Characterization of Uniform Pro-p Groups

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

A P Aravintakshan

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2023

Supervisor: Dr Supriya Pisolkar

Certificate

This is to certify that this dissertation entitled Characterization of Uniform Pro-p Groupstowards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by A P Aravintakshanat Indian Institute of Science Education and Research under the supervision of Dr Supriya Pisolkar, Associate Professor, Department of Mathematics , during the academic year 2022-2023.

Supriya

Dr Supriya Pisolkar

Committee:

Dr Supriya Pisolkar

Dr Debargha Banerjee

To Malini

Declaration

I hereby declare that the matter embodied in the report entitled Characterization of Uniform Pro-p Groups are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr Supriya Pisolkar and the same has not been submitted elsewhere for any other degree.

Aravint

A P Aravintakshan

Acknowledgments

I would like to express my heartfelt gratitude to Dr Supriya Pisolkar under whose supervision I had done my masters thesis. Only due to her constant guidance, encouragement and patience, I was able to produce a high quality thesis work. I am very thankful to Dr. Debargha Banerjee for agreeing to be the Expert for my masters thesis.

My entire journey at IISER would not have been possible without the guidance I have received from various esteemed set of Professors here. I would like to heartfully thank Dr. Supriya Pisolkar Dr.Vivek Mohan Mallick, Dr.M.S.Madhusudhan, Dr. Chandrasheel Bhagwat, Dr. Anupam Kumar Singh and Dr.Amit Hogadi in particular. I would also like to thank discipline-wise project coordinator Dr. Steven Spallone for their valuable feedback.

In addition I would like to thanK Ipsa, Pavith, Karthik, Biswanath, Anand, Tanuj, Varun, Aniketh, Shruthi, and Mihir for their mathematical insights and extremely friendly nature.

I would like to finally thank my mother, Malini, who's stood as my pillar of support through the highs and lows, and has never failed to encourage , motivate and Inspire me.

Abstract

Uniform pro-p groups have been studied extensively by Lazard in his seminal paper *Groupes analytiques p-adiques* (1965). Since then, many approaches have been developed to characterise various families of pro-p groups. The techniques involve- Lie theoretic methods, purely group theoretic methods and cohomological methods. In this project, we survey what is known towards characterising powerful pro-p groups and Uniform pro-p groups, primarily using Group Theoretic Methods

Contents

Introduction

Uniform Pro-p groups are specialised family of pro-p groups that have extensive applications in the field of p-adic Lie theory, and pro-p groups in general. A characterization of pro-p groups was given in [DMSS] as follows. *A pro-p group has finite rank if and only if it admits a uniform open subgroup.*

In this thesis, we look to understand and characterize different families of pro-p groups, especially uniform pro-p groups and powerful pro-p groups. The first chapter will deal with the prerequisite topics such as Powerful p-groups, Frattini subgroups, Topological which will form essential building blocks for theory of Uniform and Powerful pro-p groups. The second chapter then focuses on understanding the basic structure of a larger classes of profinite groups , pro-p groups and procyclic groups. In the third chapter, we deep dive into the the family of Powerful and Uniform pro-p groups. We look at the similarity of these groups with abelian groups. Then We cover a significant result that Uniform groups are homeomorphic to ${\mathbb{Z}_p}^d$, where d is the number of topological generators of the group. We then describe the natural additive structure on a uniform group that enables it to have a free $\mathbb{Z}_p$ module structure. Following this, An additional bracket operation on $(G, +)$ that gives a G a $\mathbb{Z}_p$-Lie Algebra structure. We discuss various examples. In our final chapter, using the theory built up, we begin to develop a characterization for Powerful and Uniform pro-p groups, based from the paper by Benjamin Klopsch and Ilir Snopce [BI].

Original Contribution : This thesis is primarily a literature review of concepts and results in the field of Powerful and Uniform pro-p groups, and using them to draw a brief characterization of Uniform pro-p groups. A few examples and certain details in proofs have been added to create better understanding of the topic for the reader. The contents of the thesis largely follow [DMSS], which was the primary reading material.

Chapter 1

Preliminaries

This chapter deals with advanced Group theory topics that would be of use in this thesis. The contents of this chapter are mostly referred from [DF] on topics related to basic group theory and [DMSS] for powerful p-groups and Inverse limits. Have referred to [KC] for proofs in Topological groups.

1.1 Group Theory

In this section, we would be discussing select advanced group theoretic and topological theories

1.1.1 Commutator Subgroups

Definition 1.1.1. *Given a Group G:*

- *The Commutator, $[a, b]$, of two elements $a, b \in G$ is defined by*

$$[a, b] := a^{-1}b^{-1}ab$$

- *The commutator $[A.B]$, of two subgroups $A, B \in G$ is defined by*

$$[A, B] := \langle [a, b] | a \in A, b \in B \rangle$$

where $\langle X \rangle$ denotes the subgroup of G generated by X, a subset of G.

Notation 1. $[x, y]^z := z^{-1}[x, y]z$

Notation 2. $[A, B, C] := [[A, B], C]$

Remark 1.1.1. *The following are few basic properties of commutators. If x,y,z are elements of G , then :*

- $[xy, z] = [x, z]^y[y, z]$
- $[x, yz] = [x, z][x, y]^z$
- $[x^n, y] = \prod_{i=1}^{n}[x, y]^{x^{n-i}}$
- $[x, y^n] = \prod_{i=0}^{n-1}[x, y]^{y^i}$
- *If $x, y \in G$ then $(xy)^n \equiv x^n y^n [y, x]^{n(n-1)/2} (\mathrm{mod}[[G, G], G])$.*

Remark 1.1.2. ***Hall Wiit's Identity*** *If x, y, z elements of normal subgroups A, B, C of G respectively. Then:*

$$\left[x, y^{-1}, z\right]^y \left[y, z^{-1}, x\right]^z \left[z, x^{-1}, y\right]^x = 1$$

Proof. consider one of the commutators $[x, y^{-1}, z]^y$

$$\begin{aligned}\left[x, y^{-1}, z\right]^y &= y^{-1}\left[\left[x, y^{-1}\right], z\right] y \\ &= y^{-1}\left[x^{-1}yxy^{-1}, z\right] y \\ &= y^{-1}(yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}z)y \\ &= x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy\end{aligned}$$

Similarly we can get expressions for other commutators and by combining all, we will get the required result. □

Proposition 1.1.1 (3-Subgroup Lemma). *If A,B,C are 3 normal subgroups of G, then* $[A, B, C] \leq [B, C, A][C, A, B]$

Proof. Consider the group $\langle (a, b^{-1}, c] \mid a \in A, b \in B, C \in C \rangle$. Using the Hall Witt Identity, we get:

$$\begin{aligned}
\big[a, b^{-1}, c\big]^{b} \big[b, c^{-1}, a\big]^{c} \big[c, a^{-1}, b\big]^{a} &= 1 \\
\big[a, b^{-1}, c\big] &= b([c, a^{-1}, b]^{a})^{-1}([b, c^{-1}, a]^{c})^{-1}b^{-1} \\
&= b(\big[c, a^{-1}, b\big]^{a})^{-1}(\big[b, c^{-1}, a\big]^{c})^{-1}b^{-1} \\
&= ((\big[c, a^{-1}, b\big]^{a})^{-1}(\big[b, c^{-1}, a\big]^{c})^{-1})^{b}
\end{aligned}$$

Since [A,B,C], [B,C,A] , [C,A,B] all are normal subgroups of G, the above result implies any element of [A,B,C] can be expressed as a product of elements of [B,C,A] and [C,A,B] hence the containment is achieved. □

1.1.2 Frattini Subgroups

In this subsection we cover Frattini subgroups and their various useful properties.

Definition 1.1.2. *Frattini Subgroup of a group G ,* $\Phi(G)$ *is defined to be the intersection of all maximal subgroups of G.*

Remark 1.1.3. *Frattini subgroups are normal, characterestic subgroups (subgroups invariant under all group automorphisms).*

Proposition 1.1.2. $\Phi(G)$ *is the smallest normal subgroup* N *of* G *such that* G/N *is an elementary abelian p-group(i..e A Group is said to be elementary abelian if it is abelian and all non trivial elements have order p)*

Proof. Let M be any maximal subgroup of G. Now, G/M is abelian as it is a cyclic group of order p. This shows that $G, G \leq M$ for all M, which implies that $[G, G] \leq \Phi(G)$, hence $G/\Phi(G)$ is abelian.

Let $x \in G$ and observe G/M. Since $|G/M| = p$ we have $(xM)^{p} \in M$. This implies that $x^{p} \in M$ for all $x \in G$ for all M. Thus, $x^{p} \in \Phi(G)$ for all $x \in G$.

Now, any element of $G/\Phi(G)$ is of the form $\Phi(G)x$ where $x \in G$. Thus, we have $(\Phi(G)x)^p = \Phi(G)x^p = \Phi(G)$. It follows that $G/\Phi(G)$ is an elementary abelian p-group. To show it's the smallest such subgroup, Take any $H \lhd G$ such that G/H is elementary abelian.If $|G/H| = p^n$, then:

$$G/H \cong \prod_{i=1}^{n} \langle Hx_i \rangle$$

where $\langle Hx_i \rangle$ are right cosets of G/H. Now, G/H has n-maximal subgroups H_i/H (each being isomorphic to product of n-1 cosets).The intersection of all these maximal subgroups is trivial, and using lattice isomorphism theorem (between subgroups of G containing H and subgroups of G/H), we can deduce that $\cap_{i=1}^{n} H_i = H$ and alson every H_i is a maximal subgroup (as it is normal and has index p in G). Since H is an intersection of finitely many maximal groups, $\Phi(G) \leq H$ □

Remark 1.1.4. *Since $G/\Phi(G)$ is elementary abelian, If G is a finitely generated p-group, one can deduce that $G/\Phi(G) \cong F_p^d$. Thus the quotient gives us more information about the generators of the group.*

Proposition 1.1.3. *If G is a p-group, then $\Phi(G) = G^p[G,G]$ where $G^p = \langle g^p | g \in G \rangle$*

Proof. Since $\Phi(G)$ contains all x^p for all $x \in G$, $G^p \subseteq \Phi(G)$ and $[G,G] \subseteq \Phi(G)$ and hence $G^p[G,G] \subseteq \Phi(G)$ To show the other way inclusion, we use the fact that $G/[G,G]G^p$ is elementary abelian. It is abelian as it contains $[G,G]$ and given a non trivial element $x \in G$, we get $x^p \in G^p$. Thus from Proposition 1.1.2, we get the reverse inclusion, and hence the result. □

Frattini subgroups give a fascinating insight into the generators of a group:

Theorem 1.1.4. *The frattini subgroup is equal to the set of all non generators of the group.*

Remark 1.1.5. *A non generator element of a Group $g \in G$ is defined as follows: If $G = \langle X, g \rangle$, then $G = \langle X \rangle$.*

Proof. Let S be the set of all generators of G. Let $g \in S$. Suppose there exists atleast one maximal proper subgroup H such that $g \notin H$, then $G = \langle H, g \rangle$. Since g is a non generator, $G = \langle H \rangle$ which is a contradiction as $H < G$. Thus $g \in \Phi(G)$ Conversely, Let $g \in \Phi(G)$. Let $G = \langle X, g \rangle$ but $G \neq \langle X \rangle$. Suppose $g \notin S$. We know that $\langle X \rangle = \cap\{K | \langle X \rangle \subseteq K \subseteq G\}$. If

M is a maximal proper subgroup containing $\langle X\rangle$, then, $g \in M$ thus $M \geq \langle X, g\rangle = G$. This shows that M is not proper subgroup of G, which is a contradiction. Thus, $g \in S$. □

Proposition 1.1.5. Burnside Basis Theorem *If G is a finite p-group, and $X \subseteq G$ such that $X\Phi(G)$ generates $G/\Phi(G)$, then X generates G.*

Proof. Suppose $\langle X\rangle < G$ then $\langle X\Phi(G)\rangle = \langle X\rangle \Phi(G) \subset H$ where H is maximal proper subgroup of G , and hence $\langle H\rangle < G/\Phi(G)$, which is a contradiction. Hence $\langle X\rangle$ generates G. □

Proposition 1.1.6. *Let H be the set of all automorphisms of a finite p-group G which induce identity on $G/\Phi(G)$. Then H is a finite p-group.*

Proof. It is enough to show that if $\alpha \neq 1 \in H$ has prime order q, then $q = p$. Let ϕ be an element of H of order q. Now given ϕ acts as the identity on $G/\Phi(G)$, so ϕ acts on each coset of $\Phi(G)$. The orbits of ϕ thus are each of length either 1 or q, which tells us that $\Phi(G)x$ contains a fixed point. Thus there is an element in each coset of $\Phi(G)$ which is invariant under ϕ. Taking their images under the quotient map from G onto $G/\Phi(G)$, we get the generating set of $G/\Phi(G)$. Choosing a basis of $G/\Phi(G)$ and using the previous result, we get that G is generated by elements that are fixed by ϕ. Hence H is a finite p-group. □

1.1.3 Nilpotent Groups and Central Series

In this section we discuss briefly about Nilpotent groups and Lower central series associated with a Group.

Definition 1.1.3. *A Group is said to be Nilpotent if it has a terminating lower central series i.e, $\gamma_{n+1}(G) = 1$ for some n.*

Remark 1.1.6. *We would be dealing with two main variants of a lower central series in this thesis, which are defined as follows:*

1. **Lower Central series** *For any group G the lower central series of G is defined recursively by*

$$\gamma_1(G) = G, \gamma_k(G) = [\gamma_{k-1}(G), G]$$

2. **Lower p-central series** *For any group G the lower p-central series of G is defined recursively by*

$$P_1(G) = G, P_k(G) = (P_{k-1}(G))^p \left[P_{k-1}(G), G\right]$$

Remark 1.1.7. *The value of n from the definition of a nilpotent group is defined as the nilpotency class of the group.*

We now prove a fairly useful property about Nilpotent groups :

Proposition 1.1.7. *If $H = \langle a_1, \ldots . a_t \rangle$ is a finitely generated nilpotent group then every element of $[H, H]$ is equal to a product of the form $[x_1, a_1] \ldots [x_d, a_d]$ with $x_1, \ldots., x_d \in H$*

Proof. By Induction on the nilpotency class c of the group, i.e, $\gamma_c(H) \subseteq Z(H)$. If $c = 1$, H becomes abelian, and the result is trivial. Thus assume $c \geq 2$. From Remark 1.1.1 and using the fact that $\gamma_c(H) \subseteq Z(H)$, we get the following: if $u \in \gamma_{c-1}(H)$, then

$$\begin{aligned}[u, a_1^{e_1} \ldots a_d^{e_d}] &= [u, a_1^{e_1}] \ldots [u, a_d^{e_d}] \\ &= [u, a_1]^{e_1} \ldots [u, a_d]^{e_d} \\ &= [u^{e_1}, a_1] \ldots . [u^{e_d}, a_d]\end{aligned}$$

and if $u_1, \ldots, u_d, v_1, \ldots, v_d \in \gamma_{c-1}(H)$ then:

$$\begin{aligned}\prod [u_i, a_i] \cdot \prod [v_i, a_i] &= \prod [u_i, a_i] [v_i, a_i] \\ &= \prod v_i^{-1} [u_i, a_i] v_i [v_i, a_i] \\ &= \prod [u_i v_i, a_i]\end{aligned}$$

From the above two computations we can say for any element $w \in \gamma_c(H)$ is of the form $w = [w_1, a_1] \ldots [w_d, a_d]$, where $[w_i, a_i]$ and $w_i \in \gamma_{c-1}(H)$. Now let $g \in [H, H]$. By induction hypothesis we have :

$$\begin{aligned}g &\equiv [y_1, a_1] \ldots [y_d, a_d] \, (\text{mod} \gamma_c(H)) \\ g &= [y_1, a_1] \ldots [y_d, a_d] \, w \\ &= \prod [y_i, a_i] \prod [w_i, a_i] \\ &= \prod [w_i y_i, a_i]\end{aligned}$$

Which gives the result. □

1.1.4 Powerful Groups

We introduce the concept

Definition 1.1.4. *1. A finite p-group G is powerful if p is odd and G/G^p is abelian, or $p = 2$ and G/G^4 is abelian.*

2. A subgroup N of a finite p-group G is powerfully embedded in G, written N p.e. G, if p is odd and $[N, G] \leq N^p$, or $p = 2$ and $[N, G] \leq N^4$.

Remark 1.1.8. *G is powerful if and only if G p.e G ; N p.e G implies that $N \lhd G$ and N is powerful.*

Remark 1.1.9. *All powerful groups are solvable as given a group G powerful. We have $[G, G] \subseteq G^p$ which implies $[G^p, G^p] \subseteq (G^p)^p$. Thus we can define a normal series by: $\gamma_1(G) = G, \gamma_i(G) = \gamma_{i-1}(G)^p$. This normal series has every quotient $\gamma_i(G)/\gamma_{i-1}(G)$ abelian, and thus is solvable.*
On the other hand, all solvable groups are not powerful. For example, the Dihedral group of 8 elements , D_8, is a solvable group that is not powerful as $D_8/(D_8)^4 \cong D_8$ is not abelian.

