group when equipped with the quotient topology.

Proof. See Proposition 2.2.1 in Chapter 2 of "Profinite Groups" by L. Ribes [RZ10, Prop. 2.2.1]. □

Before moving onto an example, we present a final result relating closed and open subgroups, to complement the ones introduced in the previous chapter.

Proposition 4.13. Let H be a closed subgroup of a profinite group G. Then H is the intersection of all open subgroups of G containing H.

Proof. See Proposition 2.2.4 in Chapter 2 of "Profinite Groups" by L. Ribes [RZ10]. □

4.2.1 Example: the p-adic integers $\mathbb{Z}_p$

As a first motivational example of profinite groups, we present here the p-adic integers[10]. Their ring is an object whose relevance in modern number theory is hard to overstate. We will show in this example some of the properties that make this object so interesting.

[10] The discussion of this example largely follows Section 2.1 of "Profinite Groups and Group Cohomology" by G. Wilkes [Wil]

Let p be a prime number and consider the inverse system given by the rings $\mathbb{Z}/p^i\mathbb{Z}$ for $i \in \mathbb{N}$:

$$\cdots \longrightarrow \mathbb{Z}/p^{i+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z} \longrightarrow \cdots \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

where the homomorphisms are the modulo reductions $\phi_{ij} : [a]_{p^j} \mapsto [a]_{p^i}$ for $i \leq j$. We call the inverse limit of such inverse system the ring of **p-adic integers**, denoted $\mathbb{Z}_p$[11,12].

Before proving facts about $\mathbb{Z}_p$, it is important to understand what its elements look like. By the inverse limit characterisation we built in Proposition 2.13, we can describe any element $\alpha \in \mathbb{Z}_p$ as a sequence $\alpha = (a_i)_{i\in\mathbb{N}}$ of elements each in $\mathbb{Z}/p^i\mathbb{Z}$, subject to the compatibility conditions of modulo reduction, i.e. for any $i \leq j$, $a_i \equiv a_j \mod p^i$ [Wil, Pg. 20]. For example, we can include any integer $a \in \mathbb{Z}$ into the ring $\mathbb{Z}_p$ by just taking $\alpha = (a + p^i\mathbb{Z})_{i\in\mathbb{N}} \in \mathbb{Z}_p$, i.e. the sequence of reductions of a modulo all p^i. We will see that this ring contains more than just the integers.

Regarding the ring structure, we are still to show how one can perform ring operations with these elements. By generalising the proof of Proposition 4.2 to rings, we have for any $(a_i), (b_i) \in \mathbb{Z}_p$, addition is given by $(a_i) + (b_i) = (a_i + b_i)_{i\in\mathbb{N}}$ and multiplication by $(a_i) * (b_i) = (a_i * b_i)_{i\in\mathbb{N}}$, i.e. the operations are carried component-wise. Note that if $\alpha = (a_i) \in \mathbb{Z}_p$, we will sometimes write $\alpha \equiv a_i \mod p^i$ for $\pi_i(\alpha) = a_i$.

Let us turn to the topology now. By Theorem 4.10, we have an open neighbourhood basis of the identity given by $\ker(\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}) = p^i\mathbb{Z}_p$. Noting that this basis is countable and can be ordered by inclusion, since $p^{i+1}\mathbb{Z} \subseteq p^i\mathbb{Z}$, it may seem natural to search for a compatible metric which has $p^i\mathbb{Z}$ as open ball around the identity $0 \in \mathbb{Z}_p$. Consider the ansatz $d : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}_{\geq 0}$ given for any $(a_i), (b_i) \in \mathbb{Z}_p$ by $d((a_i), (b_i)) = 0$ if for all $i \in \mathbb{N}, a_i \equiv b_i \mod p^i$ and $d((a_i), (b_i)) = p^{-n}$ where $n = \min\{n \in \mathbb{N} \mid a_n \not\equiv b_n \mod p^n\}$ [Wil, Pg. 20]. Note that n is well-defined since every non-empty subset of $\mathbb{N}$ is well-ordered. It is easy to check that d is indeed a metric on $\mathbb{Z}_p$, which is also translation-invariant, thus respecting the addition operation.

We now want to justify calling d the p-adic metric. To this end, consider the open balls of radius $0 < r < 1$ around the identity $0 \in \mathbb{Z}_p$:

$$\begin{aligned} B_r^d(0) &= \{(a_i) \in \mathbb{Z}_p \mid d(\alpha, 0) < r\} \\ &= \{(a_i) \in \mathbb{Z}_p \setminus \{0\} \mid i \leq -\log_p(r) \implies a_i \equiv 0 \mod p^i\} \\ &= \ker(\pi_{\lfloor -\log_p(r)\rfloor} : \mathbb{Z}_p \to \mathbb{Z}/p^{\lfloor -\log_p(r)\rfloor}\mathbb{Z}), \end{aligned}$$

which coincide with our open neighbourhood basis [Wil, Pg. 21]. By homogeneity, the topology on $\mathbb{Z}_p$

[11] Some authors denote the p-adic integers as $\hat{\mathbb{Z}}_p$ [Ber15]. Although this notation is rarer, there is an argument to be made that it would be more consistent with a general notation for pro-p completions, which will be introduced in later chapters.

[12] If we considered the morphisms $\mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^{i+1}\mathbb{Z}$ which act as multiplication by p, we could build a dual group through the direct limit construction. This is known as the p-quasicyclic group $\mathbb{Z}_{p^\infty}$ and it can be shown to be the dual of $\mathbb{Z}_p$ under the formalism of the Pontryagin Duality, which we will not discuss for brevity. The interested reader is referred to Section 2.9 of "Profinite Groups" by L. Ribes [RZ10]

induced by d is the profinite topology, hence we can rightfully call d the **p-adic metric**.

We can show that the inclusion of the integers $\iota(\mathbb{Z})$ is a dense in $\mathbb{Z}_p$ by considering for every $(a_i) \in \mathbb{Z}_p$ and $\varepsilon > 0$, an $n > -\log_p(\varepsilon)$ and taking $a \in \mathbb{Z}$ such that $a \equiv a_n \mod p^n$, which satisfies $d(\iota(a), (a_i)) = p^{-n} < \varepsilon$ [Wil, Pg. 21]. On the other hand, $\mathbb{Z}_p$ is much bigger than $\mathbb{Z}$: in fact, it can be shown that $\mathbb{Z}_p$ has the cardinality of the continuum. As consequence of Theorem 4.6, since $(\mathbb{Z}_p, d)$ is a compact metric space, it is also complete. Moreover, for any element $\alpha = (\alpha_i) \in \mathbb{Z}_p$ we can construct a sequence of integers $b_i \in \mathbb{Z}$ such that $b_i \equiv a_i \mod p^i$ and hence $\alpha = \lim_{i \in \mathbb{N}} \iota(b_i)$[13]. Thus $\mathbb{Z}_p$ is the metric completion of $\mathbb{Z}$ with respect to the p-adic metric[14].

The metric d that we defined has the interesting property of obeying a stronger version of the triangle inequality: for any three $\alpha, \beta, \gamma \in \mathbb{Z}_p$, we have $d(\alpha, \beta) \leq \max\{d(\alpha, \gamma), d(\gamma, \beta)\}$. We call metrics obeying this property **ultrametrics**. Similarly to how we defined real norm $||\cdot||_\infty : x \mapsto d(x, 0)$, we can define a norm $||\cdot||_p$ on $\mathbb{Z}_p$, which we say is **non-Archimedean**, since d is an ultrametric [Kob84, Pg. 3]. There is a sense in which these are the only interesting metrics we can define on $\mathbb{Q}$. We will move to make this more precise.

From our ring p-adic integers $\mathbb{Z}_p$ we can construct the field of p-adic numbers $\mathbb{Q}_p$ in two equivalent ways: either as the field of fractions of $\mathbb{Z}_p$ or as the completion of $\mathbb{Q}$ with respect to the extension of the p-adic metric. The properties of this field are beyond the scope of this discussion, but it is worth mentioning the following theorem by Ostrowski, which partially explains the importance of this field in modern number theory[15]:

Theorem 4.14. Every non-trivial[16] norm $||\cdot||$ on $\mathbb{Q}$ is equivalent to either $||\cdot||_\infty$ or $||\cdot||_p$ for some prime p.

Proof. See Remark 7.49 in Chapter 7 of "Algebraic Number Theory" by J. S. Milne [Mil20a] for a sketch of the proof or Theorem 1 in Chapter 2 of "p-adic Numbers, p-adic Analysis, and Zeta Functions" by N. Koblitz [Kob84] for the full proof. □

Returning to our p-adic integers $\mathbb{Z}_p$, let us consider the application of p-adic arithmetic to the solvability of integer polynomial equations, which when they involve two or more variables are usually called **Diophantine equations**. Restricting ourselves to a prototypical example with a single variable, consider the equation $x^2 + 1 = 0$ [Ber15]. Clearly this has no solution over $\mathbb{Z}$, but we can quickly solve it over $\mathbb{Z}/5\mathbb{Z}$, finding that either $x \equiv 2$ or $x \equiv 3 \mod 5$. Let us say that we decide that $x \equiv 2 \mod 5$ and we want to extend or lift this solution to a compatible one modulo 5^2, i.e. $x^2 + 1 \equiv 0 \mod 5^2$ and $x \equiv 2 \mod 5$. Through Hensel's Lemma, we find that $x \equiv 7 \mod 5^2$ and successively $x \equiv 57 \mod 5^3$, and so

[13] Here the limit is taken in $(\mathbb{Z}_p, d)$.
[14] This should not be confused with the profinite completion we will define in the next chapter.
[15] Since $\mathbb{Q}_p$ is a locally compact field, many techniques from real analysis can be employed in its study. We refer the interested reader to the discussion in "p-adic Numbers: An Introduction" by F. Q. Gouvea [Gou97].
[16] A norm $||\cdot|| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is trivial if $||x|| = 0$ for $x = 0$ and $||x|| = 1$ otherwise.

on up to arbitrary 5^n, as represented by the following diagram:

$$\cdots \longrightarrow 182 + 5^4\mathbb{Z} \longrightarrow 57 + 5^3\mathbb{Z} \longrightarrow 7 + 5^2\mathbb{Z} \longrightarrow 2 + 5\mathbb{Z}$$

Hence, even though we could not solve this equation in $\mathbb{Z}$, we can find a sequence of local solutions $(2, 7, 57, 182, \dots)$ which define an element of $\mathbb{Z}_5$. In a sense, we found a global solution to $x^2 + 1 = 0$ in $\mathbb{Z}_p$, which, although is not an integer, can be approximated by integers up to arbitrary precision. This construction by lifting is formalised by the p-adic Hensel's Lemma:

Lemma 4.15. For p prime, let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. Let $r \in \mathbb{Z}_p$ and $k \in \mathbb{N}$ such that $f(r) \equiv 0 \mod p^k$ and $f'(r) \not\equiv 0 \mod p$[17]. Then there exists a unique $\rho \in \mathbb{Z}_p$ such that $f(\rho) = 0$ and $\rho \equiv r \mod p^k$.

Proof. See Proposition 4.4.7 in "Profinite Groups and Group Cohomology" by G. Wilkes [Wil]. □

This result can also be generalised to multivariate polynomials, i.e. Diophantine equations [Zha15]. Note that the solvability of our example equation depends on the prime p: it is easy to verify that there is no square root of -1 in $\mathbb{Z}_3$ or $\mathbb{Z}_7$. But given how much easier it is to check solutions modulo p and lift them, applying this procedure for every p may sometimes be a viable strategy to check solvability over $\mathbb{Z}$ or $\mathbb{Q}$. This is known in algebraic geometry as **Hasse's local-global principle**, which for quadratic forms, i.e. homogeneous second degree polynomials, takes the form of the Hasse-Minkowski Theorem:

Theorem 4.16. Let $Q(x_1, \dots, x_n)$ be a quadratic form over $\mathbb{Q}$ in any dimension $n \geq 1$. Then

1. Given $r \in \mathbb{Q}^\times$, the equation $Q(x_1, \dots, x_n) = r$ is solvable over $\mathbb{Q}$ if and only if it is solvable over $\mathbb{R}$ and every $\mathbb{Q}_p$,
2. The equation $Q(x_1, \dots, x_n) = 0$ is non-trivially solvable over $\mathbb{Q}$ if and only if it is non-trivially solvable over $\mathbb{R}$ and every $\mathbb{Q}_p$.

Proof. See Theorem 4.1 in Chapter 4 of "The Hasse-Minkowski Theorem" by A. Gazon [Gam06]. □

To conclude this section, we can apply the Hasse-Minkowski Theorem to the equation given in the previous example $x^2 + 1 = 0$. By rewriting it into $x^2 = -1$, we can identify the 1-dimensional quadratic form $Q(x_1) = x_1^2$ over $\mathbb{Q}$. Since any solution over $\mathbb{Q}_p$ must have p-adic norm $||x||_p = 1$, it must lie in $\mathbb{Z}_p$. Moreover, we already established that the equation has no solution over $\mathbb{Z}_3$, thus by the Hasse-Minkowski Theorem it is not solvable over $\mathbb{Q}$. This is of course to be expected from our understanding of complex numbers.

[17] Here $f'(x)$ represents the formal derivative of $f(x)$, i.e. let $f(x) = \sum_{k=0}^{n} a_k x^k$, then $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$.

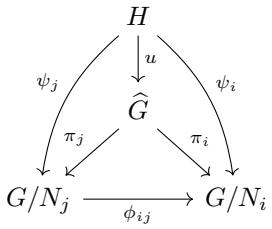
4.3 Profinite Completions

We have seen in the previous example that profinite groups may be assembled out of quotients of an abstract group. The procedure results in a bigger object[18], in which we may embed the original group. This chapter will be dedicated to formalising this procedure, known as the **profinite completion**, and derive its most salient properties. As in the $\mathbb{Z}_p$ example, we start with an abstract group:

Definition 4.17. Let G be an abstract group and (N_i) the family of finite index normal subgroups of G indexed by some set I. We call the **profinite completion** of G, denoted $\widehat{G}$, the inverse limit of the inverse system $(G/N_i, \phi_{ij}, I)$, where $\phi_{ij} : G/N_j \to G/N_i$ is the quotient map for $N_j \subseteq N_i$.

Here we note the first difference with the construction of $\mathbb{Z}_p$: we consider every finite index normal subgroup, not just some of them. Hence $\mathbb{Z}_p$ is not the profinite completion of $\mathbb{Z}$, but rather its **pro-p completion**, where the inverse limit is taken only over the normal subgroups which have index p^n for some $n \in \mathbb{N}$. The actual profinite completion of $\mathbb{Z}$ will be studied as the example at the conclusion of this section.

We can alternatively characterise the profinite completion as the solution to the universal problem represented by the following diagram [Wil, Defn. 1.2.1]:



where H is any group admitting homomorphisms $\psi_i : H \to G/N_i$. Note that G satisfies these conditions, so we have a natural homomorphism $\iota : G \to \widehat{G}$, mapping $g \in G$ to $(gN_i) \in \widehat{G}$ [Wil, Rem. 1.2.2]. An obvious problem to pose at this point is to determine under which conditions this embedding is injective. It is useful here to introduce the following definition:

Definition 4.18. Let G be an abstract group. We say G is **residually finite** if the intersection of all its finite-indexed normal subgroups is trivial.

It is easy to show the following:

Proposition 4.19. Let G be an abstract group. Then $\iota : G \to \widehat{G}$ is injective if and only if G is residually finite.

Proof. Assume G is not residually finite, i.e. there exists some $g \in \bigcap_i N_i$ distinct from the identity e. Then $\iota(g) = (gN_i) = (eN_i) = \iota(e)$, thus ι is not injective.

