Universidade de Brasília

Sobre endomorfismos virtuais de p-grupos finitos

Vítor Leite Antonelli

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 endomorfismos virtuais de p-grupos finitos

por

Vitor Leite Antonelli*

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

MESTRE EM MATEMÁTICA

Brasília, 12 de fevereiro de 2020.

Comissão Examinadora:

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

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

Prof. Dr. Adilson Antônio Berlatto – UFMT (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

AAN634s

Antonelli, Vítor Leite
Sobre endomorfismos virtuais de p-grupos finitos / Vítor Leite Antonelli; orientador Emerson Ferreira de Melo. -- Brasília, 2020.
104 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2020.

1. p-grupos finitos. 2. endomorfismos virtuais. 3. grupos self-similar. I. Melo, Emerson Ferreira de, orient. II. Título.

"A vida, no que tem de melhor, é um processo que flui, que se altera e onde nada está fixo."
(Carl Rogers)

Agradecimentos

Agradeço, primeiramente, à minha família, em especial aos meus pais e irmã, que nunca deixaram que eu conhecesse o que é não ter apoio.

Agradeço aos meus amigos Andresa, Bauer, Francês, Peixoto e Verônica, que sempre me deram amor, até mesmo em meus momentos de mais angústia.

Agradeço às meninas do apartamento 302, Gabi e Inah, cuja amizade me afastou da solidão nessa cidade de concreto.

Agradeço, também, aos amigos do grupo de cobre e da UFG, que, talvez sem perceberem, me alegraram mais dias do que consigo contar.

Agradeço à minha psicóloga, Líwia, cuja empatia me auxiliou muito no processo de tornar-me pessoa.

Agradeço aos meus colegas de mestrado, em especial à Edna, que de bom grado me ajudou todas as (muitas) vezes que precisei.

Agradeço ao meu orientador, Emerson Ferreira de Melo, por toda a sabedoria, paciência e dedicação.

Agradeço aos membros da banca, Adilson Antônio Berlatto e Alex Carrazedo Dantas, pelas correções e sugestões muito proveitosas à versão final desta dissertação.

Agradeço a todos os professores que fizeram parte da minha jornada acadêmica, em especial ao Durval José Tonon e ao Jhone Caldeira Silva, que, por serem tão incríveis e amarem tanto o que fazem, servem de inspiração a todos os seus alunos.

Por fim, agradeço ao CNPq, cujo financiamento tornou possível este e tantos outros trabalhos.

Resumo

Neste trabalho, estudamos, através dos resultados presentes nos artigos "*Finite self-similar p-groups with abelian first level stabilizers*" e "*On self-similar p-groups*", o seguinte problema: quais p-grupos finitos podem ser fielmente representados por um grupo *self-similar* de automorfismos da árvore p-ária, ou seja, quando um p-grupo finito é *self-similar*? Responderemos esta pergunta para o caso dos p-grupos finitos que possuem um subgrupo maximal abeliano e para o caso dos p-grupos de classe maximal. Também mostraremos que existem finitos p-grupos *self-similar* de um dado posto e, consequentemente, finitos p-grupos *self-similar* de uma dada coclasse. Além disso, determinaremos a melhor cota possível para a ordem de um p-grupo *self-similar* de classe maximal.

Palavras-Chave: p-grupos finitos; endomorfismos virtuais; grupos *self-similar*.

Abstract

In this work, we study, using the results presented in the articles "*Finite self-similar p-groups with abelian first level stabilizers*" and "*On self-similar p-groups*", the following question: which finite p-groups can be faithfully represented as a self-similar group of automorphisms of the p-ary tree, or, in other words, when is a finite p-group self-similar? We will answer this question for the case of finite p-groups whith an abelian maximal subgroup and for the case of p-groups of maximal class. We will also show that there are only finitely many self-similar p-groups of a given rank and, consequently, finitely many self-similar p-groups of a given coclass. Moreover, we will determine the best possible bound for the order of a self-similar p-group of maximal class.

Keywords: finite p-groups; virtual endomorphisms; self-similar groups.

Sumário

Nomenclatura

$\lvert G\rvert$	ordem de um grupo G.
$d(G)$	número mínimo de geradores do grupo G.
$\exp(G)$	expoente do grupo G.
$o(x)$	ordem de um elemento x de um grupo.
$\langle X\rangle$	subgrupo gerado pelos elementos do conjunto X.
$H < G$	H é subgrupo próprio do grupo G.
$[G:H]$	índice de H em G.
$G_1 \rtimes G_2$	produto semidireto de G_1 por G_2.
x^y	$y^{-1}xy$.
$[A_1,\ {}_n\, A_2]$	o comutador $[A_1, A_2, \cdots, A_2]$, onde A_2 aparece n vezes.
G'	o subgrupo comutador $[G,G]$ de G.
$\gamma_n(G)$	n-ésimo termo da série central inferior de G.
$\Omega_i(G)$	o subgrupo $\langle x \in G \mid x^{p^i} = 1\rangle$, onde G é um p-grupo.
$\Omega_{\{i\}}(G)$	o conjunto $\{x \in G \mid x^{p^i} = 1\}$, onde G é um p-grupo.
G^n	o subgrupo $\langle x^n \mid x \in G\rangle$.
$\Pi_i(G)$	subgrupo definido por $\Pi_0(G) = G$ e $\Pi_i(G) = \Pi_{i-1}(G)^p$, para $i \geq 1$, onde G é um p-grupo.
$Z(G)$	centro de G.
$C_G(H)$	centralizador de H em G.
$N_G(H)$	normalizador de H em G.
$\mathcal{L}(G)$	álgebra de Lie associada ao p-grupo de classe maximal G.
$\Phi(G)$	subgrupo de Frattini do grupo G.
N p.e. G	N é *powerfully embedded* em G.
N shp G	N é fortemente hereditariamente *powerful* em G.
$\mathbb{F}_p$	corpo com p elementos.
$GL_r(\mathbb{F}_p)$	grupo das matrizes $r \times r$ inversíveis com entradas em $\mathbb{F}_p$.
$U_r(\mathbb{F}_p)$	grupo das matrizes triangulares $r \times r$ com entradas em $\mathbb{F}_p$.

Introdução

Uma ação de um grupo G sobre uma árvore regular é dita *self-similar* se ela é transitiva no primeiro nível da árvore e se, dados g um elemento de G e v um vértice da árvore, temos que a secção g_v é, também, um elemento de G. De forma análoga, dizemos que um grupo G de automorfismos da árvore k-ária é *self-similar* se ele age transitivamente no primeiro nível e as seções de cada elemento do grupo em cada vértice da árvore pertence a G. Nas últimas décadas, os grupos que admitem uma ação fiel e *self-similar* sobre árvores regulares nos forneceram muitos exemplos importantes, tais como o primeiro grupo de Grigorchuk (encontrado em [11]), os p-grupos de Gupta-Sidki (encontrados em [12] e [13]), o grupo de Basilica (encontrado em [10] e [3]), dentre muitos outros.

Uma forma direta de mostrar que existe uma ação fiel e *self-similar* de um grupo G sobre uma árvore é construindo um grupo *self-similar* de automorfismos da árvore que é isomorfo a G. Esta técnica foi utilizada para criar uma ação *self-similar* fiel para grupos solúveis de Baumslag-Solitar (em [2]) e para grupos livres de posto finito (em [23], [24] e [21]). Uma abordagem mais organizada para este problema, porém, consiste no uso de endomorfismos virtuais, assunto principal desta dissertação.

Um $\frac{1}{k}$-endomorfismo virtual é um homomorfismo $\phi : H \to_k G$ tal que G é um grupo e H é um subgrupo de G de índice k. O *core* do endomorfismo virtual ϕ é o maior subgrupo ϕ-invariante normal em G contido em H, se o *core* de ϕ é trivial, dizemos que ϕ é simples. No quarto capítulo desta dissertação mostraremos que um grupo admite uma ação fiel *self-similar* transitiva no primeiro nível sobre a árvore k-ária se, e somente se, o mesmo admite um $\frac{1}{k}$-endomorfismo virtual simples. Endomorfismos virtuais foram usados, por exemplo, em [20], para construir ações de grupos abelianos livre sobre a árvore binária, e em [4], para construir ações de alguns grupos nilpotentes livres de torção.

Dados um grupo G e um primo p, a seguinte pergunta surge: G pode ser representado fielmente como um grupo de automorfismos da árvore p-ária? Se isso ocorre, dizemos que G é *self-similar* para o primo p. Nekrashevych e Sidki provaram, em [20], que todo grupo abeliano livre de posto finito é *self-similar* para o primo 2. Além disso, o estudo sobre grupos nilpotentes finitamente gerados livres de torção *self-similar* feito por Berlatto e Sidki em

[4] e o estudo sobre grupos abelianos *self-similar* feito por Brunner e Sidki em [5] possuem resultados muito importantes acerca deste problema. Nesta dissertação, trabalharemos com p-grupos finitos e nos basearemos, principalmente, nos artigos "*Finite self-similar p-groups with abelian first level stabilizers*" ([22]), de Z. Šunić, e "*On self-similar p-groups*" ([1]), de A. Babai, K. Fathalikhani, G. A. Fernández-Alcober e M. Vannacci.

A seguir, enunciamos um dos teoremas principais dos quais trataremos neste trabalho. Tal resultado caracteriza os p-grupos *self-similar* que possuem um subgrupo maximal abeliano.

Teorema A. Seja G um p-grupo finito que possui um subgrupo maximal abeliano. Então G é *self-similar* se, e somente se, G possui um subgrupo maximal abeliano elementar do qual G é uma extensão cindida.

O resultado acima foi demonstrado em [1] e é uma extensão do teorema principal do artigo [22]. Este último caracteriza os p-grupos *self-similar* que possuem um $\frac{1}{p}$-endomorfismo virtual simples cujo domínio é um subgrupo maximal abeliano.

O teorema que enunciaremos a seguir (demonstrado em [1]) nos dá que existem somente um número finito de p-grupos finitos *self-similar* de um dado posto. É possível mostrar que todo p-grupo finito pode ser fielmente representado como um grupo de automorfismos (não necessariamente *self-similar*) da árvore p-ária. Levando isto em consideração, o resultado a que nos referimos mostra que a existência de um $\frac{1}{p}$-endomorfismo virtual simples é uma forte condição a ser imposta.

Teorema B. Seja G um p-grupo finito *self-similar* de posto r. Então a ordem de G é limitada superiormente por uma função de p e r.

Como consequência, temos que a ordem de um p-grupo finito *self-similar* é, também, limitada por uma função do primo p e de sua coclasse, pois, como veremos a coclasse de um p-grupo é limitada pelo seu posto. No caso em que a coclasse do p-grupo analisado é 1, ou seja, no caso em que o p-grupo possui classe maximal, podemos conseguir informações mais detalhadas sobre sua estrutura e ordem. Nosso último teorema principal, enunciado a seguir, nos dá uma caracterização completa dos p-grupos *self-similar* de classe maximal e, também, a melhor cota superior possível para a ordem destes grupos. Este resultado foi demonstrado em [1].

Teorema C. Seja G um p-grupo de classe maximal. Então G é *self-similar* se, e somente se,

G possui um subgrupo maximal abeliano elementar do qual G é uma extensão cindida. Se este for o caso, então a ordem de G é menor ou igual a p^{p+1}.

Observe que, apesar de a maior parte dos p-grupos de classe maximal não possuírem subgrupos maximais abelianos, a caracterização obtida para os p-grupos *self-similar* de classe maximal é a mesma que obtivemos no Teorema A. Desta forma, vale, também, observar que o Teorema C nos fornece vários exemplos de p-grupos finitos que não podem ser fielmente representados por um grupo *self-similar* de automorfismos da árvore p-ária.

Neste trabalho, temos como objetivo principal a demonstração dos Teoremas A, B e C. Apesar disso, vários dos resultados apresentados nos capítulos 1, 2 e 3 não serão diretamente utilizados nas provas destes teoremas, mas julgamos que todos são necessários para a plena compreensão das demonstrações. Vale também ressaltar que, embora boa parte dos resultados contidos nos capítulos 4 e 5 não apresentem o termo "endomorfismo virtual"em seus enunciados, este tipo de endomorfismo nos forneceu as principais ferramentas utilizadas nas demonstrações.

No capítulo 1, trazemos resultados preliminares da teoria de grupos e da teoria de p-grupos. Os resultados presentes nas duas primeiras seções são bem conhecidos e, por isso, tiveram suas provas omitidas. Na terceira e última seção do capítulo, tratamos dos p-grupos de classe maximal e trazemos os conceitos e resultados necessários para a demonstração do Teorema C.

O segundo capítulo destina-se ao estudo de p-grupos *powerful*. Ele inicia-se com a apresentação dos conceitos e propriedades básicas deste tipo de grupo e finaliza-se com um estudo mais aprofundado sobre o tópico. Na última seção do capítulo trazemos resultados específicos que serão utilizados na demonstração do Teorema B.

O capítulo 3 tem como objetivo principal a demonstração de teoremas que nos ajudarão a mostrar, a partir do Teorema B, que existem finitos p-grupos *self-similar* de uma determinada coclasse. Para isso, estudaremos ações uniseriais, subgrupos hereditariamente fortemente *powerful* e alguns resultados específicos sobre coclasse de p-grupos.

No quarto capítulo adentramos, de fato, nas teorias de endomorfismos virtuais e de p-grupos *self-similar*. Nele, estudamos os resultados trazidos por Šunić em [22] e alguns resultados de [1], incluindo o nosso primeiro teorema principal, o Teorema A.

Por fim, no quinto capítulo, trazemos mais alguns resultados encontrados em [1]. Na primeira seção, nos destinamos à demonstração do Teorema B e algumas de suas consequências. Já na segunda seção, passamos a estudar p-grupos *self-similar* de classe maximal, finalizando este trabalho com a prova do Teorema C.

Capítulo 1

Preliminares

1.1 Teoria de grupos

A maior parte da teoria presente nesta seção pode ser encontrada em [9] e em [7]. Iniciamos com alguns resultados e definições básicas a respeito de comutadores.

Dado G um grupo qualquer, definimos o comutador de dois elementos $x, y \in G$ como:

$$[x,y] = x^{-1}y^{-1}xy = x^{-1}x^{y}.$$

Note, portanto, que x e y comutam se, e somente se, $[x,y] = 1$. Definimos o comutador de comprimento $n > 2$ dos elementos $x_1, x_2, x_3, \cdots, x_n \in G$ como:

$$[x_1, x_2, \cdots, x_n] = [\cdots [[x_1, x_2], x_3], \cdots, x_n].$$

Dados dois subgrupos H e K de G, definimos, também, o comutador de H e K:

$$[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle,$$

e dados $n > 2$ subgrupos $H_1, H_2, H_3, \cdots, H_n \leq G$, definimos o comutador de comprimento n $[H_1, H_2, H_3, \cdots, H_n]$ de forma similar ao definido anteriormente para elementos de G. Denotamos por G' o subgrupo $[G,G]$. Dados $x_1, x_2 \in G$ e $H_1, H_2 \leq G$, denotaremos os comutadores de comprimento $n+1$ $[x_1, x_2, x_2, \cdots, x_2]$ e $[H_1, H_2, H_2, \cdots, H_2]$ por $[x_1, {}_n\, x_2]$ e $[H_1, {}_n\, H_2]$, respectivamente.

O teorema a seguir apresenta algumas propriedades básicas de comutadores.

Teorema 1.1.1. Sejam G um grupo, $x, y, z \in G$ e $H, K, L \leq G$. Então:

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

(ii) $\sigma([x,y]) = [\sigma(x),\sigma(y)]$, para todo homomorfismo $\sigma : G \to G$.

(iii) $[xy,z] = [x,z][x,z,y][y,z]$ e $[x,yz] = [x,z][x,y][x,y,z]$.

(iv) $[x,y^{-1},z]^y[y,z^{-1},x]^x[z,x^{-1},y]^x = 1$. (Identidade de Witt)

(v) K normaliza H se, e somente se, $[H,K] \leq H$. K centraliza H se, e somente se, $[H,K] = 1$.

(vi) $[H,K] = [K,H]$.

(vii) $\sigma([H,K]) = [\sigma(H),\sigma(K)]$, para todo homomorfismo $\sigma : G \to G$.

(viii) Se N é um subgrupo normal de G, então $[{}^{HN}\!/_{N}, {}^{KN}\!/_{N}] = {}^{[H,K]N}\!/_{N}$.

(ix) Se HK é um subgrupo de G e H normaliza L, então $[HK,L] = [H,L][K,L]$.

(x) $G' \leq H$ se, e somente se, H é normal e ${}^{G}\!/_{H}$ é abeliano.

(xi) Se N é um subgrupo normal de G tal que ${}^{G}\!/_{N}$ é cíclico, então $G' = [G,N]$.

O corolário seguinte pode ser encontrado no primeiro capítulo de [17].

Corolário 1.1.2. Sejam G um grupo, $x,y \in G$ e n um inteiro positivo, então:

$$[x,y^n] \equiv [x,y]^n[x,\ {}_2\ y]^{\binom{n}{2}}[x,\ {}_3\ y]^{\binom{n}{3}} \cdots [x,\ {}_n\ y] \mod N,$$

onde N é o fecho normal em G do grupo gerado pelo conjunto de todos os comutadores $[z_1,z_2,\cdots,z_m]$ de $\{y,[x,y]\}$ tais que $z_i = [x,y]$ para pelo menos dois valores de i.

O próximo teorema é um resultado clássico na teoria de grupos e é chamado de Lema dos Três Subgrupos.

Teorema 1.1.3 (Lema dos Três Subgrupos)**.** Sejam G um grupo, H, K e L subgrupos de G e N um subgrupo normal de G. Se $[H,K,L],[K,L,H] \leq N$, então $[L,H,K] \leq N$.

Definimos a série central inferior de um grupo G indutivamente, da seguinte forma:

$$\gamma_1(G) = G \text{ e } \gamma_{i+1}(G) = [\gamma_i(G),G].$$

Note que, pelo item (vii) do Teorema 1.1.1, temos que $\gamma_i(G)$ é característico em G para todo i. A seguir temos algumas propriedades dos subgrupos $\gamma_i(G)$.

Teorema 1.1.4. Dado um grupo G, temos $[\gamma_i(G),\gamma_j(G)] \leq \gamma_{i+j}(G)$.

Corolário 1.1.5. Sejam G um grupo e $x_1, x_2, \cdots, x_i$ elementos de G, então $[x_1, x_2, \cdots, x_i] \in \gamma_i(G)$.

Corolário 1.1.6. Sejam G um grupo e N um subgrupo normal de G. Então, para todo $i \geq 1$, temos $\gamma_i({}^{G}\!/_{N}) = {}^{\gamma_i(G)N}\!/_{N}$.

Proposição 1.1.7. Seja G um grupo tal que ${}^{G}\!/_{G'} = \langle x_1G', \cdots x_sG' \rangle$ e ${}^{\gamma_i(G)}\!/_{\gamma_{i+1}(G)} = \langle y_1\gamma_{i+1}(G), \cdots, y_t\gamma_{i+1}(G) \rangle$. Então:

$$ {}^{\gamma_{i+1}(G)}\!/_{\gamma_{i+2}(G)} = \langle [x_j, y_k]\gamma_{i+2}(G) \mid j = 1, \cdots, s \ , \ k = 1, \cdots, t \rangle. $$

Proposição 1.1.8. Seja G um grupo. Se todo elemento de ${}^{\gamma_i(G)}\!/_{\gamma_{i+1}(G)}$ possui ordem divisível por n, então o mesmo vale para os elementos dos quocientes ${}^{\gamma_j(G)}\!/_{\gamma_{j+1}(G)}$, com $j \geq i$.

Dizemos que um grupo G é nilpotente se $\gamma_{c+1}(G) = 1$, para algum inteiro c. O menor valor de c tal que isso aconteça é chamado de classe de nilpotência de G.

Dado um grupo finitamente gerado G, denotamos por $d(G)$ o menor número de elementos necessário para gerar G.

Definição 1.1.9. Seja G um grupo finito, o posto de G é o inteiro $\max\{d(H) \mid H \leq G\}$.

O resultado a seguir pode ser encontrado em [15].

Proposição 1.1.10. Se um grupo G é gerado por d elementos, então, para todo inteiro n, ${}^{\gamma_n(G)}\!/_{\gamma_{n+1}(G)}$ é gerado por no máximo d^n elementos.

Corolário 1.1.11. Se um grupo nilpotente G é gerado por d elementos e tem classe de nilpotência c, então o posto de G é no máximo $d + d^2 + \cdots d^{c-1} + d^c$.

Uma ação de um grupo G sobre um conjunto A é um mapeamento

$$ \begin{aligned} f : G \times A &\to A \\ (g, a) &\mapsto g(a) \end{aligned} $$

tal que:

(i) para todo $a \in A$, temos $e(a) = a$, onde e é a identidade de G;

(ii) para todo $h, g \in G$ e $a \in A$, temos $g(h(a)) = (gh)(a)$.

Se G e H são grupos, para dizermos que G age sobre H, acrescentamos mais uma condição:

$$g(h_1h_2) = g(h_1)g(h_2), \text{ para todo } h_1, h_2 \in H \text{ e } g \in G.$$

A seguir trazemos algumas definições básicas a respeito de ações de grupos que serão utilizadas nesta dissertação.

Definição 1.1.12. A ação de um grupo G sobre um conjunto A é denominada fiel se apenas o elemento neutro de G age trivialmente sobre A.

Definição 1.1.13. Dada uma ação de um grupo G sobre um conjunto A, o estabilizador de um elemento $a \in A$ é o conjunto:

$$G_a = \{g \in G \mid g(a) = a\}.$$

Definição 1.1.14. Sejam G e H grupos com G agindo sobre H e sejam $g \in G$ e $h \in H$, então, definimos:

(i) $[h,g] = h^{-1}g(h)$;

(ii) $[H,G] = \langle [h,g] \mid h \in H, g \in G \rangle$.

Definição 1.1.15. Sejam G e H grupos com G agindo sobre H e seja K um subgrupo de H. Dizemos que K é G-invariante se $[K,G] \leq K$.

Para finalizarmos esta seção, trataremos do tema "extensão de grupos". Temos o objetivo de introduzir o conceito de extensão cindida (também conhecida como extensão *split*). Este conteúdo pode ser encontrado no capítulo 10 de [14].

Definição 1.1.16. Uma extensão de um grupo A por um grupo G é um grupo $\tilde{G}$ que possui um subgrupo normal N tal que:

$$A \cong N \ , \ \tilde{G}/N \cong G.$$

Portanto, dado um monomorfismo $\iota : A \to \tilde{G}$ tal que $\mathrm{Im}\iota \trianglelefteq \tilde{G}$, temos que $\tilde{G}$ é uma extensão de A por $\tilde{G}/\mathrm{Im}\iota$ e, dado um epimorfismo $\nu : \tilde{G} \to G$, temos que $\tilde{G}$ é uma extensão de $\ker\nu$ por G. Supondo que $\tilde{G}$ é uma extensão de A por G, existem isomorfismos $\alpha : A \to N$ e $\beta : \tilde{G}/N \to G$, podemos, então, denotar ι e ν pelas composições:

$$A \xrightarrow{\alpha} N \xrightarrow{\text{inc}} \tilde{G} \ , \ \tilde{G} \xrightarrow{\text{nat}} \tilde{G}/N \xrightarrow{\beta} G,$$

respectivamente. Logo, temos ι e ν tais que $\ker\iota = 1$, $\mathrm{Im}\iota = N = \ker\nu$ e $\mathrm{Im}\nu = G$. Isto nos motiva a criar a seguinte definição:

Definição 1.1.17. A sequência

$$A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-2}} A_{n-1} \xrightarrow{\alpha_{n-1}} A_n$$

de grupos e homomorfismos é dita exata se, para todo i tal que $1 \leq i \leq n-1$, temos $\mathrm{Im}\alpha_{i-1} = \ker\alpha_i$.

