Universidade de Brasília

Sobre Grupos p-Saturáveis

Gabriela Vasconcelos Torres

Orientador: Emerson Ferreira de Melo

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Sobre Grupos p-Saturáveis

por

Gabriela Vasconcelos Torres

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRA EM MATEMÁTICA

Brasília, 26 de maio de 2021.

Comissão Examinadora:

Emerson Ferreira De Melo

Prof. Dr. Emerson Ferreira de Melo- MAT/UnB (Orientador)

Prof. Dr. Alex Carrazedo Dantas - MAT/UnB (Membro)

Aline de Souza Lima

Profa. Dra. Aline de Souza Lima – UFG (Membro)

Não é preciso sofrer para desfrutar das coisas.
É normal não estar pronte, é normal não saber!

Agradecimentos

Agradeço primeiramente a Deus e à espiritualidade amiga pela oportunidade e pelo amparo em toda a minha caminhada até aqui.

Agradeço à minha família por sempre me incentivarem e ajudarem. Meus pais, Liliane e João Luiz, que fizeram de tudo e mais um pouco para mostrar a importância da educação e me permitir chegar aonde cheguei. Minhes irmães, Valquíria e Chris, que me influenciaram tanto, crescendo junto delus, que talvez nem saibam o quanto eu devo a elus e o quanto sou grata.

Ao Emerson Ferreira de Melo, meu orientador, por não desistir de mim inclusive diante da minha desmotivação com a matemática no início da pandemia e me fazer entender coisas que simplesmente não entravam na minha cabeça. Não teria um professor melhor para desempenhar esse papel.

À minha psicóloga, Karol, sem a qual eu não teria chegado até aqui, ou ao menos teria sofrido muito mais.

À Inah e ao Vítor, jardim do 302, que me acompanharam mais de perto no primeiro ano do mestrado, mas que nunca saíram do meu coração. Se não fossem vocês, minha mudança para Brasília teria sido extremamente difícil. Sou eternamente grata pela família que encontrei em vocês.

Ao Las Primas, que tem primas, tias e irmãs resumidas em melhores amigas. Eu não seria quem eu sou hoje se não tivéssemos nos aproximado tanto.

Ao Vini, que desde o início do mestrado me ajudou em todos os momentos e se tornou meu melhor amigo.

Ao Ali, que me entende tanto sendo tão parecido comigo e assim se tornou meu amigo a partir do momento que nos conhecemos.

Ao Eugênio, que se aproximou mais nos últimos tempos e que foi extremamente importante, não só pela amizade mas também pelo empurrão para meus estudos do espiritismo que eu tanto precisava para o meu equilíbrio emocional nesse período tão difícil da pandemia.

Aos meus professores da graduação, em especial Romildo da Silva Pina que também me orientou numa Iniciação Científica e Jhone Caldeira Silva, que foi a pessoa que mais me influenciou a amar a álgebra, com seu jeito de ser e de ensinar, que me escreveu cartas de recomendação sempre que pedi e me incentivou a vir para a UnB para essa etapa da minha vida que se encerra agora.

Aos meus amigos da sala top, especialmente Edna, Junio e Mateus, que me acolheram antes mesmo do início do curso quando fui conhecer o MAT com meus pais e desde então sempre estiveram à disposição para conversar potoca, para almoçar discutindo polêmicas, para ajudar nas disciplinas. Cada um de vocês desempenhou um papel importantíssimo no decorrer do meu mestrado.

Aos meus colegas na representação estudantil que me acompanharam também desde o início e dividiram essa carga e responsabilidade.

Aos professores da banca, Alex Carrazedo Dantas, Aline de Souza Lima e Igor dos Santos Lima por aceitarem fazer parte desse momento tão importante para mim e por todas as correções e sugestões para a versão final da minha dissertação.

Ao CNPq e à CAPES pelo financiamento durante a elaboração deste trabalho.

A todos vocês o meu sincero agradecimento.

Resumo

Esta dissertação apresenta um estudo sobre grupos p-saturáveis mostrando em especial que um grupo pro-p finitamente gerado livre de torção é p-saturável se, e somente se, é um PF-grupo. Adicionalmente, estudamos os subgrupos normais de tais grupos, provando que um subgrupo normal de um grupo p-saturável é também p-saturável quando contido no subgrupo de Frattini do grupo. Além disso, mostramos que grupos p-ádicos analíticos livres de torção de dimensão menor que p são p-saturáveis.

Palavras-Chave: Grupos pro-p; grupos p-saturáveis; PF-grupos; grupos p-ádicos analíticos; grupos *powerful*; grupos uniformemente *powerful*.

Abstract

This dissertation presents a study on p-saturable groups showing especially that a torsion free finitely generated pro-p group is p-saturable if, and only if, it is a PF-group. Moreover, we study the normal subgroups of these groups, proving that a normal subgroup of a p-saturable group is again p-saturable when contained in the Frattini subgroup of the group. Furthermore, we show that every torsion-free p-adic analytic pro-p group of dimension less than p is p-saturable.

Keywords: Pro-p groups; p-saturable groups; PF-groups; p-adic analytic groups; powerful groups; uniformely powerful groups.

Sumário

Introdução

Um grupo pro-p é o limite inverso de p-grupos finitos ou, equivalentemente, um grupo compacto, totalmente desconexo e Hausdorff no qual o índice de todo subgrupo aberto é uma potência de p. Note que em um grupo pro-p todo subgrupo aberto é fechado e um subgrupo fechado é aberto se, e somente se, tem índice finito.

Sejam G um grupo pro-p finitamente gerado e $\omega : G \to \mathbb{R}_{>0} \cup \{\infty\}$ uma função que satisfaz as seguintes propriedades, para todos $x, y \in G$:

1. $\omega(x) > (p-1)^{-1}$.
2. $\omega(x) = \infty \Leftrightarrow x = 1$.
3. $\omega\left(xy^{-1}\right) \geq min\{\omega(x), \omega(y)\}$.
4. $\omega([x,y]) \geq \omega(x) + \omega(y)$.
5. $\omega(x^p) = \omega(x) + 1$.

Nesse caso, chamamos ω de valoração de G. Dizemos que G é um grupo ***p*-saturável** se para todo $x \in G$ com $\omega(x) > p(p-1)^{-1}$, existe $y \in G$ tal que $x = y^p$. Esse trabalho tem como objetivo o estudo dos grupos p-saturáveis, explorando sua relação com outras famílias de grupos.

Um grupo pro-p é chamado p-ádico analítico se tem a estrutura de uma variedade sobre $\mathbb{Z}_p$, os inteiros p-ádicos, e as operações de grupo são analíticas com respeito a essa estrutura. Dizemos que um grupo pro-p é *powerful* se para p ímpar, $G/\overline{G^p}$ é abeliano ou para $p = 2$, $G/\overline{G^4}$ é abeliano (o fecho $\overline{H}$ de um subgrupo é o menor subgrupo fechado que o contém). E definimos um grupo uniformemente *powerful* como um grupo pro-p *powerful* finitamente gerado livre de torção.

Michel Lazard, em seu artigo *Groupes analytiques p-adiques* [11] de 1965, provou que um grupo topológico é p-ádico analítico se, e somente se, ele tem um subgrupo aberto p-saturável. Na década de 80, Lubotzky e Mann conseguiram substituir nesse resultado de Lazard a hipótese do subgrupo aberto p-saturável pela existência de um subgrupo aberto uniformemente *powerful*. As duas definições, grupos p-saturáveis e grupos uniformemente *powerful*, estão fortemente relacionadas, mas não são equivalentes. De fato, os grupos uniformemente *powerful* formam uma subfamília dos grupos p-saturáveis. Lazard provou que os Sylow pro-p de $GL_n(\mathbb{Z}_p)$ e $SL_n(\mathbb{Z}_p)$ para $n \leq p-2$ são p-saturáveis e Klopsch notou que tais grupos não são uniformemente *powerful* (veja [11] e [10]).

Como mencionamos, os conceitos não coincidem, mas existem ligações entre eles. Grupos uniformemente *powerful* são p-saturáveis e por outro lado, se um grupo G é p-saturável, então G^p é *powerful* e portanto, uniformemente *powerful*.

Em 2008 (veja [3]), Fernández-Alcober, González-Sánchez e Jaikin-Zapirain definiram uma nova família de grupos pro-p, a família dos PF-grupos. Dado um grupo pro-p G, um subgrupo fechado normal N de G é dito PF-imerso em G caso exista uma família de subgrupos fechados normais $\{N_i\}_{i\in\mathbb{N}}$ começando em N tal que $N_i \leq N_j$ para $i \geq j$, $\bigcap\limits_{i\in\mathbb{N}} N_i = 1$ e $[N_i,_{p-1} G] \leq N_{i+1}^p$. Nessas condições, $\{N_i\}_{i\in\mathbb{N}}$ é chamada de *potent filtration* de N e se $N = G$, G é dito um PF-grupo.

Com essa nova definição, González-Sánchez ([4]) provou o seguinte resultado que é uma caracterização de grupos p-saturáveis.

Teorema A. *Seja G um grupo pro-p finitamente gerado livre de torção. Então as seguintes condições são equivalentes:*

1. *G é um grupo p-saturável.*
2. *G é um PF-grupo.*
3. *$G/\Phi(G)^p$ é um PF-grupo, onde $\Phi(G)$ é o subgrupo de Frattini de G.*

Com o intuito de estudar os subgrupos dos grupos p-saturáveis, González-Sánchez provou o seguinte resultado em [4].

Teorema B. *Sejam G um grupo p-saturável e N um subgrupo fechado normal de G contido em $\Phi(G)$. Então N é p-saturável. Por outro lado, existe um grupo p-saturável G com um subgrupo normal que não está contido em $\Phi(G)$ e que não é p-saturável.*

Definimos o posto de um grupo pro-p G como $rk(G) = \sup\{d(H) | H \leq_a G\}$ e a dimensão de um grupo pro-p de posto finito G como $\dim(G) = d(H)$, onde H é um subgrupo aberto uniformemente *powerful* de G e $d(H)$ é o número de geradores de H ([1]).

Sabemos que grupos p-ádicos analíticos tem posto finito. Como vimos acima, grupos p-saturáveis são p-ádicos analíticos, mas a recíproca não é verdadeira. Em [6], González-Sánchez e Klopsch provaram o seguinte resultado.

Teorema C. *Todo grupo pro-p p-ádico analítico livre de torção de dimensão menor que p é p-saturável. Por outro lado, existe um grupo pro-p p-ádico analítico livre de torção de dimensão p que não é p-saturável.*

Nesse trabalho, apresentamos as demonstrações dos Teoremas A, B e C.

No primeiro capítulo, relembramos algumas definições e resultados clássicos acerca da teoria de grupos. Colocamos aqui seções específicas para a teoria de grupos profinitos e para a fórmula de Philip Hall e algumas de suas aplicações.

No segundo capítulo, falamos sobre grupos p-ádicos analíticos e grupos uniformemente *powerful*, apresentando definições e alguns resultados e no fim citamos um teorema relacionando as duas teorias que tem seu desenvolvimento e demonstração no capítulo 8 de [1].

O terceiro capítulo é destinado ao assunto principal desse trabalho. Nele apresentamos a definição de grupos p-saturáveis, além de outras definições importantes e resultados auxiliares para enfim apresentarmos a demonstração dos Teoremas A e B.

No quarto e último capítulo, abordamos a relação entre grupos p-ádicos analíticos e p-saturáveis, apresentando a demonstração do Teorema C.

Lista de Símbolos

$[G:H]$	Índice de H em G
$Z(G)$	Centro de G
$C_G H$	Centralizador de H em G
$N_G H$	Normalizador de H em G
$[x,y]$	$x^{-1}y^{-1}xy$
$[L,M]$	$\langle [l,m] \mid l \in L,\ m \in M \rangle$
$[a_1,a_2,\ldots,a_n]$	$[[a_1,a_2,\ldots,a_{n-1}],a_n]$
$[A_1,A_2,\ldots,A_n]$	$[[A_1,A_2,\ldots,A_{n-1}],A_n]$
$[a,_n b]$	$[a,b,\ldots,b]$ onde b aparece n vezes
$[A,_n B]$	$[A,B,\ldots,B]$ onde B aparece n vezes
$H \subseteq G$	Subconjunto de G
$H \subseteq_a G$	Subconjunto aberto de G
$H \subseteq_f G$	Subconjunto fechado de G
$H \leq G$	Subgrupo de G
$H \leq_a G$	Subgrupo aberto de G
$H \leq_f G$	Subgrupo fechado de G
$H \lhd G$	Subgrupo normal de G
$H \lhd_a G$	Subgrupo aberto normal de G

$H \triangleleft_f G$	Subgrupo fechado normal de G
$G^{(n)}$	n-ésimo termo da série derivada de G
$\gamma_1(G) = G$,	$\gamma_i(G) = [\gamma_{i-1}(G), G]$
$\gamma_n(G)$	n-ésimo termo da série central inferior de G
$P_1(G) = G$,	$P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}$
$P_n(G)$	n-ésimo termo da p-série inferior de G
$\|G\|$	Ordem de G
$\Phi(G)$	Subgrupo de Frattini de G
$\overline{H}$	Fecho de H
$\langle X \rangle$	Subgrupo gerado pelos elementos do conjunto X
$d(G)$	Número de geradores do grupo G
$\mathbb{Q}_p$	Corpo dos números p-ádicos
$\mathbb{Z}_p$	Inteiros p-ádicos
$\mathbb{F}_p$	Corpo com p elementos
$Mat_d(\mathbb{F}_p)$	Grupo das matrizes $d \times d$ com entradas em $\mathbb{F}_p$
$GL_d(\mathbb{F}_p)$	Grupo das matrizes $d \times d$ inversíveis com entradas em $\mathbb{F}_p$
$v_p(x)$	Valoração p-ádica de x
$\|x\|_p$	Valor absoluto p-ádico de x
$\lfloor \alpha \rfloor$	Maior inteiro menor que α
$\lceil \alpha \rceil$	Menor inteiro maior que α

Capítulo 1

Preliminares

1.1 Teoria de Grupos

Os resultados de Teoria de Grupos se baseiam principalmente no livro *Fundamentals of the Theory of Groups* [7].

Como usualmente, definimos um grupo como *livre de torção* se apenas a identidade tem ordem finita e chamamos de *centro do grupo* G o conjunto $Z(G) = \{x \in G \mid x^g = x, \forall g \in G\}$.

Dados um grupo G e elementos $x, y \in G$, definimos o *comutador de* x *e* y *em* G: $[x,y] = x^{-1}y^{-1}xy = x^{-1}x^y$. O subgrupo de G gerado pelos comutadores de elementos de L e M, subconjuntos de G é

$$[L,M] = \langle [l,m] \mid l \in L,\ m \in M \rangle .$$

Podemos também definir comutadores de comprimentos arbitrários indutivamente. Para $n \geq 2$ e dados $a_1, a_2, \ldots, a_n \in G$ e $A_1, A_2, \ldots, A_n \leq G$, temos:

$$[a_1, a_2, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n],$$
$$[A_1, A_2, \ldots, A_n] = [[A_1, A_2, \ldots, A_{n-1}], A_n].$$

Algumas identidades muito úteis ao trabalhar com comutadores são apresentadas a seguir.

Proposição 1.1.1. *Sejam* G *um grupo,* $a, b, c \in G$*,* $H, K, L \leq G$ *e* $\sigma : G \to G^*$ *um homomorfismo. Então:*

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

2. $[ab,c] = [a,c]^b[b,c]$.

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

4. $\sigma([a,b]) = [\sigma(a),\sigma(b)]$.

5. $[ab,c] = [a,c][a,c,b][b,c]$ *e* $[a,bc] = [a,c][a,b][a,b,c]$.

6. $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$. *(Identidade de Witt.)*

7. $[H,K] = [K,H]$.

8. *K normaliza H se, e somente se,* $[H,K] \leq H$ *e K centraliza H se, e somente se* $[H,K] = 1$.

9. $\sigma([H,K]) = [\sigma(H),\sigma(K)]$. *Em particular, o subgrupo comutador de dois subgrupos característicos (normais) é ainda característico (normal).*

10. *Se N é um subgrupo normal de G, então* $[HN/N,KN/N] = [H,K]N/N$.

11. *Se HK é um subgrupo de G e H normaliza L, então* $[HK,L] = [H,L][K,L]$.

Demonstração. Os itens 1 a 6 são consequência direta da definição e podem ser facilmente checados abrindo cada comutador. Para o item 7, note que

$$\begin{aligned}[K,H] &= \langle [k,h] | k \in K, h \in H \rangle = \left\langle [h,k]^{-1} | k \in K, h \in H \right\rangle \\ &= \langle [h,k] | h \in H, k \in K \rangle = [H,K].\end{aligned}$$

O item 8 é óbvio e 9 é consequência de 4. Além disso, 10 é imediato de 9 quando consideramos σ como sendo o epimorfismo natural de G em G/N.

Resta então mostrar o item 11. É claro que $[H,L][K,L] \leq [HK,L]$. Para a inclusão inversa, vejamos primeiro que $[H,L][K,L]$ é um subgrupo. Note que para quaisquer $k \in K$ e $l,l' \in L$,

$$[k,l]^{l'} = [k,l][k,l,l'] = [k,l']^{-1}[k,ll'] \in [K,L],$$

pelo item 5. Então L normaliza $[K,L]$. Como H normaliza L, $[H,L]$ também normaliza $[K,L]$ e, em particular, $[H,L][K,L]$ é um subgrupo. Agora, para provar que $[HK,L]$ está contido nesse subgrupo, é suficiente notar que qualquer gerador $[hk,l]$ está nele. Como $[hk,l] = [h,l][h,l,k][k,l]$ e $[h,l,k] \in [H,L,K] \leq [L,K] = [K,L]$, o resultado segue. □

Um resultado importante com relação a comutadores é o lema dos três subgrupos:

Lema 1.1.2. *(Lema dos Três Subgrupos) Sejam* A,B,C *subgrupos e N um subgrupo normal de G. Se* $[[A,B],C] \leq N$ *e* $[[B,C],A] \leq N$, *então* $[[C,A],B] \leq N$.