[18] The completion is only bigger when the abstract group has enough finite index normal subgroups. For example, the profinite completion of $\mathbb{R}$ is the trivial group.

Assume now G is residually finite. Then for every $g \in G$ distinct from the identity e, there exists some $i \in I$ such that $g \notin N_i$. Hence $g \notin \ker(\iota)$ and ι is injective. □

Many groups we are familiar with are residually finite. For instance, it can be shown that finitely generated abelian groups are residually finite [Wil, Prop. 3.1.7]. Moreover, every subgroup of a residually finite group is residually finite, and a partial converse holds if the subgroup is of finite index [Wil, Prop. 3.1.4].

A very useful property that we discovered in our $\mathbb{Z}_p$ example was the ability to approximate elements of $\mathbb{Z}_p$ by elements of $\mathbb{Z}$. This is a general feature of profinite completions:

Proposition 4.20. Let G be an abstract group. Then $\iota(G)$ is dense in $\widehat{G}$.

Proof. For all $i \in I$, the image of $\iota(G)$ under the projection map $\pi_i : \widehat{G} \to G/N_i$ is

$$\pi_i(\iota(G)) = G/N_i = \pi_i(\widehat{G}),$$

hence the result follows by Corollary 4.10.2 [Wil, Rem. 3.1.1]. □

Moreover, it is possible to show that profinite completions act as a functor, carrying not only groups to profinite groups, but also group homomorphisms to continuous profinite group homomorphisms.

Lemma 4.21. Let $\psi : G \to H$ be a group homomorphism. There exists a unique continuous homomorphism $\widehat{\psi} : \widehat{G} \to \widehat{H}$.

Proof. See Lemma 3.2.1. in Chapter 3 of "Profinite Groups" by L. Ribes [RZ10]. □

We must now to turn the question of what happens if we take the profinite completion of a profinite group. Surprisingly enough, the completion would not always be isomorphic to starting group. From the definition, we can see that it suffices for G to have a non-open normal subgroup for it to be non-isomorphic to its completion. We have a special name for profinite groups exempt from this problem:

Definition 4.22. Let G be a profinite group. We say G is **strongly complete** if every subgroup of finite index in G is open.

Determining which classes of profinite groups are strongly complete is a highly non-trivial task. For example, the following result was proved only recently by N. Nikolov and D. Segal.

Theorem 4.23. Every finitely generated profinite group is strongly complete.

Proof. See Theorem 1.1 in "On Finitely Generated Profinite Groups, I: Strong Completeness and Uniform Bounds" by N. Nikolov, et al. [NS07]. □

For an example of a profinite group which is not strongly complete, we can follow the construction given in "Non-open subgroups of finite index" in Chapter 7 of "Fields and Galois Theory" by J. S. Milne [Mil20b]. This example was originally given in the context of Galois theory, but we will present it in the equivalent profinite form. We first need to introduce the following Proposition:

Proposition 4.24. Let V be an infinite-dimensional vector space. For all $n \in \mathbb{N}$, there exists a subspace V_n of V such that V/V_n has dimension n.

Proof. By Zorn's Lemma, V contains maximal linearly independent subsets, which can be shown to be spanning V. Hence we can choose a basis for V and take V_n to be the subspace spanned by the set obtained by removing n elements from the basis [Mil20b, Lemma 7.25]. □

Proposition 4.25. Let $G = \prod_{n\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ be the product of countable copies of $\mathbb{Z}/2\mathbb{Z}$, viewed as a profinite group[19]. Then for all $n \in \mathbb{N}$, G has a non-open normal subgroup of index 2^n.

Proof. Let H be the subset of G defined as

$$H = \{(g_n)_{n\in\mathbb{N}} \in G \mid g_n = 0 \text{ for all but finitely many } n\}.$$

Clearly H is a subgroup of G. Moreover H is dense in G since every element $(g_n) \in G$ can be approximated by the sequence

$$(g_1, 0, 0, 0, \dots), (g_1, g_2, 0, 0, \dots), (g_1, g_2, g_3, 0, \dots), \dots,$$

of elements in H. Regarding the quotient group G/H as a vector space over $\mathbb{F}_2$, we can apply Propisition 4.24 to construct subgroups G_n with index 2^n in G containing H. If G_n were open in G, by Proposition 3.7, it would be closed. But since $H \subseteq G_n$, G_n would be G itself, which is a contradiction. Hence G_n is a non-open normal subgroup of index 2^n in G [Mil20b, Prop. 7.26]. □

Hence the profinite completion of $\prod_{n\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ is definitely going to be a significantly bigger object.

Furthermore, two groups may have the same profinite completion and be non-isomorphic. We will not present an example here, but the interested reader is recommended to "The classifications of countably based profinite abelian groups" by J. Kiehlmann [Kie12] for construction of infinitely many topologically non-isomorphic profinite groups isomorphic to $\prod_{i\in I} \mathbb{Z}/p^i\mathbb{Z}$, with the same profinite completion [Kie12, Pg. 1].

4.3.1 Example: the profinite integers $\hat{\mathbb{Z}}$

Having developed significant theoretical results on profinite completions, we will focus on the example of the profinite completion of the ring of integers $\mathbb{Z}$. Moving to construct the inverse system, we note that every non-trivial additive subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for some $n \in \mathbb{N}$. Since we have $[\mathbb{Z} : n\mathbb{Z}] = n$ and $\mathbb{Z}$ is abelian, all subgroups are of finite index and normal. From elementary ring theory we find that

[19] To see G as a profinite group, consider the inverse system given in Example 2.0.1 for the Cantor set.

there exists a non-trivial ring homomorphism $\phi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ if and only if n divides m, hence will use $(\mathbb{N}, |)$ as the index poset. It follows that

$$\hat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z},$$

is the profinite completion of $\mathbb{Z}$, which we will call, unsurprisingly, the ring of **profinite integers**. Since we are interested in knowing whether the inclusion mapping is injective, we need to prove residual finiteness of $\mathbb{Z}$:

Proposition 4.26. $\mathbb{Z}$ is residually finite.

Proof. Every finite index additive subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Let $a \in \mathbb{Z}$ be an integer distinct from 0 and ± 1. By the Fundamental Theorem of Arithmetic we can write it as a product of distinct primes $a = \pm p_1^{l_1} \cdots p_k^{l_k}$ and by Euclid's Theorem we can find a prime q distinct from all p_i, for $1 \leq i \leq k$. Since q does not divide a, $a \notin q\mathbb{Z}$. We also have that $\pm 1 \notin 2\mathbb{Z}$, hence the intersection of all $n\mathbb{Z}$ is trivial. □

The structure of this ring can now be studied by decomposing it into a product of the now-familiar p-adic integers trough the Chinese Remainder Theorem:

Theorem 4.27. There exists an isomorphism of topological rings

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

Proof. Each natural number n may be written as a product of primes $n = \prod_p n^{e_p(n)}$, where all but finitely many $e_p(n)$ are non-zero. The classical Chinese Remainder Theorem gives a canonical isomorphism:

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \textstyle\prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}$$

These maps are compatible with the quotient maps $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, in the sense that all natural diagrams

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \xrightarrow{\cong} & \prod_p \mathbb{Z}/p^{e_p(mn)}\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\cong]{} & \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z} \end{array}$$

commute. Passing to inverse limits gives an isomorphism

$$\hat{\mathbb{Z}} \cong \varprojlim_{n\in\mathbb{N}} \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}.$$

It suffices now to show that this inverse limit really is $\prod_p \mathbb{Z}_p$. To this end, consider that the natural continuous surjections $\prod_p \mathbb{Z}_p \to \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}$ form a cone, hence by the definition of limit we have a

homomorphism

$$\psi : \prod_p \mathbb{Z}_p \to \varprojlim_{n\in\mathbb{N}} \prod_p \mathbb{Z}/p^{e_p(n)}\mathbb{Z}.$$

By Proposition 4.8, ψ is continuous and by Corollary 4.10.2 and compactness of $\prod_p \mathbb{Z}_p$, it is also surjective. Moreover, since every non-trivial element of $\prod_p \mathbb{Z}_p$ is non-trivial in some $\mathbb{Z}/p^i\mathbb{Z}$ for some p prime and $i \in \mathbb{N}$, ψ is injective. This shows that ψ is a topological isomorphism [Wil, Thm. 2.2.1]. □

This has an immediate corollary:

Corollary 4.27.1. The ring $\hat{\mathbb{Z}}$ is not an integral domain.

Proof. This follows from elementary ring theory. □

We use this decomposition to prove that $\hat{\mathbb{Z}}$ is torsion-free. We must first establish this fact about each $\mathbb{Z}_p$:

Proposition 4.28. For p prime, the additive group $\mathbb{Z}_p$ is torsion-free.

Proof. Let $0 \neq \alpha = (a_i) \in \mathbb{Z}_p$ and suppose there exists some $n \in \mathbb{N}_0$ such that $n\alpha = 0$. By contradiction, assume that $n \neq 0$. Write $n = p^r s$ where s is coprime to p and recall that by assumption $na_i \equiv 0 \mod p^i$ for all $i \in \mathbb{N}$. Let $N \in \mathbb{N}$ be such that $a_N \not\equiv 0 \mod p^N$ and consider a_{N+r}. We have $ma_{N+r} \equiv 0 \mod p^{N+r}$, i.e. $p^{N+r} | p^r s a_{N+r}$. Since s is coprime to p, we have $p^N | a_{N+r}$, thus $a_{N+r} \equiv 0 \mod p^N$, a contradiction since $a_{N+r} \equiv a_N \mod p^N$ [Wil, Prop. 2.1.4]. □

Corollary 4.28.1. The additive group $\hat{\mathbb{Z}}$ is torsion-free.

Proof. Let $(0)_p \neq (\alpha_p)_p \in \prod_p \mathbb{Z}_p$ and suppose there exists $n \in \mathbb{N}_0$ such that $(n\alpha_p)_p = (0)_p$. Hence there exists some prime q such that $n\alpha_q = 0 \in \mathbb{Z}_q$. Thus $n = 0$. □

We will come back to this ring at later stages to prove additional properties of its structure.

4.4 Sylow's Theorems

This section will be dedicated to the generalisation to profinite groups of the finite Sylow's Theorems[20]. For finite groups, these results were critical in establishing sufficient conditions for the converse of Lagrange's Theorem. Although we always have that the order of a subgroup divides the order of the whole group, it is easy to find groups such as A_4 with order 12 but no subgroup of order 6 [Hal99, Pg. 43]. However, if we restrict ourselves to subgroups which have for order powers of a prime p, which we call **p-subgroups**, the converse does hold true. Sylow's Theorems deal with a particular class of p-subgroups, the **Sylow p-subgroups**, which are maximal p-subgroups with respect to inclusion. We present the first two theorems in the following form:

[20] The following discussion is largely inspired by Section 2.3 of Chapter 2 in "Profinite Groups" by L. Ribes [RZ10]

Theorem 4.29. Let G be a finite group and let p be a prime. Then

1. If p divides the order of G, G contains a Sylow p-subgroup,
2. Any p-subgroup of G is contained in some Sylow p-subgroup,
3. Any two Sylow p-subgroups of G are conjugate

Proof. See Theorem 6.2 and Theorem 6.3 of Chapter 1 in "Algebra" by S. Lang [Lan02]. □

There is a third Sylow Theorem, which concerns the number of Sylow p-subgroups, but it has no immediate generalisation to profinite groups, hence we will not discuss it.

The first roadblock to our generalisation of Sylow's Theorems for profinite groups lies in determining the meaning of a prime dividing the order of a profinite group. Since profinite groups are either finite or uncountable, a new notion of order is needed to make any progress at all. The solution to this problem starts from introducing a new number system, the supernatural numbers:

Definition 4.30. A **supernatural number** is a formal product $n = \prod_p p^{n(p)}$, where p runs through the set of all prime numbers and $n(p) \in \mathbb{N} \cup \{\infty\}$.

If we have a family of supernatural numbers, we can take product, least common multiple and greatest common divisor, which are intuitively generalised. For instance, for supernatural numbers $(n_i)_{i\in I}$, the LCM is

$$\operatorname{lcm}\{n_i\} = \prod_p p^{n(p)}, \text{ where } n(p) = \sup_{i\in I}\{n_i(p)\},$$

where the supremum is defined in the obvious sense [RZ10, Pg. 33].

Once we have a supernatural numbers, we can define the order of a profinite group and the index of a subgroup:

Definition 4.31. Let G be a profinite subgroup and H a closed subgroup of G. Let $\mathcal{U}$ be the set of all open normal subgroups of G. We define the **index** $[G : H]$ of H in G as the supernatural number

$$[G : H] = \operatorname{lcm}\{[G/U : HU/U] \mid U \in \mathcal{U}\}.$$

Moreover, we define the **order** $\#G$ of G as the order of the trivial subgroup $[G : \{e\}]$, i.e.

$$\#G = \operatorname{lcm}\{\#(G/U) \mid U \in \mathcal{U}\}.$$

Note that this definition is independent of the choice of inverse system and is compatible with a profinite Lagrange's Theorem, which we will not cite for brevity. Furthermore, we say that a supernatural number

$n = \prod_q q^{n(q)}$ is a **p-number** if $n(q) = 0$ whenever $q \neq p$. With p-numbers defined, we can give the profinite equivalent of finite p-groups:

Definition 4.32. Let G be a profinite group. We say G is a **pro-p group** if its order $\#G$ is a p-number.

Unsurprisingly, pro-p-groups can be realised as inverse limits of p-groups:

Proposition 4.33. Let G be a profinite group and p a prime. Then G is pro-p if and only if G is the inverse limit of an inverse system of groups of order p^i for some $i \in \mathbb{N}$.

Proof. This follows trivially from the definition of order of G as a least common multiple. □

Similarly, we define Sylow pro-p-subgroups:

Definition 4.34. Let G be a profinite group and p a prime. A **Sylow pro-p-subgroup** of G is a pro-p-subgroup H such that $[G : H]$ is a q-number, for some q coprime to p.

Some authors call both finite Sylow p-subgroups and infinite Sylow pro-p-subgroups, Sylow p-subgroups or p-Sylow subgroups [Wil98, RZ10]. We prefer to follow the terminology of "Lectures in Profinite Topics in Group Theory" by B. Klopsch, et al. [KVSN11] to avoid ambiguities in the following theorems.

Through a few supernatural number calculations it is possible to show the following result:

Lemma 4.35. Let p be a prime and G the inverse limit of a surjective inverse system of finite groups (G_i, ϕ_{ij}, I). A closed subgroup H of G is a Sylow pro-p-subgroup of G if and only if each $\pi_i(H)$ is a Sylow p-subgroup of G_i.

Proof. See Lemma 2.3.4 in Chapter 2 of "Profinte Groups" by L. Ribes [RZ10]. □

With the previous Lemma in place, we have all the necessary ingredients to prove the profinite Sylow Theorems:

Theorem 4.36. Let p be a prime and G the inverse limit of a surjective inverse system of finite groups (G_i, ϕ_{ij}, I). Then

1. If p divides the order of each G_i, G contains a Sylow pro-p-subgroup,
2. Any closed pro-p-subgroup of G is contained in some Sylow pro-p-subgroup,
3. Any two Sylow pro-p-subgroups of G are conjugate.