Note que, no caso em que A_0 e A_n são triviais e $n = 4$, a sequência:

$$1 \to A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} A_3 \to 1$$

é exata se, e somente se, $\ker\alpha_1 = 1$, $\mathrm{Im}\alpha_1 = \ker\alpha_2$ e $\mathrm{Im}\alpha_2 = A_3$. Neste caso, a sequência acima é chamada de sequência exata curta. Temos, então, o seguinte resultado:

Proposição 1.1.18. O grupo $\tilde{G}$ é uma extensão de A por G se, e somente se, existe uma sequência exata curta

$$1 \to A \xrightarrow{\iota} \tilde{G} \xrightarrow{\nu} G \to 1.$$

Desta forma, sempre podemos ver uma extensão como uma sequência exata curta, e vice-versa. Definimos, agora, uma extensão cindida.

Definição 1.1.19. Uma extensão

$$1 \to A \xrightarrow{\iota} \tilde{G} \xrightarrow{\nu} G \to 1$$

é dita uma extensão cindida se existe um homomorfismo $\sigma : G \to \tilde{G}$ tal que $\nu\sigma$ é a função identidade de G. Nesse caso, σ é chamado de cisão.

Finalizamos esta seção com um resultado que nos permite entender melhor o que é uma extensão cindida.

Proposição 1.1.20. O grupo $\tilde{G}$ é uma extensão cindida de A por G se, e somente se, $\tilde{G}$ é um produto semi-direto $A \rtimes G$.

1.2 Teoria de p-grupos

Dado um número primo p, um p-grupo é um grupo tal que cada um de seus elementos possui como ordem uma potência de p. Podemos, portanto, definir um p-grupo finito como um

grupo finito cuja ordem é uma potência de p. Este tipo de grupo será o foco do restante desta dissertação. Iniciamos com alguns resultados básicos.

Teorema 1.2.1. Sejam G um p-grupo e N um subgrupo normal não trivial de G. Então $N \cap Z(G) \neq 1$. Em particular, o centro de um p-grupo não trivial é não trivial.

Teorema 1.2.2. Sejam G um p-grupo e M um subgrupo maximal de G, então $M \trianglelefteq G$ e $[G : M] = p$.

Teorema 1.2.3. Seja G um p-grupo finito de ordem p^m. Então:

(i) Se N é um subgrupo normal de G de ordem p^k, então existe uma série:

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = N \leq \cdots \leq G_m = G$$

tal que $G_i \trianglelefteq G$ e $[G_{i+1} : G_i] = p$, para todo i. Em particular, um p-grupo possui subgrupos normais de todas as ordens possíveis.

(ii) Seja H um subgrupo de G de ordem p^k, então existe uma série:

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = H \leq \cdots \leq G_m = G$$

tal que $G_i \trianglelefteq G_{i+1}$ e $[G_{i+1} : G_i] = p$, para todo i.

Teorema 1.2.4. Seja G um p-grupo de ordem $p^m \geq p^2$. Então:

(i) G é nilpotente.

(ii) A classe de nilpotência de G é no máximo $m-1$.

(iii) $[G : G'] \geq p^2$.

Corolário 1.2.5. Sejam G um p-grupo e N um subgrupo normal de G com índice $p^i \geq p^2$. Então $\gamma_i(G) \leq N$.

O Teorema 1.2.4 nos motiva à seguinte definição:

Definição 1.2.6. Dizemos que um p-grupo de ordem $p^m \geq p^2$ é de classe maximal se o mesmo possui classe de nilpotência $m-1$.

Este tipo de p-grupo será o assunto da próxima seção deste capítulo. Seguimos com mais uma definição de fundamental importância e que será frequentemente utilizada no decorrer desta dissertação.

Definição 1.2.7. Seja G um p-grupo e i um inteiro não negativo qualquer. Definimos:

(i) $G^{p^i} = \langle x^{p^i} \mid x \in G \rangle$.

(ii) $\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1 \rangle$.

Se G é um grupo finito, definimos o Subgrupo de Frattini de G como a interseção de todos os subgrupos maximais de G e o denotamos por $\Phi(G)$. Como a imagem de um subgrupo maximal por um automorfismo é, também, um subgrupo maximal, temos que $\Phi(G)$ é um subgrupo característico. O Subgrupo de Frattini terá grande importância nesta dissertação devido, principalmente, aos próximos dois teoremas:

Teorema 1.2.8. Sejam G um p-grupo finito e $x_1, x_2, \cdots, x_d$ elementos de G. Então $G = \langle x_1, x_2, \cdots, x_d \rangle$ se, e somente se, $G/\Phi(G) = \langle x_1\Phi(G), x_2\Phi(G), \cdots, x_d\Phi(G) \rangle$.

Teorema 1.2.9 (Teorema da Base de Burnside)**.** Seja G um p-grupo finito. Então:

(i) $G/\Phi(G)$ é um p-grupo abeliano elementar e, consequentemente, pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$. Além disso, $\Phi(G) = G'G^p$.

(ii) O conjunto $\{x_1, \cdots, x_d\}$ é um conjunto minimal gerador de G se, e somente se, $\{x_1\Phi(G), \cdots, x_d\Phi(G)\}$ é uma base de $G/\Phi(G)$.

(iii) A dimensão do espaço vetorial $G/\Phi(G)$ é $d(G)$, ou seja, $[G : \Phi(G)] = p^{d(G)}$.

A fórmula presente no resultado a seguir é chamada de Fórmula de Compilação de Hall. O próximo teorema trará, também, uma segunda versão da fórmula de Hall feita para p-grupos. Ambas as versões serão muito utilizadas neste trabalho.

Teorema 1.2.10 (Fórmula de Compilação de Hall)**.** Sejam G um grupo e $x, y \in G$. Então existem elementos $c_i = c_i(x,y) \in \gamma_i(\langle x, y \rangle)$ tais que:

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \cdots c_n^{\binom{n}{n}},$$

para todo inteiro positivo n.

Além disso, se G é um p-grupo e i é um inteiro, então:

$$(xy)^{p^i} \equiv x^{p^i} y^{p^i} \mod \gamma_2(H)^{p^i} \gamma_p(H)^{p^{i-1}} \cdots \gamma_{p^i}(H),$$

onde $H = \langle x, y \rangle$.

Teorema 1.2.11. Sejam G um grupo e $x,y \in G$. Se p é um primo, então os elementos $c_p = c_p(x,y)$ da Fórmula de Compilação de Hall satisfazem a seguinte congruência:

$$c_p \equiv [y,\ {}_{p-1}\ x]^a \prod_i v_i^{a_i} \mod \gamma_{p+1}(\langle x,y\rangle),$$

onde $a \equiv -1 \mod p$, a_i são inteiros e cada v_i é um comutador da forma $[y,x,z_3,\cdots,z_p]$ tal que $z_j \in \{x,y\}$ para todo j e $z_j = y$ para pelo menos um valor de j.

A seguir definiremos p-grupos regulares.

Definição 1.2.12. Seja G um p-grupo finito. Dizemos que G é um p-grupo regular se $x^p y^p \equiv (xy)^p \mod (\langle x,y\rangle')^p$ para todo $x,y \in G$.

Note, portanto, que, pela Fórmula de Compilação de Hall, a definição acima é equivalente a:

$$c_p(x,y) \in (\langle x,y\rangle')^p, \text{ para todo } x,y \in G.$$

Finalizamos esta seção com alguns resultados a respeito de p-grupo regulares.

Teorema 1.2.13. Seja G um p-grupo finito.

(i) Se a classe de nipotência de G é menor que p, então G é regular. Em particular, qualquer p-grupo de ordem menor ou igual a p^p é regular.

(ii) Se $\gamma_{p-1}(G)$ é cíclico, então G é regular. Em particular, se $p > 2$ e G' é cíclico, então G é regular.

(iii) Se G é um 2-grupo regular, então G é abeliano.

Teorema 1.2.14. Seja G um p-grupo regular e seja $i \geq 0$ um inteiro qualquer. Então:

(i) Dados $x,y \in G$ quaisquer, temos $x^{p^i} = y^{p^i}$ se, e somente se, $(x^{-1}y)^{p^i} = 1$.

(ii) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(iii) $G^{p^i} = \{x^{p^i} \mid x \in G\}$.

(iv) $[G : \Omega_i(G)] = |G^{p^i}|$ (e, consequentemente, $[G : G^{p^i}] = |\Omega_i(G)|$).

Corolário 1.2.15. Se um p-grupo regular G é gerado por elementos de ordem menor ou igual a p^e, então $\exp G \leq p^e$.

Teorema 1.2.16. Seja G um p-grupo tal que todos os seus subgrupos próprios são regulares e sejam M e N subgrupos normais de G. Então:

$$[M^{p^i}, N^{p^j}] = [M,N]^{p^{i+j}},$$

para todo $i, j \geq 0$.

Teorema 1.2.17. Se G é um p-grupo tal que $[G : G^p] \leq p^{p-1}$, então G é regular.

1.3 p-Grupos de classe maximal

Esta seção final de nosso capítulo preliminar dirá respeito a p-grupos de classe maximal (definidos na Definição 1.2.6). A teoria aqui presente pode ser encontrada em [7]. Nesta seção, definiremos os chamados centralizadores de 2-passos, i.e. os subgrupos maximais $C_G(\gamma_i(G)/\gamma_{i+2}(G)) = \{x \in G \mid [x, \gamma_i(G)] \leq \gamma_{i+2}(G)\}$. Introduziremos, também, a notação $G_0 = G$, $G_1 = C_G(\gamma_2(G)/\gamma_4(G))$ e $G_i = \gamma_i(G)$, para $i \geq 2$. Um dos objetivos principais desta seção é mostrar que todo grupo de classe maximal possui elementos uniformes, ou seja, elementos de ordem menor ou igual a p^2 que não estão contidos em nenhum centralizador de 2-passos.

Iniciamos com o seguinte resultado:

Teorema 1.3.1. Seja G um p-grupo de classe maximal de ordem p^m. Então:

(i) $|G : G'| = p^2$ e $[\gamma_i(G) : \gamma_{i+1}(G)] = p$, para $2 \leq i \leq m-1$. Portanto, $[G : \gamma_i(G)] = p^i$, para $2 \leq i \leq m-1$.

(ii) A menos que G seja cíclico de ordem p^2, temos $\Phi(G) = G'$ e $d(G) = 2$.

(iii) Os únicos subgrupos normais de G são os subgrupos $\gamma_i(G)$ e os subgrupos maximais. Isto é, se N é um subgrupo normal de G de índice $p^i \geq p^2$, então $N = \gamma_i(G)$.

(iv) Se N é um subgrupo normal de G de índice maior ou igual a p^2, então G/N é, também, de classe maximal.

Demonstração.

(i) Temos $p^m = |G| = [G : G'] \prod_{i=2}^{m-1} [\gamma_i(G) : \gamma_{i+1}(G)]$. Note, porém, que $[\gamma_i(G) : \gamma_{i+1}(G)] \geq p$, para $2 \leq i \leq m-1$, e que, pelo Teorema 1.2.4, $[G : G'] \geq p^2$.

(ii) Sabemos que $G' \leq \Phi(G)$, donde, pelo item (i) deste teorema, temos $[G : \Phi(G)] \leq p^2$. Se $[G : \Phi(G)] = p$, então $G/\Phi(G)$ é cíclico, donde G é cíclico e, portanto, de ordem p^2. Caso contrário, $[G : \Phi(G)] = p^2$, nesse caso G não pode ser cíclico (pois sua ordem é maior que p^2), donde $d(G) = d(G/\Phi(G)) = 2$.

(iii) Seja N um subgrupo normal em G e seja p^i, com $0 \leq i \leq m$, o índice de N em G. Se $i = 0$, então $N = G = \gamma_1(G)$, e, se $i = 1$, então N é maximal em G. Por outro lado, se $i \geq 2$, então, pelo Corolário 1.2.5, temos $\gamma_i(G) \leq N$. Como $[G : \gamma_i(G)] = p^i$, temos $N = \gamma_i(G)$.

(iv) Como $G/\gamma_i(G)$ tem classe $i-1$, para $2 \leq i \leq m$, temos, pelos itens (i) e (iii) deste teorema, o resultado desejado.

□

Todo grupo de ordem p^2 é abeliano e, portanto, isomorfo a C_{p^2} ou a $C_p \times C_p$. Sabemos que se $p = 2$, os grupos de ordem p^3 não abelianos são isomorfos a D_8 ou a Q_8. Além disso, se p é ímpar, então os grupos não abelianos desta ordem são isomorfos a $M_{p^3} = \langle a, b \mid a^{p^2} = b^p = 1, a^b = a^{1+p} \rangle$ ou a $E_{p^3} = \langle a, b, c \mid a^p = b^p = c^p, a^c = ab, [a,b] = [b,c] = 1 \rangle$. Portanto, os grupos de ordem p^3 são, também, bem conhecidos. Desta forma, nesta seção trabalharemos somente com os p-grupos de ordem maior ou igual a p^4.

No decorrer desta seção utilizaremos a seguinte notação:

$$G_0 = G \text{ e } G_i = \gamma_i(G), \text{ para } i \geq 2.$$

A próxima definição nos dá um subgrupo característico maximal que desempenhará função fundamental na teoria de p-grupos de classe maximal:

Definição 1.3.2. Seja G um p-grupo de classe maximal de ordem p^m. Definimos $G_1 = C_G(G_2/G_4)$ (o centralizador da ação de G sobre G_2/G_4 induzida pela conjugação). Em outras palavras, G_1 é composto pelos elementos $x \in G$ tais que $[x, G_2] \leq G_4$.

Teorema 1.3.3. Seja G um p-grupo de classe maximal. Então G_1 é um subgrupo maximal característico de G.

Demonstração. Tome $f \in \mathrm{Aut}(G)$. Como G_2 e G_4 são subgrupos característicos de G, dado $x \in G_1$, temos:

$$[f(x), G_2] = [f(x), f(G_2)] = f([x, G_2]) \leq f(G_4) = G_4.$$

Portanto, G_1 é característico.

Por outro lado, G_1 é o núcleo da ação de G sobre G_2/G_4, desta forma, o grupo G/G_1 pode ser visto como um subgrupo de $\mathrm{Aut}(G_2/G_4)$. Como $[G_2 : G_4] = p^2$, temos $G_2/G_4 \cong C_{p^2}$ ou $G_2/G_4 \cong C_p \times C_p$. No primeiro caso, temos $|\mathrm{Aut}(G_2/G_4)| = p(p-1)$ e, no segundo, temos $|\mathrm{Aut}(G_2/G_4)| = (p^2-1)(p^2-p)$. De qualquer forma, a maior potência de p que divide $|\mathrm{Aut}(G_2/G_4)|$ é p, donde $[G : G_1] \leq p$. Se $G_1 = G$, temos $G_3 = [G, G_2] = [G_1, G_2] \leq G_4$, logo $G_3 = 1$ e temos uma contradição, pois G é um p-grupo de classe maximal com ordem maior ou igual a p^4. Portanto $[G : G_1] = p$.

□

Vimos, no Teorema 1.1.4, que, dados $i, j \geq 1$, $[G_i, G_j] \leq G_{i+j}$. Nada impede, porém, que $[G_i, G_j]$ esteja contido num subgrupo G_{i+j+k}, para algum $k \geq 1$. Desta forma, a seguinte definição faz sentido:

Definição 1.3.4. Seja G um p-grupo de classe maximal. Definimos o grau de comutatividade de G, denotado por $l(G)$ ou simplesmente l, como:

$$l(G) = \max\{k \leq m-2 \mid [G_i, G_j] \leq G_{i+j+k}, \text{ para todo } i, j \geq 1\}.$$

O resultado a seguir é imediato.

Teorema 1.3.5. Seja G um p-grupo de classe maximal de ordem p^m e seja N um subgrupo normal de G de ordem $p^t \leq p^{m-4}$ (donde $|G/N| \geq p^4$). Então, $l(G/N) = m-t-2$ ou $l(G/N) \geq l(G)$.

A seguir definiremos o que é uma álgebra de Lie e, então, construiremos uma álgebra desse tipo associada a um grupo de classe maximal qualquer. As álgebras de Lie associadas a um grupo podem ser poderosas ferramentas, uma vez que por vezes podemos utilizar a álgebra e suas propriedades na demonstração de resultados a respeito do grupo.

Definição 1.3.6. Seja L um espaço vetorial sobre o corpo F dotado da operação $[\ ,\ ] : L \times L \to L$. Dizemos que L é uma álgebra de Lie se as seguintes condições são satisfeitas:

(i) $[\ ,\ ]$ é bilinear, isto é: $[x+y, z] = [x, z] + [y, z]$, $[x, y+z] = [x, y] + [x, z]$ e $\alpha[x, y] = [\alpha x, y] = [x, \alpha y]$, para todo $x, y, z \in L$ e $\alpha \in F$.

(ii) $[x, x] = 0$, para todo $x \in L$.

(iii) A identidade de Jacobi é satisfeita, isto é: $[x, y, z] + [y, z, x] + [z, x, y] = 0$, para todo $x, y, z \in L$.

Dado um grupo G qualquer, costumamos definir uma álgebra de Lie $L(G)$ utilizando o produto $[xG_{i+1}, yG_{j+1}] = [x,y]G_{i+j+2}$, para $i, j \geq 0$. Esta álgebra é uma ferramenta de extrema importância que pode nos ajudar a demonstrar inúmeros resultados da teoria de grupos. Se G é um p-grupo de classe maximal, é possível definir uma álgebra de Lie mais específica associada a ele. Para isto, construiremos um produto $[\ ,\ ]$ que leva em consideração o grau de comutatividade do grupo. Definimos a álgebra de Lie associada a um p-grupo G de classe maximal e ordem p^m como o conjunto $\mathcal{L}(G) = \oplus_{i\geq 0}\mathcal{L}_i$, onde $\mathcal{L}_i = {}^{G_i}\!/_{G_{i+1}}$, dotado de uma adição $+$ tal que $xG_{i+1} + yG_{i+1} = xyG_{i+1}$, para todo $x, y \in G_i$, e de um produto $[\ ,\ ]$ tal que, dados $x \in G_i$ e $y \in G_j$:

$$[xG_{i+1}, yG_{j+1}] = \begin{cases} [x,y]G_{i+j+2}, & \text{se } i = 0 \text{ ou } j = 0 \\ [x,y]G_{i+j+l+1}, & \text{se } i, j \geq 1, \end{cases}$$

onde $l = l(G)$ é o grau de comutatividade de G. Note que, se $a \in \mathcal{L}(G)$, então $pa = 0$, donde $\mathcal{L}(G)$ é uma álgebra de Lie de dimensão m sobre $\mathbb{F}_p$.

Dado um p-grupo G de classe maximal, já temos $G_1 = C_G(G_2/G_4)$. De forma mais geral, definimos:

Definição 1.3.7. Seja G um p-grupo de classe maximal e ordem p^m, os subgrupos $C_G(G_i/G_{i+2})$, com $1 \leq i \leq m-2$ são denominados centralizadores de 2-passos.

Assim como o subgrupo G_1, os demais centralizadores de 2-passos são subgrupos característicos e maximais de G, pois são os centralizadores de uma ação de G sobre um grupo de ordem p^2. Note que $C_G(G_1/G_3) = G_1$ (pois $[G_1, G_1] = [G_1, G_2]$), desta forma, consideraremos apenas os centralizadores de 2-passos com $i \geq 2$.

Definição 1.3.8. Seja G um p-grupo de classe maximal e ordem p^m. Dizemos que $s \in G$ é um elemento uniforme se $s \notin \cup_{i=2}^{m-2} C_G(G_i/G_{i+2})$.

Ao final desta seção, demonstraremos o Teorema de Blackburn, que nos diz, entre outras coisas, que qualquer p-grupo de classe maximal possui elementos uniformes. Até provarmos isso, porém, adicionaremos a algumas de nossas hipóteses a existência destes elementos.

Dado G um p-grupo de classe maximal, $G/\Phi(G) \cong C_p \times C_p$, donde $G/\Phi(G)$ e, portanto, G possuem exatamente $p+1$ subgrupos maximais. Porém, um p-grupo qualquer não pode ser igual à união de menos que $p+1$ subgrupos próprios, uma vez que a interseção dos mesmos é não vazia e cada um deles possui índice no mínimo p. Temos, então, que se G é a união de seus centralizadores de 2-passos, então todos os $p+1$ subgrupos maximais de G serão desse tipo. Portanto, se o número de centralizadores de 2-passos de G for menor ou igual a p, então G possui elementos uniformes.

Lema 1.3.9. Seja G um p-grupo de classe maximal de ordem p^m e suponha que G possua um elemento uniforme s. Se $1 \leq i \leq m-2$ e $x \in G_i \backslash G_{i+1}$, então $[s,x] \in G_{i+1} \backslash G_{i+2}$.

Demonstração. Como $x \in G_i$, obviamente $[s,x] \in G_{i+1}$. Suponha, por absurdo, $[s,x] \in G_{i+2}$. Tome $\overline{G} = {}^{G}\!/_{G_{i+2}}$, então $\bar{s}$ e $\bar{x}$ comutam em $\overline{G}$. Como $[s,G_{i+1}] \leq G_{i+2}$, temos que $\bar{s}$ centraliza $\overline{G_{i+1}}$, porém, $G_i = \langle x, G_{i+1} \rangle$, donde $\bar{s}$ centraliza $\overline{G_i}$. Portanto, $[s,G_i] \leq G_{i+2}$ e, então, $s \in C_G({}^{G_i}\!/_{G_{i+2}})$, o que contraria a hipótese de que s é um elemento uniforme. □

Teorema 1.3.10. Seja G um p-grupo de classe maximal de ordem p^m e suponha que G possua um elemento uniforme s. Então temos:

(i) $C_G(s) = \langle s \rangle Z(G)$.

(ii) $s^p \in Z(G)$, donde, consequentemente, $o(s) \leq p^2$ e $|C_G(s)| = p^2$.

(iii) Os conjugados de s são exatamente os elementos da classe lateral sG_2.

(iv) Se $0 \leq t \leq m-4$, então o subgrupo $H = \langle s, G_{t+1} \rangle$ é um p-grupo de classe maximal de ordem p^{m-t} tal que $H_i = G_{i+t}$, para todo $i \geq 1$. Portanto, ou $l(H) = m-t-2$, ou $l(H) \geq l(G)+t$.

Demonstração.

(i) Tome $g \in G$ qualquer. Como $G = \langle s \rangle G_1$, temos $g = s^i x$, para algum i inteiro e $x \in G_1$. Portanto, $g \in C_G(s)$ se, e somente se, $[s,x] = 1$. Porém, pelo Lema 1.3.9, se $x \in G_i \backslash G_{i+1}$, com $1 \leq i \leq m-2$, então $[s,x] \in G_{i+1} \backslash G_{i+2}$, donde, em particular, $[s,x] \neq 1$. Desta forma, se $g = s^i x$ é tal que $g \in C_G(s)$, então $x \in G_{m-1} = Z(G)$. Portanto, $C_G(s) = \langle s \rangle Z(G)$.

(ii) Seja $x = s^p$. Note que $x \in G_1$ e $[s,x] = 1$. Como na demonstração do item anterior, se $x \in G_i \backslash G_{i+1}$, com $1 \leq i \leq m-2$, então $[s,x] \neq 1$. Desta forma, $x \in G_{m-1} = Z(G)$.

(iii) A cardinalidade da classe de conjugação de s em G é $[G : C_G(s)] = p^{m-2} = |sG_2|$. Note porém, que dado $g \in G$ qualquer, $s^g = s[s,g] \in sG_2$, donde temos o resultado desejado.

(iv) Se $t = 0$, então $H = G$ e não há o que provar, portanto, assumiremos $t \geq 1$. Pelo item (ii) deste teorema, temos $|H| = p|G_{t+1}| = p^{m-t}$. Dado $x \in G_{t+1} \backslash G_{t+2}$, temos, aplicando repetidamente o Lema 1.3.9, $[x, {}_i\, s] \in G_{i+t} \backslash G_{i+t+1}$, para $2 \leq i \leq m-t-1$. Em particular, tomando $i = m-t-1$, temos que $[x, {}_i\, s] \neq 1$ e $[x, {}_i\, s] \in \gamma_{m-t-1}(H)$, donde H tem classe maximal.

