KASDI MERBAH UNIVERSITY OUARGLA

Faculty of Mathematics and Sciences Material

N° d'ordre :
N° de série :

Department of: Mathematics

Masterial

Path: Mathematics

Speciality: Algebra and Geometry

Present by:SIHEM TOUAHR

Theme:

SUBGROUP GROWTH IN P ADIC ANALYTIC GROUPS

Represented in : 11/10/2020

Limb from jury:

Mr. Guerboussa Yassine	Kasdi Merbah University-Ouargla	Supervisor
Mr. Benmoussa M.Tayeb	Kasdi Merbah University-Ouargla	Examiner
Mr. Boussaid Mohamed	Kasdi Merbah University-Ouargla	Examiner
Mr. Bahayou Amine	Kasdi Merbah University-Ouargla	Examiner

Dedication

I dedicate this work :
To my dear father (Mammer) who is the reason for my presence and who taught me the meaning of success and patience in the face of difficulties
To my dear mother (Fatima) who was always a candle illuminating my path and spared no effort in raising me and guiding me
To my supervisor (Mr. Yassine Guerboussa)
To my sisters who shared my childhood : (Zahra,Aicha,Nesrine,Miada).
To my only brother and my companion (Belkacem). and my cousin who supported me in this work (Lazhar), to (my uncles / aunts), each in his name .
To my fiance (Adel Belabbas)
To o my friends who were the cause of my laugh and my smile in life :(Z.Salma, Z.Zainab, G.Sabah, Salima, Masouda, T.Karima,H.Farida).
To my colleagues who was with me on my university course : (Zineb.M, , Al-Romaissa, Izdihar.K. Zineb.S,Imane.H, kaouthar.M,Hinda.O,Ibtissam.B) and all my teachers from university.

Sihem Touahr

Contents

Notation

The notation is standard and follows mainly that of [3]. In particular, If G is a group, and H is a subset of G, then

- $|H|$ denotes the cardinality of H
- $H \leq G$ means that H is a subgroup of G
- $H < G$ means that H is a proper of G
- $H \lhd G$ means that H is a normal subgroup of G
- $|G : H|$ the index of H in G
- $H \leq_f G$ means that H is a subgroup of G of finite index.
- $C_G(H)$ the centralizer of H in G, that is $C_G(H) := \{x \in G \,|\, xh = hx, h \in H\}$
- $Z(G)$ the centre G, that is $Z(G) := C_G(G)$.
- $[x, y]$, the commutator of $x, y \in G$, that is $[x, y] := x^{-1}y^{-1}xy$
- For $H, K \subseteq G$, $[H, K]$ is the subgroup generated by all the commutators $[x, y]$, $x \in H$ and $y \in K$.

If G is a topological group, then

- $\overline{H}$ is the topological closure of H, i.e., the intersection of all the closed subsets of G containing H
- $H \leq_o G$ (resp. $H \leq_c G$) signify that H is an open (resp. closed) subgroup of G.
- Similarly, $H \lhd_o G$ and $H \lhd_c G$ have their obvious meaning.

Introduction

Let G be a finitely generated group. It is well-known that for every integer $n \geq 1$, G has only finitely many subgroups of index n, the number that we shall denote $a_n(G)$ (note that we could have $a_n(G) < \infty$ for all n, without assuming G finitely generated). The investigation of the interplay between the structure of G and the behaviour of the sequence $(a_n(G))$, known as the subgroup growth of G, has flourished in the last thirty years. If R denotes the intersection of all subgroups of finite index in G, then $R \lhd G$, and $a_n(G) = a_n(G/R)$; thus there is no loss of generality if we assume that $R = 1$, that is G is residually finite. Hence, studying subgroup growth may be restricted to the category of finitely generated residually finite groups. This leads us naturally to the category of (topologically) finitely generated profinite groups, since every group G in the previous category has a canonical embedding in its profinite completion $\hat{G} = \varprojlim G/N$, where N runs over the finite index subgroups of G, and we have moreover $a_n(G) = a_n(\hat{G})$, where $a_n(\hat{G})$ has its obvious topological sense, i.e. the number of closed subgroups of $\hat{G}$ of finite index (now, we know, thanks to Segal and Nikolov (2008), that all the subgroups of $\hat{G}$ of finite index are closed!).

This work deals with the subgroup growth in p-adic analytic pro-p groups, i.e., pro-p groups that admit a structure of a Lie group over the field of p-adic numbers $\mathbb{Q}_p$ (instead of $\mathbb{R}$). The latter can be characterized as the pro-p groups Γ having polynomial subgroup growth, that is to say $a_n(\Gamma) \leq n^c$ for some positive constant c, and all n.

The above result was very important in characterizing all the groups having polynomial subgroup growth (PSG). More precisely, a finitely generated residually finite group G has PSG if, and only if, it is virtually soluble of finite rank. The proof of the latter involves the classification of finite simple groups, and serious algebraic geometry and number theory.

An interesting related subject that we'll not discuss is that of zeta functions of groups. For a group G, we define such a function as the Dirichlet series $\zeta_G(s) = \sum_{n \geq 1} a_n(G) n^{-s}$, $s \in \mathbb{C}$. Observe that for $G = \mathbb{Z}$, we recover the Riemann zeta function $\zeta(s) = \sum_{n \geq 1} n^{-s}$, so the subject can be viewed as a sort of non-commutative number theory. Note also that $\zeta_G(s)$ is particularly interesting when G is PSG; it is exactly the case where $\zeta_G(s)$ has a finite convergence abscissa.

The thesis is divided into two chapters. In the first one, we remind some basic results on finite p-groups, inverse systems of groups and projective limits, and the notions of profinite and pro-p groups. The basic notions related to subgroup growth are discussed in the third

section. The more serious things are discussed in the second chapter. As the introduction of the theory of powerful p-groups, by A. Lubotzky and A. Mann (1987), simplified notably the treatment of p-adic analytic groups, the first and the second sections are devoted to discuss the main properties of powerful p-groups, as well as powerful pro-p groups, being in principle inverse limits of powerful p-groups. We discuss the p-adic analytic pro-p groups in the third section, and we characterize them in terms of their subgroups growth as mentioned above. We give further perspectives, mainly the characterization of groups having polynomial subgroup growth (PSG), in the remaining sections.

Chapter 1

Preliminaries

1.1 Basic definitions

1.1.1 Groups

Definition 1.1 *We call group every set G together with an operation $(x, y) \mapsto xy$, from $G \times G$ to G, which saisfies the following axioms:*

(i) *For all $x, y, z \in G$, we have $(xy)z = x(yz)$. (Associativty)*

(ii) *G has an identity element, i.e., an element e so that $xe = ex = x$, for all $x \in G$.*

(iii) *Every $x \in G$ has an inverse, that is an element $x' \in G$ such that $xx' = x'x = e$.*

If G is a group, an identity element $e \in G$ is unique as if e' is another one, then $e' = ee' = e$. We shall denote this identity element by 1 if the law of G is written multiplicaively, and by 0 if it is denoted additively (i.e., by the symbol $+$).

For instance, $\mathbb{Z}$ is a group under the usual addition. For any commutative ring K, the set $\mathrm{GL}_n(K)$ of the $n \times n$ invertible matrices with coefficients in K is a group under the usual multiplication of matrices. This group is called the general linear group of degree n over K.

Definition 1.2 *Let G be a group. A subgroup of G is non empty subset H of G which satisfies $xy^{-1} \in H$ for all $x, y \in H$.*

The above definition amounts to saying that $1 \in H$, $xy \in H$ and $x^{-1} \in H$ whenever $x, y \in H$. Note that this means that H is itself a group under the law induced by that of G. We write $H \leq G$ to indicate that H is a subgroup of G. If in addition $H \neq G$, then we say that H is proper subgroup of G, and we write $H < G$.

Exemple 1 *1. For all $n \in \mathbb{N}$, the subset $n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$ is a subgroup of the additive group $\mathbb{Z}$. Conversely, one sees easily that every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some non negative integer n.*

2. If we consider the additive group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ of the integers modulo 6, then $H = \{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$.

3. For a commutative ring K, the set $\mathrm{SL}_n(K) = \{A \in M_n(k) \mid \det A = 1\}$ is a subgroup of the general linear group $\mathrm{SL}_n(K)$; it is known as the special linear group of degree n over K.

The intersection of any family of subgroups of G is likewise a subgroup. Hence, if $X \subseteq G$, then the intersection of all the subgroups of G containing X is the smallest subgroup containing X. We call the latter the subgroup generated by X, and we denote it $\langle X \rangle$.