Proof. For (1), assume that p divides the order of each G_i. Then by the finite Sylow Theorems, each G_i has a Sylow p-subgroup. Denote $\mathcal{H}_i$ the non-empty set of Sylow p-subgroups of G_i and consider the

maps

$$\Phi_{ij} : \mathcal{H}_j \ni H_j \mapsto \phi_{ij}(H_j) \in \mathcal{H}_i,$$

which is well-defined since ϕ_{ij} is surjective. It is easy to see that $(\mathcal{H}_i, \Phi_{ij}, I)$ is an inverse system of non-empty finite sets, hence Proposition 4.4 applies and

$$\varprojlim_{i \in I} \mathcal{H}_i \neq \emptyset.$$

Let $(H_i) \in \varprojlim_{i \in I} \mathcal{H}_i$. Then for every $i \in I$, H_i is a Sylow p-Subgroup of G_i and (H_i, ϕ_{ij}, I) is an inverse system of finite groups. Hence by Lemma 4.35, $H = \varprojlim_{i \in I} H_i$ is a Sylow pro-p-subgroup of G.

For (2), assume H is a closed pro-p-subgroup of G. Then $\pi_i(H)$ is a p-subgroup of G_i. By the finite Sylow Theorems, for each $i \in I$, the set $\mathcal{S}_i$ of Sylow p-subgroups of G_i which contain $\pi_i(H)$ is non-empty. As in (1), we define the maps $\Phi_{ij} : S_j \mapsto \phi_{ij}(S_j)$ and apply Proposition 4.4 to the inverse system of non-empty finite sets $(\mathcal{S}_i, \Phi_{ij}, I)$. Hence, we can take the inverse limit of the inverse system of finite groups given by the element $(S_i) \in \varprojlim_{i \in I} \mathcal{S}_i$ to find

$$H = \varprojlim_{i \in I} \pi_i(H_i) \leq \varprojlim_{i \in I} S_i = S.$$

Since each S_i is a Sylow p-subgroup of G_i, by Lemma 4.35 S is a Sylow pro-p-subgroup of G which contains H.

For (3), let H and K be two Sylow pro-p-subgroups of G. Then, by the finite Sylow theorems, $\pi_i(H)$ and $\pi_i(K)$ are conjugate subgroups of G_i, so we may consider the non-empty set

$$Q_i = \{q_i \in G_i \mid q_i \pi_i(H) q_i^{-1} = \pi_i(K)\}.$$

Clearly $\phi_{ij}(Q_j) \subseteq Q_i$, hence the inverse limit of (Q_i, ϕ_{ij}, I) is non-empty and we can take $q \in \varprojlim_{i \in I} Q_i$. Then

$$qHq^{-1} = \varprojlim_{i \in I} q_i \pi_i(H) q_i^{-1} = \varprojlim \pi_i(K) = K,$$

as desired [KVSN11, Thm 2.3.5]. □

A more general partial converse to Lagrange's Theorem for finite groups has been established by M. Hall [Hal99]. Hall's Theorem considers maximal subgroups which have powers of arbitrary primes as order, called **Hall π-subgroups**, and proves their existence in finite solvable groups. This result too has a generalisation to profinite groups, which can be found in Section 2.3 of "Profinite Groups" by L. Ribes [RZ10].

We will conclude this section by establishing the special behaviour of Sylow pro-p-groups with respect to profinite groups which arise from inverse systems of nilpotent groups. A critical result of finite Sylow Theory is that nilpotent groups decompose into a product of their unique Sylow p-subgroups. We will

see that this result can be passed to the limit. Recall that a group is nilpotent if its lower central series

$$\gamma_1(G) = G \wedge \gamma_{n+1}(G) = [\gamma_n(G), G]$$

terminates.

Definition 4.37. Let $(G_i)_{i\in I}$ an inverse system of finite groups. We say $G = \varprojlim_{i\in I} G_i$ is **pronilpotent** if each G_i is nilpotent.

Note that pronilpotent groups may not be nilpotent [RZ10, Pg. 27]. We now show that pronilpotent groups can be characterised entirely from their Sylow pro-p-subgroups:

Proposition 4.38. A profinite group G is pronilpotent if and only if for each prime p, G contains a unique Sylow pro-p-subgroup. In which case, G is the direct product $G = \prod_p G_p$ of its unique Sylow pro-p-subgroups G_p.

Proof. For a proof of the finite result see Theorem 10.3.4 in Chapter 10 of "The theory of groups" by M. Hall [Hal99]. Since inverse limits commute with products (see Proposition 4.11 or Proposition 5.3 of "Limit" in [nLa21]), we can pass the finite result to the limit. □

4.4.1 Example: $\mathbb{Z}_p$ as Sylow p-subgroup of $\hat{\mathbb{Z}}$

As an example of the theory developed so far in this section, we will explicitly find all the Sylow pro-p-subgroups of $\hat{\mathbb{Z}}$. Consider the additive group $\hat{\mathbb{Z}}$, written as the product $\prod_p \mathbb{Z}_p$ we derived in Theorem 4.27. For any prime p, we can show the following:

Proposition 4.39. For p prime, $\mathbb{Z}_p$ is the unique Sylow pro-p-subgroup of $\mathbb{Z}$.

Proof. By naive application of Definition 4.34, any Sylow pro-p-subgroup H of $\hat{\mathbb{Z}}$ will need to have a p-number as order and coprime index. From the product decomposition it is easy to see that H must be a subgroup of $\mathbb{Z}_p$ and by maximality in Theorem 4.36, we know $H = \mathbb{Z}_p$ since it is closed in $\hat{\mathbb{Z}}$. □

By establishing that $\mathbb{Z}_p$ is the unique Sylow pro-p-subgroup of $\hat{\mathbb{Z}}$, we have also proved nilpotency:

Corollary 4.39.1. $\hat{\mathbb{Z}}$ is pronilpotent.

Hence the application of Proposition 4.38 confirms the product decomposition we previously derived in Theorem 4.27.

4.5 Generators and procyclic groups

In this section we will focus on results around generators of profinite groups. In particular, we will provide a classification of the profinite groups that arise as inverse limits of cyclic groups[21]. We will apply the theory developed to find the generators of $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$. Instead of relying on the usual notion of generating set of a group, we will work with topological generating sets:

Definition 4.40. Let G be a profinite group and $X \subseteq G$ a subset. We say X **topologically generates** G if the abstract group $\langle X \rangle$ is dense in G, in which case we call X the **set of (topological) generators** of G and write $G = \overline{\langle X \rangle}$.

The topological generating set of profinite groups projects onto the abstract generating set of each finite group in the inverse system:

Lemma 4.41. Let (G_i) be a surjective inverse system of finite groups with inverse limit G and $X \subseteq G$ be a subset. Then X generates G if and only if $\pi_i(X)$ generates G_i for each $i \in I$.

Proof. If X generates G, then it is immediate that $\pi_i(X)$ generates G_i. Conversely, suppose $\pi_i(X)$ generates G_i for all $i \in I$ and let $H = \overline{\langle X \rangle}$. Then $\pi_i(H) = G_i$ for each $i \in I$, hence $H = G$ by Proposition 4.9 [RZ10, Lemma 2.4.1]. □

We can immediately provide a profinite notion corresponding to cyclic groups:

Definition 4.42. A profinite group G is called **procyclic** if it contains an element x such that $G = \overline{\langle x \rangle}$.

By Lemma 4.41, procyclic groups can be realised as inverse limits of finite cyclic groups. A natural question to ask at this point is how many such groups can we construct. More formally, we will now focus on the problem of classification of procyclic groups. We first consider procyclic groups which are pro-p, i.e. whose order is a p-number

Proposition 4.43. Let p be a prime number and p^n a supernatural number. Then,

1. There exists a unique procyclic group C of order p^n up to isomorphism; namely, if $n < \infty$, $C \cong \mathbb{Z}/p^n\mathbb{Z}$, and if $n = \infty$, $C \cong \mathbb{Z}_p$.

2. The group $\mathbb{Z}_p$ has a unique closed subgroup H of index p^n. Moreover, $H \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p$ if n is finite, and $H \cong 1$ if n is infinite.

3. Every procyclic group of order p^n appears as a quotient of $\mathbb{Z}_p$ in some unique way.

4. $\mathbb{Z}_p$ cannot be written as a direct product of non-trivial subgroup.

[21] This section is largely follows Section 2.4 of Chapter 2 in "Profinite Groups" by L. Ribes [RZ10].

Proof. For (1), the finite case follows from elementary group theory. Hence, let C be a procyclic group of order p^∞, and let U and V be open subgroups of C with same indexes. Then $U/U\cap V$ and $V/U\cap V$ are subgroups of the finite cyclic group $C/U\cap V$ with the same index, hence $U=V$. Thus for each natural number $i\in\mathbb{N}$, C has a unique open subgroup U_i of index p^i, hence

$$C\cong\varprojlim_{i\in I} C/U_i\cong\varprojlim_{i\in I}\mathbb{Z}/p^i\mathbb{Z}\cong\mathbb{Z}_p.$$

For (2), the previous argument shows that $\mathbb{Z}_p$ has a unique closed subgroup H of index p^n if n is finite, so $H\cong p^n\mathbb{Z}_p\cong\mathbb{Z}_p$. Assume now H is a closed subgroup of $\mathbb{Z}_p$ of index p^∞ let $U_i=p^i\mathbb{Z}_p$. By the definition of index, we have that for each $i\in\mathbb{N}$, there exists some $j\in\mathbb{N}$ such that $U_jH\leq U_i$, therefore

$$H=\bigcap_{i=1}^{\infty}U_iH=\{e\},$$

which proves (2).

It is easy to see that (3) follows from (2). For (4), let U,V be non-trivial subgroups of $\mathbb{Z}_p$. Then they have finite index and so does their intersection, so $U\cap V\cong\mathbb{Z}_p$ by (1). Hence, it follows that $U\times V\ncong\mathbb{Z}_p$ [RZ10, Prop. 2.7.1]. □

The previous Theorem can be expanded into a complete classification of procyclic groups through the Chinese Remainder Theorem decomposition of $\hat{\mathbb{Z}}$. For brevity, we will present only the statement of this incredible result, before proceeding with the study of the generators of $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$.

Theorem 4.44. Let $n=\prod_p p^{n(p)}$ be a supernatural number. Then

1. There exists a unique procyclic group C of order n up to isomorphism.
2. The group $\hat{\mathbb{Z}}$ has a unique closed subgroup H of index n. Moreover,

$$H\cong\prod_{p\in S}\mathbb{Z}_p,$$

   where $S=\{p\mid n(p)<\infty\}$.
3. Every procyclic group of order n is a quotient of $\hat{\mathbb{Z}}$ in some unique way.

Proof. See Theorem 2.7.2 of Chapter 2 of "Profinite Groups" by L. Ribes [RZ10]. □

4.5.1 Example: the generators of $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$

We will now apply the theory we derived regarding generators to the additive groups $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ we defined in earlier chapters. In particular, we will determine the structure of their generators and whether these groups are procyclic. We look at $\mathbb{Z}_p$ first:

Proposition 4.45. Let $\mathbb{Z}_p^\times$ be the set of elements which topologically generate $\mathbb{Z}_p$. Then $\alpha \in \mathbb{Z}_p^\times$ if and only if $\alpha \not\equiv 0 \mod p$. In particular $\mathbb{Z}_p^\times$ is an uncountable subset of $\mathbb{Z}_p$ and for every n and every generator $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ there exists some $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha \equiv a_n \mod p^n$.

Proof. If $\alpha = (a_n) \in \mathbb{Z}_p$ has $a_1 \not\equiv 0 \mod p$, then p does not divide a_n for any $n \in \mathbb{N}$. Hence a_n is coprime to p^n and thus is a generator of $\mathbb{Z}/p^n\mathbb{Z}$. Since this is true for all $n \in \mathbb{N}$, α topologically generates $\mathbb{Z}_p$ [Wil, Prop. 2.5.8]. □

A trivial consequence of this is that $\mathbb{Z}_p$ is procyclic:

Corollary 4.45.1. $\mathbb{Z}_p$ is procyclic.

This can also be seen from Lemma 4.41 since all the maps $\phi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ in the inverse system are surjective and each $\mathbb{Z}/p^i\mathbb{Z}$ is cyclic. Furthermore, note that the notation we used for the set $\mathbb{Z}_p^\times$ of generators of $\mathbb{Z}_p$ is borrowed from ring theory [Wil, Rem. 2.5.9]. In fact it can be shown that this is indeed consistent with the group of units of the ring $\mathbb{Z}_p$:

Proposition 4.46. Let $0 \neq \alpha \in \mathbb{Z}_p$. Then $\alpha \in \mathbb{Z}_p^\times$ if and only if there exists some $\beta \in \mathbb{Z}_p$ such that $\alpha\beta = 1$.

Proof. See Remark 2.5.9 in Chapter 2 of "Profinite Groups and Group Cohomology" by G. Wilkes [Wil]. □

Unfortunately, investigating the structure of the p-adic units requires the study of the p-adic exponential and logarithmic maps, which relate the multiplicative and additive structure of $\mathbb{Z}_p$. Since these topics are beyond the scope of this discussion, we will introduce the following result without proving it and refer the interested reader to Section 4.5 of "p-adic Numbers: An Introduction" by F. Q. Gouvea [Gou97].

Theorem 4.47. For any prime p, let $q = 4$ if $p = 2$ and $q = p$ otherwise. Then there exists a topological isomorphism $\mathbb{Z}_p^\times \cong V \times \mathbb{Z}_p^+$ which decomposes the multiplicative group $\mathbb{Z}_p^\times$ into a torsion part V and a torsion-free pro-p part $\mathbb{Z}_p^+$. Furthermore, $V \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is the cyclic group of order $\varphi(q)$ and it is the set of roots of unity of $\mathbb{Z}_p$.

Proof. See Corollary 4.5.10 in "p-adic Numbers: An Introduction" by F. Q. Gouvea [Gou97]. □

Returning to our generators of $\mathbb{Z}_p$, we can now use the Chinese Remainder Theorem decomposition of $\mathbb{Z}$ to immediately characterise the generators of $\hat{\mathbb{Z}}$:

Proposition 4.48. For every $n \in \mathbb{N}$ and every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ there exists a generator $\alpha \in \hat{\mathbb{Z}}^\times$ of $\hat{\mathbb{Z}}$ such that $\alpha \equiv a \mod n$.

Proof. This follows from Proposition 4.45 and Theorem 4.27. □

Once again, procyclicity follows immediately:

Corollary 4.48.1. $\hat{\mathbb{Z}}$ is procyclic.

We must stress that $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ are not abstractly generated by a single element [Wil, Rem. 2.5.2]. The subgroup generated by any topological generator in $\mathbb{Z}_p^\times$ or $\hat{\mathbb{Z}}^\times$ is only dense in the group, not identical to it.

4.6 The Frattini Subgroup

We will conclude this chapter with a discussion of the Frattini subgroup[22]. This object, first introduced by G. Frattini in "Intorno alla generazione di gruppi di operazioni" [Fra85], allows for an alternative method for finding group generators. An historical account of this interesting subgroup can be found in "The True Story Behind Frattini's Argument" by F. De Giovanni, et al. [dGTB17].

Definition 4.49. Let G be a profinite group. The **Frattini subgroup** $\Phi(G)$ of G is the intersection of all its maximal open (proper) subgroups.

Note that this subgroup is always well-defined, since profinite groups always have maximal open subgroups [RZ10, Pg. 53]. This is not necessarily true for abstract groups: for instance, it can be shown that $(\mathbb{Q}, +)$ has no maximal subgroups [Mun].

In analysing the properties of the Frattini subgroup, the first thing to note is that it is a characteristic subgroup of every profinite group:

Proposition 4.50. Let G be a profinite group. The Frattini subgroup $\Phi(G)$ of G is a characteristic subgroup of G, i.e. for every continuous automorphism ψ of G, $\psi(\Phi(G)) = \Phi(G)$.

