Profinite and pro-p groups

Simon Stead

May 29, 2015

Contents

Abstract

Profinite groups are a type of topological group of interest to group theorists and number theorists alike. They can be viewed as Galois groups of field extensions of infinite degree; as local fields [6] with a Lie Algebraic structure [7], or as the fundamental groups of Algebraic geometry.

The profinite groups with the easiest structure are called pro-p groups. Chapter 1 deals with the introduction to profinite and pro-p groups largely from a topological viewpoint, defining the machinery needed and proving any necessary theorems. We finish with the result that a uniformly powerful pro-p group of dimension d is homeomorphic to the d-dimensional p-adic integers $\mathbb{Z}_p^d$.

Chapter 2 gives a few more examples of pro-p groups, the general and special linear groups over $\mathbb{Z}_p$, and the Nottingham group - an example of a pro-p group that does not behave in the same way as the prototypical $\mathbb{Z}_p$. We show that any finite p-group can be embedded as a subgroup into the Nottingham group.

Chapter 1

Profinite and Pro-p Groups

To save heavy referencing, the theorems and proofs throughough this chapter are predominantly stated in "Analytic pro-p groups" [7], and then proved either by myself or can be found in Symth's paper [27].

1.1 Introduction

In number theory profinite groups they arise when considering a Galois group of an extension field of infinite degree. p-adic numbers and local fields are inherently linked also. An interested number theorist should read Cassels' [6] book 'Local Fields'.
In group theory the subject found its fame starting with Johnson's [24] study of automorphisms of formal power series acting by substitution, this is the foundation for what was later called the Nottingham Group. The likes of Alan and Rachel Camina [4] [3], Charles Leedham-Green [20], [21] and Marcus Du Sautoy [8] have all lead the development.
The more recent studies have looked to bridge the two, and so for example look at the Hausdorff dimension of the subgroups of a profinite group (a number theoretic property) in order to make statements on about the group itself. This has proved an extremely valuable tool, and many of the proofs have been dramatically shortened this way. We, however, will consider a group theoretic approach, with only perhaps a notional previous knowledge of p-adics.

1.2 Profinite and Pro-p Groups

1.2.1 Topological groups

Definition 1.2.1. Given a set X, we define a *topology* on X to be a family of sets τ that satisfy the following conditions:

1. X and $\emptyset$ are in τ.
2. Any union of sets in τ is in τ.
3. A finite intersection of sets in τ is in τ.

X is then called a *topological space* with respect to this topology.

Definition 1.2.2. We call the sets in τ the *open sets*, and for the purposes of both calculation and proof we restate the above in terms of open sets.

1. X and $\emptyset$ are open.
2. Any union of open sets is open.
3. Any finite intersection of open sets is open.

Definition 1.2.3. The set theoretic complement of an open set in X is called *closed*.

Notation 1. *An open subgroup will be denoted $\leq_O$, and a closed subgroup by $\leq_C$. Open and closed normal subgroups will be denoted $\lhd_O$ and $\lhd_C$ respectively.*

Definition 1.2.4. A *topological group*, is a group G which is also a topological space, such that the maps

$$m : G \times G \to G : (g, h) \mapsto gh$$

$$\iota : G \to G : g \mapsto g^{-1};$$

are both continuous.

Definition 1.2.5. A topological group (indeed more generally a topological space) G is *Hausdorff* if for any two elements of G have distinct neighbourhoods. That is for all $u \neq v \in G$ there exists open subsets U, V of G, such that $u \in U$, $v \in V$ and $U \cap V = \emptyset$.

Definition 1.2.6. A topological group (or space) G is *compact* if every open cover [1] of G has a finite subcover. That is for any arbitrary collection of open subsets $\{U_a\}_{a\in A}$, such that $G = \bigcup_{a\in A} U_a$ there exists a finite subset B of A such that $X = \bigcup_{b\in B} U_b$.

Theorem 1.2.1 (Tychonoff's Theorem)**.** *The cartesian product of a family of compact spaces is compact.*

Proof. The proof from Bourbaki can be found in *"An introduction to Abstract Harmonic Analysis"* [23]. □

Theorem 1.2.2. *The cartesian product of a family of Hausdorff spaces is Hausdorff.*

Proof. The proof from Bourbaki can be found in *"An introduction to Abstract Harmonic Analysis"* [23]. □

Lemma 1.2.2.1 (Closed map lemma)**.** *The closed map lemma states that every continuous function $f : A \to B$ from a compact space A to a Hausdorff space B is closed, and that the preimage of every compact set in B is compact in A.* [2]*.*

Definition 1.2.7. We will use the term *local field* when discussing a locally compact topological field. They are important to us as they are fields on which we can define an absolute value.

Definition 1.2.8. A function f between two topological spaces is a *homeomorphism*, or topological isomorphism, if:
(i) f is continuous;
(ii) f is bijective;
(iii) f is an open mapping, which (assuming (i) and (ii)) is equivalent to the continuity of the inverse function f^{-1}.

Theorem 1.2.3. *Let G be a topological group:*

1. *The maps $x \mapsto xg$, $x \mapsto gx$ and $x \mapsto x^{-1}$ are homeomorphisms of G, for all $g, x \in G$.*

2. *If H is a subgroup of G and H is open (respectively closed) then every coset of H is open (respectively closed).*

3. *Every open subgroup of G is closed.*

4. *G is Hausdorff if and only if $\{1\}$ is a closed subset of G.*

[1] For rigorous definitions of covers and sub covers please see [29].
[2] This second condition is known as f being *proper*

5. *If N is a closed subgroup of G and G is Hausdorff, then G/N is Hausdorff with the quotient topology.*

6. *If H is a subgroup of G containing a non-empty open subset U of G then H is open in G.*

Proof. 1. Define the right translation map by $r_g(x) = xg$. We can show it is bijective, as for any $h \in g$ we have $r_g(hg^{-1}) = h$. To show continuity, we note for any open subset U of G, $\iota^{-1}(U) \leq_O G \times G$ (as multiplication is an open mapping). The set $\{U_1 \times U_2 \mid U_1, U_2 \leq_O G\}$ forms a basis for the product topology on $G \times G$, so we can define a map $\phi_a : G \to G \times G$, defined by $g \mapsto (g, a)$. This is continuous as $\phi^{-1}(U_1 \times U_2) = U_1$ if $a \in U_2$ and $\emptyset$ otherwise. This means $r_g = m \circ \phi_a$, and is continuous as it's the composition of two continuous functions. $(r_g)^{-1} = xg^{-1} = r_{g^{-1}}$ and is continuous by the same argument. r_g is hence a homeomorphism, and so is $l_g(x) = gx$ by symmetry. Inversion $x \mapsto x^{-1}$ is a homeomorphism as $x \in G$ and inversion is continuous in a topological group.

2. Since the translation maps $x \mapsto xg$ and $x \mapsto gx$ are homeomorphisms, they map open subsets to open subsets. Hence the image gH of an open subgroup H is open. To prove the statement for closed H, we can apply the same proof to the set theoretic complement of H in G.

3. The set theoretic complement of H in G is exactly the union of all cosets of H other than H itself. Since the union of open sets is open, the set theoretic complement of H in G is open, hence H is closed.

4. ($\Rightarrow$) In a Hausdorff space, singleton sets are closed.

   ($\Leftarrow$) Suppose $\{1\}$ is closed, then by (ii) any coset of $\{1\}$ i.e. any singleton, is closed. Let $x \neq y$ be elements of G. Then $U = G \setminus \{xy^{-1}\}$ is open. Since the map $(a, b) \mapsto a^{-1}b$ is continuous, and $1 \in U$, there exist open neighbourhoods V_1 and V_2 such that $V_1^{-1}V_2 \subseteq U$. Then V_1x and V_2y are disjoint neighbourhoods of x, y.

5. Follows from 4. G/N contains $\{1\}$, which is closed by G being Hausdorff and N being closed. G/N is Hausdorff (with the quotient topology) if and only if every equivalence class is closed in G; the equivalence classes of G/N are the cosets gN, which are closed by 2.

6. $H = \bigcup_{h \in H} Uh$. Since U is open, Uh is open for each h. Then H is a union of open sets, thus open in G.

□

1.2.2 Profinite Groups

Definition 1.2.9. A *partial order* $\leq$ on a set S is a binary relation such that for all $a, b, c \in S$:
(i) $a \leq a$ (reflexivity),
(ii) if $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry),
(iii) if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity).
If S is a set with a partial order, then it is known as a *partially ordered set*, or *poset*.

Definition 1.2.10. A *directed set* is a non-empty partially ordered set $(S, \leq)$ such that for all $i, j \in S$ there exists $k \in S$ such that $i \leq k$ and $j \leq k$.

Definition 1.2.11. An *inverse system of groups* is a collection of groups $(G_i)_{i \in S}$ (S being a directed set as above) along with a family of homomorphisms $\phi_{kj} : G_k \to G_j$ whenever $j \leq k$, such that $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ whenever $i \leq j \leq k$. An *inverse limit* is then the set of all objects in the Cartesian product $\prod_{k \in S} G_k$ such that $\phi_{kj}(g_k) = g_j$ whenever $j \leq k$.

Definition 1.2.12. A *projection* is a homomorphism ϕ_i from the Cartesian product $\left(\prod_{k \in S} G_k\right) \to G_i$, for some i, such that for $g \in \prod_{k \in S} G_k$, $\phi_i(g) = g_i$.

Example 1.2.1. An simple numerical example to think of when first considering inverse limits is the successive decimal approximations of an irrational number like $\sqrt{2}$.

Let a_n be the approximation to n decimal places (e.g. $a_3 = 1.414$). The directed set is $(\mathbb{N}, \leq)$ with natural ordering, and the homomorphisms are given by $\phi_{kj}(a_k) = 10^{-j} \lfloor 10^j a_k \rfloor = a_j$, i.e. removing all decimal places after the jth position.