O seguinte lema é consequência do Lema dos Três Subgrupos e precisaremos dele mais adiante.

Lema 1.1.3. *Dados quaisquer dois subgrupos normais* A,B *de um grupo arbitrário,* $[A,\gamma_s(B)] \leq [A,_s B]$*, para* $s \in \mathbb{N}$*.*

Demonstração. Provaremos por indução em s. O caso $s = 1$ é óbvio. Suponha então $s > 1$. Aplicando a hipótese de indução a $[B,A]$, ao invés de A, temos:

$$[[B,A],\gamma_{s-1}(B)] \leq [[B,A],_{s-1} B] = [[A,B],_{s-1} B] = [A,_s B].$$

Por hipótese de indução, também temos

$$[A,\gamma_{s-1}(B),B] \leq [[A,_{s-1} B],B] = [A,_s B].$$

E pelo Lema 1.1.2,

$$[A,\gamma_s(B)] = [\gamma_s(B),A] = [[\gamma_{s-1}(B),B],A] \leq [A,_s B].$$

$\square$

O subgrupo de G gerado pelos comutadores de elementos de G é o *subgrupo comutador* ou *subgrupo derivado* de G.

Como

$$[a,b]^x = [a^x,b^x],$$

para $N,M \lhd G$, $[N,M]$ é normal em G. Em particular, $[G,G] \lhd G$.

Tomando o subgrupo comutador do subgrupo comutador e assim por diante, temos uma cadeia decrescente de subgrupos normais

$$G \geq G' \geq G'' \geq \ldots,$$

chamada série derivada de G.

Um grupo G é *nilpotente* se possui uma série central normal:

$$1 \lhd G_1 \lhd \cdots \lhd G_n = G, \; com \; \frac{G_{i+1}}{G_i} \leq Z\left(\frac{G}{G_i}\right).$$

Podemos considerar a *série central inferior*:

$$\gamma_1(G) = G, \; \gamma_i(G) = [\gamma_{i-1}(G),G]$$

e dizemos que G é nilpotente se existe n tal que $\gamma_{n+1}(G) = 1$. Nesse caso, G é dito nilpotente de classe n.

Um grupo G é um *p-grupo finito* se $|G| = p^k$ para algum k.

Elencamos a seguir duas propriedades importantes de p-grupos finitos.

Teorema 1.1.4. *Seja G um p-grupo finito. Então G é nilpotente.*

Demonstração. Vamos mostrar primeiro que um grupo finito H é nilpotente se $Z(H/N) > 1$ para todo subgrupo próprio normal N de H, daí, será suficiente mostrar que $Z(G) \neq 1$.

Mostraremos por indução na ordem de G. Por hipótese, $1 < Z(G) = Z$. Indutivamente, $\gamma_m(G/Z) = 1$ para algum m. Então $\gamma_{m+1}(G) = 1$.

Mostraremos então que para G p-grupo finito, $Z(G) \neq 1$. Sejam $h_1, \ldots, h_r$ representantes das classes de conjugações de G que não estão em $Z(G)$. Daí, $|C_G(h_i)| = p^{e_i} > 1$. Logo

$$|Z(G)| = |G| - \sum_{i=1}^{r} |G : C_G(h_i)| \equiv 0 \ (mod\ p).$$

E como $Z(G) \geq 1$, segue que $Z(G) \geq p$. $\square$

Proposição 1.1.5. *Seja G um p-grupo finito. Então todo subgrupo próprio maximal de G é normal e tem índice p em G.*

Demonstração. Seja M um subgrupo próprio maximal de G. Pelo Teorema 1.1.4, $Z(G)$ contém um elemento z de ordem p. Se $z \in M$, $M/\langle z \rangle$ é um subgrupo próprio maximal de $G/\langle z \rangle$ e argumentamos por indução. Se $z \notin M$, então $M\langle z \rangle = G$. Nesse caso, $M \lhd G$ e $|G : M| = p$. $\square$

Chamamos de *coclasse* de um p-grupo finito G de ordem $p^n \geq p^2$ o número $n - c$, onde c é a classe de nilpotência de G. E um grupo G de ordem p^n, é um *grupo de classe maximal* se sua classe de nilpotênca é $n - 1$.

O *subgrupo de Frattini* $\Phi(G)$ de um p-grupo finito G é a interseção de todos os subgrupos maximais de G ou o próprio G se não há subgrupo maximal.

Podemos descrever o subgrupo de Frattini de um p-grupo da seguinte maneira:

Teorema 1.1.6. *Seja G um p-grupo finito. Então $\Phi(G) = G^p[G,G]$.*

Demonstração. $G/G^p[G,G]$ é um p-grupo abeliano elementar, então seus subgrupos maximais próprios intersectam na identidade. Então $\Phi(G) \leq G^p[G,G]$. A inclusão inversa segue da proposição anterior. $\square$

1.2 Grupos Profinitos

Os resultados de Grupos Profinitos se baseiam principalmente nos livros *Analytic Pro-p Groups* [1] e *Profinite Groups* [13].

Um conjunto I é um *conjunto ordenado* com respeito à relação $\leq$ se $\leq$ é reflexiva, transitiva e dados $i, j \in I$, existe $t \in I$ tal que $i \leq t$ e $j \leq t$.

Um *espaço topológico* X é um conjunto associado a uma *topologia*, uma coleção $\mathcal{T}$ de subconjuntos de X tais que a união e a interseção finita de elementos de $\mathcal{T}$ pertencem a $\mathcal{T}$. Tais elementos são chamados de *abertos*.

Um *sistema inverso* de espaços topológicos X_i sobre o conjunto ordenado I, (X_i, φ_{ji}, I), ou apenas X_i, é tal que para todos $i \leq j, \varphi_{ji} : X_j \to X_i$ é um morfismo, φ_{ii} é a identidade em X_i e para $i \leq j \leq k$, $\varphi_{kj}\varphi ji = \varphi_{ki}$. Seu limite inverso é

$$X = \varprojlim X_i = \left\{(x_i) \in \prod X_i \mid \varphi_{ji}(x_j) = x_i \text{ para } i \leq j\right\}.$$

com as projeções $\varphi_i : X \to X_i$. Se os morfismos φ_{ji} forem sobrejetivos, então X é dito limite projetivo.

Definição 1.2.1. *Um grupo profinito G é um limite inverso de grupos finitos. No caso em que G é um limite inverso de p-grupos finitos, G é dito grupo pro-p.*

Um exemplo natural de grupo profinito é o *completamento profinito* de um grupo G, o grupo $\hat{G} = \varprojlim G/N$, onde G/N percorre todos os grupos quocientes finitos de G.

Exemplo 1.2.2. *Considere o grupo dos inteiros $\mathbb{Z}$. Seu completamento profinito é*

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

E seu completamento pro-p é

$$\mathbb{Z}_p = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

Exemplo 1.2.3. *O grupo das matrizes unitriangulares superiores com entradas em $\mathbb{Z}_p$ de ordem n*

$$UT_n(\mathbb{Z}_p) = \left\{ \left(\begin{array}{ccccc} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ 0 & 0 & 1 & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array} \right) \middle| \, a_{ij} \in \mathbb{Z}_p \right\}$$

é um grupo pro-p.

Um outro modo de definir Grupos Profinitos e o que mais usaremos no decorrer desse trabalho é topologicamente.

Para isso, elencamos algumas definições necessárias.

Dado um ponto $x \in X$, uma *vizinhança* de x é um subconjunto aberto de X que contém x. Um *sistema fundamental de vizinhanças de um ponto* x é um conjunto $\mathcal{S}$ de vizinhanças V de x tais que para cada V, existe W em $\mathcal{S}$ tal que $W \subseteq V$. O complemento de um subconjunto aberto em X é um *subconjunto fechado*. Chamamos de *fecho* de um subconjunto o menor subconjunto fechado que o contém e escrevemos $\overline{H}$ para $H \subseteq X$. Um subconjunto de X cujo fecho é X é dito *denso*.

Seja X um espaço topológico. A *topologia discreta* em X é definida colocando todos os subconjuntos de X como abertos. A *topologia subespaço* em um subconjunto $Y \subseteq X$ é definida colocando todas as interseções $Y \cap A$ com $A \subseteq_a X$ como abertos. A *topologia quociente* em $Y := X/\sim$ com respeito à relação de equivalência $\sim$ é definida colocando um subconjunto $B \subseteq Y$ aberto se sua pré-imagem em X pela projeção natural é aberta. Se $\{X_i\}_{i \in I}$ é uma família de espaços topológicos, então a *topologia produto* no produto cartesiano $X := \prod_{i \in I} X_i$ é definida colocando um subconjunto de X como aberto se é a união de subconjuntos abertos da forma $\prod_{i \in I} U_i$, onde $U_i = X_i$ para a maioria dos $i \in I$ e $U_i \subseteq_a X_i$ para todo $i \in I$.

Um espaço topológico X é dito:

- *Hausdorff*, se quaisquer dois pontos distintos de X possuem vizinhanças disjuntas.
- *Compacto*, se para toda família infinita de abertos cobrindo X existe uma subfamília finita que cobre X.
- *Conexo*, se não é a união de dois subconjuntos abertos disjuntos não-vazios. Chamamos de *componentes conexas* os subconjuntos conexos maximais de X.
- *Totalmente desconexo*, se toda componente conexa contém apenas um ponto.

Um *grupo topológico* é um grupo G com uma topologia que satisfaz os seguintes axiomas:

1. a função $(x, y) \mapsto xy$ de $G \times G$ em G é contínua.
2. a função $x \mapsto x^{-1}$ de G em G é contínua.

Um subconjunto X de um grupo topológico G *gera* G *topologicamente* se $G = \overline{\langle X \rangle}$. O grupo topológico G é *finitamente gerado* se é gerado topologicamente por $X \subseteq G$, onde X é finito e denominamos o *número de geradores* de G por $d(G)$.

Podemos agora definir topologicamente um grupo profinito usando o seguinte resultado cuja demonstração pode ser encontrada no Teorema 2.1.3 de [13]:

Teorema 1.2.4. *Para um grupo topológico G, são equivalentes:*

1. *G é um grupo profinito.*

2. *G é Hausdorff, compacto e totalmente desconexo.*

3. *G é compacto e a identidade 1 admite um sistema fundamental $\mathcal{U}$ de vizinhanças abertas U com interseção trivial e cada U é normal em G.*

4. *A identidade 1 de G admite um sistema fundamental $\mathcal{U}$ de vizinhanças abertas U tais que cada U é normal em G e $G = \varprojlim_{U \in \mathcal{U}} G/U$.*

Para definir grupos pro-p topologicamente, basta adicionar aos itens 2, 3 e 4 do teorema anterior a hipótese de que para cada subgrupo aberto normal U de G, G/U é p-grupo.

Assim,

Definição 1.2.5. *Um grupo profinito no qual todo subgrupo aberto normal tem índice igual a alguma potência de p, p primo, é chamado grupo pro-p.*

Usaremos as notações $H \leq_a G$, $H \lhd_a G$ e $H \subseteq_a G$ (respectivamente, $H \leq_f G$, $H \lhd_f G$ e $H \subseteq_f G$) para indicar que H é um subgrupo aberto de G, um subgrupo aberto normal de G e um subconjunto aberto de G (respectivamente, subgrupo fechado de G, subgrupo fechado normal de G e subconjunto fechado de G).

Elencamos algumas propriedades de grupos profinitos na proposições abaixo (Proposições 1.2 de [1] e 2.1.4 e 2.1.5 de [13]):

Proposição 1.2.6. *Seja G um grupo profinito.*

1. *Todo subgrupo aberto de G é fechado, tem índice finito em G e contém um subgrupo aberto normal de G. Um subgrupo fechado de G é aberto se, e somente se, tem índice finito. A família de todos os subgrupos abertos de G intersecta em $\{1\}$.*

2. *Um subconjunto de G é aberto se, e somente se, é a união de classes laterais de subgrupos abertos normais.*

3. *Para qualquer subconjunto X de G,*

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

Se X é um subgrupo de G, então

$$\overline{X} = \cap \{K | X \leq K \leq_a G\}.$$

4. *Se X e Y são subconjuntos fechados de G, então o conjunto $XY = \{xy | x \in X, y \in Y\}$ também é. Se X é fechado e n é um inteiro, então o conjunto $\{x^n | x \in X\}$ é fechado.*

5. *Seja H um subgrupo fechado de G. Então H é um grupo profinito. Todo subgrupo aberto de H é da forma $H \cap K$ com $K \leq_a G$.*

6. *Seja N um subgrupo fechado normal de G. Então G/N é um grupo profinito e o homomorfismo natural $G \to G/N$ é uma função contínua fechada e aberta.*

7. *A sequência (g_i) em G converge se, e somente se, é uma sequência de Cauchy: isto é, para cada $N \lhd_a G$, existe $n = n(N)$ tal que $g_i^{-1} g_j \in N$ para todos $i \geq n$ e $j \geq n$.*

Dizemos que uma coleção $\mathcal{S}$ de subconjuntos de um grupo G é filtrada por baixo se para todo par de subconjuntos $S_1, S_2 \in \mathcal{S}$, existe algum $S_3 \in \mathcal{S}$ tal que $S_3 \leq S_1 \cap S_2$.

Proposição 1.2.7. *Seja H um subgrupo fechado de um grupo profinito G.*

1. *Se $\{U_i | i \in I\}$ é uma família de subconjuntos fechados de G filtrada por baixo, então*

$$\bigcap_{i \in I} HU_i = H(\bigcap_{i \in I} U_i).$$

2. *Seja $\varphi : G \to R$ um epimorfismo de grupos profinitos. Suponha que $\{U_i | i \in I\}$ seja uma família de subconjuntos fechados de G filtrada por baixo. Então*

$$\varphi(\bigcap_{i \in I} U_i) = \bigcap_{i \in I} \varphi(U_i).$$

3. *Todo subgrupo aberto de G que contenha H, contém um subgrupo aberto da forma HU para algum subgrupo aberto normal U de G.*

4. *H é a interseção de todos os subgrupos abertos de G que contêm H. Se H é normal em G, então H é a interseção de todos os subgrupos abertos normais de G que contêm H.*

Demonstração. 1. Pela suposição de *filtration*, o resultado é claramente verdade se o conjunto I for finito. Para o caso geral, é certo que $\bigcap_{i \in I} HU_i \geq H \bigcap_{i \in I} U_i$. Seja $x \in \bigcap_{i \in I} HU_i$ e seja $\{J_t | t \in T\}$ a coleção de todos os subconjuntos finitos J_t de I tais que

$\left\{U_j | j \in J_t\right\}$ é filtrada por baixo. Então, para cada $t \in T$, $x \in \bigcap_{j\in J_t} HU_j = H \bigcap_{j\in J_t} U_j$ e então, $Hx \cap (\bigcap_{j\in J_t} U_j) \neq \emptyset$. Logo, pela propriedade de interseção finita do espaço compacto G, temos

$$Hx \cap (\bigcap_{i\in I} U_i) = \bigcap_{t\in T} (Hx \cap (\bigcap_{j\in J_t} U_j)) \neq \emptyset.$$

Assim, $x \in H(\bigcap_{i\in I} U_i)$, como queríamos.

2. Seja $H = Ker(\varphi)$ e identifique R com G/H. Então, usando a parte 1,

$$\bigcap_{i\in I} \varphi(U_i) = \bigcap_{i\in I} (U_i H/H) = (\bigcap_{i\in I} U_i H)/H = (\bigcap_{i\in I} U_i)H/H = \varphi(\bigcap_{i\in I} U_i).$$

3. Seja V um subgrupo aberto de G que contém H. Então seu core

$$V_G = \bigcap_{g\in G} V^g$$

é aberto e normal; além disso, $HV_G \leq V$.

4. Segue das partes 1 e 3 tomando $\{U_i | i \in I\}$ em 1 como sendo a coleção de todos os subgrupos abertos normais de G.

$\square$

Proposição 1.2.8. *1. Seja $\{H_i | i \in I\}$ uma coleção de subgrupos fechados de um grupo profinito G e seja $\bigcap_{i\in I} H_i \leq U \leq_a G$. Então existe um subconjunto finito J de I tal que $\bigcap_{j\in J} H_j \leq U$.*

2. Seja $\{U_i | i \in I\}$ uma coleção de subgrupos abertos de um grupo profinito G tal que $\underset{i\in I}{U_i} = 1$. Seja

$$\mathcal{V} = \left\{ \bigcap_{j\in J} U_j | J \text{ é um subconjunto finito de } I \right\}.$$

Então $\mathcal{V}$ é um sistema fundamental de vizinhanças de 1 em G.

Demonstração. A parte 2 segue imediatamente de 1. Para provar 1, considere a cobertura aberta $\{G - H_i | i \in I\}$ do espaço compacto $G - U$. Escolha uma subcobertura finita, digamos $\left\{G - H_j | j \in J\right\}$. Então $G - U \subseteq \bigcup_{j\in J} (G - H_j)$. Logo, $\bigcap_{j\in J} H_j \subseteq U$. $\square$

Como o subgrupo de Frattini é um subgrupo muito importante, elencamos alguns resultados sobre esse subgrupo para grupos profinitos.