Proof. Let ψ be a continuous automorphism of G and let H, K be open subgroups of G. Then $\psi^{-1}(H)$ and $\psi^{-1}(K)$ are open subgroups of G. Moreover, since ψ is a bijection, if $H \subseteq K$, we have $\psi^{-1}(H) \subseteq \psi^{-1}(K)$, hence if H is a maximal open subgroup, so is $\psi^{-1}(H)$. Thus, $\Phi(G)$ is invariant under ψ. □

Hence, normality follows:

Corollary 4.50.1. The Frattini subgroup $\Phi(G)$ is normal in G.

Proof. Since ψ is invariant under all continuous automorphisms, it is invariant under all inner automorphisms, i.e. the conjugations. □

The quotient $G/\Phi(G)$ called the **Frattini quotient**. It is an object of special interest and we will see that it exhibits a particularly simple structure in the case of pro-p groups.

[22] This section is largely based on Section 2.8 of Chapter 2 in "Profinite Groups" by L. Ribes [RZ10].

Since computing the intersection of maximal open sets of a profinite group is not immediate, we now turn to realising $\Phi(G)$ as an inverse limit. In doing so, we will show that if G is a profinite group, $\Phi(G)$ is also a profinite group.

Proposition 4.51. Let G be a profinite group.

1. If $N \triangleleft G$ is closed ($N \triangleleft_C G$) and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$,
2. If $\rho : G \to H$ is a surjective homomorphism of profinite groups, then $\rho(\Phi(G)) \leq \Phi(H)$,
3. If (G_i, ϕ_{ii}, I) is a surjective inverse system of finite groups, then $\Phi(\varprojlim_{i\in I} G_i) = \varprojlim_{i\in I} \Phi(G_i)$

Proof. For (1), by applying the definition we obtain

$$\Phi(G)/N = \bigcap_{M\in\mathcal{M}} M\Big/N = \bigcap_{M\in\mathcal{M}} M/N = \Phi(G/N),$$

where $\mathcal{M}$ is the set of maximal open subgroups of G.

For (2), it is sufficient to note that $\rho^{-1}(M)$ is a maximal open subgroup of G whenever M is a maximal open subgroup of H.

For (3), let $G = \varprojlim_{i\in I} G_i$ and note that the projection maps $\pi_i : G \to G_i$ are surjective. By (2), we have $\pi_i(\Phi(G)) \leq \Phi(G_i)$, hence

$$\Phi(G) = \varprojlim_{i\in I} \pi_i(\Phi(G)) \leq \varprojlim_{i\in I} \Phi(G_i).$$

Suppose there exists an element $g \in \varprojlim_{i\in I} \Phi(G_i)$ such that $g \notin \Phi(G)$. Then there exists a maximal open subgroup M of G with $g \notin M$. Hence $g_i \notin \pi_i(M)$ and $\pi_i(M)$ is a maximal subgroup of G_i, thus we have $g_i \notin \Phi(G_i)$, a contradiction. Therefore

$$\Phi(G) \geq \varprojlim_{i\in I} \Phi(G_i),$$

which concludes the proof [RZ10, Prop. 2.8.2]. □

Corollary 4.51.1. The Frattini subgroup $\Phi(G)$ of a profinite group G is profinite.

We conclude this section by establishing to the link between the Frattini subgroup and generators of a profinite group. To this end, we formally define non-generating elements:

Definition 4.52. Let G be a topological group and $g \in G$. We say G is a **non-generator** if for every $X \subseteq G$ such that $\overline{\langle X, g\rangle} = G$, we have $\overline{\langle X\rangle} = G$.

This definition allows us to introduce the most important result of this discussion:

Lemma 4.53. Let G be a profinite group. The Frattini subgroup $\Phi(G)$ coincides with the set S of non-generators of G.

Proof. Assume $g \in S$. If H is a maximal open subgroup of G and $g \notin H$, then $G = \overline{\langle H, g \rangle}$ but $G \neq H$. This contradicts S being a non-generator. Thus there is no such maximal open subgroup H of G and $s \in \Phi(G)$.

Assume now $g \notin S$, i.e. there exists a subset X of G such that $G = \overline{\langle X, g \rangle}$ but $G \neq \overline{\langle X \rangle}$. Note that we have $\overline{\langle X, g \rangle} = \overline{\langle \overline{\langle X \rangle}, g \rangle}$ and, by Proposition 4.13, $\overline{\langle X \rangle}$ is the intersection of the open subgroups of G containing $\overline{\langle X \rangle}$. Therefore there exists an open subgroup H of G which is maximal with respect to the properties of containing $\overline{\langle X \rangle}$ and not containing g. We can show H is maximal by considering an open subgroup K such that $H < K \leq_O G$, which would imply $K \geq \langle X, g \rangle$ and thus $K = G$. Hence H is maximal and since $g \notin H$, we have $g \notin \Phi(G)$ [RZ10, Lemma 2.8.1]. □

Hence, it suffices to find a complete description the Frattini subgroup to obtain a complete list of generators of a profinite group. By Proposition 4.51, this problem can be reduced to finding the Frattini subgroups of each G_i in the inverse system. Moreover, for pro-p groups, a more direct construction is available:

Lemma 4.54. Let p be a prime number and G be a pro-p group.

1. Every maximal closed subgroup M of G has index p,
2. The Frattini quotient $G/\Phi(G)$ is a p-elementary abelian profinite group, and hence a vector space over $\mathbb{F}_p$,
3. $\Phi(G) = \overline{G^p[G,G]}$ where $G^p = \{x^p \mid x \in G\}$ and $[G,G]$ is the commutator subgroup of G.

Proof. See Lemma 2.8.7 of Chapter 2 of "Profinite Groups" by L. Ribes [RZ10]. □

Although we have not proved this result, we will provide an example of its application on the Nottingham group.

4.6.1 Example: the Nottingham group $\mathcal{J}(\mathbb{F}_p)$

We will now look at an example of how Frattini groups can be calculated in practice. We will deviate from the $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ examples provided thus far, since we have an explicit list of their generating elements. Hence, by Lemma 4.53, the Frattini subgroup can be identified with the set of non-generating elements. The focus of this example will be the Nottingham group, which is defined as follows:

Definition 4.55. Let p be a prime and $\mathbb{F}_p$ be the finite field $\mathbb{Z}/p\mathbb{Z}$. The **Nottingham group** $\mathcal{J}(\mathbb{F}_p)$

on $\mathbb{F}_p$ is the group of formal power series of the form

$$f(t) = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^k\right) \in t + t^2\mathbb{F}_p[[t]],$$

under formal substitution:

$$\forall g \in \mathcal{J}(\mathbb{F}_p),\ f(t) \circ g(t) = g(t)\left(1 + \sum_{k=1}^{\infty} \alpha_k g(t)^k\right).$$

The fact that this is indeed a group was first proven by S. A. Jennings in "Substitution groups of formal power series" [Jen54]:

Proposition 4.56. The Nottingham group is a group.

Proof. Associativity is given by function composition and the identity element is the formal power series $f(t) = t$. Inverses are constructed by solving an infinite system of polynomial equations. This is shown with due rigour in Theorem 1.1 in "Substitution groups of formal power series" by S. A. Jennings [Jen54]. □

It is common to view the Nottingham group as the group of wild automorphisms of $\mathbb{F}_p((t))$, the field of formal power series over $\mathbb{F}_p$. This link is formally established by the following homomorphism:

Proposition 4.57. The homomorphism $\theta : \mathcal{J}(\mathbb{F}_p) \to \mathrm{Aut}(\mathbb{F}_p((t)))$ given extending

$$\theta(f)(t) = f(t),$$

is injective.

Proof. See Theorem 1 of "The Nottingham Group" by R. Camina [Cam00]. □

Our aim for this example is to construct the Frattini subgroup of $\mathcal{J}(\mathbb{F}_p)$ for odd p[23] and thus find the minimal generating set of the Nottingham group. The discussion will be largely based on "The Nottingham Group" by R. Camina [Cam00], with notation inspired by an exercise in "Lectures in Profinite Topics in Group Theory" by B. Klopsch, et al. [KVSN11]. To avoid the most verbose calculations, we will sometimes cite the aforementioned article by S. A. Jennings [Jen54].

Consider now for each $n \in \mathbb{N}$ and $f(t), g(t) \in \mathcal{J}(\mathbb{F}_p)$, the equivalence relationship $\sim_n$ on $\mathcal{J}(\mathbb{F}_p)$ defined by $f(t) \sim_n g(t)$ if and only if $f(t) - g(t) \in t^{n+1}\mathbb{F}[[t]]$. We may also write $f(t) \sim_n g(t)$ as $f(t) \equiv g(t) \mod t^{n+1}$. Note that these equivalence classes contain canonical representatives consisting of nth degree polynomials and every other element is characterised by sharing the leading n coefficients with this polynomial. Furthermore, this equivalence relationship respects group multiplication and inverts:

[23] For a discussion of the $p = 2$ case, the reader is recommended to Section 7 of "The Nottingham Group" by R. Carmina [Cam00].

Proposition 4.58. Let $f(t), g(t), h(t), l(t) \in \mathcal{J}(\mathbb{F}_p)$. If $f(t) \sim_n h(t)$ and $g(t) \sim_n l(t)$, then $f(t) \circ g(t) \sim_n h(t) \circ l(t)$ and $f^{-1}(t) \sim_n h^{-1}(t)$.

Proof. See Theorem 2.2 in "Substitution groups of formal power series" by S. A. Jennings [Jen54]. □

Let $\Gamma_n = \mathcal{J}(\mathbb{F}_p)/\sim_n$ be the set of equivalence classes under $\sim_n$. By the previous Proposition, Γ_n is a group and the map $\pi_n : \mathcal{J}(\mathbb{F}_p) \to \Gamma_n$, which sends each element $f(t)$ to its equivalence class $[f(t)]_{\sim_n}$, is a group homomorphism.

Consider now $\mathcal{J}_n(\mathbb{F}_p) = \ker(\pi_n) = \{f(t) \in \mathcal{J}(\mathbb{F}_p) \mid f(t) \equiv t \mod t^{n+1}\}$. This is a normal subgroup of $\mathcal{J}(\mathbb{F}_p)$ whose index can be shown to be p^{n-1} by counting the number of nth degree polynomials with coefficients in $\mathbb{F}_p$ representing the equivalence classes in Γ_n[24]. Since we have defined a chain of normal subgroups with the property $[\mathcal{J}_n(\mathbb{F}_p) : \mathcal{J}_{n+1}(\mathbb{F}_p)] = p$, we can see that $\mathcal{J}(\mathbb{F}_p) = \varprojlim_{n\in\mathbb{N}} \mathcal{J}(\mathbb{F}_p)/\mathcal{J}_n(\mathbb{F}_p)$ is a pro-p group [Cam00, Pg. 207]. As usual, the topology on $\mathcal{J}(\mathbb{F}_p)$ is given by taking the normal subgroups $\mathcal{J}_n(\mathbb{F}_p)$ as an open neighbourhood base of the identity [Jen54, Pg. 330].

Moreover, we note that $\mathcal{J}_1(\mathbb{F}_p)$ is the whole group $\mathcal{J}(\mathbb{F}_p)$, hence results on the structure of $\mathcal{J}_n(\mathbb{F}_p)$ will apply globally. In particular, by explicitly constructing the Frattini subgroup of each $\mathcal{J}_n(\mathbb{F}_p)$, we will gain insight into the generators of the whole Nottingham group. In order to do this, according to Lemma 4.54, we need to understand both the power structure and the commutator structure of $\mathcal{J}_n(\mathbb{F}_p)$.

To this end, consider for each $i \in \mathbb{N}$ the elements $e_i(t) := t + t^{i+1} \in \mathcal{J}(\mathbb{F}_p)$. Their powers in modulo exhibit interesting structure:

Proposition 4.59. Let $i \in \mathbb{N}$, $\lambda \in \mathbb{Z}$. Then $e_i^\lambda(t) \equiv t + \lambda t^{i+1} \mod t^{i+2}$.

Proof. We consider the $\lambda \geq 0$ case first. We have that $e_i^0(t) = t$, so we have an induction base. For the induction step, assume $\lambda \in \mathbb{N}$ and $e_i^{\lambda-1}(t) \equiv t + (\lambda-1)t^{i+1} \mod t^{i+2}$. Then:

$$\begin{aligned} e_i^{\lambda-1}(t) \circ e_i(t) &\equiv (t + t^{i+1}) + (\lambda-1)(t + t^{i+1})^{i+1} \mod t^{i+2} \\ &\equiv (t + t^{i+1}) + (\lambda-1)t^{i+1}(1 + t^i)^{i+1} \mod t^{i+2} \\ &\equiv (t + t^{i+1}) + (\lambda-1)t^{i+1} \mod t^{i+2} \\ &\equiv t + \lambda t^{i+1} \mod t^{i+2}. \end{aligned}$$

[24] This last requirement forces the first coefficient to be 1, hence p^{n-1} (and not p^n) equivalence classes are possible.

Assume now $\lambda < 0$. By elementary group theory we have $e_i^{\lambda}(t) \circ e_i^{-\lambda}(t) = t$. Thus,

$$\begin{aligned}
& e_i^{-\lambda}(t) + \lambda(e_i^{-\lambda}(t))^{i+1} \equiv t \mod t^{i+2} \\
\implies & e_i^{-\lambda}(t) \equiv t - \lambda(e_i^{-\lambda}(t))^{i+1} \mod t^{i+2} \\
\implies & e_i^{-\lambda}(t) \equiv t - \lambda t^{i+1}\left(1 + \sum_{k=1}^{\infty} \alpha_k t^k\right)^{i+1} \mod t^{i+2} \\
\implies & e_i^{-\lambda}(t) \equiv t - \lambda t^{i+1} \mod t^{i+2}.
\end{aligned}$$

□

We can use this result to establish a relationship between the subgroups $\mathcal{J}_n(\mathbb{F}_p)$ for successive n.

Proposition 4.60. For each $n \in \mathbb{N}$, we have $\mathcal{J}_n(\mathbb{F}_p) = \langle e_n(t) \rangle \mathcal{J}_{n+1}(\mathbb{F}_p)$

Proof. Let $f(t) \in \mathcal{J}_n(\mathbb{F}_p)$, i.e. $f(t) \equiv t \mod t^{n+1}$. Then there exists some $\lambda \in \{0, 1, \ldots, p-1\}$ such that $f(t) \equiv t + \lambda t^{n+1} \mod t^{n+2}$. Hence $f(t) \equiv e_n^{\lambda}(t) \equiv e_n^{\lambda}(t) \circ t \mod t^{n+2}$, so $\mathcal{J}_n(\mathbb{F}_p) \subseteq \langle e_n(t) \rangle \mathcal{J}_{n+1}(\mathbb{F}_p)$.

Now let $g(t) \in \mathcal{J}_{n+1}(\mathbb{F}_p)$, i.e. $g(t) \equiv t \mod t^{n+2}$. For every $\lambda \in \{0, 1, \ldots, p-1\}$, we have

$$e_n^{\lambda}(t) \circ g(t) \equiv g(t) + \lambda g^{n+1}(t) \equiv t + \lambda t^{n+1} \mod t^{n+2},$$

hence $e_n^{\lambda}(t) \circ g(t) \equiv t \mod t^{n+1}$, so $\mathcal{J}_n(\mathbb{F}_p) \supseteq \langle e_n(t) \rangle \mathcal{J}_{n+1}(\mathbb{F}_p)$ □

We now turn to the commutator structure of our e_i elements:

Proposition 4.61. Let $i, j \in \mathbb{N}$. Then $e_i \circ e_j \equiv e_j \circ e_i \mod t^{i+j+1}$ and $[e_i(t), e_j(t)] \equiv e_{i+j}^{i-j}(t) \mod t^{i+j+2}$.

