FINITELY GENERATED POWERFUL PRO-P GROUPS

Daniel Clifford Smyth

Supervisor: Dr. Daniel Chan

School of Mathematics,
The University of New South Wales.

October 2010

Submitted in partial fulfillment of the requirements of the degree of
Bachelor of Science with Honours

Acknowledgements

In retrospect, this year has gone by rather quickly. It has been almost sad over the last semester knowing that these are the last weeks and months that I will spend at this university which has given me so much, while at the same time I am working so hard that I know it will be over before I realise it. To all the friends, family, faculty, and peers who have helped me not only get through these four amazing years, but get everything out of them, I thank you.

In particular I would like to thank Dr. Daniel Chan, my supervisor, and mentor throughout the year and on many occasions prior. Without his guidance and reassurance I am sure I would not be leaving the honours year in the somewhat still together condition I am. Also, to Ian Doust, who always had an open door to discuss pretty much anything on the minds of any of the honours students. Especially for the many times he sat we me as I sought advice on whichever country I was planning to pursue a PhD in that week.

I would also like to extend gratitude to Dr. Hendrik Grundling and Dr. Jie Du for teaching two of the best courses I have taken at UNSW. Similarly to Prof. Gregory Eskin and Dr. Neelesh Tiruviluamala for teaching me an amazing two courses on Real Analysis at UCLA.

Thanks also to Nina, who provided me with a winter break in sunny Holland completely devoid of thesis work. To my mother and father who made the mistake one night of asking me what my thesis was about, and my sister and Puki for never asking.

Contents

Prelude 1
Introduction . . . 1
Author's Note . . . 2
Chapter Progression . . . 3
Notation . . . 4

Chapter 1 Beginnings: Inverse Limits in Topological Groups 5
1.1 Topological Groups . . . 5
1.2 Inverse Limits and the p-adic Numbers . . . 7
1.3 Profinite Groups . . . 12

Chapter 2 Pro-p Groups 18
2.1 Finite p-groups . . . 18
2.2 Pro-p groups . . . 25
2.3 Powerful Groups . . . 34

Chapter 3 The Iwasawa Algebra 42
3.1 Normed Rings . . . 42
3.2 The Group Algebra . . . 47
3.3 Completing the Group Algebra . . . 51

Chapter 4 p-adic Analytic Groups 54
4.1 p-adic Analytic Functions . . . 54
4.2 p-adic Analytic Manifolds . . . 60
4.3 Analytic Functions on Uniform Pro-p Groups . . . 64
4.4 p-adic Analytic Groups . . . 73
4.5 Compactness and Dimension . . . 76

Chapter 5 Closing Remarks 79

Chapter 6 Background: Unipotent Groups 80

References 82

Prelude

Lie groups, groups with a manifold structure such that the group operations are "smooth", have been of extensive interest to mathematicians throughout the 20th Century. While the study of real and complex Lie groups has been motivated by extensive applications, especially to theoretical physics, Lie groups over the p-adic numbers have been shown to be very useful in arithmetic geometry and number theory. In 1965 Michel Lazard published a solution to Hilbert's fifth problem over the p-adic numbers, giving a complete algebraic characterisation of p-adic Lie groups (p-adic analytic groups).

Building upon the work of Bruce King [Kin74], Alexander Lubotzky and Avinoam Mann developed the notion of a *powerful* finite p-group and extended it to pro-p groups (in [LM87a] and [LM87b]). This allows us to restate Lazard's result as follows.

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

Much of the beauty of Lazard's theorem is that it characterises an inherently geometric object, the p-adic analytic groups, in terms of groups whose topology, as we will see, is merely inherited from the product topology of a family of discrete spaces. Furthermore, we also establish that the topology on these groups is completely determined from their group structure, and so our characterisation is in this sense completely algebraic.

After defining the p-adic analytic groups it becomes quite clear that $(\mathbb{Z}_p, +)$ is the prototypical example, as one would expect. The notion of a powerful group allows us to introduce the groups that are central to Theorem A in an intuitive way by generalising the properties of $\mathbb{Z}_p$. The aim of this thesis is to introduce the powerful finitely generated pro-p groups underlying Lazard's Theorem in this way and demonstrate that the topological groups containing an open subgroup of this form are p-adic analytic groups. That is, providing a proof of one direction of Theorem A.

We also introduce the Iwasawa algebra of a powerful finitely generated pro-p group and establish a generalisation of the following result presented without proof in [AB06].

Theorem B *Let G be a uniform pro-p group, and let I denote the augmentation ideal of $\mathbb{F}_p[G]$. Then $\mathbb{F}_p[[G]] := \varprojlim_{N \trianglelefteq_o G} \mathbb{F}_p[G/N]$ is isomorphic to the I-adic completion of $\mathbb{F}_p[G]$. There is a similar result for $\mathbb{Z}_p[G] := \varprojlim_{N \trianglelefteq_o G} \mathbb{Z}_p[G/N]$.*

Author's Note

Initially my, somewhat loosely defined, thrust for this thesis was to investigate the ring theoretic results on Iwasawa algebras presented in the survey [AB06]. I was, however, quite decisively distracted by one seemingly small result mentioned in passing in the first pages of the survey:

> "*...a topological group G is compact p-adic analytic if and only if G is profinite, with an open subgroup which is pro-p of finite rank...*"

This led me down a somewhat skewed path, as I focused my early study entirely upon the groups themselves rather than their group algebras (and the completions of these algebras). The material thus had an entirely different flavour, becoming inherently both more topological and geometrical, though with a firm algebraic grounding in both cases. I did not, however, remain completely removed from my initial goals, still progressing into the theory of Iwaswas algebras, though they will only make a brief appearance here.

What has resulted is a very proof heavy thesis, the main aim of which is to develop the theory of the topological groups in question and provide a complete proof that these groups are p-adic analytic groups. The proofs of the results are, in my eyes, the true insight into the material. I would attribute any intuition I have gained into the area to the meticulous way I have studied them. Due to this I have omitted few, and even then only when they were well known results, standard constructions, or beyond the scope of the thesis.

While all of the results presented in this thesis can be found in existing sources, many of the proofs are original (though I certainly do not claim them to be unique). I have also taken great care to make each proof my own, either by generalising the result, simplifying the proof, or generally increasing the readability.

I have also tried to assume little knowledge outside of that presented in undergraduate studies at UNSW. In particular, group theory and topology are extensively assumed along with, to a lesser extent, the theory of rings, modules, and finite fields. The excellent [Hus66] was my main topological reference, while all of the assumed algebraic results can be found in [DF04] and [Art91]. Being devoted to developing the same notions over $\mathbb{Z}_p$, much of the later parts in the thesis discuss geometric notions (such as manifolds) over $\mathbb{R}$ and $\mathbb{C}$ without digression.

Lastly, though this thesis is dense in material, it is clearly but the footnote at the beginning of the vast field. The interest of the groups and their algebras stems from Iwasawa's work into Galois groups and has had startling applications in number theory including its use in Andrew Wiles' proof of Fermat's Last Theorem. The p-adic analytic groups are also of use to number theory and in arithmetic geometry. Some of the areas immediately beyond this thesis are discussed in Chapter 5.

Chapter Progression

The following is an outline of the structure of the thesis. Each chapter relies heavily on those preceding it, so it is essential that it is read in order to maintain coherence.

In Chapter 1 we introduce the basic ideas which form the foundations of the thesis, that of a topological group and of the inverse limit. We then show how an inverse limit of finite groups with the discrete topology gives rise to a topological group, first in constructing the p-adic numbers and then, in greater generality, in showing that any profinite group has this structure.

Chapter 2 is based around the pro-p groups, and introduces the notion of a powerful pro-p group and a uniform pro-p group. The chapter begins with a survey on the group theoretic results that are required in the remainder of the thesis, particularly in reference to the notion of the commutator and the properties of finite p-groups. These are extended to pro-p groups and the properties of finitely generated pro-p groups are discussed. The chapter concludes by building up the theory of powerful finite groups and powerful pro-p group simultaneously leading to the result that every uniform pro-p group is homeomorphic to $\mathbb{Z}_p^d$ for some d.

In Chapter 3 we develop the theory of normed rings extending the properties of the p-adic absolute value to arbitrary rings and discuss limits in, and completions of these rings. This is applied to the group algebra of a finitely generated pro-p group and we devote much of the chapter to defining the Iwasawa algebra and showing that it is isomorphic to the completion of the group algebra with respect a certain ring norm (Theorem B).

Chapter 4 is dedicated to establishing that every topological group containing a uniform pro-p group as an open subgroup is a p-adic analytic group. Beginning with the definitions of a p-adic analytic function and a p-adic analytic manifold, we see that each uniform pro-p group is such a manifold from our work in Chapter 3. We then discuss certain analytic functions on the manifold structure on uniform groups which leads into our discussion our major proof. Finally we mention some of the corollaries to Theorem A, particularly to do with when such a group is compact, and defining the dimension of such a group. We also mention some theorems just out of the scope of this thesis.

The thesis is concluded in Chapter 5, while Chapter 6 merely defines unipotent algebraic groups and establishes a result required in one of the central proofs in Chapter 3.

Notation

To avoid confusion most of the notation in this thesis follows [DSMS91]. One distinct difference in the presentation of the material is that any homomorphism, say ι, will act on an element a by $\iota(a)$. This is consistent with the entirety of undergraduate lecturing at UNSW though not the $a\iota$ notation used in [DSMS91].

Also, throughout this thesis p will always denote a prime integer. However, from Chapter 2 onwards we restrict to the case where p is odd. This is as the case $p = 2$ often needs to be dealt with separately (though in much the same manner) and in the interest of brevity we simply disregard it. However, all the stated results can be shown for $p = 2$, albeit with modified definitions in some places. As well as this, we reserve the notation $\mathbb{Z}_p$ for the ring (or group) of p-adic integers and denote the finite group/field of order p, $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$.

The identity in a group G will always be denoted $1 = 1_G$ unless G has been specifically stated to be an additive group.

$\subseteq$	subset
$\subseteq_o$, $\subseteq_c$	open subset, closed subset
$\leq$	subgroup
$\leq_o$, $\leq_c$	open subgroup, closed subgroup
$\lhd$	normal subgroup
$\lhd_o$, $\lhd_c$	open normal subgroup, closed normal subgroup
$\overline{X}$	closure of X
$\langle X \rangle$	the group generated by the set X
$\overline{\langle X \rangle}$	the group generated topologically by the set X
$[A, B]$	the commutator subgroup of A and B
$[G : N]$	the index of N in G
AB	the set of elements $\{ab \mid a \in A, b \in B\}$
A^p	the group generated by $\{a^p \mid a \in A\}$, $\langle a^p \mid a \in A \rangle$
$R^\times$	the group of units in the ring R

Lastly for any n-tuple $\mathbf{X} = (X_1, \ldots, X_n)$ and any $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ we set

$$\mathbf{X}^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n} \text{ and } \langle \alpha \rangle = \alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

Similarly if $u_1, \ldots, u_n$ are elements of a pro-p group and $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}_p^n$ then

$$\mathbf{u}^\lambda = u_1^{\lambda_1} \ldots u_n^{\lambda_n}.$$

Chapter 1

Beginnings: Inverse Limits in Topological Groups

We begin our exposition by considering the two notions underpinning what will follow, that of topological groups and the category theoretic construction of the inverse limit of a system of objects. Topological group theory, as the name suggests, is the intersection of the fields of group theory and topology. Being endowed with a continuous group structure yields some immediate and useful observations which we begin with.

It is then shown that we can use the inverse limit to define the p-adic integers $\mathbb{Z}_p$, and that $\mathbb{Z}_p$ inherits a topology from this inverse limit with respect to which $(\mathbb{Z}_p, +)$ is a topological group. Lastly we extend the fundamental topological properties of $\mathbb{Z}_p$ to define the profinite groups as the class of topological groups which are Hausdorff, compact, and whose subgroups form a base for the neighbourhoods of the identity. In our main result of this chapter we will show that a group is profinite if and only if it is isomorphic to an inverse system of finite groups.

The exposition in this chapter follows that of [Hus66] for our introduction to topological groups, [Ser73] for our construction of p-adic numbers, and [DSMS91] and [RZ00] for the basic properties of profinite groups.

1.1 Topological Groups

Definition 1.1. A group $(G, *)$ that is also a topological space is called a *topological group* if the multiplication and inversion mappings

$$\begin{aligned} g_1 : G \times G \to G \quad &: \quad g_1(a, b) = a * b \\ g_2 : G \to G \quad &: \quad g_2(a) = a^{-1} \end{aligned}$$

are both continuous.

Example 1.2. [Topological Groups.]

(i) Any group G endowed with the discrete topology. Such groups are called *discrete groups*.

(ii) The additive group $(\mathbb{R}, +)$ with the usual topology on $\mathbb{R}$.

(iii) The multiplicative group $GL_n(\mathbb{R})$ with the topology defined by viewing our group as a subspace of $\mathbb{R}^{n^2}$.

□

So some of the groups we are most familiar with are topological groups. While relatively easy to establish, the following proposition (and its corollaries) give us much insight into the inherent structure of the topology in a topological group.

Proposition 1.3. *The group homomorphisms $r_a, l_a : G \to G$ defined by*

$$\begin{aligned} r_a(x) &= xa \\ l_a(x) &= ax \end{aligned}$$

are homeomorphisms of G.

Proof. Firstly, r_a is bijective as for any $b \in G$, $r_a(ba^{-1}) = b$, and by cancellation r_a is injective. Also, for any $O \subseteq_o G$ we have $g_1^{-1}(O) \subseteq_o G \times G$. Recall that $\{O_1 \times O_2 \mid O_1, O_2 \subseteq_o G\}$ is a basis for the product topology on $G \times G$.It is clear then that the map $\phi : G \to G \times G$ defined by $x \mapsto (x, a)$ is continuous as $\phi^{-1}(O_1 \times O_2) = O_1$ if $a \in O_2$ and $\varnothing$ otherwise. Hence as $r_a = g_1 \circ \phi$, the composition of continuous maps, r_a is continuous. It is clear that $r_a^{-1} = r_{a^{-1}}$ and is continuous by the same argument, and thus r_a is a homeomorphism. The result holds for l_a similarly. □

Corollary 1.4. *Let $C \subseteq_c G$ and $O \subseteq_o G$ where G is a topological group. Then for any $a \in G$ and $A \subseteq G$*

(i) aC and Ca are both closed subsets of G;
(ii) aO and Oa are both open subsets of G;
(iii) AO and OA are also open in G.

Proof. This is clear as r_a and l_a are homeomorphisms and hence both open and closed, and

$$OA = \bigcup_{a \in A} Oa, \quad AO = \bigcup_{a \in A} aO.$$

□

Another nice, and immediate corollary to Proposition 1.3 is that every topological group is a homogeneous topological space. That is, for any $g, h \in G$, there exists a homeomorphism f of G such that $f(g) = h$. However, for our work the most important consequence stems from the following definition.

Definition 1.5. A subfamily $\mathcal{U}$ of neighbourhoods of a point x in any topological space is said to be a *base* or *fundamental system of neighbourhoods* if for any neighbourhood V of x there is a $U \in \mathcal{U}$ such that $U \subseteq V$.

So if we have a base for the neighbourhoods around any one element of a topological group we can obtain a base for the neighbourhoods around any other element by translation. In the same manner we can clearly extend a base of neighbourhoods around the identity to a base for our topology. Let $\mathcal{U}$ be a base of the neighbourhoods of the identity 1 in a topological group G. If we have any non-empty $W \subseteq_o G$ and take any $w \in W$, then $w^{-1}W$ is an open set containing 1 and hence we have a $U \in \mathcal{U}$ such that $U \subseteq w^{-1}W$ and thus $wU \subseteq W$. Thus

$$\mathcal{V} := \{xU \mid x \in G, U \in \mathcal{U}\}$$

is a base for the topology on G. Furthermore, the topology on G is actually completely determined by a base for the neighbourhoods of the identity (see [Hus66] page 46 for a proof).

Lastly, we present a result ensuring that quotient map from any topological group to a quotient group endowed with the quotient topology is both continuous and open.

Proposition 1.6. *Let G be a topological group and $H \triangleleft G$. If G/H is the quotient space, endowed with the quotient topology, and ϕ the canonical mapping of G into G/H, then:*

(i) *ϕ is onto;*
(ii) *ϕ is continuous;*
(iii) *ϕ is open;*
(iv) *the quotient topology is the finest topology on G/H with respect to which ϕ is continuous.*

Proof. (i) and (ii) follow from the definition of the quotient topology. To establish (iii) we must show that $\phi(U) \subseteq_o G/H$ for all $U \subseteq_o G$. That is $\phi^{-1}(\phi(U)) \subseteq_o G$. But $\phi^{-1}(\phi(U)) = UH = \bigcup_{h \in H} Uh$ which is open, and hence ϕ is open. Now for (iv), let μ be any other topology on G/H such that $\phi : G \to G/H$ is continuous. Then for each μ-open set V in G/H, $\phi^{-1}(V) = VH \subseteq_o G$. But then by (iii) V is open is the quotient topology. Thus the quotient topology is finer than μ. □

1.2 Inverse Limits and the p-adic Numbers

We move forward to introducing the notion of an inverse system and defining the inverse limit of such a system, though we first recall the following set theoretic definition.

Definition 1.7. Given a set S, a *partial order* on S is a binary relation $\leq$ such that for all $a, b, c \in S$

(i) $a \leq a$ (reflexivity),
(ii) if $a \leq b$ and $b \leq a$ then $a = b$ (antisymmetry),
(iii) if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity).

If S has a partial order is called a *partially ordered set* or *poset*. Furthermore, if a poset S has the additional property that each pair of elements has an upper bound then we say that S is a *directed set*.

Definition 1.8. An *inverse (or projective) system of groups* is a family of groups $\{A_\lambda\}$ indexed over a poset Λ and a family of homomorphisms $\{f_{\lambda\mu}\}$ for all $\lambda \leq \mu$ in Λ, where $f_{\lambda\mu} : A_\mu \to A_\lambda$ and

$$\begin{aligned} f_{\lambda\lambda} &= id_{A_\lambda}, \text{ and} \\ f_{\lambda\nu} &= f_{\lambda\mu} \circ f_{\mu\nu}, \text{ for all } \lambda \leq \mu \leq \nu. \end{aligned}$$

We denote this inverse system by $(A_\lambda, f_{\lambda\mu})$.

Given such a system we can consider elements in the product group $\prod_{i\in\Lambda} A_i$ whose 'entries' are images of one another under the homomorphisms. We define the *inverse limit* to be the group of the these elements

$$\varprojlim_{\lambda\in\Lambda} A_\lambda = \{(a_\lambda) \in \prod_{\lambda\in\Lambda} A_\lambda \mid f_{\lambda\mu}(a_\mu) = a_\lambda, \text{ for all } \lambda \leq \mu\}.$$

Though our definition above is in terms of groups, the inverse limit can be defined in any category. In particular, exactly the same construction can be used when we are considering sets with set functions, rings with ring homomorphisms, or algebras with algebra homomorphisms. These are the only four categories we will take inverse limits over in what follows. In an arbitrary category, however, the inverse limit is defined with reference to the following universal property. We present it as a consequence of our construction when we have an inverse system of groups, though the same method will yield the corresponding result for sets, rings, and algebras.

Proposition 1.9. *[Universal Property of Inverse Limits.]*
Suppose that $(A_\lambda, f_{\lambda\mu})_\Lambda$ is an inverse system of groups and let X denote its inverse limit with natural projection maps $\pi_\lambda : X \to A_\lambda$. Then for any group Y and family of homomorphisms $\{\omega_\lambda\}_{\lambda\in\Lambda}$ such that $\omega_\lambda = f_{\lambda\mu} \circ \omega_\mu$ (for all $\lambda < \mu$) there exists a unique group homomorphism $\phi : Y \to X$ such that

$$\omega_\lambda = \pi_\lambda \circ \phi$$

for all $\lambda \in \Lambda$.

Proof. Let $\phi : Y \to X$ be defined by $\phi(y) = (\omega_\lambda(y))_{\lambda\in\Lambda}$. As $\omega_\lambda = f_{\lambda\mu} \circ \omega_\mu$, ϕ is clearly well defined. Also ϕ is a homomorphism as

$$\begin{aligned} \phi(yy') = (\omega_\lambda(yy')) &= (\omega_\lambda(y)\omega_\lambda(y')) \\ &= (\omega_\lambda(y))(\omega_\lambda(y')) \\ &= \phi(y)\phi(y'). \end{aligned}$$

It remains only to show that ϕ is unique. Take any $\psi : Y \to X$ such that $\omega_\lambda = \pi_\lambda \circ \psi$ for all λ and suppose that there exists a $y \in Y$ such that $\psi(y) \neq \phi(y)$. Then, by the definition of the inverse limit, there exists a $\lambda \in \Lambda$ such that $\pi_\lambda(\psi(y)) \neq \pi_\lambda(\phi(y)) = \omega_\lambda(y)$. This is an obvious contradiction, and thus ϕ is unique. □

It is using the theory of inverse limits that we construct the p-adic integers $\mathbb{Z}_p$. We begin by considering the family of finite p-rings $\mathbb{Z}/p^n\mathbb{Z}$ for any fixed prime p. Now, for any positive integers m and n such that $m \leq n$ we can define $\pi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ sending $g + p^n\mathbb{Z} \mapsto g + p^m\mathbb{Z}$. It is clear that each π_{mn} is onto and $\ker \pi_{mn} = p^m\mathbb{Z}/p^n\mathbb{Z}$. Thus for positive integers $l \leq m \leq n$

$$\pi_{mm} = id_{\mathbb{Z}/p^m\mathbb{Z}} \text{ and } \pi_{ln} = \pi_{lm} \circ \pi_{mn}.$$

So the sequence

$$\ldots \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

forms an inverse system indexed by $\{1, 2, 3, \ldots\}$.

Definition 1.10. The ring of *p-adic integers* $\mathbb{Z}_p$ is defined as the inverse limit of the system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_{mn})$:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \pi_{mn}(a_n) = a_m \text{ for all } m \leq n\}.$$

If we give each $\mathbb{Z}/p^n\mathbb{Z}$ the discrete topology, $(\mathbb{Z}_p, +)$ becomes a topological group with the topology it inherits from the product topology in $\prod \mathbb{Z}/p^n\mathbb{Z}$. Hence $\mathbb{Z}_p$ is an additive topological group that is also a ring under the multiplication operation. Directly from its definition we can deduce some of the topological properties of $\mathbb{Z}_p$.

Theorem 1.11. *The p-adic integers $\mathbb{Z}_p$ form a Hausdorff, compact topological space.*

The proof of this result relies on Tychonoff's theorem which is equivalent to the axiom of choice and is stated below. We will continue to use it throughout what follows and while proof is omitted here it can be found in [Hig74].

Theorem 1.12. *[Tychonoff's Theorem.]*
The product of any family of compact topological spaces is compact.

Proof of Theorem 1.11. As $\mathbb{Z}_p$ is a subspace of a product of Hausdorff spaces it is clearly Hausdorff. It is also clear by Tychonoff's theorem that $\prod \mathbb{Z}/p^n\mathbb{Z}$ is a compact space and hence it suffices to show that $\mathbb{Z}_p$ is a closed subspace. If we take any $(a_n) \in (\prod_{i=1}^{n} \mathbb{Z}/p^n\mathbb{Z}) \backslash \mathbb{Z}_p$ we have, for some positive integers $m \leq n$, $\pi_{mn}(a_n) \neq a_m$. Now

$$U = \prod_{l \neq m,n} \mathbb{Z}/p^l\mathbb{Z} \times \{a_m\} \times \{a_n\}$$

is open in $\prod \mathbb{Z}/p^n\mathbb{Z}$ and $U \cap \mathbb{Z}_p = \varnothing$. Hence $(\prod_{i=1}^{n} \mathbb{Z}/p^n\mathbb{Z}) \backslash \mathbb{Z}_p$ is open and $\mathbb{Z}_p$ is closed as required. □

We now turn to the algebraic properties of $\mathbb{Z}_p$.

Proposition 1.13. *If $\epsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is the natural projection map. Then*

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} \mathbb{Z}/p^n\mathbb{Z} \to 0$$

is a short exact sequence.

Proof. If we have $x = (x_n) \in \mathbb{Z}_p$ such that $px = 0$ then $px_n = 0$ in $\mathbb{Z}/p^n\mathbb{Z}$ for all n and $x_{n+1} = p^n y_{n+1}$ for some $y_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$. But now $x_n = \pi_{n(n+1)}(p^n y_{n+1}) = 0$, so $x = 0$ and multiplication by p is injective. It follows that multiplication by p^n is also injective.

Now, ϵ_n is obviously onto and so it remains to show only that $\ker \epsilon_n = p^n\mathbb{Z}_p$. Clearly $\ker \epsilon_n$ contains $p^n\mathbb{Z}_p$. Conversely, if $x = (x_m) \in \ker \epsilon_n$ we have $x_m = 0$ for all $m \leq n$ and $x_m \equiv 0 \pmod{p^n}$ for all $m > n$. Then for each $m > n$ there exists $y_{m-n} \in \mathbb{Z}/p^{m-n}\mathbb{Z}$ such that under the natural isomorphism $\phi : \mathbb{Z}/p^{m-n}\mathbb{Z} \to$

$p^n\mathbb{Z}/p^m\mathbb{Z}$, $\phi(y_{m-n}) = p^n y_{m-n} = x_n$. Then $y := (y_i) \in \mathbb{Z}_p$ and $p^n y = x$. Thus $\ker \epsilon_n = p^n\mathbb{Z}_p$ and our sequence is short exact. □

An obvious consequence of the above is that $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ an equivalence property which we will be using without mention throughout this thesis. Now, $\mathbb{Z}_p$ is clearly abelian as each $\mathbb{Z}/p^n\mathbb{Z}$ is an multiplication is coordinate-wise. However, $\mathbb{Z}_p$ is not a field. In fact only those elements not divisible by p are invertible as the proposition below establishes.

Proposition 1.14.

(i) If $x \in \mathbb{Z}_p$, x invertible (in $\mathbb{Z}_p$) if and only if $p \nmid x$.

(ii) If $\mathbb{U}_p$ denotes the group of units in $\mathbb{Z}_p$ then any non-zero $x \in \mathbb{Z}_p$ can be written as $p^n u$ for some $u \in \mathbb{U}_p$.

Proof. (i) If $x \in \mathbb{Z}_p$ is invertible then, as operations occur coordinate-wise, its image in $\mathbb{Z}/p\mathbb{Z}$ must be invertible. Hence $p \nmid x$. Conversely suppose that $p \nmid x \in \mathbb{Z}_p$. Then if $x_n = \epsilon_n(x)$ (with ϵ_n as above) we see $x_n \notin p\mathbb{Z}/p^n\mathbb{Z}$ for all n, and hence its image in $\mathbb{Z}/p\mathbb{Z}$ is invertible. Thus there exists $y \in \mathbb{Z}/p^n\mathbb{Z}$ such that $x_n y \equiv 1 \pmod{p}$, that is $x_n y = 1 - pz$ for some $z \in \mathbb{Z}_p$. So

$$x_n y(1 + pz + \ldots + p^{n-1}z^{n-1}) = (1 - pz)(1 + pz + \ldots + p^{n-1}z^{n-1}) = 1$$

and x is thus invertible.

(ii) As $x \neq 0$ we have a smallest n such that $\epsilon_n(x) \neq 0$. Then $x = p^n u$ with $p \nmid u$ implying that $u \in \mathbb{U}_p$ by (i). □

This proposition tells us that for each non-zero $x \in \mathbb{Z}_p$ there is a unique $n \geq 0$ such that $x = p^n u$ for some unit u, motivating the following definition.

Definition 1.15. The *p-adic absolute value* $|\cdot|_p$ on $\mathbb{Z}_p$ is defined by

$$|x|_p = p^{-n}$$

where $x = p^n u$ as above for any non-zero $x \in \mathbb{Z}_p$. We set $|0|_p = 0$.

The p-adic absolute value is an example of a non-Archimedean norm on the ring $\mathbb{Z}_p$ as for all a, b it satisfies:

(i) $|a|_p \geq 0$ and $|a|_p = 0$ if and only if $a = 0$;
(ii) $|1|_p = 1$ and $|ab|_p \leq |a|_p\,|b|_p$; and
(iii) $|a \pm b|_p \leq \max\{|a|_p, |b|_p\}$.

The first condition is clear by our definition, as is that $|1|_p = 1$. Suppose that $p^n|a$ and $p^m|b$, assuming $m \leq n$ without loss of generality. Then $p^{n+m}|ab$ and $p^m|a \pm b$, from which the rest of the conditions follow. In fact these three conditions imply something stronger than (iii).

Corollary 1.16. *For any $a, b \in \mathbb{Z}_p$ such that $|a|_p \neq |b|_p$*

$$|a \pm b|_p = \max\{|a|_p, |b|_p\}.$$

Proof. Assume without loss of generality that $|a|_p > |b|_p$. Then

$$|a|_p = |a + b - b|_p \leq \max\{|a + b|_p, |b|_p\} \leq \max\{|a|_p, |b|_p\} = |a|_p.$$

□

This also holds in an arbitrary ring R with identity and non-Archimedean norm $||\cdot||$ as we will encounter later. We return now to the topology on $\mathbb{Z}_p$ briefly and show that the topology defined by the absolute value in fact coincides with the p-adic topology.

Lemma 1.17. *The open ball*

$$B(a, p^{-h}) := \{x \in \mathbb{Z}_p \mid |x - a|_p < p^{-h}\}$$

is both open and closed in $\mathbb{Z}_p$.

Proof. Note that if $a = (a_n) \in \mathbb{Z}_p$

$$B(a, p^{-h}) = \mathbb{Z}_p \cap \left(\{a_1\} \times \ldots \{a_h\} \times \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}\right)$$

which is open by the definition of the product topology. Now, if we take any $x \in \mathbb{Z}_p \backslash B(a, p^{-h})$ then $|x - a|_p \geq p^{-h}$, and thus for any $y \in B(x, p^{-h})$

$$|y - a|_p = |y - x + x - a|_p = |x - a|_p \geq p^{-h}$$

by Corollary 1.16. Hence $B(a, p^h) \cap B(x, p^{-h}) = \varnothing$ for all such x and it follows that $B(x, p^{-h})$ is closed as required. □

Proposition 1.18. *The topology on $\mathbb{Z}_p$ coincides with the topology defined by $|\cdot|_p$. With respect to the metric defined by $|\cdot|_p$, $\mathbb{Z}_p$ is a complete metric space in which $\mathbb{Z}$ is a dense subring.*

Proof. Let the p-adic topology (inherited from the product topology) be denoted $\mathcal{A}$ and the metric topology be denote $\mathcal{B}$. Then for any $O \in \mathcal{B}$ the lemma above shows us that $O \in \mathcal{A}$. Conversely, the ideals $p^n\mathbb{Z}_p$ form a basis for the neighbourhoods of 0 in $\mathcal{A}$, and hence by the discussion in the previous section, the additive translates of these sets form a basis for the open sets in $\mathcal{A}$. But $p^n\mathbb{Z}_p = B(0, p^{-n})$ and so $\mathcal{A}$ and $\mathcal{B}$ coincide. Since every compact metric space is complete, and $\mathbb{Z}_p$ is compact, it is complete. Finally, if we take any $x = (x_n) \in \mathbb{Z}_p$ and $y_n \in \mathbb{Z}$ such that $y_n \equiv x_n \pmod{p^n}$ then $\lim_{n\to\infty} y_n = x$ and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ as required. □

Finally we define the p-adic numbers:

Definition 1.19. The field of *p-adic numbers* $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$.

From Proposition 1.14 it is clear that $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$ and so every element in $\mathbb{Q}_p$ can be written uniquely in the form $p^n u$ with $n \in \mathbb{Z}$, $u \in \mathbb{U}_p$. We can hence extend our definition of the p-adic absolute value to $\mathbb{Q}_p$. We immediately see that $\mathbb{Q}_p$ is

topologically defined by $|\cdot|_p$ and contains $\mathbb{Z}_p$ as an open (and closed) subring. It is also clear that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

It is worthy noting that the construction of $\mathbb{Q}_p$ is often done by completing $\mathbb{Q}$ with respect to the metric defined by $|\cdot|_p$. The p-adic integers $\mathbb{Z}_p$ are then taken to be those $x \in \mathbb{Q}_p$ such that $|x|_p \leq 1$. This is especially the case in texts with an analytic focus as in [Kob80].