Definition 1.3 *Let G and G' be two groups and $\psi : G \to G'$ be a map. We say that ψ is a group homomorphism (or just a homomorphism) if $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in G$.*

A bijective group homomorphism is called an *isomorphism*. An isomorphism from G to itself is called an *automorphism* of G; we denote by $\mathrm{Aut}(G)$ the set of these automorphisms. It is readily seen that $\mathrm{Aut}(G)$ is a subgroup of the permutation group on G, that is $\mathrm{Aut}(G)$ form a group under the usual composition of maps.

For every $g \in G$, we have a canonical homomorphism $\tau_g : G \to G$ where $\tau_g(x) = x^g$ for all $x \in G$ (where x^g denotes $g^{-1}xg$). We call the latter the inner automorphism induced by g (it is indeed an automorphism as it admits $\tau_{g^{-1}}$ as an inverse). The map $g \mapsto \tau_g$, from G to $\mathrm{Aut}(G)$ is a group homomorphism whose kernel is known as the center of G, usually denoted $Z(G)$. Clearly $Z(G)$ is formed by all the $g \in G$ so that $gx = xg$ for all $x \in G$. The image of τ is called the group of inner automorphisms of G, and denoted $\mathrm{Inn}(G)$.

Let $H \leq G$. We say that H is normal (resp. characteristic) if it is invariant under all the inner automorphisms (resp. automorphisms) of G, that is to say $g^{-1}hg \in H$ for all $h \in H$ and $x \in G$ (resp. $h^a \in H$ for all $h \in H$ and $a \in \mathrm{Aut}(G)$. We write $H \lhd G$ to indicate that H is a normal subgroup of G.

If $H \lhd G$, the set G/H of left cosets xH, $x \in G$, can be endowed with a group structure by setting :

$$(xH)(yH) = xyH.$$

It is readily seen that the latter operation is well defined, for which the group axioms are fulfilled. Note that the canonical projection $x \mapsto xH$, from G to G/H is a surjective group homomorphism.

1.1.2 Commutators

Let G be a group. If $x, y \in G$, the commutator $[x, y]$ is defined as $[x, y] = x^{-1}y^{-1}xy$. If $X, Y \subseteq G$, we define $[X, Y]$ as the subgroup generated by all the commutators $[x, y]$, with $x \in X$ and $y \in Y$.

For $g \in G$, we have clearly $[x, y]^g = [x^g, y^g]$. It follows in particular that if $H, K \lhd G$, then so is $[H, K]$.

Sometimes we denote $[G, G]$ simply by G', and we call it the commutator subgroup of G. It has the following important property:

Proposition 1.1 *The quotient G/G' is abelian; and if $H \lhd G$ so that G/H is abelian, then $G' \leq H$. In other words, G/G' is the largest abelian quotient of G.*

Indeed, if $x, y \in G$, then by definition $[x, y] \in G'$; hence the class $\overline{[x, y]}$ mod G' is trivial, so $[\overline{x}, \overline{y}] = 1$ in G/G', and so G/G' is abelian. If $N \lhd G$ has an abelian quotient , then $[\overline{x}, \overline{y}] = 1$ mod N, or equivalently $\overline{[x, y]} = N$. It follows that N contains all the commutators $[x, y]$, with $x, y \in G$, so N contains G' as desired.

The following identities can be checked by straightforward calculation:

(i) $[x, y] = [y, x]^{-1}$

(ii) $[x, y, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$

(iii) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$

(iv) $[[x, y^{-1}], z]^y[[y, z^{-1}], x]^z[[z, x^{-1}], y]^x = 1$ (the Hall-Witt identity).

We shall write simply $[x, y, z]$ for $[[x, y], z]$, and more generally $[x_1, \ldots, x_n]$ instead for $[[\ldots[x_1, x_2], \ldots, x_{n-1}], x_n]$.

1.1.3 Finite p-groups

Definition 1.4 *We say that a group G is a p-group if its order is a power of p, that is $|G| = p^n$ for some positive integer n.*

The most fundamental property of a p-group G is that $Z(G) \neq 1$ if G is non trivial. Indeed, if $G \neq 1$ is p-group, then by letting G act on itself by conjugation, the classes equation gives

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

where the g_i's are representatives of the non trivial conjugacy classes; since p divides $|G|$ and $|G : C_G(g_i)|$ for all i, it follows that p divides $|Z(G)|$, and since $1 \in Z(G)$, then necessarily $|Z(G)| > 1$ as desired.

If we define by induction $Z_0(G) = 1$, and $Z_{n+1}(G)$ to be the unique subgroup satisfying $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$, then it follows that $G = Z_c(G)$ for some integer c whenever G is a p-group (a group that satisfies the latter property is termed *nilpotent*); hence every p-group is nilpotent.

Proposition 1.2 *Let G be a nilpotent group. For every proper subgroup H of G we have $H < N_G(H)$ (where $N_G(H)$ is formed by the $g \in G$ that normalize H, that is $g^{-1}Hg \subseteq H$).*

To see that, consider $H < G$, and let n be the smallest positive integer such that $Z_n(G) \nsubseteq H$ (if no such integer exists then all the terms $Z_l(G)$ are in H, and since G is nilpotent, one should have $H = G$, a contradiction). Pick $g \in Z_n(G) \setminus H$; then by definition $h^{-1}h^g \subseteq Z_{n-1}(G)$ for all $h \in H$, and by the minimality of n, $Z_{n-1} \subseteq H$, thus $g \in N_G(H) \setminus H$; this completes the proof.

It follows for instance that if G is a p-group and M is a maximal subgroup of G, then $M \lhd G$, and M has index p. Indeed, we have $M < N_G(M)$, so by the previous result $N_G(M) = G$, which proves that M is normal in G. Moreover, G/M is a simple group, with nontrivial center, so certainly $G/M \cong \mathbb{Z}/p\mathbb{Z}$ normal and has index p in G.

Definition 1.5 *The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G.*

For the case where G has no maximal subgroups, the above is defined as $\Phi(G) = G$. This is the case for example of $G = (\mathbb{Q}, +)$, or G is a Prüfer p-group, i.e. the group of all the p^n-th roots of unity in $\mathbb{C}$, with n runs over $\mathbb{N}$.

The Frattini subgroup has the following interesting property:

Proposition 1.3 *Let G be a group in which every proper subgroup is contained in a maximal subgroup of G. If we have $X \subseteq G$ such that $\langle X \cup \Phi(G)\rangle = G$, then $\langle X\rangle = G$.*

Note that the above proposition holds in particular for the finite groups. To prove it, let $X \subset G$ such that $\langle X \cup \Phi(G)\rangle = G$; if $\langle X\rangle$ is a proper subgroup of G, then it can be embedded by assumption in a maximal subgroup, M say, but $\Phi(G) \subseteq M$, so $X \cup \Phi(G) \subseteq M$, and then $\langle X \cup \Phi(G)\rangle \leq M$, a contradiction.

Proposition 1.4 *Let G be a finite p-group. Then*

(i) *$\Phi(G) = G'G^p$, where $G^p = \langle x^p \mid x \in G\rangle$.*

(ii) *If $X \subseteq G$ and $X\Phi(G)$ generates $G/\Phi(G)$ then X generates G.*

(iii) *$G/\Phi(G) \cong \mathbb{F}_p^n$ where d is the minimal cardinality of any generating set for G.*

Proof. As we have already seen, if M is a maximal subgroup of G, then $M \lhd G$ and $G/M \cong \mathbb{Z}/p\mathbb{Z}$. In particular, $[x, y], x^p \in M$ for all $x, y \in G$; this shows that M contains all the generators of G' and G^p, so it contains both of them, that is $G'G^p \subseteq M$. The latter is true for all the maximal subgroups M of G, thus $G'G^p \subseteq \Phi(G)$. Conversely, $G/G'G^p$ can be viewed as a vector space over the field of p elements, and the maximal subgroups of G correspond to the hyperplane in the latter quotient; as the hyperplane has trivial intersection, it follows that $\Phi(G) \subseteq G'G^p$.

The second statement follows at once from the previous proposition, and the third one from (i) and (ii).

■

It follows that every minimal generating set X of G (i.e., X generates G and no proper subset of X does) has cardinality $d(G)$, where $d(G) = \dim_{\mathbb{F}_p} G/\Phi(G)$. This last statement is known as *the Burnside basis theorem*.