Definição 1.2.9. *Seja G um grupo profinito. O subgrupo de Frattini de G é*

$$\Phi(G) = \bigcap \{M \mid M \text{ é um subgrupo aberto maximal próprio de } G\}.$$

Proposição 1.2.10. *Para G um grupo profinito, temos:*

1. $\Phi(G) \triangleleft_f G$.
2. *Se $K \triangleleft_f G$ e $K \leq \Phi(G)$, então $\Phi(G/K) = \Phi(G)/K$.*
3. *Dado $X \subseteq G$, são equivalentes:*
   (a) *X gera G topologicamente.*
   (b) *$X \cup \Phi(G)$ gera G topologicamente.*
   (c) *$X\Phi(G)/\Phi(G)$ gera $G/\Phi(G)$ topologicamente.*

Demonstração. Os itens 1 e 2 seguem da definição de $\Phi(G)$. Em 3, é fácil ver que (a) $\Rightarrow$ (b) $\Rightarrow$ (c). Resta mostrar (c) $\Rightarrow$ (a). Suponha então que (c) valha e seja $K \leq_a G$ com $X \subseteq K$. Se $K \neq G$, então $K \leq M$ para algum subgrupo próprio maximal aberto de M de G e então

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

o que contradiz (c). Logo, $K = G$ e o resultado segue pelo fato de que para qualquer subconjunto X de G, $\overline{X} = \cap\{K \mid X \leq K \leq_a G\}$. $\square$

Proposição 1.2.11. *Dado G um grupo pro-p, temos $\Phi(G) = \overline{G^p[G,G]}$, onde $[G,G]$ é o subgrupo derivado de G e $G^p = \langle g^p \mid g \in G \rangle$.*

Demonstração. Em um p-grupo finito, todo subgrupo próprio maximal é normal e tem índice p. Assim, se M é um subgrupo aberto próprio maximal de G, conseguimos $N \triangleleft_a G$ com $N \leq M$. Observe que M/N é um subgrupo maximal do p-grupo finito G/N e concluímos que $M \triangleleft G$ e $|G : M| = p$. Segue daí que $G^p[G,G] \leq M$. O que nos dá

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

e como $\Phi(G)$ é fechado, $\Phi(G) \geq \overline{G^p[G,G]}$.

Consideremos então o grupo $Q = G/\overline{G^p[G,G]}$. Esse é um grupo pro-$p$, então a interseção de seus subgrupos abertos normais é a identidade. Se $N \triangleleft_a Q$ então Q/N é um p-grupo finito abeliano elementar e então $\Phi(Q/N) = 1$. Logo $\Phi(Q) \leq \bigcap_{N \lhd_a Q} N = 1$ e segue pela Proposição 1.2.10, item 2, que

$$\Phi(G)/\overline{G^p[G,G]} = \Phi(Q) = 1.$$

□

Teorema 1.2.12. *Seja G um grupo pro-p. Então G é finitamente gerado se, e somente se, $\Phi(G)$ é aberto em G.*

Demonstração. Se $\Phi(G)$ é aberto, então $G/\Phi(G)$ é finito. Então existe $X \subseteq G$ finito tal que $G = X\Phi(G)$ e então X gera G topologicamente pela Proposição 1.2.10.

Para a implicação contrária, suponha $G = \overline{\langle X \rangle}$, com $|X| = d$ finito. Se $\Phi(G) \leq N \lhd_a G$ então G/N é um p-grupo abeliano elementar pela Proposição 1.2.11 e pode ser gerado por d elementos. Daí, $|G : N| = p^d$. Dentre esses subgrupos, escolha N_0 de modo que seu índice em G seja o maior possível. Então $N_0 \leq N$ sempre que $\Phi(G) \leq N \lhd_a G$. Como $\Phi(G) \lhd_f G$, segue que

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

Logo $\Phi(G)$ é aberto em G. □

Agora introduzimos uma importante série de subgrupos (topologicamente) característicos (um subgrupo de G é topologicamente característico se é invariante por automorfismos contínuos de G), a *p-série inferior*:

Definição 1.2.13. *Seja G um grupo pro-p. Definimos $P_1(G) = G$ e para $i \geq 1$,*

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

Para simplificar a notação, em alguns momentos usaremos

$$G_i = P_i(G).$$

Pela Proposição 1.2.11, $P_2(G) = \Phi(G)$. Note que $P_{i+1}(G) \geq \Phi(P_i(G))$ para cada i.

Proposição 1.2.14. *Seja G um grupo pro-p.*

1. *$P_i(G/K) = P_i(G)K/K$ para todo $K \lhd_f G$ e todo i.*
2. *$[P_i(G), P_j(G)] \leq P_{i+j}(G)$ para todos i e j.*
3. *Se G é finitamente gerado, então $P_i(G)$ é aberto em G para cada i e o conjunto $\{P_i(G) \mid i \geq 1\}$ é uma base para as vizinhanças de 1 em G.*

Demonstração. Escreva $G_i = P_i(G)$ para cada i.

1. Seja $K \lhd_f G$. Então $(P_i(G/K))$ é a série decrescente de subgrupos fechados normais de G/K mais rápida tal que cada fator é central e de expoente divisor de p. Como (G_iK/K) é uma série com essas propriedades, segue que $P_i(G/K) \leq G_iK/K$ para todo i. Agora suponha que para algum n, $P_n(G/K) = G_nK/K$. Escreva $M/K = P_{n+1}(G/K)$. Então M é fechado em G e $M \geq G_n^p[G_n, G]K$, daí $M \geq G_{n+1}K$. Logo $M = G_{n+1}K$ e o resultado segue por indução.

2. Certamente $[G_i, G_1] \leq G_{i+1}$ para todo i. Seja $n \geq 2$ e suponha indutivamente que $[G_i, G_{n-1}] \leq G_{i+n-1}$ para todo i. Agora fixamos $m \geq 1$ e queremos mostrar que $[G_m, G_n] \leq G_{m+n}$. Como G_{m+n} é fechado, é suficiente mostrar que $[G_m, G_n] \leq N$ sempre que $G_{m+n} \leq N \lhd_a G$. Então, pelo item 1, podemos substituir G pelo p-grupo G/N e supor mais ainda que $G_{m+n} = 1$. Então $[G_m, G_{n-1}] \leq G_{m+n-1}$ é central e tem expoente divisor de p. Se $g \in G_m$ e $x \in G_{n-1}$, temos

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

então $[G_m, G_{n-1}^p] = 1$. Além disso,

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

pelo Lema dos Três Subgrupos e pela hipótese de indução. Segue que

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

Como G é finito, isso é o mesmo que $[G_m, G_n] = 1$, que é o que queríamos demonstrar.

3. Agora suponha que G seja finitamente gerado. Obviamente, $G_1 = G$ é finitamente gerado e aberto em G. Seja $n \geq 1$ e suponha indutivamente que G_n é finitamente gerado e aberto em G. Então a Proposição 1.2.12 diz que $\Phi(G_n)$ é aberto em G_n. Como $\Phi(G_n) \leq G_{n+1} \leq G_n$, segue que G_{n+1} é abeto em G_n, portanto, também é aberto em G e então G_{n+1} é finitamente gerado. A primeira afirmação segue por indução.

   Para mostrar que $\{G_i | i \geq 1\}$ é uma base de vizinhanças de 1 em G, é suficiente mostrar que todo subgrupo aberto normal de G contém G_i para algum i. Isso segue do item 1, já que se $N \lhd_a G$, então G/N é um p-grupo finito e então $P_i(G/N) = 1$ para todos i suficientemente grande.

□

1.3 Fórmula de P. Hall e Aplicações

Aqui elencamos algumas fórmulas que relacionam comutadores com potências de subgrupos normais de p-grupos finitos (ou, equivalentemente, de subgrupos fechados normais de grupos pro-p, como usaremos no terceiro capítulo). Todas essas fórmulas são consequência da fórmula de Philip Hall, enunciada abaixo. Se F é um grupo livre livremente gerado por dois símbolos x e y, a fórmula de Hall afirma que existem palavras $c_i(x,y) \in \gamma_i(F)$ tais que

$$(xy)^n = x^n y^n c_2(x,y)^{\binom{n}{2}} c_3(x,y)^{\binom{n}{3}} \ldots c_{n-1}(x,y)^{\binom{n}{n-1}} c_n(x,y) \tag{1.1}$$

para todo $n \in \mathbb{N}$. Segue que essa fórmula vale em geral para todos os elementos x,y de qualquer grupo G, com todo $c_i(x,y)$ em $\gamma_i(\langle x,y\rangle)$. Como o coeficiente binomial $\binom{p^k}{i}$ é divisível por p^{k-j} para $p^j \leq i \leq p^{j+1}$, temos o seguinte resultado.

Teorema 1.3.1. *Sejam G um grupo e x,y elementos de G. Então:*

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} \pmod{\gamma_2(L)^{p^n} \gamma_p(L)^{p^{n-1}} \gamma_{p^2}(L)^{p^{n-2}} \gamma_{p^3}(L)^{p^{n-3}} \ldots \gamma_{p^n}(L)} \tag{1.2}$$

onde $L = \langle x,y\rangle$, e

$$[x,y]^{p^n} \equiv [x^{p^n}, y] \pmod{\gamma_2(M)^{p^n} \gamma_p(M)^{p^{n-1}} \gamma_{p^2}(M)^{p^{n-2}} \ldots \gamma_{p^n}(M)} \tag{1.3}$$

onde $M = \langle x, [x,y]\rangle$.

Demonstração. Basta notar que 1.3 é consequência de 1.2, pois $[x,y] = x^{-1}x^y$. □

Corolário 1.3.2. *Sejam G um grupo e $x_1, x_2, \ldots, x_k$ elementos de G. Então*

$$(x_1 \ldots x_k)^{p^n} \equiv x_1^{p^n} \ldots x_k^{p^n} \pmod{\gamma_2(L)^{p^n} \gamma_p(L)^{p^{n-1}} \gamma_{p^2}(L)^{p^{n-2}} \ldots \gamma_{p^n}(L)}$$

onde $L = \langle x_1, \ldots, x_k\rangle$. Em particular, temos

$$\Omega_i^{p^n} \leq \Omega_{i-k} \gamma_2(\Omega_1)^{p^n} \gamma_p(\Omega_i)^{p^{n-1}} \gamma_{p^2}(\Omega_i)^{p^{n-2}} \ldots \gamma_{p^n}(\Omega_i),$$

onde $\Omega_l = \Omega_l(G)$ para $l \geq 1$ e $\Omega_l = \{1\}$ para $l \leq 0$ e $\Omega_i(G) = \left\langle g \in G \mid g^{p^i} = 1 \right\rangle$.

Demonstração. A demonstração é por indução em k. O caso $k = 2$ é dado pelo teorema anterior. Suponha que o resultado valha para $k > 2$ e vamos provar que então vale também para $k+1$. Note que podemos reescrever o produto $(x_1 \dots x_k x_{k+1})^{p^n}$ como $(xx_3 \dots x_{k+1})^{p^n}$, onde $x = x_1x_2$. Daí, pela hipótese de indução,

$$(xx_3 \dots x_{k+1})^{p^n} \equiv (x_1x_2)^{p^n} x_3^{p^n} \dots x_{k+1}^{p^n} \ (mod\ \gamma_2(L')^{p^n} \gamma_p(L')^{p^{n-1}} \gamma_{p^2}(L')^{p^{n-2}} \dots \gamma_{p^n}(L'))$$

onde $L' = \langle x, x_3, \dots, x_{k+1} \rangle = \langle x_1x_2, x_3, \dots, x_{k+1} \rangle$.

Como $L' \leq L = \langle x_1, x_2, \dots, x_k \rangle$ e

$$(x_1x_2)^{p^n} \equiv x_1^{p^n} x_2^{p^n} \ \ (mod\ \gamma_2(M)^{p^n} \gamma_p(M)^{p^{n-1}} \gamma_{p^2}(M)^{p^{n-2}} \gamma_{p^3}(M)^{p^{n-3}} \dots \gamma_{p^n}(M)),$$

onde $M = \langle x_1, x_2 \rangle$, temos o que queríamos. □

Lema 1.3.3. *Sejam G um p-grupo finito e N e M subgrupos normais de G. Se $N \leq M[N,G]$, então $N \leq M$.*

Demonstração. Aplicando a inclusão várias vezes, obtemos $N \leq M[N,_k G]$. E como p-grupos finitos são nilpotentes, temos que $[N,_k G] \leq [G,_k G] = 1$ para algum k, e então $N \leq M$. □

Teorema 1.3.4. *Seja G um grupo pro-p. Se $G = \langle X \rangle$, então, para todo $k \geq 0$,*

$$G^{p^k} \equiv \left\langle x^{p^k} \mid x \in X \right\rangle \ (mod\ \gamma_2(G)^{p^k} \gamma_p(G)^{p^{k-1}} \dots \gamma_{p^k}(G)).$$

Demonstração. Se $x_1, \dots, x_r \in X$, basta mostrar que $(x_1 \dots x_r)^{p^k}$ e $x_1^{p^k} \dots x_r^{p^k}$ são congruentes com respeito ao módulo do teorema. E isso segue imediatamente por indução em r usando a fórmula 1.2. □

Usaremos o símbolo $[H,_k K]$ para indicar o subgrupo comutador $[H, K, \dots, K]$, onde K aparece k vezes.

Teorema 1.3.5. *Sejam G um grupo pro-p e N e M subgrupos fechados normais de G. Então*

$$[N^{p^k}, M] \equiv [N, M]^{p^k} \ \ (mod\ [M,_p N]^{p^{k-1}} [M,_{p^2} N]^{p^{k-2}} \dots [M,_{p^k} N]).$$

Demonstração. Pela fórmula 1.3, para todo $n \in N$ e $m \in M$, temos

$$[n^{p^k}, m] \in [N, M]^{p^k} [M,_p N]^{p^{k-1}} [M,_{p^2} N]^{p^{k-2}} \dots [M,_{p^k} N],$$

ou seja, $[N^{p^k}, M]$ está contido nesse produto de subgrupos. Para provar a outra inclusão, usaremos indução na ordem de N. Como $[N, M]$ é gerado pelos comutadores $[n, m]$ com

$n \in N$ e $m \in M$, combinando o Teorema 1.3.4 e a equação 1.3, temos

$$[N,M]^{p^k} \leq [N^{p^k},M][M,N,N]^{p^k}[M,_p N]^{p^{k-1}} \dots [M,_{p^k} N].$$

Pela hipótese de indução,

$$\begin{aligned}[M,N,N]^{p^k} &\leq [[M,N]^{p^k},N] \prod_{r=1}^{k} [N,_{p^r}[M,N]]^{p^{k-r}} \\ &\leq [[M,N]^{p^k},N] \prod_{r=1}^{k} [M,_{p^r} N]^{p^{k-r}}.\end{aligned}$$

Consequentemente,

$$[N,M]^{p^k} \leq [N^{p^k},M][[N,M]^{p^k},N] \prod_{r=1}^{k} [M,_{p^r} N]^{p^{k-r}}.$$

e o resultado segue do Lema 1.3.3. □

Para comutadores de comprimento arbitrário, as fórmulas ficam cada vez mais complicadas e é mais fácil tomar um dos subgrupos como sendo o grupo todo. Para isso, temos as duas congruências do teorema a seguir.

Teorema 1.3.6. *Sejam G um grupo pro-p e N um subgrupo fechado normal de G. Então as congruências seguintes valem para todo $k,l \geq 0$:*

1. $[N^{p^k},_l G] \equiv [N,_l G]^{p^k} \pmod{\prod_{r=1}^{k} [N,_{p^r+l-1} G]^{p^{k-r}}}$.

2. $[N^{p^k},_l G] \equiv [N,_l G]^{p^k} \pmod{\prod_{r=1}^{k} [N^{p^{k-r}},_{r(p-1)+l} G]}$.

Demonstração. 1. Provaremos por indução em l. O caso $l = 0$ é trivial. Suponhamos então $l \geq 1$. Seja $T = \prod_{r=1}^{k} [N,_{p^r+l-1} G]^{p^{k-r}}$. Pela hipótese de indução, $[N^{p^k},_{l-1} G] \equiv [N,_{l-1} G]^{p^k} \pmod{U}$, onde $U = \prod_{r=1}^{k} [N,_{p^r+l-2} G]^{p^{k-r}}$ e consequentemente $[N^{p^k},_l G] \equiv [[N,_{l-1} G]^{p^k}, G] \pmod{[U,G]}$. Por outro lado, aplicando o Teorema 1.3.5, obtemos que $[[N,_{l-1} G]^{p^k}, G] \equiv [N,_l G]^{p^k} \pmod{T}$. Então é suficiente mostrar que $[U,G] \leq T$. Para isso, considere um fator geral $[[N,_{p^r+l-2} G]^{p^{k-r}}, G]$ em $[U,G]$. Novamente pelo

Teorema 1.3.5, temos

$$\begin{aligned}[][N,_{p^r+l-2}G]^{p^{k-r}},G] &\leq \prod_{s=0}^{k-r}[G,_{p^s}[N,p^r+l-2G]]^{p^{k-r-s}}\\ &= \prod_{s=0}^{k-r}[[N,p^r+l-1G],_{p^s-1}[N,p^r+l-2G]]^{p^{k-r-s}}\\ &\leq \prod_{s=0}^{k-r}[[N,p^r+l-1G],_{p^s-1}\gamma_{p^r+l-1}(G)]^{p^{k-r-s}}.\end{aligned}$$

Como $[K,\gamma i(G)][K,_i G]$ para $K \lhd G$, segue que

$$[[N,p^r+l-1G],_{p^s-1}\gamma_{p^r+l-1}(G)]^{p^{k-r-s}} \leq [N,p^s(p^r+l-1)G] \leq [N,p^{r+s}+l-1G].$$

Logo, $[[N,_{p^r+l-2}G]^{p^{k-r}},G] \leq T$, como queríamos demonstrar.

2. Usaremos indução em k. Seja $V = \prod_{r=1}^{k}[N^{p^{k-r}},_{r(p-1)+l}G]$. Por 1., basta mostrar que $T \leq V$. Para $1 \leq r \leq k$, a hipótese de indução nos dá que

$$[N,_{p^r+l-1}G]^{p^{k-r}} \equiv [N^{p^{k-r}},_{p^r+l-1}G] \ \ (mod \prod_{s=1}^{k-r}[N^{p^{k-r-s}},_{s(p-1)+p^r+l-1}G]).$$

Como $s(p-1)+p^r+l-1 \geq (r+s)(p-1)+l$, segue que $[N,_{p^r+l-1}G]^{p^{k-r}} \leq V$. Daí, $T \leq V$, como desejado.