1.3 Profinite Groups

Above we constructed the p-adic integers as the inverse limit of a system of finite groups and established that, with the topology inherited from the product topology on $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Z}_p$ is a compact, Hausdorff space. It is also clear that the additive subgroups

$$\{1 + p^n\mathbb{Z}_p \mid n = 1, 2, \ldots\}$$

form a base for the neighbourhoods of the identity. We now generalise these properties of $\mathbb{Z}_p$ to an arbitrary topological group, thus defining the profinite groups. What is surprising is that each such group is isomorphic to the inverse limit of some system of finite groups and conversely any inverse limit of a system of finite groups satisfies these properties. In the next chapter each of the classes of groups we will restrict to will be a subset of the profinite groups, and they are hence the loosest generalisation of $\mathbb{Z}_p$ we will consider in this thesis.

Definition 1.20. A *profinite group* is a compact, Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity.

Note that by our exposition in Section 1.1 it is clear that the translates of open subgroups form a base for the topology on a profinite group. We can use this idea to establish some preliminary results about profinite groups, proving the following proposition that is presented without proof in [DSMS91].

Proposition 1.21. *Let G be a profinite group.*

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

(ii) A subset of G is open if and only if it is a union of cosets of open normal subgroups.

(iii) If X and Y are closed subsets of G then so are the sets $XY = \{xy \mid x \in X, y \in Y\}$ and $\{x^n \mid x \in X\}$ for any integer n.

(iv) If $H \leq_c G$ then H (with the induced topology) is a profinite group. Also, every open subgroup of H is of the form $H \cap K$ where $K \leq_o G$.

(v) If $M \lhd_c G$ then G/M (with the quotient topology) is a profinite group.

Proof. We prove each part:

(i) Take $O \leq_o G$. Clearly $G\backslash O = \bigcup_{g \in G\backslash O} gO$ and hence $G\backslash O \subseteq_o G$ and thus $O \subseteq_c G$. Also, as G is compact there must exist a finite subcover of $\bigcup_{g \in G} gO = G$ and thus $[G : O] < \infty$. Consider now S a transversal of the cosets of O, and define $N = \bigcap_{s \in S} sOs^{-1}$. N is obviously an open subgroup so it just remains to show that

it is normal. Take any $g \in G$ and note that for any $s \in S$, $(sg)^{-1} = t_s o_s$ for some $t_s \in S$ and $o_s \in O$. Hence

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

as each t_s is a distinct element of S. Thus $N \lhd_o G$ and $N \subseteq O$.

We have already shown that if $C \subseteq_o G$ then C is closed and has finite index. Conversely suppose $[G : C] < \infty$ and let $\mathcal{C}$ be the set of cosets of C in G. It follows that $\bigcup_{D\in\mathcal{C}\setminus\{C\}} D = G\backslash C$ is closed in G and hence $C \leq_o G$.

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

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

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

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

(v) If $M \lhd_o G$ then G/M is a finite group with the discrete topology and the result is clear. Assume then that M is not open in G. Let $\pi : G \to G/M$ be the canonical quotient map which is continuous and open by Proposition 1.6. Thus if $\bigcup_{i\in I} H_i$ is an open cover fro G/M then $\bigcup_{i\in I} \pi^{-1}(H_i)$ is an open cover for G. The compactness of G/N thus follows from that of G.

If K is any neighbourhood of the identity in G/M, which we can assume without loss of generality to be open, then $\pi^{-1}(K) \subseteq_o G$ and thus there is a subgroup $H \leq_o G$ such that $H \subseteq \pi^{-1}(K)$. It is clear then that $\pi(H) \leq_o G/M$ and thus the open subgroups form a base for the neighbourhoods of the identity.

If $x \in G/M$ then as M is closed, $xM \subseteq_c G$. As π is an open mapping it follows that $\pi(G \backslash xM) \subseteq_o G$ which precisely gives us that $\{x\} \subseteq_c G/M$ so that G/M is a regular (or T_1) space. Every regular topological group is Hausdorff ([Hus66] Theorem 4, Part III) and thus G/M is profinite. □

In order to prove the equivalent characterisation of profinite groups as the inverse limit of a system of finite groups we must recall the following purely topological result.

Proposition 1.22. *Any continuous bijection $f : A \to B$ where A is compact and B is Hausdorff is a homeomorphism.*

Proof. It suffices to show that f is closed. That is for all $C \subseteq_c A$, $f(C) \subseteq_c B$. Take then any $C \subseteq_c A$. As A is compact, C is compact, and thus $f(C)$ is compact as f is continuous. If $f(C) = B$ then clearly $f(C) \subseteq_c B$. Otherwise take any $b \in B \backslash f(C)$. As B is Hausdorff for all $c \in f(C)$ we have $N_{b,c}$, N_c disjoint open neighbourhoods of b and c respectively. Now $\{N_c\}_{c \in f(C)}$ is an open cover and thus admits a finite subcover, $\{N_c\}_{c \in D}$, for $D \subset f(C)$. But then $\bigcap_{c \in D} N_{b,c}$ is a finite intersection of open sets, thus open; and it is distinct from $f(C)$. Thus $B \backslash f(C)$ is open and $f(C)$ is closed as claimed. □

We have the following immediate corollary:

Corollary 1.23. *Any continuous group isomorphism between profinite groups is a topological isomorphism (homeomorphism).*

We can now prove the main theorem of this part, noting that $(G/N, \pi_{M,N})_{N \lhd_o G}$ is an inverse system where $\pi_{M,N} : G/N \to G/M$ is the natural surjection for all $N \subseteq M$. Hence the inverse limit we propose is well defined.

Theorem 1.24. *If G is a profinite group then G is (topologically) isomorphic to $\varprojlim (G/N)_{N \lhd_o G}$. Conversely, the inverse limit of any system of finite groups is a profinite group.*

Proof. First we let G be any profinite group and $\hat{G} = \varprojlim (G/N)_{N \lhd_o G}$, and consider the natural homomorphism

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

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

Now Proposition 1.6 gives us that the natural projection $\phi_N : G \to G/N$ is continuous for all $N \lhd_o G$. However, ι is merely the map $g \mapsto (\phi_N(G))$, and hence for any open set in $\prod_{N \lhd_o G} G/N$, say

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

we have

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

But this is just a finite union of open sets in G and so ι is continuous. Thus by Proposition 1.22 that ι is a homeomorphism and hence our (topological) isomorphism is established.

For the converse we consider an inverse system of finite groups G_λ ($\lambda \in \Lambda$), each with the discrete topology. Then $\prod_{\lambda \in \Lambda} G_\lambda$ is Hausdorff, and Tychonoff's theorem shows it is compact. If we take any open neighbourhood of the identity O then by the definition of the product topology,

$$O \supseteq U(S) := \prod_{\lambda \notin S} G_\lambda \times \prod_{\lambda \in S} \{1\}$$

for some finite $S \subseteq \Lambda$. As G_λ is endowed with the discrete topology $\{1\} \leq_o G_\lambda$ for all λ and it follows that $U(S) \leq_o \prod G_\lambda$. Thus $\prod G_\lambda$ is a profinite group and it suffices to show that $\varprojlim G_\lambda = \hat{G}$ is a closed subgroup.

Taking any $\hat{g} = (g_\lambda) \in \big(\prod G_\lambda\big) \backslash \hat{G}$. Then there exists $\mu, \nu \in \Lambda$ such that $\pi_{\mu\nu}(g_\nu) \neq g_\mu$. Hence $\hat{g}U(\{\mu, \nu\})$ is an open neighbourhood of $\hat{g}$ such that $\hat{g}U(\{\mu, \nu\}) \cap \hat{G} = \varnothing$. Thus $\hat{G}$ is closed as required. □

We now present two examples of profinite groups that we will carry throughout the thesis, that of $GL_n(\mathbb{Z}_p)$ and $SL_n(\mathbb{Z}_p)$. Here they help demonstrate how one can use either of the two alternate characterisations shown equivalent above to demonstrate that a certain group is profinite.

Example 1.25. [$GL_n(\mathbb{Z}_p)$ is profinite.]

We show that the group $GL_n(\mathbb{Z}_p)$ is profinite from Definition 1.20, where

$$GL_n(\mathbb{Z}_p) = \{a \in M_n(\mathbb{Z}_p) \mid \det(a) \not\equiv 0 \pmod{p}\}.$$

By Theorem 1.11 we have that $M_n(\mathbb{Z}_p) \cong \mathbb{Z}_p^{n^2}$ is both Hausdorff and compact. Also as $p\mathbb{Z}_p$ is both open and closed in $\mathbb{Z}_p$, $pM_n(\mathbb{Z}_p)$ is open and closed in the product topology of $M_n(\mathbb{Z}_p)$. Now, if $b \equiv a \pmod{p}$ and $a \in GL_n(\mathbb{Z}_p)$ then so $b \in GL_n(\mathbb{Z}_p)$ and hence $GL_n(\mathbb{Z}_p)$ is a finite union of additive cosets of $pM_n(\mathbb{Z}_p)$. Thus $GL_n(\mathbb{Z}_p)$ is both open and closed in $M_n(\mathbb{Z}_p)$ and it follows that it is a Hausdorff, compact space. If we consider now,

$$\Gamma_i := \{a \in GL_n(\mathbb{Z}_p) \mid a \equiv I_n \pmod{p^i}\}$$

then $\{\Gamma_i\}_i$ is clearly a base for the neighbourhoods of the identity in $GL_n(\mathbb{Z}_p)$, and each is obviously a subgroup. Also, as Γ_i corresponds to the product of n^2 open balls of radius p^{-i} in $\mathbb{Z}_p^{n^2}$, these are open subgroups. So the open subgroups of $GL_n(\mathbb{Z}_p)$ form a base for the neighbourhoods of the identity and hence $GL_n(\mathbb{Z}_p)$ is profinite. □

Example 1.26. [$SL_n(\mathbb{Z}_p)$ is profinite.]

Here the matrix a is taken to have (i,j)th entry $a^{(ij)}$.

We begin by considering the groups $G_m = SL_n(\mathbb{Z}/p^m\mathbb{Z})$. Recall from our construction of $\mathbb{Z}_p$ that $(\mathbb{Z}/p^s\mathbb{Z}, \pi_{st})$ is an inverse system of rings, where π_{st} is the natural surjection from $\mathbb{Z}/p^t\mathbb{Z}$ to $\mathbb{Z}/p^s\mathbb{Z}$ (for $s \leq t$). Now if we consider $\omega_{lm} : G_m \to G_l$ (where $l \leq m$) defined by $a^{(ij)} \mapsto \pi_{nm}(a^{(ij)})$ we have that (G_m, ω_{lm}) is an inverse system. Also, each G_m is finite as it is a subset of $M_n(\mathbb{Z}/p^m\mathbb{Z})$ and

$$|M_n(\mathbb{Z}/p^m\mathbb{Z})| = p^{m^{n^2}}.$$

Hence $\varprojlim SL_n(\mathbb{Z}/p^m\mathbb{Z})$ is a profinite group. All that remains to be shown is that

$$\varprojlim_m G_m \cong SL_n(\mathbb{Z}_p) = \{g \in GL_n(\mathbb{Z}_p) \mid \det(g) = 1\}.$$

Recall that we have the projection maps $\epsilon_m : \mathbb{Z}_p \to \mathbb{Z}/p^m\mathbb{Z}$, and define the homomorphism $\alpha : SL_n(\mathbb{Z}_p) \to \varprojlim G_m$ by $g \mapsto (g_m)_{m\in\mathbb{Z}}$ where $g_m^{(ij)} = \epsilon_m(g^{(ij)})$. This map is well defined as if $g \in SL_n(\mathbb{Z}_p)$ then $\det(g) = 1 \equiv 1 \pmod{p^m}$ for all m. Similarly, if $\det(g_m) \equiv 1 \pmod{p^m}$ for all m then the matrix $g \in M_n(\mathbb{Z}_p)$ defined by

$$g^{(ij)} = (g_m^{(ij)})_m$$

has determinant 1, and thus α is sujective. Also, α is injective as $(g_m) = (f_m) \in \varprojlim G_m$ if and only if $(g_m^{(ij)}) = (f_m^{(ij)})$. Thus α is an isomorphism. Finally α is continuous as

$$S_m = \prod_{i=1}^{m} \{1\} \times \prod_{i=m}^{\infty} G_m$$

form a base for the neighbourhoods of the identity of $\varprojlim G_m$ and $\alpha^{-1}(S_m) = SL_n(p^m\mathbb{Z}_p) \subseteq_o SL_n(\mathbb{Z}_p)$,

Now, if $g \in M_n(\mathbb{Z}_p)\backslash SL_n(\mathbb{Z}_p)$ then there exists h such that $\det(g) \not\equiv 1 \pmod{p^h}$. It follows that for all $h \equiv g \pmod{p^h}$, $\det(h) \equiv \det(g) \pmod{p^h}$ and so $h \notin SL_n(\mathbb{Z}_p)$. Hence $SL_n(\mathbb{Z}_p)$ is closed and thus compact and we can apply Proposition 1.22. Thus α is an homeomorphism and $SL_n(\mathbb{Z}_p)$ is a profinite group as claimed.

It is worth noting that our result would have followed immediately upon noting that $SL_n(\mathbb{Z}_p)$ is closed in the profinite $GL_n(\mathbb{Z}_p)$ by Proposition 1.21 (iv). □

Finally we present a set-theoretic theorem of significant importance throughout our work as it ensures that the inverse limits we take are non-empty.

Theorem 1.27. *Let $(X_\lambda, \pi_{\lambda\mu})$ be an inverse system of non-empty compact spaces over a directed set Λ. Then $\varprojlim X_\lambda$ is not empty.*

Proof. Let $P := \prod_{\lambda\in\Lambda} X_\lambda$, and for each finite $S \subseteq \Lambda$ we let

$$L(S) := \{(x_\lambda) \in P \mid \pi_{\mu\lambda}(x_\lambda) = x_\mu \text{ for all } \lambda, \mu \in S\}.$$

Now, for any $(x_\lambda) \in P\backslash L(S)$ there exists $\mu, \nu \in S$ such that $\pi_{\mu\nu}(x_\nu) \neq x_\mu$. But then if $U(T)$ is defined for any finite set $T \subset \Lambda$ as in Theorem 1.24, $(x_\lambda)U(\{\mu, \nu\})$ is open, and obviously $(x_\lambda)U(\{\mu, \nu\}) \cap L(S) = \varnothing$. Hence $P\backslash L(S)$ is open and $L(S)$ is closed.

As Λ is directed there must exists a $\nu \in \lambda$ with $\nu \geq \lambda$ for each $\lambda \in S$ and hence $L(S) \neq \{0\}$. Now choosing any $x_\nu \in X_\nu$ and defining $x_\lambda = \pi_{\nu\lambda}(x_\nu)$ for each $\lambda \in S$ and taking an arbitrary x_λ for $\lambda \notin S \cup \{\nu\}$ then $(x_\lambda) \in L(S)$. By Tychonoff's theorem P is compact and thus

$$L := \bigcap\{L(S) \mid S \text{ is a finite subset of } \Lambda\}$$

is non-empty. But $L = \varprojlim_{\lambda} X_\lambda$ and we have our result. □

Chapter 2

Pro-p Groups

We saw in the previous chapter that generalising the fundamental properties of $\mathbb{Z}_p$ to arbitrary topological groups generates the class of profinite groups. However, $\mathbb{Z}_p$ has many properties that profinite groups in general do not share, and the aim of this chapter is to slowly reduce the classes of groups we are considering so they look more and more like $\mathbb{Z}_p$.

We begin with the fact that $\mathbb{Z}_p$ is an inverse limit of finite p-groups and define the pro-p groups to be those profinite groups sharing this property. Knowing that $\mathbb{Z}_p = \overline{\langle 1 \rangle}$ we then consider those pro-p groups which have a dense subgroup generated by a finite set. The simplest of these being the procyclic groups which, like $\mathbb{Z}_p$, contain a dense subgroup generated by a one element set. Each procyclic group is shown to be homeomorphic to $\mathbb{Z}_p$, and much of the rest of the chapter is devoted to generalising this result.

The powerful pro-p groups defined by Lubotzky and Mann in [LM87b] yield the first of these generalisations in that we show that each finitely generated powerful pro-p group is a product of procyclic groups. This result and those leading toward it are particularly important when it comes to our work on the group algebra of such a group in Chapter 3. Lastly we define the uniform pro-p groups as a further restriction to the class of finitely generated powerful pro-p groups, and show that each is in fact homeomorphic to $\mathbb{Z}_p^d$ for some d. This which is the basis for our work on Theorem A in Chapter 4.

This chapter is based primarily on material from [DSMS91], [Khu97], [LM87a], and [LM87b].

2.1 Finite p-groups

As the inverse limit of a system of finite p-groups, we will see that much of the structure of pro-p groups is a generalisation of that of the finite p-groups, so we begin our discussion here. While finite p-groups form a major part of basic group theory, in terms of Sylow p-subgroups and cyclic groups, it is not these properties that interest us here. Instead we are initially concerned with the fact that each finite p-group is nilpotent, a notion which originated in the theory of Lie Algebras. Nilpotency can be viewed as somewhat a generalisation of a group being abelian. Continuing along these lines we conclude the section by introducing the powerful p-groups, another generalisation of an abelian group.

Definition 2.1. Let G be a finite group. If $|G| = p^n$ for some integer $n > 0$ we say G is a *finite p-group*. Furthermore if $g^p = 1$ for all $g \in G$ we say that G is *elementary*.

Before discussing the useful properties of finite p-groups we establish some of the non-standard group theoretic concepts that are essential to that which follows.

In any group G the *commutator*, $[a, b]$, of two elements $a, b \in G$ is defined by

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

The following basic properties are easily verified:

(C1) $[xy, z] = y^{-1}[x, z]y[y, z]$;
(C2) $[x, yz] = [x, z]z^{-1}[x, y]z$;
(C3) $[x^n, y] = \prod_{i=1}^{n} x^{-(n-i)}[x, y]x^{n-i}$;
(C4) $[x, y^n] = \prod_{i=0}^{n-1} y^{-i}[x, y]y^i$.

It is clear that $[a, b] = 1$ if and only if a and b commute. Also, if we define $[A, B] = \langle [a, b] \mid a \in A, b \in B\rangle$ we see that G is abelian if and only if $[G, G] = \{1\}$. In this sense the commutator tells us where the operation on G fails to be commutative. We call $[G, G]$ the *commutator subgroup* of G. By (C1) above $[G, G] \triangleleft G$ as for any $a, b, g \in G$

$$g^{-1}[a, b]g = [ag, b]([g, b])^{-1} \in [G, G].$$

Also $[G/[G, G], G/[G, G]] = 1_{[G,G]}$ and hence $G/[G, G]$ is abelian. These facts, and many others, are quickly seen also as consequences of the following proposition.

Proposition 2.2. *Let $\phi : G \to H$ be a group homomorphism. Then $\phi([a, b]) = [\phi(a), \phi(b)]$ and thus $\phi([G, G]) \subseteq [H, H]$. Furthermore, if ϕ is onto, $\phi([G, G]) = [H, H]$.*

Proof. For any $a, b \in G$

$$\phi([a, b]) = \phi(a^{-1}b^{-1}ab) = \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)]$$

and so $\phi([a, b]) \in [H, H]$. As $\phi(\{[a, b] \mid a, b \in G\}) \subseteq [H, H]$ and this set generates $[G, G]$ we see that $\phi([G, G]) \subseteq [H, H]$.

Now if ϕ is onto, for all $h, k \in H$ we have $a, b \in G$ such that $\phi(a) = h, \phi(b) = k$. So then $\phi([a, b]) = [h, k]$ and as above, since $\{[h, k] \mid h, k \in H\} \subseteq \phi([G, G])$, $[H, H] = \phi([G, G])$. □

We also require the following commutator identity, which is slightly less obvious than (C1)-(C4) presented above.

Proposition 2.3. *If $x, y \in G$ then $(xy)^n \equiv x^n y^n [y, x]^{n(n-1)/2}$ (mod $[[G, G], G]$).*

Proof. That $[[G,G],G] \lhd G$ follows from Proposition 2.2 as for any $a,b,c,g \in G$

$$g^{-1}[[a,b],c] = [g^{-1}[a,b]g, g^{-1}cg]$$

and $g^{-1}[a,b]g \in [G,G]$ as $[G,G] \lhd G$. It is clear that $[G,G] \leq Z(G/[[G,G],G])$, and that the result holds for $n=1$. If we assume it holds for all $k<n$ then we have that (using (C3))

$$\begin{aligned}(xy)^n = (xy)^{n-1}xy &\equiv x^{n-1}y^{n-1}[y,x]^{(n-1)(n-2)/2}xy \pmod{[[G,G],G]}\\ &\equiv x^n y^n y^{-n}x^{-1}y^{n-1}xy[y,x]^{(n-1)(n-2)/2} \pmod{[[G,G],G]}\\ &\equiv x^n y^n y^{-1}[y^{n-1},x]y[y,x]^{(n-1)(n-2)/2} \pmod{[[G,G],G]}\\ &\equiv x^n y^n [y,x]^{n-1}[y,x]^{(n-1)(n-2)/2} \pmod{[[G,G],G]}.\end{aligned}$$

Hence the result follows by induction. □

Commutator subgroups are used extensively throughout this chapter, but our initial application is in defining what it means for a group to be nilpotent.

Definition 2.4. For any group G the *lower central series* of G is defined recursively by

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

We say G is *nilpotent* if $\gamma_k(G) = \{1\}$ for some integer $k>0$. If c is the smallest positive integer such that $\gamma_{c+1}(G) = \{1\}$ then we say that G is *nilpotent of class* c. If $G = \{1\}$ then G is nilpotent of class 0.

It is clear from the definition that $\gamma_c(G) \subseteq Z(G)$ for any nilpotent group of class c. We also have:

Corollary 2.5. *For any group G, $\gamma_k(G) \lhd G$ for all integers $k>0$. Also if G is nilpotent of class c then $G/\gamma_k(G)$ is nilpotent of class $k-1$ for all $1 \leq k \leq c+1$.*

Proof. By the discussion above we have that $\gamma_1(G), \gamma_2(G) \lhd G$. We proceed then by induction, supposing that $\gamma_j(G) \lhd G$ for all $j<k$. For any $a \in \gamma_k(G)$ we know that $a=[b,c]$ for some $b \in \gamma_{k-1}(G)$, $c \in G$. So for any $g \in G$ we have, by Proposition 2.2,

$$g^{-1}ag = [g^{-1}bg, g^{-1}cg].$$

However, our inductive assumption tells us that $g^{-1}bg \in \gamma_{k-1}(G)$ and clearly $g^{-1}cg \in G$, and hence $g^{-1}ag \in \gamma_k(G)$. Thus $\gamma_k(G) \lhd G$ for all integers $k>0$.

Now we consider the quotient group $G/\gamma_k(G)$ of a nilpotent G (of class c) for any $k \in \{1,\ldots,c+1\}$. It is clear that for any $a,b \in G$

$$[a\gamma_k(G), b\gamma_k(G)] = [a,b]\gamma_k(G)$$

and it follows that $\gamma_k(G/\gamma_k(G)) = \{1\}$. Thus $G/\gamma_k(G)$ is nilpotent of class at most $k-1$. Now if $\gamma_{k-1}(G/\gamma_k(G)) = \{1\}$ it would follow that $\gamma_{k-1}(G) = \gamma_k(G)$. This would clearly defy the nilpotency of G and hence $G/\gamma_k(G)$ must be nilpotent of class $k-1$. □

Nilpotent groups are often thought of as a generalisation of abelian groups as they are, in the sense of the above definition, on a finite number of 'steps' away from being abelian. One of the benefits of working with the abelian groups is that every subgroup is automatically normal. While such a strong result does not apply here, we are guaranteed a wide supply of normal subgroups in any finite nilpotent group.

Proposition 2.6. *If G is a finite nilpotent group and $1 < N \triangleleft G$ then there is a maximal subgroup M of N such that $M \triangleleft G$.*

Proof. We begin by showing that if N is any normal subgroup $Z(G) \cap N \neq 1$. As G is nilpotent, there must exist a k such that $\gamma_k(G) \cap N \neq 1$ and $\gamma_{k+1}(G) \cap N = 1$. Then $\gamma_k(G) \cap N \leq Z(G) \cap N$ and so $\mathbb{Z}(G) \cap N \neq 1$.

Now, taking any $N \triangleleft G$, if $Z(G) \cap N = N$ (that is $[N, G] = 1$) then any maximal subgroup of G would be normal. Otherwise we assume $Z(G) \cap N \neq N$ and the result holds for all subgroups of order less than N. Then, as $[N, G] \triangleleft G$, the remark above gives us that $1 < [N, G] \cap Z(G) = K < N$ and hence $1 < N/K \triangleleft G/K$. By our inductive hypothesis we have some maximal $M \leq N$ such that $M/K \triangleleft G/K$, and so M is normal in G. □

We now return our focus to p-groups, establishing the following important results.

Lemma 2.7. *The center of a finite p-group is non-trivial.*

Proof. This follows directly from the class equation

$$|G| = |Z(G)| + \sum_i [G : C_G(g_i)]$$

where g_i are representatives of the conjugacy classes of G not contained in the center (and $C_G(g_i) = \{x \in G \mid xg_i = g_i x\}$ is the centraliser of g_i in G). □

Proposition 2.8. *If G is a finite p-group of order p^a then G is nilpotent of class at most $a - 1$.*

Proof. If G is abelian the proposition is obvious. Assuming then that G is not abelian the lemma above gives us that $\{1\} \neq Z(G) \triangleleft G$. Hence $G/Z(G)$ is a finite p-group (though not G) and so $Z(G/Z(G)) \neq \{1\}$. Let $Z_0(G) = 1$, $Z_1(G) = Z(G)$, and define $Z_{i+1}(G)$ by

$$Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G).$$

As each $G/Z_i(G)$ is either a finite p-group, or $\{1\}$, we know that $Z_{i+1}(G) \geq Z_i(G)$, and as G is finite we are assured that for some $b \leq a$, $Z_i(G) = G$ for all $i \geq b$. Hence $G/Z_{b-1}(G)$ is abelian and so $[G, G] \leq Z_{b-1}(G)$. Then, as $Z_{b-1}(G)/Z_{b-2}(G) = Z(G/Z_{b-2}(G))$ it follows that $\gamma_3(G) = [[G, G], G] \leq Z_{b-2}(G)$. Continuing along these lines we have that $\gamma_b(G) = \{1\}$ and it follows that G is nilpotent of class at most a. That G cannot be nilpotent of class a follows from the fact that every finite p-group of order p^2 is abelian ([DF04] Corollary 4.9). □

This series of centers

$$1 = Z_0(G) \leq Z_1(G) \leq \ldots \leq Z_n(G) \leq \ldots$$

is called the *upper central series* and what the above proof effectively shows is that the upper central series and lower central series have the same length in a nilpotent group. That is, if G is of nilpotency class c then $Z_{c+1}(G) = G$ and $Z_c(G) < G$.

Proposition 2.9. *If M is a maximal subgroup of a finite p-group G then $M \lhd G$ and $[G : M] = p$.*

Proof. We argue by induction on n where $|G| = p^n$. Clearly the result holds for $n = 1$. Now, let M be a maximal subgroup of G where G is an arbitrary finite p-group. As $Z(G) \neq \{1\}$ there exists a $z \in Z(G)$ of order p. If $z \notin M$ then $M \langle z \rangle = G$ and hence $M \lhd G$ and $[G : M] = p$. Otherwise $z \in M$ implying that $M/\langle z \rangle$ is a maximal proper subgroup of $G/\langle z \rangle$ and the result follows by induction. □

Many of the essential properties of pro-p groups are related to certain properties of the subgroup formed by intersecting all maximal open subgroups; the Frattini subgroup. This is an extension of the Frattini subgroup of finite groups, a notion developed analogous to the radical of a Lie algebra.

Definition 2.10. The *Frattini subgroup* of a finite group G is the intersection of all maximal subgroups

$$\Phi(G) = \bigcap \{M \mid M \text{ maximal subgroup of } G\}.$$

Clearly if G is a finite p-group $\Phi(G) \lhd G$. In fact in any group G the Frattini subgroup is characteristic and hence normal. The two parts of the next result give alternate characterisations of the Frattini subgroup, both of which being extended to pro-p groups in the next section. While the first is based solely on the definition, the second draws upon the previous proposition on normal subgroups in finite p-groups.

Proposition 2.11.

(i) For any group G the Frattini subgroup is exactly the set of non-generating elements of G. That is, for any $g \in G$, $g \in \Phi(G)$ if and only if $X \backslash \{g\}$ generates G for each generating set X of G containing g.

(ii) If G is a finite p-group then $\Phi(G) = G^p[G, G]$. Recall $G^p = \langle g^p \mid g \in G \rangle$.

Proof. (i): Suppose $g \notin \Phi(G)$, that is there exists a maximal subgroup M such that $g \notin M$. Then $\langle M, g \rangle = G$ and $\langle M \rangle = M$. Thus $g \in \Phi(G)$ for any non-generating element $g \in G$. Conversely suppose $g \in \Phi(G)$, and $\langle \alpha_1, \ldots, \alpha_n, g \rangle = G$ and $g \notin \langle \alpha_1, \ldots, \alpha_n \rangle$. Suppose M is a proper maximal subgroup containing $\langle \alpha_1, \ldots, \alpha_n \rangle$. Since $g \in M$ however, $M \geq \langle \alpha_1, \ldots, \alpha_n, g \rangle = G$ and so is not proper. Hence $\langle \alpha_1, \ldots, \alpha_n \rangle = G$.

(ii): If we have any maximal subgroup M of G we know by Proposition 2.9 that $M \lhd G$ and $|G/M| = p$. Thus, as G/M is abelian, $M \geq [G, G]$, and as each element

of G/M has order p, $M \geq G^p$. Hence $\Phi(G) \geq G^p[G,G]$. Now, as $G/G^p[G,G]$ is an elementary abelian p-group, it is generated by some n elements in G (assuming $|G| = p^n$), say $\mathcal{G} = \{g_1, \ldots, g_n\}$. It follows that $M_i = \langle \mathcal{G} \backslash \{g_i\} \rangle$ is maximal for all i and so $\Phi(G/G^p[G,G]) = \{1\}$. The reverse inequality follows. □

We now turn to the powerful finite p-groups defined in [LM87a]. In many ways the condition on powerful p-groups is one assuring that they are closer to being abelian than finite p-groups in general. Directly from the definition we see that $ab \equiv ba \pmod{G^p}$ for all $a, b \in G$, and in the last section of the chapter we extend this and see that $ab \equiv ba$ modulo pth powers of elements in G.

Definition 2.12. A finite p-group G is said to be *powerful* if G/G^p is abelian. A subgroup H of a finite p-group is said to be *powerfully embedded* in G, written H p.e. G, if $H^p \geq [H,G]$.

Clearly any H p.e. G is normal in G as, for any $h \in H$, $g \in G$

$$g^{-1}hg = h[h,g] \in H.$$

Also a group G is powerful if and only if $\Phi(G) = G^p$, and any powerfully embedded subgroup is powerful as $[H,H] \leq [H,G] \leq H^p$. In this sense being powerfully embedded in a larger subgroup is a stronger condition than being powerful. We list some elementary, but useful, properties of these groups below.

Proposition 2.13. *If G is a finite p-group, N, K, and W are normal subgroups of G, and $N \leq W$ then*

(i) If N p.e. G then NK/K p.e. G/K.
(ii) If $K \leq N^p$ then N p.e. G if and only if N/K p.e. G/K.
(iii) If N p.e. G and $x \in G$ then $\langle N, x \rangle$ is powerful.
(iv) If N is not powerfully embedded in W then there exists $J \lhd G$ such that $N^p[[N,W],W] \leq J \leq N^p[N,W]$ and $[N^p[N,W] : J] = p$.

Proof. If N p.e. G then for all $nK \in NK/K$ and $gK \in G/K$ we have $[nK, gK] = [n,g]K = mK$ for some $m \in N^p$ from which we have (i). Suppose now that $K \leq N^p$ and N/K p.e. G/K. Then for any $n \in N$, $g \in G$ we have that $[n,g] \in N^pK = N^p$ and hence N p.e. G and (ii) follows. Now, in (iii), let $H = \langle N, x \rangle$. As $N \lhd G$ we have that $[H,H] = [N,H] \leq [N,G] \leq N^p \leq H^p$. Thus $H = \langle N, x \rangle$ is powerful.