We define the *rank* of G, denoted $\mathrm{rk}(G)$ as the maximum among the $d(H)$, where $H \leq G$. We shall use this notion extensively in the next chapter.

1.2 Pro p-groups

1.2.1 Inverse systems; inverse limits

Let Λ be a poset (partially ordered set). We say that Λ is directed if for all $\alpha, \beta \in \Lambda$, there exists $\gamma \in \Lambda$ such that $\gamma \geqslant \alpha$ and $\gamma \geqslant \beta$.

Note that we can view each poset Λ as a category whose objects are the elements of Λ, and for any two objects $\alpha, \beta \in \Lambda$, there is a unique morphism $\alpha \to \beta$ if $\alpha \leqslant \beta$, and none of them otherwise. We suppose in the sequel that Λ is a directed poset.

Let $\mathcal{C}$ be a category. We call an *inverse system* (or projective system) in $\mathcal{C}$, indexed by Λ, every family $(X_\alpha)_{\alpha\in\Lambda}$ of objects in $\mathcal{C}$ together with a family of morphisms $f_{\alpha\beta} : X_\beta \to X_\alpha$ defined whenever $\beta \geqslant \alpha$, which satisfy the following conditions:

(i) For all $\alpha, \beta, \gamma \in \Lambda$ such that $\gamma \geqslant \beta \geqslant \alpha$, the two morphisms $X_\gamma \xrightarrow{f_{\beta\gamma}} X_\beta \xrightarrow{f_{\alpha\beta}} X_\alpha$ and $X_\gamma \xrightarrow{f_{\alpha\gamma}} X_\alpha$ coincide, that is $f_{\alpha\beta} \circ f_{\beta\gamma} = f_{\alpha\gamma}$.

(ii) For all $\alpha \in \Lambda$, the morphism $X_\alpha \xrightarrow{f_{\alpha\alpha}} X_\alpha$ is the identity morphisme X_α, that is $f_{\alpha\alpha} = 1_{X_\alpha}$.

We shall denote such a system simply by $(X_\alpha, f_{\alpha\beta})$.

One sees immediately that the inverse systems in $\mathcal{C}$ indexed by Λ are exactly the contravariant functors from the category Λ to $\mathcal{C}$. It follows that these systems form a category which we denote $\mathrm{Mor}(\Lambda^{op}, \mathcal{C})$; its morphisms are the natural transformations: if $(X_\alpha, f_{\alpha\beta})$

and $(Y_\alpha, g_{\alpha\beta})$ are two objects in $\mathrm{Mor}(\Lambda^{op}, \mathcal{C})$, a morphism from the first to the second is a family of morphisms $(\varphi_\alpha : X_\alpha \to Y_\alpha)_{\alpha\in\Lambda}$ in $\mathcal{C}$ such that for all $\beta \geqslant \alpha$, the following diagram commutes

We shall be mainly interested in the category of finite groups, p-groups (we see them as well as subcategories of that of discrete topological groups).

Let G be a group. We write $N \trianglelefteq_f G$ to indicate that N is a normal subgroup of G of finite index. The set of the latter subgroups is ordered by reverse inclusion "$\succcurlyeq$": $N \succcurlyeq M$ means $N \subseteq M$ for $N, M \trianglelefteq_f G$. This set is directed since $M \cap N \succcurlyeq M$ and N, and plainly $M \cap N \trianglelefteq_f G$. Let $N, M \trianglelefteq_f G$ be such that $N \succcurlyeq M$, then the assignment $xN \mapsto xM$ defines a group morphism $G/N \to G/M$. It follows that the family $(G/N)_{N\trianglelefteq_f G}$ together with the above canonical morphisms is an inverse system of finite groups (i.e. in the category of finite groups). We can view each G/N as a discrete topological group, so we have in fact an inverse system of topological groups.

Note that we can replace the finite quotients of G by the one which are finite p-groups, so the above example yields an inverse system of finite p-groups.

Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system in a category $\mathcal{C}$. We call an *inverse limit* of this system every object $X \in \mathcal{C}$ together with family a $\{\pi_\alpha : X \to X_\alpha\}_{\alpha\in\Lambda}$ that is compatible with the morphisms $f_{\alpha\beta}$ (i.e. whenever $\alpha \geq \beta$ we have $f_{\alpha\beta} \circ \pi_\alpha = \pi_\beta$) and satisfies the following universal property:

For any family $\{\varphi_\alpha : Y \to X_\alpha\}_{\alpha\in\Lambda}$ of morphisms in $\mathcal{C}$ which is compatible with the $f_{\alpha\beta}$'s, there is a unique morphism $\varphi : X \to Y$ such that $\pi_\alpha \circ \varphi = \varphi_\alpha$ for all $\alpha \in \Lambda$.

The forgoing universal property guarantees that if an inverse limit of the system $(X_\alpha, f_{\alpha\beta})$ exists, then it is unique up to isomorphism. We may hence denote it by $\varprojlim_{\alpha\in\Lambda} X_\alpha$.

Assume $\mathcal{C}$ is the category of toplogical groups, so $(X_\alpha, f_{\alpha\beta})$ is an inverse system of topological groups. The inverse limit of such a system always exists and can be constructed as follows:

Consider the direct product $\prod_{\alpha\in\Lambda} X_\alpha$ endowed with the product topology, so it is a topological group in a natural way, and consider next the subspace:

$$X = \{(x_\alpha) \in \prod_{\alpha\in\Lambda} X_\alpha \mid x_\beta = f_{\alpha\beta}(x_\alpha) \text{ for all } \alpha \geq \beta\}.$$

It is readily seen that X is a subgroup of $\prod_{\alpha\in\Lambda} X_\alpha$, so it is a topological group; the canonical projections $\pi_\lambda : X \to X_\lambda$, $\pi_\lambda(x_\alpha) = x_\lambda$, are compatible with the $f_{\alpha\beta}$'s, and it follows easily from the universal property of the product $\prod_{\alpha\in\Lambda} X_\alpha$ that $X = \varprojlim_{\alpha\in\Lambda} X_\alpha$.

1.2.2 Pro-p groups: definition and basic properties

Definition 1.6 *We call a pro-p group every inverse limit of finite p-groups (each endowed with the discrete topology).*

We may define likewise a *profinite group* to be an inverse limit of finite groups.

The following is a useful characterization of the pro-p groups.

Proposition 1.5 *For a topological group G to be pro-p, it is necessary and sufficient that G be Hausdorff, compact, and admits a basis for the neighbourhoods of 1 formed by normal subgroups of p-power index.*

Assume first that G is a pro-p group, so $G = \varprojlim_\alpha G_\alpha$ for some inverse system $(G_\alpha, f_{\alpha\beta})$ of p-groups. As we have seen above, we may identify G as:

$$G = \{(x_\alpha) \in \prod_\alpha G_\alpha \mid x_\beta = f_{\alpha\beta}(x_\alpha) \text{ for all } \alpha \geq \beta\}.$$

Now, the product $\prod_\alpha G_\alpha$ is Hausdorff, and compact by the well-known Tychonoff's theorem. It follows that G is Hausdorff, and to see that it is compact it suffices to show that G is a closed subset in $\prod_\alpha G_\alpha$. Let $x = (x_\alpha)$ be in $\prod_\alpha G_\alpha \setminus G$; hence there exist $\alpha \geq \beta$ such that $f_{\alpha\beta}(x_\alpha) \neq x_\beta$. Let $U = \prod_\lambda U_\lambda$, where $U_\alpha = \{x_\alpha\}$, $U_\beta = \{x_\beta\}$ and $U_\lambda = G_\lambda$ otherwise. Plainly, U is open $\prod_\alpha G_\alpha$, and if $(g_\lambda) \in U$, then in particular $g_\alpha = x_\alpha$ and $g_\beta = x_\beta$; therefore $f_{\alpha\beta}(g_\alpha) \neq g_\beta$, and so $g \notin G$. This proves that $U \subseteq (\prod_\alpha G_\alpha) \setminus G$; so $(\prod_\alpha G_\alpha) \setminus G$ is open in $\prod_\alpha G_\alpha$. Thus G is a closed subset, as desired. Now, for each finite set of indices ω, define N_ω to be $\prod_\lambda A_\lambda$, where $A_\lambda = \{1\}$ if $\lambda \in \omega$ and $A_\lambda = G_\lambda$ for $\lambda \neq \alpha$. Plainly, N_ω is an open normal subgroup of G, and $(\prod_\alpha G_\alpha)/N_\omega \cong \prod_{\alpha\in\omega} G_\alpha$, so N_ω has p-power index in $\prod_\alpha G_\alpha$. Moreover, by definition of the product topology, each neighbourhood of 1 in $\prod_\alpha G_\alpha$ contains one of these N_ω. It follows now that the family $(G \cap N_\omega)_\omega$, where ω runs over all the finite subsets of indices, form a basis for the neighbourhood of 1 in G, and has the desired properties.