Para provarmos que $H_i = G_{i+t}$, suporemos, primeiramente, $i \geq 2$. Sabemos que $[x,\ _k\ s]$ pertence a H_i e a $G_{k+t}\backslash G_{k+t+1}$, para todo k tal que $i \leq k \leq m-t-1$. Mas $[G_{k+t} : G_{k+t+1}] = p$, donde $G_{i+t} \leq H_i$ e, portanto, como os dois grupos possuem a mesma ordem, temos $G_{i+t} = H_i$. Por outro lado, $[G_{t+1}, H_2] = [G_{t+1}, G_{t+2}] \leq G_{2t+3} \leq G_{t+4} = H_4$, donde $H_1 = G_{t+1}$. Por fim, seja $l = l(G)$ o grau de comutatividade de G, então $[H_i, H_j] = [G_{i+t, G_{j+t}}] \leq G_{i+j+l+2t}$, para todo $i, j \geq 1$, donde $l(H) = m-t-2$ ou $l(H) \geq l(G)+t$.

□

Definição 1.3.11. Sejam G um p-grupo de classe maximal, $s \in G$ um elemento uniforme e $s_1 \in G_1\backslash G_2$. Definimos recursivamente $s_i = [s_{i-1}, s]$, para $i \geq 2$, e dizemos que a sequência de elementos $\{s, s_1, s_2, \dots\}$ é uma cadeia de G.

Pelo Lema 1.3.9, temos $s_i \in G_i\backslash G_{i+1}$, além disso, a existência de cadeias de G equivale à existência de elementos uniformes. Note, também, que se $\{s, s_1, s_2, \dots\}$ é uma cadeia de G e $\overline{G}$ é um quociente de G de ordem maior ou igual a p^4, então $\{\overline{s}, \overline{s_1}, \overline{s_2}, \dots\}$ é uma cadeia de $\overline{G}$. Para perceber isto, basta notar que $\overline{s}$ é um elemento uniforme de $\overline{G}$.

Por vezes denotaremos s por s_0 e a cadeia $\{s, s_1, s_2, \dots\}$ por $\{s_i\}$. Desta forma, $s_i \in G_i\backslash G_{i+1}$, para $0 \leq i \leq m-1$ e $s_i = 1$, para $i \geq m$. Seja $l = l(G)$ o grau de comutatividade de G. Definimos a função:

$$\begin{aligned} \alpha : \{(i,j) \in \mathbb{N}^2 \mid i+j \leq m-l-1\} &\to \quad \mathbb{F}_p \\ (i,j) &\mapsto \alpha(i,j) \end{aligned}$$

tal que:

$$[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \mod G_{i+j+l+1}.$$

Observe que, se $l \geq m-2$, o domínio da função é vazio. Como $G_i = \langle s_i, G_{i+1}\rangle$, $G_j = \langle s_j, G_{j+1}\rangle$ e $[G_i, G_{j+1}]$,$[G_{i+1}, G_j] \leq G_{i+j+l+1}$, temos, pela congruência acima, que $\alpha(i,j) = 0$ se, e somente se, $[G_i, G_j] \leq G_{i+j+l+1}$. Desta forma, se $l \leq m-3$, temos, pela definição de $l(G)$, que a função α não é identicamente nula.

A seguir, utilizaremos a álgebra de Lie $\mathcal{L}(G)$ para conseguirmos uma série de propriedades da função α. Com elas, esta função se tornará uma importante ferramenta nos estudos de p-grupos de classe maximal. Definimos $e_i = s_i G_{i+1}$, em $\mathcal{L}(G)$. Claramente $\{e_1, e_2, \cdots, e_{m-1}\}$ forma uma base de $\mathcal{L}(G)$ e, para $i \geq m$, $e_i = 0$. Desta forma, pela definição de $\mathcal{L}(G)$ e pela congruência acima, temos:

$$[e_i, e_j] = \alpha(i,j) e_{i+j+l}, \text{com } i, j \geq 1, i+j \leq m-l-1.$$

Logo, uma vez que o restante dos produtos $[e_i, e_j]$ ou são da forma $[e_i, e_0] = e_{i+1}$, ou são iguais a zero, conseguimos, através da função α, determinar todos os produtos de $\mathcal{L}$.

Pela definição do produto $[\ ,\ ]$ e pelas propriedades básicas dos comutadores, temos $\alpha(i,i) = 0$ e $\alpha(i,j) = -\alpha(j,i)$. Por outro lado, se $i, j \geq 0$, temos, pela identidade de Jacobi (item (iii) da Definição 1.3.6):

$$\begin{aligned} 0 &= [e_0, e_i, e_j] + [e_i, e_j, e_0][e_j, e_o, e_i] \\ &= [-e_{i+j}, e_j] + [\alpha(i,j)e_{i+j+l}, e_0] + [e_{j+1}, e_i] \\ &= -\alpha(i+1,j)e_{i+j+l+1} + \alpha(i,j)e_{i+j+l+1} + \alpha(j+1,i)e_{i+j+l+1}, \end{aligned}$$

donde:

$$\alpha(i,j) = \alpha(i+1,j) + \alpha(i,j+1), \text{com } i+j \leq m-l-2.$$

Uma consequência direta deste resultado é: $\alpha(i,i+1) = \alpha(i,i+2)$. Analogamente, pela identidade de Jacobi, para $i, j, k \geq 1$ e $i+j+k \leq m-2l-1$, temos:

$$\alpha(i,j)\alpha(i+j+k,k) + \alpha(j,k)\alpha(j+k+l,i) + \alpha(k,i)\alpha(k+i+l,j) = 0.$$

O seguinte teorema reúne as principais propriedades da função α.

Teorema 1.3.12. Seja G um p-grupo de classe maximal, de ordem p^n e de grau de comutatividade $l < m-2$. Suponha que G possua uma cadeia e seja α a função associada a ela. Então temos as seguintes propriedades:

(P1) α não é identicamente nula.

(P2) $\alpha(i,i) = 0$, para $2i \leq m-l-1$.

(P3) $\alpha(i,j) = -\alpha(j,i)$, para $i+j \leq m-l-1$.

(P4) $\alpha(i,j) = \alpha(i+1,j) + \alpha(i,j+1)$, para $i+j \leq m-l-2$.

(P5) $\alpha(i,i+2) = \alpha(i,i+1)$, para $2i \leq m-l-3$.

(P6) $\alpha(i,j)\alpha(i+j+k,k) + \alpha(j,k)\alpha(j+k+l,i)_\alpha(k,i)\alpha(k+i+l,j) = 0$, para $i+j+k \leq m-2l-1$.

Note que, pelos itens P2 e P3 deste teorema, para conhecermos os valores que α assume, basta conhecermos os valores de $\alpha(i,j)$, para $i < j$. No teorema a seguir, refinamos a propriedade P1.

Teorema 1.3.13. Seja G um p-grupo de classe maximal, de ordem p^m e de grau de comutatividade $l < m-2$. Suponha que G possua uma cadeia e seja α a função associada a ela. Então existe $j \in \{1, \cdots, m-l-2\}$ tal que $\alpha(1,j) \neq 0$. Ou seja, existe j tal que $[G_1, G_j] = G_{j+l+1} \neq 1$.

Demonstração. Suponha $\alpha(1,j)=0$ para todo j. Pela propriedade P4, temos $\alpha(i,j)=\alpha(i-1,j)-\alpha(i-1,j+1)$, donde, por indução, temos $\alpha(i,j)=0$, para todo i e j possível. Portanto, pela propriedade P1, temos uma contradição.

□

O próximo teorema nos dará o valor de qualquer $\alpha(i,j)$ a partir dos valores $\alpha(r,r+1)$. Para demonstrá-lo, estenderemos a definição dos coeficientes binomiais $\binom{n}{k}$ para todo $n,k\in\mathbb{Z}$:

$$\binom{n}{k}=\begin{cases}\dfrac{n(n-1)\cdots(n-k+1)}{k!}, & \text{se } k\geq 1\\ 1, & \text{se } k=0\\ 0, & \text{se } k<0\end{cases}$$

Os coeficientes binomiais generalizados apresentados acima ainda satisfazem a identidade $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$. Além disso, pela definição acima, temos $\binom{n}{k}=0$, para $0\leq n<k$, e $\binom{n}{k}=\binom{n}{n-k}$, para $n\geq 0$.

Teorema 1.3.14. Seja G um p-grupo de classe maximal de ordem p^m e grau de comutatividade $l<m-2$. Suponha que G possua uma cadeia e seja α a função associada a ela. Se tomarmos $x_r=\alpha(r,r+1)$, então:

$$\alpha(i,j)=\sum_{r=i}^{[(i+j-1)/2]}(-1)^{r-i}\binom{j-r-1}{r-i}x_r,\text{ para } i<j,$$

onde $[(i+j-1)/2]$ denota o maior inteiro menor ou igual $(i+j-1)/2$.

Demonstração. Utilizando a definição de binômio estendida, note que, se $r>(i+j-1)/2$, então $0\leq j-r-1\leq r-i$, donde $\binom{j-r-1}{r-i}=0$. Portanto, temos:

$$\sum_{r=i}^{[(i+j-1)/2]}(-1)^{r-i}\binom{j-r-1}{r-i}x_r=\sum_{r=i}^{j-1}(-1)^{r-i}\binom{j-r-1}{r-i}x_r.$$

Alguns valores x_r podem não estar definidos, mas isso é irrelevante, pois os coeficientes correspondentes são iguais a 0. Provaremos o teorema por indução sobre $j-i$. Se $j-i=1$ ou 2, o resultado é imediato. Suponha, agora, $j-i\geq 3$ e que o resultado é válido para valores

menores que $j-i$. Temos:

$$\begin{aligned}\alpha(i,j) &= \alpha(i,j-1)-\alpha(i+1,j-1)\\ &= \sum_{r=i}^{j-2}(-1)^{r-i}\binom{j-r-2}{r-i}x_r - \sum_{r=i+1}^{j-2}(-1)^{r-i-1}\binom{j-r-2}{r-1}x_r\\ &= \sum_{r=i}^{j-2}(-1)^{r-i}\binom{j-r-2}{r-i}x_r + \sum_{r=i+1}^{j-2}(-1)^{r-i}\binom{j-r-2}{r-i-1}x_r\end{aligned}$$

Note, porém, que $\binom{j-r-2}{i-i-1}=0$, donde:

$$\begin{aligned}\alpha(i,j) &= \sum_{r=i}^{j-2}(-1)^{r-i}\binom{j-r-2}{r-i}x_r + \sum_{r=i}^{j-2}(-1)^{r-i}\binom{j-r-2}{r-i-1}x_r\\ &= \sum_{r=i}^{j-2}(-1)^{r-i}\binom{j-r-1}{r-i}x_r.\end{aligned}$$

Como $\binom{j-(j-1)-1}{(j-1)-i}=0$ (lembre-se que supomos $j-i\geq 3$), temos, por fim:

$$\alpha(i,j)=\sum_{r=i}^{j-1}(-1)^{r-i}\binom{j-r-1}{r-i}x_r.$$

□

A seguir, provamos o Teorema de Blackburn para o caso em que $|G|\leq p^{p+2}$.

Teorema 1.3.15. Seja G um p-grupo de classe maximal e ordem $p^m \leq p^{p+2}$. Então:

(i) G possui elementos uniformes.

(ii) Se $l(G)=0$, então $p\geq 5$, m é par e $6\leq m\leq p+1$.

(iii) $l(G/Z(G))\geq 1$.

Demonstração.

(i) Como o número máximo de centralizadores de 2-passos distintos é $m-3\leq p-1\leq p+1$, temos que existem elementos uniformes.

(ii) Primeiramente, lembre-se que se $|G|=p^4$, então $l(G)=2$, portanto, temos $m\geq 5$. Provaremos por indução sobre m que se m é ímpar, então $l(G)\geq 1$. Pelo item (i)

deste teorema, G possui uma cadeia, trabalharemos sobre a função α associada a ela. Suponha $m = 5$. Se $l(G) = 0$, então, como $[G_1, G_2] \leq G_4$, temos $\alpha(1,2) = 0$. Logo, pela propriedade P5, $\alpha(1,3) = 0$ e, portanto, pelo Teorema 1.3.13, temos uma contradição. Concluímos, assim, a prova da nossa base de indução. Em particular, temos $|G| \leq p^{p+2}$ e $l(G) = 0$, donde $p \geq 5$.

Suponha, agora, $m = 2n+1 > 5$ e $l(G) = 0$. Pela hipótese de indução, temos $l(G/G_{m-2}) \geq 1$. Logo, se $i+j \leq m-3$, então $[G_i, G_j] \leq G_{i+j+1}$ e, portanto, $\alpha(i,j) = 0$. Por outro lado, pela propriedade P6, temos:

$$\alpha(1,2)\alpha(3,m-4) + \alpha(2,m-4)\alpha(m-2,1) + \alpha(m-4,1)\alpha(m-3,2) = 0,$$

donde $\alpha(2,m-4)\alpha(m-2,1) = 0$. Pelo Teorema 1.3.14 (e lembrando que se $i+j \leq m-3$, então $\alpha(i,j) = 0$), temos $\alpha(1,m-2) = (-1)^{n-2}(n-1)x_{n-1}$ e $\alpha(2,m-4) = (-1)^{n-3}x_{n-1}$ (onde $m = 2n+1$). Portanto, $(n-1)x_{n-2}^2 = 0$ no corpo $\mathbb{F}_p$. Porém, uma vez que $m \leq p+2$, temos $n-1 \neq 0$ em $\mathbb{F}_p$, donde $x_{n-1} = \alpha(n-1,n) = 0$. Com isso, temos $\alpha(r,r+1) = 0$ para todo r, donde, pelo Teorema 1.3.14, α é uma função identicamente nula, o que é uma contradição. Portanto, m é par e $m \geq 6$. Temos, assim, o resultado desejado.

(iii) Se m é par, então $m-1$ é ímpar, donde, como $|G/Z(G)| = p^{m-1}$, temos $l(G/Z(G)) \geq 1$. Se m é ímpar, então $l(G) \geq 1$, logo, pelo Teorema 1.3.5, temos $l(G/Z(G)) = m-3$ ou $l(G/Z(G)) \geq l(G)$, donde $l(G/Z(G)) \geq 1$.

□

Teorema 1.3.16. Seja G um p-grupo de classe maximal de ordem menor ou igual a p^{p+1}. Então $\exp(G/Z(G)) = \exp(G_2) = p$.

Demonstração. Sabemos que G possui $p+1$ subgrupos maximais. Como o números de centralizadores de 2-passos distintos de G é no máximo $m-3$ e $m \leq p+1$, temos que G possui pelo menos dois subgrupos maximais, M e N, que não são deste tipo. Tome dois elementos uniformes $s \in M$ e $t \in N$. Como $[G : \Phi(G)] = p^2$, temos $G = \langle s,t\rangle\Phi(G)$, donde $G = \langle s,t\rangle$. Por outro lado, pelo Teorema 1.3.10, temos $s^p, t^p \in Z(G)$. Portanto, $G/Z(G)$ pode ser gerado por dois elementos de ordem p. Como $|G/Z(G)| \leq p^p$, temos que $G/Z(G)$ é regular, donde $\exp(G/Z(G)) = p$.

Em particular, temos $G_1^p \leq G^p \leq Z(G)$. Como G_1 tem ordem menor ou igual a p^p e é, portanto, regular, temos $[G_1 : \Omega_1(G_1)] \leq |G_1^p| \leq |Z(G)| \leq p$. Logo, $[G : \Omega_1(G)] \leq p^2$, donde, como $\Omega_1(G_1)$ é normal em G, temos $G_2 \leq \Omega_1(G_1)$. Por fim, como G_1 é regular, temos $\exp G_2 = 2$.

□

Lema 1.3.17. Seja G um p-grupo de classe maximal de ordem p^{p+2} e seja $\{s_i\}$ uma cadeia de G. Então temos:

(i) $s_1 \equiv s_p^{-1} \mod G_{p+1}$.

(ii) $\Omega_1(G_1) = G_p$.

Demonstração.

(i) Pela Fórmula de Compilação de Hall (Teorema 1.2.10), temos $s_0^p s_1^p \equiv (s_0 s_1)^p c_p \mod G_2^p$. Aplicando o Teorema 1.3.16 ao grupo G/G_{p+1}, temos $\exp(G_2/G_{p+1}) = p$, donde $G_2^p \leq G_{p+1}$. Portanto, temos $s_0^p s_1^p \equiv (s_0 s_1)^p c_p \mod G_{p+1}$. Por outro lado, s_0 é um elemento uniforme, donde $s_0^p \in Z(G) = G_{p+1}$. Além disso, pelo Teorema 1.3.15, temos $l(G) \geq 1$ e, portanto, qualquer elemento em $G \backslash G_1$ é um elemento uniforme. Em particular $s_0 s_1$ é um elemento uniforme, donde $(s_0 s_1)^p \in G_{p+1}$. Temos, então, $s_1^p \equiv c_p \mod G_2^p$ e resta mostrar que $c_p \equiv s_p^{-1} \mod G_{p+1}$. Pelo Teorema 1.2.11, temos:

$$c_p \equiv s_p^{-1} \prod_i v_i^{a_i} \mod G_{p+1},$$

onde cada v_i é um comutador da forma $[s_1, s_0, z_3, \cdots, z_p]$, com $z_j \in \{s_0, s_1\}$ e pelo menos um z_j igual a s_1. Como $l(G) \geq 1$, temos $v_i \in G_{p+1}$, para todo i, e, consequentemente, $c_p \equiv s_p^{-1} \mod G_{p+1}$.

(ii) Pelo item (i) deste teorema, temos $s_1^p \notin G_{p+1}$ e, em particular, $G_1^p \not\leq G_{p+1}$. Por outro lado, aplicando o Teorema 1.3.16 sobre o grupo G/G_{p+1}, temos $\exp(G/G_p) = p$ e, portanto, $G_1^p \leq G_p$. Desta forma, como $G_1^p \trianglelefteq G$, temos $G_1^p = G_p$.

□

Teorema 1.3.18. Seja G um p-grupo de classe maximal de ordem $p^m \geq p^{p+2}$. Então:

(i) G_1 é regular.

(ii) $G_i^p = G_{i+p-1}$, para todo $i \geq 1$.

(iii) Se $1 \leq i \leq m-p$ e $x \in G_i \backslash G_{i+1}$, então $x^p \in G_{i+p-1} \backslash G_{i+p}$.

Demonstração.

(i) Aplicando o item (ii) do Lema 1.3.17 ao grupo G/G_{p+2}, temos $(G/G_{p+2})^p = G_p/G_{p+2}$, donde $G_1^p G_{p+2} = G_p$. Como G_1^p é normal em G, temos $G_1^p = G_i$, para algum inteiro i, desta forma, $G_1^p = G_p$ e, portanto, $[G_1 : G_1^p] = p^{p-1}$. Logo, pelo Teorema 1.2.17, temos que G_1 é regular.

(ii) Assim como na demonstração do item anterior, temos $G_1^p = G_p$. Lembre-se, porém, que G_1 é regular, donde, pelo Teorema 1.2.16, temos $[G_{i-1}^p, G] = G_i^p$. Portanto, através de uma indução simples, conseguimos que $G_i^p = G_{i+p-1}$.

(iii) Tome $x \in G_i \backslash G_{i+1}$. Pelo item (ii) deste teorema, temos $x^p \in G_{i+p-1}$. Suponha, por contradição, que $x^p \in G_{i+p}$. Como $G_{i+1}^p = G_{i+p}$, temos que $G_i/G_{i+p} = \langle \overline{x}, \overline{G_{i+1}} \rangle$ é um grupo regular gerado por elementos de ordem p. Portanto, pelo Corolário 1.2.15, temos $\exp(G_i/G_{i+p}) = p$, donde $G_i^p \leq G_{i+p}$, o que é uma contradição.

□

Teorema 1.3.19. Seja G um p-grupo de classe maximal de ordem maior ou igual a p^{p+2}. Então:

(i) G possui elementos uniformes.

(ii) $l(G) \geq 1$.

Demonstração.

(i) Provaremos por indução sobre i, com $i \geq 1$, que $[G_1, G_i] \leq G_{i+2}$. Provado isto, teremos que todos os centralizadores de 2-passos coincidem com G_1, donde G possui elementos uniformes. Pelo Teorema 1.3.15, temos $l(G/G_{p+2}) \geq 1$, donde $[G_1, G_i] \leq G_{i+2}$, para $1 \leq i \leq p$, e temos nossa base de indução. Por outro lado, se $i > p$, então, pelos Teoremas 1.3.18 e 1.2.16, temos:

$$[G_1, G_i] = [G_1, G_{i-p+1}^p] = [G_1, G_{i-p+1}]^p \leq G_{i-p+3}^p = G_{i+2}.$$

(ii) Suponha $l(G) = 0$. Pelo item (i) deste teorema, podemos assumir que G possui uma cadeia, seja α a função associada a ela. Como vimos na demonstração do item anterior, $[G_1, G_j] \leq G_{j+2}$ para todo j, donde $\alpha(1, j) = 0$, para todo j, e temos uma contradição. Portanto $l(G) \geq 1$.

□

Desta forma, podemos, juntando os Teoremas 1.3.19 e 1.3.15, concluir o Teorema de Blackburn.

Teorema 1.3.20. Seja G um p-grupo de classe maximal de ordem p^m. Então:

(i) G possui elementos uniformes.

(ii) Se $l(G) = 0$, então $p \geq 5$, m é par e $6 \leq m \leq p+1$.

(iii) $l(G/Z(G)) \geq 1$.

A seguir, provamos outros dois resultados que nos serão úteis no capítulo final desta dissertação.

Proposição 1.3.21. Seja G um p-grupo de classe maximal e ordem p^m. Então G possui no máximo dois centralizadores de 2-passos distintos, G_1 e $C_G(G_{m-2})$. Além disso, $G_1 \neq C_G(G_{m-2})$ se, e somente se, $l(G) = 0$.

Demonstração. Suponha, primeiramente, $l(G) \geq 1$. Seja $i \leq m-2$ um inteiro qualquer. Tome $x \in G_1$ e $y \in G_i$ quaisquer. Temos $[x,y] \in G_{i+1+l(G)}$, donde $[x,y] \in G_{i+2}$. Desta forma, como $y \in G_i$ é qualquer, temos $x \in C_G(G_i/G_{i+2})$. Portanto, $G_1 \leq C_G(G_i/G_{i+2})$, donde, como ambos são maximais, temos $G_1 = C_G(G_i/G_{i+2})$. Suponha, agora, $l(G) = 0$. Sabemos que $G/Z(G)$ é um p-grupo de classe maximal tal que $l(G/Z(G)) \geq 1$. Desta forma, como $Z(G) = G_{m-1}$, temos, de forma análoga ao demonstrado acima, $G_1 = C_G(G_i/G_{i+2})$, para $i \leq m-3$.

Resta mostrarmos que, se $l(G) = 0$, então $G_1 \neq C_G(G_{m-2})$. Suponha $G_1 = C_G(G_{m-2})$, mostraremos que $l(G) \geq 1$. Pelo mostrado anteriormente, temos $[G_1, G_i] \leq G_{i+2}$, para todo inteiro i. Utilizaremos, agora, indução sobre j para mostrar que $[G_j, G_i] \leq G_{i+j+1}$, para todo $i \geq 1$. A base de indução já foi mostrada. Suponha, agora, $j \geq 2$ e $[G_{j-1}, G_k] \leq G_{k+j}$, para todo $k \geq 1$. Seja $i \geq 1$ qualquer, então $[G_j, G_i] = [G_{j-1}, G, G_i]$, mas, utilizando a hipótese de indução, temos $[G, G_i, G_{j-1}] = [G_{i+1,G_{j-1}} \leq G_{i+j+1}]$ e $[G_i, G_{j-1}, G] \leq [G_{i+j}, G] \leq G_{i+j+1}$. Portanto, utilizando o Lema dos Três Subgrupos, temos $[G_j, G_i] \leq G_{i+j+1}$, donde $l(G) \geq 1$. □

Proposição 1.3.22. Seja G um p-grupo tal que G/G_{p+1} tem classe maximal, então G também possui classe maximal.