Lastly, for (iv), let $M = N^p[N,W] \neq N^p$. As G is a p-group, so is M, and thus there exists a (maximal) $J \lhd M$ such that $N^p \leq J$ and $[M : J] = p$. Also, as $M \lhd G$ and J is maximal in M we can assume (by Proposition 2.6) that $J \lhd G$. Finally, M/J being central in G/J implies that

$$N^p[[N,W],W] \leq J \leq N^p[N,W]$$

completing the proof. □

Corollary 2.14. *If G is a finite p-group and $N \leq G$ then if N p.e. G then N^p p.e. G.*

Proof. This proof is mostly just manipulation of commutator products. By (iv) above, if N^p does not powerfully embed in G we have a $J \triangleleft G$ such that

$$(N^p)^p[[N^p, G], G] \leq J \text{ and } [(N^p)^p[N^p, G] : J] = p.$$

It follows then by (ii) above that we can assume (by reducing modulo J) that $(N^p)^p[[N^p, G], G] = \{1\}$. That is $(N^p)^p = [[N^p, G], G] = \{1\}$ implying that $[N^p, G] \leq Z(G)$ and thus as N p.e. G, $[[N, G], G] \leq Z(G)$. Hence, by (C2), the map $w \mapsto [[x, g], w]$ from G to $Z(G)$ is a homomorphism for any $x \in N$, $g \in G$. This, (C3), and the fact that $[[N, G], G] \leq Z(G)$ imply

$$\begin{aligned}
[x^p, g] &= \prod_{i=1}^{p} x^{-(p-i)}[x, g]x^{p-i} \\
&= \prod_{i=1}^{p} [x, g][[x, g], x^{p-i}] \\
&= \prod_{i=1}^{p} [x, g][[x, g], x]^{p-i} \\
&= [x, g]^p[[x, g], x]^{p(p-1)/2} = 1.
\end{aligned}$$

Thus $[N^p, G] \leq (N^p)^p$, contradicting our assumption and so N^p p.e. G as required. □

It is clear from the definition that any abelian finite p-group is powerful, though an example of a finite p-group that is not powerful is not immediately obvious. We mention the following example taken from [MM07].

Example 2.15. [A finite p-group that is not powerful.]

For any positive integers $s \geq t$ the finite p-group

$$P_{s,t} = \left\langle y_1, \ldots, y_d \mid y_i^{p^s} = [y_j, y_k]^{p^t} = [[y_i, y_j], y_k] = 1, i, j, k \in \{1, \ldots, d\}, j \neq k \right\rangle$$

is not powerful. □

We do, however, have the following theorem from Mann and Posnick-Fradkin [MPF03].

Theorem 2.16. *Every finite p-group is isomorphic to a section of a powerful finite p-group. That is for any finite p-group G there exists a powerful finite p-group P containing subgroups N and H such that $N \triangleleft H$ and $G \cong H/N$.*

Finally we present a proposition which we require later that shows how we can express the commutator subgroup of a finitely generated nilpotent group in a convenient way in terms of its generators.

Proposition 2.17. *If H is any nilpotent group generated by $\{a_1, \ldots, a_n\}$ then $[H, H] = \{[h_1, a_1] \ldots [h_n, a_n] \mid h_1, \ldots, h_n \in H\}$.*

Proof. Note first that if H is of nilpotency class c and $u \in \gamma_{c-1}(H)$ then, as $\gamma_c(H) \subseteq Z(H)$, for any $a, b \in G$

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

and so by induction $[u, a^n] = [u, a]^n = [u^n, a]$.

Now, for any $h \in H$ we have $h = \prod_j^m b_j$ with $b_j = a_i$ for some $i \in \{1, \ldots, n\}$, and setting e_i to be the number of times a_i occurs in the product,

$$[u, h] = [u^{e_1}, a_1] \ldots [u^{e_d}, a_d].$$

Thus for any $w \in \gamma_c(H)$ there exists $w_1, \ldots, w_d \in \gamma_{c-1}(H)$ such that

$$w = [w_1, a_1] \ldots [w_n, a_n].$$

Trivially the result holds for $c = 1$ and so proceeding by induction we assume it holds for all nilpotent groups of class $k < c$. Then if H is nilpotent of class c, any $h \in [H, H]$ satisfies

$$h \equiv [y_1, a_1] \ldots [y_n, a_n] \pmod{\gamma_c(H)}$$

for some $y_1, \ldots, y_n \in H$. However, by the above we know that any $w \in \gamma_c(H)$ can be written as $w = [w_1, a_1] \ldots [w_n, a_n]$ for some $w_1, \ldots, w_n \in \gamma_{c-1}(H)$. So there exists $w \in \gamma_c(H)$ such that

$$\begin{aligned} h &= [y_1, a_1] \ldots [y_n, a_n]w \\ &= [y_1, a_1] \ldots [y_n, a_n][w_1, a_1] \ldots [w_n, a_n] \\ &= \prod_{i=1}^{d} y_i^{-1}[w_i, a_i]y_i[y_i, a_i] \\ &= [w_1y_1, a_1] \ldots [w_dy_d, a_d]. \end{aligned}$$

Noting that the above follows from the fact that $\gamma_c(H) \subseteq Z(H)$ we have our result by induction. □

2.2 Pro-p groups

As mentioned prior, the pro-p groups are the first step in our attempt to generalise $\mathbb{Z}_p$ adequately. Being the inverse limit of a system of finite p-groups we expect similarities to occur and this is most obvious in the characterisation of the Frattini subgroup of a pro-p group

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

While this does not seem like a particularly important result it leads to some startling discoveries. Firstly that a pro-p group has a dense finitely generated subgroup if and only if $\Phi(G)$ is open, and secondly that if $\Phi(G)$ is open, any subgroup of finite index is open. The latter result in particular has some startling consequences which much of this section builds up to.

Before defining the notion of a pro-p group we establish some more properties of profinite groups.

Proposition 2.18. *For any profinite group G we have, for any subset X of G,*

$$\overline{X} = \bigcap_{N \lhd_o G} XN.$$

Furthermore, if X is a subgroup of G then

$$\overline{X} = \bigcap \{K \mid X \leq K \leq_o G\}.$$

Proof. For each $N \lhd_o G$, $[G : N] < \infty$ and thus there exists a finite $S_N \subseteq X$ such that

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

It follows that $XN \subseteq_c G$ for each N and so

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

To see the reverse inclusion, take any $y \in \bigcap_{N \lhd_o G} XN$. 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 the open normal subgroups form a base for the neighbourhoods of the identity in G, for any neighbourhood M of y there exists $N \lhd_o G$ such that $yN \subseteq M$. Hence the net $\{x_N\}$ clearly converges to y and $y \in \overline{X}$.

Now if $X \leq G$ then clearly

$$\overline{X} \subseteq \bigcap \{K \mid X \leq K \leq_o G\}.$$

However, by the above $\overline{X} = \bigcap_{N \lhd_o G} XN$ and each $XN \leq_o G$ so the reverse inclusion is also clear. □

We also have the following result concerning the convergence of sequences of elements in the profinite topology.

Proposition 2.19. *If G is a profinite group then a sequence $\{g_i\} \subseteq G$ converges if and only if for each $N \lhd_o G$ there exists $n = n(N)$ such that $g_i^{-1} g_j \in N$ for all $i, j \geq n$ (such a sequence is called Cauchy).*

Proof. Suppose (g_i) is a Cauchy sequence. If (g_i) contains only finitely many terms then define $C_n := \{g_i^{-1} g_j \mid i, j \geq n\}$, a finite set for all n. Suppose, for every $n > 0$ there exists $1 \neq a \in C_n$. But then it would follow that $a \in N$ for all $N \lhd_o G$ contradicting $\bigcap_{N \lhd_o G} N = \{1\}$. Hence, there exists an n such that $C_n = \{1\}$ and it follows that g_i is constant for all $i \geq n$.

Otherwise, $\{g_i \mid i \in \mathbb{N}\}$ is an infinite set and has a limit point g in the compact space G. Now take any $N \lhd_o G$. The neighbourhood gN of g must contain infinitely many of the g_i's, and hence there exists $i \geq n(N)$ such that $g_i \in gN$. As for all $j \geq n(N)$, $gN = g_i N = g_j N$ we have also $g_j \in gN$. Thus if M is any neighbourhood

of g we take $N \lhd_o G$, such that $N \subseteq g^{-1}M$, and see $g_i \in N \subset g^{-1}M$ for all $i \geq n(N)$. Hence g_i converges to g.

Conversely, suppose (g_i) converges, say to $g \in G$. Then for any $N \lhd_o G$, there exists $n(N)$ such that $g_i \in gN$ for all $i \geq n(N)$. It follows that $g_iN = gN$ for all $i \geq n(N)$ and hence $g_iN = g_jN$ for all $i, j \geq n(N)$ as required. □

Definition 2.20. A profinite group G is said to be a *pro-p group* if every $N \lhd_o G$ satisfies $[G : N] = p^n$ for some n.

It is clear then that every open subgroup has finite index as if $O \leq_o G$ then there exists normal $N \leq_o O$ and hence $[G : O]$ divides $[G : N] = p^n$. In the same vain, it is often much easier to show that a profinite group is a pro-p group by showing each member of a family of open subgroups forming a base for the neighbourhoods of the identity has pth power index in G. That the p-adic numbers are a pro-p group can hence be seen as $\mathbb{Z}_p/p^i\mathbb{Z}_p \cong \mathbb{Z}/p^i\mathbb{Z}$ (Proposition 1.13) and $\{p^i\mathbb{Z}_p\}$ is a base for the neighbourhoods of the identity. The same techniques are applied to the more in depth examples below.

Example 2.21. [$GL_n(\mathbb{Z}_p)$ is not a pro-p group.]

We saw in Section 1.3 that both $SL_n(\mathbb{Z}_p)$ and $GL_n(\mathbb{Z}_p)$ are profinite groups, however, neither are pro-p groups. In $GL_n(\mathbb{Z}_p)$ we have the open normal subgroups $\Gamma_i = \{g \in GL_n(\mathbb{Z}_p) \mid g \equiv 1_n \pmod{p^i}\}$. Now each of these subgroups is the kernel of the natural projection $GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{Z}/p^i\mathbb{Z})$ and hence

$$GL_n(\mathbb{Z}_p)/\Gamma_i \cong GL_n(\mathbb{Z}/p^i\mathbb{Z}).$$

It is also well known that when $\mathbb{F}$ is a finite field (of order q say) $|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$ ([DF04] Example page 413). Thus $[GL_n(\mathbb{Z}_p) : \Gamma_1] = |GL_n(\mathbb{F}_p)|$ is not a pth power, and so $GL_n(\mathbb{Z}_p)$ is not a pro-p group. Similarly it can be shown that $SL_n(\mathbb{Z}_p)$ is not a pro-p group. □

Example 2.22. [Γ_1 and Γ_1^* are both pro-p groups.]

While $GL_n(\mathbb{Z}_p)$ and $SL_n(\mathbb{Z}_p)$ are not a pro-p groups, it turns out that Γ_1 and $\Gamma_1^* := \{g \in SL_n(\mathbb{Z}_p) \mid g \equiv 1_n \pmod{p}\}$ are. Beginning with Γ_1 we note that for any $a \in M_n(\mathbb{Z}_p)$, $1 + pa$ is invertible (that is, $1 + pa \in GL_n(\mathbb{Z}_p)$). We then consider Γ_1/Γ_i. Clearly, $\{(1 + pa)\Gamma_i \mid a \in M_n(\mathbb{Z}_p),\ a \equiv 0 \pmod{p^{i-1}}\}$ is contained in Γ_1/Γ_i, and we show that it is in fact all of Γ_1/Γ_i. Take any $g \in \Gamma_1$ such that $g = 1+pa+p^ib$ where $a, b \in M_n(\mathbb{Z}_p)$ and $a \equiv 0 \pmod{p^{i-1}}$. But then

$$\begin{aligned}(1 + pa)(1 + p^i(1 + pa)^{-1}b) &= 1 + pa + p^i(1 + pa)^{-1}b + p^{i+1}a(1 + pa)^{-1}b \\ &= 1 + pa + p^i(1 + pa)(1 + pa)^{-1}b \\ &= 1 + pa + p^ib.\end{aligned}$$

So $\Gamma_1/\Gamma_i = \{(1 + pa)\Gamma_i \mid a \in M_n(\mathbb{Z}_p),\ a \equiv 0 \pmod{p^i}\}$ and hence $[\Gamma_1 : \Gamma_i] = p^{n^2(i-1)}$. Now as the family $\{\Gamma_i\}$ is a base for the neighbourhoods of the identity, if we take any $N \lhd_o \Gamma_1$, there exists i such that $\Gamma_i \leq N$. Thus $[\Gamma_1 : N] \mid [\Gamma_1 : \Gamma_i]$ and it follows that Γ_1 is a pro-p group.

As $\Gamma_1^* \leq \Gamma_1$ and $\Gamma_1^* \lhd_o SL_n(\mathbb{Z}_p)$ it follows that $\Gamma_1^* \lhd_c \Gamma_1$. By Proposition 1.21 (iv) then, Γ_1^* is a profinite group and any $H \leq_o \Gamma_1^*$ satisfies $H = B \cap \Gamma_1^*$ for some $B \leq_o \Gamma_1$. As for any group G with normal subgroup N and subgroup S

$$[G : S] = [G/N, SN/N][N : N \cap S]$$

we have that $[\Gamma_1^* : H]$ divides $[\Gamma_1 : B]$ and hence is of pth power order. That is, Γ_1^* is a pro-p group as required. □

The last paragraph of the example above can be obviously generalised to show that any closed subgroup of a pro-p group is itself a pro-p group. We now present the much quoted characterisation of pro-p groups in terms of inverse limits of finite p-groups.

Proposition 2.23. *A topological group is a pro-p group if and only if it is the inverse limit of an inverse system of finite p-groups.*

Proof. If G is a pro-p group, then it is profinite and hence $G \cong \varprojlim (G/N)_{N \lhd_o G}$ where $|G/N| = [G : N] = p^n$ for some n.

Conversely suppose $G = \varprojlim (G_\lambda)_{\lambda \in \Lambda}$ where each G_λ is a finite p-group. By the definition of the product topology we know that every open subgroup of G contains the subgroup

$$G(S) = G \cap \Big(\prod_{\lambda \notin S} G_\lambda \times \prod_{\lambda \in S} \{1\} \Big)$$

for some finite $S \subseteq \Lambda$. Now taking any $N \lhd_o G$ and letting

$$\hat{G} = \prod_{\lambda \in \Lambda} G_\lambda$$

we see that $[G : N][N : G(S)] = [G : G(S)]$ and $[\hat{G} : G][G : G(S)] = [\hat{G} : G(S)]$ so

$$[G : N] \big| [\hat{G} : G(S)] = \prod_{\lambda \in S} |G_\lambda|$$

and hence $[G : N] = p^n$ for some n. We have G is profinite by Theorem 1.24 and thus G is pro-p as required. □

It is natural then to extend the notion of a powerful finite p-group to the pro-p groups.

Definition 2.24. Let G be a pro-p group.

(i) G is *powerful* if $G/\overline{G^p}$ is abelian.
(ii) Let $N \leq_o G$. N is *powerfully embedded* in G (written N p.e. G) if $[N, G] \leq \overline{N^p}$.

As with powerful finite p-groups we have that G is powerful if and only if $[G, G] \leq \overline{G^p}$ and that any N p.e. G is normal in G and powerful.

Example 2.25. [Γ_1^* is powerful.]

We saw in Example 2.22 that Γ_1^* is a pro-p group and in fact it turns out to be powerful. It is quite clear for any $g = 1 + pa$ and $h = 1 + pb$ in Γ_1^* we have that

$$gh = (1 + pa)(1 + pb) = 1 + pa + pb + p^2ab$$

and so modulo Γ_2^*, $gh = hg$ (where $\Gamma_i^* = \Gamma_i \cap SL_n(\mathbb{Z}_p)$). Hence $[\Gamma_1^*, \Gamma_1^*] \leq \Gamma_2^*$. Also, by the binomial theorem we have

$$g^p = (1 + pa)^p = 1 + p^2c$$

for some $c \in M_n(\mathbb{Z}_p)$ (such that $1 + p^2c \in SL_n(\mathbb{Z}_p)$). So we have $(\Gamma_1^*)^p \leq \Gamma_2^*$. The same calculation in fact shows us that $(\Gamma_{i-1}^*)^p \leq \Gamma_i^*$.

Claim: For each i, $\Gamma_i^* = (\Gamma_{i-1}^*)^p = \{g^p \mid g \in \Gamma_{i-1}^*\}$.

To establish the claim it suffices to show that each element of Γ_i^* is a pth power of an element in Γ_{i-1}^*. In fact we will demonstrate that the equation

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

has a solution for all $a \in M_n(\mathbb{Z}_p)$. Now, $1 + p^n a \equiv (1 + p^{n-1}a)^p \pmod{p^{n-1}}$, so proceeding by induction assume there exists x_r commuting with a such that

$$(1 - p^{n-1}x_r)^p = 1 + p^n a + p^{n+r}c.$$

Then x_r and a commute with c (as $p^{n+r}c$ is a sum of powers of a and x_r), and so defining

$$x_{r+1} = x_r - p^r(1 + p^{n-1}x_r)^{-(p-1)}c$$

it is clear that x_{r+1} commutes with a. Noting that $1 + p^{n-1}x_r$ invertible and so x_{r+1} is well defined we see

$$\begin{aligned}(1 + p^{n-1}x_{r+1})^p &= \big((1 + p^{n-1}x_r) - p^{n+r-1}(1 + p^{n-1}x_n)^{-(p-1)}c\big)^p \\ &\equiv (1 + p^{n-1}x_r)^p - p^{n+r}c \pmod{p^{n+r+1}} \\ &\equiv 1 + p^n a \pmod{p^{n+r+1}}.\end{aligned}$$

Hence we have a convergent sequence in $M_n(\mathbb{Z}_p)$ which converges to some limit x. It is clear that $1 + p^{i-1}x$ is invertible and as $\det(1 + p^{i-1}x)^p = \det(1 + p^i a) = 1$, $1 + p^{i-1}x \in \Gamma_{i-1}^*$ as required.

Thus in the case where $i = 2$, $(\Gamma_1^*)^p = \Gamma_2^* \geq [\Gamma_1^*, \Gamma_1^*]$, and Γ_1^* is a powerful pro-p group. □

The following proposition allows us to reduce to the finite p-groups in establishing whether or not a subgroup of G is powerful.

Proposition 2.26. *Let G be a pro-p group and $N \leq_o G$ then N p.e. G if and only if NK/K p.e. G/K for all $K \lhd_o G$.*

Proof. If N p.e. G then $[G, N] \leq \overline{N^p} = \bigcap_{K \lhd_o G} N^p K$ (Proposition 2.18). Hence for all $K \lhd_o G$, $N^p K \geq [N, G]$ and it follows that NK/K p.e. G/K. Conversely,

supposing NK/K p.e. G/K for all $K \lhd_o G$, then $N^pK/K \geq [NK/K, G/K]$ implying that $N^pK \geq [NK, G] \geq [N, G]$. Thus N p.e. G as

$$\overline{N^p} = \bigcap_{K \lhd_o G} N^pK \geq [N, G].$$

□

One consequence of the above proposition is that if G is a powerful pro-p group then G/N is powerful for all N. That is, G is the inverse limit of a system of *powerful* finite p-groups. Below we see that the inverse limit of every such system yields a powerful pro-p group.

Corollary 2.27. *A pro-p group G is powerful if and only if it is the inverse limit of a system of powerful p-groups in which all the maps are surjective.*

Note that here we have the added requirement that the maps in the inverse system are surjective. This is a condition we could have asserted in Propositions 1.24 and 2.23 as is done in [RZ00]. However, any subgroup of a finite group is finite and every subgroup of a finite p-group is a finite p-group. Similarly, when dealing with procyclic groups in the following section, every subgroup of a finite cyclic group is cyclic. The distinction here is necessary as a subgroup of a powerful p-group may not be powerful.

Proof. Suppose that G is the inverse limit of the system $(G_\lambda, \phi_{\lambda\mu})_\Lambda$ where each G_λ is a powerful finite p-group and each $\phi_{\lambda\mu}$ is surjective. By Proposition 2.23 G is a pro-p group, so it remains to show it is powerful. Given any $K \lhd_o G$ we have that (for some finite subset S of Λ)

$$G/N \cong G \cap \Big(\prod_{\lambda \in S} Q_\lambda \times \prod_{\lambda \in \Lambda \setminus S} G_\lambda \Big)$$

where for each $\lambda \in S$, Q_λ is a quotient of G_λ. Then, letting T be the set of all maximal elements of S we have that (as all the maps are surjective) $G/K \cong \prod_{\lambda \in T} Q_\lambda$. Each Q_λ is a powerful finite p-group by Proposition 2.13 and it is easy to see that their product must be powerful, and so by the proposition above G is powerful as required. □

For any pro-p group G we define the Frattini subgroup of G by

$$\Phi(G) := \bigcap \{M \mid M \text{ is a maximal proper open subgroup of } G\}.$$

Recalling that each open subgroup of G is closed in G it is clear that $\Phi(G) \leq_c G$. The Frattini subgroup is also normal in G as, for any $g \in G$, $\psi : G \to G$ defined by $x \mapsto g^{-1}xg$ is a homeomorphism (by Proposition 1.22), and clearly then maximal open subgroups are mapped to maximal open subgroups by both ψ and ψ^{-1}. That is $\psi(\Phi(G)) = \Phi(G)$. Similarly, it is easy to see that if $K \lhd_c G$ and $K \leq \Phi(G)$ then $\Phi(G/K) = \Phi(G)/K$ as the maximal open subgroups in G/K are in 1-1 correspondence with the maximal open subgroups in G (as each contains K).

It was shown in the previous section that the Frattini subgroup of a finite group is the set of non-generating elements. We can show a similar equivalence for the Frattini subgroup of a pro-p group G but first need a definition.

Definition 2.28. If G is a topological group G is said to be *topologically generated* by $\{a_1, \ldots, a_n\}$ if $G = \overline{\langle a_1, \ldots, a_n \rangle}$.

Proposition 2.29. *For any pro-p group G the following are equivalent:*

(i) *X generates G topologically;*
(ii) *$X \cup \Phi(G)$ generates G topologically;*
(iii) *$X\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$ topologically.*

Proof. Clearly (i) implies (ii) and (ii) implies (iii). Assume then that $X\Phi(G)/\Phi(G)$ is a topological generating set for $G/\Phi(G)$ and $\overline{\langle X \rangle} \neq G$. Taking any $H \leq_o G$, such that $X \subseteq H$ (and thus $\langle X \rangle \subseteq H$), if $H \neq G$ then there exists a maximal proper open subgroup M such that $H \leq M$. It is clear that $\overline{\langle X \rangle}\Phi(G)/\Phi(G) \leq M/\Phi(G)$ which is not all of $G/\Phi(G)$, contradicting (iii). Hence $H = G$ for all open subgroups containing X and so (by Proposition 2.18) $\overline{\langle X \rangle} = G$ as required. □

Hence the Frattini subgroup of a pro-p group G is precisely the set of non-topologically generating elements of G. We also have the corresponding result to (ii) in Proposition 2.11.

Proposition 2.30. *If G is pro-p group $\Phi(G) = \overline{G^p[G,G]}$. Furthermore, if G is powerful $\Phi(G) = \overline{G^p}$.*

Proof. If M is a maximal open proper subgroup of G there is some $N \lhd_o G$ contained in M by Proposition 1.21. If follows that M/N is a maximal subgroup in the finite p-group G/N. As G/N is a finite p-group, M/N is normal and has index p. So $M \lhd G$ and $[G : M] = [G/N : M/N] = p$. Thus G/M is abelian and so $[G, G] \leq M$ and $G^p \leq M$. Hence we have

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

but as $\Phi(G)$ is closed we obtain $\Phi(G) \geq \overline{G^p[G, G]}$.

Now we consider $Q = G/\overline{G^p[G, G]}$, which is a pro-$p$ group by the comment after Example 2.22, and thus its open normal subgroups intersect in the identity. If we take any $N \lhd_o Q$, Q/N is a finite elementary abelian p-group, and thus its maximal subgroups intersect in the identity ($\Phi(Q/N) = 1$), thus $\Phi(Q) \subseteq N$. It follows that $\Phi(Q) \leq \bigcap_{N \lhd_o Q} N = \{1\}$, and thus as we know that $\overline{G^p[G, G]} \leq \Phi(G)$ we have $\{1\} = \Phi(Q) = \Phi(G)/\overline{G^p[G, G]}$, and we are done. The result for powerful pro-p groups is obvious then from the definition. □

We now turn to consider those pro-p groups which contain a dense subgroup generated by a finite set.

Definition 2.31. A pro-p group G is said to be *finitely generated* if G is topologically generated by a finite set of elements, $\{a_1, \ldots, a_n\} \subseteq G$. That is, if

$$G = \overline{\langle a_1, \ldots, a_n \rangle}.$$

If G can be topologically generated by a one element subset, G is said to be *procyclic*.

We know that an arbitrary (not necessarily topological) group can be generated by a finite set and have a subgroup which is cannot be generated by a finite set, but that a subgroup of finite index is finitely generated. We have a similar result for the topological generating sets in pro-p groups.

Proposition 2.32. *Let G be a finitely generated pro-p group, then every open subgroup $H \leq_o G$ is finitely generated.*

Proof. Let X be a finite topological generating set for G, and assume (without loss of generality) that $\{x^{-1} \mid x \in X\} = X$. Let $H \leq_o G$, and let T be a right transversal of H in G such that $1 \in T$. For each $x \in X$ and $t \in T$ there exists $s = s(t, x) \in T$ such that $Htx = Hs$. We put

$$Y = \{tx.s(t, x)^{-1} \mid t \in T, x \in X\}$$

and claim Y generates H topologically (note that $Y \subset H$ as $Hxt = Hs$ by definition and so $Hstx^{-1} = H$).

Consider the subgroup $M = \overline{\langle Y \rangle}$ of G. If $a \in M, t \in T$, and $x \in X$, then

$$at \cdot x = atxs(t, x)^{-1} \cdot s(t, x) \in MT;$$

so $MTX = MT$. Since $1 \in MT$ and $X = X^{-1}$, it follows that $MT \supseteq \langle X \rangle$. As T is finite, $MT = \bigcup_{t \in T} Mt$ is a finite union of closed sets and is thus closed. Therefore $MT = G$. See then $H = G \cap H = MT \cap H$. But for any $mt \in MT \cap H$, $mt = h$ for some $h \in H$. It follows that $t = m^{-1}h \in H$ (as $M \leq H$ clearly as H is closed), so $t = 1$ and thus $H = M$ as claimed. As X and T are clearly finite the result is established. □

We find that we can completely characterise which groups are finitely generated by the index of the Frattini subgroup.

Proposition 2.33. *For any pro-p group G the following are equivalent:*

(i) *G is finitely generated;*
(ii) *$\Phi(G)$ is open;*
(iii) *$[G : \Phi(G)] = p^n$ for some positive integer n.*

Proof. Suppose that $G = \overline{\langle X \rangle}$ where $|X| = n$. Then $G/\Phi(G)$ is a elementary abelian p-group and as $\Phi(G) \geq [G, G]$ for all $N \geq \Phi(G)$, $N \lhd G$. Hence for any $N \leq_o G$ containing $\Phi(G)$, G/N is a finite elementary abelian p-group which can be generated by n elements. It follows that $[G : N] \leq p^n$ and if we take $N_0 \lhd_o G$ to

maximise $[G : N_0]$ it is clear that $N_0 \leq N$ for all $N \lhd_o G$. Hence by Proposition 2.18 as $\Phi(G) \lhd_c G$ we have

$$\Phi(G) = \bigcap \{N \mid \Phi(G) \leq N \lhd_o G\} = N_0.$$

Thus (i) implies (ii).

Now, if $\Phi(G)$ is open we have that $\Phi(G) \lhd_o G$ and hence by the definition of a pro-p group, $[G : \Phi(G)] = p^n$ for some positive integer n giving (ii) implies (iii). Assuming (iii) then, we have $G/\Phi(G)$ is a finite group and thus there is a finite set $X \subseteq G$ such that $X\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$. Hence by Proposition 2.29 we have $G = \overline{\langle X \rangle}$ and we have (i) as required. □

Example 2.34. [Γ_1^* is a finitely generated pro-p group.]

In Example 2.25 we demonstrated that Γ_1^* was a powerful pro-p group, and $\Phi(\Gamma_1^*) = (\Gamma_1^*)^p = \Gamma_2^*$. However, as $\Gamma_2^* = SL_n(\mathbb{Z}_p) \cap \Gamma_2$ and $\Gamma_2 \subseteq_o GL_n(\mathbb{Z}_p)$ we have $\Gamma_2^* \subseteq_o SL_n(\mathbb{Z}_p)$. Then by the proposition above, Γ_1^* is a finitely generated powerful pro-p group. □

It turns out that we can further simplify the Frattini subgroup when G is a finitely generated pro-p group, which becomes essential to our main theorem below.

Lemma 2.35. *For any finitely generated pro-p group G, $\Phi(G) = G^p[G, G]$.*

Proof. Let $G = \overline{\langle a_1, \ldots, a_n \rangle}$. As $\Phi(G)$ is open in G it suffices to show $G^p[G, G] \subseteq_c G$. By Proposition 1.21 (iii), $G^{\{p\}} = \{g^p \mid g \in G\} \subseteq G$ is closed. Now as $G/[G, G]$ is abelian we have that $G^p[G, G] = G^{\{p\}}[G, G]$ and thus if $[G, G] \subseteq_c G$ the result follows.

Hence it remains to show that $[G, G] \subseteq_c G$. Consider the map $\phi : G \times \ldots \times G \to G$ defined by $(g_1, \ldots, g_n) \mapsto [g_1, a_1] \ldots [g_n, a_n]$. As multiplication and inversion are continuous in G, ϕ is clearly continuous. Also $G \times \ldots \times G$ is compact and hence $\phi(G \times \ldots \times G) = X = \{[g_1, a_1] \ldots [g_n, a_n] \mid g_1, \ldots, g_n \in G\}$ is closed in G. Now if we take any $N \lhd_o G$ then G/N is nilpotent (being a finite p-group). Clearly G/N is generated by $\{a_1 N, \ldots, a_d N\}$ and hence $[G/N, G/N] = XN/N$ by Proposition 2.17.

It is clear that $X \subseteq [G, G]$, and by the above we have $[G, G]N = XN$ for each $N \lhd_o G$. Hence by Proposition 2.18

$$[G, G] \subseteq \bigcap_{N \lhd_o G} [G, G]N = \bigcap_{N \lhd_o G} XN = \overline{X} = X.$$

It follows that $[G, G] = X \subseteq_c G$ and the lemma is established. □

Theorem 2.36. *Let G be a finitely generated pro-p group, then every subgroup of finite index in G is open.*

Proof. Let K be an arbitrary normal subgroup of finite index in G. If $[G : K] = 1$ the result is obvious and so proceeding by induction on the index of K in G we can assume that K is open in any finitely generated pro-p group M such that

$K \leq M < G$. Consider then $M = G^p[G,G]K$. It is clear that $M \lhd_o G$ by the above lemma, and hence that M is a finitely generated pro-p group (Proposition 2.32). It remains to show that $M \neq G$.

Let $[G:K] = p^m q$ for some q not divisible by p, and put $X = \{g^{p^m q} \mid g \in G\} \subseteq_c G$. It is clear that $X \subseteq K$ and similarly that for any $N \lhd_o G$ (as G/N is a finite p-group) there exists an n such that $g^{p^n} \in N$ for all $g \in G$. Assuming without loss of generality that $n > m$ there exists $a, b \in \mathbb{Z}$ such that

$$ap^m q + bp^n = p^m$$

and hence

$$g^{p^m} = (g^a)^{p^m q}(g^{p^n})^b \in XN.$$

Thus for all $g \in G$, $g^{p^m} \in X \subseteq K$ and so G/K is a finite p-group. It follows that $G^p[G,G]K/K = \Phi(G/K) \neq G/K$ (as every finite p-group has a maximal subgroup) and so $M < G$ as claimed. Thus $K \lhd_o G$. As each subgroup of finite index contains a normal subgroup of finite index we have established our result. □

The power of the above theorem, and its main use to us, is revealed in the following corollary.