For example, $\phi_{4,2}(a_4) = \phi_{4,2}(1.4142) = 1.41 = a_2$. A example of a projection would be $\phi_4(\sqrt{2}) = 1.4142$.

Definition 1.2.13. A *profinite group* G is an inverse limit of finite groups. That is $G = \varprojlim (G_i)_{i \in S}$. This is equivalent to saying G is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity.

Definition 1.2.14. A left (right) *transversal* of a subgroup H of a group G, is a set containing exactly one member of each left (right) coset of H.

Definition 1.2.15. The *closure* of a set X is denoted $\overline{X}$ and is the smallest closed set containing X.

Theorem 1.2.4. *Let G be a profinite group.*

1. *Every open subgroup of G is closed, has finite index in G, and contains an open normal subgroup of G. A closed subgroup of G is open if and only if it has finite index. The family of all open subgroups of G intersects in $\{1\}$.*

2. *A subset of G is open if and only if it is a union of cosets of open normal subgroups.*

3. *For any subset X of G,*
$$\overline{X} = \bigcap_{N \lhd_O G} XN.$$

4. *If X and Y are closed subsets of G then so is the set $\{XY \mid x \in X, y \in Y\}$. If X is closed and n is an integer then the set $\{x^n | x \in X\}$ is closed.*

5. *Let H be a closed subgroup of G. Then G/H with the quotient topology is a profinite group. Every open subgroup of H is of the form $H \cap K$ with $K \leq_O G$.*

6. *Let N be a closed normal subgroup of G. Then G/N with the quotient topology is a profinite group.*

7. *A sequence (g_i) in G converges if and only if it is a Cauchy sequence: i.e. for each $N \lhd_O G$ there exists $n = n(N)$ such that $g_i^{-1} g_j \in N$, for all $i \geq n$ and $j \geq n$.*

Proof. 1. Let U be an open normal subgroup, that is $U \lhd_O G$. Since left cosets partition a group, $G \setminus U = \bigcup_{g \in G \setminus U} gU$. A union of cosets of an open normal subgroup is open, and hence $G \setminus U \leq_O G$ and so U is a closed subgroup of G; $U \leq_C G$. Also, as G is compact there must exist a finite subcover of $\bigcup_{g \in G} gU = G$ and thus $[G : U] \leq \infty$.

Now consider a transversal of the cosets of U, and define $N = \bigcap_{s \in S} sUs^{-1}$. N is an open subgroup because it's a finite intersection of open subgroups, so it just remains to show that it is normal. Take any $g \in G$ and note that for any $s \in S, (sg)^{-1} = t_s o_s$ for some $t_s \in S$ and $o_s \in U$. Hence

$$g^{-1} N g = \bigcap_{s \in S} (sg)^{-1} U (sg) = \bigcap_{s \in S} t_s U t_s^{-1} = N$$

as each t_s is a distinct element of S. Thus $N \lhd_O G$ and $N \subseteq U$. We have already shown that if $C \leq_O G$ then C is closed and has finite index. Conversely suppose $[G : C] \leq \infty$ and let $\mathcal{C}$ be the set of cosets of $C \in G$. it follows that $\bigcup_{D \in \mathcal{C} \setminus C} D = G \setminus C$ is closed in G and hence $C \leq_O G$.

Finally let $P = \bigcap_{N \lhd_O G} N$ and suppose there exists $g \in P$ such that $g \neq 1$. As G is Hausdorff there exists a neighbourhood of 1, say W, such that $g \notin W$. Hence there exists and open subgroup, and thus (by the above) an open normal subgroup contained in W, contradicting $g \in P$. Thus $P = 1$ as claimed.

2. Any union of cosets of open normal subgroups is open. Conversely if $S \leq_O G$ then for any $s \in S$ we have a neighbourhood of s (sayN_s) contained in S. Thus $s^{-1}N_s$ is a neighbourhood of 1 which must contain an open normal subgroup M_s. It follows that $sM_s \subseteq N_s \subseteq S$ and thus $S = \bigcup_{s \in S} sM_s$.

3. An open normal subgroup has finite index, that is $[G : N] \leq \infty$. Thus there exists a finite subset of X, S_N such that

$$XN = \bigcup_{x \in X} xN = \bigcup_{x \in S_N} xN.$$

   XN is a union of open sets, so open, so closed. That is $XN \leq_C G$ for each N and so

$$\overline{X} \subseteq \bigcap_{N \lhd_O G} XN.$$

   For the reverse inclusion take some $y \in \cap_{N \lhd_O G} XN$. Then for each N there exists an $x_N \in X$ such that $y \in x_N N$. This is the same as $x_N \in yN$. Open normal subgroups form a base for the neighbourhoods of the identity in G, so for any open ball U centred at y there exists $N \lhd_O G$ such that $yN \subseteq U$. This means we can find a sequence of open normal subgroups N such that $\{x_N\}$ converges to y. As y is a limit point in G we have $y \in \overline{X}$.

4. Recalling the closed map lemma, we have that continuous functions from a compact space to a Hausdorff space are closed. This immediately gives us that if $A, B \leq_C G$ then $\{ab \,|\, a \in A, b \in B\} \leq_C G$ as multiplication is continuous in G. For the second part, if $n = 0$ the result is obvious. If $n \geq 0$ consider the map $x \mapsto (x, x, \ldots, x)$ from G to $G \times G \times \ldots G$. For any open set $O_1 \times \cdots \times O_n$ in the codomain, the inverse image under the map in G is merely $O_1 \cap \cdots \cap O_n$ which is clearly open. Hence the map $x \mapsto x^n$ is the composition of the above map and multiplication and thus is continuous. If $n \leq 0$, the map $x \mapsto x^n$ is the composition of inversion and the continuous map $x \mapsto x^{-n}$ and so is also continuous. Thus for any integer n (by the closed map lemma), $\{x^n \,|\, x \in X\} \leq_C G$ whenever $X \leq_C G$.

5. That H is compact and Hausdorff is clear as $H \leq G$. Also if N is any open set containing the identity in H there exists an open set containing the identity in G, say M, such that $M \cap H = N$. Thus we have a $A \leq_O G$ such that $A \subseteq M$. Thus $A \cap H \leq_O H$ and $A \cap H \subseteq N$. Thus it follows that H is profinite. Also, taking any $B \leq_O H$ there exists an $N \lhd_O G$ such that $N \cap H \subseteq B$. It is clear that $BN = \{bn \,|\, b \in B, n \in N\} \leq_O G$ and that $BN \cap H \supseteq B$. Now if $bn = h$ for some $b \in B, n \in N$ and $h \in H$, then $n = b^{-1}h$ which would imply that $h \in B$ and so $BN \cap H = B$ as required.

6. If $M \lhd_O G$ then G/M is a finite group with the discrete topology and the result is clear. Assume then that M is not open in G. Let $\pi : G \to G/M$ be the canonical quotient map which is continuous and open (Let G be a topological group ϕ be the canonical mapping to G/H then ϕ is onto continuous, open). Thus if $\bigcup_{i\in I} H_i$ is an open cover from G/M then $\bigcup_{i\in I} \pi^{-1}(H_i)$ is an open cover for G. The compactness of G/N thus follows from that of G.

   If K is any neighbourhood of the identity in G/M, which we can assume without loss of generality to be open, then $\pi^{-1}(K) \leq_O G$ and thus there is a subgroup $H \leq_O G$ such that $H \subseteq \pi^{-1}(K)$. It is clear then that $\pi(H) \leq_O G/M$ and thus the open subgroups form a base for the neighbourhoods of the identity. If $x \in G/M$ then as M is closed, $xM \leq_C G$. As π is an open mapping it follows that $\pi(G \setminus xM) \leq_O G$ which precisely gives us that $\{x\} \leq_C G/M$ so that G/M is a regular (or T_1) space. Every regular topological group is Hausdorff and thus G/M is profinite.

7. ($\leftarrow$) Let (g_i) be a Cauchy sequence in G. Since G is compact and Hausdorff, there exists a subsequence $g_{i_{(j)}}$ which converges to an element g in G. Let $N \lhd_O G$. For sufficiently large j, $g_{i_{(j)}} \in gN$ while for sufficiently large i and j we have $g_{i_{(j)}}^{-1} g_i \in N$. Hence for sufficiently large i we have $g_i \in gN$. Since the sets gN form a base for the neighbourhoods of g in G, this shows that (g_i) converges to g.

   ($\rightarrow$) Let (g_i) converge to an element $g \in G$, and let $N \lhd_O G$ Then as the gN form a base for the neighbourhoods of g, $g_i \in gN$ for some sufficiently large i, implying $g_j^{-1} g_i \in N$ for all $j \geq i$, sufficiently large. Hence (g_i) is a cauchy sequence.

□

Theorem 1.2.5. *A profinite group G and $\varprojlim (G/N)_{N\lhd_O G}$, where $\lhd_O$ are isomorphic as profinite groups*

Proof. Let G be a profinite group, and let $\hat{G} = \varprojlim (G/N)_{N\lhd_O G}$. Consider the natural homomorphism

$$\iota : G \to \hat{G}$$

given by $\iota(g) = (gN)_{N\lhd_O G}$. As $\bigcap_{N\lhd_O G} = \{1\}$, ι is injective. To establish surjectivity of ι we take $(g_N N) \in \hat{G}$. Considering any finite collection of cosets $\{g_N N\}_{N\in\mathcal{N}}$ we have that $M := \cap_{N\in\mathcal{N}} N \lhd_O G$, and hence $g_M N \subseteq g_N N$ for all $N \in \mathcal{N}$. As every open subgroup in G is closed and G is compact, we have $\bigcap_{N\lhd_O G} g_N N$ is non-empty. Choosing g to lie in this intersection we have $\iota(g) = (g_N N)_{N\lhd_O G}$. The

projection $\phi_N : G \to G/N$ is continuous for all $N \lhd_O G$, however ι is merely the map $g \mapsto (\phi_N(G))$. and hence for any open set in $\prod_{N \lhd_O G} G/N$, say

$$O = O_{N_1} \times \cdots \times O_{N_n} \times \prod_{N \neq N_i} G/N$$

we have

$$\iota^{-1}(O) = \bigcap_{i=1}^{n} \phi_{N_i}^{-1}(O_{N_i}).$$

Since this is a finite intersection of open sets in G, ι is continuous. Any continuous bijection from a compact space to a Hausdorff space is a homeomorphism, so our topological isomorphism is established. □

1.2.3 Pro-p groups

Definition 1.2.16. A p-group is a group G in which all elements have prime power order; i.e. for each $g \in G \; \exists n \in \mathbb{N}$ such that $|g| = p^n$.