Demonstração. Para provarmos este teorema, suporemos que, para algum $k \geq p+1$, o quociente G/G_k é de classe maximal e mostraremos que G/G_{k+1} também é. Fatorando G por G_{k+1}, podemos assumir $G_{k+1} = 1$ e $G_k \neq 1$. Como G/G_k tem classe maximal, temos que

G_{k-1}/G_k tem ordem p, donde, pela Proposição 1.1.8, temos que G_k/G_{k+1} tem exponente p. Como $[G/G_k : G'/G_k] = p^2$, temos que o número mínimo de geradores de G/G' é no máximo dois. Desta forma, pela Proposição 1.1.7, temos que G_k/G_{k+1} pode ser gerado por dois elementos e, portanto, tem ordem no máximo p^2.

Suponha que p é ímpar. Seja $\{\overline{s_i}\}$ uma cadeia de G/G_k e seja N um subgrupo normal de G tal que $[G_k : N] = p$. Note que G/N possui classe maximal e que $\{s_i\}$ é uma cadeia de G/N. Além disso, como $|G/N| \geq p^{p+2}$, temos $l(G/N) \geq 1$ (pelo Teorema de Blackburn). Com isso, temos $[s_{k-1}, s_1] \in G_{k+1}$, donde $[s_{k-1}, s_1] = 1$. Temos, porém, $G_{k-1}/G_k = \langle s_{k-1}G_k \rangle$ e $G/G' = \langle s_1G', xG' \rangle$, para algum $x \in G$, logo, pela Proposição 1.1.7, $G_k = \langle [s_1, s_{k-1}], [x, s_{k-1}] \rangle = \langle [x, s_{k-1}] \rangle$. Portanto, como $\exp G_K = p$, temos $G_k = 1$ e G é de classe maximal.

Suponha, agora, $p = 2$. Seja N um subgrupo normal qualquer de G tal que $[G_k : N] = 2$. Temos que G/N é de classe maximal e possui ordem p^{k+1}. Lembre-se que estamos trabalhando com p-grupos de ordem maior ou igual p^4, logo, podemos aplicar o Teorema 1.3.18 para concluir que $(G_{k-1}/N)^p = G_k/N$. Portanto $G_k = G_{k-1}^p N$, para todo $N \trianglelefteq G$ tal que $[G_k : N] = 2$. Sabemos que $(G_{k-1}/N)^p \neq 1$ é normal em G, logo $G_k = G_{k-1}^p$, pois, caso contrário, bastaria tomar $N = G_{k-1}^p$ e teríamos uma contradição (lembre-se que $|G_k| \leq p^2$). Note, porém, que se $|G_{k-1}^p| = p^2$, então $|G_{k-1}| = p^3$, donde G_{k-1} é cíclico, mas isso implicaria que G_k é, também, cíclico, o que é uma contradição, pois $\exp G_k = p$. Portanto $|G_k| = p$ e G é de classe maximal.

□

Capítulo 2

p-Grupos *powerful*

Trataremos, agora, de um tipo de p-grupos que compartilha algumas propriedades com os grupos abelianos, os p-grupos *powerful*. A maior parte dos resultados deste capítulo pode ser encontrada no capítulo 2 de [6] e no capítulo 11 de [16]. Embora toda a teoria de p-grupos *powerful* aqui desenvolvida seja útil no decorrer desta dissertação, somente alguns resultados serão de fato utilizados nas demonstrações dos teoremas principais deste trabalho.

Neste capítulo trataremos somente de p-grupos finitos.

2.1 Definições e propriedades básicas

Definição 2.1.1. Um p-grupo G é dito *powerful* se $G' \leq G^p$, quando p é ímpar, e se $G' \leq G^4$, se $p = 2$.

Desta forma, é imediato que, se G é *powerful*, então $\Phi(G) = G^p$.

Definição 2.1.2. Dados um p-grupo finito G e um subgrupo $N \leq G$, dizemos que N é *powerfully embedded* em G se $[N,G] \leq N^p$, quando p é ímpar, e se $[N,G] \leq N^4$, quando $p = 2$.

Para indicar que N é *powerfully embedded* em G, utilizaremos a notação N p.e. G. Note que um p-grupo finito G é *powerful* se, e somente se, G é *powerfully embedded* em si mesmo. Além disso, se N p.e. G, então $N \trianglelefteq G$ e N é *powerful*.

A seguir mostramos alguns exemplos de p-grupos que são e de p-grupos que não são *powerful*.

Exemplo 2.1.3.

(i) Claramente, se G é um p-grupo abeliano, então G é *powerful* e todos os seus subgrupos são *powerfully embedded* em G.

(ii) Todo p-grupo metacíclico, com p ímpar, é um p-grupo *powerful*. Para observarmos isto, tome G um p-grupo metacíclico e $N = \langle y \rangle$ um subgrupo normal de G tal que $G/N = \langle xN \rangle$. Sabemos que $G = \langle x, y \rangle$, donde $y \notin \Phi(G)$. Porém, como G/N é abeliano, temos $G' \leq N$, donde $[x,y] = y^r \in \Phi(G)$, para algum r. Desta forma, temos que p divide r e, portanto, $G' \leq G^p$.

(iii) Os 2-grupos $\langle y, x \mid y^8 = x^2 = 1, y^x = y^5 \rangle$ e $\langle a, x, y \mid a^4 = x^2 = 1, y^4 = a^2, [x,a] = a^2, [x,y] = [a,y] = 1 \rangle$ são exemplos de 2-grupos *powerful*.

(iv) Todo p-grupo não abeliano de expoente p, sendo p ímpar, não é *powerful*.

(v) Analogamente, todo 2-grupo não abeliano de expoente 4 (como, por exemplo, o diedral de ordem 8) não é *powerful*.

Nos próximos resultados trazemos algumas propriedades básicas envolvendo as noções introduzidas nas duas últimas definições.

Lema 2.1.4. Sejam G um p-grupo finito e N um subgrupo de G.

(i) Se N p.e. G e $K \trianglelefteq G$, então NK/K p.e. GK/K.

(ii) Seja $K \trianglelefteq G$. Então:

- Se p é ímpar e $K \leq N^p$, então N p.e. G se, e somente se, N/K p.e. G/K
- Se $p = 2$ e $K \leq N^4$, então N p.e. G se, e somente se, N/K p.e. G/K

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

(iv) Se N e W são subgrupos normais de G com $N \leq W$ e N não é *powerfully embedded* em W, então existe $J \trianglelefteq G$ 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 $p = 2$:

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

Demonstração. Levando em conta que, neste lema, as provas para o caso $p = 2$ são similares às do caso em que p é ímpar, demonstraremos apenas o caso em que $p > 2$. Os itens (i) e (ii) são obtidos diretamente da definição. Para provar o item (iii), basta notar que $\langle N,x \rangle / N$ é cíclico, donde $\langle N,x \rangle' = [N, \langle N,x \rangle]$ e, como N p.e. G, $\langle N,x \rangle' \leq N^p \leq \langle N,x \rangle^p$.

Como G é um p-grupo, podemos tomar $J \trianglelefteq G$ tal que $N^p \leq J < N^p[N,W]$ e $[N^p[N,W] : J] = p$ (pelo Teorema 1.2.3). Logo, como ${}^{N^p[N,W]}\!/_J$ tem ordem p e é normal em ${}^{G}\!/_J$, temos que o mesmo é central. Portanto, $[N^p[N,W],W] \leq J$, donde $[N,W,W] \leq J$ e $N^P[N,W,W] \leq J$. □

O lema seguinte é um resultado direto do item (iv) do Lema 2.1.4.

Lema 2.1.5. Sejam G um p-grupo finito e $N \trianglelefteq G$. Se p é ímpar e $[N,G] \leq N^p[N,G,G]$, então N p.e. G. Se $p = 2$ e $[N,G] \leq N^4[N,G]^2[N,G,G]$, então N p.e. G.

O lema anterior e a afirmação (iv) do Lema 2.1.4 são importantes ferramentas na demonstração de vários resultados, inclusive o próximo.

Proposição 2.1.6. Sejam G um p-grupo finito e N um subgrupo de G. Se N p.e. G, então N^p p.e. G.

Demonstração. Primeiramente, provemos o caso em que p é ímpar. Utilizaremos o quociente de G por $(N^p)^p[N^p,G,G]$. Para simplificar as notações, simplesmente consideraremos $(N^p)^p[N^p,G,G] = 1$, donde, pelo Lema 2.1.5, basta mostrar $[N^p,G] = 1$.

Como $[N,G] \leq N^p$, temos $[N,G,G,G] \leq [N^p,G,G] = 1$, donde $[N,G,G] \leq Z(G)$. Logo, dados $x \in N$ e $g \in G$ quaisquer, temos, para todo $w_1, w_2 \in G$:

$$[x,g,w_1w_2] = [x,g,w_1][x,g,w_2][x,g,w_1,w_2] = [x,g,w_1][x,g,w_2].$$

Portanto:

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

Desta forma, utilizando o item (iii) do Teorema 1.1.1, temos:

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

Donde $[x^p,g] \in N^p$ e, portanto, $[N,G]^p = 1$.

Provemos agora o resultado para o caso em que $p = 2$. Analogamente ao que fizemos na demonstração do caso em que p é ímpar, consideraremos $(N^2)^4 = [N^2,G]^2 = [N^2,G,G] = 1$ e nos basta provar que $[N^2,G] = 1$. Dados $x \in G$ e $g \in G$ quaisquer, temos:

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

donde $N^4 \leq Z(G)$. Porém, $(N^2)^4 = 1$, logo $\exp N \leq 8$. Portanto, N^4 é um grupo abeliano gerado por elementos de ordem 2, e, com isso, temos que $(N^4)^2 = 1$. Logo, levando em

conta que $[N,G,G] \leq [N^4,G] = 1$ e que $[N,G]^2 \leq (N^4)^2 = 1$, temos:

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

Então, por fim, temos $[N^2,G] = 1$.

□

A seguinte proposição pode ser encontrado em [18].

Proposição 2.1.7. Se M, N p.e. G, então $[M,N]$ p.e. G.

Demonstração. Para demonstrar esta proposição, utilizaremos o Lema 2.1.5, analisando o quociente do grupo G pelos subgrupos convenientes de forma a bastar provarmos que $[M,N,G] = 1$ nesses quocientes. Em ambos os casos teremos que $[M,N,G]$ é central, donde, dados $m \in M$ e $n \in N$, não é difícil provar que $[n^p,m] = [n,m]^p[n,m,n]^{\frac{p(p-1)}{2}}$ (algo semelhante foi mostrado na demonstração da Proposição 2.1.6).

Demonstraremos, primeiramente, o caso em que p é ímpar. Suponha, então, $[N,M]^p = [N,M,G,G] = 1$. Desta forma, como p divide $\frac{p(p-1)}{2}$, temos que $[N^p,M] = 1$. Analogamente, temos $[M^p,N] = 1$. Portanto, $[M,G,N] = [N,G,M] = 1$, donde, pelo Lema dos Três Subgrupos (Teorema 1.1.3), temos $[M,N,G] = 1$.

Demonstremos, agora, o caso em que $p = 2$. Suponha $[M,N]^{p^2} = [M,N,G]^p = [M,N,G,G] = 1$ e sejam $m \in M$ e $n \in N$ quaisquer. Note que $\langle m,[m,n]\rangle$ tem classe de nilpotência menor ou igual a 2. Além disso, temos:

$$(m^4)^n = (m^n)^4 = (m[m,n])^4 = m^4[m,n]^4[m,n,m]^6 = m^4.$$

Logo, $[M^4,N] = 1$, donde $[M,G,N] = 1$. Analogamente, temos $[N,G,M] = 1$. Portanto, novamente pelo Lema dos Três Subgrupos, temos $[M,N,G] = 1$.

□

Definimos indutivamente os seguintes subgrupos: $\Pi_0(G) = G$ e $\Pi_{i+1}(G) = \Pi_i(G)^p$. Perceba que, embora $\Pi_1(G) = G^p$, não podemos afirmar que $\Pi_i(G) = G^{p^i}$, para $i \geq 2$ (note, por exemplo, que $\Pi_2(G) = (G^p)^p$ pode ser diferente de G^{p^2}). Veremos, porém, que se G é um p-grupo *powerful*, de fato temos, para todo i, $\Pi_i(G) = G^{p^i}$.

Lema 2.1.8. Seja G um p-grupo *powerful*. Então, para todo inteiro $i \geq 0$, temos:

(i) $\Pi_i(G)$ p.e. G e $\Pi_{i+1}(G) = \Phi(\Pi_i(G))$;

(ii) O mapeamento $x \mapsto x^p$ induz um homomorfismo de $\Pi_i(G)/\Pi_{i+1}(G)$ sobre $\Pi_{i+1}(G)/\Pi_{i+2}(G)$.

Demonstração. Para provar o primeiro item, basta utilizar a Proposição 2.1.6 em uma indução sobre i e teremos $\Pi_i(G)$ p.e. G, para todo i. Com isso, temos que $\Pi_i(G)$ é *powerful*, donde $\Pi_{i+1}(G) = \Pi_i(G)^p = \Phi(\Pi_i(G))$, para todo i.

Provemos agora o item (ii). Consideraremos o quociente de $\Pi_i(G)$ por $\Pi_{i+2}(G)$, e, como $\Pi_i(G)$ é *powerful*, podemos mudar a notação para $\Pi_i(G) = \Pi_0(G) = G$. Portanto, simplesmente assumiremos $\Pi_2(G) = 1$. Temos $[G,G,G] \leq [G^p,G] \leq (G^p)^p = 1$, donde $[G,G] \leq Z(G)$. Portanto, note que $[y^n,x] = [y,x]^n$. Temos então:

$$\begin{aligned}(xy)^p &= xyxy\cdots xy \\ &= xyx[x,y][y,x]y\cdots xy \\ &= x^2y^2xy\cdots xy[y,x] \\ &= x^2y^2x[x,y^2][y^2,x]y\cdots xy[y.x] \\ &= x^3y^3xy\cdots xy[y,x][y^2,x]\end{aligned}$$

Recursivamente, teremos $(x,y)^p = x^py^p[y,x]^{\frac{p(p-1)}{2}}$. Caso, p seja ímpar, teremos $p|p(p-1)/2$, donde $(xy)^p = x^py^p$. Caso $p = 2$, temos $[G,G] \leq G^4 \leq (G^2)^2 = 1$, donde, da mesma forma, $(xy)^p = x^py^p$. Portanto, o mapeamento $x \mapsto x^p$ induz, de fato, um homomorfismo.

□

Lema 2.1.9. Se $G = \langle a_1,\cdots,a_d\rangle$ é um p-grupo *powerful*, então $G^p = \langle a_1^p,\cdots,a_d^p\rangle$.

Demonstração. Como o mapeamento $x \mapsto x^p$ induz um homomorfismo de G/G^p em $G^p/\Pi_2(G)$ e $\Pi_2(G) = \Phi(G^p)$, temos que $\langle \overline{a_1^p},\cdots,\overline{a_d^p}\rangle$ gera $G^p/\Phi(G^p)$, donde $G^p = \langle a_1^p,\cdots,a_d^p\rangle$.

□

Proposição 2.1.10. Se G é um p-grupo *powerful*, então $G^p = \{g^p | g \in G\}$.

Demonstração. Para demonstrarmos esse resultado, utilizaremos indução sobre a ordem de G. Obviamente, se $|G| = 1$, temos o resultado. Suponha agora que o resultado vale para p-grupos com ordem menor que a de G. Seja $g \in G^p$, pelo Lema 2.1.8, existem $x \in G$ e $y \in (G^p)^p$ tais que $g = x^py$. Tome $H = \langle G^p,x\rangle$. Pelos Lemas 2.1.8 e 2.1.4, temos que H é *powerful*. Além disso, $g \in H^p$. Se $H \neq G$, temos, pela hipótese de indução, $g \in \{h^p | h \in H\}$. Se $G = H$, temos $G = \langle G^p,x\rangle = \Phi(G)\langle x\rangle$, então $G/\Phi(G)$ é cíclico e, portanto, G também é. Logo, temos o resultado desejado.

□

O teorema a seguir resume as principais propriedades básicas dos subgrupos G^{p^i}, com $i \geq 0$, de p-grupos *powerful*.

Teorema 2.1.11. Seja $G = \langle a_1, \cdots, a_d \rangle$ um p-grupo *powerful*, então:

(i) G^{p^i} p.e. G;

(ii) $\Pi_{i+k}(G) = \Pi_i(G)^{p^k}$;

(iii) $\Pi_i(G) = G^{p^i} = \{x^{p^i} | x \in G\} = \langle a_1^{p^i}, \cdots, a_d^{p^i} \rangle$.

(iv) o mapeamento $x \mapsto x^{p^k}$ induz um homomorfismo de $G^{p^i}/G^{p^{i+1}}$ em $G^{p^{i+k}}/G^{p^{i+k+1}}$, para todo i e k.

Demonstração. O item (i) já foi provado e o item (iv) é um resultado direto do Lema 2.1.8. Note, também, que o item (ii) é um resultado direto do item (iii). Como $\Pi_i(G)$ é *powerful*, temos, pela Proposição 2.1.10, que $\Pi_i(G) = \{x^p | x \in \Pi_{i-1}(G)\}$. Utilizando uma simples indução, temos $\Pi_i(G) = \{x^p | x \in G\}$. Além disso, aplicando repetidamente o Lema 2.1.9, temos $\Pi_i(G) = \langle a_1^{p^i}, \cdots, a_d^{p^i} \rangle$. Com isso, temos $\Pi_i(G) \leq G^{p^i}$, donde $\Pi_i(G) = G^{p^i}$. Finalizamos, portanto, a demonstração.

□

Corolário 2.1.12. Se $G = \langle a_1, \cdots, a_d \rangle$ é um p-grupo *powerful*, então $G = \langle a_1 \rangle \cdots \langle a_d \rangle$.

Demonstração. Utilizaremos indução sobre $|G|$. Se G é trivial, não há o que demonstrar. Suponha que o resultado vale para p-grupos de ordens menores que a de G. Seja n o inteiro tal que $G^{p^n} > G^{p^{n+1}} = 1$. Então, temos, utilizando a hipótese de indução sobre G/G^{p^n}, que $G = \langle a_1 \rangle \cdots \langle a_d \rangle G^{p^n}$. Mas $G^{p^n} = \langle a_1^{p^n}, \cdots a_d^{p^n} \rangle$ e G^{p^n} p.e. G, donde $[G^{p^n}, G] \leq G^{p^{n+1}} = 1$ e, portanto, G^{p^k} é central. Desta forma, temos o resultado desejado.

□

Finalizamos esta seção com o seguinte teorema, que é um dos principais resultados deste capítulo.

Teorema 2.1.13. Sejam G um p-grupo *powerful* e H um subgrupo de G, então $d(H) \leq d(G)$, ou seja, o posto de G é $d(G)$.

Demonstração. Para a demonstração deste teorema, utilizaremos indução sobre a ordem de G. Se $|G| = 1$, o resultado é trivial. Suponha agora que o resultado vale para p-grupos *powerful* de ordem menor que a de G. Sejam $d = d(G)$ e $m = d(G^p)$, e tome $H \leq G$ qualquer. Como G^p é *powerful*, temos, por hipótese de indução, que $d(K) \leq m$, onde $K = H \cap G^p$. Tome o epimorfismo $\theta : G/G^p \to G^p/G^{p^2}$, definido a partir do mapeamento $x \mapsto x^p$.

Como $[G,G] \leq G^p$, temos que ${}^{G}\!/_{G^p}$ é abeliano elementar, donde $\ker(\theta)$ também é. Além disso, como $G^p = \Phi(G)$ e $G^{p^2} = \Phi(G^p)$, temos $d({}^{G}\!/_{G^p}) = d$ e $d({}^{G^p}\!/_{G^{p^2}}) = m$. Note, também, que:

$$|\ker\theta| = \frac{{}^{|G|}\!/_{|G'|}}{{}^{|G^p|}\!/_{|G^{p^2}|}} = p^{d-m},$$

donde a dimensão de $\ker\theta$ é $d-m$ e, portanto, a dimensão de $\ker\theta \cap {}^{HG^p}\!/_{G^p}$ é menor ou igual a $d-m$.

Seja e a dimensão de ${}^{HG^p}\!/_{G^p}$, então, pelo Teorema do Núcleo e da Imagem:

$$\begin{aligned}\dim(\theta(HG^p/G^p)) &= \dim(HG^p/G^p) + \dim(\ker\theta \cap {}^{HG^p}\!/_{G^p}) \\ &\geq e-(d-m) \\ &= m-(d-e).\end{aligned}$$

Sejam $h_1,\cdots,h_e \in H$ elementos tais que $HG^p = \langle h_1,\cdots,h_e\rangle G^p$. Temos $\Phi(K) = [K,K]K^p$, logo $\Phi(K) \leq [G^p,G^p](G^p)^p = (G^p)^p = G^{p^2}$. Note que $h_i^p \in K$, donde $\langle h_1^p,\cdots,h_e^p\rangle\Phi(K)/\Phi(K)$ é um subespaço vetorial de ${}^{K}\!/_{\Phi(K)}$. Note, também, que, pela definição de θ, $\theta(HG^p/G^p) = (HG^p)^pG^{p^2} = H^pG^{p^2}/G^{p^2}$. Portanto, $\dim(\langle h_1^p,\cdots,h_e^p\rangle\Phi(K)/\Phi(K)) \geq \dim(\theta(HG^p/G^p)) \geq m-(d-e)$.

Portanto, como $d(K) \leq d$, existem $d-e$ elementos $y_1,\cdots,y_{d-e} \in K$ tais que:

$$K = \langle h_1^p,\cdots,h_e^p,y_1,\cdots,y_{d-e}^p\rangle\Phi(K).$$

Donde:

$$K = \langle h_1^p,\cdots,h_e^p,y_1,\cdots,y_{d-e}^p\rangle.$$

Portanto:

$$\begin{aligned}H &= H \cap \langle h_1,\cdots,h_e\rangle G^p \\ &= \langle h_1,\cdots,h_e\rangle K \\ &= \langle h_1,\cdots,h_e,y_1,\cdots,y_{d-e}^p\rangle.\end{aligned}$$

Donde $d(H) \leq d$, como desejávamos.

□

2.2 O subgrupo $V(G,r)$

Nesta seção mostraremos que um p-grupo finito G possui um subgrupo característico cujo índice é limitado pelo seu posto. Para tal, utilizaremos as relações que um p-grupo finito qualquer possui com o grupo de matrizes $GL_r(\mathbb{F}_p)$.

Definição 2.2.1. O grupo uni-triangular inferior, denotado $U_r(\mathbb{F}_p)$, é o grupo formado pelas matrizes triangulares inferiores de $GL_r(\mathbb{F}_p)$.

Definição 2.2.2. Seja G um p-grupo finito e r um inteiro positivo. Definimos $V(G,r)$ como a interseção dos núcleos de todos os homomorfismos de G sobre $GL_r(\mathbb{F}_p)$.

Não é difícil provar que $|GL_r(\mathbb{F}_p)| = p^{\binom{r}{2}} \prod_{i=0}^{r-1}(p^{n-i}-1)$ e que $|U_r(\mathbb{F}_p)| = p^{\binom{r}{2}}$. Desta forma, pode-se observar que $U_r(\mathbb{F}_p)$ é um p-subgrupo de Sylow de $GL_r(\mathbb{F}_p)$. Logo, temos que qualquer p-subgrupo de $GL_r(\mathbb{F}_p)$ é um conjugado de algum subgrupo de $U_r(\mathbb{F}_p)$. Dado um p-grupo finito G, portanto, podemos equivalentemente definir $V(G,r)$ como a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$.