Proof. For the first claim, we expand out the left hand side

$$\begin{aligned}
e_i \circ e_j &= (t + t^{j+1}) + (t + t^{j+1})^{i+1} \\
&= (t + t^{j+1}) + t^{i+1}(1 + t^j)^{i+1} \\
&\equiv t + t^{j+1} + t^{i+1} + (i+1)t^{i+j+1} \mod t^{i+j+2}.
\end{aligned}$$

Similarly $e_j \circ e_i \equiv t + t^{i+1} + t^{j+1} + (j+1)t^{i+j+1} \mod t^{i+j+2}$, which proves the first claim when reduced modulo t^{i+j+1}. For the second claim, we rewrite the formula in an equivalent form:

$$\begin{aligned}
& [e_i(t), e_j(t)] \equiv e_{i+j}^{i-j}(t) \mod t^{i+j+2} \\
\iff & (e_j(t) \circ e_i(t))^{-1} \circ (e_i(t) \circ e_j(t)) \equiv e_{i+j}^{i-j}(t) \mod t^{i+j+2} \\
\iff & (e_i(t) \circ e_j(t)) \equiv (e_j(t) \circ e_i(t)) \circ e_{i+j}^{i-j}(t) \mod t^{i+j+2}.
\end{aligned}$$

By Proposition 4.59, we can write $e_{i+j}^{i-j}(t) \equiv t + (i-j)t^{i+j+1} \mod t^{i+j+2}$, so by putting together with our previous calculations, we get:

$$\begin{aligned}(e_j(t) \circ e_i(t)) \circ e_{i+j}^{i-j}(t) &\equiv (t + (i-j)t^{i+j+1}) + (t + (i-j)t^{i+j+1})^{i+1} + (t + (i-j)t^{i+j+1})^{j+1} \\ &\quad + (j+1)(t + (i-j)t^{i+j+1})^{i+j+1} \mod t^{i+j+2} \\ &\equiv t + (i-j)t^{i+j+1} + t^{i+1} + t^{j+1} + (j+1)t^{i+j+1} \mod t^{i+j+2} \\ &\equiv t + t^{i+1} + t^{j+1} + (i+1)t^{i+j+1} \mod t^{i+j+2},\end{aligned}$$

which matches our calculation for $e_i \circ e_j$. □

We will now restrict ourselves to considering odd primes and use the previous result to calculate the Frattini subgroups. First, we need to find the commutator subgroup of $\mathcal{J}_n(\mathbb{F}_p)$:

Proposition 4.62. For $p \neq 2$, $\overline{[\mathcal{J}_n(\mathbb{F}_p), \mathcal{J}_n(\mathbb{F}_p)]} = [\mathcal{J}_n(\mathbb{F}_p), \mathcal{J}_n(\mathbb{F}_p)] = \mathcal{J}_{2n+1}(\mathbb{F}_p)$.

Proof. Let $m \geq 2n+1$. Since $p \neq 2$, there exists $u, v \in \mathbb{N}$ such that $u \not\equiv v \mod p$, $u + v = m$ and $u, v \geq n$, i.e. $e_u, e_v \in \mathcal{J}_n(\mathbb{F}_p)$. By Proposition 4.60 and 4.61, we have

$$\langle [e_u(t), e_v(t)]\mathcal{J}_{m+1}(\mathbb{F}_p)\rangle = \langle e_{u+v}^{u-v}(t)\mathcal{J}_{m+1}(\mathbb{F}_p)\rangle = \langle e_m(t)\mathcal{J}_{m+1}(\mathbb{F}_p)\rangle = \mathcal{J}_m(\mathbb{F}_p)/\mathcal{J}_{m+1}(\mathbb{F}_p),$$

which proves $[\mathcal{J}_n(\mathbb{F}_p), \mathcal{J}_n(\mathbb{F}_p)] = \mathcal{J}_{2n+1}(\mathbb{F}_p)$. However, since $\mathcal{J}_{2n+1}(\mathbb{F}_p)$ is open, by Proposition 3.7, it must be closed. This concludes the proof [Cam00, Thm. 2]. □

Next, $\mathcal{J}_n^p(\mathbb{F}_p)$ can be found by inductive application of the group multiplication, so we will omit the proof:

Proposition 4.63. For $p \neq 2$, $\mathcal{J}_n^p(\mathbb{F}_p) \subseteq \mathcal{J}_{np}(\mathbb{F}_p)$

Proof. See Theorem 2.5 in "Substitution groups of formal power series" by S. A. Jennings [Jen54]. □

We can now find the Frattini subgroup of $\mathcal{J}_n(\mathbb{F}_p)$ by putting everything together:

Theorem 4.64. For $p \neq 2$, $\Phi(\mathcal{J}_n(\mathbb{F}_p)) = \mathcal{J}_{2n+1}(\mathbb{F}_p)$.

Proof. By Lemma 4.54, we have $\Phi(\mathcal{J}_n(\mathbb{F}_p)) = \overline{\mathcal{J}_n^p(\mathbb{F}_p)[\mathcal{J}_n(\mathbb{F}_p), \mathcal{J}_n(\mathbb{F}_p)]}$. Since $\mathcal{J}_n^p(\mathbb{F}_p) \subseteq \mathcal{J}_{np}(\mathbb{F}_p) \subseteq \mathcal{J}_{2n+1}(\mathbb{F}_p)$, we have

$$\Phi(\mathcal{J}_n(\mathbb{F}_p)) = \overline{\mathcal{J}_n^p(\mathbb{F}_p)[\mathcal{J}_n(\mathbb{F}_p), \mathcal{J}_n(\mathbb{F}_p)]} = \overline{\mathcal{J}_n^p(\mathbb{F}_p)\mathcal{J}_{2n+1}(\mathbb{F}_p)} = \mathcal{J}_{2n+1}(\mathbb{F}_p).$$

□

Recall that $\mathcal{J}_1(\mathbb{F}_p)$ is the whole group $\mathcal{J}(\mathbb{F}_p)$, hence the minimal generating set can be easily obtained:

Corollary 4.64.1. For $p \neq 2$, $\mathcal{J}(\mathbb{F}_p)$ is generated by $e_1(t)$ and $e_2(t)$.

Proof. Since

$$\mathcal{J}(\mathbb{F}_p) = \mathcal{J}_1(\mathbb{F}_p) = \langle e_1(t)\rangle\langle e_2(t)\rangle\mathcal{J}_3(\mathbb{F}_p) = \langle e_1(t)\rangle\langle e_2(t)\rangle\Phi(\mathcal{J}(\mathbb{F}_p)),$$

we have $\mathcal{J}(\mathbb{F}_p) = \overline{\langle e_1(t), e_2(t), \Phi(\mathcal{J}(\mathbb{F}_p))\rangle}$. By Lemma 4.53, the Frattini subgroup is the set of non-generators, hence we can remove it from the generating set to obtain $\mathcal{J}(\mathbb{F}_p) = \overline{\langle e_1(t), e_2(t)\rangle}$. □

Thus by constructing the Frattini subgroup we have shown how a group with a daunting structure like $\mathcal{J}(\mathbb{F}_p)$ can be topologically generated by just two elements. We will conclude this example by citing a final result that relates a significant family of pro-p groups to the Nottingham group:

Proposition 4.65. Every countably-based pro-p group can be embedded as a closed subgroup of $\mathcal{J}(\mathbb{F}_p)$.

Proof. See Theorem 11 of "The Nottingham Group" by R. Camina [Cam00]. □

5 Infinite Galois Theory

This chapter will be dedicated to showing the deep connection between profinite groups and infinite Galois theory. The key result from finite Galois theory, the Fundamental Theorem, relates intermediate extensions to subgroups of the Galois group. This profound result can be understood as an equivalence of the two poset categories in question, intermediate fields and subgroups [Bow17]. Since finite extensions have finite Galois groups, infinite extensions, which are obtained by taking direct limits of finite extensions, should intuitively correspond to inverse limits of finite subgroups, i.e. profinite groups. The goal of this chapter will be to formalise this intuition[25].

5.1 Finite Galois Theory

To this end, recall the following definitions from finite Galois theory:

Definition 5.1. Let K be a field and $f \in K[X]$ with degree d. We say f is **separable** if it has d distinct roots in its splitting field over K.

Definition 5.2. Let K be a field, L an extension of K and $\alpha \in L$. We say α is **separable** over K if α is algebraic over K and its minimal polynomial $m_{\alpha,K} \in K[X]$ is separable. We say L is **separable** over K if every element $\alpha \in L$ is separable over K.

Definition 5.3. Let $K \subseteq L$ be a field extension. We say L is **normal**[26] over K if L is algebraic over K and for all $\alpha \in L$, the minimal polynomial $m_{\alpha,K}$ splits completely in $L[X]$.

Normal extensions are sometimes characterised in an equivalent manner:

Proposition 5.4. Let $K \subseteq L$ be a field extension. Then L is normal if and only if for every extension M of L and K-embeddings $\sigma : L \to M$ we have $\sigma(L) \subseteq L$.

Proof. See Theorem 3.3, Chapter V of "Algebra" by S. Lang [Lan02]. □

Definition 5.5. Let $K \subseteq L$ be a field extension. We say that L is **Galois** over K if L is separable and normal over K.

Note that all these definitions are valid for both finite and infinite extensions. There is an alternative description of Galois extensions, given by the following proposition:

Proposition 5.6. Let $K \subseteq L$ be an algebraic field extension. L is Galois over K if and only if for all $\alpha \in L$, the minimal polynomial $m_{\alpha,K}$ has $\deg m_{\alpha,K}$ distinct roots in L.

Proof. Assume L is Galois over K and let $\alpha \in L$. Since L is separable over K, $m_{\alpha,K}$ has no repeated roots. Since L is normal over K, $m_{\alpha,K}$ splits completely in $L[X]$. Thus $m_{\alpha,K}$ has $\deg m_{\alpha,K}$ distinct

[25] The structure of the chapter largely follows Chapter 7 of "Fields and Galois Theory" by J. S. Milne [Mil20b]
[26] Normal extensions are referred to as quasi-Galois by Bourbaki

roots in L.

Conversely, assume for all $\alpha \in L$, $m_{\alpha,K}$ has $\deg m_{\alpha,K}$ distinct roots in L. Since $m_{\alpha,K}$ has no repeated roots, L is separable over K. Since $m_{\alpha,K}$ splits completely, L is normal over K. Hence L is Galois over K. □

We will use the previous proposition to characterise the behaviour of Galois extensions with respect to intermediate fields:

Proposition 5.7. Let $K \subseteq E \subseteq L$ be a tower of algebraic extensions with L Galois over K. Then L is Galois over E.

Proof. Let $\alpha \in L$, by the definition of minimal polynomial we know $m_{\alpha,E} | m_{\alpha,K}$ in $L[X]$. Since L is Galois over K, by Proposition 5.6 we know $m_{\alpha,K}$ has $\deg m_{\alpha,K}$ distinct roots, thus $m_{\alpha,E}$ has $\deg m_{\alpha,K}$ distinct roots. By Proposition 5.6, we conclude that L is Galois over E. □

The automorphism group of a Galois extension has an interesting structure and thus deserves its own name:

Definition 5.8. Let $K \subseteq L$ be a finite Galois extension. We call the group of K-automorphisms $L \to L$, $\mathrm{Aut}(L|K)$, the **Galois group** of L over K, denoted $\mathrm{Gal}(L|K)$.

We will not immediately give the same label to automorphism groups of infinite Galois extensions. Instead we will follow Milne's notation in [Mil20b, Pg. 91], and restrain from calling them Galois groups until we equip them with a topology. We are justified in giving the previous definition at this stage because finite Galois groups are canonically equipped with discrete topology.

With this notation, we can state the finite Fundamental Theorem of Galois Theory:

Theorem 5.9. Let $K \subseteq L$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(L|K)$. The map $H \mapsto L^H$ is a bijection from the set of subgroups of G to the set of intermediate fields $K \subseteq E \subseteq L$, with inverse $E \mapsto \mathrm{Gal}(L|E)$. Moreover,

1. The correspondence is inclusion reversing, i.e. $H_1 \supset H_2 \implies L^{H_1} \subset L^{H_2}$,
2. The index equals the degree, i.e. $[G : H] = [L^H : K]$,
3. If H corresponds to E, for all $\sigma \in G$, $\sigma H \sigma^{-1}$ corresponds to σE,
4. H is normal in G if and only if L^H is Galois over K, in which case $\mathrm{Gal}(L^H|K) \cong G/H$.

Proof. See Theorem 3.16, Chapter 3 of "Fields and Galois Theory" by J. S. Milne [Mil20b]. □

As mentioned in the introduction, this theorem can be translated in categorical language. Since the correspondence carries the inclusion maps, i.e. the morphisms of our subobject posets, we can understand it as a contravariant functor. Although this is discussed in depth in "Category Theory and Galois Theory" by A. Bower [Bow17], we are interested only in the following statement:

Theorem 5.10. Let $K \subseteq L$ be finite Galois extension with Galois group $G = \mathrm{Gal}(L|K)$. Let $\mathscr{P}$ be the poset category of subgroups of G, ordered by inclusion, and $\mathscr{Q}$ the poset category of intermediate fields between L and K, also ordered by inclusion. Then $\mathscr{F} : \mathscr{P} \to \mathscr{Q}$ and $\mathscr{G} : \mathscr{Q} \to \mathscr{P}$, defined by

$$\begin{aligned} \mathscr{F}(H) &= L^H, & \mathscr{F}(H_1 \hookrightarrow H_2) &= L^{H_2} \hookrightarrow L^{H_1}, \\ \mathscr{G}(E) &= \mathrm{Gal}(L|E), & \mathscr{G}(E \hookrightarrow F) &= \mathrm{Gal}(L|F) \hookrightarrow \mathrm{Gal}(L|E), \end{aligned}$$

are mutually inverse contravariant functors, which give an isomorphism of categories between $\mathscr{P}$ and $\mathscr{Q}'$.

Proof. See Theorem 3.8 of "Category Theory and Galois Theory" by A. Bower [Bow17]. □

Generalising the Fundamental Theorem to infinite Galois extensions is not immediate. When considering the posets of intermediate fields and all the subgroups of an infinite Galois group, we no longer have an isomorphism of categories. The usual[27] route to proving the infinite FTGT is to introduce a profinite topology on $\mathrm{Aut}(L|K)$ and restrict the correspondence to closed subgroups to obtain an isomorphism of categories.

Our approach will be somewhat different: we will show how the profinite profinite topology on $\mathrm{Aut}(L|K)$ arises naturally out of the Galois correspondence. This will be the main proof of the chapter.

5.2 Galois Connections and Closures

To prove how iterated applications of the Galois correspondence act on subgroups of $\mathrm{Aut}(L|K)$, we introduce the formalism of Galois connections, which abstract and generalise mappings like the Galois correspondence. We will follow the definitions given in "A Primer on Galois Connections" by M. Erné, et al. [EKMS92], which offers many other examples of Galois connection to the interested reader.

Definition 5.11. Let $\mathscr{P} = (P, \leq)$ and $\mathscr{Q} = (Q, \sqsubseteq)$ be posets. Let $\pi_* : P \to Q$ and $\pi^* : Q \to P$ be functions such that for all $p \in P$ and $q \in Q$:

$$p \leq \pi^*(q) \iff \pi_*(p) \sqsubseteq q,$$

then the quadruple $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q})$ is a **monotone Galois connection**.

If $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q})$ is a monotone Galois connection, $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q}')$ is an **antitone Galois connection**.