□

Capítulo 2

Grupos Pro-p p-Ádicos Analíticos e Grupos Uniformemente Powerful

Em 1965, Lazard provou que um grupo topológico é p-ádico analítico se, e somente se, ele tiver um subgrupo aberto p-saturável. Alguns anos mais tarde, Lubotzky e Mann provam que é possível mudar a hipótese de Lazard, mostrando que podemos substituir a existência de um subgrupo aberto p-saturável pela existência de um subgrupo aberto uniformemente *powerful*. Essas duas definições, grupos p-saturáveis e grupo uniformemente powerful, não são equivalentes. O que encontramos é que os grupos uniformemente *powerful* formam uma subfamília dos grupos p-saturáveis.

Dadas essas relações, apresentamos as definições e alguns resultados acerca dos grupos citados.

2.1 Grupos Pro-p p-Ádicos Analíticos

Primeiramente daremos uma ideia da construção dos grupos $\mathbb{Q}_p$ e $\mathbb{Z}_p$.

A maneira tradicional de descrever o tamanho de um número racional é usando valores absolutos. Um *valor absoluto* em um corpo K é uma função com valores reais $|\cdot| : K \to [0, \infty)$ que satisfaz:

1. $|x| = 0$ se, e somente se, $x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. $|x + y| \leq |x| + |y|$.

Um valor absoluto pode ser *não-arquimediano* ou *arquimediano* se satisfizer ou não a seguinte condição, chamada de desigualdade triangular forte:

3'. $|x+y| \leq max\{|x|,|y|\}$.

Podemos restringir o valor absoluto usual em $\mathbb{R}$, dado por $|x|_\infty = max\{x,-x\}$, a um valor absoluto arquimediano em $\mathbb{Q}$.

Adicionalmente, existem infinitos valores absolutos não-arquimedianos em $\mathbb{Q}$, um para cada p primo. Podemos escrever unicamente cada número racional $x \neq 0$ como

$$x = p^n \cdot \frac{a}{b}$$

com $n,a,b \in \mathbb{Z},\ b > 0,\ mdc(a,b) = 1$ e $p \nmid ab$.

Definimos:

$$v_p(x) := n,\ |x|_p := p^{-n}.$$

Colocando $v_p(0) := \infty$ e $|0|_p := 0$, obtemos o *valor absoluto p-ádico* $|\cdot|_p$ em $\mathbb{Q}$ e a função $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, chamada de *valoração p-ádica* em $\mathbb{Q}$.

O corpo $\mathbb{R}$ dos números reais pode ser entendido como o completamento de $\mathbb{Q}$ com respeito à métrica $d_\infty = |x-y|_\infty$ induzida pelo valor absoluto arquimediano usual. Formalmente, podemos construir $\mathbb{R}$ adicionando a $\mathbb{Q}$ todos os limites de sequências de Cauchy com respeito a d_∞ não pertencentes a $\mathbb{Q}$. Todo elemento $\alpha \in \mathbb{R}$ é o limite de uma sequência de Cauchy $\alpha = \lim\limits_{n\to\infty} x_n$ com $x_n \in \mathbb{Q}$ e o valor absoluto estende para $\mathbb{R}$ por $|\alpha|_\infty = \lim\limits_{n\to\infty} |x_n|_\infty$.

Usando a notação decimal usual, podemos pensar em um número real α como o limite de uma sequência de Cauchy particular da forma

$$\alpha = \lim_{n\to\infty} x_n,\ \ x_n = \lfloor \alpha \rfloor + \sum_{k=1}^{n} a_k \cdot 10^{-k},$$

onde $\lfloor \alpha \rfloor$ denota a parte inteira de α e $a_k \in \{0,1,\ldots,9\}$.

Similarmente, podemos formar, para cada primo p, o completamento $\mathbb{Q}_p$ de $\mathbb{Q}$ com respeito à métrica $d_p(x,y) = |x-y|_p$ induzida pelo valor absoluto p-ádico. Nesse caso, deve-se adicionar todos os limites de sequências de Cauchy com respeito a d_p. Todo elemento $\alpha \in \mathbb{Q}_p$ é o limite de uma sequência de Cauchy $\alpha = \lim\limits_{n\to\infty} x_n$ com $x_n \in \mathbb{Q}$ e o valor absoluto é estendido para $\mathbb{Q}_p$ colocando $|\alpha|_p = \lim\limits_{n\to\infty} |x_n|_p$. Da mesma maneira estendemos para $\mathbb{Q}_p$ a função valoração v_p e as operações de anel, adição e multiplicação. $\mathbb{Q}_p$ é então um corpo com valor absoluto $|\cdot|_p$. Os elementos de $\mathbb{Q}_p$ são chamados de *números p-ádicos*.

Uma notação conveniente para cálculos com números p-ádicos é a seguinte. Todo $\alpha \in \mathbb{Q}_p$ pode ser escrito como a série

$$\alpha = \sum_{k\in\mathbb{Z}} a_k p^k = \sum_{k=v_p(\alpha)}^{\infty} a_k p^k,$$

onde os coeficientes a_k são tomados do conjunto $R_p := \{0, 1, \ldots, p-1\}$, $a_k = 0$ para $k < v_p(\alpha)$ e $a_{v_p(\alpha)} \neq 0$ se $\alpha \neq 0$. Note que ao invés de R_p, poderíamos usar qualquer conjunto de representantes de $\mathbb{Z}$ módulo $p\mathbb{Z}$.

O valor absoluto p-ádico induz assim uma métrica e portanto uma topologia em $\mathbb{Q}_p$. É uma característica inerente do processo de completamento que as operações de corpo são contínuas. Enquanto espaço topológico, $\mathbb{Q}_p$ é Hausdorff, localmente compacto e totalmente desconexo.

A desigualdade triangular forte implica que o conjunto aberto compacto

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in R_p \right\}$$

forma um subanel de $\mathbb{Q}_p$. Este é o fecho topológico dos inteiros $\mathbb{Z}$ em $\mathbb{Q}_p$ e seus elementos são chamados *inteiros p-ádicos*.

Quanto à estrutura do anel dos inteiros p-ádicos, temos que seu grupo de unidades é dado por

$$\mathbb{Z}_p^* = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p = 1\} = \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in R_p,\ a_0 \neq 0 \right\}.$$

Além disso, os ideais de $\mathbb{Z}_p$ são principais e da forma $p^n\mathbb{Z}_p$; eles formam uma cadeia decrescente

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots \supset 0.$$

Os anéis quocientes próprios de $\mathbb{Z}_p$ são os anéis finitos $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Assim, uma definição alternativa de $\mathbb{Z}_p$ é tomando o limite inverso do sistema de anéis

$$(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}.$$

Para definirmos grupos pro-p p-ádicos analíticos, precisaremos de mais algumas definições, que apresentamos a seguir.

O *conjunto de séries de potência formais* sobre $\mathbb{Q}_p$ em n variáveis que comutam $x_1, \ldots x_n$ é denotado por $\mathbb{Q}_p[[x]]$. Seus elementos são os somatórios formais $F(x) = \sum_{m\in\mathbb{N}^n} b_m x^m$ com $b_m \in \mathbb{Q}_p$, onde $x^m = x_1^{m_1} \ldots x_n^{m_n}$. Em $\mathbb{Q}_p[[x]]$ definimos a adição, multiplicação por escalar e uma multiplicação dada por

$$\sum_{m\in\mathbb{N}^n} a_m x^m \sum_{m\in\mathbb{N}^n} b_m x^m = \sum_{m\in\mathbb{N}^n} c_m x^m$$

onde
$$c_m = \sum_{s+t=m} a_s b_t.$$

Tendo em mente essas definições, definiremos agora funções analíticas.

Consideremos inicialmente funções em $\mathbb{Z}_p^r$. Escrevemos $x = (x_1, \ldots, x_r)$, $x \in \mathbb{Z}_p^r$, e para $y \in \mathbb{Z}_p^r$ e $h \in \mathbb{N}$, definimos:

$$\begin{aligned} B(y, p^{-h}) &= \left\{ z \in \mathbb{Z}_p^r \mid |z_i - y - 1| \leq p^{-h} \text{ para } i = 1, \ldots, r \right\} \\ &= \left\{ y + p^h x \mid x \in \mathbb{Z}_p^r \right\}. \end{aligned}$$

Definição 2.1.1. *Seja V um subconjunto não-vazio de $\mathbb{Z}_p^r$ e seja $f = (f_1, \ldots, f_s)$ uma função de V em $\mathbb{Z}_p^s$.*

1. *Seja $y \in V$. f é dita analítica em y se existe $h \in \mathbb{N}$ com $B(y, p^{-h}) \subseteq V$ e séries de potência formais $F_i(x) \in \mathbb{Q}_p[[x]]$ $(i = 1, \ldots, s)$ tais que*
$$f_i(y + p^h x) = F_i(x) \text{ para todo } x \in \mathbb{Z}_p^r.$$

2. *A função f é analítica em V se é analítica em todo ponto de V.*

Definição 2.1.2. *Seja X um espaço topológico.*

1. *Seja U um subconjunto aberto não-vazio de X. (U, ϕ, n) é uma carta em X se ϕ é um homeomorfismo de U em um subconjunto aberto de $\mathbb{Z}_p^n$ para algum $n \in \mathbb{N}$. A dimensão da carta é n. E é dita uma carta global se $U = X$.*

2. *Duas cartas (U, ϕ, n) e (V, ψ, m) em X são compatíveis se as funções $\psi \circ \phi^{-1}|_{\phi(U \cap V)}$ e $\phi \circ \psi^{-1}|_{\psi(U \cap V)}$ são funções analíticas em $\phi(U \cap V)$ e $\psi(U \cap V)$ respectivamente.*

3. *Um atlas em X é um conjunto de cartas duas a duas compatíveis que cobre X, ou seja, é um conjunto*
$$A = \{(U_i, \phi_i, n_i) \mid i \in I\}$$
com as seguintes propriedades:

   - *para cada $i \in I$, (U_i, ϕ_i, n_i) é uma carta em A;*
   - *para todos $i, j \in I$, (U_i, ϕ_i, n_i) e (U_j, ϕ_j, n_j) são compatíveis;*
   - *$X = \bigcup\limits_{i \in I} U_i$.*

   A é um atlas global se para algum $i \in I$, a carta (U_i, ϕ_i, n_i) for global.

4. *Sejam A e B atlas em X. Então A e B são compatíveis se as cartas de A forem compatíveis com as cartas de B, em outras palavras, se $A \cup B$ for um atlas em X.*

Denotando por X_A um espaço topológico X munido de um atlas A, dizemos que uma função $f : X_A \to Y_B$ é analítica se para cada par de cartas $(U, \phi, n) \in A$ e $(V, \psi, m) \in B$, valem:

1. $f^{-1}(V)$ é aberto em X, e

2. a composição
$$\psi \circ \phi^{-1}|_{\phi(U \cap f^{-1}(V))}$$
é uma função analítica do conjunto aberto $\phi(U \cap f^{-1}(V)) \subseteq \mathbb{Z}_p^n$ em $\mathbb{Z}_p^m$.

Definição 2.1.3. *Seja X um espaço topológico. Uma estrutura de variedade p-ádica analítica é uma classe de equivalência de atlas compatíveis em X. Se tal estrutura existe, X é uma variedade p-ádica analítica. Qualquer atlas nessa classe de equivalência é dito um atlas da variedade X e qualquer carta em um desses atlas é dita uma carta da variedade X.*

Podemos então definir um grupo pro-p p-ádico analítico.

Definição 2.1.4. *Um grupo topológico G é p-ádico analítico se tem a estrutura de uma variedade p-ádica analítica com a seguinte propriedade:*

1. *a função $g : G \times G \to G$ definida por $(x, y) \mapsto xy^{-1}$ é analítica.*

E em particular, um grupo pro-p é *p-ádico analítico* se tem a estrutura de uma variedade sobre $\mathbb{Z}_p$ e as operações de grupo são analíticas com respeito a essa estrutura.

Podemos ainda caracterizar um grupo pro-p p-ádico analítico em termos do grupo $GL_d(\mathbb{Z}_p)$ das matrizes inversíveis $d \times d$ sobre o anel dos inteiros p-ádicos $\mathbb{Z}_p$.

Seja $d \in \mathbb{N}$ e considere o grupo $GL_d(\mathbb{Z}_p)$. O conjunto $Mat_d(\mathbb{Z}_p)$ das matrizes $d \times d$ tem uma topologia p-ádica natural, a topologia produto induzida da topologia p-ádica de $\mathbb{Z}_p$. Como multiplicação de matrizes é uma operação contínua, também o é o processo de tomar a inversa de matrizes inversíveis. Daí, $GL_d(\mathbb{Z}_p)$ equipado com a topologia subespaço é um grupo topológico. Assim, enunciamos o seguinte resultado de Lazard ([11]).

Teorema 2.1.5. *Um grupo topológico compacto admite uma estrutura p-ádica analítica se, e somente se, for isomorfo a um subgrupo fechado de $GL_d(\mathbb{Z}_p)$ para algum d.*

Restringimos ainda o Teorema 2.1.5 para grupos pro-p. Existe um homomorfismo de anel natural de $\mathbb{Z}_p$ no corpo finito $\mathbb{F}_p$. Como $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash p\mathbb{Z}_p$, isso induz um homomorfismo de grupo sobrejetivo $\eta : GL_d(\mathbb{Z}_p) \to GL_d(\mathbb{F}_p)$. O núcleo de η é o grupo $GL_d^1(\mathbb{Z}_p) = \{g \in GL_d(\mathbb{Z}_p) | g \equiv 1 \ (mod\ p)\}$. A pré-imagem por η de qualquer p-subgrupo de Sylow do grupo finito $GL_d(\mathbb{F}_p)$ é um subgrupo pro-p de Sylow de $GL_d(\mathbb{Z}_p)$. Um p-subgrupo de Sylow particular de $GL_d(\mathbb{F}_p)$ é o grupo das matrizes uni-triangulares superiores. E pelos Teoremas de Sylow, todos os outros p-subgrupos de Sylow de $GL_d(\mathbb{F}_p)$ são conjugados a este.

Corolário 2.1.6. *Um grupo pro-p p-ádico analítico é um grupo topológico que é isomorfo a um subgrupo fechado de um subgrupo pro-p de Sylow de $GL_d(\mathbb{Z}_p)$ para algum d.*

2.2 Grupos Powerful

Antes da definição de grupos uniformemente *powerful*, precisamos definir grupos *powerful*.

Aqui elencamos alguns resultados no intuito de complementar a teoria preliminar mas que não serão necessários ao entendimento desse trabalho.

Definição 2.2.1.

1. *Um p-grupo finito G é dito powerful se p é ímpar e G/G^p é abeliano ou $p = 2$ e G/G^4 é abeliano.*
2. *Um subgrupo N de um p-grupo finito G é powerfully imerso em G e escrevemos N p.e. G (do inglês powerfully embedded), se p é ímpar e $[N,G] \leq N^p$ ou $p = 2$ e $[N,G] \leq N^4$.*

Assim, um p-grupo finito G é *powerful* se, e somente se, G p.e G e se N p.e G, então $N \triangleleft G$ e N é *powerful*. Quando p é ímpar, G é *powerful* se, e somente se, $G^p = \Phi(G)$.

Exemplo 2.2.2. *Todo p-grupo finito abeliano G é powerful e seus subgrupos são powerfully imersos em G.*

Exemplo 2.2.3. *Sejam G um p-grupo com p ímpar e $a_1, \ldots, a_d$ elementos de G tais que $G = \langle a_1 \rangle \langle a_2 \rangle \ldots \langle a_d \rangle$, onde $d = d(G)$. Então G é powerful.*

Nosso foco aqui são os grupos pro-p. Mas como muitos resultados que valem para os grupos pro-p podem ser herdados, de uma certa maneira, dos resultados que valem para p-grupos finitos, elencamos abaixo alguns resultados para p-grupos finitos que podem ser encontrados no Capítulo 2 de [1].

Lema 2.2.4. *Seja G um p-grupo finito e sejam N, K e W subgrupos normais de G com $N \leq W$.*

1. *Se N p.e. G, então NK/K p.e. G/K.*
2. *Se p é ímpar e $K \leq N^p$ ou se $p = 2$ e $K \leq N^2$, então N p.e. G se, e somente se, N/K p.e. G/K.*

3. *Se N p.e. G e $x \in G$, então $\langle N,x\rangle$ é powerful.*

4. *Se N não é powerfully imerso em W, então existe um subgrupo normal J de G tal que*

   - *se p é ímpar,*

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

   - *se p=2,*

$$N^4[N,W]^2[N,W,W] \leq J < N^4[N,W] \text{ e } |N^4[N,W] : J| = 2.$$

Demonstração. Os itens 1 e 2 são diretos da definição. Para provarmos o item 3, seja $H = \langle N,x\rangle$. Daí $[H,H] = [N,H]$ já que $N \lhd H$, então se N p.e. G, temos que $[H,H] \leq N^p < H^p$ (respectivamente, $[H,H] \leq H^4$ se $p = 2$). Para a parte 4, suponha p ímpar e que $[N,W] \nleq N^p$. Então $N^p < N^p[N,W] = M$, digamos. Como G é um p-grupo e M e N são normais em G, existe $J \lhd G$ tal que $N^p \leq J < M$ e $|M : J| = p$. Então M/J é central em G/J e o resultado segue. Um argumento parecido nos dá o caso $p = 2$. □

Proposição 2.2.5. *Sejam G um p-grupo finito e $N \leq G$. Se N p.e. G, então N^p p.e. G.*

Demonstração. Vamos dividir a prova em dois casos. Primeiramente, suponha p ímpar. Temos que $[N,G] \leq N^p$ e podemos supor que $(N^p)^p = 1 = [N^p,G,G]$. Então $[N,G,G] \leq Z(G)$ e segue que para quaisquer $x \in N$ e $g \in G$, a função $\omega \mapsto [x,g,\omega]$ é um homomorfismo de G em $Z(G)$. Então

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

Daí,

$$\begin{aligned}
[x^p,g] &= [x,g]^{x^{p-1}}[x,g]^{x^{p-2}}\dots[x,g] \\
&= \prod_{j=p-1}^{0}[x,g][x,g,x^j] \\
&= [x,g]^p\prod_{j=0}^{p-1}[x,g,x^j] \text{ já que } [x,g,x^j] \in Z(G) \text{ para cada j} \\
&= [x,g]^p[x,g,x]^{p(p-1)/2} = 1
\end{aligned}$$

uma vez que $[N,G]^p = 1$. Então $[N^p,G] = 1$, como queríamos demonstrar.