Dado um inteiro positivo r, defina $\lambda(r)$ como o inteiro tal que:

$$2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}.$$

Lema 2.2.3. Dados r um inteiro positivo e G um p-grupo finito, temos:

(i) $U_r(\mathbb{F}_p)$ possui uma série de comprimento $\lambda(r)$ de subgrupos normais com fatores abelianos;

(ii) $G/V(G,r)$ possui uma série de comprimento menor ou igual a $\lambda(r)$ com essas mesmas propriedades.

Demonstração.

(i) Seja s o menor inteiro tal que $s \geq \frac{r}{2}$. Tome $x \in U_r(\mathbb{F}_p)$ qualquer, então x é da forma:

$$x = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix},$$

onde $A \in U_s(\mathbb{F}_p)$ e $C \in U_{r-s}(\mathbb{F}_p)$. Defina o homomorfismo θ_1 de $U_r(\mathbb{F}_p)$ em $U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)$ a partir do mapeamento $x \mapsto (A,C)$. Então $\ker\theta_1$ é normal em G e, dados $x_1, x_2 \in \ker\theta_1$, temos:

$$x_1 = \begin{pmatrix} 1 & 0 \\ B_1 & 1 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 1 & 0 \\ B_2 & 1 \end{pmatrix}.$$

Donde:

$$x_1 x_2 = \begin{pmatrix} 1 & 0 \\ B_1 + B_2 & 1 \end{pmatrix}$$

e,portanto, $\ker\theta_1$ é abeliano elementar.

Seja, agora, s' o menor inteiro tal que $s' \geq \frac{s}{2}$, podemos definir, de forma análoga, um homomorfismo θ_2 de $U_r(\mathbb{F}_p)$ em $U_{s'}(\mathbb{F}_p) \times U_{s-s'}(\mathbb{F}_p)$ tal que $\ker\theta_2 \leq \ker\theta_1$, e $\ker\theta_2$ é subgrupo normal de G tal que ${}^{\ker\theta_2}\!/_{\ker\theta_1}$ é abeliano elementar. Recursivamente, conseguimos a série $\ker\theta_1 \leq \cdots \leq \ker\theta_{\lambda(r)}$, que é tal qual desejávamos.

(ii) Sejam $\{\psi_1, \cdots, \psi_n\}$ todos os homomorfismos de G em $U_r(\mathbb{F}_p)$. Então $V(G,r)$ será o núcleo do homomorfismo:

$$\begin{aligned} \psi : G &\to U_r(\mathbb{F}_p)^n \\ g &\mapsto (\psi_1(g), \cdots, \psi_n(g)). \end{aligned}$$

Logo, ${}^{G}\!/_{V(G,r)} \cong \mathrm{Im}\psi \leq U_r(\mathbb{F}_p)^n$, donde, pelo item (i) deste lema, temos que ${}^{G}\!/_{V(G,r)}$ possui uma série com as propriedades desejadas.

□

Proposição 2.2.4. Sejam G um p-grupo finito e r um inteiro positivo. Considere $V = V(G,r)$ e tome $W = V$, se p é ímpar, ou $W = V^2$, se $p = 2$. Se $N \trianglelefteq G$, $d(N) \leq r$ e $N \leq W$, então N p.e. W.

Demonstração. A prova se dará por indução sobre $|N|$. Caso $|N| = 1$, é trivial que N p.e. G.

Primeiramente, consideremos o caso em que p é ímpar. Suponha, por absurdo, que $[N,V] \not\leq N^p$. Pelo item (iv) do lema 2.1.4, existe $J \trianglelefteq V$ tal que $N^p \leq J < N^p[N,V]$ e $[N^p[N,V] : J] = p$. Cortando G por J, podemos, então, supor $N^p = 1$ e $|[N,V]| = p$. Como G é um p-grupo, existe $M \trianglelefteq G$ tal que $[N,V] \leq M < N$ e $[N : M] = p$. Como ${}^{N}\!/_{[N,V]}$ é abeliano elementar (pois $N^p = 1$), temos que $d({}^{M}\!/_{[N,V]}) \leq d({}^{N}\!/_{[N,V]}) \leq r-1$. Portanto, pela hipótese de indução, $[M,V] \leq M^p \leq N^p = 1$, donde M é central em N. Note, porém, que, como ${}^{N}\!/_{M}$ é cíclico, temos que N é abeliano.

Portanto N é um $\mathbb{F}_p$ espaço vetorial de dimensão no máximo r. Como $[N,V] \neq 1$, temos que existe $g \in V$ tal que g age não trivialmente (pela conjugação) sobre o $\mathbb{F}_p$ espaço vetorial

N, donde existe um homomorfismo de G em $GL_r(\mathbb{F}_p)$ tal que g não pertence ao núcleo, o que é uma contradição, pela definição de $V(G,r)$. Portanto $[N,V] \leq N^p$.

Consideremos, agora, o caso em que $p = 2$. Analogamente ao feito acima, pelo Lema 2.1.4, podemos assumir $N^4 = 1$ e $|[N,W]| = 2$. Suponha $a,b \in N$ quaisquer. Caso $[a,b] = 1$, obviamente $[a^2,b] = 1$; caso contrário, também temos $[a^2,b] = 1$ pois $[N,W]$ possui ordem 2. Temos, portanto, $N^2 \leq Z(N)$. Como N/N^2 é um 2-grupo de exponente 2, temos que N/N^2 é abeliano e, portanto, é um $\mathbb{F}_2$ espaço vetorial de dimensão no máximo r, donde, pela definição de $V(G,r)$, temos $[N,V] \leq N^2$. Desta forma, dados $a \in N$ e $v \in V$, temos $[a,v] \in N^2$, e, uma vez que $N^2 \leq Z(N)$, temos:

$$(a^2)^v = (a^v)^2 = (a[a,v])^2 = a^2.$$

Portanto $[N^2,V] = 1$, donde $[N,V,V] = 1$ e, pelo item (iii) do Teorema 1.1.1:

$$[N,W] = [N,V^2] \leq [N,V]^2[N,V,V] = 1,$$

o que é uma contradição. Portanto $[N,W] \leq N^4$.

□

Com este último resultado, é simples demonstrarmos o teorema que tínhamos por objetivo desta seção. Perceba que, pela sua definição, é fácil ver que $V(G,r)$ e, portanto, $V(G,r)^2$ são subgrupos característicos de G.

Teorema 2.2.5. Seja G um p-grupo finito de posto r. Então G possui um subgrupo característico *powerful* de índice menor ou igual a $2^{r\lambda(r)}$, se p é ímpar; ou $2^{r+r\lambda(r)}$, se $p = 2$.

Demonstração. Pelo Lema 2.2.3, $G/V(G,r)$ possui uma série de subgrupos normais de comprimento no máximo $\lambda(r)$ com fatores abelianos elementares. Como o posto de G é r, temos que cada fator tem ordem no máximo p^r. Desta forma, temos $[G : V(G,r)] \leq p^{r\lambda(r)}$. Caso p seja ímpar, temos, pela Proposição 2.2.4, que $V(G,r)$ é um subgrupo *powerful* como desejado. Caso $p = 2$, temos, pela mesma proposição, que $V(G,r)^2$ é *powerful*. Além disso, como $V(G,r)/V(G,r)^2$ é abeliano, temos $[V(G,r) : V(G,r)^2] \leq 2^r$, donde $[G : V(G,r)^2] \leq 2^{r+r\lambda(r)}$.

□

2.3 Os subgrupos omega de um p-grupo *powerful*

Nesta seção, traremos alguns resultados acerca dos subgrupos Omega de um p-grupo *powerful*. A maioria dos resultados aqui trazidos, estão no artigo "*Omega subgroups of powerful*

p-groups" de Gustavo A. Fernández-Alcober ([8]). O lema a seguir, porém, é um exercício do segundo capítulo de [6].

Lema 2.3.1. Se N p.e. G e M p.e. G, então $[N^{p^i}, M^{p^j}] = [N,M]^{p^{i+j}}$, para todo i e j.

Demonstração. Para demonstrar este resultado, basta aplicarmos indução sobre $i+j$. Demonstremos primeiramente a nossa base de indução, isto é, o caso em que $i+j=1$. Suponha, sem perda de generalidade, que $i=1$. É fácil ver que $[N,M,G,G] \leq [N,M]^p$ e $[N,M,G,G] \leq [N^p,M]$, por isso, analisaremos o quociente de G pelo subgrupo $[N,M,G,G]$, no qual $[N,M,G]$ é central. De forma análoga ao que foi feito na demonstração da Proposição 2.1.6, podemos conseguir que, dados $n \in N$ e $m \in M$ quaisquer, temos $[n^p,m] = [n,m]^p[n,m,n]^{\frac{p(p-1)}{2}}$, donde, como $[N,M,G] \leq [N,M]^p$ (pela Proposição 2.1.7), temos $[N^p,M] \leq [N,M]^p$. Por outro lado, pelo item (iii) do Teorema 1.1.1, temos $[n,m,n] = [n,m]^{-1}[n^2,m][n,m]^{-1}$, donde $[n,m,n] \in [N^p,M]$ e, portanto, $[N,M]^p \leq [N^p,M]$. Logo, $[N^p,M] = [N,M]^p$.

Suponha, agora, que o resultado vale para todo i' e j' tais que $i'+j' = i+j$. Como M é *powerful* e M^p p.e. G, temos, aplicando a hipótese de indução, que:

$$[N^{p^i}, M^{p^j}] = [(N^p)^{p^{i-1}}, M^{p^j}] = [N^p,M]^{p^{i+j-1}} = ([N,M]^p)^{p^{i+j-1}}.$$

Logo, como $[N,M]$ é *powerful*, temos o resultado desejado.

□

No teorema a seguir, dado um grupo G, um subgrupo H e um subgrupo normal N, diremos que H é cíclico sobre N se HN/N é cíclico.

Teorema 2.3.2. Seja G um p-grupo *powerful*. Então, para todo inteiro $i > 0$, temos:

(i) Se $x,y \in G$ e $o(y) \leq p^i$, então $o([x,y]) \leq p^i$.

(ii) Dados $x,y \in G$ com $o(x) \leq p^{i+1}$ e $o(y) \leq p^i$, temos $o([x^{p^j}, y^{p^k}]) \leq p^{i-j-k}$, para todo $j,k \geq 0$.

(iii) Se p é ímpar, então $\exp \Omega_i(G) \leq p^i$.

(iv) Se $p=2$, então $\exp \Omega_i(T) \leq 2^i$, para todo subgrupo T de G que é cíclico sobre G^2. Em particular, $\exp \Omega_i(G^2) \leq 2^i$.

Demonstração. Para demonstrarmos este teorema, aplicaremos uma indução sobre a ordem de G em todas as afirmações, simultaneamente. Note que, se G é cíclico de ordem p, os resultados são triviais. Suponha, agora, que as afirmações (i), (ii), (iii) e (iv) são válidas para qualquer p-grupo *powerful* de ordem menor que $|G|$. Caso G seja abeliano, não há o que provar. Desta forma, assumiremos que G é não abeliano.

(i) Suponha $x, y \in G$ com $o(y) \leq p^i$. Pelo Lema 2.1.4, temos que $T = \langle y, G' \rangle$ é *powerful*, uma vez que G' p.e. G. Note que $[x,y] \in \Omega_i(T)$ (pois $o((y^{-1})^x) = o(y) \leq p^i$), portanto, é suficiente provar que $\exp \Omega_i(T) \leq p^i$. Provemos, primeiramente, o caso em que p é ímpar. Note que T é um subgrupo próprio de G, pois, caso contrário, teríamos que $G/[G,G]$ é cíclico, o que implicaria $[[G,G],G] = [G,G]$, donde teríamos $[G,G] = 1$ e que G é abeliano. Então, $|T| < |G|$. Logo, aplicando, pela hipótese de indução, a afirmação (iii), temos $\exp \Omega_i(T) \leq p^i$.

Provemos, agora, o caso em que $p = 2$. Novamente pelo Lema 2.1.4, temos que $H = \langle y, G^2 \rangle$ é *powerful*. Note que H é próprio, pois, caso contrário, teríamos que G é cíclico. Além disso, note que T é um subgrupo de H e que T é cíclico sobre H^2 (pois $G' \leq G^4 \leq H^2$). Portanto, aplicando, pela hipótese de indução, a afirmação (iv), temos $\exp \Omega_i(T) \leq p^i$.

(ii) Suponha $x, y \in G$, com $o(x) \leq p^{i+1}$ e $o(y) \leq p^i$. Aplicaremos indução inversa sobre i. Seja $p^e = \exp G$. Pelo Lema 2.3.1, temos $[x^{p^j}, y^{p^k}] \in [G,G]^{p^{j+k}}$, donde, se $i \geq e$, não há mais o que provar. Desta forma, está provada a base da indução reversa. Seja, portanto, $i < e$ e suponha que o resultado é válido para todo i' tal que $i' > i$. Tome $T = \langle x, [x, y^{p^k}] \rangle$, como G não é abeliano, temos que T é um subgrupo próprio de G. Pela segunda versão dada da Fórmula de Compilação de Hall (Teorema 1.2.10), temos:

$$[x^{p^j}, y^{p^k}] \equiv [x, y^{p^k}]^{p^j} \mod \gamma_2(T)^{p^j} \gamma_p(T)^{p^{j-1}} \cdots \gamma_{p^j}(T).$$

Pelo item (i) deste teorema, temos $o([x, y^{p^k}]) \leq o(y^{p^k}) \leq p^{i-k}$, donde $[x, y^{p^k}]^{p^j} \in \Omega_{i-j-k}(T)$. Note que $T \leq \langle x, G' \rangle$, donde, pelo mesmo argumento utilizado na demonstração do item anterior, temos $\exp \Omega_n(T) \leq p^n$. Mas $x, [x, y^{p^k}] \in \Omega_{i+1}(T)$, donde $T = \Omega_{i+1}(T)$ e $\exp(T) \leq p^{i+1}$. Note que é suficiente provar que todos os subgrupos que aparecem no módulo da congruência acima estão contidos em $\Omega_{i-j-k}(T)$.

Sabemos que $o([x, y^{p^k}]) \leq p^{i-k}$, donde $o([x, y^{p^k}, x]) \leq p^{i-k}$ e $\gamma_2(T) = \langle [x, y^{p^k}, x]^t \mid t \in T \rangle \leq \Omega_{i-k}(T)$. Como $\gamma_2(T)$ é *powerful*, temos $\gamma_2(T)^{p^j} \leq \Omega_{i-j-k}(T)$. Provaremos por indução sobre r que $\gamma_{r+2}(T) \leq \Omega i - k - r(T)$, para todo inteiro positivo r. O caso base ($r = 0$) está feito acima. Basta mostrarmos que, dados $a \in \gamma_{r+1}(T)$ e $b \in T$, temos $o([a,b]) \leq p^{i-k-r}$. Pela hipótese de indução, $\gamma_{r+1}(T) \leq \Omega_{i-j-k+1}(T)$, donde $o(a) \leq p^{i-k-r-1}$. Note, porém, que $\gamma_2(T) \leq [G, G^{p^k}, G] = [G^{p^k}, G, G]$, logo, $a \in \gamma_{r+1}(T) \leq [G^{p^k}, {}_{r+1}\, G] \leq G^{p^{k+r+1}}$. Portanto, $a = g^{p^{k+r+1}}$, para algum $g \in G$, donde $o(g) \leq p^{i+2}$. Porém, $o(b) \leq p^{i+1}$ (pois $\exp(T) \leq p^{i+1}$), então, podemos aplicar a hipótese de indução da indução reversa. Desta forma, temos $o([a,b]) = o([g^{p^{k+r+1}}, b]) \leq p^{i+1-f-r+1} = p^{i-k-r}$. Portanto, $\gamma_{r+2}(T) \leq \Omega_{i-k-r}(T)$.

Provaremos, agora, que os subgrupos presentes no módulo acima estão contidos em $\Omega_{i-j-k}(T)$. Caso p seja ímpar, temos que $p^r \geq r+2$, para todo $r \geq 1$, donde $\gamma_{p^r}(T) \leq \gamma_{r+2}(T) \leq \Omega_{i-k-r}(T)$ e $\gamma_{p^r}(T)^{p^{j-r}} \leq \Omega_{i-j-k}$. Caso $p = 2$, temos, de forma análoga $\gamma_{r+2}(T) \leq \Omega_{i-k-r}(T)$, para $r \geq 2$. Resta mostrarmos que $\gamma_2(T)^{p^{j-1}} \leq \Omega_{i-j-k}(T)$. Temos, porém, que $[x, y^{2^k}] \leq G^{2^{k+2}}$, donde $[x, y^{2^k}, x] \leq [g^{2^{k+2}}, x]$, para algum $g \in G$ com $o(g) \leq 2^{i+2}$ (pois $o(y^{p^k}) \leq p^{i-k}$). Portanto, pela hipótese de indução da indução reversa, temos $[x, y^{2^k}, x] \leq 2^{i-k-1}$, donde $\gamma_2(T)^{p^{j-1}} \leq \Omega_{i-j-k}(T)$. Logo, temos o resultado desejado.

(iii) Suponha que p seja ímpar e que $x, y, z \in G$ sejam elementos de ordem p. Temos que $[x, y] \in G^p$ é um elemento de ordem no máximo p, logo, $[x, y] = g^p$ para algum $g \in G$ tal que $o(g) \leq p^2$. Portanto, pelo item (ii) deste teorema, temos $[x, y, z] = [g^p, z] = 1$. Logo, a classe de nilpotência de $\Omega_1(G)$ é no máximo 2, donde $\Omega_1(G)$ é regular (pelo Teorema 1.2.13). Desta forma, $\exp \Omega_1(G) \leq p$ (pelo Teorema 1.2.14). Pela hipótese de indução que fizemos no início da demonstração deste teorema, temos $\exp_{i-1}(G/\Omega_1(G)) \leq p^{p-1}$. Seja g um gerador de $\Omega_i(G)$, então $g\Omega_i(G) \in \Omega_{i-1}(G/\Omega_1(G))$ e, portanto, $\Omega_i(G)/\Omega_1(G) \leq \Omega_{i-1}(G/\Omega_1(G))$, donde, $\exp \Omega_i(G)/\Omega_1(G) \leq p^{i-1}$. Por fim, como $\exp \Omega_1(G) \leq p$, temos $\exp \Omega_i(G) \leq p^i$.

(iv) Suponha $p = 2$. Seja $T \leq G$ um subgrupo cíclico sobre G^2 qualquer. Note que, se provarmos o resultado para TG^2, obviamente ele estará provado para T, desta forma, como TG^2 é, também, cíclico sobre G^2, simplesmente consideraremos $G^2 \leq T$. Note que T é normal em G, pois $[G, G] \leq G^4 \leq T$. Mostraremos que $\Omega_1(T)$ é abeliano.

Tome $a, b \in T$ com $o(a) = o(b) = 2$ quaisquer. Caso $a \in G^2$ ou $b \in G^2$, temos, pelo item (ii) deste teorema, que $[a, b] = 1$. Suponhamos, agora, $a, b \in T \setminus G^2$. Como T é cíclico sobre G^2 e $o(a) = o(b) = 2$, temos $aG^2 = bG^2$, donde $b = av$, para algum $v \in G^2$. Desta forma, temos $v = ab$, donde $v^2 = [a, b] = [a, av]$. Logo, $v^2 = [a, v]$ e, uma vez que G^2 p.e. G, $v^2 \in G^8$. Portanto, existe $u \in G^4$ tal que $u^2 = v^2$. Note que, pelo item (i) deste teorema, $o(v^2) \leq 2$, donde $o(u) = o(v) \leq 4$. Logo, pelo item (ii) deste teorema, u e v comutam.

Seja $w = v^{-1}u$ (donde $w \in G^2$). Obviamente w comuta com v e, além disso, pelo item (ii), w comuta com a. Logo:

$$(au)^2 = (avw)^2 = (av)^2 w^2 = b^2 (v^2)^{-1} u^2 = 1$$

Aplicaremos, agora, a hipótese de indução feita no início da demonstração deste teorema sobre o grupo $\langle a, G^2 \rangle$. Note que $G^4 \leq \langle a, G^2 \rangle^2$, donde $\langle a, G^4 \rangle$ é cíclico sobre

$\langle a, G^2\rangle^2$. Portanto, $\exp\Omega_1(\langle a, G^4\rangle) \leq 2$ e, uma vez que $a, au \in \Omega_1(\langle a, G^2\rangle)$, temos que u tem ordem no máximo 2. Desta forma, $[a,b] = v^2 = u^2 = 1$.

Por fim, temos que $\Omega_1(T)$ é abeliano, donde $\exp\Omega_1(T) \leq 2$. De forma análoga ao demonstrado no item (iii), temos, de $\exp\Omega_{i-1}(T/\Omega_1(T)) \leq 2^{i-1}$ e $\exp\Omega_1(T) \leq 2$, que $\exp\Omega_i(T) \leq 2^i$.

□

Dado G um 2-grupo *powerful*, em geral não podemos afirmar que o expoente do subgrupo $\Omega_1(G)$ é igual 2. Um exemplo que nos mostra isso é o grupo $G = \langle a, x, y \mid a^4 = x^2 = 1, y^4 = a^2, [x,a] = a^2, [x,y] = [a,y] = 1\rangle$. Este grupo é *powerful*, uma vez que $G' = G^4 = \langle a^2\rangle$, mas temos $\Omega_1(G) = \langle a, x\rangle$, donde $\Omega_1(G)$ tem expoente 4.

Continuamos, agora, com um corolário do último teorema.

Corolário 2.3.3. Seja G um 2-grupo *powerful*. Então:

(i) $\exp[\Omega_i(G), G] \leq 2^i$.

(ii) $\exp\Omega_i(G) \leq 2^{i+1}$.

Demonstração.

(i) Pelo item (i) do Teorema 2.3.2, temos que $[\Omega_i(G), G]$ pode ser gerado por elementos de ordem menor ou igual a 2^i. Como G é *powerful*, temos $[\Omega_i(G), G] \leq G^2$. Portanto, $[\Omega_i(G), G] \leq \Omega_i(G^2)$ e basta, então, aplicarmos o item (iv) do Teorema 2.3.2 e teremos o resultado desejado.

(ii) Como observado na demonstração do item anterior, temos $[\Omega_i(G), G] \leq \Omega_i(G^2)$, consequentemente, $\Omega_i(G)/\Omega_i(G^2)$ é um grupo abeliano. Note, porém, que $\Omega_i(G)/\Omega_i(G^2)$ pode ser gerado por elementos de ordem 2, donde $\exp(\Omega_i(G)/\Omega_i(G^2)) \leq 2$. Podemos, então, concluir a partir do item (i) deste corolário que $\exp\Omega_i(G) \leq 2^{i+1}$.

□

Lema 2.3.4. Seja G um p-grupo *powerful* de exponente p^e. Então, para todo $0 \leq i \leq e-1$, dados $x \in G$ e $y \in G^{p^{e-i-1}}$, temos $(xy)^{p^i} = x^{p^i} y^{p^i}$.

Demonstração. Pela segunda versão dada da Fórmula de Compilação de Hall (Teorema 1.2.10), temos:

$$(xy)^{p^i} \equiv x^{p^i} y^{p^i} \mod \gamma_2(H)^{p^i} \gamma_p(H)^{p^{i-1}} \cdots \gamma_{p^i}(H),$$

onde $H = \langle x, y \rangle$. Mostraremos que todos os grupos no módulo da congruência acima são triviais. Suponhamos, primeiramente, p ímpar. Note que $\gamma_2(H) \leq [G^{p^{e-i-1}}, G]$, donde, como $G^{p^{e-i-1}}$ p.e. G, temos $\gamma_2(H) \leq G^{p^{e-i}}$. Logo, $\exp \gamma_2(H) \leq p^i$ e, portanto, $\gamma_2(H)^{p^i} = 1$.

Suponha, agora, $p = 2$. Então temos $\gamma_2(H) \leq [G^{p^{e-i-1}}, G]$, o que implica $\gamma_2(H) \leq G^{p^{e-i+1}}$. Portanto, $\exp \gamma_2(H) \leq p^{i-1}$ e $\gamma_2(H)^{p^{i-1}} = 1$. O restante dos grupos no módulo, tanto no caso $p = 2$, quanto no caso em que p é ímpar, serão triviais devido ao fato de que G^{p^n} p.e. G, para todo inteiro positivo n. Por fim, temos $(xy)^{p^i} = x^{p^i} y^{p^i}$.