[27] See Chapter 7 of "Fields and Galois Theory" by J. S. Milne [Mil20b] or Section 9.22 of "The Stacks Project" [The21]

We will now establish that the Galois correspondence is indeed a Galois connection, even for infinite extensions:

Proposition 5.12. Let $K \subseteq L$ be a (finite or infinite) Galois extension. Let $\mathscr{P} = (P, \leq)$, $\mathscr{Q} = (Q, \sqsubseteq)$ be the posets defined as

$$\begin{aligned} \mathscr{P} &= \{\text{subgroups of } \operatorname{Aut}(L|K)\}, & H \leq G &\iff H \subseteq G, \\ \mathscr{Q} &= \{\text{intermediate fields } K \subseteq E \subseteq L\}, & E \sqsubseteq F &\iff E \supseteq F, \end{aligned}$$

and let

$$\begin{aligned} &\pi_* : P \ni H \mapsto L^H = \{\alpha \in L \mid \forall \sigma \in H : \sigma(\alpha) = \alpha\} \in Q, \\ &\pi^* : Q \ni E \mapsto \operatorname{Aut}(L|E) \in P. \end{aligned}$$

Then $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q})$ is a monotone Galois connection.

Proof. First, we note that the maps π_* and π^* are well defined. Indeed, L^H is a field and $K \subseteq L^{\operatorname{Aut}(L|K)} \subseteq L^H \subseteq L^{\{e\}} = L$. Moreover, by Proposition 5.7, L is Galois over any intermediate field $K \subseteq E \subseteq L$.

Assume that $H \leq \pi^*(E)$. Then

$$\begin{aligned} & H \leq \pi^*(E) \\ \implies & H \subseteq \operatorname{Aut}(L|E) \\ \implies & L^H = \{\alpha \in L \mid \forall \sigma \in H : \sigma(\alpha) = \alpha\} \supseteq \{\alpha \in L \mid \forall \sigma \in \operatorname{Aut}(L|E) : \sigma(\alpha) = \alpha\} \supseteq E \\ \implies & \pi_*(H) \sqsubseteq E. \end{aligned}$$

Conversely, assume that $\pi_*(H) \sqsubseteq E$. Then

$$\begin{aligned} & \pi_*(H) \sqsubseteq E \\ \implies & L^H \supseteq E \\ \implies & H \subseteq \{\sigma \in \operatorname{Aut}(L|K) \mid \forall \alpha \in L^H : \sigma(\alpha) = \alpha\} \\ & \qquad \subseteq \{\sigma \in \operatorname{Aut}(L|K) \mid \forall \alpha \in E : \sigma(\alpha) = \alpha\} = \operatorname{Aut}(L|E) \\ \implies & H \leq \pi^*(E). \end{aligned}$$

□

Note that the inclusion relationships for the intermediate field poset ($\mathscr{Q}$ in the above) are reversed. That is because the Galois connection established by the FTGT is actually antitone. However, most literature deals only with monotone Galois connections, so it is preferable to work with the dual poset.

Recall now the notion of a closure operation:

Definition 5.13. Let $\mathrm{Cl} : P \to P$ be a self-map on the poset $\mathscr{P} = (P, \leq)$. We say Cl is a **closure operation** if Cl is

1. Isotone: $\forall p, p' \in P : p \leq p' \implies \mathrm{Cl}(p) \leq \mathrm{Cl}(p')$,
2. Increasing: $\forall p \in P : p \leq \mathrm{Cl}(p)$,
3. Idempotent: $\forall p \in P : \mathrm{Cl}(\mathrm{Cl}(p)) \leq \mathrm{Cl}(p)$[28].

These are the properties that can be found in topological closures. This is no accident: topological closures are just an example of Moore closures, which generalise many closure-like operations. For the interested reader, they are discussed in depth in Chapter 4 of "Handbook of Analysis and Its Foundations" by E. Schechter [Sch97].

The relevance of closure operations to Galois connection is clarified by the following proposition:

Proposition 5.14. Let $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q})$ be a monotone Galois connection. Then $\pi^*\pi_* : P \to P$ is a closure operation on $\mathscr{P}$.

Proof. Let $p, p' \in P$, $q, q' \in Q$. First we show $\pi^*\pi_*$ is increasing:

$$\pi_*(p) \sqsubseteq \pi_*(p) \iff p \leq (\pi^*\pi_*)(p).$$

Similarly, we can show that $\pi_*\pi^* s$ is decreasing:

$$\pi^*(q) \leq \pi^*(q) \iff (\pi_*\pi^*)(q) \sqsubseteq q.$$

Next, $\pi^*\pi_*$ and $\pi_*\pi^*$ are isotone:

$$\begin{aligned} p \leq p' &\implies p \leq (\pi^*\pi_*)(p') \implies \pi_*(p) \sqsubseteq \pi_*(p'), \\ q \sqsubseteq q' &\implies (\pi_*\pi^*)(q) \sqsubseteq q' \implies \pi^*(q) \leq \pi^*(q'). \end{aligned}$$

Finally, $\pi^*\pi_*$ and $\pi_*\pi^*$ are idempotent:

$$\begin{aligned} (\pi_*\pi^*)(\pi_*(p)) \sqsubseteq \pi_*(p) &\implies (\pi_*\pi^*\pi_*)(p) \sqsubseteq \pi_*(p) \implies (\pi^*\pi_*\pi^*\pi_*)(p) \leq (\pi^*\pi_*)(p), \\ \pi^*(q) \leq (\pi^*\pi_*)(\pi^*(q)) &\implies \pi^*(q) \leq (\pi^*\pi_*\pi^*)(q) \implies (\pi_*\pi^*)(q) \sqsubseteq (\pi_*\pi^*\pi_*\pi^*)(q). \end{aligned}$$

□

We will call the elements of P^π, the $\pi^*\pi_*$-image of P, **π-closed**. Since $\pi^*\pi_*$ is idempotent, it acts as the identity map on P^π. It is easy to see that π_* and π^* are mutual inverses when restricted to P^π [EKMS92, Prop. 3]. Thus we have found a class of subgroups on which the Galois connection given

[28] Note that for idempotency, equality follows by applying the increasing property.

by the FTGT acts as an isomorphism of categories. We will show later that every intermediate field occurs as a fixed field of some Galois group, i.e. our map π_* is a surjection.

5.3 Constructing the Krull Topology

We will now focus on giving a topological meaning to the π-closed subgroups. It seems natural to take them as the closed subgroups, interpreting the closure operation we derived from the Galois connection as the topological closure restricted to subgroups. If a coherent topology can be constructed on this premise, it would allow for a generalisation of the finite FTGT restricted to topologically closed subgroups.

The simplest way to construct our topology would be picking a set of open subgroups and constructing an open neighbourhood base of the identity. Then, through Lemma 3.6, we can reconstruct the topology from the neighbourhood base. As for the selection of our open subgroups, we recall that by Proposition 3.7, all the open subgroups of our desired topology must be π-closed. Moreover, since we are trying to construct a profinite topology, which is compact, by Proposition 3.9 the open subgroups will be exactly the π-closed, finite index subgroups. Having made this selection, we are now left to prove this is a valid topology, with the properties we expect. In doing so, we will recover the traditional characterisation of the Krull topology, given in terms of finite Galois extensions.

Definition 5.15. Let G be a group and S a G-set. Then the **stabilizer** of G with respect to S is defined as

$$G(S) = \{g \in G \mid \forall s \in S : g(s) = s\} = \bigcap_{s \in S} G(\{s\}).$$

Clearly, for any G-set, the stabilizer of G is a subgroup of G. We will now show that our "open" subgroups arise exactly as stabilizer of $\mathrm{Aut}(L|K)$ with respect to finite sets.

Lemma 5.16. Let $K \subseteq E \subseteq L$ be an infinite Galois extension and suppose $H = \mathrm{Aut}(L|E)$ is a finite index subgroup of $G = \mathrm{Aut}(L|K)$. Then $H = G(S)$ for some finite subset $S \subset E$.

Proof. By definition, we have

$$H = \{\sigma \in G \mid \forall \alpha \in E : \sigma(\alpha) = \alpha\} = G(E).$$

Thus we must show that there exists a finite subset of E that has the same stabilizer.

By contradiction, assume false, i.e. there is no finite subset $S \subset E$ such that $G(S) = H$. Then we can construct the following sequence of sets $(S_i)_{i \in \mathbb{N}}$: let $S_1 = \emptyset$ and for each $i > 1$, $S_i = S_{i-1} \cup \{\alpha_i\}$, where α_i chosen in E such that there exists some $\sigma_i \in G(S_{i-1}) \setminus H$, which is non-empty by assumption, with $\sigma_i(\alpha_i) \neq \alpha_i$. This implies that $G = G(S_1)$ and for each $i \in \mathbb{N}$, $H < G(S_{i+1}) < G(S_i)$.

By inductive application of Lagrange's theorem, we get

$$[G(S_1) : G(S_2)][G(S_2) : G(S_3)] \cdots [G(S_{n+1}) : H] = [G : H] = n.$$

But we have by assumption $[G(S_i) : G(S_{i+1})] > 1$, hence

$$\prod_{i=1}^{n} [G(S_i) : G(S_{i+1})] \geq 2^n > n,$$

which is a contradiction. □

We must also show that the other direction holds, i.e. every stabilizer with respect to a finite subset of our field L is a π-closed subgroup of finite index. To show this we introduce the following results:

Proposition 5.17. Let $K \subseteq E \subseteq L$ be an infinite Galois extension. Every K-homomorphism $E \to L$ extends to a K-isomorphism $L \to L$.

Proof. See Proposition 7.4 in Chapter 7 of "Field and Galois Theory" by J. S. Milne [Mil20b]. □

Lemma 5.18. Let $K \subseteq L$ be a Galois extension. Then $L^{\mathrm{Gal}(L|K)} = K$.

Proof. Clearly $K \subseteq L^{\mathrm{Gal}(L|K)}$. Moreover, suppose $K \neq L^{\mathrm{Gal}(L|K)}$ and let $\alpha_1 \in L^{\mathrm{Gal}(L|K)} \backslash K$. We know α_1 lies in some finite Galois extension $K(\alpha_1, \ldots, \alpha_n)$ of K. Then we can find some $\sigma \in \mathrm{Gal}(K(\alpha_1, \ldots, \alpha_n)|K)$ which does not fix α_1. But by Proposition 5.17, σ can be extended to an element of $\mathrm{Gal}(L|K)$ that does not fix α_1, contradicting the assumption [Mil20b, Prop. 7.9]. □

Note that the Lemma above is equivalent to the surjectivity of π_* in the Galois connection defined in Proposition 5.12.

Lemma 5.19. Let $K \subset L$ be an infinite Galois extension and suppose $H = G(S)$ is the stabilizer of $G = \mathrm{Aut}(L|K)$ with respect to some finite $S \subset L$. Then H is of finite index and π-closed, i.e. $H = \mathrm{Aut}(L|E)$ for some intermediate field $K \subseteq E \subseteq L$ by Lemma 5.18.

Proof. Take $E = K(S)$. Since S is finite, this is a finite extension of K. Moreover, we know L is Galois over E. By expanding the definitions, we get

$$\begin{aligned} \mathrm{Aut}(L|E) &= \{\sigma \in G \mid \forall \alpha \in K(S) : \sigma(\alpha) = \alpha\} \\ &= \{\sigma \in G \mid \forall \alpha \in S : \sigma(\alpha) = \alpha\} = G(S) = H. \end{aligned}$$

Since H is in the image of the Galois connection, it is π-closed. Consider the restriction map

$$\theta : G \ni \sigma \mapsto \sigma|_E \in \mathrm{Hom}_K(E, L).$$

Since by Proposition 5.17 every K-homomorphism $E \to L$ can be extended to a K-isomorphism $L \to L$, θ is surjective. Since it has kernel H, it is injective on the coset space. Thus θ defines a bijection between the coset space G/H and $\mathrm{Hom}_K(E, L)$, which is finite because E is a finite extension of K. Thus H is of finite index. □

We can now finally show that the previous steps lead to a valid topology:

Theorem 5.20. Let $K \subset L$ be an infinite Galois extension. There exists a unique structure of topological group on $G = \mathrm{Aut}(L|K)$ for which the subgroups $G(S)$ for finite $S \subset L$ form an open neighbourhood base of the identity. For this topology, the subgroups $G(S)$ where S is G-stable form an open neighbourhood base of the identity consisting of normal subgroups.

Proof. For the first statement, we must check our collection of $G(S)$ satisfies conditions (1,2,3,4) of Lemma 3.6. Condition (1) is satisfied since $G(S_1 \cup S_2) = G(S_1) \cap G(S_2)$. Conditions (2) and (3) are satisfied because each $G(S)$ is a group.

Let $S \subset L$ be finite. Then $K(S)$ is a finite extension of K, so there are finitely many K-homomorphisms $K(S) \to L$. Since $\sigma|_{K(S)} = \tau|_{K(S)}$ implies $\sigma(S) = \tau(S)$, we know $\overline{S} = \bigcup_{\sigma \in G} \sigma(S)$ is finite. Clearly for all $\sigma \in G$, we have $\sigma(\overline{S}) = \overline{S}$, so $G(\overline{S})$ is normal in G. Therefore, $\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subseteq G(S)$, which satisfies (4) and proves the second statement [Mil20b, Prop. 7.6]. □

The topology established by the previous proposition is called the Krull topology. To present it in the more typical form, we need one more proposition:

Proposition 5.21. Let $K \subseteq E \subseteq L$ be a Galois extension. If E is stable under $\mathrm{Aut}(L|K)$ then it is Galois over K.

Proof. Let $\alpha \in E$ with minimal polynomial $m_{\alpha,K} \in K[X]$. Since L is Galois over K, $m_{\alpha,K}$ has $n = \deg(m_{\alpha,K})$ distinct roots $\alpha_1, \ldots, \alpha_n \in L$. Then for each α_i, there is a K-isomorphism $K(\alpha) \to K(\alpha_i)$ which sends α to α_i. By Proposition 5.17, this can be extended to a K-isomorphism $L \to L$. Since E is stable under $\mathrm{Aut}(L|K)$, $\alpha_i \in E$, thus E is Galois over K [Mil20b, Cor. 7.5]. □

Definition 5.22. Let $K \subset L$ be an infinite Galois extension. The **Krull topology** on $\mathrm{Aut}(L|K)$ is the unique topology which has

$$\{\mathrm{Gal}(L|E) \mid E \text{ finite and Galois over } K\}$$

as an open neighbourhood base of the identity consisting of normal subgroups. When equipped with the Krull topology, we call $\mathrm{Aut}(L|K)$ the **Galois group** of L over K and denote it $\mathrm{Gal}(L|K)$.

We haven't yet shown that Galois groups are profinite. To prove that, we need to introduce the following proposition:

Proposition 5.23. Let $K \subseteq E \subset L$ be an infinite Galois extension with E finite and Galois over K, the restriction map

$$\theta : \mathrm{Gal}(L|K) \ni \sigma \mapsto \sigma|_E \in \mathrm{Gal}(E|K),$$

is a continuous surjection when $\mathrm{Gal}(E|K)$ is given the discrete topology.

Proof. Let $\sigma \in \mathrm{Gal}(E|K)$ and regard it as a K-isomorphism $E \to L$. Then by Proposition 5.17, we can extend σ to a K-isomorphism $L \to L$, thus θ is surjective.

Let S be a finite set of generators of E. We have $\mathrm{Gal}(L|E) = G(S)$, so the inverse of $e_{\mathrm{Gal}(E|K)}$ under θ is open in G. By homogeneity, this is true for every element of $\mathrm{Gal}(E|K)$, so θ is continuous [Mil20b, Prop. 7.7]. □

Instead of directly proving infinite Galois groups are profinite, we will show that they are compact, Hausdorff and totally disconnected, from which it will follow that they are profinite.