Powerful p-groups share many common structural features with Abelian groups, some of them discussed in the below lemma:

Lemma 1. *Let G be a finite p-group and $K, N, W \lhd G$ with $N \leq W$. Then :*

1. *If N p.e. G then NK/K p.e.G/K.*
2. *If p is odd and $K \leq N^p$, or if $p = 2$ and $K \leq N^4$, then N p.e. G if and only if N/K p.e. G/K.*
3. *If N p.e. G and $x \in G$ then $\langle N, x\rangle$ is powerful.*
4. *If N is not powerfully embedded in W, then there exists a normal subgroup J of G such that given p is odd, then :*

$$N^p[N, W, W] \leq J < N^p[N, W] \text{ and } |N^p[N, W] : J| = p$$

Proof. (1) follows as $[NK/K, G/K] = [N, G]\, K/K \leq N^pK/K = (NK/K)^p$.

(2). From (1) we have $[NK/K, G/K] \leq (NK/K)^p$. Since $K \leq N^p$, we can say that $[NK/K, G/K] \leq (N/K)^p$. To show converse, $[NK/K, G/K] = [N, G]\, K/K \leq (N/K)^p$. From here we get, $[N, G]\, K \leq N^p$ and thus $[N, G] \leq N^p$.

For (3),Take $H = \langle N, x \rangle$. As $N \lhd H$, we get that $[H, H] = [N, H]$, and since N p.e in G, we have $[H, H] = [N, H] \leq [N, G] \leq N^p \leq H^p$.

In (4), taking p to be an odd prime, Let $M = N^p[N, W] > N^p$. Now since G is a finite p-group and M, N are normal in G, we know there exists $J \lhd G$ such that $N^p \leq J < M$ and $|M : J| = p$ [DF]. Now $M/J \in Z(G/J)$, thus, $[M, G] \leq J$ implying $N^p\, [N, W] \leq N^p\, [N, W, W] \leq N^p\, [N, W, G] \leq J$, which is our required result. □

Proposition 1.1.8. *Let G be a finite p- group and $N \leq G$. If N p.e G, then N^p p.e in G.*

Proof. If N^p does not powerfully embed in G there exists a $J \lhd G$ such that $(N^p)^p\, [[N^p, G]\, , G] \leq J$ and $[(N^p)^p\, [N^p, G] : J] = p$. Going modulo J, i.e, $(N^p)^p = (N^p)^p\, [[N^p, G]\, , G] = 1$. This implies $[N^p, G] = [N, G, G] < Z(G)$, and thus the map $f : G \to Z(G)$ given by $x \longmapsto [n, g, x]$ is a homomorphism for all $n \in N$ and $g \in G$. Thus:

$$\prod_{j=0}^{p-1} [n, g, n^j] = \prod_{j=0}^{p-1} [n, g, n]^j = [n, g, n]^{p(p-1)/2}$$

So, if $y \in N$ and $g \in G$:

$$\begin{aligned}
[y^p, g] &= [y, g]^{y^{p-1}} \ldots [y, g] \\
&= \prod_{j=p-1}^{0} [y, g][y, g, y^j] \\
&= [y, g]^p \prod_{p-1}^{0} [y, g, y^j] \\
&= [y, g]^p [y, g, y]^{p(p-1)/2} \quad = 1 \text{ since } [x, g, x^j] \in Z(G)
\end{aligned}$$

Now $[N, G]^p = 1$. Using all results and removing the modulo,

$$\begin{aligned}
[N^p, G] &\subseteq [N, G]^p\, [[N, G]\, , N]^p \\
&\subseteq N^{p^p}\, [N^p, G]^p \\
&\subseteq N^{p^p}
\end{aligned}$$

Thus N^p p.e in G. □

Lower p-series of a powerful p-group have various useful and interesting properties, some of which discussed below:

Proposition 1.1.9. *Let $G = (a_1, \ldots, a_d)$ be a powerful p-group, and put $G_i = P_i(G)$ for each i.*

1. *G_i p.e. G , and $G_{i+1} = \Phi(G_i) = G_i^p$*
2. *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ for each $k \geq 0$*
3. *The map $x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} onto G_{i+k}/G_{i+k+1}, for each i and k.*
4. *Every element of G^p is a p^{th} power in G*
5. *$G_i = G^{p^{i-1}} = \left\{x^{p^{i-1}} \mid x \in G\right\} = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{t-1}}\right\rangle$*
6. *If $G = \langle a_1, \ldots, a_d\rangle$ is a powerful p-group then $G = \langle a_1\rangle \ldots \langle a_d\rangle$, i.e, G is the product of its cyclic subgroups $\langle a_i\rangle$*

Proof. (1) The base case $i = 1$ is trivial. Suppose if G_i p.e in G, then $G_{i+1} = G_i^p [G, G] = G_i^p$ and $\Phi(G_i) = G_i^p [G_i, G_i] = G_i^p$.

(2) Proceed by Induction on k. The base case $k = 1$ follows from (1). Suppose the statement true up to $k = n$, i.e, $G_{i+n} = P_{n+1}(G_i) = G_i^{p^n}$. Now $G_{i+n+1} = \Phi(G_{i+n}) = P_2(G_{i+n}) = P_2(P_n(G_i)) = P_{n+2}(G_i)$. Also, $G_{i+n+1} = \Phi(G_{i+n}) = G_{i+n}^p = G_i^{p^{n+1}}$, this proves the case $n + 1$,and thus the result follows by Induction.

(3) Let's prove for the case $k = 1$, i.e,The map $x \mapsto x^p$ induces a homomorphism from G_i/G_{i+1} onto G_{i+1}/G_{i+2}. Let's take $G = G_i$. We go modulo $G_3 = P_3(G_i) = G_2^p$, then $[G, G] \leq G_2 \leq \mathrm{Z}(G)$ Thus given $x, y \in G$, we get that $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$. If p odd, then $p | p(p - 1)/2$, so $[y, x]^{p(p-1)/2} \in G_2^p = G_3 = 1$. If $p = 2$, then $[G, G] \leq G^4 \leq G_3 = 1$ and thus we get $(xy)^p = x^p y^p$ and thus $x \mapsto x^p$ is a homomorphism from G/G_2 onto G_2/G_3. Now to prove for all k, take composition of all homomorphisms from G_i/G_{i+1} onto G_{i+1}/G_{i+2} and from G_{i+1}/G_{i+2} to G_{i+2}/G_{i+3} and so on to get the required result.

(4) Proceed by Induction on $|G|$. Let $g \in G^p$. From (3), there exists $x \in G$ and $y \in G_3$ such that $g = x^p y$. Now Let $H = \langle G^p, x\rangle$. Then G^p p.e in G, from Lemma 1, we get that H is powerful. Also, $g \in H^p$ as $y \in G_3 = G_2^p$. If $H = G$, $G = \langle G^p, x\rangle = \langle \Phi(G), x\rangle = \langle x\rangle$ and

since G is a finite p-group, it follows. If $H \neq G$, then by Induction we get g is a p^{th} power in H.

(5) We know $G_{i+k} = G_i^{p^k} = G^{p^{i+k-1}}$. Also from (4), we know $G_i = \{x^p | x \in G_i - 1\} = \{x^{p^{i-1}} | x \in G\}$. From (3), take the map $\theta : G/G_2 \to G_i/G_{i+1}$ given by $x \mapsto x^{p^{i-1}}$. Then, G_i/G_{i+1} is generated by $\{\theta(a_1G_2), \ldots, \theta(a_dG_2)\}$, so $G_i = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle G_{i+1}$. Since $G_{i+1} = \Phi(G_i) = G_i^p = G^{p^{i-1}}$, we get that $G^{p^{i-1}} = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle$.

(6)Say $G_{k+1} = 1$. Arguing by induction on k, we may suppose that $G = \langle a_1 \rangle \ldots \langle a_d \rangle G_k$. But $G_k = \left\langle a_1^{p^{k-1}}, \ldots, a_d^{p^{k-1}} \right\rangle$ and $G_k \subseteq Z(G)$, and thus $G = \langle a_1 \rangle \ldots \langle a_d \rangle$. □

Notation 3. *d(G) is defined as the minimum cardinality of a set of generators for a finite p-group G. Thus* $d(G) = dim_{\mathbb{F}_p}(G/\Phi(G))$

Definition 1.1.5. *Rank of a finite p-group is defined by* $rk(G) := \sup\{d(H) | H \leq G\}$

Proposition 1.1.10. *If G is a powerful p-group and $H \leq G$ then $d(H) \leq d(G)$. In other words if G is a powerful p-group, then $rk(G) = d(G)$*

Proof. The proof is by induction on $|G|$. Let $d = d(G)$ and put $m = d(G_2)$. Since G_2 is powerful, so by the inductive hypothesis we may suppose that the subgroup $K = H \cap G_2$ satisfies $d(K) \leq m$. The map $\pi : G/G_2 \to G_2/G_3$ given by $x \mapsto x^p$ is an epimorphism. So we have $dim_{\mathbb{F}_p}(ker\pi) + dim_{\mathbb{F}_p}(Im\pi) = dim_{\mathbb{F}_p}(G/G_2) = d(G) = d$ and thus $dim(ker\pi) = d - dim_{\mathbb{F}_p}(Im\pi) = d - d(G_2) = d - m$.

Now let $dim(HG_2/G_2) = e$, i.e, $HG_2 = \langle h_1, \ldots, h_e \rangle G_2$ where $h_1, \ldots, h_e \in H$. From earlier computations, we get $dim\,(ker\pi \cap HG_2/G_2) \leq d - m$ and thus:

$$\begin{aligned} dim(\pi(HG_2/G_2)) &= dim(HG_2/G_2) - dim(ker\pi \cap HG_2/G_2) \\ &\geq e - (d - m) = m - (d - e) \end{aligned}$$

Since $\Phi(K) \leq K^p$ and $\Phi(K) \leq G_3$, the subspace of $K/\Phi(K)$ spanned by $h_1^p, \ldots, h_e^p$ has dimension at least $dim(\pi(HG_2/G_2)) \geq m - (d - e)$. Thus we have $m - (d - e) \leq d(K) \leq m$, and there exist elements $k_1, \ldots, k_{d-e}$ of K such that $K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e} \rangle \Phi(K) = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e} \rangle$. Therefore, $H = H \cap \langle h_1, \ldots, h_e \rangle G_2 = \langle h_1, \ldots, h_e \rangle (H \cap G_2) = \langle h_1, \ldots, h_e \rangle K = \langle h_1, \ldots, h_e, k_1, \ldots, k_{d-e} \rangle$. Thus $d(H) \leq d - e + e = d$. This gives us that $rk(G) = \sup\{d(H) | H \leq G\} = d = d(G)$ and completes the proof. □

1.2 Topological Groups

We will be studying properties of Topological groups.

Definition 1.2.1. *A topological group is a set G which is a group as well as a topological space such that the following maps are continuous.*

$$g \mapsto g^{-1}; G \longmapsto G \qquad\qquad (g,h) \mapsto gh; G \times G \longmapsto G$$

Remark 1.2.1. *For each $g \in G$, the maps $x \mapsto xg$, $x \mapsto gx$ and $x \mapsto x^{-1}$ are all homeomorphisms of G.*

Let's discuss some basic properties of Topological groups:

Proposition 1.2.1. *If G is a topological group, then:*

1. *Cosets of open subgroup of G are open.*
2. *Every open subgroup of G is closed.*
3. *G is Hausdorff if and only if $\{1\}$ is a closed subset of G.*
4. *If N is a closed normal subgroup of a Hausdorff group G, then G/N is Hausdorff.*
5. *If H is a subgroup of G and if H contains a non empty open subset U of G then H is open in G.*

Proof. (1) follows as the maps $x \mapsto xg$, $x \mapsto gx$ are all homeomorphisms, every coset of an open subgroup is open .

For (2) we use (1) to get that the complement of every open subgroup is union of open cosets, hence every open subgroup is closed.

(3) In Hausdorff spaces, singletons are closed. Conversely if singletons are closed, Let $h \neq g$ be elements of G. Then $h^{-1}g \neq 1$. Let U be a neighbourhood of e such that $h^{-1}g \notin U$. Since the map $(x,g) \mapsto x^{-1}g$ is continuous, there exists a neighbourhood V of e such that $VV^{-1} \subseteq U$. Now gV and hV are neighbourhoods of g an h respectively. And $gV \cap hV = \emptyset$, as if not, then there exists $v_1, v_2 \in V$ such that $gv_1 = hv_2$. This gives us $h^{-1}g = v_2v_1^{-1} \in VV^{-1} \subseteq U$ which is a contradiction.

(4) Consider the map $\pi : G \to G/N$. This map is open, so consider the open mapping $\Pi : G \times G \to G/H \times G/H$ given by $\Pi(x,y) = (xH, yH)$, the image of the open set $W =$

$\{(x,y) \in G \times G | x^{-1}y \notin H)$ maps to the complement of the diagonal of $G/H \times G/H$ (which is given by $\{gH, gH | g \in G\}$). Since the complement is open, the diagonal is a closed subspace, and thus G/H is Hausdorff since distinct cosets of G/H can have disjoint open neighbourhoods.

(5) $H = \bigcup_{h \in H}(Uh)$ and arbitrary union of open sets are open, hence H is open in G. $\square$

1.3 Inverse Systems and Inverse Limits

Definition 1.3.1. *An inverse system of Groups over Λ (Λ being a directed set) is a family of groups $(G_\lambda)_{\lambda \in \Lambda}$ with homomorphisms $\pi_{\lambda\mu} : G_\lambda \to G_\mu$ whenever $\lambda \geq \mu$, satisfying the conditions $\pi_{\lambda\mu}\pi_{\lambda\lambda} = Id_{G_\lambda}$ and $\pi_{\mu\upsilon} = \pi_{\lambda\upsilon}$ whenever $\lambda \geq \mu \geq \upsilon$.*

Definition 1.3.2. *The Inverse limit $\varprojlim(G_\lambda)_{\lambda \in \Lambda}$ is a subgroup of the cartesian product $\prod_{\lambda \in \Lambda} G_\lambda$ consisting of all elements (g_λ) in G such that $\pi_{\lambda\mu}(g_\lambda) = (g_\mu)$ whenever $\lambda \geq \mu$*

Now we develop a topological group structure on an inverse system of finite groups. If G_λ are finite groups, then by giving them discrete topology, and the $\prod G_\lambda$ the product topology, the inverse limit $\widetilde{G}$ becomes a topological group with the induced topology.

Going the other way, If Λ is a family of open normal subgroups of a given group G, by ordering Λ by reverse inclusion '$\succeq$' ($N \succeq M$ if $N \leq M$) and the maps being natural epimorphisms $\pi_{NM} : G/N \to G/M$ where $N \succeq M$, we get an inverse system $\{(G/N)_{N \in \Lambda}; \pi_{NM}\}$ for which $\widetilde{G}$ is the inverse limit. This actually forms the *profinite completion* of G.

$$\widetilde{G} = \varprojlim(G/N)_{N \lhd_o G}$$

Chapter 2

Profinite Groups

In this Chapter, we explain the basic theory of Profinite Groups, and later we discusss about specialised families of Profinite Groups such as a pro-p groups, finitely generated pro-p groups and procyclic groups. The contents of this chapter are referred from [DMSS] and certain proofs from [DS].

2.1 Profinite Groups

Definition 2.1.1. *A topological group G is profinite if it is Compact, Hausdorff and open subgroups of G form basis for the neighbourhoods of identity.*

Remark 2.1.1. *The second part of the definition essentially implies any open set of a Profinite group G that contains the identity contains an open subgroup.*

The following proposition will enlist more such consequences about profinite Groups:

Proposition 2.1.1. *Let G be a profinite group, then:*

1. *If $H \leq_o G$, then H is closed, has finite index in G, and contains an open normal subgroup.*
2. *If $H \leq_c G$, then H is open if and only if it has finite index.*
3. *All normal subgroups of G intersect in identity*
4. *Closed subgroups of a profinite group is profinite*
5. *If $N \lhd_c G$, G/N with the quotient topology is a profinite group.*

6. *(a) If $X \subseteq G$, then $\overline{X} = \cap_{N \lhd_o G} XN$*
   (b) If If $X \leq G$, then $\overline{X} = \cap\{K | X \leq K \leq_o G\}$

7. *If X and Y closed subsets of G, then so are $XY = \{xy | x \in X, y \in Y\}$ and $X^n = \{x^n | x \in X\}$*

8. *A sequence (g_i) in G converges if and only if it is cauchy.*

Let us define the notions of a convergent and cauchy sequences in a profinite group before going into the proof:

Definition 2.1.2. *A sequence (g_i) is said to be convergent (to 1) if for every $N \lhd_o G$ contains all but finitely many elements of the sequence.*

Definition 2.1.3. *A sequence (g_i) is said to be cauchy if for each $N \lhd_o G$, there exists n such that $(g_i)^{-1} g_j \in N$ for all $i \geq n, j \geq n$*

Proof. (1) Take $H \leq_o G$. Now $G = \cup_{g \in G} gH$ and all cosets gH are disjoint and open in G (Translations of H with each element from G).Now, $G \setminus H = \bigcap_{g \in G \setminus H} gH$ is a union of open sets and thus is open which implies H is closed. Given G is compact, there exists a finite subcover for the open cover $\{gH\}_{g \in G}$ of G , i.e, there exists $g_1 H, \dots, g_n H$ such that $\cap_{i=1}^{n} g_i H = G$ and thus finitely many cosets of H cover G, thus H has finite index in G. To show existence of normal subgroup, take $S = \cap_{x \in G} x H x^{-1} \geq H$. Then, $g S g^{-1} = \cap_{x \in G} (gx) H (gx)^{-1} = \cap_{y \in G} y H y^{-1} = S$ (where $y = gx$). Thus S is an open normal subgroup contained inside $H \leq_o G$.