Definition 1.2.17. Let $N \lhd_O G$ be an open normal subgroup of a profinite group G. G is said to be a *pro-p group* if G/N is a (finite) p-group for all N. Since in a profinite group all open subgroups are closed and have finite index, the quotient group G/N is always finite.

The prototypical example of a pro-p group is the (additive) group of p-adic integers.

Definition 1.2.18. $\mathbb{Z}_p = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})$.

All finite p-groups are pro-p groups, but $\mathbb{Z}_p$ is the simplest kind of infinite pro-p group we can construct, as it's parts are the cyclic groups of p^n elements. In fact for this reason, $\mathbb{Z}_p$ is said to be *pro-cyclic*.

Definition 1.2.19. An element of $\mathbb{Z}_p$ is written $\sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \mathbb{F}_p$, the finite field of p elements.

$\mathbb{Z}_p$ is actually more than just a topological space as we might expect. We can endow it with a metric (in fact a complete metric) in order to determine distances between two elements of $\mathbb{Z}_p$.

Definition 1.2.20 (p-adic valuation)**.** The p-adic valuation is an absolute value on $\mathbb{Z}_p$. For $\alpha = \sum_{i=k}^{\infty} a_i p^i \quad \in \mathbb{Z}_p$, $|\,\alpha\,|_p = p^{-k}$.

Example 1.2.2. Let $\alpha \in \mathbb{Z}_p = 1 + p + p^2 + \dots$. Then $|\alpha|_p = p^{-0} = 1$. This is a unit of $\mathbb{Z}_p$.

Example 1.2.3. Let $\alpha \in \mathbb{Z}_p = 2p^3 + 4p^6 + p^7 + \dots$. Then $|\alpha|_p = p^{-3}$.

Example 1.2.4. Let $\alpha \in \mathbb{Z}_p = p + 2p^2 + 2p^3 + p^4 + \dots$ and let $\beta \in \mathbb{Z}_p = p + 2p^2 + 2p^3 + 3p^4 + \dots$ Then

$$\begin{aligned} |\beta - \alpha|_p &= |(p + 2p^2 + 2p^3 + 3p^4 + \dots) - \big(p + 2p^2 + 2p^3 + p^4 + \dots\big)|_p \\ &= |2p^4|_p \\ &= p^{-4} \end{aligned}$$

Recall a metric space X is said to be complete if every Cauchy sequence in X converges to a limit in X. That is for $x_m, x_n \in X$ if $|x_m - x_n| \to 0$ as $m, n \to \infty$, then there exists an $x \in X$ such that $|x_m - x| \to 0$.

Theorem 1.2.6. *$\mathbb{Z}_p$ is complete (as a metric space) with respect to $|\cdot|_p$*

Proof. By the Heine-Borel theorem, a metric space is compact only if it is complete and totally bounded. For proofs, one can see [29]. By definition our profinite group $\mathbb{Z}_p$ is compact, hence complete. □

Indeed, from the definition of $\mathbb{Z}_p$ we can see elements of $\mathbb{Z}_p$ are just limits of cauchy sequences in $\mathbb{Z}$ anyway, so completeness should not be a surprise.

In fact, $\mathbb{Z}_p$ is actually just the ring of integers of the complete space of p-adic rationals, the set

$$\left\{ \alpha : \alpha = \sum_{i=k}^{\infty} a_i p^i \mid a_i \in \mathbb{F}_p \right\}$$

where $k \in \mathbb{Z}$ as opposed to just $\mathbb{N}^0$. This set is denoted $\mathbb{Q}_p$ (and is the field of fractions $\mathbb{Z}_p$).

If we were to start from the set $\mathbb{Z}_p$ without the knowledge that it is profinite, we are still able to easily show it is both compact and Hausdorff.

Theorem 1.2.7. *$\mathbb{Z}_p$ is a compact, Hausdorff topological space.*

Proof. Consider the Heine-Borel theorem from the reverse perspective now. We know elements of $\mathbb{Z}_p$ are limits of Cauchy sequences in $\mathbb{Z}$ (with $\mathbb{Z}$ as a dense subset). The maximum distance two elements can be apart is when they are both units

with respect to the p-adic metric, and in different equivalence classes modulo p. Hence the diameter of ball $\mathbb{Z}_p$ is 1. Hence $\mathbb{Z}_p$ is compact as it is both complete and totally bounded.

To show $\mathbb{Z}_p$ is Hausdorff, consider $\alpha = \sum_{i=k}^{\infty} \alpha_i p^i, \beta = \sum_{i=j}^{\infty} \beta_i p^i, \in \mathbb{Z}_p$, where $k, j \in \mathbb{N}^0$, such that $\alpha \neq \beta$. Without loss of generality, assume $k \geq j$.

Then $\beta - \alpha = \sum_{i=j}^{\infty} (\beta_i - \alpha_i) p^i$. The p-adic valuation of $\gamma = \beta - \alpha$ depends only on when the first $\gamma_i = \beta_i - \alpha_i$ is only non zero. This must happen for some i as $\alpha \neq \beta$. Then $a_m \neq \beta_m$ and so $|\beta - \alpha|_p = p^{-m}$. This implies the open balls

$$B_\alpha(p^{-m}) = \left\{x \in \mathbb{Z}_p : |\alpha - x|_p \leq p^{-m}\right\}$$

and

$$B_\beta(p^{-m}) = \left\{x \in \mathbb{Z}_p : |\beta - x|_p \leq p^{-m}\right\}$$

are disjoint. □

1.3 Commutators of a Group

Definition 1.3.1. The commutator of a group G is defined by $[a, b] = a^{-1}b^{-1}ab$, $\forall a, b \in G$.

Definition 1.3.2. The conjugate of an element x by an element y is denoted $x^y := y^{-1}xy$.

Definition 1.3.3. For any 3 elements α, β, γ of a group G, $[\alpha, \beta, \gamma] = [[\alpha, \beta], \gamma]$.

Definition 1.3.4. Let A,B be subgroups of G. The commutator subgroup of G is the subgroup generated by all commutators of elements of G. That is $[A, B] = \langle\{[a, b] : a \in A, b \in B\}\rangle$

The importance of a commutator is that, as the name suggests, $[a, b] = 1$ if and only if a and b commute. A finite group G is abelian if the *derived subgroup* $[G, G] = \{1\}$.

Theorem 1.3.1. $[xy, a] = [x, a]^y[y, a]$

Proof.

$$\begin{aligned}
[x, a]^y[y, a] &= y^{-1}[x, a]y[y, a] \\
&= y^{-1}(x^{-1}a^{-1}xa)y(y^{-1}a^{-1}ya) \\
&= y^{-1}x^{-1}a^{-1}xya \\
&= (xy)^{-1}a^{-1}xya \\
&= [xy, a].
\end{aligned}$$

□

Theorem 1.3.2. $[x, ya] = [x, a][x, y]^a$

Proof.

$$\begin{aligned}[x, a][x, y]^a &= [x, a]a^{-1}[x, y]a \\ &= (x^{-1}a^{-1}xa)a^{-1}(x^{-1}y^{-1}xy)a \\ &= x^{-1}a^{-1}y^{-1}xya \\ &= x^{-1}(ya)^{-1}xya \\ &= [x, ya].\end{aligned}$$

□

Theorem 1.3.3 (Hall-Witt Identity)**.** *Let G be a group containing elements α, β, γ. Then $[\alpha, \beta^{-1}, \gamma]^\beta [\beta, \gamma^{-1}, \alpha]^\gamma [\gamma, \alpha^{-1}, \beta]^\alpha = 1$*

Proof.

$$\begin{aligned}\left[\alpha, \beta^{-1}, \gamma\right]^\beta &= \left[\alpha^{-1}\beta\alpha\beta^{-1}, \gamma\right]^\beta = \beta^{-1}\left[\alpha^{-1}\beta\alpha\beta^{-1}, \gamma\right]\beta \\ &= \beta^{-1}\left(\alpha^{-1}\beta\alpha\beta^{-1}\right)^{-1}\gamma^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\gamma\beta \\ &= \beta^{-1}\beta\alpha^{-1}\beta^{-1}\alpha\gamma^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\gamma\beta \\ &= \alpha^{-1}\beta^{-1}\alpha\gamma^{-1}\alpha^{-1}\beta\alpha\beta^{-1}\gamma\beta\end{aligned}$$

By simply mapping (α, β, γ) to (β, γ, α) and (γ, α, β) respectively, we see

$$\left[\beta, \gamma^{-1}, \alpha\right]^\gamma = \beta^{-1}\gamma^{-1}\beta\alpha^{-1}\beta^{-1}\gamma\beta\gamma^{-1}\alpha\gamma$$

and

$$\left[\gamma, \alpha^{-1}, \beta\right]^\alpha = \gamma^{-1}\alpha^{-1}\gamma\beta^{-1}\gamma^{-1}\alpha\gamma\alpha^{-1}\beta\alpha.$$

On multiplication, these three commutators clearly cancel down to the identity. □

Lemma 1.3.3.1 (Three Subgroup Lemma)**.** *Let A, B and C be normal subgroups of a group G. Then $[A, B, C] \leq [B, C, A][C, A, B]$. This can be equivalently stated as "Let $N \lhd G$. If $[A, B, C] \leq N$ and $[C, A, B] \leq N$, then $[B, C, A] \leq N$."*

Proof. We prove the second form of the lemma.