Agora vamos ao caso em que $p = 2$. Podemos supor agora que $[N,G] \leq N^4$ e que

$$[N^2,G,G] = [N^2,G]^2 = (N^2)^4 = 1.$$

Para $x \in N$ e $g \in G$, temos

$$[x^4,g] = [x^2,g][x^2,g,x^2][x^2,g] = [x^2,g]^2 = 1$$

então $N^4 \leq Z(G)$. Como o expoente de N divide 8, N^4 é gerado por elementos de ordem 2, donde $(N^4)^2 = 1$. Então com x e g como acima, temos

$$[x^2,g] = [x,g][x,g,x][x,g] = [x,g]^2 = 1$$

pois $[x,g,x] \in [N,G,G] \leq [N^4,G] = 1$ e $[x,g] \in [N,G] \leq N^4$. Então $[N^2,G] = 1$ e o resultado segue. $\square$

Lema 2.2.6. *Seja G um p-grupo powerful.*

1. *Para cada i, G_i p.e. G e $G_{i+1} = G_i^p = \Phi(G_i)$.*

2. *Para cada i, a função $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} em G_{i+1}/G_{i+2}.*

Demonstração. 1. Como $G = G_1$ é *powerful*, G_1 pe. G. Suponha G_i p.e. G para algum $i \geq 1$. Então $G_{i+1} = G_i^p[G_i,G] = G_i^p$ e a Proposição 2.2.5 mostra que G_{i+1} p.e. G. Já que $G_i^p \leq \Phi(G_i) = G_i^p[G_i,G_i] \leq G_{i+1}$ e isso implica também que $G_{i+1} = \Phi(G_i)$. O resultado segue por indução.

2. A parte 1. mostra que G_i é *powerful*, $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$. Então, fazendo uma mudança de notação, podemos supor que $i = 1$, daí, substituindo G por G/G_3, podemos supor que $G_3 = 1$. Então $[G,G] \leq G_2 \leq Z(G)$ e para $x,y \in G$ temos

$$(xy)^p = x^p y^p [y,x]^{p(p-1)/2}.$$

Se p é ímpar então $p|p(p-1)/2$, e

$$[y,x]^{p(p-1)/2} \in G_2^p = G_3 = 1.$$

Se $p = 2$ então $[G,G] \leq G^4 \leq G_3 = 1$. Logo, em ambos os casos, temos $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ e $G^p = G_2$, isso mostra que $x \mapsto x^p$ induz um homomorfismo de G/G_2 em G_2/G_3 e isso completa a prova. $\square$

Lema 2.2.7. *Se $G = \langle a_1,\ldots,a_d \rangle$ é um p-grupo powerful, então $G^p = \left\langle a_1^p,\ldots,a_d^p \right\rangle$.*

Demonstração. Seja $\theta : G/G_2 \mapsto G_2/G_3$ o homomorfismo dado no lema anterior. Então G_2/G_3 é gerado por $\{(a_1G_2)\theta, \ldots (a_dG_2)\theta\}$, daí $G_2 = \left\langle a_1^p, \ldots, a_d^p \right\rangle G_3$. Como $G_3 = \Phi(G_2)$ e $G_2 = G^p$, pelo Lema 2.2.6, temos o resultado. □

Proposição 2.2.8. *Se G um p-grupo powerful, então todo elemento de G^p é uma p-ésima potência em G.*

Demonstração. Argumentamos por indução em $|G|$. Seja $g \in G^p$. Pelo Lema 2.2.6, existe $x \in G$ e $y \in G_3$ tais que $g = x^p y$. Defina $H = \langle G^p, x \rangle$. Como $G^p = G_2$ p.e. G pelo Lema 2.2.6, o Lema 2.2.4 (3.) nos dá que H é *powerful*. Além disso, $g \in H^p$, já que $y \in G_3 = G_2^p$. Se $H \neq G$, então a hipótese de indução diz que g é uma p-ésima potência em H. Se $H = G$, então $G = \langle x \rangle$ é cíclico, pois nesse caso $G = \langle G^p, x \rangle = \Phi(G) \langle x \rangle$ e nesse caso, o resultado é trivial. □

Teorema 2.2.9. *Seja $G = \langle a_1, \ldots, a_d \rangle$ um p-grupo powerful e escreva $G_i = P_i(G)$ para cada i.*

1. *G_i p.e G.*
2. *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ para cada $k \geq 0$.*
3. *$G_i = G^{p^{i-1}} = \left\{ x^{p^{i-1}} \mid x \in G \right\} = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle$.*
4. *a função $x \mapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para cada i e k.*

Demonstração. Já provamos o item 1 e observamos que $G_{i+1} = G_i^p = P_2(G_i)$ para cada i. Segue então da Proposição 2.2.8 que $G_{i+1} = \{x^p | x \in G_i\}$ e por indução, $G_1 = x^{p^{i-1}} | x \in G$. Como G_1 é um subgrupo, isso implica que $G_i = G^{p^{i-1}}$. Repetidas aplicações do Lema 2.2.7 mostram então que $G_i = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle$. E assim provamos 3.

A parte 4 segue do Lema 2.2.6, item 2. E finalmente, tomando G_i no lugar de G e $k+1$ no lugar de i, em 3, obtemos

$$\begin{aligned} P_{k+1}(G_i) = G_i^{p^k} &= \left\{ x^{p^k} | x \in G_i \right\} \\ &= \left\{ y^{p^{i-1+k}} | y \in G \right\} = G_{i+k}, \end{aligned}$$

provando 2. □

Para grupos pro-p, tomamos, na Definição 2.2.1, os fechos dos subgrupos G^p, G^4, N^p e N^4 e N aberto.

Como $\overline{N^p} = \bigcap\{K \mid N^p \leq K \lhd_a G\}$ (respectivamente, $\overline{N^4}$), obtemos o seguinte critério para um subgrupo aberto ser *powerfully* imerso:

Proposição 2.2.10. *Sejam G um grupo pro-p e $N \leq_a G$. Então N p.e. G se, e somente se, NK/K p.e. G/K para todo $K \lhd_a G$.*

Corolário 2.2.11. *Um grupo topológico G é um grupo pro-p powerful se, e somente se, G é o limite inverso de um sistema inverso de p-grupos finitos powerful no qual todas as funções são sobrejetivas.*

Demonstração. Seja G um grupo pro-p *powerful*. Então $G \cong \varprojlim G/N$ onde N percorre os subgrupos abertos normais de G e cada G/N é um p-grupo *powerful* finito.

Suponha agora que $G = \varprojlim G_\lambda$, onde cada G_λ é um p-grupo finito *powerful* e $G_\mu \to G_\lambda$ é sobrejetivo para $\mu \geq \lambda$. Então G é um grupo pro-p e se $K \lhd_a G$, então G/K é um quociente de algum G_λ e portanto, é *powerful*. Pela Proposição 2.2.10, G é então, *powerful*. □

A partir desse resultado, podemos então pegar os resultados que valem para p-grupos finitos e levá-los para grupos pro-p. No entanto, temos que nos restringir aos grupos pro-p finitamente gerados, nos quais a p-série inferior consiste de subgrupos abertos, como mostra a Proposição 1.2.14.

Lema 2.2.12. *Seja G um grupo pro-p powerful finitamente gerado. Então todo elemento de G^p é uma p-ésima potência em G e $G^p = \Phi(G)$ é aberto em G. Se $p = 2$, então G^4 é aberto em G.*

Demonstração. Seja $g \in \overline{G^p}$. Então $gN \in (G/N)^p$ para cada $N \lhd_a G$. Então, pela Proposição 2.2.8, temos que gN é uma p-ésima potência em G/N para cada N. Segue que g é uma p-ésima potência em G. Então $\overline{G^p} \leq G^p$ e então $G^p = \overline{G^p}$ consiste de p-ésimas potências. Como $[G,G] \leq \overline{G^p}$, temos que $G^p = \Phi(G) = P_2(G)$, que é aberto, pela Proposição 1.2.14. E finalmente, se $p = 2$, um argumento parecido mostra que $G^4 = \overline{G^4} \geq P_3(G)$, nos dando que G^4 é aberto. □

Corolário 2.2.13. *Seja G como no Lema 2.2.12. Então, para cada i, temos*

$$G^{p^i} = (G^{p^{i-1}})^p = \left\{x^{p^i} \mid x \in G\right\} \text{ p.e. } G^{p^{i-1}}. \tag{2.1}$$

Demonstração. Segue das Proposições 2.2.5 e 2.2.10 que $\overline{G^p}$ p.e G. Logo, o caso $i = 1$ de (2.1) reduz ao Lema 2.2.12. O caso geral segue por indução, substituindo G por $G^{p^{i-1}}$. □

Teorema 2.2.14. *Seja $G = \overline{\langle a_1, \ldots, a_d \rangle}$ um grupo pro-p powerful finitamente gerado e escreva $G_i = P_i(G)$ para cada i.*

1. *G_i p.e G.*

2. *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ para cada $k \geq 0$ e, em particular, $G_{i+1} = \Phi(G_i)$.*

3. *$G_i = G^{p^{i-1}} = \left\{x^{p^{i-1}} \mid x \in G\right\} = \overline{\left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle}$.*

4. *a função $x \mapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} em G_{i+k}/G_{i+k+1} para cada i e k.*

Demonstração. A segunda igualdade em 3 segue do Corolário 2.2.13. Todo o resto segue do Teorema 2.2.9, aplicado aos p-grupos finitos G/G^{p^n} para n suficientemente grande, uma vez que os subgrupos G^{p^n} são abertos pelo Corolário 2.2.13 (pela Proposição 1.2.14, item 4, tais subgrupos formam uma base para as vizinhanças de 1 em G, já que $G^{p^n} \leq P_{n+1}(G)$ para cada n). □

2.3 Grupos Uniformemente Powerful

Tendo em vista a definição de grupo *powerful* e alguns resultados com respeito a tais grupos, damos agora uma definição mais forte que essa, a de grupos uniformemente *powerful*, que são um caso particular dos grupos *powerful*.

Definição 2.3.1. *Um grupo pro-p G é uniformemente powerful se*

1. *G é finitamente gerado;*

2. *G é powerful;*

3. *para todo i, $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$.*

Em geral, usaremos o termo "uniforme"para abreviar esta definição.

Se um grupo pro-p G satisfaz as condições 1 e 2 dessa definição, então, pelo Teorema 2.2.14, sabemos que a função $x \mapsto x^p$ induz um epimorfismo $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$ para cada i. Assim, a condição 3 da Definição 2.3.1 é equivalente a:

3.$'$ para cada $i \geq 1$, a função f_i é um isomorfismo.

Temos então o seguinte teorema:

Teorema 2.3.2. *Seja G um grupo pro-p powerful finitamente gerado. Então $P_k(G)$ é uniforme para todo k suficientemente grande.*

Demonstração. Escreva $G_i = P_i(G)$ e suponha $|G_i/G_{i+1}| = p^{d_i}$. Pelo Teorema 2.2.14, item 4, temos $d_1 \geq d_2 \geq \cdots \geq d_i \geq d_{i+1} \geq \dots$, então existe m tal que $d_k = d_m$ para todo $k \geq m$. Pelo Teorema 2.2.14, item 2, $P_i(G_k) = G_{k+i-1}$ para todos i e k e então, pelo item 1 do mesmo teorema, G_k é *powerful*. □

Uma outra maneira de caracterizar grupos uniformes é dada pelo seguinte teorema:

Teorema 2.3.3. *Um grupo pro-p powerful finitamente gerado é uniforme se, e somente se, é livre de torção.*

Demonstração. Seja G um grupo pro-p *powerful* finitamente gerado e escreva $G_i = P_i(G)$ para cada i. Primeiros suponhamos que G não seja livre de torção. Então G possui um elemento x de ordem p, pois se ele tivesse ordem finita coprima com p, tal elemento deveria estar em G_i para todo i, mas então ele seria 1. Digamos então $x \in G_i \backslash G_{i+1}$. Então $1 \neq xG_{i+1} \in G_i/G_{i+1}$ e $1 = x^p G_{i+2} \in G_{i+1}/G_{i+2}$, mas então a função $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ não é injetiva. Daí, G não é uniforme. Para a implicação contrária, suponhamos que G não seja uniforme. Então, para algum i, o epimorfismo $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ não é injetivo e então existe $x \in G_i \backslash G_{i+1}$ tal que $x^p \in G_{i+2}$. Coloque $x_2 = x$ e suponha que para algum $n \geq 2$, encontramos $x_2, \dots, x_n$ tais que $x_j^p \in G_{i+j}$ e $x_j \equiv x_{j-1}$ $(mod\ G_{i+j-2})$ para $2 < j \leq n$. Existe $z \in G_{i+n-1}$ tal que $z^p = x_n^p$; então escrevemos $x_{n+1} = z^{-1} x_n$. Assim, $x_{n+1} \equiv x_n$ $(mod\ G_{i+n-1})$. Além disso, $x_{n+1}^p \in G_{i+n+1}$: Se p é ímpar, temos

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

já que $[G_{i+n+1}, G, G][G_{i+n+1}, G]^p \leq G_{i+n+1}$; e se $p = 2$, temos

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

pois $[G_{i+n+1}, G] \leq G_{i+n+1}^4 = G_{i+n+1}$ já que G_{i+n+1} p.e. G.

Então a sequência $x_2, \dots, x_n, \dots$ pode ser construída recursivamente, é uma sequência de Cauchy e então converge para algum elemento $x_\infty \in G$. Então $x_\infty \equiv x \not\equiv 1$ $(mod\ G_{i+1})$ e $x_\infty \equiv x_n^p \equiv 1$ $(mod\ G_{i+n-1})$ para todo n. Logo $x_\infty^p = 1$ e então G não é livre de torção. □

Um exemplo simples de grupo uniforme é o grupo dos inteiros p-ádicos, $\mathbb{Z}_p$, para p ímpar.

As duas teorias vistas nesse capítulo se unem no seguinte resultado.

Teorema 2.3.4. *Seja G um grupo topológico. Então G tem a estrutura de um grupo p-ádico analítico se, e somente se, G contém um subgrupo aberto que é um grupo pro-p uniforme.*

Um estudo sobre esse assunto e a prova desse resultado estão contidos no capítulo 8 de [1].

Capítulo 3

Grupos p-Saturáveis e PF-Filtrations

Acerca do assunto principal dessa dissertação, trazemos então um estudo sobre grupos p-saturáveis, onde veremos a relação desses grupos com os PF-grupos, chegando no Teorema A apresentado na introdução; um pouco sobre subgrupos normais de grupos p-saturáveis, chegando no Teorema B; e entraremos um pouco mais na relação entre os grupos p-saturáveis e os grupos p-ádicos analíticos, culminando na demonstração do Teorema C.

3.1 Grupos p-Saturáveis

Vejamos então algumas definições e alguns resultados para embasar nosso estudo de grupos p-saturáveis e para provarmos o Teorema A, que relembramos a seguir.

Teorema A. *Seja G um grupo pro-p finitamente gerado livre de torção. Então as seguintes condições são equivalentes:*

1. *G é um grupo p-saturável.*
2. *G é um PF-grupo.*
3. *$G/\Phi(G)^p$ é um PF-grupo, onde $\Phi(G)$ é o subgrupo de Frattini de G.*

A primeira definição que precisaremos é a de valoração.

Definição 3.1.1. *Seja G um grupo pro-p finitamente gerado. Dizemos que G é p-valorado se existe uma função $\omega : G \to \mathbb{R}_{>0} \cup \{\infty\}$, a qual chamamos de valoração, que satisfaz as seguintes propriedades, para todos $x, y \in G$:*

1. $\omega(x) > (p-1)^{-1}$.

2. $\omega(x) = \infty \Leftrightarrow x = 1$.

3. $\omega\left(xy^{-1}\right) \geq min\{\omega(x), \omega(y)\}$.

4. $\omega([x,y]) \geq \omega(x) + \omega(y)$.

5. $\omega(x^p) = \omega(x) + 1$.

Definição 3.1.2. *Um grupo pro-p G com uma valoração ω é chamado p-saturável se para todo $x \in G$ com $\omega(x) > p(p-1)^{-1}$, existe $y \in G$ tal que $x = y^p$.*

Exemplo 3.1.3. *Fazendo uma pequena alteração na valoração p-ádica apresentada no capítulo anterior, temos que o grupo $\mathbb{Z}_p$ com a valoração $v_p(x)$ é um grupo p-saturável. Assim, para $p = 2$, $\mathbb{Z}_2$ é 2-saturável com a valoração dada por $v_2(x) := n+2$, se $x \neq 0$ e $v_2(x) := \infty$ se $x = 0$ e para p ímpar, $\mathbb{Z}_p$ é p-saturável com a valoração dada por $v_p(x) := n+1$, se $x \neq 0$ e $v_p(x) := \infty$ se $x = 0$.*

Podemos usar a valoração ω para definir em G uma topologia escolhendo como um sistema fundamental de vizinhanças da identidade os subgrupos $G_v = \{g \in G | \omega(g) \geq v\}$ com $v \in \mathbb{R}_{>0}$.

Lema 3.1.4. *Seja G um grupo p-valorado. Então a topologia de G vinda da valoração coincide com a topologia de G enquanto grupo pro-p.*

Demonstração. Sabemos que os subgrupos abertos de G na topologia pro-p são os subgrupos de índice finito. Pelas propriedades 4 e 5 da Definição 3.1.1, se $n = \lceil v \rceil$, então $\gamma_{n(p-1)}(G)G^{p^n}$ está contido em G_v. Daí, G_v tem índice finito em G e é aberto na topologia pro-p. Segue então da Proposição 1.2.8, item 2, que os subgrupos G_v formam um sistema fundamental de vizinhanças da identidade na topologia pro-p. Daí, a topologia dada pela valoração coincide com a topologia pro-p. □

Definição 3.1.5. *Sejam G um grupo pro-p e $\{N_i\}_{i\in\mathbb{N}}$ uma família de subgrupos fechados normais. Dizemos que $\{N_i\}_{i\in\mathbb{N}}$ é uma potent filtration de G se valem as seguintes condições:*

1. $N_i \leq N_j$ *para todo* $i \geq j$.