Conversely, assume that G is a Hausdorff compact topological group, and that there exists a basis $\mathcal{N}$ for the neighbourhoods of 1 formed by open normal subgroups of p-power index. Clearly, $\mathcal{N}$ is a directed poset under reverse inclusion, and for all $N, M \in \mathcal{N}$ satisfying $M \subseteq N$, we have a canonical morphism $G/N \to G/M$, sending each xN to xM; so we have an obvious inverse system $(G/N)_{N\in\mathcal{N}}$ of p-groups, and consequently the pro-p group $\hat{G} = \varprojlim_{N\in\mathcal{N}} G/N$. The canonical projections $G \to G/N$, $N \in \mathcal{N}$, are obviously compatible with our inverse system, so they induce a continuous group homomorphism $\mathrm{j} : G \to \hat{G}$ (explicitly, $\mathrm{j}(x) = (xN)_{N\in\mathcal{N}}$, for all $x \in G$). We claim that j is an isomorphism of topological groups (so in particular G is pro-p). We have $\ker \mathrm{j} = \bigcap_{N\in\mathcal{N}} N$, and the latter is equal to the intersection of all the neighbourhoods of 1, hence $\ker \mathrm{j} = 1$ since G is Hausdorff. Now, as G is compact, and $\hat{G}$ is Hausdorff, it follows that G is isomorphic to $j(G)$ (in the category

topological groups), so it remains only to see that j is surjective. Let $(x_N N) \in \hat{G}$; since every $N \in \mathcal{N}$ is closed in G (N is open, so all its cosets are, but $G \setminus N$ is a union of cosets of N; this justifies why N is closed), the $x_N N$ are closed subsets of G. If $\bigcap_{N\in\mathcal{N}} x_N N$ is empty, then since G is compact, we can find a finite subset $\omega \subset \mathcal{N}$ such that $\bigcap_{N\in\omega} x_N N = \emptyset$; now let $M = \bigcap_{N\in\omega} N$, so $M \in \mathcal{N}$, and by definition, $x_M N = x_N N$ for all $N \in \omega$; in particular $x_M \in \bigcap_{N\in\omega} x_N N$, a contradiction. Thus $\bigcap_{N\in\mathcal{N}} x_N N \neq \emptyset$; let x be an element of the latter, so $xN = x_N N$ for all N, and thus $\mathrm{j}(x) = (x_N N)$. This completes the proof of prop. 1.5.

We have a similar characterization of the profinite groups, namely a topological group G is profinite if, and only if, G is Hausdorff, compact, and its identity element has a basis for its neighbourhoods formed by normal subgroups of finite index. To see this, we could imitate the above proof verbatim, replacing only "p-group" by "finite group".

More generally, for every group G, we can consider the inverse system $(G/N)_{N\in\mathcal{N}}$, where $\mathcal{N}$ denotes the collection of the normal subgroups of G of finite index (resp. p-power index) ordered by reverse inclusion, and consider hence the inverse limit $\varprojlim_{N\in\mathcal{N}} G/N$, which we denote $\hat{G}$ (resp. $G_{\hat{p}}$), and call the *profinite completion* (resp. the *pro-p completion*) of G. We have a canonical group homomorphism $\mathrm{j} : G \to \hat{G}$ (resp. $\mathrm{j} : G \to G_{\hat{p}}$), sending every $x \in G$ to $(xN)_{N\in\mathcal{N}}$. This morphism is injective if, and only if, G is residually finite (resp. residually-p), that is the intersection of normal subgroups of G of finite index (resp. p-power index) is the trivial subgroup. Moreover, $\mathrm{j}(G)$ is dense in $\hat{G}$ (resp. $G_{\hat{p}}$), that is $\overline{\mathrm{j}(G)} = \hat{G}$ (resp. $\overline{\mathrm{j}(G)} = G_{\hat{p}}$). The latter morphism, allows us to carry over problems on abstract groups to ones on profinite or pro-p groups.

If G is a profinite group, then every closed subgroup H of G of finite index is open, and vice versa (this holds in fact in every compact topological group). Indeed, if $H \leq_c G$, and H has fi finite index, then $G \setminus H$ is a union of finitely many cosets xH, each being closed in G since for the left translations $g \mapsto xg$ are homeomorphisms of G onto itself; thus H is open in G. Conversely, if $H \leq_o G$, then since the cosets of H form an open (irredundant) cover of G, this cover should be finite as G is compact; so H has only finitely many cosets, that is H has finite index, and plainly H is closed as the cosets of H are open.

Note also that every closed subgroup H of a pro-p group G is likewise pro-p. Indeed, such an H is necessarily Hausdorff, and compact since it is closed, and if (N_α) is a basis for the neighbourhoods of $1 \in G$ formed by normal subgroups of p-power index, then so is $(H \cap N_\alpha)$ for H. One sees similarly, that if $N \lhd_c G$, then G/N, endowed with the quotient topology, is a pro-p group. The fact that N is closed is necessary to assure that G/N is Hausdorff (equivalently, $\{N\}$ is closed in G/N); the remaining conditions can be checked easily.

Let G be a profinite group. We say that $X \subseteq G$ generates G topologically if the subgroup $\langle X \rangle$ is dense in G. Define

$$d(G) = \min\{|X| \mid X \subseteq G \text{ which generates } G \text{ topologically}\}.$$

We say that G is finitely generated if $d(G)$ is finite; in this case $d(G)$ is in fact the minimal number of generators of G. For example, if G is a finitely generated, then so is its profinite completion (pro-p completion) since G is dense in $\hat{G}$ (in $G_{\hat{p}}$).

Proposition 1.6 *Let G be a profinite group, and $X \subseteq G$. Then X generates G topologically if, and only if, XN/N generates G/N, for all $N \lhd_o G$.*

Indeed, let $N \lhd_o G$. We have $\overline{\langle X \rangle} N/N \subseteq \overline{(\langle X \rangle N/N)}$, so if $\overline{\langle X \rangle} = G$, then $\overline{(\langle X \rangle N/N)} = G/N$; but every such N has finite index, so G/N is discrete; it follows that $\overline{(\langle X \rangle N/N)} = \langle X \rangle N/N$, so XN/N generates G/N. Conversely, if the latter holds, then in particular, $\langle X \rangle N = G$ for all $N \lhd_o N$, that is $\bigcap_{N \lhd_o G} \langle X \rangle N = G$; but clearly $\bigcap_{N \lhd_o G} XN = \overline{\langle X \rangle}$. Q.E.D.

We define the Frattini subgroup $\Phi(G)$ of G as the intersection of all (proper) maximal open subgroups of G. As every open subgroup of G is closed, it follows in particular that $\Phi(G) \lhd_c G$.

Proposition 1.7 *Let G be a pro-p group. Then*

1. $\Phi(G) = \overline{[G,G]G^p}$.
2. *G is finitely generated if and only if $\Phi(G)$ is open in G (equivalently, $\Phi(G)$ has finite index in G).*

Indeed, if M is an open maximal subgroup of G, then M contains some $N \lhd_o G$, and it follows that M/N is a maximal subgroup of the p-group G/N, thus $[G,G]G^p \subseteq M$, as we have seen for p-groups; subsequently, $[G,G]G^p \subseteq \Phi(G)$, and so $\overline{[G,G]G^p} \subseteq \Phi(G)$ as $\Phi(G)$ is closed. For the reverse inclusion, observe that for every $N \lhd_o G$ containing $/\overline{[G,G]G^p}$, G/N is elementary abelian, and in particular $\Phi(G) \subseteq N$; but $\Phi(G)$ is the intersection of all these N's; this proves the first assertion.

If G is finitely generated, say by d elements , then in particular $G/\overline{[G,G]G^p}$ is. As indicated above, if $N \lhd_o G$ containing $\Phi(G)$, G/N is elementary abelian, hence $|G:N| \leq p^d$. It follows that the intersection of all these N has finite index, but the former is just $\Phi(G)$, so $\Phi(G)$ is a closed subgroup of finite index in G; this shows that $\Phi(G)$ is open. Conversely, if the latter holds, then we can find a finite set, say X, such that $X \cup \Phi(G)$ generates G (as an abstract group). If $N \lhd_o G$, then by the first part, $\Phi(G/N) = \Phi(G)N/N$. As $(X \cup \Phi(G))N/N$ generates G/N, it follows that XN/N generates G/N; the results is obvious now by Proposition 1.6. Q.E.D.