By definition $[[B, C,], A]$ is generated by the elements $[x, a]$ with $x \in [B, C]$ and $A \in A$. any element $x \in [B, C]$ is a product of commutators $[b, c]$ with $b \in B$ and $c \in C$. Now we observe that the identity $[xy, a] = [y, x]^x[x, a]$ holds for all $x, y, a, \in G$; this is easily verified by writing out the commutators explicitly. It

follows that $[[B,C],A]$ can be generated by the elements of the form $[[b,c]a]^z$ where $a \in A, b \in B, c \in C$ and $z \in [B,C]$.

Take an arbitrary commutator $[[b^{-1},c],a] \in [[B,C],A]$. Then $([[b^{-1},c],a]^b)^{-1} = [[a^{-1},b],c]^a[[c^{-1},a],b]^c$, by the Hall-Witt identity. Now $[[a^{-1},b],c] \in [[A,B],C] \leq N$, and since N is normal we have $[[a^{-1},b],c] \in N$. Similarly $[[c^{-1},a],b]^c \in N$ and so $[[b^{-1},c],a]^b \in N$. But N is normal, and so $[[b^{-1},c],a]^z \in N$ for all $z \in G$ (and in particular for all $z \in [B,C]$.

Since the elements $[[b^{-1},c],a]^z$ generate $[[B,C],A]$, we have $[[B,C],A] \leq N$. □

Theorem 1.3.4. *Let $\psi : G \to H$ be a group homomorphism. Then $\psi([a,b]) = [\psi(a),\psi(b)]$ and thus $\psi([G,G]) \subseteq \psi([H,H])$. Moreover if ψ is onto, then $\psi([G,G]) = \psi([H,H])$.*

Proof. Let $a,b \in G$. Then $\psi([a,b]) = \psi(a^{-1}b^{-1}ab) = \psi(a^{-1})\psi(b^{-1})\psi(a)\psi(b) = \psi(a)^{-1}\psi(b)^{-1}\psi(a)\psi(b) = [\psi(a),\psi(b)]$. This implies $\psi[G,G] \subseteq [\psi(G),\psi(G)] = [H,H]$. Now assume ψ is onto, so that for all $h_1,h_2 \in H$ we can find g_1,g_2 such that $g_1,g_2]) = [h_1,h_2]$, which means $\{[h_1,,h_2] : h_1,h_2 \in H\} \subseteq \psi([G,G])$. Since we have a double sided inclusion, $\psi([G,G]) = [H,H]$.

□

Definition 1.3.5. The lower central series can then be defined by $\gamma_1(G) = G$, $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

Definition 1.3.6. A profinite group G is said to have *finite width* if $[\gamma_{i+1}(G) : \gamma_i(G)]$ is finite for all $i \in \mathbb{N}$.

1.4 The Frattini subgroup

A subgroup integral to our understanding of pro-p groups is the Frattini subgroup $\Phi(G)$.

Definition 1.4.1. The frattini subgroup $\Phi(G) = \bigcap_{N \lhd_O G} N$ is the intersection of all open maximal subgroups of G.

Theorem 1.4.1. *Let G be a profinite group*

1. *$\Phi(G) \lhd_C G$.*
2. *If $H \lhd_C G$ and $K \leq \Phi(G)$ then $\Phi(G/K) = \Phi(G)/K$.*
3. *For a subset X of G the following are equivalent:*
   - *(a) X generates G topologically;*
   - *(b) $X \cup \Phi(G)$ generates G topologically;*
   - *(c) $X\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$ topologically.*

Proof. 1. By De Morgan's laws, the set theoretic complement of a set of intersections is the union of the complements. $(\Phi(G))' = \bigcup_{N \lhd_O G} N'$, where $'$ denotes set complement. Now N is an open subgroup, so closed, so it's complement is open. Hence $(\Phi(G))'$ is the union of open sets, so open. This implies $\Phi(G)$ is closed in G.

2. Let $H \lhd_C G$ and $K \leq \Phi(G)$. Then

$$\begin{aligned}\Phi(G/K) &= \bigcap_{N \lhd_O G/K} N \\ &= \bigcap_{N \lhd_O G} NK \\ &= \left(\bigcap_{N \lhd_O G} N \right) K \\ &= \Phi(G)/K.\end{aligned}$$

3. (a) implies (b) is clear, as $X \cup \Phi(G)$ contains X, which generates G topologically. (b) implies (c) is also clear, as if $X \cup \Phi(G)$ generates G, any element of G can be decomposed as $g = x\phi$ for $x \in X, \phi \in \Phi(G)$. Now suppose (c) holds, and let K be an open subgroup of G containing X. If $K \neq G$, then K is contained in a maximal proper open subgroup M of G, and then

$$\overline{\langle X \rangle}\Phi(G)/\Phi(G) \leq M\Phi)(G) \neq G/\Phi(G),$$

contradicting (c). Hence K = G, and it follows from theorem 1.2.4(iii) that $\overline{\langle X \rangle} = G$. Thus (c) implies (a).

□

Theorem 1.4.2. *Let G be a pro-p group. Let $G^p = \{g^p : g \in G\}$, and $[G, G]$ be the derived group of G. Then*

$$\Phi(G) = \overline{G^p[G, G]}.$$

Proof. If M is a maximal open proper subgroup of G then there is some $N \lhd_O G$ contained in M by theorem 1.2.4. It follows that M/N is a maximal subgroup in the finite p-gorup G/N. As G/N is a finite p-group, M/N is normal and has index p. So $M \lhd G$ and $[G : M] = [G/N : M/N] = p$. Thus G/M is abelian and so $[G, G] \leq M$ and $G^p \leq M$. Hence we have

$$\Phi(G) = \bigcap M \geq G^p[G, G]$$

but as $\Phi(G)$ is closed we obtain $\Phi(G) \geq \overline{G^p[G,G]}$.
Now we consider $Q = G/\overline{G^p[G,G]}$, which is a pro-$p$ group as any closed subgroup of a pro-p group is itself a pro-p group, and thus its open normal subgroups intersect in the identity. If we take any $N \lhd_O Q$, Q/N is a finite elementary abelian p-group (define elementary), and thus its maximal subgroups intersect in the identity ($\Phi(Q/N) = 1$) thus $\Phi(Q) \subseteq N$. It follows that $\Phi(Q) \leq \bigcap_{N \lhd_O Q} N = \{1\}$, and thus as we know that $\overline{G^p[G,G]} \leq \Phi(G)$ we have $\{1\} = \Phi Q = \Phi(G)/\overline{G^p[G,G]}$ and we are done. □

Theorem 1.4.3. *Let G be a pro-p group. Then G is finitely generated if and only if $\Phi(G)$ is open in G.*

Proof. ($\leftarrow$) If $\Phi(G)$ is open then $G/\Phi(G)$ is finite. Thus there is a finite subset X of G such that $G = X\Phi(G)$, so X generates G topologically.

($\rightarrow$) Suppose $G = \overline{\langle X \rangle}$ where $|X| = d$ is finite. If $\Phi(G) \leq N \lhd_O G$ then G/N is an elementary[3] abelian p-group and can be generated by d elements. Consequently $|G : N| \leq p^d$. Among all such N we may choose one such that the degree is minimal. Then $N_0 \leq N$ for every $N \lhd_O G$. Since $\Phi(G)$ is closed and normal in G, it follows that

$$\Phi(G) = \bigcap \{N \mid \Phi(G) \leq N \lhd_O G\}.$$

Thus $\Phi(G)$ is open in G. □

This is an extremely important result in the study of pro-p groups as it allows us to define the following.

Definition 1.4.2. Let G be a pro-p group. The *Frattini Series* or *lower p series* is defined by $P_1(G) = G$, and $P_{i+1}(G) = \overline{G^p\,[P_i(G), G]}$.

Notice $P_2(G) = \overline{G^p[G,G]} = \Phi(G)$.

Theorem 1.4.4. *Let G be a pro-p group.*
(i) $P_i(G/K) = P_i(G)K/K$, for all $K \lhd_C G$ and all i.

(ii) $[P_i(G), P_j(G)] \leq P_{i+j}(G)$ for all i, j.

(iii) If G is finitely generated then $P_i(G)$ is open in G for each i and the set $\{P_i(G) \mid i \geq 1\}$ is a base for the neighbourhoods of 1 in G.

[3] all elements have order exactly p

Proof. Write G_i for $P_i(G)$ for each i. for (i) let $K \lhd_C G$. Then $(P_i(G/K))$ is the fastest descending series of closed normal subgroups of G/K such that each factor is central and of exponent dividing p. Since (G_iK/K) is a series with these properties, it follows that $P_i(G/K) \leq G_iK/K$ for all i.

Now suppose that, for some n, $P_n(G/K) = G_nK/K$. Put $M/K = P_{n+1}(G/K)$. Then M is closed in G and $M \geq G_n^p[G_n, G]K$, so $M \geq G_{n+1}K$, Hence $M = G_{n+1}K$, and the result follows by induction.