Lemma 5.24. Let $K \subset L$ be an infinite Galois extension. The Galois group $\mathrm{Gal}(L|K)$ is compact, Hausdorff and totally disconnected.

Proof. Take distinct $\sigma, \tau \in G$. Then there must exist some $\alpha \in L$ such that $\sigma(\alpha) \neq \tau(\alpha)$. For any finite $S \subset L$ containing α, $\sigma G(S)$ and $\tau G(S)$ are disjoint, since their elements act differently on α. So we have found disjoint open sets containing σ and τ, which means G is Hausdorff.

By the argument in Theorem 5.20, if S is stable under G, $G(S)$ is a finite index normal subgroup of G. Since every finite set is contained in some finite stable set, let $\mathcal{S}$ be the family of finite and stable subsets of L and consider the homomorphism

$$\psi : G \ni \sigma \mapsto (\sigma G(S))_{S \in \mathcal{S}} \in \prod_{S \in \mathcal{S}} G/G(S).$$

By the previous argument ψ is injective. Endowing $\prod G/G(S)$ with the product topology, the induced topology on G has the subgroups $G(S)$ as an open neighbourhood base of the identity, so it coincides with the Krull topology. Moreover, we have that $\prod G/G(S)$ is compact by Tychonoff's theorem, so it remains to check that G is a closed subgroup.

Let $S_1 \subset S_2 \in \mathcal{S}$ and consider the following diagram:

$$\begin{array}{ccc} & \prod G/G(S) & \\ {\scriptstyle \rho_2}\swarrow & & \searrow{\scriptstyle \rho_1} \\ G/G(S_2) & \xrightarrow[\gamma]{} & G/G(S_1) \end{array}$$

where ρ_1, ρ_2 are the projection maps and γ is the quotient map. Let $E(S_1, S_2)$ be the closed subset of $\prod G/G(S)$ for which the diagram commutes. Then $G = \bigcap_{S_1 \subset S_2 \in \mathcal{S}} E(S_1, S_2)$ is closed, hence compact.

Finally, for each $S \in \mathcal{S}$, $G(S)$ is a subgroup that is open and hence closed. The connected component of G containing the identity e is $\bigcap G(S) = \{e\}$. By homogeneity, this is true for every element of G, so G is totally disconnected [Mil20b, Prop. 7.8]. □

Corollary 5.24.1. Every Galois group is canonically isomorphic as a topological space to a profinite group.

Proof. This follows from Theorem 4.7, with the isomorphism given by the homomorphism ψ defined above. □

This incredible result has several weaker converse statements. Since Galois groups must be specified over some base field, this choice of base field must be clarified when stating the converse theorem. The strongest version currently proven is the following:

Theorem 5.25. Every profinite group is isomorphic as topological space to the Galois group of some Galois extension over a field of characteristic zero.

Proof. See Corollary to Theorem 1.3 in "Cohomologie des groupes compact totalement discontinus" by A. Douady [Dou60] or Theorem 3.3.2 in "Profinite Groups" by J. S. Wilson [Wil98] for explicit construction. □

5.4 The Infinite Fundamental Theorem

Having covered a lot of ground, it is useful to stop and summarise our results so far. We started by extending the Galois correspondence to infinite Galois extensions, proving it was an example of a Galois connection. We then showed that the connection acted as closure, and gave it topological meaning, constructing the Krull topology. Finally, we showed that this made Galois groups profinite.

Before concluding the chapter with some examples, we will prove the full infinite Fundamental Theorem of Galois Theory.

Theorem 5.26. Let $K \subset L$ be an infinite Galois extension with Galois group $G = \mathrm{Gal}(L|K)$, equipped with Krull topology. The Galois connection $(\mathscr{P}, \pi_*, \pi^*, \mathscr{Q})$ defined in Proposition 5.12, is an isomorphism of categories when restricted the closed subgroups of G. Moreover,

1. The connection is inclusion reversing, i.e. it defines a contravariant functor,
2. For a closed subgroup H of G, H is open $\iff$ H has finite index in G $\iff$ L^H has finite degree over K, in which case $[G : H] = [L^H : K]$,
3. If H corresponds to E, for all $\sigma \in G$, $\sigma H \sigma^{-1}$ corresponds to σE,
4. A closed subgroup of H of G is normal if and only if L^H is Galois over K, in which case $G/H \cong \mathrm{Gal}(L^H|K)$

Proof. By Lemma 5.16 and Lemma 5.19, we know P^π is exactly the poset of closed subgroups of G. By Lemma 5.18, we know every intermediate field occurs as some fixed field of a closed subgroup. Hence, the connection is a bijection between the closed subgroups and the intermediate fields, i.e. between P^π and Q.

Since, when restricted, π_* and π^* are mutual inverses, we have

$$\forall p, p' \in P^\pi,\ p \leq p' \iff \pi_*(p) \sqsubseteq (\pi^*)^{-1}(p') \iff \pi_*(p) \sqsubseteq \pi_*(p'),$$
$$\forall q, q' \in Q,\ q \sqsubseteq q' \iff (\pi_*)^{-1}(q) \leq \pi^*(q') \iff \pi^*(q) \leq \pi^*(q').$$

Therefore the connection carries morphisms. It is easy to see that it indeed defines an isomorphism of categories. This also proves (1), since we defined $\mathscr{Q}$ by duality, i.e. with the inclusions reversed.

For the first claim of (2):

- Assume H has finite index in G. Since H is closed, by Proposition 3.8, H is open.
- Assume H is open. Since the subgroups corresponding to finite Galois extensions form an open neighbourhood base of the identity, there must be some $N = \mathrm{Gal}(L|E)$ for some finite Galois extension E of K such that $N \subseteq H$. Since by (1) the connection is inclusion reversing, $L^H \subseteq L^N = E$, thus by Tower Law $[E : L^H][L^H : K] = [E : K]$, which is finite, so $[L^H : K]$ must also be finite.
- Assume $[L^H : K]$ is finite. Write $L^H = K(S)$ where $S = \{\alpha_1, \ldots, \alpha_n\}$, and consider $E = K(\overline{S})$, where $\overline{S} = \bigcup_{\sigma \in G} \sigma(S)$. By the same argument as Theorem 5.20, E is finite Galois over K. Clearly, $L^H \subseteq E$, thus $N = \mathrm{Gal}(L|E) \subseteq H$. But N is open, so by Proposition 3.9 it has finite index. So $[G : H] \leq [G : N] < \infty$, so H has finite index in G [SR18, Thm. 2.17].

For the second claim of (2), suppose $[L^H : K] = n$. From finite Galois theory, we know there are exactly n injective K-homomorphisms $L^H \to L$. By Proposition 5.17, they can be extended to K-automorphisms of L. It is easy to see that these correspond to the cosets of H in G, thus proving the claim [Wil98, Prop. 3.2.2].

For (3), consider $\tau \in G$ and $\alpha \in L$. We have $\tau(\alpha) = \alpha$ if and only if $(\sigma\tau\sigma^{-1})(\sigma(\alpha)) = \sigma(\alpha)$. Hence $\mathrm{Gal}(L|\sigma E) = \sigma\,\mathrm{Gal}(L|E)\sigma^{-1}$, which proves the claim [Mil20b, Thm. 7.12].

For (4), suppose H corresponds to E. From (3), H is normal in G if and only if E is stable under G. But E is stable under G if and only it is the union of finite extensions of K stable under G, or finite Galois extensions of K. Hence H is normal in G if and only E is Galois over K. Applying the First Isomorphism Theorem to the restriction homomorphism $\sigma \mapsto \sigma|_E$ proves the claim [Mil20b, Thm. 7.12]. □

5.5 Examples

5.5.1 Example: $\mathbb{Z}_p$ as a Galois group over $\mathbb{Q}$

We will now turn to an example application of the infinite Fundamental Theorem of Galois Theory, in which we will show how the additive group of p-adic integers $\mathbb{Z}_p$ can be realised as a Galois group over $\mathbb{Q}$. This example is of fundamental importance to Iwasawa Theory, which is a topic well beyond the scope of this discussion. Nevertheless, we can present a brief introduction to cyclotomic extensions as

discussed in "Introduction to Iwasawa Theory" by D. Burns [Bur18] and "An Introduction to Iwasawa Theory" by J. L. Brown [Bro06].

To this end, let p be an odd prime and, taking $\mathbb{Q}$ as the base field, consider for each $n \in \mathbb{N}$ the extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$, where ζ_n is the n-th root of unity $\exp(\frac{2\pi i}{n})$. We call extensions of the form $\mathbb{Q}(\zeta_n)$ **cyclotomic extensions** of $\mathbb{Q}$. In this example we will consider cyclotomic extensions of the form $K_n = \mathbb{Q}(\zeta_{p^n})$, whose Galois groups can be parametrised as follows:

Proposition 5.27. For $n \in \mathbb{N}$, we have $\mathrm{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof. First, we observe that every element of $\sigma \in \mathrm{Gal}(K_n|\mathbb{Q})$ can be specified by where it sends ζ_{p^n} and that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$ for some $a \in \mathbb{Z}$. Consider now the map

$$\theta : \mathrm{Gal}(K_n|\mathbb{Q}) \ni (\sigma : \zeta_{p^n} \mapsto \zeta_{p^n}^a) \mapsto [a]_{p^n} \in (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

We know that θ is well-defined since if $\sigma : \zeta_{p^n} \mapsto \zeta_{p^n}^a$ is in the Galois group $\mathrm{Gal}(K_n|\mathbb{Q})$ then p does not divide a. Moreover, θ is surjective since the Galois group acts transitively on $\{\zeta_{p^n}^a \mid 1 \leq a < p^n \wedge \gcd(a,p) = 1\}$[29] and injective since if $\sigma(\zeta_{p^n}) = \tau(\zeta_{p^n})$ then $\sigma = \tau$. Finally, θ is a homomorphism since

$$\theta((\sigma : \zeta_{p^n} \mapsto \zeta_{p^n}^a) \circ (\tau : \zeta_{p^n} \mapsto \zeta_{p^n}^b)) = \theta(\sigma \circ \tau : \zeta_{p^n} \mapsto \zeta_{p^n}^{ab}) = [ab]_{p^n} = \theta(\sigma)\theta(\tau).$$

□

Consider now the field

$$K_\infty = \varinjlim_{n\in\mathbb{N}} K_n = \bigcup_{n\in\mathbb{N}} K_n,$$

where the direct limit is taken with respect of the direct system $(K_n, \iota_{nm}, \mathbb{N})$, where $\iota_{nm} : \mathbb{Q}(\zeta_{p^n}) \to \mathbb{Q}(\zeta_{p^m})$ are the inclusion homomorphisms. By the duality established by the FTGT, the Galois group of K_∞ over $\mathbb{Q}$ will be given by the inverse limit

$$\mathrm{Gal}(K_\infty|\mathbb{Q}) = \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(K_n|\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times,$$

where the last equality holds because $\mathbb{Z}_p^\times$ is a closed subgroup of $\mathbb{Z}_p$, hence Proposition 4.9 applies.

Recall the decomposition of $\mathbb{Z}_p^\times$ for odd primes p through the logarithm map we analysed in Theorem 4.47. Hence

$$\mathrm{Gal}(K_\infty|\mathbb{Q}) \cong \mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p^+,$$

so we can identify a torsion and a torsion-free component of $\mathrm{Gal}(K_\infty|\mathbb{Q})$. We can realise $\mathbb{Z}_p^+$ as a Galois group by considering the fixed field of K_∞ given by K_∞^Δ, where $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Definition 5.28. Let K_∞ and Δ be as above. We call $\mathbb{Q}_\infty = K_\infty^\Delta$ the **cyclotomic $\mathbb{Z}_p$-extension** of $\mathbb{Q}$.

[29] This is equivalent to proving that K_n is the splitting field of the polynomial $\Phi_{p^n}(x) = (x^{p^n} - 1)/(x^{p^{n-1}} - 1)$ over $\mathbb{Q}$. For a proof of this equivalent statement, see Theorem 5.10 in Chapter 5 of "Fields and Galois Theory" by J. S. Milne [Mil20b].

To see that $\mathrm{Gal}(\mathbb{Q}_\infty|\mathbb{Q})$ is indeed topologically isomorphic to $\mathbb{Z}_p$ we can turn to the infinite FTGT: $\mathbb{Z}_p$ is a finite index closed normal subgroup of $\mathbb{Z}_p^\times$ hence

$$\mathrm{Gal}(\mathbb{Q}_\infty|\mathbb{Q}) \cong \mathrm{Gal}(K_\infty|\mathbb{Q}) \Big/ \mathrm{Gal}(K_\infty|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p^+ \Big/ (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}_p^+.$$

Similarly, since for every $n \in \mathbb{N}$, $p^n\mathbb{Z}_p$ is a finite index closed normal subgroup of $\mathbb{Z}_p$, there exists a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ [Bur18, Pg. 5].

Cyclotomic extensions of number fields have an incredible importance in infinite Galois theory. In particular, we cite a particularly significant result known as Kronecker-Weber Theorem, which states the following:

Theorem 5.29. Every finite abeliean extension[30] of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$.

Proof. See Theorem 2 in "The Kronecker-Weber Theorem" by E. Ghate [Gha99]. □

To conclude the example, we note that we can also construct a cyclotomic $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}$ by adjoining all $\mathbb{Q}(\zeta_n)$ for each $n \in \mathbb{N}$, where the inverse system is indexed by the poset $(\mathbb{N}, |)$. Since this construction is very similar to the $\mathbb{Z}_p$ case we have shown, we will focus instead on the more interesting example of realising $\hat{\mathbb{Z}}$ as a Galois group over the finite field $\mathbb{F}_p$.

5.5.2 Example: $\hat{\mathbb{Z}}$ as a Galois group over $\mathbb{F}_p$

Having provided an example of realising profinite groups as Galois groups over a field of characteristic zero, we now present an example of the same procedure over a field of positive characteristic. In particular, we wish to show how $\hat{\mathbb{Z}}$ arises as the absolute Galois group over the finite field $\mathbb{F}_p$. Once again the discussion follows "Introduction to Iwasawa Theory" by D. Burns [Bur18]. Moving from the basics, let $q = p^n$ for some $n \in \mathbb{N}$ and denote by $\mathbb{F}_q$ the splitting field of $X^q - X$ over $\mathbb{F}_p$. By finite Galois theory, we can find a generator of $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$ for every $n \in \mathbb{N}$:

Proposition 5.30. The Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$ is cyclic and generated by the Frobenius automorphism $\sigma(\alpha) = \alpha^p$.

Proof. See Proposition 4.20 in Chapter 4 of "Fields and Galois Theory" by J. S. Milne [Mil20b]. □

It follows that $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Consider now the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ given by

$$\overline{\mathbb{F}_p} = \varinjlim_{n\in\mathbb{N}} \mathbb{F}_{p^n} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n},$$

[30] An abelian extesion is a Galois extension whose Galois group is abelian.

where the index poset is $(\mathbb{N}, |)$. By duality, the absolute Galois group can be written as

$$\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p) = \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

This shows how $\hat{\mathbb{Z}}$ can be realised as a Galois group over $\mathbb{F}_p$. It follows that $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ is not generated by the Frobenius automorphism as an abstract group, but only topologically generated by it with respect to the Krull topology.

6 Conclusion

To conclude this discussion, let us summarise the concepts we covered. In the first chapter, we looked at how category theoretical machinery can help us construct global objects from finite projections through the inverse limit construction. To aid our understanding of inverse limits of finite groups, in the second chapter we explored the basic properties of objects which are equipped with compatible topological and group structure. Our focus then shifted to profinite groups themselves. We characterised them as topological groups and constructed a procedure to obtain profinite groups out of abstract groups. We then concerned ourselves with the order and generators of profinite groups, exploring the Frattini subgroup as an efficient way to compute generators of pro-p groups. Finally, we wrapped our discussion with a self-contained proof of the infinite Fundamental Theorem of Galois Theory.