(2) From(1) we know a closed subgroup which is open has finite index. Thus it remains to show that a closed subgroup having finite index is open, Let $H \leq_c G$ such that $|G : H| \leq \infty$. Let $C = \{gH | g \in G\}$ be the set of all left cosets of H in G. Thus $\cap_{C_i \in C \setminus H} C_i = G \setminus H$, a union of finitely many closed sets and hence closed. Hence H is open in G.

(3) Let $K = \bigcap_{N \lhd_o G} N$. Assume $K \neq \{1\}$ i.e, there exists $g \in K$ such that $g \neq 1$. Since G is Hausdorff, there exists an open neighbourhood U_1 of 1 such that $g \notin U_1$. G is profinite, hence open subgroups form neighbourhood basis around identity, thus there exists an open subgroup contained inside U_1 which contains an open normal subgroup N_1. But $g \notin U_1$ hence $g \notin N_1$ and thus $g \notin \cap_{N \lhd_o G} N$ which is a contradiction to our assumption, hence $\bigcap_{N \lhd_o G} N = 1$

(4) Take H closed subgroup of G, where G is profinite. H is compact and Hausdorff is clear as $H \leq G$.If N is any open set containing the identity in H there exists an open set M containing the identity in G, such that $M \cap H = N$. Thus if we have a $K \leq_o G$ such

that $K \subseteq M$, then $K \cap H \leq_o H$ and $K \cap H \subseteq N$. We can thus find open subgroups of H which are contained in an open set of H containing 1, and thus open subgroups of H form a neighbourhood basis for identity, and thus H is profinite.

(5)Let $\pi : G \to G/N$ be the quotient map. It is continuous, surjective. π is also an open map Take U open in G. Since π quotient map, $\pi(U)$ open in G/N if and only if $\pi^{-1}(\pi(U)) \subseteq_o G$. Also, $\pi^{-1}(\pi(U)) = UN = \cup_{n\in N} Un$ which is open if and only if U open in G. Thus $\pi(U)$ open in G/N if U open in G.

To show that G/N is compact , Let $\{H_i\}_{i\in I}$ be an open cover of G/N. Since π is an open mapping, H_i open in G/N implies $\pi^{-1}(H_i) \subseteq_o G$. Let $x \in G$, there exists $y \in G/N$ such that $\pi(x) = y$. Since $\{H_i\}$ covers G/N, we have $\pi(x) \in H_i$ for some i, implying $x \in \pi^{-1}(H_i)$ for some i, thus $\pi^{-1}(H_i)$ forms an open cover for G. Now G is compact, if we take any open cover $\{\pi^{-1}(H_i)\}_{i\in I}$ for G, there exists a finite subcover $\cup_{j=1}^{n} \pi_j^{-1}(H_i) = G$. So we have,$\pi(\cup_{j=1}^{n} \pi_j^{-1}(H_i)) = \cup_{j=1}^{n} \pi(\pi_j^{-1}(H_i)) = \cup_{j=1}^{n} (H_i N)_j = G/N$ which gives the finite subcover for G/N.

To show G/N is hausdorff, If $x \in G/N$ then as N is closed, $xN \subseteq_c G$. As π is an open mapping it follows that $\pi(G \backslash xN) = (G/xN) \setminus N \subseteq_o G/N$, implying $(G/N) \setminus \{x\} \subseteq_o G/N$, thus $\{x\} \subseteq_c G/N$, implying G/N is Hausdorff.

To show open subgroups of G/N form base for neighbourhoods of 1, take K which is an open neighbourhood of 1 in G/N. Then $\pi^{-1}(K) \subseteq_o G$. Thus there exists H open subgroup such that $h \subseteq \pi^{-1}(K)$. Thus $\pi(H) \leq_o G/M$ and $\pi(H) \subseteq \pi(\pi^{-1}(K)) = K$, thus for open neighbourhoods of 1, we can find open subgroups contained in them, which form the neighbourhood basis of identity for G/N.

(6) (a) Given $X \subseteq G$. For each $N \lhd_o G, [G : N] < \infty$ and thus there exists a finite $M_N \subseteq X$ such that $XN = \bigcup_{x\in X} xN = \bigcup_{x\in M_N} xN$. It follows that $X \subseteq XN \subseteq_c G$ for each $N \lhd_o G$. Thus $\overline{X} \subseteq \cap_{N \lhd_o G} XN$. Now let $y \in \bigcap_{N\lhd_o G} XN$. Then for each N there exists an $x_N \in X$ such that $y \in x_N N$ or equivalently $x_N \in yN$.As all open normal subgroups of G form basis for neighbourhoods for identity, for every neighbourhood U_y of y. There exists $N \lhd_o G$ such that $yN \subseteq U_y$. Thus $y \in \overline{X}$ and thus $\overline{X} = \cap_{N\lhd_o G} XN$.

(b) from (a), we know that XN open in G and $\overline{X}$ is intersection of open subgroups containing X in G thus $\bar{X} \supseteq \bigcap \{K \mid X \leq K \leq_o G\}$ and if $X \leq G$ then clearly $\bar{X} \subseteq \bigcap \{K \mid X \leq K \leq_o G\}$, giving both way inclusion.

(7) $f : G \times G \to G$ given by $(x, y) \mapsto xy$ is a continuous map and $G \times G$ is compact (via Tychonoff's theorem) and G is Hausdorff, thus the image $f(X \times Y) = \{xy | x \in X, y \in Y\} = XY$ is closed in G. Similarly, if $g_1 : G \to G \times G \ldots G$ given by $x \mapsto (x, \ldots, x)$ and

$g_2 : G \times G \dots G \to G$ and $(x, \dots, x) \mapsto x^n$ both continuous maps between Compact Hausdorff spaces. Hence $g_2 \circ g_1 : G \to G$ is a homeomorphism(composition of 2 homeomorphisms) and thus $\{x^n \mid x \in X\} \subseteq_c G$ whenever $X \subseteq_c G$.

(8) Every convergent sequence is cauchy. It remains to show that a cauchy sequence converges.If $\{g_i\}$ is a cauchy sequence in G, for all $N \triangleleft_o G$, there exists $n \in \mathbb{N}$ such that $g_i(g_j)^{-1} \in \mathbb{N}$. Let $C_n := \{g_i(g_j)^{-1} | i, j \geq n\}$. Enough to show that $C_n = \{1\}$. Let's prove by contradiction: If $\{g_i\}$ is a finite set and $C_n \neq 1$. This implies there exists an $a \neq 1$ such that $a \in C_n$. Thus $a \in N$ for all $N \triangleleft_o G$ and since all open normal subgroups intersect in the identity, $a = 1$. If $\{g_i\}$ is an infinite set, then it has a limit point as G is compact. Let $N \triangleleft_o G$, thus any neighbourhood gN of G must contain infinitely many g_i. Thus $g_i \in gN$ for all $i \geq n$. This implies that for $j \geq n$, $g_i \in g_j N = gN$, thus if M is any neighbourhood of $g \in G$, and let $N \triangleleft_o G$, such that $N \subseteq g^{-1}M$ then $g_i \in N \subset g^{-1}M$ for all $i \geq n$. Thus

□

Alternatively using the theory of Inverse limits developed in Section 1.3, we can derive at another definition of a Profinite group.

Theorem 2.1.2. *A profinite group G is topologically isomorphic to $\varprojlim(G/N)_{N \triangleleft_o G}$. Conversely, Inverse limit of an inverse system of finite groups is profinite.*

Proof. If G is profinite and $\widetilde{G} = \varprojlim(G/N)_{N \triangleleft_o G}$, then the map $\pi : G \longrightarrow \widetilde{G}$ given by $\pi(g) = (gN)_{N \triangleleft_o G}$ is a homomorphism. π is injective as since $\cap_{N \triangleleft_o G} N = 1$, we have

$$\begin{aligned}
&\pi\left(g_1\right) = \pi\left(g_2\right) \\
&\left(g_1 N\right)_{N \triangleleft_O G} = \left(g_2 N\right)_{N \triangleleft_O G} \\
&\left(g_1 N_1, g_1 N_2 \dots, \cdot\right) = \left(g_2 N_1, g_2 N_2, \dots\right) \\
&g_2^{-1} g_1 N \in N \text{ for all } N \Rightarrow g_2^{-l} g_1 \in \cap_{N \triangleleft_o G} N = 1 \\
&g_2^{-1} g_1 = 1 \text{ thus } g_1 = g_2
\end{aligned}$$

To show π is surjective: Let $(g_N N)_{N \in \aleph} \in \widetilde{G}$ be a finite collection of left cosets. Let $M = \cap_{N \in \aleph}(g_N N) \neq \phi$. Then, $M \triangleleft_o G$ and $g_M M \subseteq g_N N$ for all $N \in \aleph$. Thus $\cap_{N \in \aleph}(g_N N) \neq \phi$. Since G is compact, hence has finite intersection property, and thus $\cap_{N \triangleleft_o G}(g_N N) \neq \phi$. Thus there exists $g \in \cap_{N \triangleleft_o G}(g_N N)$. Thus π is surjective .

Given $U \subseteq_{open} \widetilde{G}$, $U \cong \prod_{N \in \aleph} U_N \times \prod_{N \notin \aleph} G/N$. $\pi^{-1}(U) = \cap_{N \in \aleph} \pi^{-1}(U_N)$ which is open, thus π is continuous.

Conversely If G_λ is a system of finite groups, then by giving them discrete topology, and the $\prod G_\lambda$ the product topology. It remains to show the inverse limit $\widetilde{G}$ is Profinite. Now

$\prod_{\lambda\in\Lambda} G_\lambda$ is compact (Tychonoff theorem), Hausdorff, and given any open neighbourhood of 1, for a finite subset $S \subseteq \Lambda$, we can create an open subgroup $G_S = \prod_{\lambda\notin S} G_\lambda \times \prod_{\lambda\in S}\{1\}$ which forms the neighbourhood basis for identity. Hence $\prod_{\lambda\in\Lambda} G_\lambda$ is Profinite.
It remains to show that $\widetilde{G} \subseteq \prod_{\lambda\in\Lambda} G_\lambda$ is a closed group of a profinite group, hence profinite: Let $g_\lambda \in \prod G_\lambda \setminus \widetilde{G}$. Then $\exists \mu \geq \nu$; $\mu, \nu \in \Lambda$ such that $\pi_{\mu\nu}(g_\mu) \neq g_\nu$ Now take open neighbourhood $U(\mu,\nu) = \prod_{\lambda=\mu,\nu} 1 \times \prod_{\lambda\neq\mu,\nu} G_\lambda$. Then $g_\lambda U(\mu,\nu)$ is an open neighbourhood of g_λ in $\widetilde{G}$, and $g_\lambda U(\mu,\nu) \cap \widetilde{G} = \phi$. This implies that there exists an open set in $\prod G_\lambda \setminus \widetilde{G}$, hence making it open, and complement $\widetilde{G}$ closed. Thus G is profinite. □

A few examples of Profinite Groups are discussed in detail below:

Example 1. *Any finite group is profinite and can be considered as the inverse limit of a trivial Inverse system.*

Example 2. *The ring of p- adic integers$\mathbb{Z}_p = \varprojlim_{i\in I} \mathbb{Z}/p^i\mathbb{Z}$ is a profinite Group.*

Example 3. *$GL_n(\mathbb{Z}_p)$ for $n \geq 1$ is a Profinite Group.*

Proof. $GL_n(\mathbb{Z}_p) = \{a \in M_n(\mathbb{Z}_p) \mid det(a) \not\equiv 0(\text{mod} p)\}$ and $M_n(\mathbb{Z}_p) \cong \mathbb{Z}_p^{n^2}$ is both Hausdorff and compact. Now, $p\mathbb{Z}_p$ is clopen(open and closed) in $\mathbb{Z}_p$ (they form the open balls $B(0, p^{-n})$ in $\mathbb{Z}_p$ which are defined using the p-adic metric). Thus, $pM_n(\mathbb{Z}_p)$ is also clopen in the product topology of $M_n(\mathbb{Z}_p)$. Now, if $b = a + pk \equiv a\,(\text{mod} p)$ where $k \in \mathbb{Z}_p$ and $a \in GL_n(\mathbb{Z}_p)$ then $det(b) \equiv 0\,(\text{mod} p)$ and thus $b \in GL_n(\mathbb{Z}_p)$. This implies that $GL_n(\mathbb{Z}_p)$ is a finite union of additive cosets of $pM_n(\mathbb{Z}_p)$. Therefore $GL_n(\mathbb{Z}_p)$ is clopen in $M_n(\mathbb{Z}_p)$. Now, $\Gamma_i := \{a \in GL_n(\mathbb{Z}_p) \mid a \equiv I_n\,(\text{mod} p^i)\}$ will form a base for the neighbourhoods of the identity in $GL_n(\mathbb{Z}_p)$ (are open subgroups of the form $\{I_n + p^i\mathbb{Z}_p\}$). Since open subgroups of $GL_n(\mathbb{Z}_p)$ form a basis for neighbourhoods of identity and is compact and hausdorff, it is profinite □

Proposition 2.1.3. *Let (X_i, ϕ_{ij}) be an inverse system of non-empty compact spaces over a directed set I. Then $\lim X_i$ is not empty.*

Proof. Let $Y_j = \{(x_i)_i \in \prod_i X_i \mid \phi_{jk}(x_j) = x_k\,,\ j \in I\ ; k \leq j\}$. Each Y_j is non empty. Now consider $\prod X_i - Y_j$, if $(x_i)_i \in \prod X_i - Y_j$ then there exists x_k such that $x_k \neq \phi_{jk}(x_j)$ for some $k \in I$. Since each X_i are compact and Hausdorff $\prod X_i$ is compact and Hausdorff. And since $x_k \neq \phi_{jk}(x_j)$ are distinct points, there exists neighbourhoods U and V of $\phi_{jk}(x_j)$ and x_k respectively such that $U \cap V = \emptyset$. As ϕ_{jk} is continuous there exists a neighbourhood U' of x_j in X_j such that $\phi_{jk}(U') \subseteq U$. Now consider $W = \prod W_i$ where $W_i = U'$ for $i = j, W_i = V$ for $i = k$ and $W_i = X_i$ otherwise. This makes W a open neighbourhood of $(x_i)_i$. Now if $(y_i)_i \in W$ then $\phi_{jk}(y_j) \neq y_k$, since $\phi_{jk}(y_j) \in U$ and $y_k \in V$, but $U \cap V = \emptyset$. Thus

$(y_i)_i \in \prod X_i - Y_j$, which give us that $W \subseteq \prod X_i - Y_j$ so that $\prod X_i - Y_j$ is open, hence Y_j is closed. Since I is a poset, we observe that if $j \leq j'$ then $Y_j' \subseteq Y_j$. This observation along with the fact that I is a directed poset gives that the collection $\{Y_i\}_{i \in I}$ has the finite intersection property. Now since $\prod X_i$ is compact, $\bigcap_{i \in I} Y_i \neq \emptyset$, but $\lim_{\leftarrow} X_i = \bigcap_{i \in I} Y_i$ and thus we are done. □

Finitely Generated Profinite Groups

Remark 2.1.2. *A group is said to be finitely generated if $\overline{\langle X \rangle} = G$ where X is a finite subset of G.*

Proposition 2.1.4. *Let G be a profinite group and let H be a closed subgroup:*

1. *Let $X \subseteq H$. Then X generates H topologically if and only if XN/N generates HN/N for every $N \lhd_0 G$.*

2. *Let d be a positive integer. If HN/N can be generated by d elements for every $N \lhd_o G$, then H can be generated topologically by a d -element subset.*

Proof. (1) From 1-1 correspondence between subgroups of G/N and subgroups of G that contain N, Since $\langle XN/N \rangle = HN/N$ for all $N \lhd_0 G$, we have $\langle XN \rangle = HN$. This implies $\cap_{N \lhd_o G} XN = \cap_{N \lhd_o G} HN$. Since $\overline{X} = \cap_{N \lhd_o G} XN$, we can conclude that $\overline{\langle X \rangle} = \overline{H} = H$.