Define inductively, $P_1(G) = G$, and $P_{n+1}(G) = \overline{[P_n(G), G]P(G)^p}$ for $n \geq 1$. One can see in the similar way that the $P_n(G)$ are all open provided that G is finitely generated.

1.3 Subgroup growth

Let G be a group. For every positive integer n we define $a_n(G)$ to be the number of subgroups of G of index n. We may define likewise $s_n(G)$ to be the number of subgroups of G of index at most n, that is $s_n(G) = \sum_{i=1}^{n} a_i(G)$.

For example, if $G = \mathbb{Z}$, then there is exactly one subgroup of index $n \geq 1$, namely $n\mathbb{Z}$, so $a_n(\mathbb{Z}) = 1$ for all $n \geq 1$. It follows at once that $s_n(\mathbb{Z}) = n$.

It may happen that $a_n(G) = \infty$, although, we have:

Proposition 1.8 *If G is finitely generated, then G has only finitely many subgroups of index n, for every positive integer n.*

Proof. Every subgroup H of index n in G gives rise to a homomorphism $\rho : G \to S_{G/H} = S_n$ (we identify H with $1 \in \{1, \ldots, n\}$), where $\rho(g)$ maps every class xH to $(gx)H$. Observe that $H \subseteq G$ is characterized by the property of being the stabilizer of $\{1, \ldots, n\}$. As every homomorphism from G to S_n is completely determined by its values on a generating set of G, if $G = \langle x_1, \ldots, x_d \rangle$, then there are at most $(n!)^d$ homomorphism from G to S_n, so there are only finitely many stabilizers of 1 in G; thus there are only finitely many of such H.
■

Thus if G is finitely generated, then $a_n(G) < \infty$, and we can safely speak about the subgroup growth G. Note, although, that we could have $a_n(G) < \infty$ for all n, without the assumption that G is finitely generated (for instance, when $G = \mathbb{Q}$, we have $a_n(G) = 0$ for all n). Note also that J. Wilson proved that if G satisfies the maximal conditions on normal subgroups (i.e. every ascending sequence of normal subgroups of G is stable), then $a_n(G) < \infty$. In the sequel, we focus our interest on finitely generated groups. While we have far-reaching results on the subgroup growth of the latter groups, much remains to do for infinitely generated ones.

Denote by R the intersection of all normal subgroups of G of finite index. If $H \leq_f G$, then H has only finitely many conjugates H^g; thus $\bigcap_{g \in G} H^g$ is a normal subgroup of G of finite index, and consequently $R \subseteq \bigcap_{g \in G} H^g \subseteq H$; thus R is contained in all the $H \leq_f G$. Since we have a one-to-one correspondence between the subgroups of G containing R and the subgroups of G/R, it follows at once that $a_n(G/R) = a_n(G)$. So we lose nothing in this context if we assume that $R = 1$, that is to say G is residually finite. Henceforth, unless otherwise stated, all the groups that we shall consider will be supposed residually finite.

If we have a profinite group Γ, we define $a_n(\Gamma)$ (resp. $s_n(\Gamma)$) to be the number of closed subgroups of Γ of index n (reps. index $\leq n$). Since every $H \leq_c \Gamma$ of finite index is open, and vice versa; it that $a_n(\Gamma)$ is in fact the number of open subgroups of Γ of index n.

Consider now the canonical map from G to its profinite completion $\hat{G}$; the assumption that G is residually finite implies that the latter map is injective, so we may identify G with its image in $\hat{G}$. We have then, $\overline{G} = \hat{G}$ as mentioned previously. This suggests to consider the map $H \mapsto \overline{H}$ from the set of finite index subgroups of G to that of the open subgroups of $\hat{G}$. We claim that $|G : H| = |\hat{G} : \overline{H}|$ for all $H \leq G$. Note that once this is proved, then it follows immediately that

$$a_n(G) = a_n(\hat{G}), \quad \text{for all } n \geq 1.$$

To prove our claim, observe only that $G \cap \overline{H} = H$, so the map $G/H \to \hat{G}/\overline{H}$ sending every xH to $x\overline{H}$, is a well-defined bijection.

Chapter 2

Subgroup growth in p-adic analytic groups

The introduction of the theory of powerful p-groups, by A. Lubotzky and A. Mann (1987) simplified notably the treatment of p-adic analytic groups, i.e. the analogues of Lie groups over the field of p-adic numbers $\mathbb{Q}_p$ (instead of $\mathbb{R}$). One may compare the exposition of the theory in [3] with that of Lazard's [2], to realize the advantages. The first and the second section are devoted to discuss the main properties of powerful p-groups, as well as powerful pro-p groups, being in principle inverse limits of powerful p-groups. We discuss the p-adic analytic pro-p groups in the third section, and we characterize them in terms of their subgroups growth, and give further perspectives in the remaining sections.

2.1 Powerful p-groups

Definition 2.1 *Let G be a p-group and $N \trianglelefteq G$. We say that N is powerfully embedded in G, if $[N, G] \subseteq N^p$ (for $p = 2$ we require that $[N, G] \leq N^4$). We say that G is poweful if it is powerfully embedded in itself.*

If N is powerfully embedded in G, we write N p.e. G. Obviously, N p.e G implies that N is normal in G.

The previous definition is equivalent to saying that N p.e G if and only if $[N, G] \subseteq N^{2p}$.

Lemma 2.1 *Let G be a nilpotent group, and $N, M \trianglelefteq G$. If $N \subseteq M[N, G]$, then $N \subseteq M$.*

Proof. We proceed by induction on n to show that

$$N \subseteq M[N,_n G], \quad \text{pour tout entier } n > 0. \tag{2.1}$$

The latter is trivial for $n = 1$. Let $x \in M$, $y \in [N,_n G]$ and $g \in G$; we have $[xy, g] = [x, g]^y [y, g]$; since $[M, G] \trianglelefteq G$, we have $[x, g]^y \in [M, G]$, hence

$$[xy, g] \in [M, G][N,_{n+1} G],$$

it follows that

$$[M[N,_n G], G] = [M, G][N,_{n+1} G].$$

By induction we have $N \subseteq M[N,_n G]$, so

$$[N, G] \subseteq [M, G][N,_{n+1} G];$$

as $[M, G] \subseteq M$,

$$N \subseteq M[N, G] \subseteq [M, G][N,_{n+1} G];$$

and (2.1) follows. Since G is nilpotent, there exists $n > 0$ such that $[N,_n G] = \{1\}$; the result now is immediate from (2.1). ∎

Remark 1 *Let $N \lhd G$, and set $\overline{G} = G/[N, G, G]$ and $\overline{N} = N/[N, G, G]$. For N to be p.e. in G, it is necessary and sufficient that $\overline{N}$ be p.e. in $\overline{G}$. Indeed, the property $[\overline{N}, \overline{G}] \subseteq \overline{N}^{2p}$ is equivalent to $[N, G] \subseteq N^{2p}[N, G, G]$; but by the previous lemma, the latter is equivalent to $[N, G] \subseteq N^{2p}$.*

Hence, to prove that N p.e G, we can always assume that $[N, G, G] = \{1\}$; in other words, we can replace G and N by $G/[N, G, G]$ and $N/[N, G, G]$.

To fix the ideas, we assume in the sequel that $p > 2$. The arguments for $p = 2$ need slight modifications, cf. [3].

Proposition 2.1 *Let $N, M \leq G$. If N and M are p.e. in G, then the same is true for N^p, $[N, M]$, et NM.*

Proof.

(i) N^p p.e G.