Corollary 2.37. *If G is a finitely generated pro-p group then every homomorphism from G to a profinite group is continuous.*

Proof. Suppose that $f : G \to H$ is a homomorphism where H is a profinite group. Taking any $N \lhd_o H$ we see that $[G : f^{-1}(N)] \leq [H : N]$ and so $f^{-1}(N) \leq_o G$ by the theorem above. As the open normal subgroups form a base for the neighbourhoods of the identity in G we have that f is continuous. □

Combining this with Proposition 1.22 we have that every isomorphism from such a G to a profinite group is a homeomorphism. In particular if we were to take G with any other profinite topology it would be homeomorphic to G with its original topology (via the identity map). Hence the topology of any finitely generated pro-p group G is determined by its group structure.

Another corollary is that each subgroup of finite index in a finitely generated pro-p group is finitely generated (following directly from Proposition 2.32). So again the corresponding result for finite groups, that any subgroup of finite index in a group generated by a finite set can also be generated by a finite set, holds for pro-p groups.

These significant corollaries to Theorem 2.36 made the question of whether or not it generalised to finitely generated profinite groups of much interest. The affirmative was recently demonstrated by Nikolov and Segal in [NS06].

2.3 Powerful Groups

As mentioned in the previous section, the simplest finitely generated pro-p groups are the procyclic groups, those generated topologically by a single element. We begin this section with a discussion of the properties of these groups from which we show that the procyclic groups are the inverse limit of a system of finite cyclic groups. More importantly, however, we show that each infinite procyclic group is

powerful and homeomorphic to $\mathbb{Z}_p$. The procyclic groups turn out to be the building blocks of all powerful finitely generated pro-p groups in the sense that any finitely generated pro-p group is the product of its procyclic subgroups. Furthermore, considering a certain subgroup of the powerful finitely generated pro-p groups, the uniform pro-p groups, we see that just as each procyclic group is homeomorphic to $\mathbb{Z}_p$, each uniform group is homeomorphic to $\mathbb{Z}_p^d$ where d is the size of a minimal generating set. These are the two main results of this chapter, and most of the remainder of the thesis relies on these results alone.

We know that $\langle a\rangle = \{a^\lambda \mid \lambda \in \mathbb{Z}\}$ and want to similarly describe the elements of $\overline{\langle a\rangle}\setminus\langle a\rangle$. If we consider any pro-p group G, and take a sequence integers $\{\lambda_i\}$ which converges in $\mathbb{Z}_p$, it turns out that for any $g \in G$, g^{λ_i} converges in the topology of G. As λ_i converges for any $n > 0$ there exists an M_n such that $\lambda_i \equiv \lambda_j \pmod{p^n}$ for all $i, j > M_n$. Since for any $N \trianglelefteq_o G$ we have $|G/N| = p^n$ for some n it follows that $g^{\lambda_i} \equiv g^{\lambda_j} \pmod{N}$ for all $i, j > M_n$ and hence by Proposition 2.19 the sequence converges in G, say to $\hat{g}$.

Furthermore, any other sequence of integers $\{\mu_i\}$ converging to λ in $\mathbb{Z}_p$ will converge to the same element of G. To see this suppose the sequence $\{g^{\mu_i}\}$ converges to $\hat{h}$, take any $N \trianglelefteq_o G$ with $|G/N| = p^n$ as before. As both sequences of integers converge to λ we have $M > 0$ such that for all $i, j > M$, $\lambda_i \equiv \mu_j \pmod{N}$. Since for any $i > M$, $g^{\lambda_i} \equiv \hat{g} \pmod{N}$ and $g^{\mu_i} \equiv \hat{h} \pmod{N}$ we have

$$\hat{g}\hat{h}^{-1} \equiv g^{\lambda_i - \mu_i} \equiv 1 \pmod{N}.$$

Thus $\hat{g}\hat{h}^{-1} \in N$ for all $N \trianglelefteq_o G$ and, as the open normal subgroups intersect in the identity, $\hat{g} = \hat{h}$.

The discussion above yields the following definition

Definition 2.38. If G is a pro-p group then for any $\lambda \in \mathbb{Z}_p$, $g \in G$

$$g^\lambda := \lim_{i\to\infty} a^{\lambda_i} \in G$$

where $\{\lambda_i\}$ is any sequence of integers converging to λ in $\mathbb{Z}_p$.

It is easy to see that for any $\lambda, \mu \in \mathbb{Z}_p$ we have the ordinary exponent laws holding. That is for any $g, h \in G$, $g^{\lambda+\mu} = g^\lambda g^\mu$, $g^{\lambda\mu} = (g^\lambda)^\mu$, and $(gh)^\lambda = g^\lambda h^\lambda$ if $gh = hg$.

The importance of this p-adic exponentiation of elements of pro-p groups is that it allows us to completely characterise the elements of the procyclic group $\overline{\langle a\rangle}$. We begin with a lemma that is also of use to us later.

Lemma 2.39. *If G is a pro-p group then for any $g \in G$ the map, $\phi_g : \mathbb{Z}_p \to G$ defined by $\lambda \mapsto g^\lambda$ is a continuous homomorphism whose image is the procyclic subgroup $\overline{\langle g\rangle}$.*

Proof. The discussion above shows that ϕ_g is a homomorphism, and it is continuous by Corollary 2.37. It is clear that $\phi_g(\mathbb{Z}_p) \geq \langle g\rangle$ and that $\phi_g(\mathbb{Z}_p) \leq \overline{\langle g\rangle}$. However $\phi_g(\mathbb{Z}_p)$ is compact (as $\mathbb{Z}_p$ is) and thus closed and so $\phi_g(\mathbb{Z}_p) = \overline{\langle g\rangle}$ □

Proposition 2.40. *For any pro-p group G the following are equivalent.*

(i) G *is procyclic;*
(ii) $G = g^{\mathbb{Z}_p} = \{g^\lambda \mid \lambda \in \mathbb{Z}_p\}$ *for some* $g \in G$*;*
(iii) Either G *is finite and cyclic or homeomorphic to the topological group* $(\mathbb{Z}_p, +)$*;*
(iv) G/N *is cyclic for all* $N \lhd_o G$*. That is,* G *is the inverse limit of cyclic groups.*

Proof. The lemma above gives us that (i) implies (ii) immediately. Assuming (ii), $\phi : \mathbb{Z}_p \to G$ given by $\phi(\lambda) = g^\lambda$ is clearly surjective. Hence by the first isomorphism theorem $\mathbb{Z}_p/K \cong G$ where $K = \ker(\phi)$. Also, ϕ is continuous by Corollary 2.37, and thus by Proposition 1.22, $\mathbb{Z}_p/K$ is homeomorphic to G. However, as any subgroup of the (additive) group $\mathbb{Z}_p$ is of the form $p^m\mathbb{Z}_p$ it is clear that either $\mathbb{Z}_p/K$ is $\mathbb{Z}_p$ or it is cyclic. That (iii) implies (iv) is clear as ϕ is a homomorphism.

Finally, if we assume (iv) and suppose that G has two (distinct) maximal open subgroups M, N, then $M \cap N \supseteq G^p[G, G]$. As G/M and G/N are cyclic abelian elementary p-groups we must have $[G : M] = [G : N] = p$. But then $[G : M \cap N] \geq p^2$ and so $G/M \cap N$ is an elementary cyclic abelian p-group with at least p^2 elements. This is a clear contradiction and hence G must have a unique maximal open subgroup, $\Phi(G)$. It follows that $G/\Phi(G)$ is cyclic and hence can be generated by a single element. By Proposition 2.29, G can be generated topologically by a single element and is thus procyclic. □

It is clear from the above that every procyclic group $G = \overline{\langle a \rangle}$ is abelian as for any $g, h \in G$, $g = a^\lambda$ and $h = a^\mu$ for some $\lambda, \mu \in \mathbb{Z}_p$, and so

$$gh = a^\lambda a^\mu = a^{\lambda+\mu} = a^\mu a^\lambda = hg.$$

It follows that every procyclic group is powerful.

As is suggested by Corollary 2.27, just as many of the properties of profinite and pro-p groups rely on the properties of finite groups and finite p-groups respectively the properties of powerful finitely generated pro-p groups follows those of powerful finite p-groups almost exactly. We now present a series of results on powerful groups, in each case beginning with a result for powerful finite p-groups before extending it to the corresponding result over powerful finitely generated pro-p groups.

Recalling that $G^p := \langle g^p \mid g \in G \rangle$, we begin with a definition.

Definition 2.41. If G is a finite p-group or a finitely generated powerful pro-p group we let $G_1 = G$ and define $G_i = G_{i-1}^p$. In both cases we denote the series of subgroups, $\{G_i\}$, the *lower p-series*.

If G is a powerful finite p-group it is clear that $G_2 = G^p = \Phi(G)$. However, Corollary 2.14 gives us that G_2 p.e. G and thus G_2 is powerful. Hence $\Phi(G_2) = G_3$. We also see that the map $x \mapsto x^p$ induces a natural surjective homomorphism from $G/G_2 \to G_2/G_3$ which follows from Proposition 2.3. This leads to the following result.

Proposition 2.42. *If* G *is a powerful finite* p*-group then every element of* G^p *is a* p*th power in* G*.*

Proof. We proceed by induction on n where $|G| = p^n$. If $n = 1$ then $G^p = \{1\}$ and the result is obvious. So assuming the proposition holds for all powerful finite p-groups of order p^m with $m < n$ we take G such that $|G| = p^n$ and let $g \in G^p$. As $x \mapsto x^p$ is a surjective homomorphism from $G/G_2 \to G_2/G_3$ there exists $x \in G$ and $y \in G_3$ such that $g = x^p y$. By Proposition 2.13 the group $H = \langle G^p, x\rangle$ is a powerful finite p-group, and $g \in H^p$ as $y \in G_3 = (G^p)^p$. Thus if $|H| \neq |G|$ we have by the inductive hypothesis an $h \in H \leq G$ such that $h^p = g$. Otherwise $H = G$ and then $G = \langle \Phi(G), x\rangle$ implying that G is cyclic in which case the result is trivial. □

Proposition 2.43. *For any powerful finitely generated pro-p group G each element of G^p is a pth power in G. Furthermore $\Phi(G) = G^p \lhd_o G$.*

Proof. 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 pth power in G/N by the proposition above. Letting $X_N := \{h \in G/N \mid h^p = g_N\}$ it is clear that, with respect to the natural maps $\pi_{MN} : G/N \to G/M$ whenever $N \leq M$, $(X_N, \pi_{MN})_{N \lhd_o G}$ forms an inverse system of sets which by the above are non-empty. Hence by Proposition 1.27 there is an $h = (h_N) \in \varprojlim X_N \subseteq G$. Clearly $h^p = g$ and so we have that $\overline{G^p} = G^p = \{g^p \mid g \in G\}$. It follows that $\Phi(G) = G^p \lhd_o G$ from Lemma 2.35 and that G is powerful. □

These properties extend to each element of the lower p-series in both the finite and finitely generated pro-p cases.

Proposition 2.44. *If $G = \langle a_1, \ldots, a_n\rangle$ is a powerful finite p-group then for all i, G_i is powerfully embedded in G and*

$$G_i = \Phi(G_{i-1}) = G^{p^{i-1}} = \{g^{p^{i-1}} \mid g \in G\} = \left\langle a_1^{p^{i-1}}, \ldots, a_n^{p^{i-1}} \right\rangle \lhd G.$$

Also, the map $x \mapsto x^{p^k}$ induces a surjective homomorphism from G_i/G_{i+1} to G_{i+k}/G_{i+k+1}.

Proof. We have already established that $G_2 = \Phi(G_1) \lhd G$, $G_3 = \Phi(G_2) \lhd G$ and that $\theta_1 : G/G_2 \to G_2/G_3$ defined by $x \mapsto x^p$ is a surjective homomorphism. Supposing G_i p.e. G, then $G_{i+1} = G_i^p$ which is powerfully embedded in G by Proposition 2.14. Hence G_i is powerful and so $\Phi(G_i) = G_i^p = G_{i+1}$, and also replacing G with G_i we have the map $x \mapsto x^p$ inducing a surjective homomorphism from $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$.

Then, by induction on i, Proposition 2.42 implies that $G_i = \{g^{p^{i-1}} \mid g \in G\}$ and hence $G_i = G^{p^{i-1}}$. For $i = 2$ the last equality follows from the fact that $G_3 = \Phi(G_2)$ and G_2/G_3 is generated by $\{\theta_1(a_1G_2), \ldots, \theta_1(a_nG_2)\}$. Repeated applications of this give us that

$$G_i = \left\langle a_1^{p^{i-1}}, \ldots, a_n^{p^{i-1}} \right\rangle.$$

Lastly, the map $x \mapsto x^{p^k}$ induces precisely $\theta_{i+k-1} \circ \theta_{i+k-2} \circ \ldots \circ \theta_i$, a surjection from G_i/G_{i+1} to G_{i+k}/G_{i+k+1}. □

Proposition 2.45. *If $G = \overline{\langle a_1, \ldots, a_n \rangle}$ is a powerful pro-p group then for all i, G_i is powerfully embedded in G and*

$$G_i = \Phi(G_{i-1}) = G^{p^{i-1}} = \{g^{p^{i-1}} \mid g \in G\} = \overline{\left\langle a_1^{p^{i-1}}, \ldots, a_n^{p^{i-1}} \right\rangle} \lhd_o G.$$

Also, the map $x \mapsto x^{p^k}$ induces a surjective homomorphism from G_i/G_{i+1} to G_{i+k}/G_{i+k+1}.

Proof. Proposition 2.43 gives us that $G_2 = \Phi(G_1) = G^p = \{g^p \mid g \in G\} \lhd_o G$. If $N \lhd_o G$ then G/N is a powerful finite p-group and hence by the proposition above $G^{p^{i-1}}N/N$ p.e. G/N for all i. As this holds for all $N \lhd_o G$, $G_i = G^{p^{i-1}}$ p.e. G (Proposition 2.26). So it is clear that

$$G_i = \Phi(G_{i-1}) = G^{p^{i-1}} = \{g^{p^{i-1}} \mid g \in G\} \lhd_o G.$$

As $\Phi(G_i) = G_{i+1} = \{g^p \mid g \in G_i\}$ it is clear that the map $x \mapsto x^p$ is a surjective homomorphism from $G_i/G_{i+1} \to G_{i+1}/G_{i+2}$, composing these maps (as in the proof above) gives that $x \mapsto x^{p^k}$ is a surjection from G_i/G_{i+1} to G_{i+k+1}/G_{i+k}.

Lastly, this map implies that $G_2 = \langle a_1^p, \ldots, a_n^p \rangle G_3$ and so by induction, $G_i = \left\langle a_1^{p^{i-1}}, \ldots, a_n^{p^{i-1}} \right\rangle G_{i+1}$. As $\Phi(G_i) = G_{i+1}$ we have

$$G_i = \overline{\left\langle a_1^{p^{i-1}}, \ldots, a_n^{p^{i-1}} \right\rangle}$$

by Proposition 2.29. □

We note in the previous proposition that for each i, $G_i \lhd_o G$ for a powerful finitely generated pro-p group G. This is why we restrict to the finitely generated pro-p groups, so that the lower p-series is composed of open normal subgroups, and furthermore, so these subgroups form a base for the neighbourhoods of the identity.

Proposition 2.46. *If G is a finitely generated powerful pro-p group the set $\{G_i \mid i \geq 1\}$ forms a base for the neighbourhoods of the identity in G.*

Proof. It clearly suffices to show that for any $N \lhd_o G$ there exists an i such that $G_i \leq N$. As G/N is a finite p-group there exists an i such that $(G/N)^{p^{i-1}} = \{1\}$. Hence $G^{p^{i-1}} = G_i \leq N$. □

We now come to the first of two theorems which show how finitely generated powerful pro-p groups can be thought of as extensions of the procyclic groups, beginning again, however, with the corresponding result for powerful finite p-groups.

Proposition 2.47. *If $G = \langle a_1, \ldots, a_n \rangle$ is a powerful finite p-group then $G = \langle a_1 \rangle \ldots \langle a_n \rangle$.*

Proof. We know that for some k, $G_{k+1} = \{1\}$. If $k = 1$ then G is an elementary abelian p-group and thus the product of its cyclic subgroups. Proceeding then by induction we suppose that the result holds for all G such that $G_{j+1} = \{1\}$ with $j < k$. Then if we take any G such that $G_{k+1} = \{1\}$, $G = \langle a_1 \rangle \ldots \langle a_n \rangle G_k$. Also,

as G_k p.e. G, $\{1\} = G_k^p \geq [G_k, G]$ implying that $G_k \leq Z(G)$. However Proposition 2.44 also tells us that

$$G_k = \left\langle a_1^{p^{k-1}}, \dots a_n^{p^{k-1}} \right\rangle \leq Z(G)$$

and so $G = \langle a_1 \rangle \dots \langle a_n \rangle$ as required. □

Theorem 2.48. *If G is a powerful pro-p group which is generated topologically by the set $\{a_1, \dots, a_n\}$, then $G = \overline{\langle a_1 \rangle} \dots \overline{\langle a_n \rangle}$.*

Proof. If we set $A = \overline{\langle a_1 \rangle} \dots \overline{\langle a_n \rangle}$ then by Proposition 1.21 (iii) A is closed. Also we see by the proposition above that $AN/N = G/N$ and hence

$$A = \bigcap_{N \lhd_o G} AN = \bigcap_{N \lhd_o G} GN = G$$

by Proposition 2.18. □

The last theorem tells us that $G = \{a_1^{\lambda_1} \dots a_n^{\lambda_n} \mid \lambda_1, \dots, \lambda_n \in \mathbb{Z}_p\}$. However, it does not affirm that to each $g \in G$ corresponds a unique n-tuple of p-adic integers and bisa-versa. One can clearly see this as we have not required $\{a_1, \dots, a_n\}$ be a minimal topological generating set, though even if we do it is not necessarily a bijective correspondence. We need an added condition, and therefore define the uniform pro-p group as follows.

Definition 2.49. A finitely generated powerful pro-p group G is said to be *uniform* if for all $i \in \mathbb{N}$, $[G_i : G_{i+1}]$ is constant. The *dimension* of a uniform pro-p group is defined to be the size of a minimal topological generating set.

If G is an arbitrary powerful pro-p group with minimal topological generating set $\{a_1, \dots, a_d\}$ then as $G = \overline{\langle a_1 \rangle} \dots \overline{\langle a_n \rangle}$ and G is abelian modulo $G^p = G_2$ it is clear that $[G : G_2] \leq p^d$. However, as $\{a_1, \dots, a_d\}$ is a minimal generating set we must have equality as $[G : G_2] = |G/\Phi(G)| < p^d$ would imply the existence of a smaller generating set. The first half of this argument holds also for $[G_i : G_{i+1}]$, as G_i is a finitely generated powerful pro-p group and $\Phi(G_i) = G_{i+1}$. However, while there exists a generating set of G_i of size d

$$G_i = \overline{\left\langle a_1^{p^{i-1}}, \dots, a_d^{p^{i-1}} \right\rangle}$$

we do not know that this is a minimal generating set for G_i. Hence, while we are assured that $[G_i : G_{i+1}] \leq p^d$ do not necessarily have equality. Thus saying a pro-p group is uniform is equivalent to saying for all i

$$\{a_1^{p^{i-1}}, \dots, a_d^{p^{i-1}}\}$$

is in fact a minimal topological generating set for G_i. It is with this extra structure that we obtain the bijective correspondence mentioned above as we establish below.

Theorem 2.50. *If G is a uniform pro-p group then the mapping*

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

is a homeomorphism from $\mathbb{Z}_p^d$ to G where $\{a_1, \ldots, a_d\}$ is a minimal generating set for G.

Proof. $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$ (by Theorem 2.48) and so for any $g \in G$, $g = a_1^{\lambda_1} \ldots a_d^{\lambda_d}$ for some $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}_p$. So we consider the map $\psi : G \to \mathbb{Z}_p^d$ defined by $a_1^{\lambda_1} \ldots a_d^{\lambda_d} \mapsto (\lambda_1, \ldots, \lambda_d)$. We show that ψ is a well defined bijection and that its inverse θ is the homeomorphism we require.

Take any integer k and recall $|G/G_{k+1}| = [G : G_{k+1}] = p^{kd}$. It is clear that $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \ldots \langle a_d G_{k+1} \rangle$, and as $G_{k+1} = \{g^{p^k} \mid g \in G\}$ 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 $a_1^{\mu_1} \ldots a_d^{\mu_d} G_{k+1}$ where $\mu_1, \ldots, \mu_d \in \{0, 1, \ldots, p^k - 1\}$ 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.

Then $\theta : \mathbb{Z}_p^d \to G$ defined by $(\lambda_1, \ldots, \lambda_d) \mapsto a_1^{\lambda_1} \ldots a_d^{\lambda_d}$ is the inverse bijection. However, θ is merely the composition of the two maps $\alpha : \mathbb{Z}_p^d \to G \times G \times \ldots \times G$ and $\beta : G \times G \times \ldots \times G \to G$ given by (where ϕ_g is the map defined in Lemma 2.39)

$$\alpha((\lambda_1, \ldots, \lambda_d)) = (\phi_{a_1}(\lambda_1), \ldots, \phi_{a_d}(\lambda_d));$$

$$\beta(g_1, \ldots, g_d) \mapsto g_1 g_2 \ldots g_d.$$

We know that each ϕ_{a_i} is continuous, and β is continuous as multiplication in G is and hence θ is also continuous. It follows that θ is a homeomorphism as both $\mathbb{Z}_p$ and G are profinite (recall Proposition 1.22). □

Hence the uniform pro-p groups are the true extension of the procyclic groups in that they are homeomorphic to $\mathbb{Z}_p^d$ where d is the dimension of the group.

We conclude this chapter by showing that in a way we have not reduced our class of groups by restricting to the uniform pro-p groups.

Proposition 2.51. *Every finitely generated powerful pro-p group G contains an open uniform subgroup.*

Proof. By Proposition 2.45, for each i we have $G_i \triangleleft_o G$ and a surjection from G_i/G_{i+1} to G_{i+1}/G_{i+2}. It follows that $[G_i : G_{i+1}] \geq [G_{i+1} : G_{i+2}]$ for all i. Thus setting $[G_i : G_{i+1}] = p^{n_i}$ we clearly have

$$n_1 \geq n_2 \geq \ldots \geq n_i \geq \ldots$$

and hence (as each $n_i \geq 0$) for some integer $J > 0$, $n_i = n_j$ for all $i, j \geq J$. It follows that $G_J \triangleleft_o G$ is uniform. □

Remark 2.52. As the notion and theory behind the powerful finite p groups and finitely generated pro-p groups was only developed by Lubotzky and Mann in the 1980's, these are not the terms used by Lazard in his original wording of Theorem A. Instead his result relied upon the pro-p groups of *finite rank*. The rank of a

profinite group is defined to be the common number ([DSMS91] Proposition 3.11) defined by (where $d(H)$ is the size of a minimal generating set for H)

(1) $r_1 = \sup\{d(H) \mid H \leq_c G\}$
(2) $r_2 = \sup\{d(H) \mid H \leq_c G \text{ and } d(H) < \infty\}$
(3) $r_3 = \sup\{d(H) \mid H \leq_o G\}$.

While the notion of groups of finite rank is traditionally common in an exposition of this kind we avoid in favour of the more streamlined path to our main results given by considering powerful finitely generated pro-p groups. We simply present the following result ([DSMS91] Theorem 3.13) to assure us that we are in essence dealing with the same family of groups. □

Theorem 2.53. *A pro-p group G has finite rank if and only if G is finitely generated and contains an open subgroup which is powerful.*

Chapter 3

The Iwasawa Algebra

Much of the mathematical community's interest in $\mathbb{Z}_p$ stems from the fact that it appears as a Galois group of certain field extensions of infinite degree. These field extensions were first studied by Kenkichi Iwasawa in the 1950's who used the theory developed to establish numerous results from number theory. In fact each profinitie group can be realised as a Galois group of such an extension, and most of the current research in the field is aimed at generalising the results of commutative Iwasawa Theory to the general non-commutative case, which we will deal with here.

One of the central objects of interest in both cases is the Iwasawa Algebra which is defined to be the inverse limit of the system of group rings $\mathbb{Z}_p[G/N]$ where $N \triangleleft_o G$. Our main aim in this chapter is to establish that the Iwasawa algebra arises as the completion of the group ring $\mathbb{Z}_p[G]$ under a suitably defined norm (Theorem B). While our work here mainly serves as an introduction to the Iwasawa algebra we also require the theory developed in the, quite substantial, proof of Section 4.3, which is essential to our proof of Theorem A.

Though our exposition follows that in [DSMS91], with the exception of Proposition 3.13 and Corollary 3.14 the proofs presented are original. Also, many of the results (in particular Lemma 3.19 and Lemma 3.20) have been generalised, though I have no doubt this generalisation is not new.

3.1 Normed Rings

We begin by introducing the notion of a norm on a ring, a generalisation of the p-adic absolute value, $|\cdot|_p$, defined in Chapter 1. Such a norm yields the obvious metric and allows us to introduce intuitive notions of limits in our ring as well as completions of our ring. As these norms carry the ultrametric quality ((iii) below) we can obtain far stronger results about the limiting behaviour of sequences and series. For instance we show

$$\sum_{i=1}^{\infty} a_i \text{ converges if and only if } \lim_{i\to\infty} a_i = 0.$$

This section is dedicated to providing the usual definitions associated with a normed space and setting up this theory of limits.

Definition 3.1. A *normed ring* $(R, ||\cdot||)$ is a ring R with a function $||\cdot|| : R \to \mathbb{R}$ such that for all $a, b \in R$

(i) $||a|| \geq 0$; $||a|| = 0$ if and only if $a = 0$;
(ii) $||1_R|| = 1$ and $||ab|| \leq ||a||\ ||b||$; and
(iii) $||a \pm b|| \leq \max\{||a||, ||b||\}$.

Such a function $||\cdot||$ is said to be a *ring norm*.

As mentioned in Chapter 1, such norms are called *non-Archimedean* as the satisfy they stronger version of the triangle inequality (iii). Hence by the same reasoning as for $(\mathbb{Z}_p, |\cdot|_p)$,

$$||a \pm b|| = \max\{||a||, ||b||\}, \text{ for any } ||a|| \neq ||b||.$$

Our norm defines the metric $d(a,b) = ||a-b||$ on R and with respect to this metric R is a topological space. Again following exactly the same argument as for $(\mathbb{Z}_p, |\cdot|_p)$ we have

Proposition 3.2. *The open ball*

$$B(a,r) := \{x \in R \mid ||x-a|| < r\}$$

is both open and closed in R.

Using our norm, and the induced metric, we can make the usual definitions consistent with an arbitrary metric space.

Definition 3.3. Let $(R, ||\cdot||)$ be a normed ring

(i) A sequence $\{a_n\} \subseteq R$ is *Cauchy* if for any $\epsilon > 0$ there exists $N > 0$ such that $||a_m - a_n|| < \epsilon$ for all $m, n > N$.

(ii) R is said to be *complete* if every Cauchy sequence converges to an element of R.

(iii) A subset S of R is *dense* in R if for every $a \in R$ there is a Cauchy sequence $\{a_n\} \subseteq S$ converging to a.

(iv) A complete normed ring $(R, ||\cdot||')$ is a *completion* of R if R is dense in R' and $||\cdot||'\big|_R = ||\cdot||$.

We will study the notion of the completion of a normed ring in more depth in the following section, though now we begin by investigating basic properties of sequences and series. We introduce, as in [DSMS91] a more general notion of convergence which will be useful later.

Definition 3.4. If $(R, ||\cdot||)$ is any normed ring such that $a, s \in R$ and $\{a_n\}_{n\in T} \subseteq R$ where T is a countably infinite set.

(i) The family $\{a_n\}$ converges to a if for each $\epsilon > 0$ there exists finite $T_\epsilon \subset T$ such that for all $n \in T \backslash T_\epsilon$, $||a - a_n|| < \epsilon$. We write this as

$$\lim_{n\in T} a_n = a.$$

(ii) The series $\sum_{n\in T} a_n$ converges to s if for each $\epsilon > 0$ there exists finite T_ϵ such that for all finite T' satisfying $T_\epsilon \subseteq T' \subset T$

$$\Big|\Big|s - \sum_{n\in T'} a_n\Big|\Big| < \epsilon.$$

We write this as $\sum_{n\in T} a_n = s$.

It is clear that the limit defined in (i) satisfies the basic limit properties, for $\{a_n\}, \{b_n\}$ convergent sequences in R and $\lambda \in R$

- $\lim_{n\in T} a_n + \lim_{m\in T} b_m = \lim_{n\in T}(a_n + b_n)$;
- $\lambda \lim_{n\in T} a_n = \lim_{n\in T} \lambda a_n$.

Below we establish more important properties of the above limit. The first two indicate that it is equivalent to our usual notion of the limit, as indexed by the natural numbers.

Proposition 3.5. *Let $(R, ||\cdot||)$ be a complete normed ring, $\{a_n\}_{n\in T}$ a sequence in R where T is a countably infinite set, and $i \mapsto n(i)$ any bijection from $\mathbb{N}$ to T.*

(i) $\lim_{n\in T} a_n$ *converges if and only if* $\lim_{i\to\infty} a_{n(i)}$ *does.*

(ii) The following are equivalent:

I. The series $\sum_{i=0}^{\infty} a_{n(i)}$ *converges;*

II. The series series $\sum_{n\in T} a_n$ *converges;*

III. $\lim_{n\in T} a_n = 0$.

(iii) If $\sum_{n\in T} a_n = s$ *then* $||s|| \leq \sup\{||a_n|| \mid n \in T\}$ *and if there is an* $m \in T$ *such that* $||a_m|| > ||a_n||$ *for all* $n \in T\backslash\{m\}$ *then* $||s|| = ||a_m||$.

Proof. We prove each part:

(i) Suppose first that $\lim_{n\in T} a_n$ converges. Then for any $\epsilon > 0$ there exists finite $T_\epsilon \subset T$ such that $||a - a_n|| < \epsilon$ for all $n \in T\backslash T_\epsilon$. Setting $M = \max\{i \in \mathbb{N} : n(i) \in T_\epsilon\}$ gives us $||a - a_{n(i)}|| < \epsilon$ for all $i > M$ and hence $\lim_{i\to\infty} a_{n(i)}$ converges. Conversely, if $\lim_{i\to\infty} a_{n(i)}$ converges for any $\epsilon > 0$ there exists $M > 0$ such that for all $i > M$, $||a - a_{n(i)}|| < \epsilon$. Then setting $T_\epsilon = \{n(i) \mid i \leq M\}$ we have that for all $n \in T\backslash T_\epsilon$, $||a - a_n|| < \epsilon$. Hence $\lim_{n\in T} a_n$ converges.

(ii) Supposing the series $\sum_{i=0}^{\infty} a_n$ converges (to s say) we have for any $\epsilon > 0$, $M > 0$ such that for all $m > M$

$$||s - \sum_{i=0}^{m} a_{n(i)}|| < \epsilon.$$

This also implies that for any $m > M + 1$, $||a_m|| < \epsilon$ as

$$||a_m|| = ||s - \sum_{i=0}^{m-1} a_{n(i)} - (s - \sum_{i=0}^{m} a_{n(i)})|| \leq \max\{||s - \sum_{i=0}^{m} a_{n(i)}||, ||s - \sum_{i=0}^{m-1} a_{n(i)}||\}.$$

Thus we again set $T_\epsilon = \{n(i) \ : \ i \leq M\}$ and take any finite $T' \subset T$ containing T_ϵ. So, I implies II as

$$\begin{aligned} ||s - \sum_{n\in T'} a_n|| &= ||s - \sum_{n\in T_\epsilon} a_n + \sum_{n\in T\backslash T_\epsilon} a_n|| \\ &\leq \max\{||s - \sum_{n\in T_\epsilon} a_n||, \max_{n\in T\backslash T_\epsilon}\{||a_n||\}\} \\ &< \epsilon. \end{aligned}$$

Now assume that $\sum_{n\in T} a_n$ converges, say to s, and take any $\epsilon > 0$. Then we have T_ϵ as in the definition and set $M = \max\{i \in \mathbb{N} \ : \ n(i) \in T_\epsilon\}$. But then for any $m > M$, as $T' := T_\epsilon \cup \{a_{n(m)}\}$ is a finite subset of T containing T_ϵ,

$$\begin{aligned} ||a_m|| &= ||s - \sum_{n\in T_\epsilon} a_n - (s - \sum_{n\in T'} a_n)|| \\ &\leq \max\{||s - \sum_{n\in T_\epsilon} a_n||, ||s - \sum_{n\in T'} a_n||\} \\ &< \epsilon. \end{aligned}$$

And hence II implies III.