(2) Let Y_N be the set of all d-tuples of elements of G/N which generate HN/N. Given $\pi_{MN} : G/M \to G/N$ is the natural projection for $M \leq N$ where $M, N \lhd_o G$ then $\pi_{MN}(Y_M) \subseteq Y_N$, thus $\{Y_N, \pi_{MN}\}$ forms an inverse system. From Proposition 2.1.3 we get that the inverse limit of this system is non empty as G/N is compact and non empty. Thus there exists $x_1, \ldots x_d \in G$,such that for each $N \lhd_o G$, $X_N = (x_1 N, \ldots, x_d N)$. Now since X_N, generates HN/N for every $N \lhd_o G$, using (1) we get that $\{x_1, \ldots, x_d\}$ generates H topologically. □

Proposition 2.1.5. *If G is a finitely generated profinite group and m is a positive integer, then G has only finitely many subgroups of a given index, and every open subgroup of G contains an open topologically characterestic subgroup(subgroup invariant under all continuous automorphisms of G).*

Proof. Let $G = \overline{\langle X \rangle}$ and $X = \{x_1, \ldots, x_d\}$. Let $H \leq_o G$ such that $|G : H| = m$. If $x \in G$, then $x \in H$ if and only if $xH = H$. Thus $H = stab_G(H) = \{g \in G | \phi(g)(H) = H\}$ where $\phi : G \to S_{|G/H|}$ (S_m is the permutation group on m-elements). So $H = \phi^{-1}(\{1\}_{G/H})$ and thus the number of possible H would be dependent on the number of choices of ϕ. Also

$\phi(X)$ is generated by $\{\phi(x_1), \dots, \phi(x_d)\}$. Each x_i can map to $m!$ possible elements, and for each ϕ we get H via the inverse image of a single point stabiliser in G/H. Thus maximum possible number of $H = m.m!^d$ which is finite.

If $H \leq_o G$, then $|G : \alpha(H)| = |G : H|$ for each automorphism α, and $\alpha(H)$ is open when α is continuous and thus the topologically characterestic subgroup $S = \cap\{\alpha(H) | \alpha \in Aut(G)\}$ is an intersection of finitely many open sets in G and thus is open in G. □

Proposition 2.1.6. *Every open subgroup of a finitely generated profinite group is finitely generated.*

Proof. Let $\overline{\langle X \rangle} = G$ and $|X| < \infty$. WLOG assume $X^{-1} = X$(else we can assume $X' = X \cup X^{-1}$). Let $H \leq_o G$ and T be the transversal of right cosets of H in G and $1 \in T$. Now, T is finite as $|G : H| < \infty$. For all $x \in X, t \in T$, there exists $s \in T$ such that $Htx = Hs$. Let $Y = \{txs^{-1} | t \in T, x \in X\}$. Let $M = \overline{\langle Y \rangle}$. We claim that $M = H$.

If $a \in M, t \in T, x \in X$ then $(at)x = a(txs^{-1})s$. Now as $(at)x \in MTX$ and $a(txs^{-1})s \in MT$ implying $X \subseteq MTX \subseteq MT$. From here using our assumption that $X = X^{-1}$ we can say $X^n \subseteq MT$ for all n. Hence, $\cap_{i=1}^{\infty} X^i = \langle X \rangle \subseteq MT$, M is closed and T is finite. So, we have that $MT = \cap_{i=1}^{n} MT_i$ is closed. Thus $\overline{\langle X \rangle} \subseteq MT$ and hence $MT = G$. It follows that $M \leq H$ as $Htx = Hs$ implies $txs^{-1} \in H$. Hence $Y \subseteq H$ and hence $\overline{\langle Y \rangle} \subseteq \overline{H} = H$. Using this, we finally get $H = G \cap H = MT \cap H = MT \cap MH = M(T \cap H) = M\{1\} = M$. □

Frattini Subgroups

We briefly discuss about Frattini Subgroups in the context of Profinite Groups

Definition 2.1.4. *The Frattini subgroup $\Phi(G)$ of a profinite group G is equal to the intersection of all maximal proper open subgroups of G.*

Remark 2.1.3. *Frattini Subgroup is a closed normal subgroup of G, as it is the intersection of arbitrarily many closed subgroups.*

Remark 2.1.4. *If $K \triangleleft_c G$ and $K \leq \Phi(G)$,then $\Phi(G/K) = \Phi(G)/K$. It follows from the $1-1$ correspondence between maximal open subgroups in G/K and the maximal open subgroups in G, as all of them contain K by definition.*

Proposition 2.1.7. *Let G be a profinite group, $X \subseteq G$, then the following statements are equivalent:*

1. *X generates G topologically*

2. $X \cup \Phi(G)$ *generates* G *topologically*

3. $X\Phi(G)/\Phi(G)$ *generates* $G/\Phi(G)$ *topologically.*

Proof. (1) $\implies$ (2) : Since $\Phi(G)$ is the set of all non generators of G, we have that if X generates G topologically then $X \cup \Phi(G)$ generates G topologically. Also, (2) $\implies$ (3) as $\overline{\langle X\rangle}\Phi(G)/\Phi(G) = G/\Phi(G)$. It remains to show that (3) $\implies$ (1). Let K be an open subgroup of G containing X. If $K \neq G$, then $K \leq M$ for some maximal open proper subgroup M of G. Thus : $\overline{\langle X\rangle}\Phi(G)/\Phi(G) \leq M/\Phi(G) \neq G/\Phi(G)$, which contradicts our assumption that $K \neq G$, and therefore $K = G$. Using $\overline{X} = \cap\{K | X \leq K \leq_o G\}$, we get that $\overline{X} = G$. Thus (3) $\implies$ (1) and proof is complete. □

2.2 Pro-p Groups

Definition 2.2.1. *A pro-p group is a profinite group in which every open normal subgroup has index equal to some power of p. Alternatively, they are also defined as the inverse limit of finite p-groups.*

Index in a Profinite Group

Definition 2.2.2. *Let* G *be a profinite group, and* H *be 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 *to be the supernatural number* $|G : H| = lcm\{|G/U : HU/U| \mid U \in \mathcal{U}\} = lcm\{|G/U : H/H \cap U| \mid U \in \mathcal{U}\}$

Proposition 2.2.1. *If* H *and* K *are closed subgroups of a profinite group* G*, such that* $K \subseteq H \subseteq G$*, then* $|G : K| = |G : H||H : K|$*.*

Proof. If $N \lhd_0 G$ then $|G : NK| = |G : NH||NH : NK| = |G : NH||H : (N \cap H)K|$ and $N \cap H \lhd_O H$. Therefore $|G : K|$ divides $|G : H||H : K|$. To show the converse, we use the fact that any open subgroup of $H \leq_c G$ is of the form $H \cap K$ where $K \leq_o G$. Let $N_1 \lhd_0 G$ and $N_2 \lhd_O H$. Using the above fact, find $M \lhd_0 G$ with $M \cap H \leqslant N_2$. Let $N = M \cap N_1$. Thus, $|G : N_1H||H : N_2K|$ divides $|G : NH||H : (N \cap H)K| = |G : NK|$ for every $N \lhd_o G$. Thus using the definition of the index $|G : H| = lcm\{|G : NH||N \lhd_o G\}$, we get that $|G : H||H : K|$ divides $|G : K|$, thus $|G : H||H : K| = |G : K|$ □

Proposition 2.2.2. *Let* G *be a pro-p Group. Then:*

1. *$H \leq_c G$ is also a pro-p group.*

2. *Let $K \lhd_c G$. Then G is a pro-p group if and only if both K and G/K are both pro-p groups.*

Proof. (1) Let $N \lhd_o G$. Then $|G : N|$ is a p- power. $|G : N| = |G : HN||HN : N| = |G : HN||H : H \cap N|$. Thus $|H : H \cap N|$ is a p-power. Since any open normal subgroup of H is of the form $H \cap N$ where $N \lhd_o G$, we conclude H is a pro-p group.
(2) If K and G/K are both pro-p groups, then $|G/K : H/K| = |G/H|$ where $H/K \lhd_o G/K$ is a p-power index. This gives us H open normal in G such that it's index is a p-power. Thus G is pro-p. Conversely if G is pro-p, we know K is pro-p. Take $H/K \lhd_o G/K$, then $|G/K : H/K| = |G : H|$ which gives a finite index. Also $H \lhd_c G$, thus $H \lhd_o G$ and $|G : H|$ is a p-power. It follows that G/K is a pro-p group. □

Now we look at a few non-trivial examples of pro-p groups:

Example 4. *Sylow p-subgroups of any arbitrary profinite group are the maximal pro-p subgroups, hence are pro-p.*

Example 5. *The ring of p-adic integers $\mathbb{Z}_p = \varprojlim_{i \in I} \mathbb{Z}/p^i\mathbb{Z}$ is a pro-p Group.*

Example 6. *$GL_n(\mathbb{Z}_p)$ for $n \geq 1$ and $SL_n(\mathbb{Z}_p)$ for $n \geq 1$ are not pro-p groups.*

Proof. The open normal subgroups of $GL_n(\mathbb{Z}_p)$ are of the form $\Gamma_i = \{g \in GL_n(\mathbb{Z}_p) \mid g \equiv 1_n \,(\text{mod} p^i)\}$. They also are the kernel of the natural projection $GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{Z}/p^i\mathbb{Z})$ (i.e, $GL_n(\mathbb{Z}_p)/\Gamma_i \cong GL_n(\mathbb{Z}/p^i\mathbb{Z})$). Since $GL_n(\mathbb{Z}/p^i\mathbb{Z})$ is not a p-group, hence Γ_i are open normal subgroups in $GL_n(\mathbb{Z}_p)$ that do not have a p-power index, and hence not a pro-p Group.

Similarly, $SL_n(\mathbb{Z}_p)$ is not also a pro-p group.

Example 7. *The Principal Congruence classes of $SL_n(\mathbb{Z}_p)$ given by $\Gamma_i = \{g \in SL_n(\mathbb{Z}_p) | g \equiv 1_n \mod p^i\}$ and $GL_n(\mathbb{Z}_p)$ are pro-p Groups.*

Proof. Γ_i are closed normal subgroups of $SL_n(\mathbb{Z}_p)$ and have finite index, as they are the kernel of the homomorphism between $SL_n(\mathbb{Z}_p)$ and $SL_n(\mathbb{Z}/p^i\mathbb{Z})$. Thus these Γ_i form open normal subgroups of $SL_n(\mathbb{Z}_p)$. Furthermore, each of Γ_i for $i \geq 2$ are open normal subgroups in Γ_1. We now claim that Γ_1/Γ_i is a p- group for all i. Any element of Γ_1/Γ_i is of the form $\{(1 + pa)\Gamma_i \mid a \in M_n(\mathbb{Z}_p), a \equiv 0 \,(\text{mod} p^i)\}$. From here we get:

$$(1 + pa)^{p^{i-1}} = 1 + (pa)^{p^{i-1}} + \cdots \equiv 1 + p^i a \left(\text{mod} p^i\right)$$

Thus $|\Gamma_1/\Gamma_i| = p^{ki}$ and thus we can get from here that given any open subgroup of Γ_1 has p-power index in Γ_1, and thus Γ_1 is pro-p. Similarly, we can say Γ_i for all $i \geq 2$ are also pro-p groups.

Frattini Subgroups in Pro-p groups

Frattini Subgroups are extensively used in understanding about pro-p groups, and in finitely generated pro-p groups:

Proposition 2.2.3. *If G is a pro-p group, then*

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

Where $[G,G]$ is the derived group of G and $G^p = \overline{\langle g^p | g \in G\rangle}$

Proof. If M is a maximal proper open subgroup of G, there exists $N \triangleleft_0 G$ with $N \leq M$, and we can see M/N is a maximal subgroup of the finite p-group G/N, and thus $|G/N : M/N| = |G : M| = p$, and $M \triangleleft_o G$.Thus $[G,G]$ and G^p both are contained in M. Thus $\Phi(G) = \bigcap M \geq G^p[G,G]$ and since $\Phi(G)$ is closed, we have $\Phi(G) \geq \overline{G^p[G,G]}$. To show the other way inclusion, let $Q = G/\overline{G^p[G,G]}$. From Proposition 2.2.2, Q is pro-p, and if $N \triangleleft_0 Q$ then Q/N is a finite elementary abelian p-group, Hence $\Phi(Q/N) = 1 = \Phi(Q)/N$. Thus $\Phi(Q) \leq \cap_{N \triangleleft_o Q} N = 1$. From this we get that $\Phi(G/\overline{G^p[G,G]}) = \Phi(G)/\overline{G^p[G,G]} = 1$ which gives the reverse inclusion and concludes the proof. □

Finitely Generated pro-p Groups

Proposition 2.2.4. *Let G be a pro-p group. Then G is finitely generated if and only if $\Phi(G)$ is open in G*

Proof. If $\Phi(G)$ is open then $G/\Phi(G)$ is finite. Hence we can find a finite subset X of G such that $G = \overline{\langle X\rangle}\Phi(G)$, and thus $G = \overline{\langle X\rangle}$. To show converse, suppose $G = \overline{\langle X\rangle}$ where $|X| = d < \infty$. Then If $\Phi(G) \leq$, $N \triangleleft_0 G$ then G/N is an elementary abelian p-group (from the previous proposition, we know $\Phi(G)$ kills all p-powers). Thus, $G/\Phi(G) \cong \mathbb{F}_p^d$ and $\Phi(G) \leq N$ gives us $|G : N| \leq p^d$, and that G/N can be generated by a d-element subset. Choose the smallest possible N such that $|G : N| \leq p^d$, let it be N'. Given $N' \leq N$ whenever $\Phi(G) \leq N \triangleleft_0 G$. Thus we get $\overline{\Phi(G)} = \Phi(G) = \bigcap\{N \mid \Phi(G) \leq N \triangleleft_0 G\} = N'$. Thus N' is open in G □

We define now an important family of topologically characteristic subgroups- the *lower p-series* :

Definition 2.2.3. *Let G be a pro-p group. The lower p- series is defined recursively as follows: Let $P_1(G) = G$*

$$P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}$$

Remark 2.2.1. *Note that $P_2(G) = \Phi(G)$*

Lower-p series of finitely generated pro-p groups are studied extensively, as the subgroups are all open and also form the basis for neighbourhoods of identity.

Proposition 2.2.5. *Let G be a pro-p group, then:*

- *$P_i(G/K) = P_i(G)K/K$ for all $K \triangleleft_c G$ and all i.*
- *$[P_i(G), P_j(G)] \leq P_{i+j}(G)$ for all i and j.*
- *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.*

Proof. (1) Let $K \triangleleft_c G$ and proceed by Induction. Base case follows as $P_1(G/K) = G/K = GK/K = P_i(G)K/K$. Let us assume the statement holds true upto i, i.e, $P_i(G/K) = P_i(G)K/K$, we will show it holds true for $i + 1$. Then :

$$\begin{aligned} P_{i+1}(G/K) &= \overline{P_i(G/K)^p[P_i(G/K), G/K]} \\ &= \overline{(P_i(G)K/K)^p[P_i(G/K), G/K]} \\ &= \overline{(P_i(G)K/K)^p[P_i(G), G]K/K} \\ &= \overline{(P_i(G))^[P_i(G), G]K/K} \\ &= \overline{P_{i+1}(G)K/K} \end{aligned}$$

Thus the result follows by Induction.

(2) WLOG proceed by Induction on j keeping i fixed. We know that $[P_i(G), G] \leq P_{i+1}(G)$ for all i. Let $n \geq 2$ and suppose inductively that $[P_i(G), P_{n-1}(G)] \leq P_{i+n-1}(G)$ for all i. Now we fix $m \geq 1$, and want to show that $[P_i(G), P_n(G)] \leq P_{i+n}(G)$. Since $P_{i+n}(G)$ is closed we can say $P_{i+n}(G) = \bigcap\{N \mid P_{i+n}(G) \leq N \triangleleft_0 G\}$. Thus it suffices to show that $[P_i(G), P_n(G)] \leq N$ whenever $P_{i+n}(G) \leq N$. Thus going modulo N, and assuming $P_{i+n}(G) = 1$, we get $P_{i+n-1}(G) \leq Z(G)$. If $g \in P_i(G)$ and $x \in P_{n-1}(G)$, then we get $[g, x^p] = [g, x]^p = 1$, and

thus $[P_i(G), P_{n-1}(G)^p] = 1$. Also using the 3-subgroup lemma, we get

$$\begin{aligned}[P_i(G), [P_{n-1}(G), G]] &\leq [G, [P_i(G), P_{n-1}(G)]]\,[P_{n-1}(G), [G, P_i(G) \\ &\leq [G, P_{i+n-1}(G)]\,[P_{n-1}(G), P_{i+1}(G)] \\ &\leq P_{i+n}(G) = 1\end{aligned}$$

Thus $[P_i(G), P_{n-1}(G)^p[P_{n-1}(G), G]] = [P_i(G), P_n(G)] = 1$, and the inequality follows .