(ii) Certainly $[G_i, G_1] \leq G_{i+1}$ for all i. Let $n \geq 2$ and suppose inductively that $[G_i, G_{n-1}] \leq G_{i+n-1}$ for all i. Now we fix $m \geq 1$, and want to show that $[G_m, G_n] \leq G_{m+n}$. Since G_{m+n} is closed, it will suffice to show that $[G_m, G_n] \leq N$ whenever $G_{m+n} \leq N \lhd_O G$. Thus in view of (i) we may replace G by the finite p-group G/N, and assume further that $G_{m+n} = 1$. Then $[G_m, G_{n-1}] \leq G_{m+n-1}$ is central and has exponent dividing p. If $g \in G_m$ and $x \in G_{n-1}$ we have

$$[g, x^p] = [g, x]^p = 1;$$

so $[G_m, G_{n-1}^p] = 1$. Also

$$\begin{aligned}[G_m, [G_i, G_1]] &\leq [G, [G_m, G_{n-1}]][G_{n-1}, [G, G_m]] \\ &\leq [G, G_{m+n-1}][G_{n-1}, G_{m+1}] \\ &\leq G_{m+n} = 1\end{aligned}$$

by the three subgroup lemma and inductive hypothesis. It follows that

$$[G_m, G_{n-1}^p[G_{n-1}, G]] = 1.$$

Since G is finite, this is the same as $[G_m, G_n] = 1$, which is what we wanted to show.

(iii) Now assume that G is finitely generated. Certainly $G_1 = G$ is finitely generated and open in G. Let $n \geq 1$ and suppose inductively that G_n is finitely generated and open in G. Then proposition 1.14 shows $\Phi(G_n)$ is open in G_n. Since $\Phi(G_n) \leq G_{n+1} \leq G_n$ it follows that G_{n+1} is open in G_n and hence in G, and prop 1.17 shows that G_{n+1} is finitely generated. The first claim follows by induction.

To show that $\{P_i(G) \mid i \geq 1\}$ is a base for the neighbourhoods of 1 in G, it now suffices to show that every open normal subgroup of G contains G_i for some i. This follows from (i), since if $N \lhd_O G$ then G/N is a finite p-group and so $P_i(G/N) = 1$ for sufficiently large i.

□

1.5 Uniformly powerful pro-p groups

1.5.1 Powerful pro-p groups

There are almost identical definitions for finite and pro-p groups. We will only be concerned with the latter, but give both definitions for completeness.

Definition 1.5.1. Let G be a finite p-group. Then
(i) G is powerful if p is odd and G/G^p is abelian (or $p = 2$ and G/G^4 is abelian).
(ii) A subgroup N of a finite-p group G is powerfully embedded in G is if p is odd and $[N, G] \leq N^p$ (or $p = 2$ and $[N, G] \leq N^4$).

Definition 1.5.2. Let G be a pro-p group. Then
(i) G is powerful if p is odd and $G/\overline{G^p}$ is abelian.
(ii) A subgroup N of a finite-p group G is powerfully embedded in G is if p is odd and $[N, G] \leq \overline{N^p}$.

Theorem 1.5.1. *Let G be a powerful pro-p group. Then $\Phi(G) = \overline{G^p}$.*

Proof. $\Phi(G) = \overline{G^p[G, G]}$. The definition of a powerful pro-p group says that $[G, G] \leq G^p$, hence $\Phi(G) = \overline{G^p}$. □

Theorem 1.5.2. *A powerful pro-p group is the product of its procyclic subgroups. That is if $G = \overline{\langle a_1, \ldots, a_d \rangle}$ is a powerful pro-p group, then $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$.*

Proof. Let $A = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$. As a product of finitely many closed, hence compact, subsets of G, A is a closed subset of G. So $A = \bigcap_{N \lhd_O G} AN$. But for each normal subgroup $N \lhd_O G$, $AN/N = G/N$, so consequently $A = G$. □

1.5.2 Uniform pro-p groups

Definition 1.5.3 (Uniform pro-p group)**.** A pro-p group G is said to be uniformly powerful, or uniform, if it is finitely generated, powerful and for all $i \in \mathbb{N}$, $[G_i : G_{i+1}]$ is constant.

The condition of constant index for the Frattini series is equivalent to the map $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$ such that $xP_{i+1}(G) \mapsto x^p P_{i+2}(G)$ is an isomorphism.

Theorem 1.5.3. *Every finitely generated powerful pro-p group G contains an open uniform subgroup.*

Proof. $G_i \lhd_O G$ for all $i \in N$. There also exists a surjection from G_i/G_{i+1} to G_{i+1}/G_{i+2}, which means $[G_i : G_{i+1}] \leq [G_{i+1} : G_{i+2}]$ for all i. Since all subgroups have index equal to a (non-negative) pth power, we have

$$p^{n_1} \geq p^{n_2} \geq \cdots \geq p^{n_i} \geq \ldots$$

with $n_i \geq$ for all i. Hence there must be some positive integer k for which $n_i = n_j$, for all $i, j \geq k$. Hence $G_k \lhd_O G$ is uniform. □

Theorem 1.5.4. *Let G be a uniform pro-p group. Then G is homeomorphic to $\mathbb{Z}_p^d$ for some d.*

Proof. Let G be a uniform pro-p group, and let its minimal topological generating set be $\{a_1, \ldots, a_d\}$. Then G is generated from the product of the pro-cyclic subgroups $\overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$. Each element in G can therefore be expressed as $a_1^{\lambda_1} \ldots a_d^{\lambda_d}$, for $\lambda_i \in \mathbb{Z}_p$.

Consider $G/G_{k+1}$for some positive integer k. This has order p^{kd}, and because it is equal to the product of its d pro-cyclic subgroups $\overline{\langle a_1 G_{k+1} \rangle} \ldots \overline{\langle a_d G_{k+1} \rangle}$ each must have order p^k.

It follows that each element of G/G_{k+1} can be expressed as $a_1^{e_1} \ldots a_d^{e_d} G_{k+1}$, where each of the e_i are uniquely determined modulo p^k. This implies the λ_i are uniquely determined modulo p^k for all $k \in \mathbb{N}$, so the λ_i are uniquely determined p-adic integers. The mapping:

$$\theta : G \to \mathbb{Z}_p^d, \text{ where } a\theta = (\lambda_1, \ldots, \lambda_d)$$

and its inverse

$$\psi : \mathbb{Z}_p^d \to G, \text{ such that } (\lambda_1, \ldots, \lambda_d)\psi = a_1^{\lambda_1} \ldots a_d^{\lambda_d}$$

are then continuous, bijective functions between compact Hausdorff spaces, and so are homeomorphisms.

□

1.6 Rank

Let G be a finitely pro-p group, generated by the set $\{a_1, \ldots, a_d\}$. The number of generators, d, is one of the key notions in the study of pro-p groups.

Definition 1.6.1. Let H be a subgroup of a pro-p group G. Then $d(H)$ is the size of the smallest generating set of H.

Theorem 1.6.1. *Let G be a profinite group, and put*

$$\begin{aligned} r_1 &= \sup\{d(H) | H \leq_C G\} \\ r_2 &= \sup\{d(H) | H \leq_C G \text{ and } d(H) \leq \infty\} \\ r_3 &= \sup\{d(H) | H \leq_O G\} \\ r_4 &= \sup\{rk(G/N) | H \lhd_O G\}. \end{aligned}$$

Then $r_1 = r_2 = r_3 = r_4$.

Proof. It is clear that $r_1 \geq r_2$, and because every open subgroup of G is closed, $r_1 \geq r_3$. If $N \lhd_O G$ and $M/N \leq G/N$, then $d(M/N) \leq d(M) \leq r_3$, so $r_3 \geq r_4$. Also for such M and N we have $M = NX$, where X is some finite subset of G. Putting $H = \overline{\langle X \rangle}$ we see $d(M/N) = d(HN/N) \leq d(H) \leq r_2$, giving $r_4 \geq r_2$. Finally let $H \leq_C G$. If HN/N ca be generated by d elements for every $N \lhd_O G$ then H can be generated topologically by a d-element subset, so $d(H) = \sup\{d(HN/N) \mid N \lhd_O G\} \leq r_4$. Hence $r_1 \leq r_4$. □

Historically, results in this topic referred to the concept of rank, for example Lazard's result which we will state later. Lubotsky and Mann later generalised the ideas to that of uniform pro-p groups. We now state a theorem without proof, to see this connection.

Theorem 1.6.2. *A pro-p group G has finite rank if and only if G is finitely generated and contains an open subgroup which is powerful.*

1.7 p-adic analytic groups

Definition 1.7.1. A topological group G is a p-adic analytic group if G has the structure of a p-adic analytic manifold (that is we can describe a point by a local power series) such that multiplication and inversion in G are both analytic functions. That is to say with the properties:
(i) the function $f : G \times G \to G$ defined by $(x, y) \mapsto xy$ is analytic and
(ii) the function $\iota : G \to G$ defined by $x \mapsto x^{-1}$ is analytic.

From the results of the last section, we can start to draw some conclusions about pro-p groups. We know that a uniform pro-p group is homeomorphic to $\mathbb{Z}_p^d$ and that every finitely generated powerful pro-p group contains a uniform pro-p group. This means every finitely generated pro-p group contains a subgroup topologically isomorphic to $\mathbb{Z}_p^d$.

Theorem 1.7.1. *A finitely generated profinite group G is a p-adic analytic group if and only if it contains an open subgroup that is a powerful finitely generated pro-p group.*

We do not prove prove the following theorems, as it would require much more analytic machinery than we care to employ, but instead give some explanation.

Since the subgroup lies in the Frattini series (recall the Frattini subgroup is the set of non-generating elements) we would expect the group as a whole to inherit some of this structure. We can also see that as group being p-adic analytic is equivalent to saying that the pro-p group has finite rank.

There is also a proposition that characterises uniformly powerful pro-p groups as being torsion-free, which is a good way of checking whether of not a group in question is in fact p-adic analytic.

Definition 1.7.2. A group is said to be *torsion-free* if the only element of finite order is the identity.

Theorem 1.7.2. *A powerful finitely generated pro-p group is uniform if and only if it is torsion-free.*

Proof. Let G be a finitely generated powerful pro-p group and write $G_i = P_i(G)$ for each i. Suppose that G is not torsion-free. Then G contains an element of order p (an element of finite order coprime to p would have to lie in G_i for every i and hence be 1). Say $x \in G_i/G_{i+1}$. Then $1 \neq xG_{i+1} \in G_i/G_{i+1}$ and $1 = x^pG_{i+2} \in G_{i+1}/G_{i+2}$, so the map $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is not injective. It follows that G is not uniform.