2. $\bigcap_{i\in\mathbb{N}} N_i = 1$.

3. $[N_i, G] \leq N_{i+1}$.

4. $[N_i,_{p-1} G] \leq N_{i+1}^p$.

Se existe uma potent filtration de G que começa no subgrupo N, dizemos que N é PF-imerso em G. Um grupo pro-p G é um PF-grupo se G é PF-imerso em G.

As principais propriedades com respeito a *potent filtrations* e subgrupos PF-imersos estão listadas nas proposições a seguir.

Proposição 3.1.6. *Sejam G um grupo pro-p, N um subgrupo PF-imerso em G e $\{N_i\}_{i\in\mathbb{N}}$ uma potent filtration que começa no subgrupo N. Então:*

1. *N/K é PF-imerso em G/K para todo subgrupo fechado normal K em G.*
2. *Se $g\in G$ e $x\in N_i$, então $(xg)^p \equiv x^p g^p \left(\mathrm{mod}\ N_{i+1}^p\right)$.*
3. *$\left\{N_i^p\right\}_{i\in\mathbb{N}}$ e $\{[N_i,G]\}_{i\in\mathbb{N}}$ são potent filtrations, portanto N^p e $[N,G]$ são subgrupos PF-imersos em G.*
4. *$N^{p^k} = \left\{x^{p^k} \mid x\in N\right\}$.*
5. *Para todos $i,j\geq 0$, $[N^{p^i},G^{p^j}] = [N,G]^{p^{i+j}}$.*

Demonstração.

1. É suficiente ver que $\bigcap\limits_{i\in\mathbb{N}} N_iK = (\bigcap\limits_{i\in\mathbb{N}} N_i)K = K$, onde a primeira igualdade segue da Proposição 1.2.7, item 1.
2. É consequência direta da fórmula de P. Hall e da definição de *potent filtration*.
3. Vamos primeiro mostrar que $[N_i^p,G] = [N_i,G]^p$ para todo i. Pra isso, podemos supor G um p-grupo finito e argumentar por indução reversa em i. Como G é finito, existe i_0 tal que $N_i = 1$ para todo $i\geq i_0$. Tomemos $i=i_0$ e a igualdade é válida. De acordo com o Teorema 1.3.5, temos $[N_i^p,G]\equiv[N_i,G]^p$ $(\mathrm{mod}\ [N_i,_p G])$. Como $\{N_i\}$ é uma *potent filtration*, temos que $[N_i,_p G]\leq[N_{i+1}^p,G]$. E pela hipótese de indução, $[N_{i+1}^p,G] = [N_{i+1},G]^p$. Daí, por um lado,

$$[N_i^p,G]\leq[N_i,G]^p[N_i,_p G]\leq[N_i,G]^p[N_{i+1}^p,G] = [N_i,G]^p[N_{i+1},G]^p = [N_i,G]^p.$$

E por outro lado,

$$[N_i,G]^p\leq[N_i^p,G][N_i,_p G]\leq[N_i^p,G][N_{i+1}^p,G] = [N_i^p,G].$$

Logo, $[N_i^p,G] = [N_i,G]^p$ para todo i.

Para $\{[N_i, G]\}$, as três primeiras condições da definição de *potent filtration* são diretas e a quarta condição segue do que acabamos de provar:

$$[[N_i, G],_{p-1} G] \leq [N_{i+1}^p, G] = [N_{i+1}, G]^p.$$

E para $\{N_i^p\}$, note que, pelo que mostramos, temos que $[N_i^p, G] = [N_i, G]^p \leq N_{i+1}^p$ e $[N_i^p,_{p-1} G] = [N_i,_{p-1} G]^p \leq (N_{i+1}^p)^p$.

4. Novamente, é suficiente pensarmos no caso em que G é um p-grupo finito. Note que pelo item 3, só precisamos mostrar que $N^p = \{x^p \mid x \in N\}$.

   Seja $\{N_i\}$ uma *potent filtration* com $N = N_1$. É suficiente provar, por indução reversa em i que $x^p y^p$ é uma p-ésima potência para todos $x \in N$ e $y \in N_i$. Isso segue imediatamente do item 2 aplicando duas vezes a hipótese de indução.

5. Pelos itens 3 e 4, já temos que $[N^{p^i}, G] = [N, G]^{p^i}$. Então nos resta mostrar que $[N, G^{p^j}] = [N, G]^{p^j}$. Mostraremos para o caso em que G é um p-grupo finito, por indução na ordem de N. Pelo Teorema 1.3.5,

$$[N, G^{p^j}] \equiv [N, G]^{p^j} \ (mod\ [N,_p G]^{p^{j-1}} \ldots [N,_{j(p-1)+1} G]) \tag{3.1}$$

   Temos então que esse módulo está contido em $[N_2, G]^{p^j}$. Pela hipótese de indução, $[N_2, G]^{p^j} = [N_2, G^{p^j}]$ e então, por 3.1, $[N, G^{p^j}] = [N, G]^{p^j}$.

□

Proposição 3.1.7. *Seja G um grupo pro-p. Então, para cada subgrupo fechado normal K de G, existe um subgrupo fechado T de G, que contém K e satisfaz as propriedades:*

1. *Se N é PF-imerso em G, então $N \cap T$ é PF-imerso em T. Mais precisamente, se $\{N_i\}$ é uma potent filtration de G, então $\{N_i \cap T\}$ é uma potent filtration de T.*

2. *Para todo subgrupo PF-imerso M de T, temos $[M^{p^i}, T^{p^j}]^{p^k} = [M^{p^r}, K^{p^s}]^{p^t}$, sempre que $i + j + k = r + s + t \geq 1$.*

Demonstração. Seja $\mathcal{T}$ a família de todos os subgrupos fechados de G contendo K e que satisfaz a propriedade 1. $\mathcal{T}$ é não vazio, pois $G \in \mathcal{T}$. Afirmamos que $\mathcal{T}$ tem subgrupos minimais. Pelo Lema de Zorn, apenas precisamos considerar uma cadeia $\{T_j\}$ de subgrupos de $\mathcal{T}$ e provar que $T = \bigcap_j T_j$ também pertence a $\mathcal{T}$. Escolha então uma *potent filtration* $\{N_i\}$ de G e mostremos que $\{N_i \cap T\}$ é uma *potent filtration* de T. Para isso, tome $x \in [N_i \cap T,_{p-1} T]$ e provaremos que $x = t^p$ para algum $t \in N_{i+1} \cap T$. Como $x \in [N_i \cap T_j,_{p-1} T_j] \leq (N_{i+1} \cap$

$T_j)^p$, podemos escrever $x = t_j^p$ com $t_j \in N_{i+1} \cap T_j$ (recordando a Proposição 3.1.6, item 4). Definimos então $F_j = \left\{t_j \in N_{i+1} \cap T_j : t_j^p = x\right\}$. Como N_{i+1} e T_j são fechados em G e tomar potências é contínuo em G, segue que F_j é um subconjunto fechado não-vazio de G. Note que a família $\{F_j\}$ de subconjuntos fechados tem a propriedade da interseção finita. De fato, como $\{T_j\}$ é uma cadeia, para qualquer coleção finita de índices $j_1, j_2, \ldots, j_n$ existe um índice j_k tal que $T_{j_1} \cap \cdots \cap T_{j_n} = T_{j_k}$ e consequentemente $F_{j_1} \cap \cdots \cap F_{j_n} = F_{j_k}$ é não-vazio. Com G é compacto, existe ao menos um elemento t na interseção de todos os F_j. Segue que $t \in N_{i+1} \cap T$ e $t^p = x$, como desejado.

Agora, seja T um subgrupo minimal da família $\mathcal{T}$. Precisamos mostrar que T satisfaz 2. Primeiro provamos que $[M^{p^r}, T] = [M^{p^r}, K]$ para todos M PF-imerso em T e todo $r \geq 1$. Como $M^{p^{r-1}}$ é também PF-imerso em T e K está contido em T, é suficiente notar que $[M^p, T] \leq [M^p, K]$. Suponha por contradição que esta inclusão não valha para algum M. Então ela deve falhar em algum quociente G/V, onde V é um subgrupo aberto normal de G. Seja $\{M_i\}$ uma *potent filtration* que começa no subgrupo M. Como G/V é finito, deve existir um índice j tal que $[M_j^p, T] \nleq [M_j^p, K]V$ mas $[M_{j+1}^p, T] \leq [M_{j+1}^p, K]V$. Defina então

$$T^* = \left\{t \in T : [M_j^p, t] \leq [M_j^p, K]V\right\},$$

em outras palavras, T^* é o centralizador em T de $M_j^p V/[M_j^p, K]V$. Então T^* é um subgrupo fechado normal próprio de T contendo K. Dada uma *potent filtration* $\{N_i\}$ de G, provamos a seguir que $\{N_i \cap T^*\}$ é uma *potent filtration* de T^*, o que é uma contradição com a definição de T. Escolha $x \in [N_i \cap T^*,_{p-1} T^*]$ e vejamos que $x \in (N_{i+1} \cap T^*)^p$. Como $[N_i \cap T^*,_{p-1} T^*] \leq [N_i \cap T,_{p-1} T] \leq (N_{i+1} \cap T)^p$, podemos escrever $x = t^p$ com $t \in N_{i+1} \cap T$ e é suficiente ver que $t \in T^*$. Agora, pela congruência 1.3 do Teorema 1.3.1,

$$[M_j^p, t] \leq [M_j, t^p][M_j, T, T]^p[M_j,_p T] \leq [M_j, x][M_{j+1}^p, T] \leq [M_j, x][M_{j+1}^p, K]V$$

e por outro lado, como $x \in \gamma_p(T)$,

$$[M_j, x] \leq [M_j, \gamma_p(T)] \leq [M_j,_p T] \leq [M_{j+1}^p, T] \leq [M_{j+1}^p, K]V$$

Então $[M_j^p, t] \leq [M_{j+1}^p, K]V$ e $t \in T^*$, como desejado.

Mostramos então que $[M^{p^r}, K] = [M, K]^{p^r} = [M, K^{p^r}]$ para todo $r \geq 0$. Obviamente, podemos assumir que $r \geq 1$ e que G é um p-grupo finito. Agora

$$[M^{p^r}, K] \equiv [M, K]^{p^r} \equiv [M, K^{p^r}] \ (mod\ [M,_p T]^{p^{r-1}} \ldots [M,_{r(p-1)+1} T]),$$

e esse módulo está contido em $[M_2^{p^r}, T]$, que coincide com $[M_2^{p^r}, K]$ como visto acima. Então o resultado segue por indução na ordem de M.

Agora podemos concluir a prova de 2. Como $i+j+k = r+s+t \geq 1$, temos

$$[M^{p^r}, K^{p^s}]^{p^t} = [[M^{p^{r+s+t}}, K] = M^{p^{r+s+t}}, T] = [M^{p^i}, T^{p^j}]^{p^k},$$

pelos resultados nos dois últimos parágrafos e pelo item 5 da Proposição 3.1.6. $\square$

Na próxima proposição mostramos que em um PF-grupo livre de torção, raízes de elementos são tomadas de maneira única.

Proposição 3.1.8. *Sejam G um grupo pro-p e N um subgrupo PF-imerso em G livre de torção. Se $x^{p^k} \in N^{p^k}$, então $x \in N$. Mais ainda, se $x, y \in N$ e $x^{p^k} = y^{p^k}$, então $x = y$.*

Demonstração. É suficiente mostrarmos o resultado para o caso $k = 1$. Considere N PF-imerso em G e a respectiva *potent filtration* $\{N_i\}$. Façamos $x_1 = x$. Pela hipótese, existe $a_1 \in N_1$ tal que $x_1^p = a_1^p$. Pondo $x_2 = x_1 a_1^{-1}$, pelo item 2 da Proposição 3.1.6, temos $x_2^p = (x_1 a_1^{-1})^p \equiv x_1^p a_1^{-p} = 1 \ (mod\ N_2^p)$, ou seja, $x_2^p \in N_2^p$. Generalizando, temos que se $x_i^p \in N_i^p$, existe $a_1 \in N_i$ tal que $x_i^p = a_i^p$ e então $x_{i+1} = x_i a_i^{-1}$ satisfaz $x_{i+1}^p \in N_{i+1}^p$ e $x_{i+1} \equiv x_i \ (mod\ N_i)$.

Construímos então uma sequência de Cauchy $\{x_i\}_{i \in \mathbb{N}}$ tal que $x_i^p \in N_i^p$. Então, $(\lim\limits_{i \to \infty} x_i)^p = \lim\limits_{i \to \infty} x_i^p = 1$. N é livre de torção, então $\lim\limits_{i \to \infty} x_i = 1$. E $h_i = x x_i^{-1}$ também é uma sequência de Cauchy, já que multiplicar por x e pegar inversos são operações contínuas. Como $h_1 = x x_1^{-1} = 1$ e $h_{i+1} = x x_{i+1}^{-1} \equiv x x_i^{-1}\ mod\ N$, h_i está contido em N. Logo $\lim\limits_{i \to \infty} h_i \in N$ e $x = \lim\limits_{i \to \infty} h_i x_i = (\lim\limits_{i \to \infty} h_i)(\lim\limits_{i \to \infty} x_i) \in N$.

Considere agora $x, y \in N$ tal que $x^p = y^p$. É suficiente mostrar que $xy^{-1} \in N_i$, para todo i. Provaremos por indução. Como $N_1 = N$, o caso $i = 1$ é óbvio. Agora suponha que a afirmação valha para todo i e mostraremos que vale para $i+1$. Novamente pelo item 2 da proposição anterior, temos $(xy^{-1})^p \equiv x^p y^{-p} \ (mod N_{i+1}^p)$. Logo $(xy^{-1})^p \in N_{i+1}^p$ e então $xy^{-1} \in N_{i+1}$. $\square$

Lema 3.1.9. *Sejam G um grupo pro-p e N um subgrupo fechado normal de G. Então:*

1. *Se M é um subgrupo fechado normal de G tal que $N \leq M[N, G]$, então $N \leq M$.*

2. *Para todo $l \geq 0$, $[N^p, {}_l G] \leq [N, {}_l G]^p [N, {}_{(p-1)+l} G]$.*

Demonstração. 1. Como um grupo pro-p é o limite inverso de p-grupos finitos, podemos reduzir a prova a um p-grupo finito e esse caso foi provado no Capítulo 1, no Lema 1.3.3.

2. O resultado segue como caso particular do Teorema 1.3.6.

$\square$

O lema a seguir mostra que não há necessidade de checar a hipótese da interseção trivial dos subgrupos para conseguirmos uma *potent filtration* que começa no subgrupo fechado normal N, pois mostramos que basta algum dos subgrupos estar em $[N,G]N^p$.

Lema 3.1.10. *Sejam G um grupo pro-p e N um subgrupo fechado normal para o qual existe um série de subgrupos $N = N_1 \geq N_2 \geq \cdots \geq N_{t+1} = [N,G]N^p$ que satisfaz $[N_i,G] \leq N_{i+1}$ e $[N_i,_{p-1} G] \leq N_{i+1}^p$ para $1 \leq i \leq t$. Defina:*

$$M_i = \begin{cases} [N_s,_j G]N^p, \ se \ i = jt+s \leq t(p-1) \ com \ 1 \leq s \leq t, \\ M_{i-t(p-1)}^p, \ se \ i > t(p-1). \end{cases} \tag{3.2}$$

Então $\{M_i\}$ é uma potent filtration de G. Em particular, N é PF-imerso em G.

Demonstração. É claro que $\{M_i\}$ é uma série decrescente de subgrupos fechados normais de G com interseção trivial. Vamos provar que $[M_i,G] \leq M_{i+1}$ e $[M_i,_{p-1} G]M_{i+1}^p$ por indução em i.

Suponhamos que $i \leq t(p-1)$. Escrevendo $i = jt+s$ com $1 \leq s \leq t$, temos $M_i = [N_s,_j G]N^p$. Então $[M_i,G] = [[N_s,_j G]N^p,G] \leq [N_{s+1},_j G]N^p = M_{i+1}$. Por outro lado, temos $[M_i,_{p-1} G] = [[N_s,_j G]N^p,_{p-1} G] \leq [N_{s+1}^p,_j G][N^p,_{p-1} G]$.

Vamos mostrar primeiramente que $[N_k^p,_j G] \leq [N_k,_j G]^p$ para $1 \leq k \leq t$. Pela parte (2) do Lema 3.1.9,

$$[N_k^p,_j G] \leq [N_k,_j G]^p [N_k,_{j+p-1} G] \leq [N_k,_j G]^p [N_{k+1}^p,_j G],$$

e repetindo esse argumento,

$$[N_k^p,_j G] \leq [N_k,_j G]^p [N_{t+1}^p,_j G]. \tag{3.3}$$

Aplicando novamente o Lema 3.1.9, dessa vez para $[N_{t+1}^p,_j G]$, teremos

$$\begin{aligned} [N_{t+1}^p,_j G] &\leq [N_{t+1},_j G]^p [N_{t+1},_{j+p-1} G] && (3.4)\\ &\leq [N_{t+1},_j G]^p [N^p,_{j+p-1} G][N,_{j+p} G] \leq [N_{t+1},_j G]^p [N^p,_{j+1} G]. && (3.5) \end{aligned}$$

Consequentemente,

$$[N_k^p,_j G] \leq [N_k,_j G]^p [N^p,_{j+1} G] \leq [N_k, jG]^p [N,_{j+1} G]^p [N_{t+1}^p,_{j+1} G]$$
$$\leq [N_k,_j G]^p [N_k^p,_{j+1} G],$$

onde a segunda inclusão segue de 3.3 para $k=1$. Concluímos então, do Lema 3.1.9 que $[N_k^p,_j G] \leq [N_k,_j G]^p$. Aplicando esse resultado para $[N_{s+1}^p,_j G][N^p,_{p-1} G]$ (e para 3.4 para $s=t$), segue que $[M_i,_{p-1} G] \leq M_{i+1}^p$.