Finally we assume that $\lim_{n\in T} a_n = 0$ and for each $k \in \mathbb{N}$ set $s_k = \sum_{i=0}^{k} a_{n(i)}$. Now, for each $\epsilon > 0$ we have a M such that $||a_{n(i)}|| < \epsilon$ for all $i > M$. It follows that for any $M < j < k$

$$||s_k - s_j|| = \max\{||a_{n(i)}|| \ : \ j < i \leq k\} < \epsilon.$$

So $\sum_{i=0}^{\infty} a_{n(i)}$ converges and as R is complete and III implies I as required.

(iii) Suppose that $\sum_{n\in T} a_n = s$ and $||s|| > \sup\{||a_n||\}$. Now for any $\epsilon > 0$ there exists T_ϵ such that $||s - \sum_{n\in T_\epsilon} a_n|| < \epsilon$. However, as T_ϵ is finite

$$||\sum_{n\in T_\epsilon} a_n|| \leq \sup\{||a_n||\} < ||s||$$

and so $||s - \sum_{n\in T_\epsilon} a_n|| = ||s|| < \epsilon$. As ϵ was arbitrary we have $||s|| = 0$ which is obviously a contradiction, so $||s|| \leq \sup\{||a_n||\}$.

Consider now that there exists an m such that $||a_m|| > ||a_n||$ for all $n \in T\backslash\{m\}$. We have from the above that $||s|| \leq ||a_m||$. Suppose that $||a_m|| > ||s||$. Again, for any $\epsilon > 0$ we have finite $T_\epsilon \subset T$ such that for all finite $T' \subset T$ containing T_ϵ

$$||s - \sum_{n\in T'} a_n|| < \epsilon.$$

However, setting now $T' = T_\epsilon \cup \{m\}$ we have $||\sum_{n\in T'} a_n|| = ||a_m||$ and thus

$$||s - \sum_{n\in T'} a_n|| = ||a_m|| < \epsilon$$

which is again an obvious contradiction. □

The generality of the following proposition yields two important corollaries dealing with double series and the multiplication of two series (when indexed over a set with a binary operation).

Proposition 3.6. *Let $(R, ||\cdot||)$ be a complete normed ring, and $\{a_n\}_{n\in T}$ be a sequence in R such that T is the disjoint union of a countable family of countable sets $\{T_\lambda \mid \lambda \in \Lambda\}$. If $\sum_{n\in T} a_n$ converges to s then each $\sum_{n\in T_\lambda} a_n$ converges say to s_λ and $\sum_{\lambda\in\Lambda} s_\lambda = s$.*

Proof. This is obvious if T is finite, so assume T is infinite. As $\lim_{n\in T} a_n = 0$, $\lim_{n\in T_\lambda} a_n = 0$ if T_λ is infinite and thus $\sum_{n\in T_\lambda} a_n$ converges for all λ, say to s_λ. Now if we fix $\epsilon > 0$ we have finite $T_\epsilon \subseteq T$ such that for all finite $T' \subset T$ containing T_ϵ, $||s - \sum_{n\in T'} a_n|| < \epsilon$. Similarly, for each $\lambda \in \Lambda$ there exists finite $S_\lambda \subset T_\lambda$ such that $||s_\lambda - \sum_{n\in S'} a_n|| < \epsilon$ for all finite $S' \subset T_\lambda$ containing S_λ. Hence if we define $U_\lambda = S_\lambda \cup (T_\epsilon \cap T_\lambda)$ then we have

$$||s_\lambda - \sum_{n\in U_\lambda} a_n|| = || \sum_{n\in T_\lambda \setminus U_\lambda} a_n|| < \epsilon.$$

Set $\Lambda_\epsilon = \{\lambda \in \Lambda \mid T_\lambda \cap T_\epsilon \neq \varnothing\}$, noting that $|\Lambda_\epsilon| \leq |T_\epsilon| < \infty$, and take any finite $\Lambda' \subset \Lambda$ containing Λ_ϵ. Then if $S = \bigcup_{\lambda\in\Lambda'} S_\lambda$, which is finite as Λ' is and S_λ is finite for all λ, we have

$$||s - \sum_{\lambda\in\Lambda'} s_\lambda|| = ||s - \sum_{n\in T_\epsilon \cup S} a_n - \sum_{\lambda\in\Lambda'} \sum_{n\in T_\lambda\setminus U_\lambda} a_n|| < \epsilon.$$

Hence $\sum_{\lambda\in\Lambda} s_\lambda = s$. □

Corollary 3.7. *Let $(R, ||\cdot||)$ be a complete normed ring containing $\{a_{mn}\}_{(m,n)\in S\times T}$ where S, T are countable sets. If $\sum_{(m,n)\in S\times T} a_{mn}$ converges (say to s) then $\sum_{m\in S}(\sum_{n\in T} a_{mn})$ and $\sum_{n\in T}(\sum_{m\in S} a_{mn})$ both converge to s.*

Proof. As $S \times T = \bigcup_{m\in S}\{m\} \times T$, the above proposition gives us directly that

$$\sum_{m\in S}(\sum_{n\in T} a_{mn}) = s,$$

and the other double sum follows similarly. □

Corollary 3.8. *Suppose that $(R, ||\cdot||)$ is a complete normed ring containing $\{a_l\}_{l\in T}$ and $\{b_m\}_{m\in T}$ where T is a countable set equipped with a binary operation $*$. If $\sum_{l\in T} a_l$ and $\sum_{m\in T} b_m$ both converge (say to s_a and s_b respectively) then, where $S_n := \{(l, m) \in T \times T \mid l * m = n\}$, $\sum_{(l,m)\in S_n} a_l b_m$ converges to some c_n in R. Furthermore, $\sum_{n\in T} c_n$ converges to $s_a s_b$.*

Proof. As $\sum_{l\in T} a_l$ and $\sum_{m\in T} b_m$ converge we have $\lim_{l\in T} a_l = 0$ and $\lim_{m\in T} b_m = 0$. Hence for any $\epsilon > 0$ we have finite sets $A, B \subset T$ such that $||a_l|| < \sqrt{\epsilon}$ and $||b_m|| < \sqrt{\epsilon}$ for all $l \in T\setminus A$ and $m \in T\setminus B$. So for any $(l, m) \in T \times T\setminus A \times B$ we have

$$||a_l b_m|| \leq ||a_l||\ ||b_m|| < \epsilon$$

and it follows that $\lim_{(l,m)\in T\times T} a_l b_m = 0$. Now, $T \times T = \bigcup_{n\in T} S_n$ and so by our proposition we have $\sum_{(l,m)\in S_n} a_l b_m$ converges to some c_n and that

$$\sum_{n\in T} c_n = \sum_{(l,m)\in T\times T} a_l b_m.$$

But then by the above corollary

$$\begin{aligned}\sum_{(l,m)\in T\times T} a_l b_m &= \sum_{l\in T}(\sum_{m\in T} a_l b_m)\\ &= (\sum_{l\in T} a_l)(\sum_{m\in T} b_m)\\ &= s_a s_b.\end{aligned}$$

So $\sum_{n\in T} c_n = s_a s_b$ as required. □

3.2 The Group Algebra

Recall that for any ring R and any group G the *group algebra* or *group ring*, denoted $R[G]$, is the free module over R with basis G. That is, it is the algebra of formal sums (with $r_g \in R$ for all $g \in G$)

$$\sum_{g\in G} r_g g.$$

The addition and multiplication in the ring are defined by

$$\sum_{g\in G} r_g g + \sum_{h\in G} s_h h = \sum_{g\in G}(r_g + s_g)g, \text{ and;}$$

$$\Big(\sum_{g\in G} r_g g\Big)\Big(\sum_{h\in G} s_h h\Big) = \sum_{g\in G}\Big(\sum_{ab=g} r_a s_b\Big)g.$$

Definition 3.9. The *Iwasawa Algebra* or *Completed Group Algebra* of a finitely generated powerful pro-p group G, Λ_G is defined by

$$\Lambda_G = \mathbb{Z}_p[[G]] = \varprojlim_{N\lhd_o G} (\mathbb{Z}_p[G/N]).$$

The natural epimorphism from $\mathbb{Z}_p$ onto $\mathbb{F}_p$ yields the *epimorphic image*

$$\Omega_G = \mathbb{F}_p[[G]] = \varprojlim_{N\lhd_o G} (\mathbb{F}_p[G/N]).$$

Both of these inverse limits are clearly well defined as the natural surjection $\pi_{M,N} : G/N \to G/M$, for $N \subseteq M$, defined in Section 1.3 induces a surjection from $\mathbb{Z}_p[G/N] \to \mathbb{Z}_p[G/M]$. As mentioned above, our main aim in this chapter is to introduce the Iwasawa Algebra and show how it can defined as the completion of the group algebra $\mathbb{Z}_p[G]$ with respect to a a ring norm which we define. In essence we prove the *"similar result for $\mathbb{Z}_p$"* in Theorem B.

Theorem B *Let G be a uniform pro-p group, and let I denote the augmentation ideal of $\mathbb{F}_p[G]$. Then $\mathbb{F}_p[[G]] := \varprojlim_{N\lhd_o G}\mathbb{F}_p[G/N]$ is isomorphic to the I-adic completion of $\mathbb{F}_p[G]$. There is a similar result for $\mathbb{Z}_p[G] := \varprojlim_{N\lhd_o G}\mathbb{Z}_p[G/N]$.*

However, we do not require G to be uniform, we show the result for any finitely generated powerful pro-p group. We begin by defining the augmentation ideal.

Definition 3.10. For any group ring $R[G]$ the kernel of the natural map $\phi : R[G] \to R$ given by

$$\phi\Big(\sum_{g\in G} r_g g\Big) = \sum_{g\in G} r_g$$

is called the *augmentation ideal* of $R[G]$.

Proposition 3.11. *The augmentation ideal is in fact an ideal of the group ring $R[G]$ and is equal to $(G-1)R[G]$ (where $G-1 := \{g - 1_G \mid g \in G\}$).*

Proof. Let the augmentation ideal be denoted I. By the definition of the group ring it is clear that ϕ above satisfies $\phi(a+b) = \phi(a) + \phi(b)$ and to see it is a ring homomorphism note that

$$\phi\Big(\sum_{g\in G}\Big(\sum_{ab=g} r_a s_b\Big)g\Big) = \sum_{g\in G}\sum_{ab=g} r_a s_b = \sum_{a\in G} r_a \sum_{b\in G} s_b.$$

Thus, as the kernel of ϕ, I is an ideal. Now, for any $\sum_{g\in G} r_g g \in R[G]$,

$$\phi\Big(\sum_{g\in G} r_g(g-1)\Big) = \phi\Big(\sum_{g\in G} r_g g - \sum_{g\in G} r_g\Big) = 0$$

and so $(G-1)R \subseteq I$. Conversely, if $\sum_{g\in G} r_g g \in I$ then $\sum_{g\in G} r_g = 0$, so

$$\sum_{g\in G} r_g g = \sum_{g\in G} r_g g - \sum_{g\in G} r_g = \sum_{g\in G} (g-1) r_g$$

and we have the desired equality. □

We next prove a constructive result presented without proof in [DSMS91]. It will allow us to define the J-adic norm for any suitable ideal J and, in the next section, the J-adic completion.

Lemma 3.12. *Let R be a (non-zero) ring and*

$$R = R_0 \supseteq R_1 \supseteq \ldots \supseteq R_i \supseteq \ldots$$

a chain of ideals such that

- $\bigcap_{i\in\mathbb{N}} R_i = \{0\}$*;*
- *for all $i, j \in \mathbb{N}$, $R_i R_j \subseteq R_{i+j}$.*

Fix a real number $c > 1$, and define $||\cdot|| : R \to [0, \infty)$ by

$$||0|| = 0; \quad ||a|| = c^{-k} \text{ if } a \in R_k \backslash R_{k+1}.$$

Then $(R, ||\cdot||)$ is a normed ring.

Proof. That $||\cdot||$ is well defined is clear from the condition that the intersection over the entire chain is $\{0\}$, and hence for any $a \neq 0$ there exists an $n \in N$ such that $a \notin R_n$. Thus it suffices to verify the three ring norm axioms. Clearly $||a|| \geq 0$

for all $a \in R$, and supposing $1_R \in R_1$ we see that $1_R \in R_2 \supseteq R_1R_1$. By induction it follows that $1_R \in R_n$ for all n, contradicting $\bigcap_{i\in\mathbb{N}} R_i = \{0\}$ (as R is non-zero and so $1_R \neq 0$). Hence $1_R \in R\backslash R_1$ and $||1_R|| = c^0 = 1$.

Now we take $a, b \in R$ such that $a \in R_i\backslash R_{i+1}$ and $b \in R_j\backslash R_{j+1}$ where $i \leq j$. As $R_iR_j \subseteq R_{i+j}$ it follows that $ab \in R_{i+j}$ and hence that $||ab|| \leq c^{-(i+j)} = c^{-i}c^{-j} = ||a||\ ||b||$. Also, as $R_j \subseteq R_i$, $a \pm b \in R_i$ and hence $||a \pm b|| \leq c^{-i} = ||a|| = \max\{||a||, ||b||\}$. Thus $||\cdot||$ is indeed a ring norm on R. □

Suppose now that there is an ideal J of R such that $\bigcap_{i=1}^{\infty} J^i = \{0\}$, then setting $J^0 = R$ it follows that

$$R = J^0 \supseteq J^1 \supseteq \ldots \supseteq J^i \supseteq \ldots$$

is a decreasing family as in the above lemma. Hence we can define such a norm which, for any choice of c, is referred to as a *J-adic norm*.

Restricting ourselves to $R = \mathbb{Z}_p[G]$ where G is a finitely generated powerful pro-p group we can show that $J = I + p\mathbb{Z}_p[G]$ is such an ideal where $I = (G-1)\mathbb{Z}_p[G]$ is the augmentation ideal of $\mathbb{Z}_p[G]$ defined above. In fact, we demonstrate that J is suitable by showing it is cofinal with the descending chain of ideals

$$\mathbb{Z}_p[G] = I_0 \supseteq I_1 \supseteq \ldots \supseteq I_n \supseteq \ldots$$

where $I_n = (G_k - 1)\mathbb{Z}_p[G] = \ker(\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/G_k])$. We present two results from [DSMS91] to establish this.

Proposition 3.13. *Let $k \geq 1$. Then*

(i) $J^k \supseteq I_k + p^k\mathbb{Z}_p[G]$;

(ii) for each $j \geq 1$, $I_k + p^j\mathbb{Z}_p[G] \supseteq J^{m(k,j)}$ where $m(k,j) = j|G/G_k|$.

Proof. (i): By definition we have $J = I_1 + p\mathbb{Z}_p[G]$ so the claim holds for $k = 1$. We now proceed by induction assuming $k > 1$ and that $J^{k-1} \supseteq I_{k-1} + p^{k-1}\mathbb{Z}_p[G]$. As $p\mathbb{Z}_p[G] \supseteq J$ we have $p^k \in J^k$ and thus it suffices to prove $I_k \subseteq J^k$. As $I_k = (G_k - 1)\mathbb{Z}_p[G]$ it is enough to show that if $x \in G_k$ then $x \equiv 1 \pmod{J^k}$. Also since $G_k = G_{k-1}^p$, we need only check that $x^p \equiv 1 \pmod{J^k}$ for any $x \in G_{k-1}$.

Letting $u = x - 1$ we see that $u \in I_{k-1}$ and

$$x^p - 1 = (u+1)^p - 1 = u^p + puw$$

for some $w \in \mathbb{Z}_p[G]$. But by the inductive hypothesis $u \in J^{k-1}$, hence $u^p \in J^{k+p-1} \subseteq J^k$ as required.

(ii): As G is a pro-p group G/G_k is a finite p-group that acts by right multiplication on the $\mathbb{F}_p$ vector space $\mathbb{F}_p[G/G_k]$. Hence by Proposition 6.2 it is a unipotent group. As the dimension of $\mathbb{F}_p[G/G_k]$ is $n = |G/G_k|$ we have that for any $x_1, \ldots, x_n \in G/G_k$, $(x_1 - 1)\ldots(x_n - 1) = 0$ in $\mathbb{F}_p[G/G_k]$ (Proposition 6.3). But $\ker(\mathbb{Z}_p[G] \to \mathbb{Z}/p\mathbb{Z}[G/G_k]) = I_k + p\mathbb{Z}_p[G]$ and hence $(g_1 - 1)\ldots(g_n - 1) \in I_k + p\mathbb{Z}_p[G]$ for all $g_1, \ldots, g_n \in G$. Hence $J^n \subseteq I_k + p\mathbb{Z}_p[G]$, and thus $J^{nj} \subseteq I_k + p^j\mathbb{Z}_p[G]$ for all j. □

Corollary 3.14. *For J defined as above*

$$\bigcap_{l=1}^{\infty} J^l = \{0\}.$$

Proof. Let $c \in \mathbb{Z}_p[G]$, $c = \sum_{g\in G} c_g g$. As $c_g \neq 0$ for only finitely many $g \in G$ we can write $c = \sum_{i=1}^{n} c_{g_i} g_i$. Hence there exists an l such that $c_{g_i} \not\equiv 0 \pmod{p^l}$ for all i as well as an m such that $x_i x_j^{-1} \notin G_m$ for all $i \neq j$ (as the x_i's are distinct). Letting $k = \max\{l, m\}$ it follows that if ϕ is the natural map

$$\phi : \mathbb{Z}_p[G] \to (\mathbb{Z}/p^k\mathbb{Z})[G/G_k]$$

the image of x_i in G/G_k is distinct from that of x_j for $i \neq j$. Thus $\phi(c) \neq 0$ and hence $c \notin I_k + p^k\mathbb{Z}_p[G] \supseteq J^m$ for some m (by the proposition above). □

Thus we define the J-adic norm $||\cdot|| : \mathbb{Z}_p[G] \to [0, \infty)$ by

$$\begin{aligned} ||0|| &= 0 \\ ||a|| &= p^{-k} \text{ if } a \in J^k \backslash J^{k+1}. \end{aligned}$$

Our choice of $c = p$ is as we want our norm to be consistent with that on $\mathbb{Z}_p$. It is clear that $\mathbb{Z}_p$ is a subalgebra and as $1 \notin (G-1)\mathbb{Z}_p[G]$, $p^k\mathbb{Z}_p \subseteq p^k\mathbb{Z}_p[G] \subseteq J^k$, and $p^k\mathbb{Z}_p \cap J^{k+1} = p^{k+1}\mathbb{Z}_p$. Hence for any $x \in \mathbb{Z}_p$, $|x|_p = ||x||$. We conclude our discussion on the J-adic norm by assuring that the topology on $\mathbb{Z}_p[G]$ also agrees with the profinite group topology on G.

Proposition 3.15. *The topology induced upon G (as a subset of $\mathbb{Z}_p[G]$) by $||\cdot||$ coincides with the original topology on G.*

Proof. Let $\overline{B}(1, \theta)$ be the closed ball of radius θ about 1 in $\mathbb{Z}_p[G]$ (which is also open). As G is a pro-p group we know that the open normal subgroups G_k ($k \geq 1$) form a base for the neighbourhoods of the identity [D, Proposition 1.16 (iii)]. Thus it suffices to show that for any k there exists $m, n \in \mathbb{Z}$ such that

$$G \cap \overline{B}(1, p^{-m}) \subseteq G_k \subseteq G \cap \overline{B}(1, p^{-n}).$$

Suppose $x \in G_k$. By Lemma 2.2 (i) above we have $J^k \supseteq I_k + p^k\mathbb{Z}_p[G]$, and thus $I_k = (G_k - 1)\mathbb{Z}_p[G] \subseteq J^k$. Hence $x - 1 \in J^k$ and thus $||x - 1|| \leq p^{-k}$. Setting $n = k$ now gives us the right inclusion.

For the left inclusion we assume $x \in G$ and $x - 1 \in I_k + p\mathbb{Z}_p[G]$. That is $x \in \ker(\phi)$ where

$$\phi : \mathbb{Z}_p[G] \to \mathbb{Z}/\mathbb{Z}_p[G/G_k]$$

so $x \in G_k$. This is clear since the image of $x - 1$ under the natural map $\mathbb{Z}_p[G] \to \mathbb{Z}/\mathbb{Z}_p[G]$ (which has kernel $p\mathbb{Z}_p[G]$) is just $x - 1$, and hence $x \equiv 1 \pmod{G_k}$. By Lemma 2.2 (ii) we have $I_k + p\mathbb{Z}_p[G] \supseteq J^m$ where $m = |G/G_k|$. Hence if $x \in G \cap \overline{B}(1, p^{-|G/Gk|})$ then $x \in G_k$ as required. □

Our selection of $c = p$ thus seems quite justified. We will however demonstrate that any choice of c gives rise to the same completion of the ring $\mathbb{Z}_p[G]$ under the J-adic norm.

3.3 Completing the Group Algebra

It is clear that our definition of the ring norm gives our normed ring all the properties of a metric space with metric $d(a, b) = ||a - b||$. Hence the property that every normed ring R has a unique completion (up to isometry) follows from the well known metric space result, and so we merely mention it here. We use this to define the J-adic completion in the obvious manner.

Theorem 3.16. *If $(R, ||\cdot||)$ is a normed ring then there exists a completion of $\hat{R}$ of R which is unique up to isomorphism. That is, given any other completion $\tilde{R}$ there exists a norm preserving isomorphism $\phi : \hat{R} \to \tilde{R}$ such that $\phi\big|_R = id_R$.*

Proof. Omitted. □

Definition 3.17. The unique completion of a ring R with respect to a J-adic norm for some ideal J is called the *J-adic completion* of R.

We are finally in position to state our version of Theorem B:

Theorem 3.18. *For any finitely generated powerful pro-p group G*

$$\Lambda_G \cong \hat{R}$$

where, as above, $\hat{R}$ is the completion of the group algebra with respect to the J-adic norm where $J = I + p\mathbb{Z}_p[G]$.

That is in the case for $\mathbb{Z}_p$ we have the Iwasawa Algebra isomorphic to the J-adic completion of $\mathbb{Z}_p[G]$. This result makes that presented in Theorem B somewhat intuitive as of course if $R = \mathbb{F}_p[G]$ then $pR = 0$. Though this is not in any way a proof, just a reassuring observation.

We establish Theorem 3.18 in three steps. First we show that $\hat{R} \cong \tilde{R} := \varprojlim_i (\mathbb{Z}_p[G]/J^i)$ which follows immediately from the following.

Lemma 3.19. *Let R be a ring with J-adic norm $||\cdot||$, then*

$$\hat{R} \cong \varprojlim_i (R/J^i).$$

Proof. Suppose first that $(a_i + J^i) \in \tilde{R}$, and take any $i > 0$. Note by the definition of the inverse limit we have that $a_j \equiv a_i \pmod{J^i}$ for all $j \geq i$. Hence for all $j, k \geq i$, $||a_j - a_k|| \leq p^{-i}$ (as $a_j - a_k \in J^i$) and it follows that (a_i) is Cauchy in R. Now, if $\iota : \tilde{R} \to \hat{R}$ is given by $\iota((r_i + J^i)) = \lim r_i$ it is clear that ι is well defined. Also, by the algebra of limits established in Section 3.1, ι is a ring homomorphism.

For any $(a_i + J^i) \in \varprojlim_i (R/J^i)$ if $\iota((a_i + J^i)) = 0$ then for any $n > 0$ there exists an I such that $||a_i|| < p^{-n}$ for all $i > I$. That is, $a_i \in J^n$ and it follows by the definition of the inverse limit that $a_j \in J^n$ for all $j < i$. Thus for all $j < n$,

$a_j \equiv 0 \pmod{p^j}$ and as n was arbitrary it follows that $(a_i + J^i) = 0$ and ι is injective. To show ι is also surjective take any $r \in \hat{R}$ and let $\{r_i\} \subseteq R$ be a Cauchy sequence converging to r. We know that for any i we can find $n(i)$ such that for all $j, k \geq n(i)$, $||r_j - r_k|| < p^{-i}$. This gives us that $r_j - r_k \in J^i$, an in particular for all $j \geq n(i)$, $r_j \equiv r_{n(i)} \pmod{J^i}$. Hence $(r_{n(i)} + J^i) \in \tilde{R}$ and clearly $\iota((r_{n(i)} + J^i)) = r$. So ι is the required isomorphism. □

Note that the J-adic norm is often defined as this inverse limit. Also as the inverse limit does not depends at all on the norm we have shown, as claimed earlier, that the choice of c in Lemma 3.12 does not effect the completion. Our second step is showing that $\varprojlim_i(\mathbb{Z}_p[G]/J^i) \cong \varprojlim_k(\mathbb{Z}_p[G]/I_k + p^k\mathbb{Z}_p[G])$ though we again prove a more general result of which this is an easy consequence.

Lemma 3.20. *Suppose R is a ring and $\{A_m\}$ and $\{B_n\}$ are cofinal descending chains of ideals then,*

$$\varprojlim_m(R/A_m) \cong \varprojlim_n(R/B_n).$$

Proof. By definition we can assume there exists $a, b : \mathbb{N} \to \mathbb{N}$ such that $A_k \supseteq B_{b(k)}$ and $B_k \supseteq A_{a(k)}$. Without loss of generality, assume $a(k) \geq k$ and $b(k) \geq k$. Define $\phi : \varprojlim(R/A_m) \to \varprojlim(R/B_n)$ by $(r_m + A_m) \mapsto (r_{a(n)} + B_n)$. As $r_j \equiv r_i \pmod{A_i}$ for all $j \geq i$ it is clear that $r_{a(j)} \equiv r_{a(i)} \pmod{B_i}$ for all $j \geq i$, and thus ϕ is well defined.

We see ϕ is injective as if $\phi((r_m + A_m)) = 0$ then $r_{a(k)} \equiv 0 \pmod{B_k}$ and hence $r_{a(k)} \equiv 0 \pmod{A_{b(k)}}$. Note that, if $r_j \equiv 0 \pmod{A_j}$ we have $r_i \equiv 0 \pmod{A_i}$ for all $i \leq j$ and so $r_j \equiv 0 \pmod{A_j}$ for all $j < k$. As k is arbitrary large $(r_m + A_m) = 0$.

Finally, to show ϕ is surjective, take any $(s_n + B_n) \in \varprojlim(R/B_n)$, then consider $(s_{b(m)} + A_m)$ (and element of $\varprojlim(R/A_m)$ by the same argument as above). Now $\phi((s_{b(m)} + A_m)) = (s_{b\circ a(n)} + B_n)$. But as $b \circ a(k) \geq k$ we see that for all k, $s_{b\circ a(k)} \equiv s_k \pmod{B_k}$ and hence

$$\phi((s_{b(m)} + A_m)) = (s_{b\circ a(n)} + B_n) = (s_n + B_n)$$

and it follows that ϕ is onto and an isomorphism. □

If we note that the kernel of the map $\mathbb{Z}_p[G] \to \mathbb{Z}/p^k\mathbb{Z}[G/G_k]$ is $I_k + p^k\mathbb{Z}_p[G]$ it is clear from the above that

$$\hat{R} \cong \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}[G/G_k].$$

We can now complete the proof of Theorem 3.18.

Proof of Theorem 3.18. It suffices to show that there exists an isomorphism

$$\psi : \mathbb{Z}_p[[G]] \to \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}[G/G_k].$$

Recalling that $G_i \triangleleft_o G$, we let π_i be the natural homomorphism from $\mathbb{Z}_p[[G]]$ to $\mathbb{Z}_p[G/G_i]$. There is also a natural projection $\rho_i : \mathbb{Z}_p[G/G_i] \to \mathbb{Z}/p^i\mathbb{Z}[G/G_i]$ and hence the pair $(\mathbb{Z}_p[[G]], \phi_i)$ is also an inverse system for $\mathbb{Z}/p^k\mathbb{Z}[G/G_k]$ where

$$\phi_i = \rho_i \circ \pi_i.$$

Thus by the universal property of inverse limits, Proposition 1.9, there exists a homomorphism

$$\psi : \mathbb{Z}_p[[G]] \to \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}[G/G_k]$$

defined by $x \mapsto (\phi_i(x))_i$. Now if we take any $(h_k) \in \varprojlim \mathbb{Z}/p^k\mathbb{Z}[G/G_k]$ then it is clear that for each k the set

$$\Lambda_k = \{x \in \mathbb{Z}_p[G/G_k] \mid \rho_k(x) = h_k\}$$

is non-empty. These sets are also compact as they are merely the inverse image in $\mathbb{Z}_p^{[G:G_k]}$ of a point in $(\mathbb{Z}/p^k\mathbb{Z})^{[G:G_k]}$. It follows by Proposition 1.27 that there exists a $(g_k) \in \varprojlim \mathbb{Z}_p[G/G_k]$ such that $\rho_k(g_k) = h_k$ for all k. We then define $s_N \in \mathbb{Z}_p[G/N]$ such that $s_{G_k} = g_k$ and s_N by $\varphi_{N,G_k}(g_k)$ where $G_k \leq N$ and $\{\varphi_{N,M}\}$ is the family of maps in the inverse system leading to the Iwasawa algebra. The value of s_N then clearly does not depend on the k used (as long as $G_k \leq N$) and as there is always one such G_k our s_N are well defined. It follows from this definition that $\psi((s_N)) = (h_k)$ and ψ is surjective.

To show that ψ is in fact an isomorphism suppose $\psi((g_N + N)) = 0$. It follows that $g_{G_i} = 0$ for all i. But G_i is a system of neighbourhoods for the identity, and so for all $N \triangleleft_o G$ there exists an i such that $G_j \leq N$ for all $j \geq i$, and hence (by a similar argument to that above) $g_N = 0$ for all $N \triangleleft_o G$. Thus ψ is injective and an isomorphism. □

We have now developed most of the algebraic background for us to study Lazard's theorem, and it is it we move to in the next chapter. As mentioned, however, the notion of the J-adic norm and the cofinal chains of ideals, J^i and $I_k + p^k\mathbb{Z}_p[G]$ are used in depth in Section 4.3. There we investigate some deeper properties of the group algebra and apply them to the proof of our main result.

Chapter 4

p-adic Analytic Groups

We are now ready to present the theory of p-adic analytic groups and the proof that every topological group containing a finitely generated pro-p group is a p-adic analytic manifold. We begin by defining the notions of p-adic analytic functions and p-adic analytic manifolds in the natural manner, and establishing the properties we expect analytic functions to have. As mentioned, the third section extends much of the material presented in Chapter 3 on the group algebra to prove that a certain class of p-adic function, defined with respect to a uniform pro-p group, is analytic. This is essentially gives us that each uniform pro-p group is a p-adic analytic group, and helps us extend this to our major proof.

The main reference for this chapter, and the origin of the proof of Theorem A which that presented is modelled on, is Chapter 8 [DSMS91]. It was used alongside Chapter 6 & 7 [DSMS91] and [Ser65], though the exposition here has been somewhat streamlined as it is presented specifically with the end goal of Lazard's Theorem in mind.

4.1 p-adic Analytic Functions

Before we can give our definition of a p-adic analytic manifold, we need to develop a notion of what it means for a function $f : \mathbb{Z}_p^r \to \mathbb{Z}_p^s$ to be analytic. Over $\mathbb{R}$ and $\mathbb{C}$ an analytic function has a convergent Taylor series expansion in a neighbourhood of each point in its domain. But what is a neighbourhood in $\mathbb{Z}_p^r$.

The topology on $\mathbb{Q}_p^r$ is merely the product topology, that is $O \subseteq_o \mathbb{Z}_p^r$ if and only if $O = O_1 \times O_2 \times \ldots \times O_r$ where $O_i \subseteq_o \mathbb{Q}_p$. We know that $B(a, p^{-h})$ form a basis for the open sets in $\mathbb{Q}_p$. Thus as the product is finite, for any $O = O_1 \times \ldots \times O_n \subseteq_o \mathbb{Q}_p^r$ and any $\mathbf{a} \in O$ we have an h such that $B(a_i, p^{-h}) \subseteq_o O_i$ for all i. It follows that if we define

$$B(\mathbf{a}, p^{-h}) = \{\mathbf{x} \in \mathbb{Q}_p^r \mid |x_i - a_i|_p < p^{-h}, \text{ for all } i\}$$

for all $O \subseteq_o \mathbb{Q}_p^r$ and any $\mathbf{a} \in O$ there exists an h such that $B(\mathbf{a}, p^{-h}) \subseteq O$. The subset defined above is the natural way, in fact, to define the r dimensional open ball in $\mathbb{Q}_p^r$. It is due to the ultrametric quality of the absolute value that this is more reminiscent to the max norm, $||\cdot||_\infty$ in $\mathbb{R}^n$ than the usual Euclidean norm. It is clear that we can equivalently write our r-dimensional ball as

$$B(\mathbf{x}, p^{-h}) = \{\mathbf{x} + p^h\mathbf{y} \mid \mathbf{y} \in \mathbb{Z}_p^r\}.$$

Recall that if $\mathbf{X} = (X_1, \ldots, X_r)$ and $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$ we set

$$\mathbf{X}^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_r^{\alpha_r}.$$

Definition 4.1. The *ring of formal power series* in the (commuting) variables $X_1, \ldots, X_r$ is the set of formal power series

$$F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{X}^\alpha$$

such that $c_\alpha \in \mathbb{Q}_p$ for all $\alpha \in \mathbb{N}^r$. We denote this ring $\mathbb{Q}_p[[\mathbf{X}]]$ or $\mathbb{Q}_p[[X_1, \ldots, X_r]]$.