□

Definimos $\Omega_{\{i\}}(G)$ como o conjunto $\{x \in G \mid x^{p^i} = 1\}$. Dado um conjunto qualquer A, considere $|A|$ a cardinalidade de A.

Teorema 2.3.5. Seja G um p-grupo *powerful*. Então $[G : G^{p^i}] = |\Omega_{\{i\}}(G)|$, para todo inteiro positivo i.

Demonstração. Para demonstrarmos este resultado, aplicaremos indução sobre a ordem de G. O caso base para esta indução é trivial. Suponha que o resultado é válido para os p-grupos *powerful* cujas ordens são menores que $|G|$. Seja p^e o exponente de G. Obviamente, só precisamos considerar o caso em que $i \leq e-1$. Por outro lado, pelo Lema 2.3.4, temos que o mapeamento $x \mapsto x^{p^{e-1}}$ induz um homomorfismo sobrejetor de G em $G^{p^{e-1}}$, desta forma, pelo Teorema do Homomorfismo, temos $|\Omega_{e-1}| = [G : G^{p^{e-1}}]$.

Assumiremos, então, a partir de agora $i \leq e-2$. Defina $\overline{G} = {}^{G}\!/_{G^{p^{e-1}}}$ e $X = \{x \in G \mid x^{p^i} \in G^{p^{e-1}}\}$. Pela hipótese de indução, temos $[G : G^{p^i}] = [\overline{G} : \overline{G}^{p^i}] = |\Omega_{\{i\}}(\overline{G})| = |X|/|G^{p^{e-1}}|$, donde nos basta mostrar que $|X| = |\Omega_{\{i\}}(G)||G^{p^{e-1}}|$.

Note que $x \in X$ se, e somente se, existe $y \in G^{p^{e-i-1}}$ tal que $x^{p^i} = y^{p^i}$, o que, pelo Lema 2.3.4, ocorre se, e somente se, $xy^{-1} \in \Omega_{\{i\}}(G)$. Desta forma, $X = \Omega_{\{i\}}(G)G^{p^{e-i-1}}$ é a união das classes laterais de elementos de $\Omega_{\{i\}}(G)$ com respeito ao subgrupo $G^{p^{e-i-1}}$. Portanto, para encontrarmos $|X|$, encontraremos quantas classes laterais desse tipo existem.

Seja $gG^{p^{e-i-1}}$ uma classe lateral tal que $g \in \Omega_{\{i\}}(G)$. Novamente pelo Lema 2.3.4, temos que os de elementos em $gG^{p^{e-i-1}}$ que possuem ordem menor ou igual a p^i são exatamente os elementos de $g(\Omega_{\{i\}}(G) \cap G^{p^{e-i-1}}) = g\Omega_{\{i\}}(G^{p^{e-i-1}})$. Note, porém, que independente do elemento g escolhido, temos $|g\Omega_{\{i\}}(G^{p^{e-i-1}})| = |\Omega_{\{i\}}(G^{p^{e-i-1}})|$. Desta forma, como o números de elementos de ordem menor ou igual a p^i em G é $|\Omega_{\{i\}}(G)|$, temos que o número de classes laterais do tipo desejado é $|\Omega_{\{i\}}(G)|/|\Omega_{\{i\}}(G^{p^{e-i-1}})|$. Logo, temos:

$$|X| = \frac{|\Omega_{\{i\}}(G)|}{|\Omega_{\{i\}}(G^{p^{e-i-1}})|} |G^{p^{e-1}}|.$$

Porém, como $i \leq e-2$, temos que $G^{p^{e-i-1}}$ é *powerful* e um subgrupo próprio de G, desta forma, pela hipótese de indução, temos $|\Omega_{\{i\}}(G^{p^{e-i-1}})| = [G^{p^{e-i-1}} : G^{p^{e-1}}]$ e, portanto, $|X| = |\Omega_{\{i\}}(G)||G^{p^{e-1}}|$, como desejávamos.

□

Definição 2.3.6. O conjunto $\{a_1, a_2, \cdots, a_d\}$ é dito uma base de um grupo G se, para cada elemento $g \in G$, temos $g = a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_d^{\alpha_d}$, onde α_i é um inteiro não negativo menor que a ordem de a_1, expresso de forma única.

Esta definição é equivalente à afirmação: $G = \langle a_1, a_2, \cdots, a_d \rangle$ e $|G| = |\langle a_1 \rangle||\langle a_2 \rangle| \cdots |\langle a_d \rangle|$. Note, então, que a ordem dos elementos na base não é importante. Desta forma, sempre assumiremos $o(a_1) \geq o(a_2) \geq \cdots \geq o(a_d)$.

O resultado a seguir é um exercício de [6].

Proposição 2.3.7. Se G é um p-grupo *powerful*, então G possui uma base de cardinalidade $d(G)$.

Demonstração. Para provarmos este resultado, utilizaremos indução sobre $|G|$. Se G tem ordem p, o resultado é trivial. Suponha, agora, que o resultado vale para p-grupos *powerful* de ordem menor que $|G|$. Seja n o inteiro tal que $G^{p^n} > G^{p^{n+1}} = 1$. Pela hipótese de indução, existe um conjunto $\{x_1 G^{p^n}, \cdots, x_d G^{p^n}\}$ que é base de G/G^{p^n}, onde $d = d(G/G^{p^n})$.

Como $G^{p^n} \leq \Phi(G)$, temos $d = d(G)$ e $G = \langle x_1, \cdots, x_d \rangle$, donde $G^{p^n} = \langle x_1^{p^n}, \cdots, x_d^{p^n} \rangle$. Seja s o menor inteiro tal que $G^{p^n} = \langle x_1^{p^n}, \cdots, x_s^{p^n} \rangle$. Como G^{p^n} é central, e, portanto, abeliano, temos que $\{x_1^{p^n}, \cdots, x_s^{p^n}\}$ é uma base de G^{p^n}. Se $s x_k = d$, temos, então, que $\{x_1, \cdots, x_d\}$ é uma base de G. Suponhamos, agora, $s < d$.

Tome k tal que $s < k \leq d$. Seja p^l a ordem de $x_k G^{p^n}$ em G/G^{p^n}. Note que, uma vez que $x_k^{p^l} \in G^{p^n}$, temos:

$$\begin{aligned} x_k^{p^l} &= (x_1^{p^n})^{\alpha_1} \cdots (x_s^{p^n})^{\alpha_s} \\ &= (x_1^{p^{n-l}\alpha_1})^{p^l} \cdots (x_s^{p^{n-l}\alpha_s})^{p^l}, \end{aligned}$$

para alguns α_i, $i = 1, \cdots, s$, inteiros. Perceba que $x_i^{p^{n-l}\alpha_i} \in G^{p^{n-l}}$, para $i = 1, \cdots, s$. Desta forma, tomando $w = x_1^{-p^{n-l}\alpha_1} \cdots x_s^{-p^{n-l}\alpha_s}$, temos, pelo Lema 2.3.4, que $x'_k = x_k w$ tem ordem p^l. Afirmamos que $\{x_1, \cdots, x_s, x'_{s+1}, \cdots, x'_d\}$ é uma base de G. Note que:

$$\begin{aligned} |G/G^{p^n}| = |G|/|G^{p^n}| &= |\langle x_1 G^{p^n} \rangle| \cdots |\langle x_s G^{p^n} \rangle||\langle x_{s+1} G^{p^n} \rangle| \cdots |\langle x_d G^{p^n} \rangle| \\ &= |\langle x_1 G^{p^n} \rangle| \cdots |\langle x_s G^{p^n} \rangle||\langle x'_{s+1} \rangle| \cdots |\langle x'_d \rangle| \\ &= |\langle x_1 \rangle| \cdots |\langle x_s \rangle||\langle x'_{s+1} \rangle| \cdots |\langle x'_d \rangle|/p^s. \end{aligned}$$

Donde, uma vez que $|G^{p^n}| = p^s$, temos:

$$|G| = |\langle x_1\rangle|\cdots|\langle x_s\rangle||\langle x'_{s+1}\rangle|\cdots|\langle x'_d\rangle|.$$

Portanto, $\{x_1,\cdots,x_s,x'_{s+1},\cdots,x'_d\}$ é uma base de G.

□

Note que se p é ímpar, então $G^2 = G$, portanto, para simplificar a escrita do próximo resultado, utilizaremos $N = G^2$. Finalizamos esta seção com o lema a seguir, que está presente no artigo [1] e nos será útil no capítulo 5 desta dissertação.

Lema 2.3.8. Seja G um p-grupo *powerful*, e seja $N = G^2$. Se $\{a_1,a_2,\cdots,a_d\}$ é uma base de N, com $d = d(N)$, e $o(a_i) = m_i$, com $i = 1,2,\cdots,d$, então:

$$\Omega_1(N) = \langle a_i^{m_i/p} \mid i = 1,2,\cdots,d\rangle.$$

Demonstração. Perceba, primeiramente, que N é *powerful*e que $\langle a_i^{m_i/p} \mid i = 1,2,\cdots,d\rangle \subseteq \Omega_1(N)$. Note que, como $\{a_1,a_2,\cdots,a_d\}$ é uma base de N, temos que $\langle a_i^{m_i/p} \mid i = 1,2,\cdots,d\rangle$ tem no mínimo p^d elementos. Mas, pelo Teorema 2.3.5, temos:

$$|\Omega_1(N)| = [N : N^p] = [N : \Phi(N)] = p^d,$$

donde $\Omega_1(N) = \langle a_i^{m_i/p} \mid i = 1,2,\cdots,d\rangle$.

□

Capítulo 3

Coclasse de p-grupos

Neste capítulo estudaremos algumas propriedades de p-grupos a partir de suas coclasses, para isso, introduziremos algumas ferramentas nas duas primeiras seções. Os resultados aqui presentes podem ser encontrados nos capítulos 4 e 6 de [17]. Nosso objetivo principal é demonstrar os Teoremas 3.3.9 e 3.3.10, nos quais mostramos que, dado um p-grupo G de coclasse r, existe uma função $m(p,r)$ tal que, para todo $i \geq m(p,r)$, G age uniserialmente sobre $\gamma_i(G)$, $\gamma_i(G)^p = \gamma_{i+d(\gamma_m(G))}(G)$ e $d(\gamma_m(G)) = (p-1)p^s$, onde $0 \leq s \leq r+1$, se $p = 2$, e $0 \leq s \leq r-1$, se p é ímpar. Também temos como objetivo demonstrar o Corolário 3.3.3, que nos dá que, dado um p-grupo G de coclasse r, o subgrupo $\gamma_i(G)$ é *powerful* para todo $i \geq r$, se p é ímpar, e para todo $i \geq r+2$, caso contrário. Para atingirmos tais objetivos, provaremos muitos resultados que não serão novamente usados nos demais capítulos desta dissertação.

3.1 Ações uniseriais

Nesta primeira seção, estudaremos as ações uniseriais, que serão uma importante ferramenta para o estudo de coclasse de p-grupos. Nesta seção, G e N serão p-grupos finitos, com G agindo sobre N. Por vezes nos será útil trabalhar com o grupo $N \rtimes G$ obtido através desta ação. Dado $H \leq N$ qualquer, denotamos:

$$H_1 = H,\ H_{i+1} = [H_i, G].$$

Em geral, não podemos afirmar que H_i é normal em H, mas, como $[H,G] \trianglelefteq H$, temos $H_{i+1} \trianglelefteq H_i$, para $i \geq 1$. Além disso, como $H \rtimes G$ é um p-grupo e, portanto, nilpotente, temos que $H_m = 1$ para algum $m \geq 1$. Desta forma, se M é um subgrupo G-invariante ($[M,G] \leq M$) minimal, então $[M,G] = 1$.

Iniciemos com a definição de ação uniserial.

Definição 3.1.1. Dizemos que G age uniserialmente sobre N se, para todo H subgrupo G-invariante e não trivial de N, temos que $[H,G]$ tem índice p sobre H.

O lema a seguir nos dá uma condição necessária e suficiente para que uma ação de grupos seja uniserial.

Lema 3.1.2. A ação de G em N é uniserial se, e somente se, $N = N_1 > N_2 > \cdots > N_{n+1} = 1$ e $[N_i : N_{i+1}] = p$, para $i = 1, \cdots, n$. Se G age uniserialmente em N, então os subgrupos N_i são todos os subgrupos G-invariantes de N.

Demonstração. Primeiramente, provaremos que se $N = N_1 > N_2 > \cdots > N_{n+1} = 1$ e $[N_i : N_{i+1}] = p$, então os subgrupos N_i são todos os subgrupos G-invariantes de N. Para isso, utilizaremos indução sobre n, o número de subgrupos N_i não triviais. Note que, se $n = 1$, então N é cíclico de ordem p, donde N_1 é o único subgrupo não trivial de N. Suponha, agora, $n \geq 2$ e que o resultado é válido para $n-1$. Seja $S \leq N$ um subgrupo G-invariante, então, aplicando a hipótese de indução no grupo N_2, temos que $N_2 \cap S = N_i$, para algum $i \geq 2$. Se $S \leq N_2$, temos $S = N_i$. Se S não está contido em N, temos $SN_2 = N$ (pois N_2 é um subgrupo maximal de N), mas $[S,G] \leq [N,G] = N_2$, donde $[S,G] = N_j$, para algum $j \geq 2$ e, portanto, $N_2 = [N,G] = [SN_2,G] = [S,G][N_2,G] = [S,G]N_3$. Temos, então, $[S,G] = N_2$, donde, como N_2 é maximal, $S = N$.

Note que se a ação de G sobre N é uniserial, então é trivial que $N = N_1 > N_2 > \cdots > N_{n+1} = 1$ e $[N_i : N_{i+1}] = p$, para $i = 1, \cdots, n$. Supondo, agora, que $N = N_1 > N_2 > \cdots > N_{n+1} = 1$ e $[N_i : N_{i+1}] = p$, temos que os subgrupos N_i são todos os subgrupos G-invariantes de N, donde temos que G age uniserialmente em N.

□

Corolário 3.1.3. Se G age uniserialmente em N, então os subgrupos N_i, com $i \geq 1$, são normais em N.

Demonstração. Para demonstrar este resultado, aplicaremos indução sobre o número de subgrupos N_i não triviais, denotaremos este número por n. Obviamente, se $n = 1$, temos que $N_1 = N$ é normal em N. Suponha agora $n \geq 2$ e que o resultado é válido para $n-1$. Note que $Z(N)$ é um subgrupo G-invariante, desta forma, como N_n tem ordem p, temos, pelo lema anterior, $N_n \leq Z(N)$. Aplicando, portanto, a hipótese de indução sobre N/N_n, temos o resultado desejado.

□

Corolário 3.1.4. Suponha $N_{d+1} \trianglelefteq N$, com G agindo uniserialmente sobre N/N_{d+1}, e seja $H \trianglelefteq N$ um subgrupo G-invariante de índice p^i em N, com $i \leq d$. Então $H = N_{i+1}$.

Demonstração. Note que G age sobre ${}^{N}\!/_{H}$, que é um grupo de ordem p^i. Desta forma, $[{}^{N}\!/_{H},\ {}_i\, G] = 1$, donde $N_{d+1} \leq N_{i+1} \leq H$. Desta forma, aplicando o Lema 3.1.2 sobre ${}^{N}\!/_{N_{d+1}}$, temos $H = N_j$, para algum j, donde, como $[{}^{N}\!/_{N_{d+1}} : {}^{H}\!/_{N_{d+1}}] = p^i$, temos $H = N_{i+1}$.

□

Na seção 3 do capítulo 1 vimos que os centralizadores de 2-passos (Definição 1.3.7) tem um papel fundamental na teoria de p-grupos de classe maximal. Neste capítulo nos será útil estender este conceito num contexto mais geral de ação de grupos.

Definição 3.1.5. Suponha que G aja uniserialmente sobre N e sejam m e i inteiros positivos tais que $1 \leq m \leq n - i + 1$. Definimos o m-ésimo centralizador de i-passos em G como o centralizador em G de ${}^{N_m}\!/_{N_{m+i}}$.

Lema 3.1.6. Suponha que G aja uniserialmente em N, seja $H \leq G$ um subgrupo contido em todo centralizador de i-passo em G e seja $K \leq G$ um subgrupo contido em todo centralizador j-passos em G. Então:

(i) $[H,K]$ está contido em todo centralizador de $(i+j)$-passos em G.

(ii) $\gamma_k(H)$ está contido em todo centralizador de (ki)-passos em G.

(iii) $[N_{i_1}, N_{i_2}] \leq N_{i_1+i_2}$, para todo $i_1, i_2 \geq 1$.

Demonstração.

(i) Suponha $m \geq 1$ um inteiro qualquer. Pelo Corolário 3.1.3, temos que N_{m+i+j} é normal em N, donde N_{m+i+j} é normal em $N \rtimes G$. Logo, pelo Lema dos Três Subgrupos (Teorema 1.1.3), temos:

$$[N_m, [H,K]] \leq [N_m, K, H][N_m, H, K] \leq [N_{m+j}, H][N_{m+i}, K] \leq [N_{m+j+i}].$$

(ii) Este resultado segue de uma indução simples utilizando o item (i) deste lema.

(iii) Note que $N \rtimes G$ age uniserialmente sobre N e que $N_{i_2} \leq \gamma_{i_2}(N \rtimes G)$, desta forma, temos $[N_{i_1}, N_{i_2}] \leq [[N_{i_1},\ {}_{i_2}\, N \rtimes G] = N_{i_1+i_2}$.

□

Definição 3.1.7. Suponha que G aja uniserialmente sobre N. Dado A um subgrupo ou um elemento de G, dizemos que A centraliza exatamente k-passos se A está em todos os centralizadores de k-passos e em nenhum centralizador de $(k+1)$-passos.

A seguir definimos a coclasse de um p-grupo, este é o tema principal deste capítulo e será mais abordado na última seção.

Definição 3.1.8. Dado G um grupo de ordem p^n e classe de nilpotência $c = n - r$, a coclasse de G é r.

Lema 3.1.9.

(i) Se $N \trianglelefteq G$, então a coclasse de G/N é menor ou igual à de G.

(ii) Se $N \trianglelefteq G$ e a coclasse de G/N é igual à de G, então $N = \gamma_i(G)$, para algum $i \geq 2$, e G age uniserialmente sobre N.

Demonstração. Sejam p^n a ordem G, r a coclasse de G, p^m a ordem de G/N e s a coclasse de G/N. Note que $\gamma_{n-r}(G) \neq 1$. Perceba, também, que $\gamma_{m-s+1}(G) \leq N$, donde $\gamma_{n-s}(G) \leq N_{n-m}$.

(i) Suponha, por absurdo, $s > r$. Temos, então, $\gamma_{n-(r+1)}(G) \leq \gamma_{n-s}(G) \leq N_{n-m}$, donde $\gamma_{n-r}(G) \leq N_{n-m+1} = 1$, o que é uma contradição.

(ii) Pelo item anterior, temos $\gamma_{n-r}(G) \leq N_{n-m}$, donde $N_{n-m} \neq 1$. Portanto, como $|N| = |G|/|G/N| = p^{n-m}$, temos que $N = N_1 > N_2 > \cdots > N_{n+1} = 1$ é uma cadeia tal que $[N_i : N_{i+1}] = p$, com $i = 1, \cdots, n$. Logo, pelo Lema 3.1.2, G age uniserialmente sobre N. Além disso, sabemos que $\gamma_{n-r}(G) \neq 1$, donde $|\gamma_{m-r+1}|(G) \geq p^{n-m} = |N|$. Logo, como $\gamma_{m-r+1}(G) \leq N$, temos $N = \gamma_{m-s+1}(G)$.

□

A seguir definimos o que é um quociente uniserial e nos próximos dois lemas mostramos algumas condições suficientes para que isso aconteça.

Definição 3.1.10. Dados $A, B \trianglelefteq G$, com $B \leq A$, dizemos que A/B é uma seção uniserial de G se a ação de G sobre A/B induzida pela conjugação é uniserial.

Lema 3.1.11. Sejam G um p-grupo de coclasse r e $K_0 \geq K_1 \geq \cdots \geq K_{r+t}$ uma série normal de G. Então pelo menos t seções desta série são uniseriais.

Demonstração. Seja u_i a coclasse de G/K_i, com $i = 0, 1, \cdots, r+t$. Note que, se $u_i = u_{i+1}$, então, pelo item (ii) do Lema 3.1.9, G age uniserialmente sobre K_i/K_{i+1}, pois $G/K_i \cong (G/K_{i+1})/(K_i/K_{i+1})$. Mas, pelo item (i) do Lema 3.1.9, temos $1 \leq u_0 \leq u_1 \leq \cdots \leq u_{r+t} \leq r$, donde $u_i = u_{i+1}$ para pelo menos t valores de i.

□

Lema 3.1.12. Sejam G um grupo finito e $A \geq C > B \geq D$ uma cadeia de subgrupos normais de G tal que A/B e C/D são uniseriais. Então A/D é uniserial.

Demonstração. Para provar este lema, aplicaremos indução sobre $[B:D]$. Se $[B:D]=1$, então $B=D$, donde A/D é uniserial. Suponha, agora $B>D$ e que o resultado é válido para subgrupos normais $A_1 \geq C_1 > B_1 \geq D_1$ com $[B_1:D_1] < [B:D]$.

Caso $[B:D] \geq p^2$, então existe $N \trianglelefteq G$ tal que $A \geq C > B > N > D$. Pela hipótese de indução, A/N é uniserial. Temos, então, $A \geq C > N > D$ com A/N e C/D uniseriais, logo, novamente pela hipótese de indução, temos que A/D é uniserial.

Caso $[B:D]=p$, suponha, por absurdo, que exista $M/D \leq A/D$ tal que $[M/D, G]=1$ e $M/D \neq B/D$. Assuma que M/D é o minimal. Então, $A \leq MB \leq B$ e $MB/B \cong (MB/D)/(B/D) \cong M$. Desta forma, MB/B é um subgrupo G-invariante de A/B, donde, como A/B é uniserial, temos $MB \leq C$ e, portanto, $M \leq C$. Logo, como C/D temos, pelo Lema 3.1.2, $M=B$, o que é uma contradição. Por fim, então, novamente pelo Lema 3.1.2, temos que A/D é uniserial.

□

Como o quociente $N/\Phi(N)$ é abeliano elementar, veremos que nos será útil ter alguns resultados a respeito de ações uniseriais sobre p-grupos abelianos elementares.

Teorema 3.1.13. Se G é um p-grupo finito agindo uniserialmente sobre um p-grupo abeliano elementar A, então $\Pi_i(G)$ centraliza exatamente p^i-passos.

Demonstração. Para demonstrarmos este resultado, utilizaremos indução sobre i. Para $i=0$ o resultado é trivial. Assuma, agora, $i \geq 1$ e que o resultado vale para $i-1$. Tome $j \geq 0$ qualquer. Dado $y \in \Pi_{i-1}(G)$, então $[A_j, y^p] = [A_j, {}_p\, y]$, pois A é abeliano elementar, donde $[A_j, y^p] \leq [A_j, {}_p\, \Pi_{i-1}(G)] \leq A_{j+p^{i-1}p} = A_{j+p^i}$. Portanto, $[A_j, \Pi_i(G)] \leq A_{j+p^i}$.

Para mostrarmos que $\Pi_i(G)$ não está contido em nenhum centralizador de (p^i+1)-passos, assumimos $A_{j+p^i} \neq 1$ e definimos C_k como o $(j+kp^{i-1}+1)$-ésimo centralizador de $(p^{i-1}+1)$-passos em G, com $k=0,1,\cdots,p-1$. Então, pela hipótese de indução, $C_k < \Pi_{i-1}(G)$. Note que um p-grupo qualquer não pode ser igual à união de p subgrupos próprios, pois cada um deles terá índice no mínimo p e eles possuem interseção não vazia. Portanto, existe $y \in \Pi_{i-1}(G)$ tal que $y \notin C_0 \cup C_1 \cup \cdots \cup C_{p-1}$.