For the converse suppose that G is not uniform. Then for some i, the epimorphism $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is not injective, so there exists $x \in G_i/G_{i+1}$ such that $x^p \in G_{i+2}$, Put $x_2 = x$, and suppose that for some $n \geq 2$ we have found $x_2, \ldots, x_n$ satisfying $x_j^p \in G_{i+j}$ and $x_j \equiv x_{j-1} \mod G_{i+j-2}$ for $2 \leq j \leq n$. There exists $z \in G_{i+n-1}$ such that $z^p = x^p$; put $x_{n+1} = z^{-1}x_n$. Then $x_{n+1} \equiv x_n \mod G_{i+n-1}$. Also $x_{n+1}^p \in G_{i+n+1}$: for if p is odd we have

$$x_{n+1}^p = (z^{-1}x_n)^p \equiv z^{-p}x_n^p \left[x_n, z^{-1}\right]^{p(p-1)/2} \equiv 1 \mod G_{i+n+1},$$

since $[G_{i+n-1}, G, G][G_{i+n-1}, G]^p \leq G_{i+n+1}$; while if $p = 2$ we have

$$x_{n+1}^p = z^{-2}[z^{-1}, z_n^{-1}]x_n^2 \equiv z^{-2}x_n^2 = 1 \mod G_{i+n+1},$$

because $[G_{i+n-1}, G] \leq G_{i+n-1}^4 = G_{i+n-1}$ since G_{i+n-1} is powerfully embedded in G.

Thus the sequence $x_2, \ldots, x_n, \ldots$ can be constructed recursively; it is a Cauchy sequence and therefore converges to an element $x_\infty \in G$, say. Then $x_\infty \equiv x \equiv 1 \mod G_{i+1}$; and $x_\infty^p \equiv x_n^p \equiv 1 \mod G_{i+n-1}$ for all n, so $x_\infty^p = 1$. Thus G is not torsion-free.

□

Chapter 2

Examples of pro-p groups, and groups of formal power series.

In the following chapter, the theorems on formal power series can typically be found in Johnson [24], and those definitions and theorems pertaining to the Nottingham group have come from Camina's work [3] [4].

2.1 Matrix groups

Theorem 2.1.1. *$GL_d(\mathbb{Z}_p)$ is profinite.*

Proof. For each $n \in \mathbb{N}$ there exists a natural projection

$$\theta_n \ : \ GL_d(\mathbb{Z}_p) \to GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p),$$

explicitly written as

$$\theta_n(g) = g \mod p^n.$$

It is simple enough to then show that $\varprojlim GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p) = GL_d(\mathbb{Z}_p)$. This is most clear by considering $GL_d(\mathbb{Z}_p)$ as a subset of the set of matrices of dimension d, $M_d(\mathbb{Z}_p)$. This is isomorphic to $\mathbb{Z}_p^{d^2}$, and as subsets of profinite groups are profinite, $GL_d(\mathbb{Z}_p)$ is profinite. □

Theorem 2.1.2. *$SL_d(\mathbb{Z}_p)$ is profinite.*

Proof. Again, as closed subgroup of a profinite group is profinite, $SL_d(\mathbb{Z}_p)$ is a closed subgroup of $GL_d(\mathbb{Z}_p)$. □

Theorem 2.1.3 (Lazard's characterisation of compact p-adic Lie groups)**.** *. A compact topological group admits a p-adic analytic structure if and only if it is isomorphic to a closed subgroup of $GL_d(\mathbb{Z}_p)$ for a suitable degree d.*

2.2 Formal Power Series

Definition 2.2.1. Let R be a commutative ring with identity. We define $R[[t]]$ to be the set of formal power series in some indeterminate variable t.

Definition 2.2.2. The field of fractions of $R[[t]]$ is denoted $R((t))$.

Abstractly we can think of $R[[t]]$ as the completion of the polynomial ring $R[t]$ equipped with a particular metric. Since this forms a complete metric space, this automatically gives $R[[t]]$ the structure of a topological ring. We've already seen this; the p-adic valuation induce a metric (and hence a topology) on $\mathbb{Z}_p$, but it is different for different groups. For example, we are soon to discuss the Nottingham group; the only valuation with respect to which this group is complete is $v(\sum_{i=k}^{\infty} \alpha_i t^i) = k$, where $\alpha_k \neq 0$.

The topological ring $R[[t]]$ has multiplication and addition, defined as

$$\sum_{k=1}^{\infty} a_k t^k \; + \; \sum_{k=1}^{\infty} b_i t^i = \sum_{k=1}^{\infty} (a_k + b_k) t^k$$

and

$$\left(\sum_{k=1}^{\infty} a_i t^i \right) \times \left(\sum_{k=1}^{\infty} b_i t^i \right) = \sum_{k=1}^{\infty} (\sum_{j=0}^{n} a_j b_{n-j}) t^k.$$

Let $f(t) = \sum_{k=1}^{\infty} a_k t^k$ and let $g(t) = \sum_{j=1}^{\infty} b_j t^j$. We can form the composition in the ring of formal power series as below.

$$\begin{aligned} g(f(t)) &= \sum_{j=1}^{\infty} b_j (f(t))^j, \\ &= \sum_{j=1}^{\infty} b_j (\sum_{k=1}^{\infty} a_k t^k)^j, \\ &= \sum_{n=1}^{\infty} c_n (t)^n. \end{aligned}$$

The constants c_n are determined by multiplying out the power series explicitly, and can be written in the formula $c_n = \sum_{k=1}^{\infty} b_k a_{j_1} a_{j_2} \dots a_{j_k}$ such that $j_1 + \dots + j_k = n$.

2.3 The Nottingham group

Pro-p groups fall into 3 main categories. The kind we've seen, which is by far the simplest, are the p-adic analytic groups (i.e. those which contain a uniformly powerful subgroup that is torsion-free and isomorphic $\mathbb{Z}_p^d$). There are also $\mathbb{F}_p[[t]]$-linear groups, i.e. those which can be embedded as a subset of $GL_d(\mathbb{F}_p[[t]])$. The third are more exotic groups, usually exemplified by the Nottingham Group and is defined as follows.

Definition 2.3.1. Let A denote the group of continuous automorphisms of $\mathbb{F}_p((t))$ under formal substitution (composition of functions). An element of this group can be defined by its action on an indeterminate t, thusly.

$$tg = \sum_{i=0}^{\infty} a_i t^i, \quad a_i \in \mathbb{F}_p.$$

The Nottingham group $\mathcal{J} = \mathcal{J}(\mathbb{F}_p)$ is defined to be the subgroup of A which acts trivially on $(t)/(t^2)$, that is those automorphisms which have $a_0 = 0$ and $a_1 = 1$. Hence an element of $\mathcal{J}$ is written

$$tg = t + \sum_{i=2}^{\infty} a_i t^i, \quad a_i \in \mathbb{F}_p.$$

$\mathcal{J}$ indeed has the ring structure defined above, but the important thing to note is that the multiplication in the group is through composition of functions, and not multiplication in the ring. Since the elements are defined by their action on t, we may at times loosen notation and identify the above element g with its image in $\mathcal{J}$, $t + \sum_{i=2}^{\infty} a_i t^i$.

Definition 2.3.2. We write $d(\alpha)$ the 'degree' or 'depth' of our power series; the first power strictly greater than 1. We write $l(\alpha)$ for the leading coefficient of said power.
That is

$$d(t + at^n + \dots) = n$$

and

$$l(t + at^n + \dots) = a.$$

Lemma 2.3.0.1. $d(\alpha) = d(\beta) \Rightarrow l(\alpha\beta) = l(\alpha) + l(\beta)$.
It then follows that $l(\alpha^n) = nl(\alpha)$.

Proof. Let $\alpha = t + at^n + \dots$ and $\beta = t + bt^n + \dots$ Then

$$\begin{aligned} \alpha\beta &= (t + bt^n + \dots) + a(t + bt^n + \dots)^n + \dots \\ &= t + (a + b)t^n + \dots \end{aligned}$$

The fact that $l(\alpha^n) = nl(\alpha)$ follows by induction. □

Lemma 2.3.0.2. $[t + at^i + \ldots, t + bt^j + \ldots] = t + ab(i-j)t^{i+j-1} + \ldots$

Proof. Let $\alpha = t + at^i + t^{i+1}f(x)$ and $\beta = t + bt^j + t^{j+1}g(x)$, where $f(x)$ and $g(x)$ are in $R[[x]]$. Work modulo t^{i+j}. Then

$$\begin{aligned}\alpha\beta &= \beta + a(t + bt^j + t^{j+1}g(x))^i + (t + bt^j + t^{j+1}g(x))^{i+1}f(\beta).\\ &= \beta + at^i + iabt^{i+j-1} + t^{i+1}f(t)\\ &= \alpha + \beta + iabt^{i+j-1} - t.\end{aligned}$$

By the above lemma replacing the power by -1, we have

$$\alpha^{-1}\beta^{-1} = \alpha^{-1} + \beta^{-1} + iabt^{i+j-1} - t,$$

and so

$$\begin{aligned}\alpha^{-1}\beta^{-1}\alpha &= t + \beta^{-1}\alpha + iab\alpha^{i+j-1} - \alpha\\ &= t + \left(\beta^{-1} + \alpha - jabt^{i+j-1} - t\right) + iab\alpha^{i+j-1} - \alpha\\ &= \beta^{-1} + ab(i-j)t^{i+j-1}.\end{aligned}$$

Finally

$$\begin{aligned}\alpha^{-1}\beta^{-1}\alpha\beta &= t + ab(i-j)\beta^{i+j-1}\\ &= t + ab(i-j)t^{i+j-1}.\end{aligned}$$

□

Theorem 2.3.1. *i) $\mathcal{J}$ is profinite. ii) $\mathcal{J}$ is a normal subgroup of index $p-1$ in A.*

Proof. Define a chain of subsets $\mathcal{J}_n = \{g \in \mathcal{J} : tg \equiv t \mod t^{n+1}\}$. $\mathcal{J}_n \lhd \mathcal{J}$ and $|\mathcal{J}/\mathcal{J}_n| = p^{n-1}$ It can then be proved that $\mathcal{J} = \varprojlim \mathcal{J}/\mathcal{J}_n$. So $\mathcal{J}$ is a pro-p group, in fact, a finitely generated pro-p group. □

Proof. Since $[t+at^i, t+bt^j] = t+ab(i-j)t^{i+j-1}+...$, we can see $[\mathcal{J}_i, \mathcal{J}_j] \leq \mathcal{J}_{i+j-1}$ □

We might have expected this pro-p group to be defined more like the inverse limits in chapter one. For example If we consider $(\mathbb{Z}_p, +) = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})$, we're looking at $\sum_{i=0}^{n} a_i p^i$ for the elements of the groups in the inverse limit. The Nottingham group on the other hand behaves differently, as it's group action is function composition and not addition or multiplication. This is one of the first signs that the Nottingham Group may not be p-adic analytic.