Agora suponhamos que $i > t(p-1)$. Então $M_i = M_{i-t(p-1)}^p$ e pela hipótese de indução,

$$[M_{i-t(p-1)}^p, G] \leq [M_{i-t(p-1)}, G]^p [M_{i-t(p-1)},_p G]$$
$$\leq [M_{i-t(p-1)}, G]^p [M_{i-t(p-1)+1}^p, G] \leq M_{i+1}.$$

Usando um argumento similar obtemos $[M_i,_{p-1} G] \leq M_{i+1}^p$. □

Como consequência direta do lema acima obtemos um critério para que um subgrupo fechado normal finitamente gerado N seja PF-imerso em G.

Corolário 3.1.11. *Sejam G um grupo pro-p e N um subgrupo fechado normal finitamente gerado de G. Então N é PF-imerso em G se, e somente se, $N/([N,G]N^p)^p$ é PF-imerso em $G/([N,G]N^p)^p$.*

Demonstração. Se N é PF-imerso em G, pelo item 1 da Proposição 3.1.6, $N/([N,G]N^p)^p$ é PF-imerso em $G/([N,G]N^p)^p$. Por outro lado, considere a *potent filtration* $\{N_i/([N,G]N^p)^p\}$ que começa no subgrupo $N/([N,G]N^p)^p$. Por N ser finitamente gerado, o subgrupo $[N,G]N^p$ é aberto e então $N_t \leq [N,G]N^p$ para algum t. Então é suficiente considerar a série de subgrupos $N = N_1[N,G]N^p \geq N_2[N,G]N^p \geq \cdots \geq N_t[N,G]N^p = [N,G]N^p$ e aplicar o lema anterior. □

Com os dois últimos resultados provamos então o teorema mais importante desse trabalho, o Teorema A apresentado na introdução.

Teorema A. *Seja G um grupo pro-p finitamente gerado livre de torção. Então as seguintes condições são equivalentes:*

1. *G é um grupo p-saturável.*

2. *G é um PF-grupo.*

3. *$G/\Phi(G)^p$ é um PF-grupo, onde $\Phi(G)$ é o subgrupo de Frattini de G.*

Demonstração. Como G é pro-p, a equivalência entre 2 e 3 segue do Corolário 3.1.11. Vamos provar então a equivalência entre 1 e 2.

Seja G um PF-grupo. Precisamos de uma valoração que satisfaça as definições 3.1.1 e 3.1.2. Considere a família de subgrupos $G = N_1 \geq N_2 \geq \cdots \geq N_{t+1} = \Phi(G)$ tal que $[N_i, G] \leq N_{i+1}$ e $\left[N_i,{}_{p-1} G\right] \leq N_{i+1}^p$ para $i \leq t$. Para todo $i \in \mathbb{Z}_{>0}$, escreva $i = rt(p-1) + jt + s$, onde $0 \leq j \leq p-2$ e $1 \leq s \leq t$ e defina $M_i = (\left[N_s,{}_j G\right] G^p)^{p^r}$. Pelo Lema 3.1.10, $\{M_i\}$ é uma *potent filtration* de G.

Definimos então, para cada $x \in M_i \backslash M_{i+1}$, uma valoração ω da seguinte maneira:

$$\omega(x) = \frac{1}{p-1}\left(\frac{2^{sp+j+1}}{2^{(t+1)p}} + j + 1\right) + r$$

onde r, j e s são dados como acima e $\omega(1) = \infty$. As propriedades 1-3 da definição de valoração dadas em 3.1.1 são obviamente satisfeitas. Se $x^p \in (\left[N_s,{}_j G\right] G^p)^{p^r}$, então, pela Proposição 3.1.8, $x \in (\left[N_s,{}_j G\right] G^p)^{p^{r-1}}$. Logo, (v) também é satisfeita. Vamos então verificar 4. Para isso, considere x_1 e $x_2 \in G$ e suponha $x_k \in M_{i_k} \backslash M_{i_k+1}$. Escrevendo $M_{i_k} = (\left[N_{s_k},{}_{j_k} G\right] G^p)^{p^{r_k}}$, temos, pela Proposição 3.1.6,

$$\begin{aligned}[x_1, x_2] &\in \left[(\left[N_{s_1},{}_{j_1} G\right] G^p)^{p^{r_1}}, (\left[N_{s_2},{}_{j_2} G\right] G^p)^{p^{r_2}}\right] \\ &= \left[\left[N_{s_1},{}_{j_1} G\right] G^p, \left[N_{s_2},{}_{j_2} G\right] G^p\right]^{p^{r_1+r_2}} \leq (\left[N_{s_1},{}_{j_1+j_2+1} G\right] G^p)^{p^{r_1+r_2}}.\end{aligned}$$

Supondo sem perda de generalidade que $s_1 p + j_1 \geq s_2 p + j_2$, temos:

Se $j_1 + j_2 < p - 2$, então

$$\omega([x_1, x_2]) \geq \frac{1}{p-1}\left(\frac{2^{s_1 p + j_1 + j_2 + 2}}{2^{(t+1)p}} + j_1 + j_2 + 2\right) + r_1 + r_2.$$

Como

$$\omega(x_1) + \omega(x_2) = \frac{1}{p-1}\left(\frac{2^{s_1 p + j_1 + 1} + 2^{s_2 p + j_2 + 2}}{2^{(t+1)p}} + j_1 + j_2 + 2\right) + r_1 + r_2$$

e

$$2^{s_1 p + j_1 + j_2 + 2} \geq 2^{s_1 p + j_1 + 2} \geq 2^{s_1 p + j_1 + 1} + 2^{s_2 p + j_2 + 1},$$

temos que $\omega([x_1, x_2]) \geq \omega(x_1) + \omega(x_2)$.

E se $j_1 + j_2 \geq p-2$, então

$$\begin{aligned}
[x_1,x_2] &\in \left[\left[N_{s_1,j_1}G\right]G^p, \left[N_{s_2,j_2}G\right]G^p\right]^{p^{r_1+r_2}} \\
&\leq \left(\left[N_{s_1,j_1+j_2+1}G\right]\left[N_{s_1,j_1+1}G\right]^p\left[N_{s_2,j_2+1}G\right]^p G^{p^2}\right)^{p^{r_1+r_2}} \\
&\leq \left(\left[N_{s_1+1,j_1+j_2-p+2}G\right]^p\left[N_{s_1,j_1+1}G\right]^p\left[N_{s_2,j_2+1}G\right]^p G^{p^2}\right)^{p^{r_1+r_2}} \\
&\leq \left(\left[N_{s_1+1,j_1+j_2-p+2}G\right]G^p\right)^{p^{r_1+r_2+1}}.
\end{aligned}$$

Daí,

$$\omega\left([x_1,x_2]\right) \geq \frac{1}{p-1}\left(\frac{2^{s_1p+j_1+j_2+3}}{2^{(t+1)p}} + j_1 + j_2 + 2\right) + r_1 + r_2.$$

Logo, $\omega\left([x_1,x_2]\right) \geq \omega\left(x_1\right) + \omega\left(x_2\right)$.

Agora precisamos provar que G satisfaz a propriedade da Definição 3.1.2. Seja $x \in \left(\left[N_{s,j}G\right]G^p\right)^{p^r}$. Se $\omega\left(x\right) > p\left(p-1\right)^{-1}$, pela definição de ω, $r \geq 1$, então $x \in G^p$. Pela Proposição 3.1.6, $x = y^p$ para algum $y \in G$. E então temos que G é p-saturável.

Por outro lado, suponha G p-saturável para uma p-valoração ω. Defina uma topologia em $((p-1)^{-1}, +\infty]$, cujos abertos são os conjuntos da forma $(v, +\infty]$ com $v \geq (p-1)^{-1}$ e o conjunto vazio. Considere os subgrupos $G_v = \{g \in G \mid \omega(g) \geq v\}$, com $v \in \mathbb{R}_{>0}$. Assim, como os G_v são abertos, ω é contínua. E $\omega(G)$ é compacto uma vez que G é compacto. Então existe $\delta > 0$ tal que $\omega(G) \subseteq [(p-1)^{-1} + \delta, +\infty]$. Vamos mostrar que $N_i = \left\{x \in G \mid \omega(x) \geq (p-1)^{-1} + \delta i\right\}$ define uma *potent filtration* de G. $\{N_i\}_{i\in\mathbb{N}}$ é uma série decrescente de subgrupos fechados com interseção trivial. E dados $x \in N_i$ e $y \in G$,

$$\omega([x,y]) \geq \omega(x) + \omega(y) \geq (p-1)^{-1} + i\delta + (p-1)^{-1} + \delta \geq (p-1)^{-1} + (i+1)\delta.$$

Então esta é uma *filtration* central de subgrupos fechados normais.

Finalmente, se $x \in N_i$ e $y_1, \ldots, y_{p-1} \in G$, então

$$\begin{aligned}
\omega([x,y_1,\ldots,y_{p-1}]) &\geq (p-1)^{-1} + i\delta + 1 + \delta(p-1) \\
&\geq p(p-1)^{-1} + (i+1)\delta > p(p-1)^{-1}.
\end{aligned}$$

Daí, $[x,y_1,\ldots,y_{p-1}] = a^p$ com $\omega(a) = \omega([x,y_1,\ldots,y_{p-1}]) - 1 \geq (p-1)^{-1} + (i+1)\delta$. Assim, $a \in N_{i+1}$ e $[N_{i,p-1}G] \leq N_{i+1}^p$, o que nos dá a condição que faltava para $\{N_i\}_{i\in\mathbb{N}}$ ser uma *potent filtration*. Logo, G é um PF-grupo. □

Corolário 3.1.12. *Seja G um grupo pro-p finitamente gerado livre de torção tal que* $\gamma_p(G) \leq \Phi(G)^p$. *Então G é um PF-grupo.*

Demonstração. Basta encontrarmos uma PF-filtration que começa em G. Para isso, considere a p-série inferior de G

$$G_1 := G \text{ e } G_i := \overline{G_{i-1}^p[G_{i-1}, G]} \text{ para } i \geq 2.$$

Note que $[G_1,_{p-1} G] = \gamma_p(G) \subseteq \Phi(G)^p = G_2^p$ e usando indução e a Proposição 3.1.6, temos para $i \geq 2$:

$$\begin{aligned}[G_i,_{p-1} G] &= [[G_{i-1}, G]G_{i-1}^p,_{p-1} G] \subseteq [G_{i-1},_{p-1} G, G][G_{i-1}^p,_{p-1} G] \\ &\subseteq [G_i^p, G[G_{i-1},_{p-1} G]^p \subseteq [G_i, G]^p(G_i^p)^p \subseteq G_{i+1}^p.\end{aligned}$$

□

Corolário 3.1.13. *Seja G um grupo pro-p finitamente gerado. Então G é p-ádico analítico se, e somente se, G tem um subgrupo aberto PF-imerso em G.*

Demonstração. A parte do "somente se"é imediata do Teorema A. Por outro lado, se N é um subgrupo aberto PF-imerso de G, então N^p é um subgrupo aberto *powerful* de G: pelo item 5 da Proposição 3.1.6, $[N^p, N^p] \leq [N,N]^{p^2}$ e $[N,N]^{p^2}$ está contido em $(N^p)^p$ se $p \geq 3$ e em $(N^2)^4$ se $p = 2$. Consequentemente, G é p-ádico analítico. □

3.2 Subgrupos Normais de Grupos p-Saturáveis

Buscando entender os grupos p-saturáveis, passamos a olhar para os seus subgrupos normais com o objetivo de identificar quando tais subgrupos são ainda p-saturáveis. Generalizaremos as definições de *potent filtrations* e PF-grupos e com alguns resultados auxiliares provaremos o Teorema B.

Teorema B. *Sejam G um grupo p-saturável e N um subgrupo fechado normal de G contido em $\Phi(G)$. Então N é p-saturável.*

Para iniciar esse estudo, relembramos o seguinte resultado, que é um caso particular da Proposição 3.1.7.

Teorema 3.2.1. *Sejam G um PF-grupo e N um subgrupo fechado normal de G. Então existe um PF-subgrupo fechado T de G que contém N tal que para todo subgrupo PF-imerso M de T, temos $[M^{p^i}, T^{p^j}]^{p^k} = [M^{p^r}, N^{p^s}]^{p^t}$, sempre que $i + j + k = r + s + t \geq 1$.*

Provaremos inicialmente que subgrupos normais contidos em G^p são p-saturáveis.

Proposição 3.2.2. *Sejam G um PF-grupo e N um subgrupo fechado normal de G contido em G^p. Então existe uma filtration*

$$N = N_1 \geq N_2 \geq N_3 \dots$$

tal que $\bigcap_{i=1}^{\infty} N_1 = 1$ *e* $[N_i, N] \leq N_{i+1}^p$. *Em particular, N é um PF-grupo.*

Demonstração. Considere $M = \langle x \in G \mid x^p \in N \rangle$. Como $N \leq G^p$, então $N \leq M^p$. Por outro lado, $M/N\gamma_p(M)$ é um grupo regular gerado por elementos de ordem p. Daí, $(M/N\gamma_p(M))^p = 1$. E então $M^p \leq N\gamma_p(M)$.

Pelo teorema anterior, existe um subgrupo normal T de G que contém M e uma *potent filtration* $\{T_i\}$ de T que começa em T tal que $[T_i^p, T] = [M^p, T_i]$. Vamos começar provando que $[M^p, T_i] \leq [N, T_i]$. Pelo Lema 1.1.3,

$$\begin{aligned} [M^p, T_i] &\leq [N, T_i][\gamma_p(M), T_i] \leq [N, T_i][T_{i,p} M] \\ &\leq [N, T_i][T_{i+1}^p, T] \leq [N, T_i][M^p, T_{i+1}]. \end{aligned}$$

Repetindo esse argumento várias vezes, obtemos que para todo k, $[M^p, T_i] \leq [N, T_i][M^p, T_{i+k}]$. Logo, $[M^p, T_i] \leq [N, T_i]$. Então concluímos que

$$[N, N] \leq [M^p, M^p] \leq [T^p, T^p] \leq [M^p, T]^p \leq [N, T]^p$$

e

$$\begin{aligned} [[N, T_k], N] &\leq [M^p, T_k, M^p] \leq [[T^p, T_k], T^p] \\ &\leq [T_{k+1}^p, T]^p \leq [M^p, T_{k+1}]^p \leq [N, T_{k+1}]^p. \end{aligned}$$

Assim, $N \geq [N, T_1] \geq [N, T_2] \geq [N, T_3] \geq \dots$ satisfaz as conclusões do enunciado. $\square$

Para estender a proposição anterior para outros subgrupos normais, precisamos generalizar as definições de *potent filtrations* e PF-grupos. Para isso, sejam G um grupo pro-p, $1 \leq k \leq p-1$ e $m \geq 1$. Dizemos que um subgrupo normal N é *PF-imerso em G de tipo* (k, m) se existe uma série decrescente de subgrupos fechados normais com interseção trivial $\{N_i\}$ tal que $[N_{i,k} G] \leq N_{i+1}^{p^m}$. Assim, $\{N_i\}$ é uma *potent filtration de tipo* (k, m). E dizemos que um grupo pro-p G é um *PF-grupo de tipo* (k, m) se G é PF-imerso em G de tipo (k, m).

Teorema 3.2.3. *Sejam G um PF-grupo de tipo (k, m) e N um subgrupo fechado normal de G. Então existe um PF-subgrupo fechado de tipo (k, m) T de G que contém N tal que para* *todo subgrupo PF-imerso de tipo (k,m) M de T, temos $[M^{p^i},T^{p^j}]^{p^k} = [[M^{p^r},N^{p^s}]^{p^t}]$, sempre que $i+j+k = r+s+t \geq k$.*

Demonstração. A demonstração é a mesma do Teorema 3.2.1. $\square$

Lema 3.2.4. *Sejam G um PF-grupo de tipo (k,m) com $k+1 \leq p-1$ e N um subgrupo fechado normal de G. Então N é um PF-grupo de tipo $(k+1,m)$.*

Demonstração. Seja N um subgrupo normal de G. Pelo teorema anterior, existe um subgrupo T de G que contém N e uma *potent filtration* $\{T_i\}$ de tipo (k,m) que começa em T tal que $[T_i^{p^k},T] = [N,T_i]^{p^k}$. Então $[N,_{k+1}N] \leq [T_2^{p^k},T] = [N,T_2]^{p^k}$ e $[[N,T_i],_{k+1}N] \leq [T_{i+1}^{p^k},T] = [T_{i+1},N]^{p^k}$. Então

$$N \geq [N,T_2] \geq [N,T_3] \geq [N,T_4] \geq \dots$$

satisfaz as conclusões de uma *potent filtration* de tipo (k,m). $\square$

Corolário 3.2.5. *Sejam G um PF-grupo e N um subgrupo fechado normal de G contido em $\Phi(G)$. Então N é um PF-grupo.*

Demonstração. O caso em que $p=2$ segue da Proposição 3.2.2. Para $p \geq 3$, considere uma *potent filtration* $\{T_i\}$ que começa em G e $H_i = [T_i,G]T_i^p$. Então $[H_i,_{p-2}\Phi(G)] = [[T_i,G]T_i^p,_{p-2}\Phi(G)] \leq [[T_i,G],_{p-2}\Phi(G)][T_i^p,_{p-2}\Phi(G)]$. Como

$$[[T_i,G],_{p-2}\Phi(G)] \leq [T_i,_{p-1}G]^p[T_i,_pG] \leq (T_{i+1}^p)^p[T_{i+1},G]^p \leq H_{i+1}^p,$$

segue que $[H_i,_{p-2}\Phi(G)] \leq H_{i+1}^p$. Logo, $\Phi(G)$ é um PF-grupo de tipo $(p-2,1)$ e pelo lema anterior, N é um PF-grupo. $\square$

Agora podemos provar o resultado principal dessa seção com respeito a subgrupos normais de grupos p-saturáveis.