Tome $a \in A_j \backslash A_{j-1}$, então, pela hipótese de indução, temos $[a, {}_p\, y] = [a, y^p] \in A_{j+p^i} \backslash A_{j+p^i+1}$. Logo, $[A_j, \Pi_i(G)] \leq A_{j+p^i}$ contém $[a, y^p]$ e, como $[A_j, \Pi_i(G)]$ é G-invariante com $[A_j, \Pi_i(G)] \not\leq A_{j+p^i+1}$, temos $[A_j, \Pi_i(G)] = A_{j+p^i}$. Como o inteiro j escolhido foi qualquer, temos o resultado desejado.

□

Corolário 3.1.14. Seja G um p-grupo finito com $\Pi_i(G) = \langle 1 \rangle$ e seja A um p-grupo abeliano elementar. Se G age uniserialmente sobre A/A_{p^i+1}, então $A_{p^i+1} = 1$.

Demonstração. Suponha $A_{p^i+1} \neq 1$ e tome $B \leq A_{p^i+1}$, com $[A_{p^i+1} : B] = p$ e $B \geq A_{p^i+2}$. Então G age uniserialmente sobre A/B e, pelo Teorema 3.1.13, $[A/B, \Pi_i(G)] = (A/B)_{p^i+1}$. Mas $(A/B)_{p^i+1} = A_{p^i+1}/B$, que não é trivial, o que é um absurdo, pois $\Pi_i(G) = 1$. Portanto, $A_{p^i+1} = 1$.

□

O Teorema 3.1.16 nos dá uma generalização do Teorema 3.1.13. Nele, o número $f_d(i)$, definido a seguir, desempenhará o papel que p^i desempenhou no Teorema 3.1.13.

Definição 3.1.15. Dados dois inteiros $i \geq 0$ e $d \geq 1$, definimos o inteiro $f_d(i)$ da seguinte forma:

$$f_d(0) = 1 \text{ e } f_d(i+1) = \min(pf_d(i), f_d(i) + d), \text{ para todo } i \geq 0.$$

Claramente $f_d(i) \geq p^i$, para todo $i \geq 0$, e é fácil mostrar por indução que se j é o menor inteiro tal que $d < p^{j+1} - p^j$, então $f_d(i)$ é igual a:

$$\begin{cases} p^i, & \text{se } 0 \leq i \leq j \\ p^j + (i-j)d, & \text{se } i \geq j \end{cases}$$

Teorema 3.1.16. Suponha que G age uniserialmente sobre N. Seja $d(N) = d$. Suponha que $[N_j, N] \leq N_j^p$ e que $N_j^p = N_{j+d}$, para todo $j \geq 1$. Então $\Pi_i(G)$ está contido em todo centralizador de $f_d(i)$-passos.

Além disso, se $d \neq (p-1) \times$ (uma potência de p), então $\Pi_i(G)$ centraliza exatamente $f_d(i)$-passos.

Demonstração. Tome $x \in N_j$ e $y \in G$ tal que y está em todo centralizador de k-passos. Então, pelo Corolário 1.1.2 e utilizando as hipóteses sobre N, temos $[x, y^p] \equiv [x,y]^p [x, {}_p\, y] \mod N_{j+2k+d}$. Em particular, temos $[x, y^p] \in N_{j+m}$, com $m = \min(k+d, pk)$, (pois $[x,y]^p \in N_{j+k+d}$, $[x, {}_p\, y] \in N_{j+pk}$ e $N_{j+2k+d} \leq N_{j+k+d}$). Para mostrarmos que $[N_j, \Pi_i(G)] \leq N_{j+f_d(i)}$, com $i, j \geq 0$, utilizaremos indução sobre i. O caso em que $i = 0$ é trivial. Suponha, agora, $i \geq 1$ e que o resultado vale para $i-1$. Pelo que mostramos acima, temos $[N_j, (\Pi_{i-1}(G))^p] \leq N_{j+m}$, com $m = \min(f_d(i-1) + d, pf_d(i-1))$, donde $[N_j, \Pi_i(G)] \leq N_{j+f_d(i)}$, para todo $i, j \geq 0$. Desta forma, a primeira parte do teorema está demonstrada.

Agora, suponha $d \neq (p-1) \times$ (uma potência de p). Para mostrarmos que, nesse caso, $[N_j, \Pi_i(G)] = N_{j+f_d(i)}$, utilizaremos, novamente, indução sobre i. Se $i = 0$, não há o que

provar. Suponha, então, $i \geq 1$ e que o resultado vale para $i-1$. Assumiremos $N_{j+f_d(i)} \neq 1$. Seja C_k o $(j+kf_d(i-1)+1)$-ésimo centralizador de $(f_d(i-1)+1)$-passos em G, para $k = 0, 1, \cdots, p-1$. Então $C_k \cap \Pi_{i-1}(G)$ é um subgrupo próprio de $\Pi_{i-1}(G)$, pela hipótese de indução. Portanto, existe $y \in \Pi_{i-1}(G)$ tal que $y \notin C_0 \cup C_1 \cup \cdots \cup C_{p-1}$ (utilizamos um argumento análogo na demonstração do Teorema 3.1.13).

Tome $x \in N_j \backslash N_{j-1}$. Pela hipótese de indução, $[x,y] \in N_{j+f_d(i-1)} \backslash N_{j+f_d(i-1)-1}$, donde $[x,y]^p \in N_{j+f_d(i-1)+d} \backslash N_{j+f_d(i-1)+d-1}$ e $[x,\ _p\ y] \in N_{j+pf_d(i-1)} \backslash N_{j+pf_d(i-1)-1}$. Pela condição imposta sobre d, temos $pf_d(i-1) \neq f_d(i-1)+d$, donde $[x,y^p] \in N_{j+f_d(i)} \backslash N_{j+f_d(i)-1}$. Temos, então, $[N_j, \Pi_i(G)] \leq N_{j+f_d(i)}$ e $[x,y^p] \in N_{j+f_d(i)}$, donde, uma vez que G age uniserialmente sobre N e $[N_j, \Pi_i(G)]$ é G invariante, temos, pelo Lema 3.1.2, $[N_j, \Pi_i(G)] = N_{j+f_d(i)}$.

□

Definimos E_{jk}, com $1 \leq j,k \leq r$, como a matriz $r \times r$ que possui todas as suas entradas nulas, exceto a (j,k)-ésima entrada, que é igual a 1. O seguinte resultado vale para matrizes de entradas em qualquer anel comutativo e, nele, I denotará a matriz identidade. Note que, como $E_{jk}^2 = 0$ para $j \neq k$, o lema a seguir pode ser facilmente verificado.

Lema 3.1.17. Dados dois inteiros j e k, com $j \neq k$, temos $(I+E_{jk})^a = I + aE_{jk}$, para todo inteiro a.

Suponha que V é um $\mathbb{F}_p$ espaço vetorial de dimensão d e seja $\{e_1, \cdots, e_d\}$ uma base de V. Identificaremos V como $\mathbb{F}_p^d$, a partir do mapeamento $(a_1e_1 + a_2e_2 + \cdots + a_de_d) \mapsto (a_1, a_2, \cdots, a_d)$. Definimos $V(i) = \langle e_i, e_{i+1}, \cdots, e_d \rangle$ e $V(d+1) = \langle 0 \rangle$, donde:

$$V = V(1) \geq V(2) \geq \cdots \geq V(d+1) = \langle 0 \rangle.$$

Seja $G = GL_d(\mathbb{F}_p)$. Então G possui uma ação sobre V induzida por $(a_1, a_2, \cdots, a_d) \mapsto (a_1, a_2, \cdots, a_d)A$, isto é, induzida pelo produto dos vetores $(a_1, a_2, \cdots, a_d) \in V$ pelas matrizes $A \in G$, pela esquerda. Definimos, dado $1 \leq m \leq d$:

$$U_m = \{A \in G \mid e_iA - e_i \in V(i+m) \forall i = 1, \cdots, d\}.$$

Note que os conjuntos U_m são subgrupos de G tais que:

$$U_d(\mathbb{F}_p) = U_1 \geq U_2 \geq \cdots \geq U_d = \{I\}.$$

Considere $U_m = \{I\}$, para $m > d$.

O seguinte resultado pode, também, ser facilmente demonstrado:

Lema 3.1.18. Se $1 \leq i,j,k \leq d$, então $[e_i, I + \sum_{jk} a_{jk}E_{jk}] = \sum_k a_{ik}e_k$.

Proposição 3.1.19. $U_r(\mathbb{F}_p)$ age uniserialmente sobre $V(i)$, para $i = 1, \cdots, d$. Além disso, o subgrupo U_m é a interseção de todos os centralizadores de m-passos em $U_r(\mathbb{F}_p)$, para $m = 1, \cdots, d$.

Demonstração. Do Lema 3.1.18, temos $[e_1, I + E_{12}, I + E_{23}, \cdots, I + E_{(i-1)i}] = e_i$, donde temos $V(i) \leq [V, {}_i\, U_r(\mathbb{F}_p)]$. Logo, uma vez que $[V : V(i)] = p^i$, temos $V(i) = [V, {}_i\, U_r(\mathbb{F}_p)]$ e, portanto, pelo Lema 3.1.2, temos que $U_r(\mathbb{F}_p)$ age uniserialmente sobre $V(i)$, para $i = 1, \cdots, d$. Desta forma, note que, pela sua definição, o subgrupo U_m é a interseção de todos os centralizadores de m-passos em $U_r(\mathbb{F}_p)$, para $m = 1, \cdots, d$.

□

A seguinte proposição é também verdadeira para a igualdade, porém nós só estamos interessados nas seguintes informações:

Proposição 3.1.20.

(i) $[U_m, U_n] \leq U_{m+n}$, para todo $m, n \geq 1$.

(ii) $\Pi_i(U_m) \leq U_{p^i m}$, para todo $m \geq 1$.

Demonstração.

(i) Como U_i é a interseção de todos os centralizadores de i-passos, então, pelo Lema 3.1.6, $[U_m, U_n]$ está contido em todo centralizador de $(m+n)$-passos. Portanto, $[U_m, U_n] \leq U_{m+n}$.

(ii) Pelo item (i) deste lema, temos $\gamma_p(U_m) \leq U_{pm}$, donde a classe de nilpotência de U_m/U_{pm} é menor ou igual a p e, portanto, U_m/U_{pm} é regular. Note, porém, que, pelo Lema 3.1.17, U_m/U_{pm} é gerado por elementos de ordem p, donde U_m/U_{pm} tem exponente p. Portanto, $U_m^p \leq U_{pm}$, donde $\Pi_i(U_m) \leq U_{p^i m}$.

□

No lema seguinte, conseguimos relacionar a teoria vista até então neste capítulo com o subgrupo $V(G,d)$, definido em 2.2.2.

Lema 3.1.21. Os subgrupos $\gamma_d(G)$ e $\Pi_i(G)$, com $p^i \geq d$, estão contidos em $V(G,d)$. Consequentemente, se p é ímpar e $d(\gamma_k(G)) \leq k$, então $\gamma_k(G)$ é *powerful*.

Demonstração. Pelo Lema 3.1.20, $\gamma_d(U_d(\mathbb{F}_p)) \leq U_d = 1$ e $\Pi_i(U_d(\mathbb{F}_p)) \leq U_{p^i} = 1$. Desta forma, como, dado um homomorfismo $\theta : G \to U$ qualquer, temos $\theta(\gamma_d(G)) \leq \gamma_d(U_d(\mathbb{F}_p))$ e $\Pi_i(G) \leq \Pi_i(U_d(\mathbb{F}_p))$, concluímos que $\gamma_d(G), \Pi_i(G) \leq V(G,d)$. A segunda parte deste lema é um consequência direta da Proposição 2.2.4.

□

3.2 Subgrupos fortemente hereditariamente *powerful*

Trabalhar com os subgrupos fortemente hereditariamente *powerful* nos será muito útil, uma vez que podemos aplicar os resultados do capítulo 2 aos subgrupos normais contidos neles. Iniciamos esta seção definindo este tipo de subgrupo.

Definição 3.2.1. Dado G um p-grupo finito e N um subgrupo normal de G, dizemos que N é fortemente hereditariamente *powerful* em G, se todo subgrupo normal de G contido em N é *powerfully embedded* em N.

Denotamos N shp G, se N é fortemente hereditariamente *powerful* em G. No decorrer desta seção, consideraremos G um p-grupo finito e N um subgrupo de G tal que N shp G.

Note que, se H é um subgrupo normal em G tal que $H \leq N$, então:

(i) H shp G e H é um grupo *powerful*.

(ii) Se p é ímpar, então $[H, {}_i N] \leq H^{p^i}$, para todo $i \geq 0$. Se $p = 2$, então $[H, {}_i N] \leq H^{4^i}$.

(iii) N é *powerful*, donde $d(H) \leq d(N)$.

(iv) Se p é ímpar e $d(V(G,d)) \leq d$, então $V(G,d)$ shp G. Se $p = 2$ e $d(V(G,d)^2) \leq d$, então $V(G,d)^2$ shp G.

Definição 3.2.2. Seja G um p-grupo. Os subgrupos $X_i = X_i(G)$ e $Y_i = Y_i(G)$ são definidos por:

$$X_i(G) = \Pi_i(G)\gamma_{p^i}(G) \text{ e } Y_i(G) = \Phi(X_i)\gamma_{2p^i}(G),$$

para todo $i \geq 0$.

O lema a seguir nos dá algumas propriedades a respeito dos subgrupos definidos acima.

Lema 3.2.3.

(i) $X_i \geq Y_i \geq X_{i+1}$ e X_i/Y_i é abeliano elementar, para todo $i \geq 0$. Além disso, $X_i = Y_i$ se, e somente se, $X_i = 1$.

(ii) Se G é um p-grupo finito agindo uniserialmente sobre um p-grupo abeliano elementar A, então X_i centraliza exatamente p^i-passos em G e Y_i está contido em todo centralizador de $(2p^i)$-passos em G (e, portanto, em todo centralizados de (p^i+1)-passos em G), para todo $i \geq 0$.

(iii) $X_i \leq V(G, p^i)$, para todo $i \geq 0$.

Demonstração.

(i) Este resultado é trivial.

(ii) Pelo Lema 3.1.6 e pelo Teorema 3.1.13, temos que X_i centraliza exatamente p^i-passos. Note que, dados $a \in A$ e $x \in X$, temos $[a,x^p] = [a,\ {}_p\, x]$, donde, pelo Lema 3.1.6, temos que $Y_i(G) = \Phi(X_i)\gamma_{2p^i}(G) = X_i^p\gamma_2(X_1)\gamma_{2p^i}(G)$ está em todo centralizador de $(2p^i)$-passos em G.

(iii) Este é um resultado direto do Lema 3.1.21.

□

Com o próximo já conseguimos uma condição suficiente para que, dado H um subgrupo normal em G, tenhamos H shp G.

Lema 3.2.4.

(i) Para p ímpar e $i \geq 0$ qualquer, se $H \trianglelefteq G$, $H \leq X_i$ e $d(H) \leq p^i$, então H shp G.

(ii) Para $p = 2$ e $i \geq 0$ qualquer, se $H \trianglelefteq G$, $H \leq X_i^2$ e $d(H) \leq 2^i$, então H shp G.

Demonstração. Em ambos os casos, uma vez que $X_i \leq V(G,p^i)$, temos, pela Proposição 2.2.4, que H é *powerful*. Desta forma, dado $K \leq H$ normal em G, temos $d(K) \leq d(H) \leq p^i$, donde, novamente pela Proposição 2.2.4, temos K p.e. H. Logo, H shp G.

□

Lema 3.2.5. Se G age uniserialmente sobre ${}^{X_i}\!/_{Y_i}$ e $i \geq 0$, então $d(X_i) \leq p^i$ e $X_i^p = Y_i$. Além disso, se p é ímpar, temos X_i shp G.

Demonstração. Sejam $A = {}^{X_i}\!/_{\Phi(X_i)}$ e $H = {}^{G}\!/_{X_i}$. Sabemos que A é abeliano elementar e que H age sobre A. Além disso:

$$A_{p^i+1} = {}^{[X_i,\ {}_{p^i}\, G]\Phi(X_i)}\!/_{\Phi(X_i)} \geq {}^{[\gamma_{p^i}(G),\ {}_{p^i}\, G]\Phi(X_i)}\!/_{\Phi(X_i)} = {}^{Y_i}\!/_{\Phi(X_i)}.$$

Note, porém, que $\Pi_i(H) = 1$ e que H age uniserialmente sobre ${}^{A}\!/_{A_{p^i+1}} \cong {}^{X_i}\!/_{Y_i}$, donde, pelo Corolário 3.1.14, A_{p^i+1} é trivial. Temos, portanto, que A possui dimensão no máximo p^i, donde $d(X_i) \leq p^i$ e $Y_i = \Phi(X_i)$. Se p é ímpar, então, pelo Lema 3.2.4, X_i shp G, logo, X_i é *powerful* e, então, $\Phi(X_i) = X_i^p$. Se $p = 2$, então ${}^{X}\!/_{X^2}$ é abeliano, donde $\gamma_2(X_i) \leq X_i^2$ e, portanto, $X_i^2 = \Phi(X_i)$.

□

Os próximos resultados são sobre ações uniseriais sobre seções de subgrupo hereditariamente *powerful*. Lembre-se que, nesta seção, estamos assumindo N shp G.

Lema 3.2.6. Suponha G age uniserialmente sobre N/N^p e que $N^{p^i} \neq 1$, com $i \geq 0$. Então G age uniserialmente sobre $N^{p^i}/N^{p^{i+1}}$.

Demonstração. Uma vez que G é *powerful*, temos, pelo Lema 2.1.8, que o mapeamento $x \mapsto x^p$ induz um epimorfismo de $N^{p^j}/N^{p^{j+1}}$ sobre $N^{p^{j+1}}/N^{p^{j+2}}$. Desta forma, por indução, temos o resultado desejado.

□

Lema 3.2.7. Seja H um subgrupo normal de G.

(i) Se $x \in N$ e $y \in H$, então $[x^p, y] \equiv [x,y]^p \mod [N,H]^{p^2}$.

(ii) Para todo $k \geq 0$, temos $[N^{p^k}, H] = [N,H]^{p^k}$.

Demonstração.

(i) Seja $K = \langle [x,y], x \rangle$. Então, $[x^p, y] \equiv [x,y]^p \mod (\gamma_2(K))^p \gamma_p(K)$, pela segunda versão dada da Fórmula de Compilação de Hall (Teorema 1.2.10). Basta, portanto, mostrar que $(\gamma_2(K))^p \gamma_p(K) \leq [N,H]^{p^2}$. Note que $\gamma_p(G) \leq [N, H, {}_{p-1}\, N]$ e $(\gamma_2(K))^p \leq [N,H,N]^p$. Além disso, como $[N,H] \trianglelefteq N$ e N shp G, temos que $[N,H]$, $[N,H,,N]$ e $[N,H]^p$ são *powerfully embedded* em N.

Se $p = 2$, temos $(\gamma_2(K))^2 \gamma_2(K) \leq \gamma_2(K) \leq [N,H,N] \leq [N,H]^4$, como desejávamos. Se p é ímpar, temos $(\gamma_2(K))^p \gamma_p(K) \leq [N,H,N]^p [N,H,N,N] \leq [N,H,N]^p \leq ([N,H]^p)^p$, donde, como $[N,H]$ é *powerful*, temos $(\gamma_2(K))^p \gamma_p(K) \leq [N,H]^{p^2}$.

(ii) Para demonstrarmos este resultado, aplicaremos indução sobre k. Se $k = 0$, não há o que provar. Suponha, agora, $k \geq 1$ e que o resultado é válido para $k-1$. Seja $M = N^{p^{k-1}}$. Como $M \trianglelefteq G$, temos M shp G. Logo, pelo primeiro item deste lema, temos $[M^p, H] \leq [M,H]^p$ e $[M,H]^p \leq [M^p,H][M,H]^{p^2}$, donde $[M,H]^p = [M^p,H][M,H]^{p^2}$. Temos, porém, uma vez que $[M,H]^p$ é *powerful*, que $[M,H]^{p^2} = \Phi([M,H]^p)$, desta forma, temos $[M^p,H] = [M,H]^p$. Portanto, como M e $[M,H]$ são *powerful*, temos, pela hipótese de indução, o resultado desejado.

□

Proposição 3.2.8.

(i) Se G age uniserialmente sobre N/N_{d+1}, onde $d = d(N)$, então G também age uniserialmente sobre N.

(ii) Se G age uniserialmente sobre N, então $N_j^p = N_{j+d}$, onde $d = d(N)$, para todo $j \geq 1$.

Demonstração. Note que, como N shp G, N_j é *powerful* e N_j shp G, para todo $j \geq 1$. Provaremos por indução sobre j que $|{}^{N_{j+d}}\!/_{N_j+d+1}| \leq p$ e que $N_j^p = N_{j+d}$. Claramente, $|{}^{N_d}\!/_{N_{d+1}}| = p$ e, como $N^p = \Phi(N)$, $[N, N^p] = p^d$. Portanto, pelo Corolário 3.1.4, temos $N^p = N_{d+1}$. Logo, temos a nossa base de indução.

Suponha, agora, $j \geq 1$, com N_{j+d-1} não trivial, e que os resultados são válidos para $j-1$. Pelo Lema 3.2.7 e pela hipótese de indução, temos $N_j^p = [N_{j-1}^p, G] = [N_{j-1+d}, G] = N_{j+d}$. Portanto, como N é *powerful*, temos:

$$[N_j : N_{j+d}] = [N_j : N_j^p] = [N_j : \Phi(N_j)] = p^{d(N_j)} \leq p^d.$$

Logo, pela hipótese de indução, $[N_{j+d-1} : N_{j+d}] \leq p$. Pelo Lema 3.1.2, temos, então, que G age uniserialmente sobre N.

□

Corolário 3.2.9. Se G age uniserialmente sobre N e H é um subgrupo normal de G tal que $H \leq N$ e $|H| \geq p^d$, onde $d = d(N)$, então $d(H) = d$.

Demonstração. Como $H \trianglelefteq G$ e G age uniserialmente sobre N, temos $H = N_j$, para algum $j \geq 1$ tal que $N_{j+d-1} \neq 1$ (pois $|H| \geq p^d$). Mas, então, pela Proposição 3.2.8, temos $H^p = N_{j+d}$, donde $[H, H^p] = [H : \Phi(H)] = p^d$. Portanto, $d(H) = d$.

□

No corolário a seguir, utilizamos a função $f_d(i)$, definida em 3.1.15.

Corolário 3.2.10. Se $d(N) \neq (p-1) \times$ (uma potência de p) e G age uniserialmente sobre N, então X_i centraliza exatamente $f_d(i)$-passos.

Demonstração. Pela Proposição 3.2.8, temos $N_j^p = N_{j+d}$, para todo $j \geq 1$. Desta forma, como N shp G, temos $[N_j, N] \leq N_j^p$, para todo $j \geq 1$. Portanto, pelo Teorema 3.1.16, $\Pi_i(G)$ centraliza exatamente $f_d(i)$-passos, para todo $i \geq 0$. Além disso, pelo Lema 3.1.6, temos $[N_j, \gamma_{p^i}(G)] \leq N_{j+p^i} \leq N_{j+f_d(i)}$, para todo $j \geq 1$ e $i \geq 0$. Logo, $X_i = \Pi_i(G)\gamma_{p^i}(G)$ centraliza exatamente $f_d(i)$-passos.

□

Proposição 3.2.11. Se G age uniserialmente sobre ${}^{N}\!/_{[N^p, G]N^{p^2}}$, então G age uniserialmente sobre N.