We say that such a series can be *evaluated* at $\mathbf{x} \in \mathbb{Q}_p^r$ if

$$F(\mathbf{x}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{x}^\alpha$$

converges in $\mathbb{Q}_p^r$.

It is worth noting that we are able to define power series similarly over non-commuting variables, as to define the notion of a analytic function over an arbitrary normed $\mathbb{Q}_p$ algebra. However, as stated above, we are reducing to the case where our $\mathbb{Q}_p$-algebra is $\mathbb{Q}_p^r$ itself and so such generality is unnecessary in this thesis.

Definition 4.2. A function $f : D \to \mathbb{Q}_p$ where $D \subseteq_o \mathbb{Q}_p^r$ $(D \neq \varnothing)$ is said to be *strictly analytic* on D if there exists $F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]]$ such that for all $\mathbf{x} \in D$

(a) $\lim_{\alpha \in N^r} |c_\alpha|_p |x_1|_p^{\alpha_1} \ldots |x_r|_p^{\alpha_r} = 0$; and,
(b) $F(\mathbf{x}) = f(\mathbf{x})$.

So a function is strictly analytic when it has a convergent formal power series representation on the entirety of its domain satisfying the 'absolute convergence' condition (a). However, we want to mirror the definition for real and complex functions and only require an analytic function to have a power series representation in a neighbourhood of each point of its domain. Before we define analytic functions however we establish the reassuring result below.

Proposition 4.3. *If $f : D \subseteq_o \mathbb{Q}_p^r \to \mathbb{Q}_p$ is strictly analytic on D then f is continuous on D.*

Proof. It suffices to show that for any $\mathbf{x} \in D$, and any $\epsilon > 0$, there exists a $\delta > 0$ such that for all $\mathbf{y} \in B(\mathbf{x}, \delta)$, $|f(\mathbf{y}) - f(\mathbf{x})|_p < \epsilon$. Pick arbitrary $\mathbf{x} \in D$ and $\epsilon > 0$, and let $F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]]$ be such that $F(\mathbf{x}) = f(\mathbf{x})$ for all $\mathbf{x} \in D$. We know, as r is finite and D is open, that there exists a common $h \in \mathbb{N}$ such that $|x_i|_p > p^{-h}$ whenever $x_i \neq 0$ and $\overline{B}(\mathbf{x}, p^{-h}) \subseteq D$. It follows that if $\mathbf{z}$ is defined by

$$\begin{aligned} z_i &= x_i \text{ if } x_i \neq 0 \\ z_i &= p^h \text{ if } x_i = 0 \end{aligned}$$

then $\mathbf{z} \in \overline{B}(\mathbf{x}, p^{-h})$. Now take any $\mathbf{y} \in \overline{B}(\mathbf{x}, p^{-h})$. If $x_i = 0$ it is obvious that $|y_i|_p \leq |z_i|_p$. Otherwise, if $x_i \neq 0$, $|x_i - y_i|_p \leq |z_i|_p$. But $|x_i - y_i|_p \neq \max\{|x_i|_p, |y_i|_p\}$

if and only if $|y_i|_p = |x_i|_p$ but $|x_i|_p = |z_i|_p$. It follows that for all i, $|y_i|_p \leq |z_i|_p$. Also as $\mathbf{z} \in D$

$$\lim_{\alpha \in \mathbb{N}^r} |c_\alpha|_p |z_1|_p^{\alpha_1} \dots |z_r|_p^{\alpha_r} = 0.$$

It follows that there exists finite $S \subseteq \mathbb{N}^r$ such that for all $\alpha \in \mathbb{N}^r \backslash S$,

$$|c_\alpha|_p |z_1|_p^{\alpha_1} \dots |z_r|_p^{\alpha_r} < \epsilon.$$

Hence, for all such α and any $\mathbf{y} \in \overline{B}(\mathbf{x}, p^{-h})$, $|c_\alpha|_p |y_1|_p^{\alpha_1} \dots |y_r|_p^{\alpha_r} < \epsilon$, and thus by the ultrametric property

$$|c_\alpha(\mathbf{x}^\alpha - \mathbf{y}^\alpha)|_p < \epsilon.$$

Now we consider $\alpha \in S$. For ease of notation let a_i be defined as follows:

$$a_i = \begin{cases} x_1 & : \ i \leq \alpha_1 \\ x_2 & : \ \alpha_1 < i \leq \alpha_1 + \alpha_2 \\ \vdots & \\ x_r & : \ \langle \alpha \rangle - \alpha_r < i \leq \langle \alpha \rangle \end{cases}$$

Define b_i similarly for y_i, then

$$\begin{aligned} |\mathbf{x}^\alpha - \mathbf{y}^\alpha|_p &= |a_1 \dots a_{\langle \alpha \rangle} - b_1 \dots b_{\langle \alpha \rangle}|_p \\ &= |(a_1 - b_1)a_2 \dots a_{\langle \alpha \rangle} + b_1(a_2 - b_2)a_3 \dots a_{\langle \alpha \rangle} + \dots \\ &\qquad + b_1 \dots b_{\langle \alpha \rangle - 1}(a_{\langle \alpha \rangle} - b_{\langle \alpha \rangle})|_p \\ &\leq \max_i |z_i|_p^{\langle \alpha \rangle - 1} \max_i |x_i - y_i|_p. \end{aligned}$$

As $|c_\alpha| \max_i |z_i|_p^{\langle \alpha \rangle - 1}$ only takes on finitely many values for $\alpha \in S$, there must exist a $\delta > 0$ (which we can assume without loss of generality to be less than p^{-h}) such that $|\mathbf{x}^\alpha - \mathbf{y}^\alpha|_p < \epsilon$ for all $\mathbf{y} \in \overline{B}(\mathbf{x}, \delta)$. It follows then from Proposition 3.5 (iii) that for all such $\mathbf{y}$

$$|f(\mathbf{x}) - f(\mathbf{y})|_p = |F(\mathbf{x}) - F(\mathbf{y})|_p \leq \sup_{\alpha \in \mathbb{N}^r} |c_\alpha(\mathbf{x}^\alpha - \mathbf{y}^\alpha)|_p < \epsilon.$$

Thus as $\mathbf{x} \in D$ was arbitrary, f is continuous on D. □

We present our definition of an analytic function below. One will note, however, that we have reduced to only considering functions from $\mathbb{Z}_p^m$ to $\mathbb{Z}_p^n$. This distinction is useful as we will be dealing with power series requiring the condition (a) in Definition 4.2, and clearly if $\mathbf{x} \in \mathbb{Z}_p^r$ to establish (a) it is sufficient (but not necessary) to show

$$\lim_{\alpha \in \mathbb{N}^r} |c_\alpha|_p = 0.$$

Also, as we will define the p-adic analytic manifold over $\mathbb{Z}_p$ (not $\mathbb{Q}_p$), we need only consider functions of this type. In the following section it will be established that we have not reduced our class of manifolds by defining them over $\mathbb{Z}_p$.

Definition 4.4. Let $\mathbf{f} = (f_1, \dots, f_m) : V \to \mathbb{Z}_p^m$ where $V \subseteq_o \mathbb{Z}_p^n$, and take any $\mathbf{y} \in V$. Then $\mathbf{f}$ is *analytic* at $\mathbf{y}$ if there exists an $h \in \mathbb{N}$ such that $\mathbf{x} \mapsto f_i(\mathbf{y} + p^h \mathbf{x})$

is strictly analytic on $\mathbb{Z}_p^n$ for each $i = 1, \ldots, m$. The function $\mathbf{f}$ is *analytic on* V if it is analytic at $\mathbf{y}$ for all $\mathbf{y} \in V$.

That is, f_i is analytic at $\mathbf{y}$ if there exists a ball $B(\mathbf{y}, p^{-h})$ and an $F_i[\mathbf{X}] \in \mathbb{Q}_p[[\mathbf{X}]]$ such that $f_i(\mathbf{y} + p^h\mathbf{x}) = F_i(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_p^r$. The following is obvious from the definition of a p-adic analytic function, and Proposition 4.3.

Proposition 4.5. *If $f : V \subseteq_o \mathbb{Z}_p^r \to \mathbb{Z}_p^s$ is analytic then f is continuous.*

When considering real and complex analytic functions we know that if f has a Taylor series expansion in a neighbourhood about a point, then f is analytic at all points in the neighbourhood. We would clearly like the same to be true for $f : V \subseteq \mathbb{Z}_p^r \to \mathbb{Z}_p$ analytic at $\mathbf{y} \in V$, though while we have some $h \in \mathbb{N}, F[\mathbf{X}] \in \mathbb{Q}_p[[\mathbf{X}]]$ such that $f(\mathbf{y} + p^h\mathbf{x}) = F(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_p^r$ it is not directly clear from our definition that f is analytic at all points in $B(\mathbf{y}, p^{-h})$. we rectify this below, though beginning with a lemma.

Lemma 4.6. *For any $F[\mathbf{X}] \in \mathbb{Q}_p[[\mathbf{X}]]$ that can be evaluated for all $\mathbf{x} \in \mathbb{Z}_p^r$, and any $\mathbf{a} \in \mathbb{Z}_p^r$ there exists a $G[\mathbf{X}] \in \mathbb{Q}_p[[\mathbf{X}]]$ such that for all $\mathbf{x} \in \mathbb{Z}_p^r$, $G(\mathbf{x}) = F(\mathbf{x}+\mathbf{a})$.*

Proof. Suppose $F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} c_\alpha \mathbf{X}^\alpha$. Then for any $\mathbf{x} \in \mathbb{Z}_p^r$

$$\begin{aligned} F(\mathbf{x}+\mathbf{a}) &= \sum_{\alpha \in \mathbb{N}^r} c_\alpha (x_1 + a_1)^{\alpha_1} \ldots (x_d + a_d)^{\alpha_d} \\ &= \sum_{\alpha \in \mathbb{N}^r} \sum_{\beta \in \mathbb{N}^r} c_\alpha \binom{\alpha_1}{\beta_1} \ldots \binom{\alpha_d}{\beta_d} a_1^{\alpha_1 - \beta_1} \ldots a_d^{\alpha_d - \beta_d} x_1^{\beta_1} \ldots x_d^{\beta_d} \\ &= \sum_{\alpha \in \mathbb{N}^r} \sum_{\beta \in \mathbb{N}^r} d_{\alpha,\beta} \mathbf{x}^\beta. \end{aligned}$$

As $\binom{\alpha_i}{\beta_i} = 0$ whenever $\beta_i > \alpha_i$ we have that for any fixed $\alpha \in \mathbb{N}^r$, $d_{\alpha,\beta} = 0$ for all but finitely many $\beta \in \mathbb{N}^r$. By assumption F can be evaluated at $(1, 1, \ldots, 1)$ and thus $\sum_{\alpha \in \mathbb{N}^r} c_\alpha$ converges implying that $\lim_{\alpha \in \mathbb{N}^r} c_\alpha = 0$. However, it is easy to see that

$$\binom{\alpha_1}{\beta_1} \ldots \binom{\alpha_d}{\beta_d} a_1^{\alpha_1 - \beta_1} \ldots a_d^{\alpha_d - \beta_d} \in \mathbb{Z}_p$$

and hence

$$\left| \binom{\alpha_1}{\beta_1} \ldots \binom{\alpha_d}{\beta_d} a_1^{\alpha_1 - \beta_1} \ldots a_d^{\alpha_d - \beta_d} \right|_p \leq 1.$$

Thus $|d_{\alpha,\beta}|_p \leq |c_\alpha|_p$ for all $\alpha, \beta \in \mathbb{N}^r$. It is clear then that $\lim_{(\alpha,\beta) \in \mathbb{N}^r \times \mathbb{N}^r} d_{\alpha,\beta} = 0$, and Corollary 3.7 gives that the double sum converges and

$$\sum_{\alpha \in \mathbb{N}^r} \sum_{\beta \in \mathbb{N}^r} d_{\alpha,\beta} \mathbf{x}^\beta = \sum_{\beta \in \mathbb{N}^r} \sum_{\alpha \in \mathbb{N}^r} d_{\alpha,\beta} \mathbf{x}^\beta.$$

Hence setting $G(\mathbf{X}) = \sum_{\beta \in \mathbb{N}^r} e_\beta \mathbf{x}^\beta$ where $e_\beta = \sum_{\alpha \in \mathbb{N}^r} d_{\alpha,\beta}$ suffices. □

Proposition 4.7. *Let $f : V \to \mathbb{Z}_p$ be a function. If $\mathbf{x} \mapsto f(\mathbf{y} + p^h\mathbf{x})$ is strictly analytic on $\mathbb{Z}_p^r$ for some h then f is analytic on $B(\mathbf{y}, p^{-h})$.*

Proof. Let $F(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ such that $F(\mathbf{x}) = f(\mathbf{y} + p^h\mathbf{x})$ for all $\mathbf{x}$ in $\mathbb{Z}_p^r$. If $\mathbf{y_0} \in B(\mathbf{y}, p^{-h})$ then $p^{-h}(\mathbf{y_0} - \mathbf{y}) \in \mathbb{Z}_p^r$ and thus

$$F(p^{-h}(\mathbf{y_0} - \mathbf{y}) + \mathbf{x}) = f(\mathbf{y} + p^h(p^{-h}(\mathbf{y_0} + \mathbf{y}) + \mathbf{x})) = f(\mathbf{y_0} + p^h\mathbf{x}).$$

Then by the previous lemma there exists a $G(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ such that $G(\mathbf{x}) = f(\mathbf{y_0} + p^h\mathbf{x})$ for all $x \in \mathbb{Z}_p^r$. Hence f is analytic at $\mathbf{y_0}$, and as $\mathbf{y_0}$ was arbitrary, f is analytic on $B(\mathbf{y}, p^{-h})$. □

The following corollary is now obvious.

Corollary 4.8. *Suppose that $f : V \to \mathbb{Z}_p$ where $V \subseteq_o \mathbb{Z}_p^r$ is the union of balls in $\mathbb{Z}_p^r$. That is,*

$$V = \bigcup_{i \in I} B(\mathbf{y_i}, p^{-h_i}).$$

If $\mathbf{x} \mapsto f(\mathbf{y_i} + p^{h_i}\mathbf{x})$ is strictly analytic on $\mathbb{Z}_p^r$ for all i then f is analytic.

Proposition 4.7 also implies that if $f : \mathbb{Z}_p^r \to \mathbb{Z}_p$ is strictly analytic on $\mathbb{Z}_p^r$ then it is analytic on $\mathbb{Z}_p^r$. These results are also useful in demonstrating that particular functions are analytic as in the following example.

Example 4.9. [$f(z) = 1/z$ is analytic on $\mathbb{Z}_p^\times$.]

Recall that the inverse function $f(z) = 1/z$ is defined on $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$, and consider the $p-1$ (additive) cosets of $p\mathbb{Z}_p$, $\{a - p\mathbb{Z}_p \mid a = 1, \ldots, p-1\}$ on which f is defined. Clearly then, for any $x \in \mathbb{Z}_p$

$$\frac{1}{a - px} = \frac{\frac{1}{a}}{1 - \frac{1}{a}px} = \sum_{k=0}^{\infty} \frac{1}{a^{k+1}} p^k x^k.$$

Thus, as $|\frac{1}{a^{k+1}}|_p = 1 \geq |x^k|_p$ and $|p^k|_p = p^{-k}$ the map $x \mapsto f(a + px)$ is strictly analytic on $\mathbb{Z}_p$ for all $a = 1, \ldots, p-1$. If follows by Corollary 4.8 that $f(z) = 1/z$ is analytic on $\mathbb{Z}_p \backslash p\mathbb{Z}_p$ as claimed. □

Another result we expect from the corresponding theory over the real and complex numbers is that the composition of analytic functions is analytic. While we could have established a similar result for strictly analytic functions we simplify the theory presented and just establish the following as it is all we require.

Proposition 4.10. *Let $\mathbf{f} : U \to V$, $\mathbf{g} : V \to W$ where $U \subseteq \mathbb{Z}_p^r$, $V \subseteq \mathbb{Z}_p^s$, and $W \subseteq \mathbb{Z}_p^t$ are non-empty and open. If $\mathbf{f}$ and $\mathbf{g}$ are analytic on U and V respectively then $\mathbf{g} \circ \mathbf{f}$ is analytic on U.*

Proof. Clearly it suffices to show that $g_i \circ \mathbf{f}$ is analytic on U for all i and hence we assume without loss of generality that $t = 1$. Now, take any $\mathbf{z} \in U$. As both $\mathbf{f}$ and g are analytic we know that there exists power series

$$F_i(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^r} b_\alpha(i)\mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]], \quad G(\mathbf{Y}) = \sum_{\beta \in \mathbb{N}^s} c_\beta \mathbf{Y}^\beta \in \mathbb{Q}_p[[\mathbf{Y}]]$$

and $h_1, h_2 \in \mathbb{N}$ such that $f_i(\mathbf{z} + p^{h_1}\mathbf{x}) = F_i(\mathbf{x})$ for all i and all $\mathbf{x} \in \mathbb{Z}_p^r$, and $g(\mathbf{f}(\mathbf{z}) + p^{h_2}\mathbf{y}) = G(\mathbf{y})$ for all $\mathbf{y} \in \mathbb{Z}_p^s$.

Claim 1: We can assume that $\mathbf{f}(\mathbf{y} + p^{h_1}\mathbb{Z}_p^r) \subseteq B(\mathbf{f}(\mathbf{z}), p^{-h_2})$ without loss of generality.

Take any $\mathbf{x} \in \mathbb{Z}_p^r$. As F_i is continuous for all i (Proposition 4.3) we have that there exists $k \in \mathbb{N}$ such that, for each i,

$$|f_i(\mathbf{z}) - f_i(\mathbf{z} + p^{h_1+k}\mathbf{x})|_p < p^{-h_2}.$$

We can then consider $\tilde{F}_i[[\mathbf{X}]] = \sum_{\alpha\in\mathbb{N}^r} \tilde{b}_\alpha(i)\mathbf{X}^\alpha$ defined by $\tilde{b}_\alpha(i) = p^{-k\langle\alpha\rangle}b_\alpha(i)$ which is obviously in $\mathbb{Q}_p[[\mathbf{X}]]$ and $f_i(\mathbf{z} + p^{h_1+k}\mathbf{x}) = \tilde{F}_i(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_p^r$. So $\mathbf{x} \mapsto f_i(\mathbf{z} + p^{h_1+k}\mathbf{x})$ is strictly analytic on $\mathbb{Z}_p^r$ and the claim follows.

By assuming that shown in Claim 1 we have that, for all $\mathbf{x} \in \mathbb{Z}_p^r$,

$$g(\mathbf{f}(\mathbf{z} + p^{h_1}\mathbf{x})) = G(\mathbf{w})$$

where $w_i = p^{-h_2}(F_i(\mathbf{x}) - f_i(\mathbf{z}))$. Our aim is to represent $G(\mathbf{w})$ by a power series in $\mathbf{X}$ but first require the following:

Claim 2: We can assume that $b_\alpha(i) \in \mathbb{Z}_p$ for all i and all $\alpha \in \mathbb{N}^r$ without loss of generality.

We show first that for each i there exists a k_i such that $p^{k_i}b_\alpha(i) \in \mathbb{Z}_p$ for each $\alpha \in \mathbb{N}^r$. Fix an i and take $\mathbf{x} = (1, 1, \ldots, 1) \in \mathbb{Z}_p^r$. As F_i is strictly analytic on all of $\mathbb{Z}_p^r$ we have that $\lim_{\alpha\in\mathbb{N}^r} |b_\alpha(i)|_p|x_1|_p^{\alpha_1} \ldots |x_r|_p^{\alpha_r} = 0$. Hence $\lim_{\alpha\in\mathbb{N}^r} |b_\alpha(i)|_p = 0$, and thus $|b_\alpha(i)|_p \leq p^{k_i}$ for some $k_i \in \mathbb{Z}$. Now as there are only finitely many i we can set $k = \max\{0, \max_i\{k_i\}\}$, and then for all $\alpha \in \mathbb{N}^r$ and all i

$$p^k b_\alpha(i) \in \mathbb{Z}_p^r.$$

Now for each i, as in the proof of Claim 1, we take $\hat{F}_i(\mathbf{X}) = \sum_{\alpha\in\mathbb{N}^r} \hat{b}_\alpha(i)\mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]]$, where $\hat{b}_\alpha(i) = p^{\langle\alpha\rangle k}b_\alpha(i)$. Then clearly $f_i(\mathbf{z} + p^{h_1+k}\mathbf{x}) = F_i(p^k\mathbf{x}) = \hat{F}_i(\mathbf{x})$ and it follows that for all $\alpha \in \mathbb{N}^r$, $\hat{b}_\alpha(i) \in \mathbb{Z}_p^r$ and our claim is established.

It is clear from the proof of Claim 2 that we can equivalently assume that $p^{-h_2}b_\alpha(i) \in \mathbb{Z}_p^r$ for each $\alpha \in \mathbb{N}^r$ and each i, and we do so. Then defining $E_i(\mathbf{X}) = p^{-h}(F_i(\mathbf{X}) - f_i(\mathbf{z})) \in \mathbb{Q}_p[[\mathbf{X}]]$ we see that if $E_i(\mathbf{X}) = \sum_{\alpha\in\mathbb{N}^r} e_\alpha(i)\mathbf{X}^\alpha$ then for all i, $e_{\mathbf{0}}(i) = 0$ and $e_\alpha(i) \in \mathbb{Z}_p$ otherwise.

Consider now the formal power series $H(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ defined as follows. For all $\beta \in \mathbb{N}^s$ let $d_{\alpha,\beta}$ be defined by

$$E_1(\mathbf{X})^{\beta_1} \ldots E_s(\mathbf{X})^{\beta_s} = \sum_{\alpha\in\mathbb{N}^r} d_{\alpha,\beta}\mathbf{X}^\alpha;$$

and let

$$H(\mathbf{X}) = \sum_{\alpha\in\mathbb{N}^r} \Big(\sum_{\beta\in\mathbb{N}^s} c_\beta d_{\alpha,\beta} \Big)\mathbf{X}^\alpha.$$

We note that as $e_{\mathbf{0}}(i) = 0$ for all i we have that $\langle\beta\rangle > \langle\alpha\rangle$ implies that $d_{\alpha,\beta} = 0$ and hence H is well defined. Our first step in showing that H is our required formal

power series is to establish that H can be evaluated at all $\mathbf{x} \in \mathbb{Z}_p^r$. In fact, as in the definition of a strictly analytic function, we show

$$\lim_{(\alpha,\beta)\in\mathbb{N}^r\times\mathbb{N}^s} |c_\beta d_{\alpha,\beta}|_p |x_1|_p^{\alpha_1} \dots |x_r|_p^{\alpha_r} = 0. \quad (*)$$

Take any $\epsilon > 0$. As $G(\mathbf{y})$ can be evaluated at all $\mathbf{y} \in \mathbb{Z}_p^s$ it can in particular be evaluated at $\mathbf{y} = (1, 1, \dots, 1)$. It follows that $\lim_{\beta\in\mathbb{N}^s} c_\beta = 0$. Also $d_{\alpha,\beta}$ is the finite sum of finite products of $e_\alpha(i) \in \mathbb{Z}_p$ and it follows that $|d_{\alpha,\beta}|_p \leq 1$. Hence, noting $x_i \in \mathbb{Z}_p$ for all i

$$\lim_{\beta\in\mathbb{N}^s} |c_\beta d_{\alpha,\beta}|_p |x_1|_p^{\alpha_1} \dots |x_r|_p^{\alpha_r} \leq \lim_{\beta\in\mathbb{N}^s} |c_\beta|_p = 0.$$

So there exists a finite $B \subseteq \mathbb{N}^s$ such that for all (α, β) where $\beta \notin B$

$$|c_\beta d_{\alpha,\beta}|_p |x_1|_p^{\alpha_1} \dots |x_r|_p^{\alpha_r} < \epsilon.$$

Similarly, as E_i can be evaluated at $(1, 1, \dots, 1) \in \mathbb{Z}_p^r$ for each i, $\lim_{\alpha\in\mathbb{N}^r} |e_\alpha(i)| = 0$. Thus for any fixed β it is clear that $\lim_{\alpha\in\mathbb{N}^r} d_{\alpha,\beta} = 0$ (as each $d_{\alpha,\beta}$ is just a finite sum of finite products of the $e_\alpha(i)$'s). So for any $\beta \in B$ there is a finite $A_\beta \subseteq \mathbb{N}^r$ such that $|c_\beta d_{\alpha,\beta}|_p |x_1|_p^{\alpha_1} \dots |x_r|_p^{\alpha_r} < \epsilon$. As the product of finite sets is finite we have $(*)$.

From $(*)$ it is clear that

$$\lim_{(\alpha,\beta)\in\mathbb{N}^r\times\mathbb{N}^s} c_\beta d_{\alpha,\beta} x_1^{\alpha_1} \dots x_r^{\alpha_r} = 0$$

for all $\mathbf{x} \in \mathbb{Z}_p^r$, and so by Corollary 3.7 H converges for all $\mathbf{x}$. It is clear that for all $\mathbf{x} \in \mathbb{Z}_p^r$, $G(E_1(\mathbf{x}), \dots, E_s(\mathbf{x})) = H(\mathbf{x})$ and by $(*)$ we have the first condition of Definition 4.2. Thus for all $\mathbf{x} \in \mathbb{Z}_p^r$, $g \circ \mathbf{f}(\mathbf{z} + p^{h_1}\mathbf{x}) = H(\mathbf{x})$ and so $g \circ \mathbf{f}$ is analytic at $\mathbf{z}$. As $\mathbf{z}$ was arbitrary we have that $g \circ \mathbf{f}$ is analytic on U as required. □

4.2 p-adic Analytic Manifolds

Having established the basic theory of analytic functions on $\mathbb{Z}_p^r$ we move forward to defining what is meant by a p-adic analytic manifold. Again the definition follows that of a real or complex analytic manifold almost exactly.

Definition 4.11. Let X be a topological space.

(i) A *chart* on X is a triple (U, ϕ, n) where $U \subseteq_o X$ and ϕ is a homeomorphism from U onto an open subset of $\mathbb{Z}_p^n$. A chart is said to be *global* if $U = X$.

(ii) Two charts (U, ϕ, n) and (V, ψ, m) are *compatible* if the maps $\psi \circ \phi^{-1}$ and $\phi \circ \psi^{-1}$ are analytic on $\phi(U \cap V)$ and $\psi(U \cap V)$ respectively.

(iii) An *atlas* is a set of pairwise compatible charts on X that covers X. If an atlas contains a global chart it is called a *global atlas*.

(iv) Two atlases A and B are *compatible* if each chart in A is compatible with each chart in B. That is, if $A \cup B$ is an atlas on X.

Notation 4.12. We temporarily let X_A denote the space X endowed with the atlas structure A. This will not be needed, however, after the proof of the next result.

Definition 4.13. A function $f : X_A \to Y_B$ is said to be *analytic* if for all $(U, \phi, n) \in A$ and $(V, \psi, m) \in B$ we have:

- $f^{-1}(V) \subseteq_o X$; and,
- the function
$$\psi \circ f \circ \phi^{-1}\Big|_{\phi(U \cap f^{-1}(V))}$$
is analytic.

From this definition it is clear that two atlases A and B of a topological space X are compatible if and only if the identity map $id : X_A \to X_B$ is analytic.

Proposition 4.14. *Let X, Y, and Z be topological spaces with atlases A, B, and C respectively. If $f : X_A \to Y_B$ and $g : Y_B \to Z_C$ are both analytic then $g \circ f : X_A \to Z_C$ is analytic.*

Proof. Take any $(W, \theta, n) \in C$. As g is analytic, $g^{-1}(W) \subseteq_o Y$ and thus for all $(V, \psi, m) \in B$, $V \cap g^{-1}(W) \subseteq_o Y$. As f is analytic, for any $(U, \phi, l) \in A$ and $(V, \psi, m) \in B$ we have
$$\psi \circ f \circ \phi^{-1}\Big|_{\phi(U \cap f^{-1}(V))}$$
is analytic, and hence continuous by Proposition 4.5, on $\phi(U \cap f^{-1}(V))$. But then as both ψ and ϕ are homeomorphisms, f is continuous on $U \cap f^{-1}(V)$. Now

$$\begin{aligned} f^{-1} \circ g^{-1}(W) &= \bigcup_{V \in B} f^{-1}(V \cap g^{-1}W) \\ &= \bigcup_{V \in B} \bigcup_{U \in A} f^{-1}(U \cap (V \cap g^{-1}(W))). \end{aligned}$$

As each term of the double union is open, $(g \circ f)^{-1}(W) \subseteq_o X$. Taking arbitrary $(U, \phi, l) \in A$ and $(W, \psi, n) \in C$, for all $(V, \psi, m) \in B$

$$\theta \circ g \circ \psi^{-1}\Big|_{\psi(V \cap g^{-1}(W))}, \text{ and } \psi \circ f \circ \phi^{-1}\Big|_{\phi(U \cap f^{-1}(V))}$$

are both analytic. So we clearly have $\theta \circ g \circ f \circ \phi^{-1}$ analytic on $\phi(U \cap f^{-1}(V \cap g^{-1}(W)))$ for all $(V, \psi, m) \in B$. As

$$\bigcup_{V \in B} \phi(U \cap f^{-1}(V \cap g^{-1}(W))) = \phi(U \cap f^{-1} \circ g^{-1}(W))$$

it follows that $g \circ f$ is analytic. □

Consider now a topological space X and let $\mathcal{A}$ be the set of all atlases on X. We can define the relation $\sim$ on $\mathcal{A}$ by $A \sim B$ if A and B are compatible. If $A \sim B$ and $B \sim C$ then by the definition of compatibility, $id_1 : X_A \to X_B$ and $id_2 : X_B \to X_C$

are both analytic functions. Hence by the above proposition $id : X_A \to X_C$ (where $id = id_2 \circ id_1$) is analytic implying $A \sim C$ and hence that $\sim$ is transitive. It is also clear from the definition of compatible charts that $\sim$ is reflexive and symmetric, so $\sim$ is an equivalence relation on $\mathcal{A}$. This motivates our definition of the p-adic analytic manifold.

Definition 4.15. A *p-adic analytic manifold structure* on a topological space X is an equivalence class of compatible atlases. If such a structure exists X endowed with this structure is called a *p-adic analytic manifold*.

Henceforth, when referring to a topological space X being a manifold or analytic manifold we will always mean that X is a p-adic analytic manifold.

Remark 4.16. It is natural for one to wonder why we have built up our theory based on the ring $\mathbb{Z}_p$ and not on the field $\mathbb{Q}_p$ as our usual notion of (analytic) manifolds is defined over a field (either $\mathbb{R}$ or $\mathbb{C}$). We could just as easily have weakened our definition by only requiring ϕ to be a homeomorphism between U and an open set in $\mathbb{Q}_p^n$ for each chart (U, ϕ, n), and defining a similar notion of a $\mathbb{Q}_p$-analytic function. However, as is shown below, $\mathbb{Q}_p^n$ is a p-adic analytic manifold, showing that we obtain the same class of manifolds regardless. □

Example 4.17. [$\mathbb{Q}_p^n$ is a p-adic analytic manifold.]

Consider the family of maps $\phi_i : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ defined by $\mathbf{x} \mapsto p^i\mathbf{x}$ (for all $i \in \mathbb{Z}$). It is clear that the map $\varphi_i : \mathbb{Q}_p \to \mathbb{Q}_p$ defined by $y \mapsto p^i y$ is a continuous as $|\varphi_i(y)|_p = |p^i y|_p = p^{-i}|y|_p$. As φ_i is bijective and $\varphi_i^{-1} = \varphi_{-i}$ it follows that φ_i is a homeomorphism for all i.