(3) G is finitely generated. Certainly $P_1(G) = G$ is finitely generated and open in G. Let $i \geq 1$ and suppose inductively that $P_i(G)$ is finitely generated and open in G. We know from Proposition 2.2.4, that $\Phi\left(G_i\right)$ is open in G_i. Since $\Phi\left(P_i(G)\right) \leq_c P_{i+1}(G) \leq_c P_i(G)$. Thus $|P_i(G) : \Phi\left(P_i(G)\right)| = |P_i(G) : P_{i+1}(G)||P_{i+1}(G) : \Phi\left(P_i(G)\right)|$. Thus $P_{i+1}(G)$ is closed and has finite index in $P_i(G)$, and hence open. Thus, $\{P_i(G) \mid i \geq 1\}$ forms a neighbourhood basis for 1 of G, as if $N \lhd_0 G$ then G/N is a finite p-group and so $P_i(G/N) = 1$ for sufficiently large i, and thus every open normal subgroup of G contains $P_i(G)$ for some i. □

Finitely Generated Pro-p Groups are of great interest due to the following major result:

Proposition 2.2.6. *If G is a finitely generated pro-p group then every subgroup of finite index in G is open.*

This result requires the following lemmas

Lemma 2. *If G is a pro-p group and K is a subgroup of finite index in G then $|G : K|$ is a power of p.*

Proof. Suppose K is a subgroup of finite index, WLOG assume it is normal in G . Say $|G : K| = m = p^r q$ with $p \nmid q$, and Let $X = \{g^m \mid g \in G\}$. Then $X \subseteq K$ as K kills all elements of order m in G , and X is a closed subset of G (being the image of the continuous mapping $g \mapsto g^m$ of G into G). Now let $g \in G$ and $N \lhd_o G$. Then $g^{p^e} \in N$ for some $e \geq r$. By Euclid's Lemma, there exist integers a and b such that $am + bp^e = p^r$, and thus $g^{p^r} = (g^a)^m \left(g^{p^e}\right)^b \in XN$ Since r is independent of N and X is closed this shows that $g^{p^r} \in X \subseteq K$. Thus G/K is a p-group. □

Lemma 3. *Proposition If G is a finitely generated pro-p group then the derived group $[G, G]$ is closed in G.*

Proof. Let $G = \overline{\langle a_1, \ldots, a_d \rangle}$. Let $X = \{(g_1, a_i\} \ldots, \{g_d, a_d|\, g_1 \ldots, g_d \in G\}$. Now,$X$ is closed in G, as it is the image of $G \times \ldots \times$ under the continuous map $(g_1, \ldots, g_d) \mapsto \prod[g_i, a_i]$. Let $N \lhd_o G$, Thus G/N is nilpotent(as it is a finite p-group) and $G/N = (a_1 N, \ldots, a_d N)$. From

Proposition 1.1.7, we have $[G/N, G/N] = XN/N$, and so $[G,G]N = XN$, thus $[G,G] \subseteq \cap_{N \triangleleft_o G} XN = \overline{X} = X$, and we know $X \subseteq [G,G]$ as $[G,G]$ contains all possible commutator products, so $X = [G,G]$ and thus $[G,G]$ is closed in G □

Now we prove the main proposition:

Let G is a finitely generated pro- p group. Then the set $G^{\{p\}} = \{g^p \mid g \in G\}$ is compact, hence closed subgroup of G, as it is image of the continuous mapping $g \mapsto g^p$ of G into G).

$G/[G,G]$ is abelian, so if $a, b \in G$, then $(ab)^p = a^p b^p$ modulo $[G,G]$. Thus $G^p[G,G] = G^{\{p\}}[G,G]$, hence $G^p[G,G]$ is closed and $\Phi(G) = G^p[G,G]$. Since G finitely generated, and $\Phi(G)$ is open. Now K be a proper normal subgroup of finite index in G. Assume by Induction, Let K be open in M, whenever M is a finitely generated pro-p group with $K \leq M < G$. Take $M = G^p[G,G]K$, now M is open in G since G/K is finite p-group , and M has thus finite index in G, and hence is open, and therefore a finitely generated pro-p Group.Since K open in M, we get that K open in G. From here, using the above result, we conclude that any normal subgroup of finite index in G is open.

For any subgroup H of finite index in G, the kernel of the homomorphism $\phi : G \to S_{|G/H|}$ (given by the action $\phi(g) = g_i$, where g_i is a coset representative of G/H that contains g) is a normal subgroup of finite index of G that is contained within H. Thus every subgroup of finite index in G is open. □

This proposition has remarkable consequences:

Proposition 2.2.7. *If G is a finitely generated pro-p group. Then $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$ for each i.*

Proof. $P_i(G)$ is a finitely generated pro-p group, $\Phi\left(P_i(G)\right)$ is open in $P_i(G)$. Thus, we get $\Phi\left(P_i(G)\right) = \left[P_i(G), P_i(G)\right]\left(P_i(G)\right)^p \leq \left[P_i(G), G\right]\left(P_i(G)\right)^p$.

Proposition 2.2.8. *Any abstract homomorphism from a finitely generated pro-p group to a profinite group is continuous.*

Proof. Let $\theta : G \to H$ be the homomorphism, where G be a finitely generated pro-p group and H be profinite group. If $K \leq_o H$, and $N = ker\theta$, we get that $G/N \cong \theta(G)$, and $|G : \theta^{-1}(K)| = |G/N : \theta^{-1}(K)N/N| = |G/N : \theta^{-1}(K)/\theta^{-1}(K) \cap N| = |\theta(G) : \theta(\theta^{-1}(K))| \leq |H : K|$. Therefore $\theta^{-1}(K)$ is open in G. Since K is an element of the neighbourhood basis of 1 for H, θ is continuous. □

Remark 2.2.2. *The topology of a finitely generated pro-p group is determined by its Group structure. It follows from the above proposition by replacing H with G and having θ to be the identity map.*

2.3 Procyclic Groups

Definition 2.3.1. *Let G be a pro-p Group, $g \in G$ and $\lambda \in \mathbb{Z}_p$, then :*

$$g^{\lambda} = \lim_{n \to \infty} g^{\lambda_n}$$

where (λ_n) is a sequence of integers with $\lim_{n \to \infty} \lambda_n = \lambda$

The operation of p-adic exponentiation is well defined in G as a result of the following lemma:

Proposition 2.3.1. *Let G be a pro-p group. Let $g \in G$ and (a_i),(b_i) be two p-adically convergent sequences converging to same limit in $\mathbb{Z}_p$. Then the sequences (g^{a_i}) and (g^{b_i}) both converge in G, and their limits are equal.*

Proof. Let $N \triangleleft_o G$. Then $|G/N| = p^j$ for some j. Since (a_i),(b_i) are convergent p-adic sequences, For large enough i, k we have $a_i \equiv a_k \,(\text{mod} p^j)$, thus $a_i = a_k + p^j l$, so $g_i^a = g^{a_k}.(g^{p^j})^l$ thus $g^{a_i} \equiv g^{a_k} \,(\text{mod} N)$. Therefore (g^{a_i}) is a Cauchy sequence in G, and converges to some element $g_1 \in G$. Similarly, the sequence $\left(g^{b_i}\right)$ converges to some element $g_2 \in G$. This means for sufficiently large k, $b_k \equiv a_k \,(\text{mod} p^j)\,, g^{b_k} \equiv g_2 \,(\text{mod} N)$ and $g^{a_k} \equiv g_1 \,(\text{mod} N)$., so $g_1 = g^{b_k} n_1^{-1}$ and $g_2 = g^{b_k} n_2^{-1}$ and thus $g_1 g_2^{-1} = g^{b_k} n' (g^{b_k})^{-1} \equiv g^{b_k - b_k} \equiv 1 \,(\text{mod} N)$ and since N was an arbitrary normal subgroup, we get that $g_1 = g_2$. □

Proposition 2.3.2. *The map $\nu \mapsto g^{\nu}$ defines a continuous homomorphism of $f : \mathbb{Z}_p \to G$. The image of $\mathbb{Z}_p$ in the map is $\overline{\langle g \rangle}$*

Proof. it's a group homomorphism by definition, it is continuous from Proposition 2.2.5 , since $\mathbb{Z}_p$ is finitely generated pro-p group. Hence the image $f(\mathbb{Z}_p)$ is compact and closed subgroup of G. Also, $f(\mathbb{Z}_p)$ contains $\overline{\langle g \rangle}$ as $\mathbb{Z}$ is a dense subring of $\mathbb{Z}_p$. Conversely, the image consists of limit of sequences of elements of $\mathbb{Z}_p$, hence contained in $\overline{\langle g \rangle}$. Thus we have 2-way inclusion. □

Definition 2.3.2. *A group G is said to be procyclic if it is topologically isomorphic to the inverse limit of finite cyclic groups.*

An important result relating pro-p groups and procyclic groups is as follows:

Proposition 2.3.3. *A pro-p group G is procyclic if and only if it is either a finite cyclic group or is topologically isomorphic to $\mathbb{Z}_p$*

Proof. We first show that G is topologically generated by a one element subset. Suppose G has two distinct proper open maximal subgroups M, N. Take $M \cap N \geq \Phi(G) \geq G^p[G, G]$, so M and N are normal subgroups of index p in G , and $|G : M \cap N| = |G : M||M : M \cap N| = |G : M||MN : N| = |G : M||G : N| = p^2$ and $G/M \cap N$ is elementary abelian . This shows us that G is not cyclic, and thus a contradiction. Therefore, any non trivial G has a unique maximal proper open subgroup, thus has $\Phi(G)$ is open in G and $G/\Phi(G)$ is cyclic. Hence G can be generated topologically by a single element, Now suppose $f : \mathbb{Z}_p \to G$ given by $\nu \mapsto g^\nu$. Using the previous result and above observation, we get that $f(\mathbb{Z}_p) = G$ for some $g \in G$. Let $K = ker(f)$, and since f is continuous, surjective and $\mathbb{Z}_p/K$ and G both profinite groups, we get that G is topologically isomorphic to $\mathbb{Z}_p/K$. If K is trivial we get G topologically isomorphic to $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is procyclic, it has a unique maximal subgroup and hence any proper finite quotient of $\mathbb{Z}_p$ is cyclic. Since it is either isomorphic to a procyclic group or is a finite cyclic group, G is procyclic. □

Chapter 3

Uniformly Powerful pro-p Groups

In this chapter we study in detail about Powerful pro-p Groups, especially Uniform pro-p Groups. The contents of this chapter are largely referred from [DMSS]

3.1 Powerful pro-p Groups

Definition 3.1.1. *Let G be a pro-p group. G is said to be powerful if $G/\overline{G^p}$ is abelian when p is odd, or $G/\overline{G^4}$ is abelian when $p = 2$.*

Definition 3.1.2. *Let G be a pro-p group. If N_oG , then N is said to be powerfully embedded in G (N p.e G) if $[N, G] \leq \overline{N^p}$ when p is odd, or $[N, G] \leq \overline{N^4}$ when $p = 2$*

Remark 3.1.1. *From above definitions we can say G is powerful if G powerfully embeds in itself.*

Some examples of Powerful pro-p groups are as follows:

Example 8. $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ *is a powerful pro-p group*

Example 9. $\Gamma_i = \{g \in SL_n(\mathbb{Z}_p) | g \equiv 1_n \mod p^i\}$ *Infact* $\Gamma_i = \Gamma_{i-1}^p = \overline{\langle g^{p^{i-1}} | g \in \Gamma_1\rangle}$

Proof. To show that $[\Gamma_i, \Gamma_i] \leq \Gamma_i^p$. Let $g, h \in \Gamma_i$. Thus $g = 1 + p^i a$ and $H = 1 + p^i b$ where $a, b \in M_n(\mathbb{Z}_p)$ such that $a, b \cong 0 \mod p^{i-1}$. From calculating, we get $gh = hg \mod p^{i+1}$ and thus $[g, h] \in \Gamma_{i+1}$ for all $[\Gamma_i, \Gamma_i] \leq \Gamma_{i+1}$. Now we claim that for each $i, \Gamma_{i+1} = (\Gamma_i)^p = \{g^p \mid g \in \Gamma_i\}$. To show this claim we will show that this equation

$$1 + p^{n+1}a = (1 + p^n x)^p$$

has a solution for all $a \in M_n(\mathbb{Z}_p)$. We proceed by Induction taking equality modulo each p^i. Now, we have

$$1 + p^n a = 1 + p^{n+1}a + ... \equiv \left(1 + p^{n+1}a\right)\left(\text{mod} p^{n+2}\right)$$

which proves the base case. Let $x_1 = a$, so proceeding by induction assume there exists x_r commuting with a such that

$$(1 - p^n x_r)^p = 1 + p^{n+1}a + p^{n+r}c \equiv 1 + p^{n+1}a \left(\text{mod} p^{n+r}\right)$$

Where $c \in M_n(\mathbb{Z}_p)$. Also let's define: $x_{r+1} = x_r - p^r c$. Thus we have :

$$\begin{aligned}(1 + p^n x_{r+1})^p &= \left((1 + p^n x_r) - p^{n+r}c\right)^p \\ &\equiv (1 + p^n x_r)^p - p^{n+r+1}c \left(\text{mod} p^{n+r+1}\right) \\ &\equiv 1 + p^{n+1}a \left(\text{mod} p^{n+r+1}\right)\end{aligned}$$

Thus for all $a \in M_n(\mathbb{Z}_p)$ such that $a \equiv 0 \bmod p^{i-1}$, there exists $x_i \in M_n(\mathbb{Z}_p)$ such that $1 + p^{n+1}a = (1 + p^n x)^p$. Thus $\{x_i\}$ is a convergent sequence in $M_n(\mathbb{Z}_p)$, which converges to a limit x. Now $1 + p^i x$ is invertible and as $\det(1 + p^i x)^p = \det(1 + p^{i+1}a) = 1$, $1 + p^i x \in \Gamma_i$.
□

Finitely generated powerful pro-p Groups have certain interesting similar properties with abelian p-groups. The following results have direct relevance with the results proven in the powerful p-groups section discussed in the 1st chapter:

Proposition 3.1.1. *If G is a finitely generated powerful pro-p group, $G_i = P_i(G)$. Then:*

1. *Every element of G^p is a p^{th} power in G and $G^p = \Phi(G)$ is open in G(if p is odd), and $G^4 = \Phi(G)$ is open in G (if $p = 2$)*

2. *The map $x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} onto G_{i+k}/G_{i+k+1} for each i and k. $P_i(G_k) = G_{i+k-1}$*

3. *If $G = \overline{\langle a_1, ..., a_d\rangle}$ is a powerful p-group, then $G = \overline{\langle a_1\rangle}......\overline{\langle a_d\rangle}$ i,e.., G is the product of its procyclic subgroups $\overline{\langle a_i\rangle}$*

Proof. (1) If we take any $g = (g_N) \in \overline{G^p}$ then for each $N \lhd_o G, g_N \in (G/N)^p$ and hence as G/N is a powerful p-group g_N is a p^{th}-power in G/N . Let $X_N := \{g \in G/N \mid h^p = g_N\}$. With respect to the natural maps $\pi_{MN} : G/N \to G/M$ whenever $N \leq M$, we get $\pi_{MN}(X_N) \subseteq X_M$ Thus, $(X_N, \pi_{MN})_{N \lhd_o G}$ forms an inverse system of non empty sets. Thus, it has an non empty inverse limit. Hence there exists $h = (h_N) \in \lim_N X_N \subseteq G$. Now $h^p = g$ and so we have that $\overline{G^p} = G^p = \{g^p \mid g \in G\}$. It follows that $\Phi(G) = G^p \lhd_o G$.

(2) Suppose if G_i p.e. G, then $G_{i+1} = G_i^p$ we get that G_i/G_i^p is abelian and so G_i powerful and therefore $\Phi(G_i) = G_i^p = G_{i+1}$. Also, the homomorphism $x \mapsto x^p$ that maps $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is thus surjective. Composing these maps k times, we get that $x \mapsto x^{p^k}$ is a surjection from G_i/G_{i+1} to G_{i+k}/G_{i+k+1}.

(3)If $A = \overline{\langle a_1 \rangle} \dots \overline{\langle a_n \rangle}$, then A is closed. Also , we have $AN/N = G/N$ for every $N \lhd_o G$. And thus: $A = \bigcap_{N \lhd_o G} AN = \bigcap_{N \lhd_o G} GN = G$

3.2 Rank of a profinite Group

Definition 3.2.1. *The rank of a profinite group rk(G) is defined as follows:*

$$rk(G) = \sup\{d(H); H \leq_c G\}$$

Proposition 3.2.1. *Given G be a profinite group, then the following definitions of rank are equivalent:*

$$r_1 = \sup\{\mathrm{d}(H) \mid H \leq_{\mathrm{c}} G\}$$
$$r_2 = \sup\{\mathrm{d}(H) \mid H \leq_{\mathrm{C}} G \textit{ and } \mathrm{d}(H) < \infty\}$$
$$r_3 = \sup\{\mathrm{d}(H) \mid H \leq_0 G\}$$
$$r_4 = \sup\{rk(G/N) \mid N \lhd_0 G\}$$

Proof. $r_2 \leq r_1$ and $r_3 \leq r_1$, as r_1 contains a bigger family of subgroups. If $N \lhd_0 G$ and $M/N \leq G/N$, M/N is finite and hence $\mathrm{d}(M/N) \leq \mathrm{d}(M) \leq r_3$ and $r_4 \leq r_3$. Since M/N finite , there exists a finite subset X for each M, N such that $M = NX$. If $H = \overline{\langle X \rangle}$ then $M = NH$ and thus $\mathrm{d}(M/N) = \mathrm{d}(HN/N) \leq \mathrm{d}(H) \leq r_2$, thus $r_4 \leq r_2$. If $H \leq_c G$. Then $\mathrm{d}(HN/N) \leq \mathrm{d}(H)$ for every $N \lhd_0 G$ and hence $\mathrm{d}(H) = \sup\{\mathrm{d}(HN/N) \mid N \lhd_0 G\} \leq r_4$. Thus $r_1 \leq r_4$. Combining all inequalities we get the equality. □

Remark 3.2.1. *A profinite group has finite rank if $rk(G) < \infty$. By definition, profinite groups of finite rank are finitely generated.*

3.3 Uniform pro-p Groups

Let $G_i = P_i(G)$

Definition 3.3.1. *A pro-p group is said to be Unifomrly powerful or Uniform, if it is finitely generated , powerful and* $|G_i : G_{i+1}| = |G : G_2|$.