We can assume by the previous remark that $[N^p, G, G] = 1$. Since N p.e G, we have $[N, G] \subseteq N^p$, so $[N, G, G, G] = \{1\}$, the latter means that $[N, G, G] \subseteq Z(G)$. Let $x \in N$ and $g \in G$; the last property implies at once that $t \mapsto [x, g, t]$ is a homomorphism from G to $Z(G)$; in particular

$$[x, g, t^j] = [x, g, t]^j \quad \text{pour tout entier } j \geq 0. \tag{2.2}$$

It follows easily by induction on n that

$$[x^n, g] = [x, g]^{x^{n-1}} [x, g]^{x^{n-1}} \cdots [x, g];$$

in particular

$$[x^p, g] = \prod_{i=1}^{p} [x, g]^{x^{p-i}} = \prod_{i=1}^{p} [x, g][x, g, x^{p-i}]. \tag{2.3}$$

It follows from the fact that $[x, g, x^{p-i}] \in Z(G)$, and the property (2.2) that

$$[x^p, g] = [x, g]^p \prod_{i=1}^{p} [x, g, x]^{p-i} = [x, g]^p [x, g, x]^{\binom{p}{2}}. \tag{2.4}$$

As $p > 2$, we have $\binom{p}{2}$ is divisible by p; the last equation implies then $[x^p, g] \in [N, G]^p$. An element of N^p is a product of elements of the form x^p, $x \in N$; hence by the left distributivity of commutators we have $[N^p, G] \subseteq [N, G]^p$; mbut, $[N, G]^p \subseteq (N^p)^p$; the result follows.

(ii) $[N, M]$ p.e. G.

We will show that

$$[N^p, M] \subseteq [N, M]^p. \tag{2.5}$$

Once this is proved , we obtain by symmetry $[M^p, N] \subseteq [M, N]^p$. Thus,

$$[N, G, M] \subseteq [N^p, M] \subseteq [N, M]^p,$$

and

$$[G, M, N] \subseteq [M^p, N] \subseteq [N, M]^p;$$

the three subgroups lemma implies then

$$[N, M, G] \subseteq [N, M]^p,$$

which proves the result. To prove (2.5) we may suppose that $[N, M, G, G] = \{1\}$, and so $[N, M, G] \subseteq Z(G)$. On can hence apply the formulae (2.2), (2.3) and (2.4), for $x \in N$ and $g \in M$. It follows immediately that $[N^p, M] \subseteq [N, M]^p$.

(iii) NM p.e G.

It is readily seen that $[NM, G] = [N, G][M, G]$; the fact that M and$N$ are p.e. in G implies that

$$[N, G][M, G] \subseteq N^p M^p,$$

and obviously, $N^p M^p \subseteq (NM)^p$; the result follows.

■

For every p-group G, the lower p-central series is defined inductively by $P_1(G) = G$, and $P_{n+1}(G) = P_n(G)^p [P_n(G), G]$ for $n \geq 1$. We define similarly $\Pi_1(G) = G$, and $\Pi_{n+1}(G) = \Pi_n(G)^p$ for $n \geq 1$.

The following result is immediate from prop. 2.1.

Proposition 2.2 *Let G be a powerful p-group. Then the subgroups $\gamma_n(G)$, $G^{(n)}$, and $P_n(G)$ are p.e. in G, for all integers $n \geq 1$.*

Note that it is straightforward to see by induction that if G is powerful, then $P_n(G) = \Pi_n(G)$ for all $n \geq 1$.

Lemma 2.2 *If $G = \langle a_1, \ldots, a_d \rangle$ is a powerful p-group, then $G^p = \langle a_1^p, \ldots, a_d^p \rangle$*

Proposition 2.3 *In a powerful p-group G, the $\{x^{p^n}, x \in G\}$ is a subgroup, for all $n \geq 1$.*

Now the power structure of G can be described in some detail.

Theorem 2.1 *Let G be a powerful p-group minimally generated, say, by $x_1, \ldots, x_d$, and set $P_i = P_i(G)$. Then*

(i) P_i *p.e. in* G.

(ii) $P_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ *for each* $k \geq 0$, *and in particular* $P_{i+1} = \Phi(P_i)$.

(iii) $P_i = P^{p^{i-1}} = \left\{ x^{p^{i-1}} \mid x \in G \right\} = \left\langle x_1^{p^{i-1}}, \ldots, x_d^{p^{i-1}} \right\rangle$.

(iv) The map $x \mapsto x^{p^k}$ induces a homomorphism from P_i/P_{i+1} onto P_{i+k}/P_{i+k+1}, for all i and k.

The following property represents one of the most important properties of powerful p-groups. For a proof we refer the reader to [3, Theorem 2.9], in which a short argument due to A. Caranti is given.

Theorem 2.2 *If G is a powerful p-group, then $d(H) \leq d(G)$ for every $H \leq G$. In other words,* $\mathrm{rk}(G) = d(G)$.

The last result has a converse; more precisely, if G is a p-group and r denotes its rank, then G contains a characteristic powerful subgroup N whose index is $\leq p^{f(r)}$, for some integer $f(r)$ depending only on r ($f(r)$ is given explicitly below). To this end, it is convenient to introduce the following definition:

For every integer $d > 0$, let $V(G, d)$ be the intersection of the kernels of all the homomorphisms $\rho : G \to \mathrm{GL}(d, p)$). It is readily seen that $V(G, d)$ is a characteristic subgroup of G, i.e., stable under all the automorphisms of G. Note that we can replace $\mathrm{GL}(d, p)$ with $\mathrm{T}_1(d, p)$ the group of upper uni-triangular matrices over $\mathbb{F}_p$; indeed, the latter is a Sylow p-subgroup in $\mathrm{GL}(d, p)$), so the image of every $\rho : G \to \mathrm{GL}(d, p)$) lies in $\mathrm{T}_1(d, p)$ up to an appropriate conjugation. For $g \in G$ to be in $V(G, d)$, it is necessary and sufficient that for every linear representation W of dimension d of G, g fixes all the elements in W. Equivalently $g \in V(G, d)$ if and only if g acts trivially in every action of G on a vector space over $\mathbb{F}_p$ of dimension d. First, let us prove the following useful fact about the $\mathrm{T}_1(d, p)$.

Lemma 2.3 *The group* $\mathrm{T}_1(d,p)$ *has a subnormal series with elementary abelian factors of length at most* $\lambda(d)$*, where* $\lambda(d)$ *is the unique integer satisfying* $2^{\lambda(d)-1} < d \leq 2^{\lambda(d)}$*.*

To see that, we proceed by induction on d. For $d = 1$, the result is trivial. Assume $d \geq 2$, and let r be the smallest integer $\geq d/2$. The map:

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \mapsto (A, B)$$

from $\mathrm{T}_1(d,p)$ to $\mathrm{T}_1(r,p) \times \mathrm{T}_1(d-r,p)$, is a well-defined group morphism, surjective, and whose kernel is isomorphic to the additive group $\mathbb{F}_p^{r(d-r)}$. Now, $\mathrm{T}_1(r,p)$ and $\mathrm{T}_1(d-r,p)$ have subnormal series (H_i) and (K_i) of length at most $\lambda(r)$ with elementary abelian factors; so $(H_i \times K_i)$ is likewise a subnormal series in $\mathrm{T}_1(r,p) \times \mathrm{T}_1(d-r,p)$ with elementary abelian factors and length $\leq \lambda(r)$. Thus $\mathrm{T}_1(d,p)$ has a similar series of length $\leq \lambda(r)+1$; but $\lambda(r)$ satisfies $2^{\lambda(r)-1} < d/2 \leq 2^{\lambda(r)}$, hence $2^{\lambda(r)} < d \leq 2^{\lambda(r)+1}$, that is $\lambda(r)+1 = \lambda(d)$. Q.E.D.

Proposition 2.4 *Let* G *be a* p*-group,* $d > 0$ *an integer, and* $N \trianglelefteq G$ *such that* $d(N) \leq d$*. Let* $V = V(G,d)$*.*

(i) If $p > 2$ *and* $N \leq V(G,d)$*, then* N *is p.e. in* V*.*

(ii) If $p = 2$ *and* $N \leq V^2$*, then* N *is p.e. in* V^2*.*

We can now prove our claimed converse of Theorem 2.2.

Theorem 2.3 *Let* G *be a* p*-group of rank* r*. Then* G *has a characteristic powerful subgroup* N *such that* $|G:N| \leq p^{r\lambda(r)}$ *(for* $p = 2$*, the latter bound reads* $2^{r+r\lambda(r)}$*).*

Proof. Let $V = V(G,r)$. By definition, G/V can be embedded in a direct product of copies of $\mathrm{T}_1(d,p)$; it follows from Lemma 2.3 that G/N has a subnormal series of length $\leq \lambda(r)$ with elementary abelian factors, but since G/V has rank r, the order of each of these factors is at most p^r, thus $|G:V| \leq p^{r\lambda(r)}$. Now, take $N = V$ if $p > 2$, and $N = V^2$ if $p = 2$, and observe that $|V:V^2| \leq 2^r$ in the last case. The result follows at once from the last proposition. ■

2.2 Powerful pro-p groups

Definition 2.2 *Let* G *be a pro-p group, and* $N \leq G$*. We say that* N *is powerfully embedded in* G*, and write* N *p.e.* G *for short, if* p *is odd and* $[N,G] \leq \overline{N^p}$*, or if* $p = 2$ *and* $[N,G] \leq \overline{N^4}$*. We say that* G *is powerful if* G *if it is powerfully embedded in itself.*

Clearly, G is powerful if, and only if, $G/\overline{G^p}$ is abelian ($G/\overline{G^4}$ is abelian, for $p=2$). Also, if N p.e. G, then $N \lhd G$ and N is powerful.