Now, ϕ is just the map φ applied to each coordinate of $\mathbb{Q}_p$ and so is also a homeomorphism. Hence for each $i \in \mathbb{N}$, if we define

$$C_i := (p^{-i}\mathbb{Z}_p^n, \phi_i\big|_{p^{-i}\mathbb{Z}_p^n}, n)$$

then C_i is a chart. The transition maps between the C_i are merely multiplication by p^k for some $k \in \mathbb{N}$, and so are analytic. As

$$\mathbb{Q}_p^n = \bigcup_{i=1}^{\infty} p^{-i}\mathbb{Z}_p^n$$

we have that $\{C_i \mid i \in \mathbb{N}\}$ is an atlas for $\mathbb{Q}_p^n$, and hence that $\mathbb{Q}_p^n$ is indeed a p-adic analytic manifold. □

The following proposition allows us to consider submanifolds of a p-adic analytic manifold.

Proposition 4.18. *If X is a manifold and $Y \subseteq_o X$, then Y is a manifold with atlas*

$$B = \{(Y \cap U, \phi\big|_{Y\cap U}, n) \mid (U, \phi, n) \in A\};$$

where A is an atlas of X. This is called the induced manifold structure.

Proof. It is clear that for each $(U, \phi, n) \in A$, $(Y \cap U, \phi\big|_{Y\cap U}, n)$ is a chart on Y, and that $\bigcup_{U\in A} U \cap Y = Y$. Similarly as for any $(U, \phi, n), (V, \psi, n) \in A$ the transition map

$$\psi \circ \phi^{-1}\big|_{\phi(U\cap V)}$$

is analytic, it is clearly analytic on the open subset $\phi(Y \cap U \cap V)$. Hence B is an atlas of Y and Y is a manifold. □

Example 4.19. [$GL_n(\mathbb{Z}_p)$ is a p-adic analytic manifold.]

Using the above proposition it is easy to show that $GL_n(\mathbb{Z}_p)$, one of the examples given of a profinite group in Section 1.3, is in fact a p-adic analytic manifold. As $M_n(\mathbb{Z}_p) \cong \mathbb{Z}_p^{n^2}$ is clearly a manifold (with global atlas) it only remains to show that $GL_n(\mathbb{Z}_p)$ is open in $M_n(\mathbb{Z}_p)$, however, this was shown in Example 1.25. Thus $GL_n(\mathbb{Z}_p)$ is a manifold with global atlas

$$\{(GL_n(\mathbb{Z}_p), \phi\big|_{GL_n(\mathbb{Z}_p)}, n^2)\}$$

where $\phi : M_n(\mathbb{Z}_p) \to \mathbb{Z}_p^{n^2}$ is the natural homeomorphism. □

Our definition of a p-adic analytic manifold and Proposition 4.14 allow us to dispense with the X_A notation as in the following definition.

Definition 4.20. Let X and Y be analytic manifolds. A function $f : X \to Y$ is *analytic* if $f : X_A \to Y_B$ is analytic for any atlases A and B of X and Y respectively.

The following proposition is then obvious from Proposition 4.14 and Proposition 4.5.

Proposition 4.21. *If X, Y and Z are p-adic analytic manifolds:*

(i) Any analytic function $f : X \to Y$ is continuous.

(ii) If $f : X \to Y$ and $g : Y \to Z$ are analytic then so is $g \circ f$.

Returning to Proposition 4.18 now, we note that if X is a topological space with atlas A, and X_i are a family of open subsets covering X each X_i has an induced atlas structure A_i upon it. However, it is easily seen that $\bigcup A_i$ is an atlas on X compatible with A and hence we have the following proposition.

Proposition 4.22. *If $f : X \to Y$ is a function where X and Y are p-adic analytic manifolds and $f|_{X_i} : X_i \to Y$ is analytic on $X_i \subseteq_o X$ with the induced manifold structure for each $i \in I$ such that $\bigcup_{i\in I} X_i = X$ then f is analytic on X.*

Finally we show that the product of two manifolds is a manifold. This is essential if we are to define multivariate functions on a manifold, especially when defining the p-adic analytic group (whose multiplication and inversion operations must be analytic).

Proposition 4.23. *If X and Y are manifolds with atlases A and B respectively, then $X \times Y$ is a manifold with atlas*

$$C = \{(U \times V, \phi \times \psi, n + m) \mid (U, \phi, n) \in A, (V, \psi, m) \in B\}.$$

where $(\phi \times \psi)(u, v) = (\phi(u), \psi(v)) \in \mathbb{Z}_p^{m+n}$.

Proof. It is clear that each $(U \times V, \phi \times \psi, n+m) \in C$ is a chart on $X \times Y$ and that $X \times Y = \bigcup_{U \in A, V \in B} U \times V$, so it just remains to show that any two charts in C are compatible. Taking any $(U \times V, \phi \times \psi, n+m), (S \times T, \theta \times \nu, n'+m')$ it suffices to show that

$$(\theta \times \nu) \circ (\phi \times \psi)^{-1}\Big|_{(\phi \times \psi)((U \times V) \cap (S \times T))}$$

is analytic. However, this is clearly satisfied as $\theta \circ \phi^{-1}$ and $\nu \circ \psi^{-1}$ are analytic on $\phi(U \cap S)$ and $\psi(V \cap T)$ respectively. Hence C is an atlas on $X \times Y$. □

4.3 Analytic Functions on Uniform Pro-p Groups

In Theorem 2.50 we established that any uniform pro-p group of dimension d is homeomorphic to $\mathbb{Z}_p^d$ via the map $\phi : G \to \mathbb{Z}_p^d$

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

where $\{a_1, \dots, a_d\}$ is a minimal generating set for G. Thus $\{(G, \phi, d)\}$ is a global atlas for G and so G is a p-adic analytic manifold. We were also able to show that every finitely generated powerful pro-p group contained an open uniform pro-p subgroup.

Our primary focus of this and the following section is to show that G is a p-adic analytic group with respect to this manifold structure and extend this structure over an arbitrary topological group containing G as an open subgroup, thus proving one direction of Lazard's Theorem. We begin by considering analytic functions on the manifold G. It is clear that the function $f : G \to G$ will be analytic if and only if

$$\phi \circ f \circ \phi^{-1}\Big|_{\phi(G \cap f^{-1}(G))}$$

is analytic. The purpose of this section is to prove the following following result which allows us to establish that G is a p-adic analytic group almost immediately and is also essential to extending the p-adic analytic group structure of G to any topological group containing G as an open subgroup.

Theorem 4.24. *Suppose that $u_1, \dots, u_r$ are arbitrary elements of a uniform pro-p group G which has topological generating set $\{a_1, \dots, a_d\}$ ($d = d(G)$). Then $\mathbf{g} : \mathbb{Z}_p^r \to \mathbb{Z}_p^d$ defined by $\mathbf{g}((\mu_1, \dots, \mu_r)) = (\lambda_1, \dots, \lambda_d)$ where*

$$u_1^{\mu_1} \dots u_r^{\mu_r} = a_1^{\lambda_1} \dots a_d^{\lambda_d}$$

is analytic.

Before establishing the above result we must return to the group algebra considered in the previous chapter. For much of this section we will work inside the completion of the group algebra with respect to the J-adic norm defined in Section 3.2 and Section 3.3 and shown to be equivalent to the Iwasawa algebra. As such we will again be working with the cofinal chains of ideals I_k and J^i and will follow much of the same notation. Here, however, G will always denote a uniform pro-p group.

Recall that if $\mathbf{u} = (u_1, \ldots, u_n)$ is any n-tuple of elements in a group G and $\alpha \in \mathbb{N}^n$, then

$$\langle \alpha \rangle = \alpha_1 + \alpha_2 + \ldots + \alpha_n, \text{ and } \mathbf{u}^\alpha = u_1^{\alpha_1} u_2^{\alpha_2} \ldots u_n^{\alpha_n}.$$

The following lemma is merely an application of the binomial theorem.

Lemma 4.25. *If G is a uniform pro-p group and $u_1, \ldots, u_r \in G$. If $v_i := u_i - 1$ then for each $\beta \in \mathbb{N}^r$:*

$$\begin{aligned} \mathbf{u}^\beta &= \sum_{\alpha \in \mathbb{N}^r} \binom{\beta_1}{\alpha_1} \ldots \binom{\beta_r}{\alpha_r} \mathbf{v}^\alpha, \\ \mathbf{v}^\beta &= \sum_{\alpha \in \mathbb{N}^r} (-1)^{\langle \beta \rangle - \langle \alpha \rangle} \binom{\beta_1}{\alpha_1} \ldots \binom{\beta_r}{\alpha_r} \mathbf{u}^\alpha. \end{aligned}$$

Also for the rest of the section we define

$$\begin{aligned} T_k &:= \{\alpha \in \mathbb{N}^d \mid \alpha_i < p^{k-1} \text{ for } i = 1, \ldots, d\}; \\ S_k &:= \{\alpha \in \mathbb{N}^d \mid \langle \alpha \rangle \leq k\}. \end{aligned}$$

And for any uniform pro-p group $G = \overline{\langle a_1 \rangle} \ldots \overline{\langle a_d \rangle}$ of dimension d we let

$$b_i = a_i - 1.$$

The proof of Theorem 4.24 relies on two results on the group algebra $\mathbb{Z}_p[G]$ of a uniform pro-p group G with minimal generating set $\{a_1, \ldots, a_n\}$ that stem from the following lemma. The first, Theorem 4.27, shows that the set $\{\mathbf{b}^\alpha \mid \alpha \in \mathbb{N}^d\} \subseteq \mathbb{Z}_p[G]$ forms a topological basis for $\mathbb{Z}_p[G]$. That is, any element $c \in \mathbb{Z}_p[G]$ can be written uniquely as the convergent sum

$$c = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha$$

with each $\lambda_\alpha \in \mathbb{Z}_p$. As discussed in [AB06] this is analogous to the Poincare-Birkhoff-Witt (PBW) Theorem for Lie Algebras, and as such the basis is referred to as a PBW basis.

The second result, Theorem 4.31, gives us the norm of any $c \in \mathbb{Z}_p[G]$ in terms of the coefficients in its PBW basis expansion

$$||c|| = \sup_{\alpha \in \mathbb{N}^r} p^{-\langle \alpha \rangle} |\lambda_\alpha|_p.$$

We use the definition of the function $\mathbf{g}$ and Corollary 4.30 to construct two representations of $\mathbf{u}^\lambda$ in terms of the PBW basis. Then we are assured that the coefficients of these convergent sequences are equal and extracting certain coefficients we can find a power series representation of g_i on all of $\mathbb{Z}_p^r$. Furthermore, Theorem 4.31 assures us that this power series representation converges to $g_i(\lambda)$ for all $\lambda \in \mathbb{Z}_p^r$, and satisfies condition (a) of Definition 4.2, completing the proof.

We provide this proof outline as what follows for the rest of the section are the most involved proofs of the thesis, and thus the reader may be inclined to skip them.

Lemma 4.26. *Let G be a uniform pro-p group with minimal topological generating set $\{a_1, \ldots, a_d\}$, and $k > 0$ and integer. Then we have the following:*

$$\begin{aligned} \mathbb{Z}_p[G] &= I_k \oplus \bigoplus_{\alpha \in T_k} \mathbb{Z}_p \mathbf{a}^\alpha \ (I^*) \\ \mathbb{Z}_p[G] &= I_k \oplus \bigoplus_{\alpha \in T_k} \mathbb{Z}_p \mathbf{b}^\alpha \ (I) \\ J^k &= J^{k+1} + \sum_{\alpha \in S_k} p^{k-\langle \alpha \rangle} \mathbb{Z}_p \mathbf{b}^\alpha \ (II). \end{aligned}$$

Proof. (I*)/(I): We view $\mathbb{Z}_p[G]$ as a free $\mathbb{Z}_p$ module with basis G. Let π be the natural module homomorphism from $\mathbb{Z}_p[G]$ to $\mathbb{Z}_p[G/G_k]$, so that $\ker(\pi) = I_k$. As $G/G_k = \{a_1^{\alpha_1} \ldots a_d^{\alpha_d} G_k \mid \alpha \in T_k\}$ we have that $\mathbb{Z}_p[G/G_k]$ (as a $\mathbb{Z}_p$ module) is clearly spanned by $\{\pi(\mathbf{a}^\alpha) \mid \alpha \in T_k\}$. However, as G is uniform,

$$|G/G_k| = \dim_{\mathbb{Z}_p}(\mathbb{Z}_p[G/G_k]) = p^{d(k-1)} = |T_k|$$

and hence $\{\pi(\mathbf{a}^\alpha) \mid \alpha \in T_k\}$ is in fact a basis for $\mathbb{Z}_p[G/G_k]$. Considering the short exact sequence

$$0 \to I_k \overset{id_{I_k}}{\to} \mathbb{Z}_p[G] \overset{\pi}{\to} \mathbb{Z}_p[G/G_k] \to 0,$$

it is clear that $\mathbb{Z}_p[G/G_k] = \bigoplus_{\alpha \in T_k} \mathbb{Z}_p a^\alpha$ and hence the identity map on $\mathbb{Z}_p[G/G_k]$ splits the sequence (by virtue of $\mathbb{Z}_p[G]$ being a free module). Hence $\mathbb{Z}_p[G] = I_k \oplus \bigoplus_{\alpha \in T_k} \mathbb{Z}_p a^\alpha$ and we have (I*). (I) follows from (I*) by the lemma above.

(II): As $p \in J$ and $b_i \in J$ for all i, it is clear that $p^{k-\langle \alpha \rangle} \mathbf{b}^\alpha \in J^k$ for all $\langle \alpha \rangle \leq k$, and hence

$$W_k := \sum_{\alpha \in S_k} p^{k-\langle \alpha \rangle} \mathbb{Z}_p \mathbf{b}^\alpha \subseteq J^k.$$

It follows that $J^k \supseteq J^{k+1} + W_k$. To establish the reverse inclusion we proceed by induction. By (I), as both I_2 and $\mathbb{Z}_p \mathbf{b}^\alpha$ are contained in J^2 for all $\langle \alpha \rangle > 1$,

$$J \subseteq I_2 + \sum_{\alpha \in T_2} \mathbb{Z}_p \mathbf{b}^\alpha \subseteq J^2 + \sum_{\alpha \in S_1} \mathbb{Z}_p \mathbf{b}^\alpha.$$

However, $\mathbb{Z}_p \mathbf{b}^{\mathbf{0}} = \mathbb{Z}_p 1_G$, and $J \cap \mathbb{Z}_p 1_G = p\mathbb{Z}_p 1_G$ so

$$J \subseteq J^2 + \sum_{\alpha \in S_1} p^{1-\langle \alpha \rangle} \mathbb{Z}_p \mathbf{b}^\alpha,$$

and our base case is established. Now assume that (II) holds for all $j < k$. It is clear that

$$J^k = J^{k-1} J = (J^k + W_{k-1})(J^2 + W_1) \subseteq J^{k+1} + W_{k-1} W_1,$$

and hence it suffices to show that $W_{k-1}W_1 \subseteq J^{k+1}+W_k$. As $W_1 = p\mathbb{Z}_p+\sum_{\langle\alpha\rangle=1}\mathbb{Z}_p\mathbf{b}^\alpha$ and $pW_{k-1} \subseteq W_k$ we need only show that for all $\alpha \in S_{k-1}$ and all $i \in \{1,\dots,d\}$, $p^{k-1-\langle\alpha\rangle}\mathbf{b}^\alpha b_i \in J^{k+1}+W_k$.

Setting $u = b_1^{\alpha_1}\dots b_{i-1}^{\alpha_{i-1}}$, $v = b_i^{\alpha_i}\dots b_d^{\alpha_d}$ and defining β by $\beta_i = \alpha_i+1$ and $\beta_j = \alpha_j$ for all $j \neq i$ we have

$$\mathbf{b}^\alpha b_i = uvb_i = \mathbf{b}^\beta + u(vb_i - b_iv).$$

Now, if we set $n = \alpha_i + \dots + \alpha_d$ it is clear that $b_iv \in J^{n+1}$. Also, $vb_i - b_iv = b_iv([v,b_i]-1)$ and as G is uniform, $[v,b_i] = z^p$ for some $z \in G$. But then if $y = z-1$,

$$z^p - 1 = (y+1)^p - 1 = y^p + pyw$$

for some $w \in G$. It is clear that $y \in J$ and hence we have $z^p - 1 \in J^p + pJ$. Thus $vb_i - b_iv \in J^{n+p+1} + pJ^{n+2}$ and hence

$$u(vb_i - b_iv) \in pJ^{\langle\alpha\rangle} + J^{\langle\alpha\rangle+2}.$$

Now, as $p^{k-1-\langle\alpha\rangle}\mathbf{b}^\beta \in W_k$, it follows that

$$p^{k-1-\langle\alpha\rangle} \in W_k + p^{k-\langle\alpha\rangle}J^{\langle\alpha\rangle} + p^{k-1-\langle\alpha\rangle}J^{\langle\alpha\rangle+2}.$$

Clearly $p^{k-1-\langle\alpha\rangle}J^{\langle\alpha\rangle+2} \subseteq J^{k+1}$, and as $\langle\alpha\rangle \leq k-1$, $J^{\langle\alpha\rangle} = J^{\langle\alpha\rangle+1} + W_{\langle\alpha\rangle}$ and

$$p^{k-\langle\alpha\rangle}J^{\langle\alpha\rangle+1} + p^{k-\langle\alpha\rangle}W_{\langle\alpha\rangle} \subseteq J^{k+1} + W_k.$$

So for all $i \in \{1,\dots,d\}$ and all $\alpha \in S_{k-1}$ we have $p^{k-1-\langle\alpha\rangle}\mathbf{b}^\alpha b_i \in J^{k+1}+W_k$, and thus (II) is established for all k by induction. □

Theorem 4.27. *If $G = \overline{\langle a_1\rangle}\dots\overline{\langle a_d\rangle}$ is a uniform pro-p group of dimension d any element of $\mathbb{Z}_p[G]$ is equal to the sum of a unique convergent series*

$$\sum_{\alpha\in\mathbb{N}^d}\lambda_\alpha\mathbf{b}^\alpha$$

where $\lambda_\alpha \in \mathbb{Z}_p$ for all $\alpha \in \mathbb{N}^d$.

Proof. Take any $c \in \mathbb{Z}_p[G]$. By (I) in the lemma above we know that for each k the set Λ_k is non-empty, as $J^k \supseteq I_k$ by Proposition 3.13, where

$$\Lambda_k = \{(\lambda_\alpha)_{\alpha\in T_k} \mid c \equiv \sum_{\alpha\in T_k}\lambda_\alpha\mathbf{b}^\alpha \pmod{J^k}\} \subseteq \mathbb{Z}_p^{|T_k|}.$$

If we let $f_{kl} : \mathbb{Z}_p^{|T_l|} \to \mathbb{Z}_p^{|T_k|}$ be the natural projection for all $l \geq k$, and $g_{kl} = f_{kl}\big|_{\Lambda_l}$ we claim that (Λ_k, f_{kl}) is an inverse system of compact spaces. As $b_i = a_i - 1 \in J$,

$b_i^k \in J^k$ and hence $\mathbf{b}^\alpha \in J^{\langle\alpha\rangle}$. Thus, for any $(\lambda_\alpha) \in \Lambda_l$ and any $k \leq l$,

$$\begin{aligned} c &\equiv \sum_{\alpha\in T_l} \lambda_\alpha \mathbf{b}^\alpha \pmod{J^l} \\ &\equiv \sum_{\alpha\in T_k} \lambda_\alpha \mathbf{b}^\alpha + \sum_{\alpha\in T_l\backslash T_k} \lambda_\alpha \mathbf{b}^\alpha \pmod{J^l} \\ &\equiv \sum_{\alpha\in T_k} \lambda_\alpha \mathbf{b}^\alpha \pmod{J^k}. \end{aligned}$$

It is clear that $f_{km} = f_{kl} \circ f_{lm}$ (for all $k \leq l \leq m$) and so (Λ_k, f_{kl}) is an inverse system as claimed. That these spaces are compact follows from that fact that if two p-adic numbers $\lambda_i \equiv \lambda_j \pmod{p^k}$ then $\lambda_i g \equiv \lambda_j g \pmod{J^k}$ for any $g \in G$. By Theorem 1.27 we know that the inverse limit of the system is non-empty and hence there is a $(\lambda_\alpha)_{\alpha\in\mathbb{N}^r}$ such that $(\lambda_\alpha)_{\alpha\in T_k} \in \Lambda_k$ for all k.

Naturally we now turn to the sum $\sum_{\alpha\in\mathbb{N}^r} \lambda_\alpha \mathbf{b}^\alpha$. To show that it converges to c, we let $\epsilon > 0$, take k such that $p^{-k} < \epsilon$, and any finite $S \supseteq T_k$. By definition of Λ_k we have

$$c \equiv \sum_{\alpha\in T_k} \lambda_\alpha \mathbf{b}^\alpha \pmod{J^k}.$$

Also, any $\alpha \in S\backslash T_k$ satisfies $\langle\alpha\rangle \geq k$ and hence $\mathbf{b}^\alpha \in J^k$. It follows that

$$||c - \sum_{\alpha\in S} \lambda_\alpha \mathbf{b}^\alpha|| = ||c - \sum_{\alpha\in T_k} \lambda_\alpha \mathbf{b}^\alpha - \sum_{\alpha\in S\backslash T_k} \lambda_\alpha \mathbf{b}^\alpha|| \leq p^{-k} < \epsilon.$$

Thus $\sum_{\alpha\in\mathbb{N}^r} \lambda_\alpha \mathbf{b}^\alpha = c$ as required. Hence it only remains to show that the sum is unique.

Suppose that

$$\sum_{\alpha\in\mathbb{N}^d} \mu_\alpha \mathbf{b}^\alpha = 0$$

where $\mu_\alpha \in \mathbb{Z}_p$ and for at least one α, $\mu_\alpha \neq 0$. We further assume, without loss of generality, that there exists a $\gamma \in \mathbb{N}^d$ such that $\mu_\gamma \in \mathbb{Z}_p\backslash p\mathbb{Z}_p$ (as otherwise we could divide through by the highest power of p). Take k sufficiently large so that $\gamma \in T_k$ and set $m = |G/G_k|$. As the sum above converges there exists a finite $S \supseteq T_k$ such that $||\sum_{\alpha\in S} \mu_\alpha \mathbf{b}^\alpha|| < p^{-m}$. Thus $\sum_{\alpha\in S} \mu_\alpha \mathbf{b}^\alpha \in J^m \subseteq I_k + p\mathbb{Z}_p[G]$ by the definition of the group algebra norm and Proposition 3.13. Also, as for any $\alpha \in \mathbb{N}^d\backslash T_k$ there exists an i such that $\alpha_i \geq p^{k-1}$, we have that $b_i^{p^{k-1}}$ is a factor of $\mathbf{b}^\alpha$. Thus as

$$b_i^{p^{k-1}} \equiv (a_i - 1)^{p^{k-1}} \equiv a_i^{p^{k-1}} - 1 \pmod{pR}$$

and $a_i^{p^{k-1}} \in G_k$, we have

$$\mathbf{b}^\alpha \in (G_k - 1)\mathbb{Z}_p[G] + p\mathbb{Z}_p[G] = I_k + p\mathbb{Z}_p[G].$$

So $\sum_{\alpha\in T_k}\mu_\alpha \mathbf{b}^\alpha \in I_k + p\mathbb{Z}_p[G]$ and by the lemma above it is clear that

$$\sum_{\alpha\in T_k}\mathbb{Z}_p\mathbf{b}^\alpha \cap (I_k + p\mathbb{Z}_p[G]) = \bigoplus_{\alpha\in T_k} p\mathbb{Z}_p\mathbf{b}^\alpha.$$

It follows that $\sum_{\alpha\in T_k}\mu_\alpha\mathbf{b}^\alpha \in \bigoplus_{\alpha\in T_k} p\mathbb{Z}_p\mathbf{b}^\alpha$. As we can equate coefficients we have $\mu_\gamma \notin p\mathbb{Z}_p$, contradicting our assumption. Hence $\mu_\alpha = 0$ for all $\alpha \in \mathbb{N}^d$ and the representation of c is unique. □

Notation 4.28. For any $\lambda \in \mathbb{Z}_p$ and any positive integer a we let

$$\binom{\lambda}{a} = \frac{\lambda(\lambda-1)\dots(\lambda-a+1)}{a!} \in \mathbb{Z}_p;$$

and set $\binom{\lambda}{0} = 1$.

The following lemma is quite easily shown

Lemma 4.29. *For any integer n, the highest power of p dividing into $n!$ is at most $(n-1)/(p-1)$.*

The following corollary to Theorem 4.27 allows us to write the product $\mathbf{u}^\lambda = u_1^{\lambda_1}\dots u_r^{\lambda_r}$ (with $\lambda \in \mathbb{Z}_p^r$) in terms of a convergent sum in terms of $\mathbf{v}^\alpha$ with $v_i = u_i - 1$ and $\alpha \in \mathbb{N}^r$. In essence this says that in the group algebra we can rewrite a product of p-adic powers of elements in G as this convergent sum of regular integer powers.

Corollary 4.30. *Let $G = \overline{\langle a_1\rangle}\dots\overline{\langle a_d\rangle}$ be a uniform pro-p group of dimension d, take any $u_1,\dots,u_r \in G$, and set $v_i = u_i - 1$ for each i. Then for any $\lambda = (\lambda_1,\dots,\lambda_d) \in \mathbb{Z}_p^d$*

$$\mathbf{u}^\lambda = \sum_{\alpha\in\mathbb{N}^r}\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r}\mathbf{v}^\alpha.$$

Proof. We show that we can approximate arbitrarily $u_1^{\lambda_1}\dots u_r^{\lambda_r}$ by $\mathbf{u}^\beta$ for some $\beta \in \mathbb{N}^r$, which can in turn be approximated by $\sum_{\alpha\in\mathbb{N}^r}\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r}\mathbf{v}^\alpha$. Let $\epsilon > 0$ and set $M, N \in \mathbb{N}$ such that $p^{-M} < \epsilon$ and $p^{-N} < \epsilon|M!|_p$. If we take $\beta \in \mathbb{N}^r$ such that $\beta_i \equiv \lambda_i \pmod{p^N}$ for all i, then as p^N divides $\lambda_i - \beta_i$ we have

$$u_i^{\lambda_i} - u_i^{\beta_i} = u_i^\beta(u_i^{\lambda_i-\beta_i} - 1) \in \mathbb{Z}_p[G](G_{N+1} - 1) = I_{N+1}.$$

As $I_{N+1} \subseteq J^{N+1}$ it follows that

$$\begin{aligned} ||\mathbf{u}^\lambda - \mathbf{u}^\beta|| &= ||(u_1^{\lambda_1} - u_1^{\beta_1})u_2^{\lambda_2}\dots u_r^{\lambda_r} \\ &\quad + u_1^{\beta_1}(u_2^{\lambda_2} - u_2^{\beta_2})u_3^{\lambda_3}\dots u_r^{\lambda_r} + u_1^{\beta_1}\dots u_{r-1}^{\beta_{r-1}}(u_r^{\lambda_r} - u_r^{\beta_r})|| \\ &\leq p^{-(N+1)} < \epsilon \end{aligned}$$

as each term is in I_{N+1}.

Now, if we take any $\alpha \in \mathbb{N}^n$ such that $\langle \alpha \rangle \leq M$ then clearly

$$\sum_{i=1}^{r} \lambda_i(\lambda_i - 1)\dots(\lambda_i - \alpha_i + 1) \equiv \sum_{i=1}^{r} \beta_i(\beta_i - 1)\dots(\beta_i - \alpha_i + 1) \pmod{p^N}$$

and hence

$$\Big|\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r} - \binom{\beta_1}{\alpha_1}\dots\binom{\beta_r}{\alpha_r}\Big|_p \leq \frac{p^{-N}}{|\prod_{i=1}^{r}\alpha_i!|_p} \leq \frac{p^{-N}}{|M!|_p}$$

as $\prod_{i=1}^{r}\alpha_i!$ divides $\langle\alpha\rangle!$. If, instead, $\langle\alpha\rangle > M$ then (as $v_i = u_i - 1 \in I_1 \subseteq J$) we have

$$||\mathbf{v}^\alpha|| \leq \prod_{i=1}^{r} ||v_i||^{\alpha_i} \leq p^{-M}.$$

So by Proposition 3.5 (iii) we have

$$\Big\|\sum_{\alpha\in\mathbb{N}^r}\Big(\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r} - \binom{\beta_1}{\alpha_1}\dots\binom{\beta_r}{\alpha_r}\Big)\mathbf{v}^\alpha\Big\| \leq \max\Big\{\frac{p^{-N}}{M!}, p^{-M}\Big\} < \epsilon.$$

Thus by Lemma 4.25

$$\begin{aligned}\Big\|\mathbf{u} - \sum_{\alpha\in\mathbb{N}^r}\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r}\mathbf{v}^\beta\Big\| &= \Big\|\mathbf{u}^\lambda - \mathbf{u}^\beta + \sum_{\alpha\in\mathbb{N}^r}\binom{\beta_1}{\alpha_1}\dots\binom{\beta_r}{\alpha_r}\mathbf{v}^\alpha \\ &\qquad - \sum_{\alpha\in\mathbb{N}^r}\binom{\lambda_1}{\alpha_1}\dots\binom{\lambda_r}{\alpha_r}\mathbf{v}^\beta\Big\| \\ &< \epsilon.\end{aligned}$$

As ϵ was arbitrary the result is established. □

Theorem 4.31. *If $G = \overline{\langle a_1\rangle}\dots\overline{\langle a_d\rangle}$ is a uniform pro-p group of dimension d then for any $c \in \mathbb{Z}_p[G]$ we have*

$$||c|| = \sup_{\alpha\in\mathbb{N}^d} p^{-\langle\alpha\rangle}|\lambda_\alpha|_p$$

where $c = \sum_{\alpha\in\mathbb{N}^d}\lambda_\alpha\mathbf{b}^\alpha$.

Proof. Recall first Proposition 3.5 (iii), that is $||c|| \leq \sup_{\alpha\in\mathbb{N}^d}||\lambda_\alpha\mathbf{b}^\alpha||$. Now, $b_i \in I_1 \subseteq J$ and thus $\mathbf{b}^\alpha \in J^{\langle\alpha\rangle}$. Also, if $|\lambda_\alpha|_p = p^{-m}$ then $\lambda_\alpha \in p^m\mathbb{Z}_p[G] \subseteq J^m$ and hence $\lambda_\alpha\mathbf{b}^\alpha \in J^{m+\langle\alpha\rangle}$ and so

$$||c|| \leq \sup_{\alpha\in\mathbb{N}^d}||\lambda_\alpha\mathbf{b}^\alpha|| \leq \sup_{\alpha\in\mathbb{N}^d} p^{-m-\langle\alpha\rangle} = \sup_{\alpha\in\mathbb{N}} p^{-\langle\alpha\rangle}|\lambda_\alpha|_p.$$

To obtain the reverse inequality assume that $||c|| = p^{-k}$. That is, $c \in J^k\backslash J^{k+1}$. Hence by Lemma 4.26 (II) we have $c_{k+1} \in J^{k+1}$, $\mu_\alpha(k) \in \mathbb{Z}_p$ that satisfy,

$$c_k := c = \sum_{\langle\alpha\rangle\leq k} p^{k-\langle\alpha\rangle}\mu_\alpha(k)\mathbf{b}^\alpha + c_{k+1}.$$

In this manner we can recursively construct a sequence $\{c_j\}_{j=k}^{\infty}$ such that

$$w_j := c_j - c_{j+1} = \sum_{\langle\alpha\rangle \leq j} p^{j-\langle\alpha\rangle}\mu_\alpha(j)\mathbf{b}^\alpha.$$

As $c_j \in J^j$, for all j, we have $w_j \in J^j$. Also, $w_k + \ldots + w_n = c - c_{n+1}$ and so $c \equiv w_1 + \ldots + w_n \pmod{J^{n+1}}$. It follows that

$$c = \sum_{j=k}^{\infty} w_j = \sum_{j=k}^{\infty} \sum_{\langle\alpha\rangle \leq j} p^{j-\langle\alpha\rangle}\mu_\alpha(j)\mathbf{b}^\alpha. \quad (*)$$

Now we see that as $p^{j-\langle\alpha\rangle}\mathbf{b}^\alpha \in J^i$, $||p^{j-\langle\alpha\rangle}\mu_\alpha(i)\mathbf{b}^\alpha|| \leq p^{-i}$. Thus if we set $T = \{(j,\alpha) \mid j \geq k, \langle\alpha\rangle \leq j\}$,

$$\lim_{(j,\alpha)\in T} p^{j-\langle\alpha\rangle}\mu_\alpha(i)\mathbf{b}^\alpha = 0.$$

By Corollary 3.7 we can hence rearrange the double series in $(*)$. If we set

$$\mu_\alpha = \sum_{i=\max\{k,\langle\alpha\rangle\}}^{\infty} p^{i-\langle\alpha\rangle}\mu_\alpha(i);$$

we have,

$$c = \sum_{j=k}^{\infty} w_j = \sum_{\alpha\in\mathbb{N}^d} \mu_\alpha \mathbf{b}^\alpha.$$

However, we know the representation of c (from Lemma 4.26) is unique and hence $\mu_\alpha = \lambda_\alpha$ for all $\alpha \in \mathbb{N}^d$. Thus

$$p^{\langle\alpha\rangle}\lambda_\alpha = \sum_{i=\max\{k,\langle\alpha\rangle\}}^{\infty} p^i\mu_\alpha(i) \in p^k\mathbb{Z}_p.$$

This gives us that $p^{-\langle\alpha\rangle}|\lambda_\alpha|_p \leq p^{-k}$ for all $\alpha \in \mathbb{N}^d$. The result follows. □

We are finally in a position to establish Theorem 4.24.