Obviously the substitution of one finite power series into another will result in a degree larger than either individually, however if we take elements of $\mathcal{J}_n$

and compose them, we see the minimum degree does not change. If we define $v(\sum_{i=n}^{\infty} g_i t^i) = n$ then this is actually very similar to the p-adic valuation on $\mathbb{Z}_p$. It is the only valuation with respect to which $\mathbb{F}_p((t))$ is complete.

The Nottingham Group $\mathcal{J}$ is not a p-adic analytic group. There are a number of ways of showing this.

For instance for every n relatively prime to p there is $\sigma \in \mathcal{J}_n/\mathcal{J}_{n+1}$ such that $\sigma^p = e$. This is just showing that there exists an element of finite order, i.e. the group has a non-trivial torsion subgroup (set of elements of finite order).

Using algebraic number theory could achieve the same outcome by observing that given a natural number relatively prime to p there exists a cyclic totally ramified extension of degree p of a local field of characteristic p with the ramification break equal to that number. For a deeper look into this, please see [10] and [1].

Another way to argue is to use the property of p-adic analytic groups to contain an open subgroup of finite rank (i.e. an open subgroup for which the supremum of the number of generators of its closed subgroups is not infinity), see [4]. The group $\mathcal{J}$ doesn't contain an open subgroup of finite rank, since the number of generators of $\mathcal{J}_i$ tends to infinity when i tends to infinity.

2.3.1 Subgroups of the Nottingham group

So now we have some sort of grasp of what the Nottingham group is, a natural question to ask is what does its subgroup structure look like?

Finite index Subgroups

Since the elements of $\mathcal{J}$ are formal power series, we might expect there to be certain subseries that arise as proper subgroups of the Nottingham group. This is indeed the case.

Take some subset $I \subseteq \mathbb{N}$. We will call this an *admissable index set* if

$$\left\{ t + \sum_{i \in I} a_i t^i : a_i \in \mathbb{F}_p \right\}$$

forms a subgroup of J. If it does, we call the subgroup and index subgroup of $\mathcal{J}$, denoted $\mathcal{J}[I]$.

The Fesenko groups studied in [14] are a special kind of index subgroup. Let $q = p^r$ for some $r \in \mathbb{N}$ and prime p. Then $T = T(r)$ is defined

$$\left\{ t + \sum_{k \geq 1} a_{q^{k+1}} t^{q^{k+1}} : a_{q^{k+1}} \in \mathbb{F}_p \right\}.$$

This, among others, are generalised and classified in Barnea, and Klopsch [1], and the 4 types of index subgroups that appear are as follows:

$$\begin{aligned}
\mathcal{A}_x &:= J[x\mathbb{N}], \quad x \in \mathbb{N}. \\
\mathcal{B}_{r,s} &:= J[p^r\mathbb{N} \cup (p^s\mathbb{N} - 1)], \quad r, s \in \mathbb{N}; r \geq s. \\
\mathcal{C}_s &:= J[p^s\mathbb{N} - 1], \quad s \in \mathbb{N}. \\
\mathcal{D}_r &:= J[\{p^n - 1 : n \in \mathbb{N}\}].
\end{aligned}$$

We focus on the subgroups $\mathcal{A}_x$, as they are the same subgroups $\mathcal{J}_{(x)}$ that Rachel Camina studies in [4].

Definition 2.3.3.

$$\mathcal{J}_{(x)} = \left\{ g \in \mathcal{J}_{(x)} \ : \ tg = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right) \right\}$$

Where $\alpha_k \in \mathbb{F}_p$.

Theorem 2.3.2. *$\mathcal{J}_{(x)}$ is a closed subgroup of the Nottingham group for $x \geq 1$. Furthermore $\mathcal{J}_{(x)}$ is not open.*

Proof. Let $g, h \in \mathcal{J}_{(x)}$, such that $tg = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right)$ and $th = t\left(1 + \sum_{j=1}^{\infty} \beta_j t^{jx}\right)$. Then

$$\begin{aligned}
tgh &= t\left(1 + \sum_{j=1}^{\infty} \beta_j t^{jx}\right)\left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\left(1 + \sum_{j=1}^{\infty} \beta_j t^{jx}\right)^{kx}\right) \\
&= t\left(1 + \sum_{i=1}^{\infty} \gamma_i t^{ix}\right)
\end{aligned}$$

For some $\gamma \in \mathbb{F}_p$. Hence $gh \in \mathcal{J}_{(x)}$.

The closure of $\mathcal{J}_{(x)}$ follows from the fact that any sequence of elements that converges in $\mathcal{J}$ clearly converges in $\mathcal{J}_{(x)}$. So $\mathcal{J}_{(x)}$ is compact, closed under multiplication and hence closed under taking inverses.

Noting that $te_{kx} = t(1 + t^{kx}) \in \mathcal{J}_{(x)}$ for all $k \geq 1$ we see that $\mathcal{J}_{(x)}$ is infinite, so for $x \geq 1$ we have that $\mathcal{J}_{(x)}$ has infinite index. A closed subgroup of a profinite group is open if and only if it has finite index, so $\mathcal{J}_{(x)}$ is not open. □

In a finite p-group, the normalizer of a subgroup is strictly greater than the subgroup. This illustrates one of the differences between finite and infinite pro-p groups.

Theorem 2.3.3. *The normaliser of* $\mathcal{J}_{(x)}$, $N_{\mathcal{J}}\left(\mathcal{J}_{(x)}\right) = \mathcal{J}_{(x)}$.

We state this theorem without proof, as it is lengthy and can be found in [4].The following is also from the same paper, but we include the proof as it illustrates some of the behaviour of the Nottingham group more explicitly.

Theorem 2.3.4.

$$\mathcal{J}_{(x)} \cong \mathcal{J} \quad \text{if } x \not\equiv 0 \mod p,$$
$$\mathcal{J}_{(x)} \ncong \mathcal{J} \quad \text{if } x \equiv 0 \mod p.$$

Proof. Let $g \in \mathcal{J}_{(x)}(t)$; then

$$tg = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right)$$

for some $\alpha_k \in \mathbb{F}_p$. So

$$t^x g = (tg)^x = t^x \left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right)^x$$

and thus $g|_{\mathbb{F}_p((t))} \in \mathcal{J}(t^x)$. So we can define a map θ:

$$\theta \,:\, \mathcal{J}_{(x)}(t) \to \mathcal{J}(t^x)$$
$$g \mapsto g|_{\mathbb{F}_p((t))}$$

We now need to show that when $x \not\equiv 0$ modulo p, then θ is an isomorphism. Then as $\mathcal{J}(t^x) \cong \mathcal{J}(t)$, since $\mathbb{F}_p((t^x)) \cong \mathbb{F}_p((t))$, we have the result for this case. Since θ is clearly a homomorphism we just have to show that given $h \in \mathcal{J}(t^x)$ then there exists a unique element $g \in \mathcal{J}(t)$ such that $(t^x)h = (t^x)g$ and in fact this solution g actually lies in $\mathcal{J}_{(x)}(t)$. The existence of g is equivalent to solving an equation of the following type:

$$\begin{aligned} t^x \left(1 + \sum_{k=1}^{\infty} \beta_k t^{kx}\right) &= (t^x)h \\ &= (t^x)g \\ &= (tg)^x \\ &= t^x \left(1 + \sum_{j=1}^{\infty} \alpha_j t^j\right)^x \end{aligned}$$

where h and hence the β_k are given, and g and so the α_j are to be found.
We now construct a solution to the above equation and hence show that g exists. If $(t^x)h = t^x$, simply set $tg = t$ and we are done. If $(t^x)h \neq t^x$, then β_r, the first non-zero coefficient in $\sum_{k=1}^{\infty} \beta_k t^k$ is well-defined. So, we want

$$t^x \left(1 + \sum_{k=1}^{\infty} \beta_k t^{kx}\right) = t^x + \beta_r t^{(r+1)x} + \dots$$
$$= t^x \left(1 + \sum_{j=1}^{\infty} \alpha_j t^{jx}\right)^x$$

As $x \not\equiv 0 \mod p$ we must choose the first non-zero coefficient in $\sum_{j=1}^{\infty} \alpha_j t^j$ to be α_s, where $s = rx$ and $x\alpha_s = \beta_r$.

Now we proceed inductively. Suppose α_j has been chosen for $1 \leq j \leq l-1$ and is zero if j is not divisible by x. Then, as all non-zero powers of t in $(t^x)h$ are powers of t^x we can choose α_l to be non-zero only if l is divisible by x. In this case α_l is uniquely defined, thus we can construct a unique solution g, of the required form.