The following criterion clarifies the relation between the powerful (finite) p-groups and pro-p groups.

Proposition 2.5 *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 every $K \lhd_o G$.*

Indeed, let $K \lhd_o G$. Note first that $[NK/K, G/K] = [N,G]K/K$ and $(N/K)^{2p} = \overline{N^{2p}}K/K = N^{2p}K/K$. Hence, if N p.e. G, then we have $[N/K, G/K] \subseteq N^{2p}K/K$, that is NK/K p.e. G/K. Conversely, if NK/K p.e. G/K holds for every $K \lhd_o G$, then $[N,G] \subseteq N^{2p}K$ for all $K \lhd_c G$. Since $G/\overline{N^{2p}}$ is Hausdorff, and $N^{2p}K/\overline{N^{2p}}$ is a basis for the neighbourhoods of its identity element $\overline{N^{2p}}$, it follows that $\bigcap_{K \lhd_c G} N^{2p}K = \overline{N^{2p}}$; thus $[N,G] \subseteq \overline{N^{2p}}$, as desired.

As a first consequence, the above with Proposition 2.2 yield:

Proposition 2.6 *Let G be a powerful pro-p group. Then the subgroups $\gamma_n(G)$, $G^{(n)}$, and $P_n(G)$ are p.e. in G, for all integers $n \geq 1$ (where each of those subgroups is interpreted topologically, i.e., we take the topological closure of the abstract analogue).*

By observing that each pro-p group G is isomorphic to $\varprojlim_{N \lhd_o G} G/N$, the following is immediate.

Corollary 2.1 *A group G is a powerful pro-p group if and only if G is the inverse limit of an inverse system of powerful p-groups in which all the morphisms are surjective.*

Proof. Assume G is a powerful pro-p group. Then $G \cong \varprojlim G/N$, where N runs over the open normal subgroups of G, and clearly each G/N is a powerful p -group. Conversely, suppose $G = \varprojlim G_\alpha$ where each G_α is a powerful p-group, and all the morphisms $G_\alpha \to G_\beta$, $\alpha \geq \beta$, are surjective. Obviously, G is a pro-p group, and the latter property assures that for every $K \lhd_c G$, G/K is a quotient of some G_α, in particular G/K is powerful. The result follows now at once from the previous proposition.

■

The last results permits to carry out the results on poweful p-groups to the (finitely generated) pro-p groups.

Proposition 2.7 *Let G be a powerful finitely generated pro-p group. Then every element in G^p is a p-th power, and $G^p = \Phi(G)$ is open in G. If $p = 2$, then G^4 is open in G.*

Proof. Let $g \in \overline{G^p}$, and $N \lhd_o G$. We have $gN \in (G/N)^p$, so by prop. 2.3, gN is a *p-th* power in G/N. It follows that g is a p-th power in G. Hence $\overline{G^p} \leq G^p$, and so $G^p = \overline{G^p}$ consists of p th powers. Now, since $[G,G] \leq \overline{G^p}$, it follows that $G^p = \Phi(G) = P_2(G)$, and $\Phi(G)$ is open by Proposition 1.7. If $p = 2$, a similar argument shows that $P_3(G) \leq G^4 = \overline{G^4}$, which proves that G^4 is open. ■

Theorem 2.4 *Let $G = \overline{\langle x_1, \ldots, x_d \rangle}$ be a finitely generated powerful pro-p group, and write P_i for $P_i(G)$. Then*

(i) *P_i p.e. G.*

(ii) *$P_{i+k} = P_{k+1}(P_i) = P_i^{p^k}$ for each $k \geq 0$, and in particular $P_{i+1} = \Phi(P_i)$.*

(iii) *$P_i = G^{p^{i-1}} = \left\{ x^{p^{i-1}} \mid x \in G \right\} = \left\langle x_1^{p^{i-1}}, \ldots, x_d^{p^{i-1}} \right\rangle$.*

(iv) *the map $x \mapsto x^{p^k}$ induces a homomorphism from P_i/P_{i+1} onto P_{i+k}/P_{i+k+1}, for all i and k.*

Proof. The above follow from Theorem 2.1 applied to the finite p -groups G/G^{p^n} for sufficiently large n. ■

Theorem 2.5 *Let G be a powerful finitely generated pro-p group and H a closed subgroup. Then $\mathrm{d}(H) \leq \mathrm{d}(G)$.*

Indeed, let $H \leq_c G$. For every $N \lhd_o G$, HN/N is a subgroup of the powerful p-group G/N; by Theorem 2.2 we have $d(HN/N) \leq d(G/N) \leq d(G)$. But by Proposition 1.6, $d(H) = \sup_{N \lhd_o G} HN/N$; the theorem follows.

Similar to Proposition 2.4 , we have:

Proposition 2.8 *Let G be a finitely generated pro-p group, $N \lhd_o G$, and r be a positive integer. Put $V = V(G, r)$. If $\mathrm{d}(N) \leq r$, and $N \subseteq V$ ($N \leq V^2$ for $p = 2$.); then N p.e. V (N p.e. V^2 if $p = 2$).*

Now, imitating the proof of Theorem 2.3, yields the following important result.

Theorem 2.6 *Let G be a finitely generated pro-p group, and suppose that $r = \sup_{N \lhd_o G} \mathrm{d}(N)$ is finite. Then G has a powerful characteristic open subgroup of index at most $p^{r\lambda(r)}$ (the latter reads $2^{r+r\lambda(r)}$ if $p = 2$).*

(Recall that $\lambda(r)$ is the integer defined by $2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}$).

2.3 p-Adic analytic pro-p-groups

Let G be a profinite group. We define the rank of G, denoted $\mathrm{rk}(G)$ to be the supremum of the $d(H)$, where H runs over all the closed subgroups of G (we refer the reader to §1.2.2, for the meaning of $d(H)$). The latter can be expressed in terms of finite groups as follows:

$$\mathrm{rk}(G) = \sup_{N \lhd_o G} \mathrm{rk}(G/N).$$

Indeed, write r for the member on the right. It should be clear that $\mathrm{rk}(G/N) \leq \mathrm{rk}(G)$ for all $N \lhd_o G$, so $r \leq \mathrm{rk}(G)$. Conversely, if $H \leq_c G$, then $d(HN/N) \leq rk(G/N) \leq r$, so $\sup_{N \lhd_o G} d(HN/N) \leq r$; but by Proposition 1.6, $\sup_{N \lhd_o G} d(HN/N) = d(H)$. It follows that $d(H) \leq r$ for all $H \leq_c G$, and subsequently $\mathrm{rk}(G) \leq r$, which completes the proof.

Definition 2.3 *We say that a pro-p group G is p -adic analytic group if G has finite rank, that is to say* $\mathrm{rk}(G) < \infty$.

In fact, saying that a topological group G is a p-adic analytic group, means naturally that G has the structure of a p-adic analytic manifold (say a manifold over the field of p-adic numbers $\mathbb{Q}_p$ instead of $\mathbb{R}$) such that the function $\mu : G \times G \to G$ defined by $(x, y) \mapsto xy^{-1}$ is analytic. For the general theory of analytic groups over arbitrary (complete) valued fields, we refer the reader to Serre's "Lie algebras and Lie groups". The theory of Lie groups over $\mathbb{Q}_p$ has been developed by Lazard in 1965 (see [2]). After the introduction of powerful p-groups in 1987, the theory became more close to abstract group theory. The formulation of the definition as above emerged from the following more general result (which may be viewed as a solution of the Hilbert's fifth problem for p-adic Lie groups).

Theorem 2.7 *A topological group G 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.*

By Theorem 2.5, every finitely generated powerful pro-p group has finite rank. Conversely, if G is a pro-p group of finite rank r, then by Theorem 2.6, G contains a powerful characteristic subgroup N of index bounded in terms of r. Thus the above theorem can be stated as follows:

A topological group G has the structure of a p-adic analytic group if and only if G has an open subgroup which is a pro-p group of finite rank.