Proof of Theorem 4.24. We show that in fact g_i is strictly analytic on $\mathbb{Z}_p^r$ for each i (and hence $\mathbf{g}$ is analytic). Setting $v_i = u_i - 1$ for each i we have by Corollary 4.30

$$\mathbf{u}^\lambda = \sum_{\alpha\in\mathbb{N}^r} \binom{\lambda_1}{\alpha_1} \ldots \binom{\lambda_r}{\alpha_r} \mathbf{v}^\alpha.$$

Then by Theorem 4.27 we have for each $\alpha \in \mathbb{N}^r$ there are $c_{\alpha\beta} \in \mathbb{Z}_p$ such that

$$\mathbf{v}^\alpha = \sum_{\beta\in\mathbb{N}^d} c_{\alpha\beta}\mathbf{b}^\beta.$$

It is clear that $v_i \in J$ for all i and hence $||v_i|| \leq p^{-1}$. Also, Theorem 4.31 gives us that $||\mathbf{v}^\alpha|| = \sup_{\beta \in \mathbb{N}^d} p^{-\langle\beta\rangle}|c_{\alpha\beta}|_p$, and so for each $\alpha \in \mathbb{N}^r$, $\beta \in \mathbb{N}^d$

$$|c_{\alpha\beta}|_p \leq p^{\langle\beta\rangle}||\mathbf{v}^\alpha|| \leq \min\{1, p^{\langle\beta\rangle - \langle\alpha\rangle}\}$$

as $c_{\alpha\beta} \in \mathbb{Z}_p$.

Now for all i, $\binom{\lambda_i}{\alpha_i} \in \mathbb{Z}_p$ and $\mathbf{b}^\beta \in J^{\langle\beta\rangle}$ and so it is clear that

$$\lim_{(\alpha,\beta)\in\mathbb{N}^r\times\mathbb{N}^d} \binom{\lambda_1}{\alpha_1} \dots \binom{\lambda_r}{\alpha_r} c_{\alpha\beta}\mathbf{b}^\beta = 0.$$

Thus by Corollary 3.7

$$\mathbf{u}^\lambda = \sum_{\beta\in\mathbb{N}^d} \Big(\sum_{\alpha\in\mathbb{N}^r} \binom{\lambda_1}{\alpha_1} \dots \binom{\lambda_r}{\alpha_r} c_{\alpha\beta} \Big) \mathbf{b}^\beta.$$

However, again by Corollary 4.30 we have

$$\mathbf{u}^\lambda = \mathbf{a}^\mu = \sum_{\beta\in\mathbb{N}^d} \binom{\mu_1}{\beta_1} \dots \binom{\mu_d}{\beta_d} \mathbf{b}^\beta.$$

As Theorem 4.27 guarantees that the sum for $\mathbf{u}^\lambda$ is unique, each coefficient in the two above sums must agree. In particular, if we fix an i and consider $\beta \in \mathbb{N}^d$ defined by $\beta_i = 1$ and $\beta_j = 0$ for $j \neq i$ we see

$$\sum_{\alpha\in\mathbb{N}^r} \binom{\lambda_1}{\alpha_1} \dots \binom{\lambda_r}{\alpha_r} c_{\alpha\beta} = \binom{\mu_1}{\beta_1} \dots \binom{\mu_r}{\beta_r} = \mu_i = g_i(\lambda_1, \dots, \lambda_r).$$

Thus all that remains to show is that this is in fact a strictly analytic function on $\mathbb{Z}_p^r$. We let $d_{\alpha\gamma}$ be defined by

$$\binom{X_1}{\alpha_1} \dots \binom{X_r}{\alpha_r} = \sum_{\gamma\in\mathbb{N}^r} d_{\alpha\gamma}\mathbf{X}^\gamma.$$

Clearly this is a finite sum as $d_{\alpha\gamma} = 0$ if there is a $j \in \{1, \dots, r\}$ such that $\gamma_j > \alpha_j$. Also, for each $\alpha, \gamma \in \mathbb{N}^r$ (by Lemma 4.29)

$$|d_{\alpha\gamma}|_p \leq \Big|\frac{1}{\alpha_1! \dots \alpha_r!}\Big|_p \leq p^{(\langle\alpha\rangle - r)/(p-1)}.$$

Since $|c_{\alpha\beta}|_p \leq p^{\langle\beta\rangle - \langle\alpha\rangle} = p^{1-\langle\alpha\rangle}$ it follows that

$$|c_{\alpha\beta}d_{\alpha\gamma}|_p \leq p^{(p-r-1-(p-2)\langle\alpha\rangle/(p-1)},$$

for all $\alpha, \gamma \in \mathbb{N}^r$ and so for all $\lambda \in \mathbb{Z}_p^r$

$$\lim_{(\alpha,\gamma)\in\mathbb{N}^r\times\mathbb{N}^r} c_{\alpha\beta}d_{\alpha\gamma}\lambda^\gamma = 0.$$

Thus again by Corollary 3.7

$$g_i(\lambda) = \sum_{\alpha \in \mathbb{N}^r} c_{\alpha\beta}(\sum_{\gamma \in \mathbb{N}^r} d_{\alpha\gamma}\lambda^\gamma) = \sum_{\gamma \in \mathbb{N}^r} e_\gamma \lambda^\gamma$$

with $e_\gamma = \sum_{\alpha \in \mathbb{N}^r} c_{\alpha\beta} d_{\alpha\gamma}$. Thus $H(\mathbf{X}) = \sum_{\gamma \in \mathbb{N}^r} e_\gamma \mathbf{X}^\gamma \in \mathbb{Q}_p[[\mathbf{X}]]$ and agrees with g_i on $\mathbb{Z}_p^r$. It is also clear as each e_γ is a finite sum of $c_{\alpha\beta}d_{\alpha\gamma}$ that H satisfies condition (a) of Definition 4.2. Hence g_i is strictly analytic on $\mathbb{Z}_p^r$ and it follows that $\mathbf{g}$ is analytic as required. □

4.4 p-adic Analytic Groups

Definition 4.32. A *p-adic analytic group* or *p-adic Lie group* is a p-adic analytic manifold G that is also a group such that the maps

$$\begin{aligned} m : G \times G \to G \quad &\text{given by} \quad (x, y) \mapsto xy \\ i : G \to G \quad &\text{given by} \quad x \mapsto x^{-1} \end{aligned}$$

are both analytic.

Note that $G \times G$ is a manifold with atlas given in Proposition 4.23. It is clear that m and i above are analytic if and only if $g : G \times G \to G$ sending $(x, y) \mapsto xy^{-1}$ is.

Example 4.33. [$GL_n(\mathbb{Z}_p)$ is a p-adic analytic group.]

We saw that $GL_n(\mathbb{Z}_p)$ is a p-adic analytic manifold with global atlas

$$\{(GL_n(\mathbb{Z}_p), \phi\big|_{GL_n(\mathbb{Z}_p)}, n^2)\}$$

where $\phi : M_n(\mathbb{Z}_p) \to \mathbb{Z}_p^{n^2}$ is the natural homeomorphism. Using Example 4.9 it is quite easy to show that $GL_n(\mathbb{Z}_p)$ is in fact a p-adic analytic group. Notice that to show that multiplication is analytic is equivalent to showing that the n^2 functions (from $\mathbb{Z}_p^{2n^2} \to \mathbb{Z}_p$) given by

$$(x_{1,1}, \ldots, x_{n,n}, y_{1,1}, \ldots, y_{n,n}) \mapsto x_{i,1}y_{i,j} + \ldots x_{i,n}y_{n,j}$$

are analytic, but this is obvious. Also we know by Cramer's rule, if $g \in GL_n(\mathbb{Z}_p)$ and $h = g^{-1}$ then

$$h_{i,j} = \frac{\det(g(i,j))}{\det(g)}.$$

where $g(i,j)$ is the matrix obtained by replacing the jth column of g with the ith standard basis vector. However, by the Leibniz formula we have for any $a \in M_n(\mathbb{Z}_p)$

$$\det(a) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

which is also clearly analytic. As the inverse function is analytic on $\mathbb{Z}_p \backslash p\mathbb{Z}_p$ (and $\det(g) \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$ for all $g \in GL_n(\mathbb{Z}_p)$) and the composition of analytic functions is

analytic we have that the functions $\iota : \mathbb{Z}_{p^{n^2}} \to \mathbb{Z}_p$ defined by

$$(g_{1,1}, \ldots, g_{n,n}) \mapsto h_{i,j}$$

with $h_{i,j}$ as above, are clearly analytic for each (i, j). Hence inversion in $GL_n(\mathbb{Z}_p)$ is analytic and $GL_n(\mathbb{Z}_p)$ is indeed a p-adic analytic manifold. □

We now present a theorem that is, in effect, one direction of Lazard's Theorem.

Theorem 4.34. *A topological group containing a open subgroup that is a uniform pro-p group is a p-adic analytic group.*

Our first step in establishing this, the main result in this chapter, is to show that every uniform pro-p group is a p-adic analytic group. Theorem 2.50 and the discussion at the start of Section 4.3 demonstrated that any uniform pro-p group is an analytic manifold and hence it only remains to show that $g : G \times G \to G$ defined by $g(x, y) = xy^{-1}$ is analytic.

Theorem 4.35. *Every uniform pro-p group G is a p-adic analytic group.*

Proof. Let $d(G) = d$ and take $\{a_1, \ldots, a_d\}$ a topological generating set for G. As discussed above, it suffices to show that g is analytic. That is, we need to establish that

$$\phi \circ g \circ (\phi \times \phi)^{-1}\Big|_{(\phi\times\phi)(G\times G \,\cap\, g^{-1}(G))}$$

is analytic. Now we consider $\rho : \mathbb{Z}_p^{2d} \to \mathbb{Z}_p^d$ defined by $(\lambda_1, \ldots, \lambda_d, \mu_1, \ldots, \mu_d) \mapsto (\nu_1, \ldots, \nu_d)$ where

$$a_1^{\lambda_1} \ldots a_d^{\lambda_d} a_d^{-\mu_d} \ldots a_1^{-\mu_1} = a_1^{\nu_1} \ldots a_d^{\nu_d}.$$

By Theorem 4.24, ρ is analytic on $\mathbb{Z}_p^{2d}$, and it is clear that $\rho = \phi \circ g \circ (\phi \times \phi)^{-1}$ on $(\phi \times \phi)(G \times G \;\cap\; g^{-1}(G))$. It follows that g is indeed analytic and G is a p-adic analytic group. □

Proof of Theorem 4.34. Let G be a topological group and $H \leq_o G$ be a uniform group of dimension d with topological generating set $\{a_1, \ldots, a_d\}$. We have that H is a manifold with global atlas $\{(H, \phi, d)\}$ with ϕ as in Theorem 2.50. Now we consider a transversal T of the cosets of H containing 1, and claim that $A = \{(aH, \phi_a, d) \mid a \in T\}$ is an atlas for G where $\phi_a : aH \to \mathbb{Z}_p^d$ is the map $x \mapsto \phi(a^{-1}x)$. It is clear as $x \mapsto g^{-1}x$ is a homeomorphism on G that each ϕ_a is a homeomorphism onto its range and hence (aH, ϕ_a, d) is a chart on G for all $a \in T$. Now take any $a, b \in T$. We have $aH \cap bH = \varnothing$ unless $a = b$ and in that case

$$\phi_a \circ \phi_a^{-1}\big|_{aH} = id_{aH}$$

which is obviously analytic. Hence the charts of A are pairwise compatible, and as A clearly covers G it is an atlas as claimed.

It remains to show that $g : G \times G \to G$ defined by $g(x, y) = xy^{-1}$ is analytic. By Proposition 4.22 it suffices to show that g is analytic on $aH \times bH$ for all $a, b \in T$. Also for any $h_1, h_2 \in H$ we have

$$g(ah_1, bh_2) = ah_1h_2^{-1}b^{-1} = ab^{-1}bh_1h_2^{-1}b^{-1},$$

from which it follows that $g = \alpha \circ \beta \circ m$ where, if we let $f_g : G \to G$ be left multiplication by g:

- $\alpha = f_{ab^{-1}}$;
- $\beta : H \to G$; $\beta(x) = bxb^{-1}$; and
- $m : H \times H \to H$ is the usual multiplication on H.

As m is analytic on H, by virtue of H being a uniform pro-p group, we need only show that α and β are analytic. To show that f_g is analytic on G it similarly suffices to show that it is analytic on cH for any $c \in T$. As $gc = sh$ for some $s \in T$, $h \in H$, we have that $gcH = sH$. It follows that for any $t \in T$, $cH \cap f_g^{-1}(tH) \neq \varnothing$ if and only if $t = s$. Hence we need only show that

$$\phi_s \circ f_g \circ \phi_c^{-1}\big|_{\phi_c(cH)}$$

is analytic. But this is precisely

$$\phi \circ f_h \circ \phi^{-1}\big|_{\phi(H)}.$$

However, m is analytic and thus it follows that f_h is analytic on G, as is f_g for any $g \in G$. Hence α is analytic on G.

To show β is analytic on H, again by Proposition 4.22, it suffices to show that for all $h \in H$, β is analytic on a neighbourhood about h. Note first that $H \cap b^{-1}Hb \leq_o H$ (clearly containing the identity), and hence by Proposition 2.46 there exists an $m \in \mathbb{N}$ such that $H_{m+1} \subseteq H \cap b^{-1}Hb$. We set $V = H_{m+1}$. Then V is a manifold with global atlas $\{(V, \phi\big|_V, d)\}$ by Proposition 4.18, where $\phi\big|_V$ maps V onto $p^m\mathbb{Z}_p^d$.

Claim: The map $\gamma : V \to H$ defined by $x \mapsto bxb^{-1}$ is analytic on V.

It is clear that, as both are manifolds with a global atlas, γ is analytic if and only if

$$\rho : \phi \circ \gamma \circ \phi\big|_V^{-1}\Big|_{\phi\big|_V(V \cap \gamma^{-1}(H))}$$

is analytic. Clearly $\gamma(V) \subseteq_o H$ and hence $\phi\big|_V(V \cap \gamma^{-1}(H)) = \phi\big|_V(V) = p^m\mathbb{Z}_p^d$. Now, $\rho(\lambda_1, \ldots, \lambda_d) = (\mu_1, \ldots, \mu_d)$ where

$$b(a_1^{\lambda_1} \ldots a_d^{\lambda_d})b^{-1} = a_1^{\mu_1} \ldots a_d^{\mu_d}.$$

Setting $\nu_i = p^{-m}\lambda_i \in \mathbb{Z}_p$, and $\omega_i = ba_i^{p^m}b^{-1}$ we have

$$\begin{aligned} b(a_1^{\lambda_1} \ldots a_d^{\lambda_d})b^{-1} &= \omega_1^{\nu_1} \ldots \omega_d^{\nu_d} \\ &= a_1^{\mu_1} \ldots a_d^{\mu_d}. \end{aligned}$$

Recalling Theorem 4.24 we note that $h : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ defined by $(\nu_1, \ldots, \nu_d) \mapsto (\mu_1, \ldots, \mu_d)$ where $\omega_1^{\nu_1} \ldots \omega_d^{\nu_d} = a_1^{\mu_1} \ldots a_d^{\mu_d}$ is analytic on $\mathbb{Z}_p^d$. As $\rho(\lambda) = h(p^{-m}\lambda)$ it follows that ρ is analytic on $p^m\mathbb{Z}_p^d$ and hence $\gamma : V \to H$ is analytic and our claim is established.

Now take any $h \in H$. It is clear that hV is a neighbourhood of h in H, and that

$$\beta\big|_{hV} = f_{bhb^{-1}} \circ \gamma \circ f_{h^{-1}}\big|_{hV}.$$

Now, by the claim we know γ is analytic, and we showed above that f_g is analytic on G for all G. Hence, as the composition of analytic functions β is analytic on a neighbourhood of h, and as h was arbitrary β is analytic on H as required. It follows that g is analytic and G is a p-adic analytic group. □

Example 4.36. [$SL_n(\mathbb{Z}_p)$ is a p-adic analytic manifold.]

In Examples 2.22, 2.25, 2.34 we showed that $\Gamma_1 \lhd_o SL_p(\mathbb{Z}_p)$ is a powerful finitely generated pro-p group. Thus, as above, $SL_n(\mathbb{Z}_p)$ contains an open uniform subgroup and is a p-adic analytic manifold. □

It is a simple extension to show that this is the unique manifold structure on G extending that of H. We have shown that any topological group containing a uniform pro-p group is p-adic analytic. However, as shown in Proposition 2.51 every powerful finitely generated pro-p group contains an open uniform subgroup.

We have thus established one direction of Lazard's theorem:

Theorem A *A topological group has the structure of a p-adic analytic group if and only if G has an open subgroup which is a powerful finitely generated pro-p group.*

While omitted here for sake of brevity, a proof of the converse in the vain as this thesis can be found in Chapter 8 of [DSMS91].

4.5 Compactness and Dimension

Lazard's Theorem yields two important corollaries. Firstly that we can completely characterise when such a group is compact, and also that any chart on such a group has a constant dimension.

It is clear that any p-adic analytic group G is locally compact as it contains a uniform pro-p group H as an open subgroup. Thus, for any $g \in G$, gH is a compact neighbourhood of g by the definition of profinite groups. It is natural to wonder when G itself is compact, and, using Theorem A we can completely characterise the p-adic analytic groups.

Theorem 4.37. *A p-adic analytic group G is compact if and only if it is a profinite group.*

Proof. By definition every profinite group is compact. To establish the converse, suppose that G is a compact p-adic analytic group. By Theorem A we have a uniform pro-p group $H \leq_o G$. As

$$G = \bigcup_{g \in G} gH$$

and H is Hausdorff, G is Hausdorff. Finally, take any neighbourhood of the identity $N \subseteq G$. Then $N \cap H$ is a neighbourhood of the identity in H and thus (as H is profinite) there exists a $H' \leq_o H$ such that $H' \subseteq N$. But then $H' \leq_o G$ and hence the open subgroups of G form a base for the neighbourhoods of the identity in G. Thus by the definition of profinite groups, G is profinite. □

Example 4.38. [Both $SL_n(\mathbb{Z}_p)$ and $GL_n(\mathbb{Z}_p)$ are compact p-adic analytic groups.]

We have shown above that both are p-adic analytic groups, and hence the result follows from the examples in Chapter 1 where we demonstrated that both are profinite. □

Example 4.39. [A p-adic analytic group that is not compact.]

Take U any uniform pro-p group and consider the product group $\mathbb{Z} \times U$ where $\mathbb{Z}$ is the additive group of integers endowed with the discrete topology. That is, the group operation $*$ on $\mathbb{Z} \times U$ is given by

$$(a, g) * (b, h) = (a + b, gh).$$

It is obvious that $(0, x) \mapsto x$ is a isomorphism between $H := \{(0, u) \mid u \in U\} \leq_o \mathbb{Z} \times U$ and U. This map is in fact a homeomorphisms as there is the natural 1-1 correspondence between the open sets in H and those in U. Hence H is an open uniform pro-p subgroup of $\mathbb{Z} \times U$ and so by Theorem A, $\mathbb{Z} \times U$ is a p-adic analytic group. As $\mathbb{Z} \times U$ is covered by an infinite number of open sets

$$\mathbb{Z} \times U = \bigcup_{a \in \mathbb{Z}} \{a\} \times U$$

it is not compact. □

We move forward now to defining the dimension of a p-adic analytic group. In the proof of Theorem 4.34 we constructed an atlas on G made up of translates of the global chart on H an open uniform pro-p subgroup. All these charts, by definition, have the same dimension, and hence every chart in the atlas described for G had dimension d where $d = d(H)$ was the dimension of H. It seems obvious that this should be the dimension of the manifold, however, we have not shown that every atlas of the manifold G (that is every atlas compatible with that constructed) contains only charts of dimension d. We rectify this now.

Theorem 4.40. *For any p-adic analytic group G with the manifold structure constructed in the proof of Theorem 4.34 with respect to the open uniform pro-p subgroup H. Then any chart of G has dimension $d(H)$. That is, any atlas compatible with that on G contains only charts of dimension d.*

Proof. We have that G is a manifold with the atlas $\mathcal{A} = \{(aH, \phi_a, d) \mid a \in T\}$ where T is a transversal of the cosets of H containing 1, and $\phi_a : aH \to \mathbb{Z}_p^d$ is defined by $x \mapsto \phi(a^{-1}x)$ where $\{(H, \phi, d)\}$ is the global manifold on H. Suppose then that (V, ψ, m) is a chart compatible with each chart in $\mathcal{A}$. Clearly there exists $a \in T$ such $aH \cap V \neq \varnothing$. But then we have an open set in $\mathbb{Z}_p^m$ homeomorphic to an open set in $\mathbb{Z}_p^d$ (via either $\psi \circ \phi_a^{-1}$ on $\phi_a(aH \cap V)$ or $\phi_a \circ \psi^{-1}$ on $\psi(aH \cap V)$. Thus $m = d$ as required. □

While we have shown that the manifold structure we constructed on G has uniform dimension across all charts, we have not shown that this is satisfied for all manifold structures on G with respect to which G is a p-adic analytic group. This is true and an obvious consequence of the following important result which is just beyond the scope of this thesis, but still interesting to now.

Theorem 4.41. *For any topological group G there is at most one p-adic analytic manifold structure on G with respect to which G is a p-adic analytic group.*

We conclude with a simple example of a p-adic analytic manifold that has two charts of different dimension.

Example 4.42. [A p-adic analytic manifold with non-uniform dimension.]

Consider the disjoint union of $A = \mathbb{Z}_p^m$ and $B = \mathbb{Z}_p^n$ (endowed with the p-adic topology),

$$X := A \sqcup B;$$

where $U \subseteq_o X$ if and only if $U \cap A \subseteq_o A$ and $U \cap B \subseteq_o B$. Clearly if ι_j is the identity map of $\mathbb{Z}_p^j$ that a global atlas for A is

$$\mathcal{A} = \{(A, \iota_m, m), (B, \iota_n, n)\}.$$

Hence X is a manifold with non-uniform dimension. □

Chapter 5

Closing Remarks

Our discussion concludes at a rather complete point, having established that each topological group containing an open uniform pro-p subgroup is a p-adic analytic manifold, and stated Theorem A along with its corollaries and some uniqueness results. One might think we have reached as far as we can go in this manner, but this is not at all the case. Clearly we have left our some of the major proofs at the end of the thesis, and on top of this, no discussion of Lie groups is ever truly complete without consideration of the corresponding Lie Algebra.

The other area we mentioned but were restricted from discussing further in this thesis was that of the group algebra and its completion, the Iwasawa algebra. While we were able to establish much of the basic theory of non-commutative Iwasawa algebras, in the Theorems of Chapter 3, and Section 4.3 especially, this is really just the beginning of a field rich in research interest today. The intrigued reader is strongly encouraged to seek [AB06], as it is a unique overview of the research in the area.

Another idea that we have not at all touched on is the notion of an analytic group over a pro-p ring. As the name suggests a pro-p ring is a generalisation of the *topological ring* of p-adic integers. As we did over $\mathbb{Z}_p$ we can define the notions of analytic functions and p-adic analytic manifolds, though the subtleties required are somewhat above the level of this thesis.

However, all these advancements stem from the basic theory of p-adic analytic groups and, in this sense, Lazard's theorem is at their core. Having completed this thesis it is hoped that the reader is equipped with a strong understanding of the basic notions progressing into each of these areas, and has a will to do so.

Thank you for reading my thesis.

Chapter 6

Background: Unipotent Groups

Being rather unrelated to the body of the thesis in the way it has been presented the concept of unipotent groups, as required for the proof of Lemma 3.13, is introduced here. We assume Section 2.1, especially the work done on finite p-groups and nilpotent groups.

Unipotent groups are, in all generality, subgroups of affine algebraic groups in algebraic geometry. However, we consider only subgroups of the general linear group over a field of finite characteristic. Thus for this chapter k will denote a field of characteristic p.

Definition 6.1. If $g \in GL_n(k)$ satisfies $(g-1)^n = 0$ for some $n \in \mathbb{N}$ we say that g is a *unipotent element* of $GL_n(k)$. If $H \leq GL_n(k)$ and each element in H is unipotent then H is said to be a *unipotent group*.

Because k is of characteristic p it is quite easy to see that any such group is a finite p-group. By definition, if $H \leq GL_n(k)$ is unipotent then for any $h \in H$ there exists n such that $(h-1)^n = 0$. Then for any $m \in \mathbb{N}$ such that $p^m > n$

$$h^{p^m} - 1 = (h-1)^{p^m} = 1$$

and so h is of pth power order. H is also clearly finite as $M_n(k)$ is. Clearly though the reverse argument works just as well, if $H \leq GL_n(k)$ is a finite p-group then there exists an $m \in \mathbb{N}$ such that $0 = h^{p^m} - 1 = (h-1)^{p^m}$. So we have

Proposition 6.2. *A subgroup H of $GL_n(k)$ is unipotent if and only if it is a finite p-group.*

Since $V = k^n$ is an additive group, and H is a group of group homomorphisms on V we can define the *semidirect product*, $V \rtimes H$, of H and V as the group on the set $V \times H$ with operation $*$ where

$$(v, h) * (v', h') = (v + h(v'), hh').$$

One can check that this operation is associative, that the identity in $V \times H$ is $(0, 1)$, and that the inverse of (v, h) is $(h^{-1}(-v), h^{-1}) = (-h^{-1}(v), h^{-1})$.

This is clearly also a p-group (as H is of order p and so is k^n) and so is nilpotent by Proposition 2.8. We consider the lower central series of $V \rtimes G$, and define $V_{(j)}$ to be the set of all $v \in V$ such that $(v, h) \in \gamma_j(V \rtimes H)$ for some $h \in H$. We

see that if $v \in V_{(j)}$ then there exists some $f \in H$ and $(w_i, h_i) \in \gamma_{j-1}(V \rtimes H)$ and $(x_i, g_i) \in V \rtimes H$ such that

$$(v, f) = [(w_1, h_1), (x_1, g_1)][(w_2, h_2), (x_2, g_2)] \dots [(w_m, h_m), (x_m, g_m)].$$

However, as

$$[(w, h), (x, g)] = (h^{-1}(-w) + h^{-1}g^{-1}(-x) + h^{-1}g^{-1}(w) + h^{-1}g^{-1}h(x), [h, g])$$

we see that v is merely the sum of transformations of w_i and x_i. It is clear then that if $V_{(j-1)}$ is a subspace of V then $V_{(j)}$ will be closed under scalar multiplication and addition and also be a subspace. Hence by induction each $V_{(j)}$ is subspace of V (as $V_{(1)} = V$). In fact this gives us that if $(v, h) \in \gamma_j$ then $(\lambda v, h) \in \gamma_j$, and in particular $(0, h) \in \gamma_j$. It follows that for any $(v, h) \in \gamma_j$)

$$(v, h) * (0, h^{-1}) = (v, 1) \in \gamma_j$$

and that $\gamma_k = V_{(j)} \times H_{(j)}$ for some $H_{(j)} \leq H$. Now for any $h \in H$ and any $v \in V_{(j)}$

$$[(v, 1), (0, h^{-1})] = (-v, 1) * (0, h) * (v, 1) * (0, h^{-1}) = (-v + h(v), 1)$$

But modulo γ_{j+1}, $[(v, 1), (0, h^{-1})]$ must be the identity, and thus $h(v) = v$ (modulo $V_{(j+1)}$).

Let $V_n = k^n$ and $V_i = V_{(l)}$ such that $V_{(l)}$ is the first $V_{(j)}$ with dimension i (we know such a $V_{(j)}$ exists as $V \rtimes H$ is nilpotent). So we have a chain of H-invariant subspaces of k^n

$$k^n = V_n > V_{n-1} > \ldots > V_1 > V_0 = 0$$

such that any element of H induces the trivial action on V_i/V_{i-1}. Then it is clear that $(h - 1)V_i \subseteq V_{i-1}$ for each i and each h in H. Our final result is then obvious.

Proposition 6.3. *If $H \leq GL_n(k)$ is unipotent then for any $h_1, \dots, h_n \in H$ we have*

$$(h_1 - 1)(h_2 - 1) \dots (h_n - 1) = 0.$$

The foremost example of a unipotent group is the set of upper (or lower) unitriangular matrices $U_n(k)$. That is matrices in $GL_n(k)$ which are upper (or lower) triangular and have all diagonal elements equal to 1.

$$\begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ 0 & 0 & 1 & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

In fact, it can be shown that for any unipotent $H \leq GL_n(k)$ there exists $g \in GL_n(k)$ such that

$$g^{-1}Hg \leq U_n(k).$$

References

[AB06] Konstantin Ardakov and Ken Brown. Ring-theoretic properties of iwasawa algebras: A survey. *Doc. Math.*, Extra Volume Coates:7–33, 2006.

[Art91] Michael Artin. *Algebra*. Prentice Hall, 1st edition, 1991.

[DF04] David Dummit and Richard Foote. *Abstract Algebra*. John Wiley and Sons, Inc, 3rd edition, 2004.

[DSMS91] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic Pro-p Groups*. Cambridge University Press, 2nd edition, 1991.

[Hig74] Phillip J. Higgins. *An Introduction To Topological Groups*. Cambridge University Press, 1st edition, 1974.

[Hus66] Taqdir Husain. *Introduction To Topological Groups*. W. B. Saunders Company, 1st edition, 1966.

[Khu97] Evgenii I. Khukhro. *p-Automorphisms of Finite p-Groups*. Cambridge University Press, 1st edition, 1997.

[Kin74] Bruce King. Normal subgroups of groups of prime-power order. In *Proceedings of the Second International Conference on The Theory of Groups*, volume 372 of *Lecture Notes in Mathematics*, pages 401–408. Springer Berlin / Heidelberg, 1974.

[Kob80] Neal Koblitz. *p-adic Analysis: a Short Course on Recent Work*. Cambridge University Press, 1st edition, 1980.

[LM87a] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. i. finite groups. *Journal of Algebra*, 105:484–505, 1987.

[LM87b] Alexander Lubotzky and Avinoam Mann. Powerful p-groups. ii. p-adic analytic groups. *Journal of Algebra*, 105:506–515, 1987.

[MM07] B. Mashayekhy and F. Mohammadzadeh. Some inequalities for nilpotent multipliers of powerful p-groups. *Bulletin of the Iranian Mathematical Society*, 33:61–71, 2007.

[MPF03] Avinoam Mann and Fania Posnick-Fradkin. Subgroups of powerful groups. *Israel Journal of Mathematics*, 138:19–28, 2003.

[NS06] Nikolay Nikolov and Dan Segal. On finitely generated profinite groups i: Strong completeness and uniform bounds. *ArXiv Mathematics e-prints*, April 2006.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer-Verlag, 1st edition, 2000.

[Ser65] J. P. Serre. *Lie Algebras and Lie Groups*. Springer-Verlag, 1st edition, 1965.

[Ser73] J. P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1st edition, 1973.