When $x \equiv 0 \mod p$ though, $\mathcal{J}_{(x)}$ does not contain any elements of finite order, unlike $\mathcal{J}$. Hence $\mathcal{J}_{(x)} \ncong \mathcal{J}$ in this case.

□

2.3.2 Embeddings into the Nottingham group

D.L. Johnson [24] was one of the first people to consider the Nottingham group. Lubotzky and Shalev [25] were also very influential. On the basis of their work, along with some papers of Witt's from the 1930s, Leedham-Green and Weiss proved the following:

Theorem 2.3.5. *Every finite p-group can be embedded as a closed subgroup into $\mathcal{J}$.*

R. Camina went on to prove the more general theorem that every countably based pro-p group can be embedded, but we shall look at the finite case for simplicity. Countably based means the topological base for neighbourhoods of the identity is countable. Real an algebraic closure of a field k is the field containing every root of a non-constant polynomial in the ring $k[x]$.

So let k be a field of characteristic p, with algebraic closure $\overline{k}$. We define a map similar to the Frobenius automorphism (the pth power map):

$$\mathcal{P} : \overline{k} \to \overline{k},$$

$$x \mapsto x^p - x.$$

Let $\mathcal{P}k = \{x^p - x \ : \ x \in k\}$.

Theorem 2.3.6 (Witt)**.** *Let Ω be a subgroup of k^+, such that $\mathcal{P}k \leq \Omega \leq k^+$ and $|\Omega/\mathcal{P}k|$ is finite. Then $\mathrm{Gal}(k(\mathcal{P}^{-1}\Omega)k) \cong \Omega/\mathcal{P}k$. Further, for every abelian extension K of k, of exponent p, there exists a group Ω such that $K = k(\mathcal{P}^{-1}\Omega)$.*

The map $\mathcal{P}$ works as when in a field of characteristic p it is a subgroup of the additive group k^+ of k, by virtue of the fact that $x^p - x + y^p - y = (x+y)^p - (x+y)$. By ensuring the existence of the subgroup Ω, it allows us to use its preimage under $\mathcal{P}$ to define a Galois group which will be isomorphic to $\Omega/\mathcal{P}k$. We can reverse the process by choosing a such a group (p-groups identify naturally with abelian extensions) and embed the group into the Galois extension field. We now need to ensure that there is such a field.

Theorem 2.3.7. *Let H be a finite p-group and $d(H)$ its minimal number of generators. For a field of characteristic p, let $[k : \mathcal{P}k] = p^N$ if it is finite, or ∞ if it is unbounded. Then there is a Galois extension field $\hat{K}$ such that $\mathrm{Gal}(\hat{K}/k) \cong H$ if and only if $d(H) \leq N$.*

The second theorem is more important for us as it ties in a lot of the key concepts we've seen throughout. Notice once again, the key condition that has to hold is on the minimal number of generators of the group. Now to turn our attention back to the Nottingham group we let $k = \mathbb{F}_p((t))$.

Lemma 2.3.7.1. *A basis for $\mathbb{F}_p((t))/\mathcal{P}\mathbb{F}_p((t))$ is the set*

$$\{1\} \cup \left\{t^{-i} \ : \ i \in \mathbb{Z}^+ \text{ and } i \not\equiv 0 \mod p\right\}.$$

Recall from algebraical number theory that a monic polynomial $f \in \mathcal{O}_k$, the ring of integers of a number field k is called *Eisenstein* at a prime p if all coefficients are divisible by p but the constant term is not divisible by p^2. A finite Galois extension L/K is said to be *totally ramified* if $L = K[\alpha]$ for some root α of an eisenstein polynomial. Totally ramified extensions act trivially on their residue fields. For more details, please see Algebraic Number Theory, by Frölich and Taylor [12].

Theorem 2.3.8. *Every finite p-group can be embedded as a closed subgroup into $\mathcal{J}$.*

Proof. Let H be a finite p-group. Then, by the theorem and lemma above, there exists an extension field K of $\mathbb{F}_p((t))$ such that $H \cong \mathrm{Gal}(K/\mathbb{F}_p((t)))$. We would then have a Galois extension field $\hat{K}$, but in fact we can simplify this, as K is a finite, totally ramified extension of $\mathbb{F}_p((t))$, which means $K \cong \mathbb{F}_p((t))$. Thus we have that $H \leq \mathrm{Aut}(\mathbb{F}_p((t)))$. We know that $\mathcal{J}$ has index $p-1$ in $\mathrm{Aut}(\mathbb{F}_p((t)))$ and since $p-1$ is prime to p and $|H| = p^n$, for some n, we must have that $H \leq J$, as required. □

2.4 Conclusion

The reader should hopefully now have a broad understanding of pro-p groups. We have seen how the field $\mathbb{Z}_p$ is constructed given both the inverse limit and topological definitions of profinite and pro-p groups. We've seen this extend to matrix groups like $SL_d(\mathbb{Z}_p)$; the more exotic Nottingham group, the different properties it can have, and some of the important theorems used to define it. The reader should also see the connection between a pro-p group containing an open, uniformly powerful subgroup and it being p-adic analytic.

For further reading for the group theorist I recommend the book "New horizons in pro-p groups", which is by far the most comprehensive references for pro-p groups. Popular mathematician Marcus Du Sautoy's writings are extremely accessible, for example [8], as well as his work with Dixon, Mann and Segal, in "Analytic Pro-p Groups" [7].

The theory of p-adics in their own right is vast and there is a plethora of resources, interesting theorems and examples available. I would recommend "A course in p-adic analysis" by Alain M. Robert, as well as Hensel's original papers. For those interested in the Nottingham group, Barnea and Klopsch [1], M Ershov[9], and I. Fesenko [14] are wonderful places to start.

Bibliography

[1] Barnea, Y., Klopsch, B., 2002. *Index subgroups of the Nottingham Group.* Advances in Mathematics 180 (2003), 187-221.

[2] Berkovich, Y., 2011. *Groups of Prime Power Order. American Mathematical Society*, Volume 48, Number 2, Pages 315-323.

[3] A. R. Camina and R. D. Camina, *Pro-p Groups of Finite Width.* School of Mathematics, University of East Anglia Norwich; DPMMS, University of Cambridge.

[4] Rachel Camina, 1997. *Some Natural Subgroups of the Nottingham Group*, Proceedings of the Edinburgh Mathematical Society (1999) 42, 333-339.

[5] Caranti, A; Mattarei, S; Newman, M.F; Scoppola, C.M. 1994. *Thin Groups of Prime Power Order and Thin Lie Algebras.*

[6] J.W.S. Cassels, 1986. *Local Fields.* London Mathematical Society.

[7] J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, (1991). *Analytic pro-p Groups.* Londom Mathematical Society Lecture Note Series 157.

[8] M.P.F. Du Sautoy, *Pro-p Groups*, Summer School in Group Theory in Banff, 1996, (ed. O. Kharlampovich) CRM Proc. Lecture Notes 17, Amer. Math. Soc., (1999), 99?130.

[9] Ershov, M. 2004. *On subgroups of the Nottingham group of positive Hausdorff dimension.*

[10] Fesenko, I, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields*

[11] C.E. Ford, *Characters of p-groups.* Proceedings of the American Mathematical Society, Vol. 101, No. 4 (Dec., 1987), pp. 595-601. http://www.jstor.org/stable/2046653.

[12] Frölich, A., Taylor, M.J., *Algebraic Number Theory*, Cambridge University Press; Reprint edition (4 Feb. 1993).

[13] D.J.H. Garling, 1986. *A Course in Galois Theory*. Cambridge University Press.

[14] Griffin, Cornelius, 2003. *The Fesenko Groups Have Finite Width*, The Mathematical Institute. http://arxiv.org/abs/math/0310038v1

[15] Hilbert, D., 1901-1902. *Mathematical Problems*. Bull. Amer. Math. Soc. 8, 437-479.

[16] Kevin Keating, 2005. *How close are pth powers in the Nottingham group?* Department of Mathematics, University of Florida. http://arxiv.org/abs/math/0207273v2

[17] E.I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, 1998.

[18] G. Klaas, C.R. Leedham-Green, W. Plesken, *Linear Pro-p-Groups of Finite Width*, Springer Verlag, 1997.

[19] Lazard. *Groupes analytiques p-adiques*, Inst. Hautes Etudes Scientifiques, Publ. Math. (26), 389?603 (1965).

[20] Leedham-Green, C.R., and McKay, S., 1975. *On p-Groups of Maximal Class I.*

[21] Leedham-Green, C.R., O'Brien E.A., Eick, B., 2001. *Constructing Automorphism Groups of p-Groups.*

[22] C.R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order*, Oxford University Press, 2002.

[23] Loomis,Lynn H., 1953. *An Introduction To Abstract Harmonic Analysis*

[24] Johnson, D. L., The Group of Formal Power Series Under Substitution. J. Austral. Math. Soc. (Series A) 45 (1988), 296-302.

[25] A. Lubotzky and A. Shalev, *On some p-analytic pro-p groups*, Israel J. Math. 85 (1994), 307-337.

[26] Reid, C, 2009/2013. *On the structure of just infinite profinite groups*. School of Mathematics, Queen Mary, University of London. http://www.arxiv.org/abs/0906.1771v2.

[27] D.C. Smyth. 2010. *Finitely Generated Powerful Pro-P Groups*. School of Mathematics, University of New South Wales.

[28] Stephen S.Shatz, 1972. *Profinite Groups, Arithmetic, and Geometry*. Princeton University Press and University of Tokyo Press.

[29] Sutherland, W.A., *Introduction to Metric and Topological Spaces*. Clarendon Press: Oxford University Press 1975.

[30] B.A.F. Wehrfritz, 1973. *Infinite Linear Groups*. Springer-Verlag.

[31] J.S. Wilson, *Profinite Groups*, Oxford University Press, 1998.