Remark 3.3.1. *This implies the map* $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ *is an isomorphism for all* $i \geq 1$

Example 10. $P_k(G)$ *is uniform pro-p group for all sufficiently large k, where G is a finitely generated powerful pro-p group. Let* $G_i = P_i(G)$*, and suppose* $|G_i : G_{i+1}| = p^{d_i}$*. The map* $x \mapsto x^{p^i}$ *is a surjection, and thus* $d_1 \geq d_2 \geq \ldots \geq d_i \geq d_{i+1} \geq \ldots$*, and there exists m such that* $d_k = d_m$ *for all* $k \geq m$*. We also know* $P_i(G_k) = G_{k+i-1}$ *for all i and k and is powerful. Thus we have* $P_k(G)$ *uniform.*

Remark 3.3.2. *Every pro-p group that is finitely generated has a characteristic open uniform subgroup. This is true, because if H is a characteristic open subgroup in a pro- p group G then* $P_k(H)$ *is also open and characteristic in G, and for sufficiently large k, we see* $P_k(H)$ *is a uniform subgroup from above proposition.*

Example 11. $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ *is a uniform pro-p group.*

Example 12. *If* $\Gamma_i := \{g \in GL_n(\mathbb{Z}_p) \,|g \equiv \mathrm{I}_d \,(\mathrm{mod} p^i)\}$*, then* Γ_1 *is a uniform pro-p group when p is an odd prime and* Γ_2 *when* $p = 2$*. Also* $P_i(G) = \Gamma_i(G)$ *when p is an odd prime and* $P_i(G) = \Gamma_{i+1}(G)$ *when* $p = 2$.

Proof. $P_1(G) = G = \Gamma_1$ where p is an odd prime. Going by Induction, suppose $r \geq 1$ and $P_r(G) = \Gamma_r$. Then $P_{r+1}(G) = P_r(G)^p[P_r(G), G] = \Gamma_r(G)^p[\Gamma_r(G), G] \leq \Gamma_{r+1}$ and also $\Gamma_{r+1} \leq \Gamma_r^p = P_r(G)^p$. Since Γ_{r+1} is a closed subgroup of G it follows that $P_{r+1}(G) = \Gamma_{r+1}$. Thus $P_i(G) = \Gamma_i(G)$ when p is an odd prime. Similarly, we can proceed for $p = 2$, using the fact that $[\Gamma_2, \Gamma_2] \leq \Gamma_4 \leq \Gamma_2^4$. Thus, Γ_1 is uniform as $|\Gamma_i : \Gamma_{i+1}| = p^{d^2}$ is constant for all $i \geq 1, G$.

Proposition 3.3.1. *Let G be a powerful finitely generated pro-p group, then the following statements are equivalent:*

1. *G is uniform*

2. $\mathrm{d}(P_i(G)) = \mathrm{d}(G)$ *for all* $i \geq 1$

3. $\mathrm{d}(H) = \mathrm{d}(G)$ *for every powerful open subgroup H of G.*

Proof. Let $G_i = P_i(G)$ for each i. Then $G_{i+1} = \Phi(G_i)$, thus $\mathrm{d}(G_i) = \mathrm{d}(G_i/G_{i+1}) \leq d(G) = d$ and $\mathrm{d}(G_i) \leq \mathrm{d}(H) \leq d(G) = d$. As H is powerful open subgroup, hence $H \geq G_i$ for some i. Since G is uniform if and only if $\mathrm{d}\left(G_i/G_{i+1}\right) = \mathrm{d}\left(G_1/G_2\right) = d$ for all i , we have $d(H) = d(G)$ and $d(P_i(G)) = d(G)$ and also $d(H) = d(P_i(G))$ for some i. □

Proposition 3.3.2. *A finitely generated powerful 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 first that G is not torsion-free. Then we claim that G contains an element x of order p. Suppose $x \in G$ has order $q \nmid p$. Then $x^q \in G_i$ for some i. Since $G_i^p = G_{i+1}$, it follows that $x^q \in G_i$ for all i, and thus $x = 1$. Let $x \in G_i \backslash G_{i+1}$. Then given $1 \neq xG_{i+1} \in G_i/G_{i+1}$ we have $1 = x^p G_{i+2} \in G_{i+1}/G_{i+2}$, so the map $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is not injective. Thus G is not uniform, which is a contradiction.

To show 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 $x_2 \in G_i \backslash G_{i+1}$ such that $x_2^p \in G_{i+2}$. Now let's assume, by induction that for $n \geq 2$ there exists $x_2, \ldots, x_n$ satisfying $x_j^p \in G_{i+j}$ and $x_j \equiv x_{j-1} \left(\bmod G_{i+j-2}\right)$ for $2 < j \leq n$. Then there exists $z \in G_{i+n-1}$ such that $z^p = x_n^p$. Let $x_{n+1} = z^{-1} x_n$. Then, $x_{n+1}^p \in G_{i+n+1}$: if p is odd , we have $[G_{i+n-1}, G, G] \leq G_{i+n+1}$ and $[G_{i+n-1}, G]^p \leq G_{i+n+1}$ and

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

From Remark 1.1.1, thus $x_2, \ldots, x_n, \ldots$ can be constructed recursively; it is a Cauchy sequence and therefore converges to an element $x \in G$, and then $x \not\equiv 1 \left(\bmod G_{i+1}\right)$ but $x^p \equiv 1 \left(\bmod G_{i+n+1}\right)$, thus $x^p = 1$, thus G is not torsion free and this concludes the proof. □

Definition 3.3.2. *Let G be a pro-p group of finite rank. The dimension of G is given by: $dim(G) = d(H)$ where H is any open uniform subgroup of G.*

Proposition 3.3.3. *Let G be a pro-p group of finite rank and N a closed normal subgroup of G. Then $dim(G) = dim(N) + dim(G/N)$*

Proof. Let's first show that if G and G/N are uniform, where $N \triangleleft_c G$ then N is uniform: First if $x \in G$, then $x^{p^n} \in N$, thus $x \in N$ as G/N is torsion-free and thus $N \cap G^p = \{g^p | g \in N\} = N^p$. Thus $N/N^p \subseteq N/N \cap G^p \subseteq G/G^p$ is abelian. N is finitely generated as G has finite rank. It is also torsion free as G is torsion free(G is uniform). Thus, N is uniform

Therefore $dim(G/N) = d(G/N)$, $dim(N) = d(N)$ and $dim(G) = d(G)$ and thus reduces to showing $d(G) = d(G/N) + d(N)$. This directly follows from taking the map $\pi : G \to G/N$ and using rank-nullity theorem.

Now H be an open uniform subgroup of G.Then, $H/H \cap N$ is powerful subgroup. We will later prove a result that the elements of finite order of finitely generated powerful pro-p group G form a characteristic subgroup H such that G/H is uniform(Proposition 3.4.3). Using this result, there exists $M/M \cap N$ which is normal subgroup of $H/H \cap N$ such that H/M is uniform.

Thus take $dim(N) = d(M)$, $dim(G) = d(H)$ and $dim(G/N) = d(H/M)$ and apply the earlier result . □

The following proposition implies that Uniform pro-p groups are basically an extension of pro-p-cyclic groups :

Proposition 3.3.4. *If G is a uniform pro-p group and $G = \overline{\langle a_1, ..., a_d \rangle}$ Then the mapping*

$$(\lambda_1, ..., \lambda_d) \mapsto a_1^{\lambda_1} ......a_d^{\lambda_d}$$

from $\mathbb{Z}_p^d$ onto G is a homeomorphism

Proof. $\mathbb{Z}_p$ and G are both compact, Hausdorff spaces and the map between them is continuous, as it is the composition of two continuous maps, it remains to show that the map $G \to \mathbb{Z}_p$ is a well defined bijection.

$G = \overline{\langle a_1 \rangle} \dots \overline{\langle a_d \rangle}$, therefore for any $g \in G, g = a_1^{\lambda_1} \dots a_d^{\lambda_d}$ for some $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$. So we consider the map $\psi : G \to \mathbb{Z}_p^d$ defined by $a_1^{\lambda_1} \dots a_d^{\lambda_d} \mapsto (\lambda_1, \dots, \lambda_d)$. We show that ψ is a well defined bijection and that its inverse ψ^{-1} is the homeomorphism we require.
$|G/G_{k+1}| = |G : G_{k+1}| = p^{kd}$. From Proposition 1.1.9, we get $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \dots \langle a_d G_{k+1} \rangle$. Since $G_{k+1} = \left\{ g^{p^k} \mid g \in G \right\}$ for each i, $|\langle a_i G_{k+1} \rangle| \leq p^k$, but by the above this must be an equality. Hence each $g \in G/G_k$ is equal to a product of the form $a_1^{\mu_1} \dots a_d^{\mu_d} G_{k+1}$ where $\mu_1, \dots, \mu_d \in \left\{0, 1, \dots, p^k - 1\right\}$ are uniquely determined by g. Hence for any $g \in G, \psi(g)$ is determined uniquely modulo p^k for any k, and hence ψ is a well defined bijection. $\psi^{-1} : \mathbb{Z}_p^d \to G$ defined by $(\lambda_1, \dots, \lambda_d) \mapsto a_1^{\lambda_1} \dots a_d^{\lambda_d}$ is the inverse bijection. However, ψ^{-1} is merely the composition of the two maps $\alpha : \mathbb{Z}_p^d \to G \times G \times \dots \times G$ given by $(\lambda_1, \dots, \lambda_d) \mapsto (a_1^{\lambda_1}, \dots, a_d^{\lambda_d})$ and $\beta : G \times G \times \dots \times G \to G$ given by $(a_1^{\lambda_1}, \dots, a_d^{\lambda_d}) \mapsto a_1^{\lambda_1} \dots a_d^{\lambda_d}$. Thus it follows that ψ is homeomorphism. □

Now we detail the process of creating an additive structure for Uniform pro-p Groups and discuss it's interesting properties:

Additive Structure

Let G be uniform pro-p group. Let $G_i = P_i(G)$

Proposition 3.3.5. *Let $n \in \mathbb{N}$. The mapping $x \mapsto x^{p^n}$ is a homeomorphism from G onto G_{n+1}. For each k and m, it restricts to a bijection $G_k \to G_{k+n}$ and induces a bijection $G_k/G_{k+m} \to G_{n+k}/G_{n+k+m}$.*

Proof. Let $f(x) = x^{p^n}$.We know that $f\left(G_k\right) = \{x^{p^n} \mid x \in G_k\} = G_{n+k}$ which implies that $f\left(G_{k+m}\right) = G_{n+k+m}$ .If $x \equiv y \, (\mathrm{mod} G_{k+m})$ then $x = yg_{k+m}$, thus $x^{p^n} = y^{p^n} g_{k+m}^{p^n}$ and so $f(x) \equiv f(y) \, (\mathrm{mod} G_{n+k+m})$. Thus f induces a surjection from G_k/G_{k+m} onto G_{n+k}/G_{n+k+m}. Since G is uniform, $|G_k/G_{k+m}| = |G_{n+k}/G_{n+k+m}|$ hence f is a bijection. If $x, y \in G_k$ and $f(x) = f(y)$ then $f(xy^{-1}) = 1$ and thus $xy^{-1} \equiv 1 \bmod G_{k+m}$ implying $xy^{-1} \equiv (\mathrm{mod} G_{k,+m})$ for all m. Since $\bigcap_m G_{k+m} = 1$, $xy^{-1} \in \bigcap_m G_{k+m} = 1$ implying $x = y$ and thus f is injective. Finally f is continuous: as G_k is a compact Hausdorff space for all k. The restriction, $f|_{G_k}$ is thus a homeomorphism from G_k to G_{k+n}. If $k = 1$, we get $f|_G = f$ which is a homeomorphism from G onto G_{n+1} □

Remark 3.3.3. *This lemma gives us that every $x \in G_{n+1}$ has a unique p^{th} root in G, say $x^{p^{-n}}$. Using this bijection and the uniqueness of p^n-th roots, we define another structure on the group G:*

Definition 3.3.3. *For $x, y \in G$, we define the additive structure $+$ on a Uniform group G as follows :*

$$x + y := \lim_{n \to \infty} x +_n y$$

where $x +_n y := (x^{p^n} y^{p^n})^{p^{-n}}$

This definition holds as a result of the following lemma which shows that $(x, y)_n$ is a cauchy sequence for $x, y \in G$ and n:

Lemma 4. *If $n > 1, x, y \in G$, and $u, v \in G_n$ then group $(G, +_n)$. Then :*

- $xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \, (\mathrm{mod} G_n)$
- $x +_m y \equiv x +_n y \, (\mathrm{mod} G_{n+1})$ *for all $m > n$*

Proof. (1)Let $P_i(G) = G_i$. $[G_n, G_n] \leq G_{2n}$. This implies that

$$\begin{aligned} x^{p^n} y^{p^n} &\equiv \left(x^{p^{n-1}} y^{p^{n-1}}\right)^p [x^{p^n}, y^{p^n}]^{p(p-1)/2} \, (\mathrm{mod} G_{2n}) \\ &\equiv \left(x^{p^{n-1}} y^{p^{n-1}}\right)^p (\mathrm{mod} G_{2n}) \\ &= (x +_{n-1} y)^{p^n} \end{aligned}$$

Thus,

$$x +_n y = \left(x^{p^n} y^{p^n}\right)^{p^{-n}} \equiv x +_{n-1} y \, (\text{mod} G_n)$$

And since $(xu)^{p^n} \equiv x^{p^n} \, (\text{mod} G_{2n})$ and $(yv)^{p^n} \equiv y^{p^n} \, (\text{mod} G_{2n})$

$$xu +_n yv = ((xu)^{p^n} yv^{p^n})^{p^{-n}} \equiv x +_n y \, (\text{mod} G_n)$$

Thus we get that $xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \, (\text{mod} G_n)$

(2). From (1) we have already proved the case where $n = 1$ and $m > n$. Let

$$x +_m y \equiv x +_k y \, (\text{mod} G_{k+1})$$

Where $m - k \geq 2$. Then:

$$\begin{aligned} x +_{m+1} y &= x +_m y \, (\text{mod} G_{m+1}) \\ &= x +_k y \, (\text{mod} G_{k+1}) \end{aligned}$$

by using Induction hypothesis and that $G_{m+1} \subseteq G_k$. This finishes the proof. □

Remark 3.3.4. *If we have $x, y \in G$ and $u, v \in G_n$,then $x + y \equiv x +_n y \, (\text{mod} G_{n+1})$ and $xu + yv \equiv x + y \, (\text{mod} G_n)$*

Proposition 3.3.6. *The set G with the operation $+$ in an abelian group, with identity element 1 and inversion given by $x \mapsto x^{-1}$*

Proof. For each n, $x +_n 1 = (x^{p^n})^{p^{-n}} = x$ and similarly $x +_n x^{-1} = 1$. Hence, by taking limits we get $x + 1 = x$ and $x + x^{-1} = 1$. To verify the associative law, let $x, y, z \in G$ and let $n > 1$. We know $x + y = x +_n y (\text{mod} G_{n+1})$, thus

$$\begin{aligned} (x + y) + z &\equiv (x +_n y) + z \, (\text{mod} G_{n+1}) \\ &\equiv (x +_n y) +_n z \, (\text{mod} G_{n+1}) \end{aligned}$$

Similarly, $x + (y + z) \equiv x +_n (y +_n z)$ (mod G_{n+1}). Since the operation $+_n$ is associative, it follows that

$$(x + y) + z \equiv x + (y + z) \, (\text{mod} G_{n+1})$$

The choice of n is arbitrary hence $+$ is associative.

We know that $\left[x^{p^n}, y^{p^n}\right] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$. Thus $x^{p^n} y^{p^n} \equiv (xy)^{p^n} \, (\text{mod} G_{2n+2}) \equiv y^{p^n} x^{p^n} \, (\text{mod} G_{2n+2})$. Taking p^n-th roots , we get that $x +_n y \equiv y +_n x \, (\text{mod} G_{n+2})$. Thus

$x + y \equiv y + x\,(\mathrm{mod} G_{n+1})$, as this holds for arbitrary n the result follows.

Notation 4. *'Additive' notation for the group operations in $(G, +)$ is as follows :*
$0_+ = 1$, $(-x)_+ = x^{-1}$, $(x - y)_+ = x + (-y)_+ = x + y^{-1}$, $(mx)_+ = x + \ldots + x$ (m times) when m is positive and $(-mx)_+ = |m|x^{-1}$.

Lemma 5. *Let $x, y \in G$. Then:*

1. *If $xy = yx$ then $x + y = xy$.*
2. *For each integer m, $mx = x^m$.*
3. *For each $n \geq 1$, $p^{n-1}G = G_n$*
4. *If $x, y \in G_n$ then $x + y \equiv xy\,(\mathrm{mod} G_{n+1})$.*

Proof. (1) $x +_n y = (x^{p^n} y^{p^n})^{p(-n)} = ((xy)^{p^n})^{p^{-n}} = xy$ for any n thus $x + y = xy$.