The latter justifies the definition we gave for p-adic analytic pro-p groups. A theory of Lie algebras of p-adic Lie group can be as well developed using mainly the powerful pro-p groups (or merely, the uniformly powerful ones). We have to note also that every p-adic analytic pro-p group can be embedded as a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$, for some n, where $\mathbb{Z}_p$ denotes the ring of p-adic integers (the pro-p completion of $\mathbb{Z}$). Proofs for all of the previous statements, and more, can be found in [3].

2.4 Subgroup growth in p-adic analytic groups

The following is the main result in this thesis. It gives a characterization of the p-adic analytic pro-p groups in terms of subgroup growth; the result is due to Mann and Lubotzky (1991).

Theorem 2.8 *Let G be a pro-p group. Then, G is analytic p-adic if, and only if, G has polynomial subgroup growth, i.e., there exists constants $c > 0$ such that $a_n(G) \leq n^c$ for all $n \geq 1$.*

Note that since $a_n(G) = 0$ if n is not a power of p, the last statement is equivalent to that $a_{p^n}(G) \leq p^{cn}$ for all n. The above amounts also to saying that $s_n(G)$ grows at most polynomially.

The remaining part of this section is devoted to prove the previous theorem.

Assume first that G has finite rank, say r. For every $H \leq_o G$, the quotient $H/\Phi(H)$ is elementary abelian (see Proposition 1.7) of rank $\leq r$. Thus H contains at most $(p^r - 1)/(p-1) < p^r$ subgroups of index p. For each $n \geq 0$, every open subgroup of index p^{n+1} is contained in some open subgroup of index p^n, hence $a_{p^{n+1}}(G) \leq p^r a_{p^n}(G)$. Now, by induction, $a_{p^n}(G) \leq p^{rn}$ for all $n \geq 0$. This proves that the p-adic analytic pro-p groups have polynomial subgroup growth.

Conversely, as $\Phi(G)$ is the intersection of open sub-groups of index p in G, and by assumption there there are at most p^c of those, it follows that $\Phi(G)$ has finite index in G; equivalently, $\Phi(G)$ is open in G. Thus G is finitely generated (see Proposition 1.7). We claim now that there exists a bound $\beta > 0$ such that

$$d(N) \leq \beta, \text{ for all } N \lhd_o G \qquad (*)$$

For every positive integer r, define $S_r = \{N \lhd_o G \mid d(H) \geq r\}$. Assume that $S_r \neq \emptyset$, and pick $N \in S_r$ such that G/N has the minimal possible order. Thus for every $M \lhd_o G$ such that $|G : M| < |G : N|$, we have $d(M) \leq r - 1$. In particular G/N has rank $\leq r - 1$. Consider the action of G on $N/\Phi(N)$ by conjugation, i.e., the one defined by $\overline{x}^g = \overline{x^g}$ for all $\overline{x} \in G/N$ and $g \in G$. Set $d = d(N)$, so $N/\Phi(N)$ is actually a vector space of dimension d over the finite field $\mathbb{F}_p$, and our action induces a group homomorphism $G \to \mathrm{T}_1(d, p)$. Denote by K the kernel of this action; thus G/K can be embedded in $\mathrm{T}_1(d, p)$. Since $[N, N] \subseteq \Phi(N)$, $N \leq K$, and in particular G/K has rank $\leq r - 1$. It follows from Lemma 2.3 that $|G : K| \leq p^{r\lambda(d)}$.

We have in fact $N = K$, as if $N < K$, then K/N is a non trivial normal subgroup of G/N, hence it intersects $Z(G/N)$ non trivially. If we pick $g \in G \setminus N$ such that gN be in the latter intersection, then $L = N\langle g \rangle$ is a normal open subgroup of G which satisfies $[L, L] = [L, N] \leq \Phi(N)$. Hence $L/\Phi(N)$ is abelian of rank $\geq r$ as it contains $N/\Phi(N)$. This contradicts the minimality of G/N. Now, we have $|G : N| \leq p^{r\lambda(d)}$.

Let $s = d/2$ if d is even, or $s = (d-1)/2$ if d is odd. The vector space $N/\Phi(N)$ has exactly $(p^d - 1) \cdots (p^{s+1} - 1)/(p^s - 1) \cdots (p - 1)$ subspaces of codimension s. One check easily that the last number is at least $p^{(d-1)^2/4}$; hence G has at least $p^{(d-1)^2/4}$ closed subgroups of index $\leq p^{r\lambda(d)+s}$. As G has polynomial subgroup growth, it follows that

$$p^{(d-1)^2/4} \leq p^{c(r\lambda(d)+s)} \text{ for some constant } c > 0.$$

The above implies that d is bounded in terms of c, and since $r \leq d$, r is likewise bounded in term of c. This shows that $S_r = \emptyset$ for all r large enough, hence $(*)$ holds true.

Finally, let $r = \sup_{N \lhd_o G} d(N)$. We know from $(*)$ that r is finite. Let $H = V(G, r)$ ($H = V(G, r)^2$ if $p = 2$). Clearly, H is an open normal subgroup of G, so $d(H) \leq r$. Proposition 2.8 implies that H is powerful; thus G has finite rank. This completes the proof.

2.5 Further results

First, let G be a pro-p group. A. Shalev (cf. [5]) proved that if $a_n(G) \leq n^{c \log_p n}$, for some $c < \frac{1}{8}$ and all n large enough, then G is p-adic analytic. In other words, if $a_n(G) \leq n^{c \log_p n}$ ($c < \frac{1}{8}$) for all n large enough, then $a_n(G) \leq n^c$ for some constant $c > 0$. Hence, for every $\varepsilon > 0$, every pro$p$-group G should satisfies $a_n(G) \geq n^{(\frac{1}{8} - \varepsilon) \log_p n}$ for infinitely many n, or G should have polynomial subgroup growth. We may say here that there is a gap for the growth type spectrum of pro-p groups. This sort of "gap theorems" occurs for other classes of groups.

It is worth noting that for every $c \geq 2$, there exists a pro-p groups G satisfying $a_n(G) \leq n^{c \log_p n}$, for all n large enough, but G is not p-adic analytic (cf. [5]). One may wonder here what is the smallest value of c for which the 'gap theorem' holds.

One of the breakthroughs in studying subgroup growth, known as the '*PSG theorem*' characterizes all the finitely generated groups having polynomial subgroup growth (PSG). More precisely:

Theorem 2.9 *A finitely generated residually finite group G satisfies $s_n(G) \leq n^s$, for some s, if and only if G is virtually soluble of finite rank.*

The result has been established by A. Lubotzky, A. Mann, and D. Segal (cf. e.g., [4, Chapter 5]). One implication in the 'PSG theorem' is relatively easy to prove. The reverse implication involves various sophisticated techniques: The classification of finite simple groups; 'Linearization' or in other words finding conditions assuring that some infinite groups are linear over some field; techniques for reducing problems on linear groups to ones on arithmetic subgroups in semi-simple algebraic groups ('strong approximation'); counting lattices in arithmetic groups, and even the Prime Number Theorem (the number of primes not exceeding some number x is approximately $x/\log x$).

We refer the reader to the brilliant book [4] for a proof of the last theorem, and other interesting results in this direction.

Bibliography

[1] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal- Analytic Pro-P Groups(Cambridge University Press)(2003)

[2] [L] M. Lazard (1965) Groupes analytiques p-adiques. Inst. Hautes Etudes Scientifiques, Publ. Math. 26, 389-603.

[3] J. Dixon, M. du Sautoy, A. Mann, D. Segal, Analytic pro-p Groups, second ed., Cambridge Univ. Press, 1999.

[4] A. Lubotzky and D. Segal, Subgroup Growth, Birkhäuser, Basel 2003.

[5] A. Shalev, Growth functions, p-adic analytic groups, and groups of finite coclass. J. London Math. Soc. 46, 111-122.

Abstract. The aim of the present thesis is to show that analytic p-adic pro-p groups are exactly the ones having polynomial subgroup growth.

Keywords: p-adic groups; pro-p groups; subgroup growth.

Résumé. Le but principal de cette thèse est de montrer que les pro-p groupes analytiques p-adiques sont exactement les pro-p groupes dont la croissance des sous-groupes est polynomiale.

Keywords: Groupes p-adiques; pro-p groupes; croissance des sous-groupes.