Teorema B. *Sejam G um grupo p-saturável e N um subgrupo fechado normal de G contido em $\Phi(G)$. Então N é p-saturável.*

Demonstração. Pelo corolário anterior, N é um PF-grupo. Como G é livre de torção e de posto finito, N é também livre de torção e finitamente gerado. Logo, pelo Teorema A, N é um grupo p-saturável. $\square$

Podemos ver a necessidade da hipótese de inclusão no exemplo a seguir.

Exemplo 3.2.6. *Sejam $A = \langle x_1, x_2, x_3 \rangle$ o produto direto de 3 cópias de $\mathbb{Z}_3$ e $B = \langle \alpha \rangle \cong \mathbb{Z}_3$. Considere agora o produto semidireto entre A e B dado pela ação*

$$\begin{aligned} x_1^{\alpha} &= x_1 x_2, \\ x_2^{\alpha} &= x_2 x_3^9, \\ x_3^{\alpha} &= x_3. \end{aligned}$$

Temos que $\gamma_3(G) \leq G^9$. Logo, G é um PF-grupo, pelo Corolário 3.1.12. Tome $N = \left\langle \alpha, x_1, x_2, x_3^9 \right\rangle$. N é um subgrupo normal de G, mas note que $\alpha^3 x_1^3$ não é uma 3-ésima potência em N, apenas em G, pois com a identidade $(xy)^n = x^n y^{x^{n-1}} \ldots y^x y$, mostramos que $\alpha^3 x_1^3 = (\alpha x_1 x_2^{-1} x_3^6)^3$ e pela Proposição 3.1.8, essa escrita é única. Daí, como $\alpha x_1 x_2^{-1} x_3^6 \notin N$, $\alpha^3 x_1^3$ não é uma 3-ésima potência em N. Logo, N não é um PF-grupo.

Capítulo 4

Grupos Analíticos Pro-p de Dimensões Pequenas

Entramos agora na relação entre grupos p-ádicos analíticos e p-saturáveis, resumida no Teorema C, que relembramos abaixo.

Teorema C. *Todo grupo pro-p p-ádico analítico livre de torção de dimensão menor que p é p-saturável. Por outro lado, existe um grupo pro-p p-ádico analítico livre de torção de dimensão p que não é p-saturável.*

4.1 Grupos Analíticos Pro-p de Dimensões Pequenas

Definimos o posto de um grupo pro-p G como $rk(G) = \sup\{d(H)|H \leq_a G\}$ e a dimensão de um grupo pro-p de posto finito G como $\dim(G) = d(H)$, onde H é um subgrupo aberto uniformemente *powerful* de G e $d(H)$ é o número de geradores de H ([1]). E dizemos que um grupo pro-p G tem coclasse r se existe $u \geq 2$ tal que $G/\gamma_u(G)$ tem coclasse r e $\gamma_i(G)/\gamma_{i+1}(G)$ tem ordem p para todo $i \geq u$; ou, equivalentemente, $G/\gamma_i(G)$ tem coclasse r para todo $i \geq u$. Assim, G é um grupo pro-p de coclasse r se for o limite inverso de p-grupos finitos de coclasse r.

Demonstraremos a primeira parte do Teorema C na forma do teorema abaixo.

Teorema 4.1. *Seja G um grupo pro-p livre de torção p-ádico analítico de dimensão menor que p. Então $\gamma_p(G) \subseteq \Phi(G)^p$. Em particular, G é um PF-grupo.*

Demonstração. Se $p = 2$, $\mathbb{Z}_2$ é o único grupo pro-p livre de torção 1-dimensional e a proposição é válida. Suponha $p \geq 3$. Pelo Corolário 3.1.12, a afirmação $\gamma_p(G) \subseteq \Phi(G)^p$, que vamos provar, implica que G é um PF-grupo. Suponha que G não seja trivial. Como

G é p-ádico analítico, existe um subgrupo próprio aberto normal N de G que é uniforme e portanto PF-grupo. Como G/N é um p-grupo finito, existe uma série finita cujos fatores são cíclicos de ordem p e argumentando por indução no comprimento dessa série, podemos supor $|G:N| = p$.

Como N é uniforme, temos $|N:N^p| = p^{dim(N)} = p^{dim(G)} \leq p^{p-1}$. O que mostra que $|G:N^p| \leq p^p$ e consequentemente, $\gamma_p(G) \subseteq N^p$.

Caso 1: Suponha que $\gamma_{p-1}(G) \subseteq N^p$. Então $\gamma_{p-1}(G) \subseteq G^p$ e a fórmula de Hall mostra que

$$\gamma_p(G) = [\gamma_{p-1}(G), G] \subseteq [G^p, G] \subseteq \gamma_{p+1}(G) \ (mod\ [G,G]^p).$$

Então, pelo Lema 3.1.9, tomando $N = \gamma_p(G)$ e $M = [G,G]^p$, temos $\gamma_p(G) \subseteq [G,G]^p \subset \Phi(G)^p$, como desejado.

Caso 2: Suponha que $\gamma_{p-1}(G) \nsubseteq N^p$. Então G/N^p é um p-grupo finito de classe maximal: G/N^p tem ordem p^p e classe de nilpotência $p-1$. Defina $N_1 := N$ e $N_i := \gamma_i(G)N^p$ para $i = 2, \ldots, p-1$. Então

$$G \supset N = N_1 \supset N_2 \supset \cdots \supset N_{p-1} \supset N^p$$

é uma série decrescente de subgrupos fechados normais tal que cada termo tem índice p no termo anterior. Mais ainda, todo subgrupo normal de G que está contido estritamente em N deve estar contido em $N_2 = \gamma_2(G)N^p$.

Primeiro suponha que $\gamma_p(G) \subsetneqq N^p$. O conjunto de elementos de ordem p no p-grupo regular $N/\gamma_p(G)$ forma um subgrupo. Daí, $M := \left\{x \in N | x^p \in \gamma_p(G)\right\}$ forma um subgrupo de G que, por suposição, está estritamente contido em N. Pela observação, M está então contido em N_2. Além disso, de acordo com a Proposição 3.1.6, item 4, temos $N^p = \{x^p | x \in N\}$ e então $M^p = \gamma_p(G)$. O que nos dá

$$\gamma_p(G) = M^p \subseteq N_2^p \subseteq \Phi(G)^p,$$

como desejado.

Afirmamos que o caso restante $\gamma_p(G) = N^p$ não ocorre. Por contradição, suponha $\gamma_p(G) = N^p$. Definimos recursivamente $N_i := N_{i-p+1}^p$ para $i \in \mathbb{N}$ com $i \geq p$. Note que $N_i = \gamma_i(G)$ para $i \in \{2, \ldots, p\}$.

Afirmação 1. N_i é PF-imerso em N para todo $i \in \mathbb{N}$.

Prova da afirmação 1. Isso é verdade para $i = 1$ pois $N = N_1$ é um PF-grupo e pela Proposição 3.1.6, item 3, é suficiente provar a afirmação para $i \in \{2, \ldots, p-1\}$. Tome i

nesse conjunto. Segue da Proposição 3.1.6, itens 2 e 5, que $[N^p,_{i-1}N] \subseteq \gamma_i(N)^p$. Isso dá

$$[N_i,_{p-1}N] = [\gamma_i(G),_{p-1}N] \subseteq [\gamma_p(G),_{i-1}N] = [N^p,_{i-1}N] \subseteq \gamma_i(N)^p.$$

Temos que $\gamma_i(N)$ é PF-imerso em N, então podemos completar a inclusão $N_i = \gamma_i(G) \supseteq \gamma_i(N)$ para uma *potent filtration* de N_i em N. Isso prova a afirmação.

Afirmação 2. $|N_i : N_{i+1}| = p$ para todo $i \in \mathbb{N}$.

Prova da afirmação 2. Isso está claro para $i \in \mathbb{N}$ com $i \leq p-1$. Agora seja $i \geq p$ e argumentaremos por indução. Pela afirmação 1, N_j é um PF-grupo para todo $j \in \mathbb{N}$; então a Proposição 3.1.6, item 4, mostra que $N_{j+p-1} = N_j^p = \{x^p | x \in N_j\}$. E conseguimos por indução que $|N_i : N_{i+1}| = |N_{i-p+1} : N_{i-p+2}| = p$.

Afirmação 3. $N_i = \gamma_i(G)$ para $i \in \mathbb{N}$ com $i \geq 2$.

Prova da afirmação 3. Seja $i \in \mathbb{N}$ com $i \geq 2$ e argumentemos por indução. Para $i \leq p$, a afirmação vale como mostrado acima. Suponha agora que $i > p$. Por indução, temos

$$N_i = N_{i-p+1}^p = \gamma_{i-p+1}(G)^p = [\gamma_{i-p}(G), G]^p = [N_{i-p}, G]^p$$

e similarmente $\gamma_i(G) = [\gamma_{i-1}, G] = [N_{i-1}, G] = [N_{i-p}^p, G]$. A fórmula de Hall nos dá $[N_{i-p}, G]^p \equiv [N_{i-p}^p, G]$ $(mod\ [G,_p N_{i-p}])$ (cf. [1.3.5]), então

$$N_i \equiv \gamma_i(G) \ \ (mod\ [G,_p N_{i-p}]).$$

Por indução, $[G,_p N_{i-p}] = [G,_p \gamma_{i-p}(G)] \subseteq \gamma_i(G)$. Novamente por indução e uma vez que N_{i-p+1} é PF-imerso em N, também obtemos

$$\begin{aligned}[G,_p N_{i-p}] &= [G, \gamma_{i-p}(G),_{p-1} N_{i-p}] \subseteq [\gamma_{i-p+1}(G),_{p-1} N] \\ &\subseteq [N_{i-p+1},_{p-1} N] \subseteq N_{i-p+2}^p = N_{i+1} \subseteq N_i.\end{aligned}$$

Então segue que $N_i = \gamma_i(G)$, como afirmamos.

As últimas duas afirmações mostram que G é um grupo pro-p de coclasse 1, pois $G/\gamma_2(G)$ tem coclasse 1 e $\gamma_i(G)/\gamma_{i+1}(G)$ tem ordem p para todo $i \geq 2$. Mas nesse caso, pelo Teorema de Blackburn, existe, nos grupos $G/\gamma_i(G)$, um elemento s, dito *uniforme*, tal que, pelo Teorema 3.15 de [2], $s^p \in Z(G/\gamma_i(G))$, para todo $i \geq 2$ e então G teria elementos de ordem p, uma contradição. □

Para mostrar que a hipótese do enunciado acima não pode ser expandida, trazemos um exemplo de um grupo pro-p p-ádico analítico livre de torção de dimensão p e que não é um PF-grupo.

Exemplo 4.2. *Sejam $M = \langle x_1, \dots, x_{p-1} \rangle \cong \mathbb{Z}_p^{p-1}$ um grupo pro-p abeliano livre de posto $p-1$ e $A = \langle \alpha \rangle \cong \mathbb{Z}_p$. Considere o produto semidireto $G := A \ltimes M$ com respeito à ação de A em M definida por*

$$x_i^\alpha = \begin{cases} x_i x_{i+1} & \textit{se } 1 \leq i \leq p-2, \\ x_{p-1} x_1^p & \textit{se } i = p-1. \end{cases}$$

G é um grupo pro-p p-ádico analítico livre de torção. Além disso, temos que $[M,_{p-1} G] = M^p$. Para uma contradição, suponha que G seja um PF-grupo e $\{G_i\}_{i \in \mathbb{N}}$ uma potent filtration de G. Então $M^p = [M,_{p-1} G] \subseteq [G,_{p-1} G] = [G_1,_{p-1} G] \leq G_2^p$ implica que $M \subseteq G_2$. Indutivamente, suponha que $M \subseteq G_i$. Então $M^p = [M,_{p-1} G] \subseteq [G_i,_{p-1} G] \leq G_{i+1}^p$, o que implica que $M \subseteq G_{i+1}$. Daí, $M \subseteq G_i$ para todo $i \in \mathbb{N}$. O que contradiz a propriedade de potent filtration de que $\cap G_i = 1$.

Do Teorema 4.1 e do Exemplo 4.2, segue diretamente o Teorema C.

Considerações Finais

No capítulo anterior vimos que um subgrupo fechado normal de um grupo p-saturável é também p-saturável se contido no subgrupo de Frattini do grupo. E ainda mostramos através de um contra-exemplo que sem a hipótese da inclusão, não é certo que o subgrupo será p-saturável. Nesse exemplo temos um grupo G pro-p de dimensão $p+1$ tal que $\gamma_p(G) \nsubseteq \Phi(G)$, mas não existem tais exemplos para dimensões menores ou iguais a p. De fato, o Teorema 4.1 implica que todo grupo G pro-p p-saturável de dimensão menor que p satisfaz $\gamma_p(G) \subseteq \Phi(G)^p$. Resta agora provar o caso em que $dim(G) = p$.

Proposição 4.3. *Todo grupo pro-p p-saturável de dimensão p satisfaz $\gamma_p(G) \subseteq \Phi(G)$.*

Demonstração. Considere o p-grupo finito $H := G/\Phi(G)^p \gamma_{p+1}(G)$. Por definição, esse é um PF-grupo de classe de nilpotência no máximo p e nosso objetivo é provar que $\gamma_p(H) = 1$.

Note que $|H : H^p| \leq |G : G^p| = p^{dim(G)} = p^p$. O que mostra que $\gamma_p(H) \subseteq H^p$. Suponhamos primeiramente que $|H : \Phi(H)| \geq p^3$. Como $\Phi(H) = \gamma_2(H)H^p$, deduzimos que $\gamma_{p-1}(H) \subseteq H^p$, e a Proposição 3.1.6 implica que

$$\gamma_p(H) = [\gamma_{p-1}(H), H] \subseteq [H^p, H] = [H, H]^p \subseteq \Phi(H)^p = 1,$$

como queríamos.

Agora suponhamos que $|H : \Phi(H)| = p^2$, ou seja, que H seja 2-gerado. Por contradição, assumimos que $\gamma_p(H) \neq 1$. Escolha $z \in \gamma_p(H) \setminus \{1\}$. Como $\gamma_p(H) \subseteq H^p$, a Proposição 3.1.6

mostra que
$$Y = \{y \in H | y^p = z\} \neq \emptyset.$$

Como $Y \cap \Phi(H) = \emptyset$, todo $y \in Y$ é parte de um par de geradores de H. A Proposição 3.1.6 mostra que $[H^p,_{p-1} H] \subseteq [H,H]^p \subseteq \Phi(H)^p = 1$, logo

$$[\Phi(H),_{p-1} H] \subseteq [H^p,_{p-1} H][[H,H],_{P-1} h] = \gamma_{p+1}(H) = 1.$$

Isso implica que $\gamma_p(H) = [y,_{p-1} H]$ para todo $y \in Y$.

Seja $(H_i)_{i\in\mathbb{N}}$ uma *potent filtration* de H. Para obter a contradição desejada, mostramos que $Y \cap H_i \neq \emptyset$ para todo $i \in \mathbb{N}$. Obviamente, isso vale para $i = 1$. Agora considere $i \geq 2$. Por indução, temos $y \in Y \cap H_{i-1}$ e então

$$z \in \gamma_p(H) = [y,_{p-1} H] \subseteq [H_{i-1},_{p-1} H] = H_i^p.$$

Daí, a Proposição 3.1.6 implica que $Y \cap H_i \neq \emptyset$. □

A respeito de grupos de dimensão p, temos ainda:

Proposição 4.4. *Todo subgrupo pro-p p-ádico analítico de dimensão p fechado de um grupo pro-p p-saturável é por sua vez p-saturável.*

Demonstração. Seja G um subgrupo de um grupo pro-p p-saturável S e suponha que $dim(G) \leq p$. Pela Proposição 3.2 de [6], podemos assumir que G tenha índice finito em S e por indução podemos ainda assumir que $|S : G| = p$. Pelo que vimos, $\gamma_p(S) \subseteq \Phi(S)^p$. Como vimos no Corolário 3.1.12, a p-série inferior

$$S_1 := S \text{ e } S_i := \overline{S_{i-1}^p[S_{i-1}, S]} \text{ para } i \geq 2.$$

é uma *potent filtration* de S. Note que $|S : G| = p$ implica que $S_2 = \Phi(S) \subseteq G$. Logo, $G \supset S_2 \supset S_3 \supset \ldots$ é uma *potent filtration* de G e G é p-saturável. □

Bibliografia

[1] Dixon, J., Du Sautoy, M., Mann, A., and Segal, D. (2003). *Analytic Pro-p Groups*. *Cambridge Studies in Advanced Mathematics. Cambridge University Press.*

[2] Fernández-Alcober, G. (2000). *An introduction to finite p-groups: regular p-groups and groups of maximal class*. *XVI Brazilian Algebra Meeting*.

[3] Fernández-Alcober, G., González-Sánchez, J., Jaikin-Zapirain, A. (2008). *Omega Subgroups of Pro-p Groups*. *Israel J. Math. in press*.

[4] González-Sánchez, J. (2007). *On p-saturable groups*. *Journal of Algebra*, 315(2):809 – 823.

[5] González-Sánchez, J., Jaikin-Zapirain, A. (2004). *On the structure of normal subgroups of potent p-groups*. *Journal of Algebra*, 276(1):193 – 209.

[6] González-Sánchez, J., Klopsch, B. (2009). *Analytic pro-p groups of small dimensions*. *Journal of Group Theory*, 12 (2009), 711 – 734.

[7] Kargapolov, M. I., Merzljakov, Ju. I. (1979). *Fundamentals of the theory of groups*. *Grad. Texts Math.*.

[8] Khukhro, E.I. (1998). *p-Automorphisms of Finite p-Groups*. *Cambridge Univ. Press*.

[9] Klopsch, B. (2007). *Five Lectures on Analytic Pro-p Groups: A Meeting-Ground Between Finite p-Groups and Lie Theory*. *University of Oxford*.

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

[11] Lazard, M. (1965). *Groupes analytiques p-adiques*. *Publ. Math. Inst. Hautes Études Sci.*, 26(1965):389 — 603.

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

[13] Ribes, L., Zalesskii, P. (2000). *Profinite Groups*. *Springer*.