(2) Take $m > 0$, then $x +_n x = x^2$ for all n, thus $x + x = x^2$. If $(m-1)x = x^{m-1}$, then from (1) , we get $mx = (m-1)x + x = x^{m-1}x = x^m$. For negative m, we get the result using the fact that $-x = x^{-1}$.

(3) Using the proposition 3.3.5 , we get that for all $x \in G$, we get that $p^{n-1}x = x^{p^{n-1}} \in G_n$, and since p^n-th roots are unique, we get the reverse inclusion.

(4) Using proposition 3.3.5 , For x, y in G_n, we have

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} [y, x]^{p(p-1)/2} \equiv x^{p^n} y^{p^n}\,(\mathrm{mod} G_{2n+1})$$

Using p^n-th roots, we get

$$xy = x +_n y(\mathrm{mod} G_{n+1})$$

and thus $x + y = xy(\mathrm{mod} G_{n+1})$ □

Proposition 3.3.7. *Given G a uniform pro-p group with the additive structure +:*

1. *For each n, G_n is an additive subgroup of G*
2. *The additive cosets of G_n in G are the same as the multiplicative cosets of G_n in G.*
3. *The identity map $G_n/G_{n+1} \to G_n/G_{n+1}$ is an isomorphism of the additive group G_n/G_{n+1} onto the multiplicative group G_n/G_{n+1}, and the index of G_n in the additive group $(G, +)$ is equal to $|G : G_n|$*

Proof. (1) $G_n = p^{n-1}G$ is an additive subgroup of $(G, +)$.

(2) let $x \in G, y \in G_n$. Then from Lemma 4, we have

$$x + y = x + 1 \cdot y \equiv x + 1 = x \,(\mathrm{mod} G_n)$$

$$xy - x = xy + (-x) \equiv x + (-x) = 0 \,(\mathrm{mod} G_n)\,,$$

Thus $xy - x \in G_n$ and $xy \in x + G_n$. Thus $xG_n \subseteq x + G_n$ This shows that the additive cosets modulo G_n are the same as the multiplicative cosets.

(3): From (2), we get G/G_n is the the same quotient set whether we consider the additive group $(G, +)$ or the multiplicative group G. Hence the index of G_n is same across operations and the identity map is a bijection between the additive group G_n/G_{n+1} and the multiplicative group G_n/G_{n+1}, hence an isomorphism. □

Proposition 3.3.8. *Given the original topology of $G, (G, +)$ is a uniform pro-p group of dimension $d = \mathrm{d}(G)$. Moreover any set of topological generators for G is a set of topological generators for $(G, +)$.*

Proof. G is a Topological group as it is Compact Hausdorff space with two continuous maps $x \mapsto x^{-1}$ and $(x, y) \mapsto x + y$ (from lemma 4). Since G_n is a subgroup of p-power index in $(G, +)$, the family $\{G_n\}_{n \in N}$ forms a base for neighbourhoods of $0_{(G,+)} = 1$, implying that $(G, +)$ is a pro-p group. It is also powerful as it is abelian. From Proposition 3.3.7, we get that $|G_n : G_{n+1}| = p^d$ for all n, and thus $(G, +)$ is a uniform pro-p group of dimension d.

If X is a topological generating set for G, then $G/G_2 = \langle X \rangle G_2/G_2$ (as multiplicative groups). From 3.3.7, we get that the additive group G/G_2 is identical to the multiplicative group, so we have $(G, +)/G_2 = \langle X \rangle_+ + G_2/G_2$, where $\langle X \rangle +$ denotes the additive subgroup generated by X. Thus $(G, +) = \langle X \rangle_+ + G_2$. Since $G_2 = pG$ is the Frattini subgroup of $(G, +)$, we get that $(G, +) = \langle X \rangle_+$ and thus X is a topological generating set for $(G, +)$. □

Proposition 3.3.9. *Let G be a uniform pro-p group of dimension d, and let $\{a_1, \ldots, a_d\}$ be a topological generating set for G. Then, with the operations defined above, $(G, +)$ is a free $\mathbb{Z}_p$-module on the basis $\{a_1, \ldots, a_d\}$*

Proof. The set $\{a_1, \ldots, a_d\}$ generates the uniform pro- p group $(G, +)$ topologically, and $\mathrm{d}(G, +) = d$. : Using the Proposition 3.3.4, we get the map between $(G, +)$ and $\mathbb{Z}_p^d$ given by the map :

$$(\lambda_1, \ldots, \lambda_d) \mapsto (\lambda_1 a_1, \ldots, \lambda_d a_d)$$

is a homeomorphism. This shows that each element of $(G, +)$ has a unique expression of the form

$$a = \lambda_1 a_1 + \cdots + \lambda_d a_d$$

with $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$ (for $x \in G$ and $\lambda \in \mathbb{Z}_p$, we have $x^\lambda = \lambda x$. This implies that the set $\{a_1, \ldots, a_d\}$ forms the basis for $(G, +)$ and thus $(G, +)$ is a free $\mathbb{Z}_p$-module. □

The additive structure on a uniform pro-p group G thus gives rise to a free $\mathbb{Z}_p$-module. Following propositions are interesting results that have quite a few applications.

Proposition 3.3.10. *Let G be a uniform pro-p group of dimension n. Then the action of $Aut(G)$ on G is $\mathbb{Z}_p$-linear with respect to the $\mathbb{Z}_p$-module structure on $(G, +)$.*

Proof. Let $\alpha \in Aut(G)$. The map α is continuous(it is a map between 2 finitely generated pro-p groups). Thus For each n, since p^n-th roots are unique, Given $x, y \in G$,

$$\alpha(x +_n y) = \alpha((x^{p^n} y^{p^n})^{p-n}) = (\alpha(x^{p^n} y^{p^n})^{p-n}) = (\alpha(x^{p^n})\alpha(y^{p^n}))^{p^{-n}} = \alpha(x) +_n \alpha(y)$$

. It follows that $\alpha(x + y) = \alpha(x) + \alpha(y)$.

Similarly for $\lambda \in \mathbb{Z}_p$ we would get $\alpha(\lambda x) = \lambda \alpha(x)$. (Use Lemma 5). And thus we get that the action of $Aut(G)$ is $\mathbb{Z}_p$-linear.

Remark 3.3.5. *Hence $Aut(G)$ may be identified with a subgroup of* $\mathrm{GL}_n(\mathrm{Z}_p)$,

Proposition 3.3.11. *Let G be a pro-p group of finite rank and dimension d. Then there is an exact sequence*

$$1 \to \mathbb{Z}_p^e \to G \to GL_d(\mathbb{Z}_p) \times F$$

for some $e \leq d$ and some finite p-group F.

Proof. Let G have a uniform open normal subgroup H and $A = \mathrm{Z}(H)$. Then A is closed in H, is torsion-free(as H is torsion free), and is abelian pro-p group with $rk(A) \leq rk(H) = d$.

It follows that $A \cong \mathbb{Z}_p^e$ for some $e \leq d$. Now for each $g \in G$. Let f denote the automorphism of H induced by conjugation with g, i.e, $f(h) = ghg^{-1}$. We have a homomorphism $\theta : G \to Aut(H) \times G/H$ given by

$$\theta(g) = (f, gH)$$

. Clearly $ker(\theta) = \{g \in G | \ \theta(g) = (id_H, H)\} = A$ as $ghg^{-1} = h$ implies $g \in Z(H)$ and $gH = H$ if and only if $g \in H$. Thus we have an exact sequence

$$1 \to \mathbb{Z}_p^e \xrightarrow{\iota} G \xrightarrow{\theta} Aut(G/H) \times G/H$$

. Using the previous proposition(3.3.10), we can extend the current exact sequence to get the desired exact sequence.

$$1 \to \mathbb{Z}_p^e \xrightarrow{\iota} G \xrightarrow{\theta} GL_d\left(\mathbb{Z}_p\right) \times F$$

□

3.3.1 Lie Algebras

Since all free-$\mathbb{Z}_p$ of a given rank are isomorphic, a lot of information on the structure of a uniform group G is left unknown by just giving the addition operation. In this section we define yet another operation- the bracket operation that will help us find more information. Let G be a uniform pro-p group of rank d, and let $G_i = P_i(G)$ for each i.

Definition 3.3.4. *The bracket operation* $(,)$ *for a uniform pro-p group* G *For* $x, y \in G$ *and* $n \in \mathbb{N}$*, is defined as*

$$(x, y) = \lim_{n\to\infty} (x, y)_n$$

where $(x, y)_n = \left[x^{p^n}, y^{p^n}\right]^{p^{-2n}}$

The above definition holds as a result of the following lemma which shows that $(x, y)_n$ is a cauchy sequence.

Lemma 6. *If* $n > 1, x, y \in G$ *and* $a, b \in G_n$*, then*

$$(xa, yb)_n \equiv (x, y)_n \equiv (x, y)_{n-1} \left(\mathrm{mod} G_{n+1}\right)$$

and for all $m > n$

$$(x, y)_m \equiv (x, y)_n \left(\mathrm{mod} G_{n+2}\right)$$

Proof. $[G_{2n}, G_{n+1}] \leq G_{3n+1}$, and using Lemma 4, we get:

$$(xa, yb)_n \equiv (x, y)_n \left(\mathrm{mod} G_{n+1}\right).$$

Now if $m \in G_i$ and $k \in G_j$, then from Remark 1.1.1, and the fact that $[G_i, G_j] \leq G_{i+j}$, we have

$$[m^p, k] \equiv [m, k]^p \left(\mathrm{mod} G_{2i+j}\right)$$

and $[m, k^p] \equiv [m, k]^p \, (\mathrm{mod} G_{i+2j})$. Taking $m = x^{p^n}$ and $k = y^{p^{n-1}}$ this gives

$$\left[x^{p^n}, y^{p^n}\right] \equiv \left[x^{p^n}, y^{p^{n-1}}\right]^p (\mathrm{mod} G_{3n+1})$$

Taking $a = x^{p^{n-1}}$ and $b = y^{p^{n-1}}$ gives

$$\left[x^{p^n}, y^{p^{n-1}}\right] \equiv \left[x^{p^{n-1}}, y^{p^{n-1}}\right]^p (\mathrm{mod} G_{3n})$$

Thus we have

$$\begin{aligned}\left[x^{p^n}, y^{p^n}\right] &\equiv \left[x^{p^{n-1}}, y^{p^{n-1}}\right]^p (\mathrm{mod} G_{3n+1}) \\ &\equiv \left[x^{p^{n-1}}, y^{p^{n-1}}\right]^{p^2} (\mathrm{mod} G_{3n+1}) \\ &= (x, y)_{n-1}^{p^{2n}}.\end{aligned}$$

Extracting p^{2n}-th roots

$$(x, y)_n \equiv (x, y)_{n-1} \, (\mathrm{mod} G_{n+1}) \, .$$

The bracket operation combined with the additive structure gives rise to a $\mathbb{Z}_p$-Lie Algebra structure $(G, +, (,))$

Proposition 3.3.12. *With the operation $(,)$, the $\mathbb{Z}_p$ module $(G, +)$ becomes a Lie algebra over $\mathbb{Z}_p$:*

Proof. The proof is quite elaborate. An outline of this proof is discussed in the exercises of Chapter 4 of [DMSS].

Remark 3.3.6. *Given $(G, +, (,))$ a uniform pro-p group with it's associated Lie algebra and . For x and $y \in G$, we have $\log(xy) = \Phi(\log x, \log y)$ where $\Phi(U, V)$ is the Campbell-Hausdorff formula. Under certain conditions, xy can be recovered from the Lie Algebra structure of $(G, +)$, and thus captures more structural information about the Group.*

Proposition 3.3.13. *Let H be a uniform closed subgroup of G, and let $N \triangleleft_c G$ be such that G/N is uniform. Then:*

1. *the inclusion map $H \to G$ is a monomorphism of Lie algebras $(H, +, (),) \to (G, +, ())$. Moreover, H is a sub-algebra of the Lie algebra $(G, +, ())$*

2. *N is uniform*

3. *N is an ideal in the $\mathbb{Z}_p$ -Lie algebra $(G, +, (),)$; and the additive cosets of N in G are the same as the multiplicative cosets, so $(G/N, +, (,)) = (G, +, ())/(N, +, (,))$.*

The natural epimorphism $\pi : G \to G/N$ is an epimorphism of $\mathbb{Z}_p$-Lie algebras from $(G, +, (,))$ onto $(G/N, +, (,))$.

Proof. (1) As H is a subgroup, it gets the subspace topology from G. Hence H is a Lie Subalgebra of the Lie algebra $(G, +, ())$.

(2) Have already proved this result in Proposition 3.3.3 .

(3) Now let $x, y \in G$ and put $z_n = x +_n y$. Then $\pi(z_n)^{p^n} = \pi(x^{p^n})\pi(y^{p^n})$, so in G/N we have $\pi(x) +_n \pi(y) = \pi(z_n)$. It follows by continuity that $\pi(x) + \pi(y) = \lim_{n\to\infty} \pi(z_n)^{=} \pi(\lim_{n\to\infty} z_n) = \pi(x + y)$. Similarly π respects bracket operation and the operation of $\mathbb{Z}_p$. Thus π is a Lie algebra homomorphism . Since N is the kernel of π it follows that N is an ideal in $(G, +, ())$. Finally, for $x, y \in G$ we have

$$x + N = y + N \Leftrightarrow x - y \in N \Leftrightarrow \pi(x - y) = 0 \Leftrightarrow \pi(x) = \pi(y) \Leftrightarrow xN = yN,$$

which shows that $(G, +)/(N, +) = G/N$. This concludes the proof. □

3.4 Automorphism Groups

In this section, the description of the topology of an automorphism group of a profinite group, specifically in the case of a finitely generated profinite/pro-p group. We then use the results to get some important results pertaining to the structure of a powerful pro-p group.

For a profinite group G, $Aut(G)$ denotes the group of all topological automorphisms of G. The group $Aut(G)$ has a natural topology, the 'congruence topology': a base for the neighbourhoods of 1 is given by the subgroups

$$\Gamma(N) = \{\gamma \in Aut(G) \mid [G, \gamma] \subseteq N\}$$

as N runs over the open normal subgroups of G

Notation 5. $[G, \gamma] := \{[g, \gamma] | g \in G, \gamma \in Aut(G)\}$ *, where* $[g, \gamma] = \{g^{-1}\gamma(g) | g \in G\}$ *for all* $\gamma \in Aut(G)$

Proposition 3.4.1. *The Automorphism Group of a finitely generated profinite group is a profinite group.*

Proof. If $K \triangleleft G$ is invariant under an automorphism ψ of G , i.e,$\psi(K) = K$. Then ψ induces an automorphism $\widetilde{\psi} : G/K \to G/K$ given by the map $\widetilde{\psi}(gK) := \psi(g)K$. If K is a characterestic subgroup then $\psi(K) = K$ for all $\psi \in Aut(G)$, then it induces a map from $\delta : Aut(G) \to Aut(G/K)$ given by $\delta(\psi) = \widetilde{\psi}$.

Since G is a finitely generated Profinite Group, every open subgroup contains a topologically open characterstic subgroup. Thus it implies that G has a neighbourhood basis of identity consisting of characterestic subgroups.

Given the basis of neighbourhoods of 1 for $Aut(G) : \Gamma(N) = \{\gamma \in Aut(G) \mid [G, \gamma] \subseteq N\}$. We can infer that if $\gamma \in \Gamma(N)$ then $\widetilde{\gamma} = 1$.

The map between $Aut(G)$ and $Aut(G/N)$ is thus a group homomorphism, and infact the kernel is given by $\Gamma(N)$, the set of all maps that in G that induce trivial map on G/N. Thus we get

$$Aut(G)/\Gamma(N) \cong Aut(G/N)$$

Using the theory developed in section 1.3, We can create an inverse system of $Aut(G)$ using the open normal subgroups $\Gamma(N)$ of $Aut(G)$ where $N \triangleleft_o G$. This implies

$$\varprojlim(Aut(G)/\Gamma(N)) \cong \varprojlim(Aut(G/N)) \cong Aut(\varprojlim(G/N))$$

And since G is profinite , we know $G \cong \varprojlim(G/N)$ thus

$$\varprojlim(Aut(G)/\Gamma(N)) \cong Aut(G)$$

giving the profinite topology to $Aut(G)$. □

Proposition 3.4.2. *If G is a finitely generated pro-p group, then $\Gamma(\Phi(G))$ is a pro-p group.*

Proof. Let $G_n = P_n(G)$ for each n. The family (G_n) is a base for the neighbourhoods of 1 in G, and consists of characteristic subgroups; also $G_2 = \Phi(G)$. It follows that the subgroups $\Gamma(G_n), n \geq 2$, are normal in $\Gamma(G_2) = \Gamma(\Phi(G))$, and form a base for the neighbourhoods of 1 in $\Gamma(G_2)$. Now let $n \geq 2$, and consider the action $\Gamma(G_2)/\Gamma(G_n)$ on G/G_n given by: $\gamma(G_n) \cdot g(G_n) = \gamma(\alpha(gG_n))$ where $\alpha \in G_n$. This action is faithful, furthermore is trivial on $G/G_2 = G/\Phi(G) = G/G_n/\Phi(G)/G_n = G/G_n/\Phi(G/G_n)$. Thus $\Gamma(G_2)/\Gamma(G_n)$ induces identity on G/G_2 which implies that $\Gamma(G_2)/\Gamma(G_n)$ is a p-group for all n. Thus $\Gamma(\Phi(G))$ is a pro-p group. □

These results helps us in understanding a very useful result in Powerful pro-p groups.