Throughout the discussion, we analysed several examples of high relevance to modern number theory, such as the p-adic integers $\mathbb{Z}_p$ and the profinite integers $\hat{\mathbb{Z}}$, which we have explored from the construction to a full description of the structure, generators and realisability as Galois groups. Furthermore, we presented the lesser known example of the Nottingham group $\mathcal{J}(\mathbb{F}_p)$, uncovering its finitely generated pro-p structure.

However, ours was by no means an exhaustive account of this area of research. Future research should focus on the topic of linear groups over the p-adics. These groups are obtained as closed subgroups of the general linear group over the p-adics $GL_n(\mathbb{Z}_p) = \varprojlim_{n\in\mathbb{N}} GL_n(\mathbb{Z}/p^n\mathbb{Z})$ and are of significant interest as an introduction to p-adic Lie theory. We recommend the interested reader to "p-adic Lie Groups" by P. Schneider [Sch11].

Acknowledgements

I would like to thank Prof. Fred Diamond for his incredible support and for suggesting this fascinating project, the project coordinator Dr. Giuseppe Tinaglia for his assistance.

Appendix - Primer on Category Theory

This Appendix is dedicated to giving a self-contained primer on the most relevant category theoretical notions necessary for our discussion. The definitions and results are distilled from "Categories and Functors" by B. Paraigis [Par70].

Definition 6.1. A **category** $\mathscr{C}$ is a class of objects $A, B, C, \cdots \in \text{Obj}\mathscr{C}$ together with

1. A family of mutually disjoint sets $\{\text{Mor}_{\mathscr{C}}(A, B)\}$ for all objects $A, B \in \text{Obj}\mathscr{C}$, whose elements $f, g, h, \cdots \in \text{Mor}_{\mathscr{C}}$ are called **morphisms**,

2. A family of maps $\{\text{Mor}_{\mathscr{C}}(A, B) \times \text{Mor}_{\mathscr{C}}(B, C) \ni (f, g) \mapsto gf \in \text{Mor}_{\mathscr{C}}(A, C)\}$ for all $A, B, C \in \text{Obj}\mathscr{C}$, called **compositions**,

satisfying

1. **Associativity**: for all $A, B, C, D \in \text{Obj}\mathscr{C}$ and for all $f \in \text{Mor}_{\mathscr{C}}(A, B)$, $g \in \text{Mor}_{\mathscr{C}}(B, C)$ and $h \in \text{Mor}_{\mathscr{C}}(C, D)$, $h(gf) = (hg)f$,

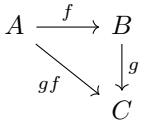
2. **Identity**: for all objects $A \in \text{Obj}\mathscr{C}$, there exist a morphism $1_A \in \text{Mor}_{\mathscr{C}}(A, A)$, called the **identity**, such that for all $B, C \in \text{Obj}\mathscr{C}$, $f \in \text{Mor}_{\mathscr{C}}(A, B)$, $g \in \text{Mor}_{\mathscr{C}}(C, A)$, $f1_A = f$ and $1_A g = g$.

The most relevant examples of categories include:

- **Set**, where the objects are sets and the morphisms are functions.
- **Grp**, where the objects are groups and the morphisms are homomorphisms.
- **Top**, where the objects are topological spaces and the morphisms are continuous functions.
- **TopGrp**, where the objects are topological groups and the morphisms are continuous homomorphisms.

Note that a rigorous description of the **Set** category requires to work within a specific set theory, hence it will be omitted here. The reader is referred to the Apprendix on "Fundamentals of Set Theory" in "Categories and Functors" by B. Pareigis [Par70].

Categories can be illustrated by **commutative diagrams**, directed graphs in which objects are represented by vertices and morphisms by edges. Commutativity refers to the invariance of under path taken of morphism application [Par70, Pg. 9]. Below is an example of a diagram, with the identity morphisms omitted for clarity.



Maps between categories which respect the structure are called functors:

Definition 6.2. Let $\mathscr{A}, \mathscr{B}$ be categories, a **covariant functor** $\mathscr{F}$ consists of

1. A map $\mathrm{Obj}\mathscr{B} \ni A \mapsto \mathscr{F}(A) \in \mathrm{Obj}\mathscr{C}$,
2. A family of maps $\{\mathrm{Mor}_{\mathscr{B}}(A,B) \ni f \mapsto F(f) \in \mathrm{Mor}_{\mathscr{C}}(\mathscr{F}(A), \mathscr{F}(B))\}$ for all $A, B \in \mathrm{Obj}\mathscr{B}$,

satisfying

1. for all objects $A \in \mathrm{Obj}\mathscr{B}$, $\mathscr{F}(1_A) = 1_{\mathscr{F}(A)}$,
2. for all $A, B, C \in \mathrm{Obj}\mathscr{B}$ and for all $f \in \mathrm{Mor}_{\mathscr{B}}(B,C)$, $g \in \mathrm{Mor}_{\mathscr{B}}(A,B)$, $\mathscr{F}(fg) = \mathscr{F}(f)\mathscr{F}(g)$.

Similarly, a **contravariant functor** $\mathscr{F}$ consists of

1. A map $\mathrm{Obj}\mathscr{B} \ni A \mapsto \mathscr{F}(A) \in \mathrm{Obj}\mathscr{C}$,
2. A family of maps $\{\mathrm{Mor}_{\mathscr{B}}(A,B) \ni f \mapsto \mathscr{F}(f) \in \mathrm{Mor}_{\mathscr{C}}(\mathscr{F}(B), \mathscr{F}(A))\}$ for all $A, B \in \mathrm{Obj}\mathscr{B}$,

satisfying

1. for all objects $A \in \mathrm{Obj}\mathscr{B}$, $\mathscr{F}(1_A) = 1_{\mathscr{F}(A)}$,
2. for all $A, B, C \in \mathrm{Obj}\mathscr{B}$ and for all $f \in \mathrm{Mor}_{\mathscr{B}}(B,C)$, $g \in \mathrm{Mor}_{\mathscr{B}}(A,B)$, $\mathscr{F}(fg) = \mathscr{F}(g)\mathscr{F}(f)$.

To each category, there corresponds a dual or opposite category, where the morphisms run in the opposite direction:

Definition 6.3. Let $\mathscr{C}$ be a category, the **dual** $\mathscr{C}'$ of $\mathscr{C}$ is defined by

1. The objects are $\mathrm{Obj}\mathscr{C}' := \mathrm{Obj}\mathscr{C}$,
2. The morphisms are $\mathrm{Mor}_{\mathscr{C}'}(A,B) := \mathrm{Mor}_{\mathscr{C}}(B,A)$,
3. The compositions are $\mathrm{Mor}_{\mathscr{C}'}(A,B) \times \mathrm{Mor}_{\mathscr{C}'}(B,C) \ni (f,g) \mapsto fg \in \mathrm{Mor}_{\mathscr{C}'}(A,C)$

The following two results about dual categories are immediate:

Lemma 6.4. For any category $\mathscr{C}$, the dual $\mathscr{C}'$ of $\mathscr{C}$ is a category.

Lemma 6.5. For any category $\mathscr{C}$, $\mathscr{C} = (\mathscr{C}')'$.

Introducing the notion of duality allows introduce the **duality principle**, which is extremely helpful in proving extending results from categories to their duals.

Definition 6.6. Let $\mathfrak{F}(\mathscr{C})$ be a formula with a free class variable $\mathscr{C}$. We call $\mathfrak{F} = \mathfrak{F}(\mathscr{C})$ a **theorem on categories** if for all classes $\mathscr{C}$, if $\mathscr{C}$ is a category then $\mathfrak{F}(\mathscr{C})$ holds.

Definition 6.7. Let $\mathfrak{F}$ be a theorem on categories, the **dual formula** $\mathfrak{F}'$ to $\mathfrak{F}$ is defined by $\mathfrak{F}'(\mathscr{D}) = \exists \mathscr{C} : \mathscr{C}$ is a category $\wedge\, \mathscr{C}' = \mathscr{D} \wedge \mathfrak{F}(\mathscr{C})$.

Theorem 6.8. Let $\mathfrak{F}$ be a theorem on categories, then $\mathfrak{F}'$ is also a theorem of categories, the so-called **dual theorem** to $\mathfrak{F}$.

We now introduce a general notion of isomorphism. For two objects in a category, we have:

Definition 6.9. Let $\mathscr{C}$ be a category. A morphism $f \in \mathrm{Mor}_{\mathscr{C}}(A, B)$ called an **isomorphism** if there is a morphism $g \in \mathrm{Mor}_{\mathscr{C}}(B, A)$ such that $fg = 1_B$ and $gf = 1_A$. Two objects $A, B \in \mathrm{Obj}\mathscr{C}$ are said to be **isomorphic** if $\mathrm{Mor}_{\mathscr{C}}(A, B)$ contains an isomorphism.

For two categories:

Definition 6.10. Two categories $\mathscr{A}$ and $\mathscr{B}$ are said to be **isomorphic** if there exists two covariant functors $\mathscr{F} : \mathscr{A} \to \mathscr{B}$ and $\mathscr{G} : \mathscr{B} \to \mathscr{A}$ which are mutually inverse, i.e. such that $\mathscr{F}\mathscr{G} = \mathrm{Id}_{\mathscr{B}}$ and $\mathscr{G}\mathscr{F} = \mathrm{Id}_{\mathscr{A}}$.

We can view the Fundamental Theorem of Galois Theory (FTGT) as an isomorphism of categories.

We conclude this Appendix by presenting products:

Definition 6.11. Let $\mathscr{C}$ be a category and $\{A_i\}_{i \in I}$ be a family of objects in $\mathscr{C}$ indexed by the set I. An object $\Pi_{i \in I} A_i$ together with a family $\{\pi_i : \Pi_{i \in I} A_i \to A_i\}_{i \in I}$ of morphisms is called a **product** of A_i if for all $C \in \mathrm{Obj}\mathscr{C}$, $f_i \in \mathrm{Mor}_{\mathscr{C}}(C, A_i)_{i \in I}$, there exists exactly one $h \in \mathrm{Mor}_{\mathscr{C}}(C, \Pi_{i \in I} A_i)$ such that for all $i \in I$, $f_i = \pi_i h$. The morphisms π_i are called **projections**.

The dual of a product is called a **coproduct**.

Bibliography

[Ber15] George M. Bergman, *An Invitation to General Algebra and Universal Constructions*, Universitext, Springer International Publishing, Cham, 2015.

[Bou95] N. Bourbaki, *General Topology: Chapters 1–4*, Elements of Mathematics, Springer-Verlag, Berlin Heidelberg, 1995.

[Bow17] Amanda Bower, *Category Theory and Galois Theory*, Rose-Hulman Undergraduate Mathematics Journal **14** (2017), no. 1.

[Bro06] Jim L. Brown, *An Introduction to Iwasawa Theory*, 2006.

[Bur18] David Burns, *Introduction to Iwasawa Theory*, 2018.

[Cam00] Rachel Camina, *The Nottingham Group*, New Horizons in pro-p Groups, 2000, pp. 205–221.

[dGTB17] Francesco de Giovanni, Marco Trombetti, and Mattia Brescia, *The True Story Behind Frattini's Argument*, Advances in Group Theory and Applications (June 2017), 117–129.

[Dou60] Adrien Douady, *Cohomologie des groupes compacts totalement discontinus*, Séminaire N. Bourbaki **189** (1960), 287–298.

[EKMS92] M. Erné, J. Koslowski, A. Melton, and G. E. Strecker, *A Primer On Galois Connections*, York Academy of Science, 1992.

[Fra85] G. Frattini, *Intorno alla generazione dei gruppi di operazioni*, Accademia dei Lincei, Rendiconti, IV. Serie **1** (1885), 281–285, 455–457.

[Gam06] Adam Gamzon, *The Hasse-Minkowski Theorem*, 2006. Honors Scholar Theses.

[Gha99] Eknath Ghate, *The Kronecker-Weber Theorem*, 1999.

[Gou97] Fernando Gouvea, *p-adic Numbers: An Introduction*, 2nd ed., Universitext, Springer-Verlag, Berlin Heidelberg, 1997.

[Hal99] Marshall Hall, *The Theory of Groups*, American Mathematical Society, 1999.

[Jen54] S. A. Jennings, *Substitution Groups of Formal Power Series*, Canadian Journal of Mathematics **6** (1954), 325–340.

[Kie12] Jonathan Kiehlmann, *The classifications of countably based profinite abelian groups*, 2012. arXiv:1101.3005 [math].

[KKM02] Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall (eds.), *Valuation Theory and Its Applications, Volume I*, American Mathematical Society, Providence, Rhode Island, 2002.

[Kob84] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Graduate Texts in Mathematics, Springer-Verlag, New York, 1984.

[KVSN11] Benjamin Klopsch, Christopher Voll, Dan Segal, and Nikolay Nikolov (eds.), *Lectures on Profinite Topics in Group Theory*, London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2011.

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, Springer-Verlag, New York, 2002.

[Mil20a] James S. Milne, *Algebraic Number Theory (v3.08)*, 2020. Available at www.jmilne.org/math/.

[Mil20b] ———, *Fields and Galois Theory (v4.61)*, 2020. Available at www.jmilne.org/math/.

[ML78] Saunders Mac Lane, *Special Limits*, Categories for the Working Mathematician, 1978, pp. 211–232.

[MLM94] Saunders Mac Lane and Ieke Moerdijk, *Categorical Preliminaries*, Sheaves in Geometry and Logic: A First Introduction to Topos Theory, 1994, pp. 10–23.

[Mos] Lee Mosher, *Cantor Set Homeomorphic to Inverse Limit Space*. Mathematics Stack Exchange.

[Mun] Muniain, $(\mathbb{Q}, +)$ *has no maximal subgroups*. Mathematics Stack Exchange.

[nLa21] nLab authors, *HomePage*, 2021. Revision 280.

[NS07] Nikolay Nikolov and Dan Segal, *On Finitely Generated Profinite Groups, I: Strong Completeness and Uniform Bounds*, Annals of Mathematics **165** (2007), no. 1, 171–238.

[Par70] Bodo Pareigis, *Categories and Functors*, Ludwig-Maximilians-Universität München, 1970.

[Ros58] Alex Rosenberg, *The Structure of the Infinite General Linear Group*, Annals of Mathematics **68** (1958), no. 2, 278–294.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza, *Topological Groups*, Fourier Analysis on Number Fields, 1999, pp. 1–45.

[RZ10] Luis Ribes and Pavel Zalesskii, *Profinite Groups*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer-Verlag, Berlin Heidelberg, 2010.

[Sch11] Peter Schneider, *Foundations*, p-Adic Lie Groups, 2011, pp. 3–43.

[Sch97] Eric Schechter, *Handbook of Analysis and Its Foundations*, Elsevier, 1997.

[Ser97] Jean-Pierre Serre, *Galois Cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin Heidelberg, 1997.

[SR18] Ignasi Sánchez Rodríguez, *Infinite Galois Theory*, 2018.

[The21] The Stacks project authors, *The Stacks project*, 2021.

[Wil98] John S. Wilson, *Profinite Groups*, London Mathematical Society Monographs, Oxford University Press, Oxford, New York, 1998.

[Wil] Gareth Wilkes, *Profinite Groups and Group Cohomology*.

[Zha15] Yifei Zhao, *Multivariate Hensel's Lemma for Complete Rings*, 2015.