Proposition 3.4.3. *Let G be a finitely generated powerful pro-p group. Then the elements* *of finite order in G form a characteristic subgroup T of G. Also T is a powerful finite p-group and G/T is uniform.*

The result requires the following lemma. Let $G_i = P_i(G)$

Lemma 7. *Let G be a uniform pro-p group, and for each i let $\mathrm{L_i}$ be the group of all automorphisms of G which induce the identity on G/G_i. Then Γ_2 is torsion-free if p is odd, Γ_3 is torsion-free if $p = 2$.*

Proof. From the Proposition 3.4.2, we get that for each $i > 2, \Gamma_2/\Gamma_i$ is a finite p-group. The map $x \mapsto x^{p^{j-1}}$ induces bijections from G/G_2 onto G_j/G_{j+1} and from G/G_3 onto G_j/G_{j+2}, from Proposition 3.3.5 . Thus Γ_2 acts trivially on G_j/G_{j+1} and that Γ_3 acts trivially on G_j/G_{j+2}, for each j. Since $\bigcap_{i=2}^{\infty} \Gamma_i = 1$, any element of finite order in Γ_2 must have p-power order. Thus it will suffice to show that Γ_2 (or Γ_3 if $p = 2$) has no elements of order p.

Now let γ satisfy $\gamma^p = 1$, where $\gamma \in \Gamma_2$ (and $\gamma \in \Gamma_3$ if $p = 2$) and suppose that for some i we have $[G, \gamma] \subseteq G_i$. Then for $g \in G$ we have

$$\begin{aligned} 1 &= [g, \gamma^p] \\ &= [g, \gamma][g, \gamma]^{\gamma} \ldots [g, \gamma]^{\gamma^{p-1}} \\ &\equiv [g, \gamma]^p \left[g, \gamma, \gamma^{p(p-1)/2}\right] \quad (\bmod G_{i+2}), \end{aligned}$$

because $[g, \gamma, \gamma^n] \in G_{i+1}$ for each n, and G_{i+2} contains both $[G_{i+1}, G]$ and $[G_{i+1}, \langle\gamma\rangle]$

If p is odd then $\gamma^{p(p-1)/2} = 1$, while if $p = 2$ and $\gamma \in \Gamma_3$ then $[g, \gamma, \gamma] \in [G_i, \Gamma_3] \subseteq G_{i+2}$. In either case, therefore, we may infer that $[g, \gamma]^p \in G_{i+2}$, and hence, $[g, \gamma] \in G_{i+1}$. Thus $[G, \gamma] \subseteq G_{i+1}$ whenever $[G, \gamma] \subseteq G_i$.
Thus it follows by induction that $[G, \gamma] \subseteq \bigcap_{i=1}^{\infty} G_i = 1$. So $\gamma = 1$ as required. □

Now we prove the main proposition:

Proof. Given G is finitely generated powerful pro-p. Then for some m, G_m is uniform. Put $K = \mathrm{C}_G(G_m)$. Then $\mathrm{Z}(K) \geq G_m \cap K$, so $K/\mathrm{Z}(K) \leq K/G_m \cap K \leq G/G_m$ is a finite p-group. This implies that K is nilpotent, and so the elements of finite order in K form a subgroup M, say. Then $M \triangleleft G$ and K/M is torsion-free.
Now G/K acts on the uniform group G_m by conjugation (i.e, : $gk \cdot g_m = g g_m g^{-1} K$). This action is faithful. Given G is powerful, G_m p.e. G (i.e, $[G_m, G] \leq (G_m)^p$), and thus if we take the action of G/K on $G_m/\Phi(G_m)$ (where $i = 2$ if p is odd, $i = 3$ if $p = 2$), the action is trivial. Thus from the above lemma, we can say that G/K is torsion free.

Thus all elements of finite order in G lie in M. Also, M is a finite p-group as $M \cap G_m = 1$ and M is powerful as given

$$[M, M] \leq M \cap [G, G] \leq M \cap \overline{G^p} = \{g^p | g \in G\} \subseteq M^p$$

if p is odd and $M \cap [G, G] \subseteq \overline{G^4}$. Thus, G/M is torsion free, and is Uniform. This concludes the proof. □

Chapter 4

Characterization of Uniform and Powerful Pro-p Groups

In this chapter, we will summarize all our understandings of Powerful and Uniformly powerful pro-p groups and draw up a characterization of Uniform Pro-p groups and then proceed to look at different families of Uniform Pro-p and powerful pro-p groups. Lastly, we conclude with a brief introduction to the characterization of Uniform pro-p groups as described in [BI]. The contents of this chapter are mostly referred from [DMSS] , [BI], [DS], [NP].

Characterization of Uniform and Powerful pro-p Groups

Uniform pro-p groups are torsion-free, and thus no finite p-group is Uniform. Being homeomorphic to ${\mathbb{Z}_p}^d$, Uniform groups are basic extensions of pro-cyclic groups. It also adopts an additive structure under which it's an abelian group and a free $\mathbb{Z}_p$ module. A bracket structure on this free $\mathbb{Z}_p$ module gives us a $\mathbb{Z}_p$ Lie-Algebra structure on a Uniform pro-p group.

Various different families of Uniform and Powerful pro-p groups are listed below:

- $\mathbb{Z}_p$ is a fundamental example for a Uniform pro-p group.
- $\Gamma_1 := \{g \in GL_n(\mathbb{Z}_p) \,|\, g \equiv \mathrm{I}_d \,(\mathrm{mod} p)\}$ is a uniform pro-p group where Γ_i form the congruence classes of subgroups of $GL_n(\mathbb{Z}_p)$, or $SL_n(\mathbb{Z}_p)$.
- Given G a finitely generated powerful pro-p group, we have $P_k(G)$ to be a uniform pro-p group for sufficiently large enough k. Additionally, every finitely generated pro-p group contains a open characteristic uniform pro-p subgroup.

- [PA] Saturable pro-p groups : A pro-p group is said to be saturable if it admits a certain valuation map. Every uniform pro-p group is said to be saturable, though the converse is not entirely true.

- [LM] All subgroups of a modular p-group are powerful p-groups.

Just-Infinite Groups

In this section, we look at a very interesting family of subgroups- the Just infinite Groups, and some interesting properties of Just-infinite groups. The results discussed in this section are mainly referred from [BI] and [BK]

Definition 4.0.1. *A group G is said to be Just-infinite if it is infinite and every non trivial normal subgroup of G has finite index in G*

Remark 4.0.1. *Any profinite group G of finite rank possesses a maximal finite normal subgroup, which is denoted as the periodic radical $\Pi(G)$ of the group.[BK]*

Some interesting properties of Just Infinite Groups are detailed below:

Proposition 4.0.1. *Let G be a finitely generated infinite group. Then G can be mapped onto a just infinite group.*

Proof. Let $\mathcal{N}$ denote the set of normal subgroups of infinite index in G. We show that every ascending chain in $\mathcal{N}$ has an upper bound in $\mathcal{N}$. Let $\{H_\alpha\}$ be such a chain of infinite index normal subgroups in G, and put $H = \bigcup_\alpha H_\alpha$. Suppose that H has finite index in G, hence H is open in G. Since G is finitely generated, so is H. But, H coincides with H_β for some β, which implies the index of H in G is infinite, a contradiction. Thus H has infinite index in G and so $H \in \mathcal{N}$. By Zorn's lemma there exists a maximal element $M \in \mathcal{N}$. If H/M is a non-trivial normal subgroup of G/M then, as M is maximal, $|G/M : H/M| = |G : H|$ is finite . Thus G/M is just infinite.

Proposition 4.0.2. *If G is a solvable pro-p group of finite rank, Let $N \lhd_c G$ such that $H = G/N$ is a just infinite group. If $\Pi(G) = 1$ then $\Pi(H) = 1$ and $\Pi(N) = 1$.*

Proof. G is pro-p group of finite rank, solvable, $\Pi(G) = 1$, $d(G) = d = dim(G)$. We claim that $\Pi(N) = 1$ and $\Pi(G/N) = 1$ where $N \lhd G$ such that G/N is Just infinite. $\Pi(N)$ is finite by definition. As $|g\Pi(N)g^{-1}| = |\Pi(N)|$ as there exist a bijection between $\Pi(N)$ and $g\Pi(N)g^{-1}$. Hence cardinalities are equal and $g\Pi(N)g^{-1}$ is finite normal subset of G.

Thus $M = \bigcup_{g \in G} g\Pi(N)g^{-1}$ is a union of finite sets. We claim that M is also a finite normal subset of G. First note that M is normal since $\Pi(N)$ is normal. As it contains the union, $M = \bigcup_{g \in G} g\Pi(N)g^{-1}$ is a finite normal subset of G. Therefore, M generates a finite normal subgroup N of G that contains $\Pi(N)$ i.e, there exists $N \triangleleft G$ st $\Pi(N) \subseteq \Pi(G)$. But $\Pi(G) = 1$, thus $\Pi(N) = 1$.

(b) Suppose there exists M/N finite normal subgroup such that $\Pi(G/N) = M/N \neq 1$. Now, $|M : N| < \infty$. Since G/N is Just infinite $|G/N| = \infty$ and for any non trivial $M/N \triangleleft G/N$ we have $|G/N : M/N| = |G : M| \leq \infty$. Thus, we get

$$|G : N| = |G : M||M : N| < \infty$$

Which is a contradiction. Hence $\Pi(G/N) = 1$. □

4.1 Characterization of Uniform Pro-p Groups

In this section, we delve into current research trends in the areas of Uniform pro-p Groups and it's characterization, The following conjecture from the paper "Characterization of Uniform pro-p Groups" by Benjamin Klopsch and Ilir Snopce(2012) [BI] will be the main focus of this section.

Conjecture: Let G be a torsion-free pro-p group of finite rank. Then G is uniform if and only if its minimal number of generators is equal to the dimension of G as a p-adic manifold, i.e., $d(G) = dim(G)$. In particular, the statement is true whenever G is solvable or $p = dim(G)$.

Now we know that if G is uniform then $d(G) = dim(G)$. Thus, we aim at getting partial results of the converse in this paper.

Proposition 4.1.1. *Suppose that $p \geq 5$ and let G be a solvable pro-p group of finite rank such that $\Pi(G) = 1$. If $d(G) = dim(G)$ then G is uniform.*

Proof. Suppose that $d(G) = dim(G)$. We need to prove that G is powerful and torsion-free.If $G = 1$ it is trivial. Hence suppose that $G \neq 1$.

Suppose G is powerful, then by Proposition 3.4.3, we know that elements of finite order form a characteristic subgroup M of G. Since $\Pi(G) = 1$, we have that $M = 1$, and thus G is torsion free. Hence it is enough to show that G is powerful.

Now let $G \geq 1$. Let $N \triangleleft G$ such that $H = G/N$ is just-infinite. From Proposition 4.0.2, we get that $\Pi(N) = \Pi(G/N) = 1$.

Also in [BK],using theorem 1.3, we get that $rk_p(G) = dim(G)$, where p is a prime, $rk(G) \leq sup\{rk_l(G)|l \text{ prime}\}$, and $rk_p(G) = sup\{d_l(H)|H \leq_o G\}$. From here we can conclude that $d(G) < dim(G)$. Applying it to N and $H = G/N$ we get that $d(N) < dim(N)$ and $d(H) < dim(H)$. Thus, we get:

$$dim(G) = d(G) \leq d(H) + d(N) \leq dim(H) + dim(N) = dim(G)$$

Thus $d(H) = dim(H)$ and $d(N) = dim(N)$. Since $dim(N) < dim(G)$, it follows by induction that N is powerful. We observe that in order to show that G is powerful it suffices to show that H is powerful: if H is powerful then

$$\begin{aligned}|G : G^p| &=| G : G^pN||N : N \cap G^p| \\ &\leq |H : H^p||N : N^p \ | \\ &= p^{d(H)+d(N)} \\ &= p^{dim(H)+dim(N)} = p^{dim(G)} = p^{d(G)} \\ &= |G : G^p[G,G]| \leq |G : G^p|\end{aligned}$$

and we obtain $[G,G] \leq G^p$.

Thus assume $H = G/N$ is just-infinite. Since G solvable, H is also solvable, and thus there exists an abelian $N \lhd_o H$. Now, let $d = d(H) = \dim(H)$ and choose an open normal subgroup $B \trianglelefteq H$ such that $B \cong \mathbb{Z}_p^d$. Let $A := \mathrm{C}_H(B) \trianglelefteq H$, the centraliser of B in H, and $\mathrm{Z}(A)$ be the centre of A. Now,$Z(A) \geq B \cap A$ .Thus $|A : \mathrm{Z}(A)| \leq |A : A \cap B| \leq |A : B| < \infty$, from which it follows that $[A,A]$ is finite by Schur's theorem. Since H is just-infinite , $|H : [A,A]| \leq \infty$ which implies that $[A,A] = 1$ .Hence A is abelian and self-centralising in H. Since $\Pi(H) = 1$, we conclude that A is torsion-free. The group $\bar{H} := H/A$ is finite and acts faithfully on $A \cong \mathbb{Z}_p^d$. Thus we obtain an embedding $\bar{H} \hookrightarrow \mathrm{GL}(A) \cong \mathrm{GL}_d(\mathbb{Z}_p)$. If $\bar{H}$ is trivial then $H = A$ is abelian, hence powerful.

In the scenario where $\bar{H} \neq 1$, $\bar{H} \neq 1$, and $C = \langle x \rangle A$ being a subgroup of H such that $\bar{C} := C/A = \langle \bar{x} \rangle$ is cyclic group of order p and contained in the centre $\mathrm{Z}(\bar{H})$ of $\bar{H}$, we infer that from the paper [HR], there are three indecomposable types of $\mathbb{Z}_p\bar{C}$-modules which are free and of finite rank as $\mathbb{Z}_p$-modules:

1. The trivial module $I = \mathbb{Z}_p$ of $\mathbb{Z}_p$-dimension 1.

2. The module $J = \mathbb{Z}_p\bar{C}/(\Phi(\bar{x}))$ of $\mathbb{Z}_p$-dimension $p-1$, where $\Phi(X) = 1 + X + \ldots + X^{p-1}$ denotes the p^{th} cyclotomic polynomial,

3. the free module $K = \mathbb{Z}_p\bar{C}$ of $\mathbb{Z}_p$-dimension p.

Given that A is a pro-p group of finite rank, we proceed computations as mentioned in [BI] (I am working on a detailed proof currently for this portion) , to get that $d(G) < dim(G)$, which will be a contradiction to our assumption that G was powerful. Thus G is powerful and it concludes the proof. □

Conclusion

In this thesis, the primarily goal was to understand the basic structure and draw up a characterization of different families of powerful and uniformly powerful pro-p groups. We started first with the basic understanding of a profinite and pro-p groups. Then we covered some advanced group theoretic techniques required to understand powerful and uniform pro-p groups.

Then we move on to a detailed structural study of Uniform pro-p groups, including the development of an additive structure and the bracket operation. Finally, we try to build up a characterization of Uniform pro-p groups using results from the paper by Benjamin Klopsch and Ilir Snopce [BI].

Bibliography

[DF] David Dummit and Richard Foote. *Abstract Algebra.* John Wiley and Sons, Inc, 3rd edition, (2004)

[BI] Benjamin Klopsch and Ilir Snopce, *A Characterisation of Uniform pro-p Groups*, Department of Mathematics, Royal Holloway, University of London, 2012

[DMSS] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic pro-p Groups.* Cambridge University Press, 2nd edition, (1994)

[PZ] Luis Ribes and Pavel Zalesskii. Profinite Groups. Springer-Verlag, 1st edition, (2000).

[BK] B. Klopsch, *On the rank of compact p-adic Lie groups*, Arch. Math. 96 (2011), 321–333

[DS] Daniel Clif and only iford Jane Smyth, *Finitely Generated Powerful Pro-p Groups*, (2010)

[NP] Marcus Sautoy, Dan Segal, Aner Shalev, *New Horizons in pro-p Groups*, Springer Science+Business Media New York 2000 , (2012)

[JS] John S Wilson, *Profinite Groups*, London Mathematical Society Monographs, (1998)

[KC] K. Chandrasekharan, *A Course on Topological Groups*, Hindustan Book Agency,1996

[JG] Jon González-Sánchez,*On p-saturable groups*,Journal of Algebra, Volume 315, Issue 2, 2007,

[LM] Alexander Lubotzky, Avinoam Mann, *Powerful p-groups. I. Finite groups*, Journal of Algebra, Volume 105, Issue 2, 1987,

[PA] Benjamin Klopsch. On the Lie theory of p-adic analytic groups. Math. Z. 249, 713–730 (2005).

[HR] Heller, A., and I. Reiner. "Representations of Cyclic Groups in Rings of Integers, I." Annals of Mathematics 76, no. 1 (1962): 73–92.