Demonstração. Sejam $H = [N^p, G]N^{p^2}$ e $d = d(N)$. Provaremos, por indução sobre j, que $N_j \geq N^p$, para $1 \leq j \leq d+1$. Se $j = 1$, o resultado é trivial. Suponha agora $1 < j \leq d+1$ e que $N_{j-1} \geq N^p$. Temos, então, $N_j = [N_{j-1}, G] \geq [N^p, G]$. Além disso, como $N^p \geq H$ e $[N, N^p] = p^d$ (lembre-se que N shp G), temos $N^p = N_{d+1}H$ (uma vez que G age uniserialmente sobre N/H). Temos, então, $N_jN_p = N_jH = N_jN_{p^2}$, donde, como $N^{p^2} = \Phi(N^p)$, temos $N^p \leq N_j$, como desejávamos.

Portanto, $N_{d+1} \geq N_p \geq [N^p, G]N^{p^2}$, donde, G age uniserialmente sobre N/N_{d+1}. Logo, pela Proposição 3.2.8, G age uniserialmente sobre N.

□

Corolário 3.2.12. Suponha que G aja uniserialmente sobre N/N^p e seja $H = N^{p^j}$, para algum $j \geq 0$. Se G age uniserialmente sobre $[H, G]H^p/[H^p, G]H^{p^2}$ mas não age uniserailmente sobre H, então H é cíclico e G centraliza $H^{p^k}/H^{p^{k+2}}$, para todo $k \geq 0$.

Demonstração. Seja $B = H^p$, $C = [H, G]H^p$ e $D = [H^p, G]H^{p^2}$. Temos, então, $H \geq C \geq B \geq D$, por hipótese G age uniserialmente sobre C/D e, como N é *powerful*, G age uniserialmente sobre A/B (pelo Lema 3.2.6). Portanto, pelo Lema 3.1.12, temos que se $C > B$, então G age uniserialmente sobre H/D. Note, porém, que, pela Proposição 3.2.11, se G age uniserialmente sobre H/D, então G age uniserialmente sobre H. Desta forma, temos $C = B$, ou seja, $H^p = [H, G]H^p$.

Temos, então, H p.e. G, donde G centraliza H/H^p. Como G age uniserialmente sobre H/H^p, temos, então, $[H : H^p]$, donde H é cíclico. Como H p.e. G, temos H^p p.e. G, donde $[H^p, G] \leq H^{p^2}$ e $D = H^{p^2}$. Como H é cíclico, temos $[H : h^{p^2}] = p^2$, donde, uma vez que G não age uniserialmente sobre H/D, G centraliza H/H^{p^2}. Portanto, $[H, G] \leq H^{p^2}$ e, pelo segundo item do Lema 3.2.7, temos $[H^{p^k}, G] = [H, G]^{p^k} \leq H^{p^{k+2}}$, para todo $k \geq 0$.

□

3.3 Teorema sobre coclasse de p-grupos

O objetivo desta seção é provar os Teoremas 3.3.9 e 3.3.10, que nos dirão, entre outras coisas, que, dado um p-grupo G de coclasse r e classe de nilpotência grande o suficiente, existe um número $m(p, r)$ tal que G age uniserialmente sobre $\gamma_m(G)$ e que $d(\gamma_m(G))$ possui uma forma determinada e é limitado por uma função de p e r. Iniciamos esta seção com dois resultados muito importantes sobre os subgrupos X_i e Y_i.

Lema 3.3.1. Para p ímpar, se G/Y_r tem coclasse no máximo r, então existe um i, dependendo de G, com $0 \leq i \leq r$, tal que X_i shp G, $d(X_i) \leq p^i$, $X_i^p = Y_i$ e X_i/Y_i é uniserial, mas $X_0/X_1, \cdots, X_{i-1}/X_i$ não são.

Além disso, X_r shp G e $d(X_r) \leq p^r$.

Demonstração. Considere a série normal $G = X_0 \geq X_1 \geq \cdots \geq X_r \geq Y_r$. Como G/Y_r tem coclasse no máximo r e a série tem $r+1$ subgrupos, temos, pelo Lema 3.1.11, que pelo menos uma das seções é uniserial. Seja i o menor inteiro tal que X_i/X_{i+1} é uniserial. Temos, então, que X_i/Y_i é uniserial, donde, pelo Lema 3.2.5, $d(X_i) \leq p^i$, $X_i^p = Y_i$ e X_i shp G. Além disso, como X_i é *powerful*, temos $d(X_r) \leq p^i \leq p^r$, donde, pelo Lema 3.2.4, temos X_r shp G. □

Lema 3.3.2. Seja G um 2-grupo finito. Se G/Y_{r+2} tem coclasse no máximo r, então existe n, com $0 \leq n \leq r+2$, tal que X_n shp G, $X_n^2 = Y_n$, $d(X_n) \leq 2^{n-1}$ e X_n/Y_n é uniserial, assim como no máximo duas das seções $X_0/X_1, \cdots, X_{n-1}/X_n$.

Além disso, X_{r+2} shp G e $d(X_{r+2}) \leq 2^{r+1}$.

Demonstração. Considere a série normal $= X_0 \geq X_1 \geq \cdots \geq X_{r+2} \geq Y_{r+2}$. Como G/Y_{r+2} tem coclasse no máximo r, temos que pelo menos três seções da série são unisseriais (pelo Lema 3.1.11). Sejam i, j e k os menores inteiros tais que $0 \leq i < j < k \leq r+2$ e X_i/X_{i+1}, X_j/X_{j+1} e X_k/X_{k+1} são unisseriais. Então, pelo Lema 3.2.5, $Y_l = X_l^2$ e $d(X_l/Y_l) = d(X_l) \leq 2^l$, para $l = i, j, k$.

Suponha $d(X_n) \leq 2^i$, com n igual j ou k, como $X_n \leq X_{i+1} \leq Y_i = X_i^2$, temos, pelo Lema 3.2.4, X_n shp G e o resultado está provado. Suponha, agora, $d(X_k) \leq p^i$. É, então, suficiente provar que $d(X_j) \leq 2^i$. Seja $U = X_j/Y_j$ e $V = X_k/Y_k$, então U e V são 2-grupos abelianos elementares com G agindo uniserialmente sobre os mesmos.

Então, usando o Teorema 3.1.13, temos que $\Pi_i(G)$ centraliza exatamente 2^i-passos para U e para V. Além disso, pelos Lemas 3.1.6 e 3.2.3, $[\Pi_i(G), G]$ e Y_i estão em todos os centralizadores de (2^i+1)-passos para U e para V. Note que G centraliza $\Pi_i(G)Y_i/[\Pi_i(G), G]Y_i$, desta forma, como G age uniserialmente sobre X_i/Y_i, temos $[\Pi_i(G)Y_i : \Pi_i(G), G]Y_i] \leq 2$. Logo, $\Pi_i(G)Y_i = \langle g \rangle [\Pi_i(G), G]Y_i$, para algum $g \in \Pi_i(G)$. Portanto, g centraliza exatamente 2^i-passos para U e para V.

Temos, porém, que $[v, g^{j-i}] = [v,\ {}_{2^{j-i}}\ g]$, para todo $v \in V$, e que $d(V) = d(X_k) > 2^j$, donde $V_{2^j+1} \neq 1$. Logo, existe $v \in V$ tal que $[v, g^{2^{j-i}}] \notin V_{2^j+2}$. Como $[X_j, G]Y_j$ está em todo centralizador de (2^i+1)-passos, temos $g \notin [X_j, G]Y_j$, mas $g \in \Pi - j(G) \leq X_j$. Note que $X_j/[X_j, G]Y_j$ também é centralizado por G, donde, como G age uniserialmente sobre X_j/Y_j, temos $[X_j : [X_j, G]Y_j] \leq 2$. Se $X_j = 1$, obviamente $d(X_j) \leq 2^i$. Caso contrário, temos

$[X_j : [X_j, G]Y_j] = 2$, donde $X_j = \langle g^{2^{j-i}} \rangle [X_j, G]Y_j$. Seja $x = g^{2^{j-i}} Y_j$, que é um elemento de U. Então $U = \langle x \rangle U_2$ e g centraliza x, o que implica $[u, x] \in U_{2^i+2}$, para todo $u \in U$.

Porém, g não está em nenhum centralizador de (2^i+1)-passos de U, donde $U_{2^i+1} = U_{2^i+2} = 1$. Desta forma, $d(X_j) = d(U) \leq 2^i$, como desejávamos.

□

Com os últimos dois lemas, conseguimos como resultado imediato o próximo corolário, que é um dos objetivos desta seção.

Corolário 3.3.3. Dado um p-grupo G de coclasse r, o subgrupo $\gamma_i(G)$ é *powerful* para todo $i \geq r$, se p é ímpar, e todo $i \geq r+2$, se $p = 2$.

O próximo resultado nos dá um número n_1 tal que G possui a mesma coclasse que $G/\gamma_{n_1}(G)$.

Teorema 3.3.4. Sejam G um p-grupo finito e $n_1 = 2p^r$, se p é ímpar, e $n_1 = 2^{r+3}$, se $p = 2$. Se $G/\gamma_{n_1}(G)$ tem coclasse r, então G tem coclasse r.

Demonstração. Usaremos indução sobre r para mostrar que se $G/\gamma_{n_1}(G)$ tem coclasse no máximo r, então a coclasse de G é igual à de $G/\gamma_{n_1}(G)$. Caso $r = 1$, $G/\gamma_{n_1}(G)$ é de classe maximal, donde, pela Proposição 1.3.22, temos que G é, também, de classe maximal. Suponha, agora, $r > 1$, que o resultado é válido para valores menores que r e que $G/\gamma_{n_1}(G)$ tem coclasse no máximo r.

Seja $N = \gamma_{n_1/2}(G)$ e $d = d(N)$. Pela Proposição 3.2.8, se N shp G e G age uniserialmente sobre N/N_{d+1}, então G age uniserialmente sobre N, donde G age uniserialmente sobre $\gamma_{n_1}(G)$ e temos o resultado desejado. Se $G/\gamma_{n_1/p}(G)$ possui coclasse menor que r, então, pela hipótese indução, temos que G possui coclasse igual à de $G/\gamma_{n_1/p}(G)$, donde G age uniserialmente sobre $\gamma_{n_1/p}(G)$ e, portanto, sobre N. Desta forma, neste caso, não há mais o que provar.

Suponha, agora, que $G/\gamma_{n_1/p}(G)$ possui coclasse r. Então $G/\gamma_{n_1/p}(G)$ e $G/\gamma_{n_1}(G)$ possuem a mesma coclasse, donde G age uniserialmente sobre $\gamma_{n_1/p}(G)/\gamma_{n_1}(G)$ e, portanto, sobre N/N_{p^r+1}.

Se p é ímpar, então G/Y_r possui coclasse no máximo r, uma vez que $Y_r \geq \gamma_{2p^r}(G) = N_{p^r+1}$ e, portanto, pelo Lema 3.3.1, X_r shp G e $d(X_r) \leq p^r$. Como $N \leq X_r$, temos N shp G e $d \leq p^r$, donde G age uniserialmente sobre N/N_{d+1}. Logo, nesse caso, temos o resultado desejado.

Se $p = 2$, analogamente, temos que G age uniserialmente sobre $N/N_{2^{r+2}+1}$. Desta forma, temos que G/Y_{r+2} tem coclasse no máximo r, uma vez que $Y_{r+2} \geq \gamma_{2^{r+3}}(G) = N_{2^{r+2}+1}$.

Portanto, pelo Lema 3.3.2, X_{r+2} shp G e $d(X_{r+2}) \leq 2^{r+1}$. Como $N \leq X_{r+2}$, temos N shp G e $d \leq 2^{r+1}$, donde G age uniserialmente sobre N/N_{d+1}. Logo, também para este caso, temos o resultado desejado.

□

Este teorema, porém, não é o melhor possível. A Proposição 1.3.22 nos mostra que, se $r = 1$, então $p+1$ é uma cota melhor que a fornecida no resultado acima. A partir do teorema anterior, conseguimos também obter os números n_2 e n_3, que serão muito importantes nesta seção.

Corolário 3.3.5. Seja G um p-grupo finito de coclasse r.

(i) Seja $n_2 = 2p^{r-1}$, se p é ímpar, e $n_2 = 2^{r+2}$, se $p = 2$, então G age uniserialmente sobre $\gamma_{n_2}(G)$.

(ii) Seja $n_3 = p^r$, se p é ímpar, e $n_3 = 2^{r+2}$, se $p = 2$, e seja $d = d(\gamma_{n_3}(G))$, então $\gamma_i(G)^p = \gamma_{i+d}(G)$, para todo $i \geq n_3$.

Demonstração.

(i) Se G não age uniserialmente sobre $\gamma_{n_2}(G)$, então $G/\gamma_{n_2}(G)$ tem coclasse menor que r, donde, pelo Teorema 3.3.4, G também tem, o que é um absurdo.

(ii) Do item (i) deste corolário, temos que G age uniserialmente sobre $\gamma_{n_3}(G)$ (pois $n_2 \leq n_3$). Logo, pelos Lemas 3.3.1 e 3.3.2, temos $\gamma_{n_3}(G)$ shp G, donde, pela Proposição 3.2.8, temos o resultado desejado.

□

Nos próximos dois resultados, voltamos a trabalhar com os subgrupos X_i e Y_i. Dado um p-grupo G de coclasse r, nosso intuito é utilizar o Corolário 3.2.10 para conseguirmos a forma do valor $d(X_r)$, se p é ímpar, e do valor $d(X_{r+2})$, se $p = 2$, além de uma cota para os mesmos.

Teorema 3.3.6. Seja G um p-grupo finito de coclasse r e classe de nilpotência c.

(i) Se p é ímpar e $c > 2p^r + q$, então G age uniserialmente sobre X_r.

(ii) Se $p = 2$ e $c > 2^{r+2} + 1$, então G age uniserialmente sobre X_{r+2}.

Demonstração. Seja $t = r$, se p é ímpar, e $t = r+2$, se $p = 2$. Suponha, por absurdo, que a ação de G sobre X_r não seja uniserial. Pelos Lemas 3.3.1 e 3.3.2, existe i, com $0 \leq i \leq t$, tal

que X_i shp G, $X_i^p = Y_i$, $d(X_i) \leq p^i$ (para p ímpar) ou $d(X_i) \leq 2^{i+1}$ (para $p = 2$), e tal que G age uniserialmente sobre X_i/Y_i e sobre no máximo $t-r$ seções de $X_0/X_1, \cdots, X_{i-1}/X_i$.

Note que $0 < i < t$, pois, se $i = 0$, então $d(X_0) = d(G) \leq 1$, donde $c = 1$; e se $i = t$, então a série normal $G = X_0 \geq X_1 \geq \cdots \geq X_t \geq 1$ não possui $t-r-1$ seções uniseriais, contradizendo o Lema 3.1.11. Seja $N = X_i$ e considere a seguinte série normal de comprimento $t+2$:

$$G = X_0 > X_1 > \cdots > X_{i-1} > [N,G]N^p > [N^p,G]N^{p^2} > \cdots > [N^{p^{t-i+1}},G]N^{p^{t-i+2}}.$$

Como no máximo $t-r$ das primeiras i seções são uniseriais, temos, pelo Lema 3.1.11, que existe um valor minimal j tal que $0 \leq j \leq t-i$ e a seção $[N^{p^j},G]N^{p^{j+1}}/[N^{p^{j+1}},G]N^{p^{j+2}}$ é uniserial.

Temos, porém, que G age uniserialmente sobre $X_i/Y_i = N/N^p$ e, tomando $H = N^{p^j}$, também sobre $[H,G]H^p/[H^p,G]H^{p^2}$. Portanto, pelo Corolário 3.2.12, G age uniserialmente sobre H, ou H é cíclico e G centraliza $H^{p^k}/H^{p^{k+2}}$, para todo $k \geq 0$. Como X_i é *powerful*, temos $d(X_i^{p^k}) \leq d(X_i) \leq p^i$ e $\Phi(X_i^{p^k}) = X_i^{p^{k+1}}$, para todo $k \geq 0$. Portanto, $X_i^{p^k}/X_i^{p^{k+1}}$ tem dimensão no máximo p^i. Logo, pelo Lema 3.2.6, G age uniserialmente sobre $X_i^{p^k}/X_i^{p^{k+1}}$, para todo $k \geq 0$. Além disso, como $j \leq t-i$, temos $(j+1)p^i \leq p^t$, donde $\gamma_{p^i}(G) \leq \gamma_{(j+1)p^i}(G) \leq X_i^{p^j}$ (pois X_i p.e. G).

Claramente $\Pi_i(G) \leq \Pi_{t-i}(X_i) \leq \Pi_j(X_i) = X_i^{p^j}$. Mas $X_t = \Pi_t(G)\gamma_{p^t}(G) \leq X_i^{p^j} = H$, logo, como assumimos que G não age uniserialmente sobre X_i, temos que G não age uniserialmente sobre H. Temos, então, que H é cíclico e que G centraliza $H^{p^k}H^{p^{k+2}}$, para todo $k \geq 0$. Seja $a = t-i-j+1$ e considere a seguinte série normal de comprimento $t+2$:

$$X_0 > X_1 > \cdots > X_{i-1} > [N,G]N^p > \cdots > [N^{p^{j-1}},G]H > H^p > H^{p^3} > \cdots > H^{p^{2a+1}}.$$

Pelas condições impostas sobre i e j, temos, pelo Lema 3.1.11, que existe k tal que $0 \leq k \leq a-1$ e $H^{p^{2k+1}}/H^{p^{2k+3}}$ é uniserial. Como G centraliza $H^{p^{2k+1}}H^{p^{2k+3}}$, temos que este grupo tem ordem no máximo p.

Portanto, $H^{p^{2k+2}} = H^{p^{2k+3}}$, donde $H^{p^{2k+2}} = X_i^{p^{j+2k+2}} = 1$ e $|X_i^{p^j}| \leq p^{2(t-i-j)+2}$ (pois $X_i^{p^j} = H$ é cíclico). Além disso, como $d(X_i) \leq p^i$ e X_i é *powerful*, temos $[X_i : X_i^{p^j}] \leq p^{jp^i}$, donde $|\gamma_{p^i}(G)| \leq |X_i| = |N| \leq p^{2(t-i-j)+2+jp^i}$. Mas $\gamma_{c+1}(G) = 1$, logo, $c \leq 2(t-i-j) + 2(j+1)p^i - 1$. Porém, como $0 < i < t$ e $0 \leq j \leq t-i$, temos $c \leq 2p^{t-1} + 1$, o que é uma contradição. Temos, então, que G age uniserialmente sobre X_t.

□

Corolário 3.3.7. Seja G um p-grupo finito de coclasse r e classe de nilpotência c.

(i) Para p-ímpar, se $c \geq 2p^r$, então $d(X_r) = (p-1)p^s$, para algum inteiro $s < r$

(ii) Para $p = 2$, se $c \geq 2^{r+3}$, então $d(X_{r+2}) = 2^s$, para algum inteiro $s < r+2$.

Demonstração. Seja $t = r$, se p é ímpar, e $t = r+2$, se $p = 2$. Sejam $N = X_r$ e $d = d(N)$, e suponha que d não é da forma dada. Pelos Lemas 3.3.1 e 3.3.2 e pelo Teorema 3.3.6, G age uniserialmente sobre N, N shp G e $d \leq p^t$. Pelo Corolário 3.2.10, temos $[N_j, N] = N_{j+f_d(t)}$, para todo $J \geq 1$, onde $f_d(T) \leq p^t$. Como N/N_2 é cíclico (pois G age uniserialmente sobre N), temos $[N,N] = [N_2,N]$, donde $N_{1+f_d(t)} = N_{2+f_d(t)}$ e $N_{1+f_d(t)} = 1$. Portanto, $|N| \leq p^{f_d(t)} \leq p^{p^t}$. Mas $\gamma_{p^t}(G) \leq N$, donde $c \leq p^t + p^t - 1$, o que é uma contradição.

□

Por fim, conseguimos, agora, provar os teorema propostos como objetivos da seção.

Definição 3.3.8. Seja p um primo e r um inteiro, definimos o inteiro $m(p,r)$ por $m(p,r) = (p-1)p^{r-1}$, se p é ímpar, e por $m(2,r) = 2^{r+2}$.

Teorema 3.3.9. Seja G um 2-grupo finito de coclasse r e classe de nilpotência c e sejam $m = m(2,r)$ e $d = d(\gamma_m(G))$. Se $c \geq 2^{r+3}$, então temos:

(i) G age uniserialmente sobre $\gamma_m(G)$.

(ii) $\gamma_i(G)^2 = \gamma_{i+d}(G)$, para todo $i \geq m$.

(iii) $d = 2^s$, com $0 \leq s \leq r+1$.

Demonstração. Note que os itens (i) e (ii) deste teorema são resultados diretos do Corolário 3.3.5. Provemos o item (iii). Seja $D = d(X_{r+2})$. Pelo Corolário 3.3.7, temos $D = 2^s$, com $s \leq r+1$. Desta forma, como G age uniserialmente sobre $\gamma_m(G)$ (pelo item (i) deste teorema), temos $|\gamma_m(G)| = 2^{c+1-m} > 2^{2^{r+2}} > 2^D$. Pelo Lema 3.3.2, temos X_{r+2} shp G e, pelo Teorema 3.3.6, temos que G age uniserialmente sobre X_{r+2}. Portanto, pelo Corolário 3.2.9 (aplicando $N = X_{r+2}$), temos $D = d$, donde $d = 2^s$, com $0 \leq s \leq r+1$.

□

Se utilizarmos p^r no papel do valor m, conseguimos, através de uma prova semelhante, um resultado análogo ao acima para p ímpar. O teorema a seguir, porém, é melhor do que este resultado.

Teorema 3.3.10. Seja G um p-grupo finito de coclasse r e classe de nilpotência c, sendo p ímpar, e denotemos $m = m(p,r)$ e $d = d(\gamma_m(G))$. Se $c \geq 2p^r$, então:

(i) G age uniserialmente sobre $\gamma_m(G)$.

(ii) $\gamma_i(G)^p = \gamma_{i+d}(G)$, para todo $i \geq m$.

(iii) $d = (p-1)p^s$, com $0 \leq s \leq r-1$.

Demonstração. Pelo Corolário 3.3.5, temos que G age uniserialmente sobre $\gamma_{2p^{r-1}}$, donde G também age uniserialmente sobre $\gamma_m(G)$. Está provado, portanto, o item (i). A seguir provaremos simultaneamente os itens (ii) e (iii). Seja $D = d(X_r)$ e $d_i = d(\gamma_i(G))$, para todo $i \geq 1$. Pelo Cololário 3.3.7, temos $D = (p-1)p^s$, com $0 \leq s \leq r-1$. Como G age uniserialmente sobre $\gamma_{p^r}(G)$, temos $|\gamma_{p^r}(G)| = p^{c+1-p^r} > p^{p^r} > p^D$. Pelo Lema 3.3.1, X_r shp G e, pelo Teorema 3.3.6, G age uniserialmente sobre X_r. Desta forma, temos, pelo Corolário 3.2.9, que $d_{p^r} = D$.

Seja n o menor inteiro tal que $n \geq 2p^{r-1}$ e $\gamma_n(G)$ shp G. Como X_r shp G, temos $\gamma_{p^r}(G)$ shp G, donde $n \leq p^r$ e, pelo Corolário 3.3.5, G age uniserialmente sobre $\gamma_n(G)$. Portanto, pela Proposição 3.2.8, se $i \geq n$, então $\gamma_j(G)^p = \gamma_{j+d_i}(G)$, para todo $j \geq i$, donde $\gamma_{j+d_i}(G) = \gamma_{j+D}(G)$, para todo $j \geq i$. Desta forma, temos $d_i = d_{p^r} = D$, para todo $i \geq n$ tal que $\gamma_{i+D}(G) \neq 1$. Logo, se $n \leq m$, temos (ii) e (iii), pois $d = d_m = D = (p-1)p^s$, com $0 \leq s \leq r-1$, e $\gamma_i(G)^p = \gamma_{i+d}(G)$, para todo $i \geq m$.

Suponha, agora, por absurdo, que $m < n$. Então G age uniserialmente sobre $\gamma_{n-1}(G)$, e, portanto, pelo Lema 3.1.2, os únicos subgrupos de $\gamma_{n-1}(G)$ que são G-invariantes são os subgrupos $\gamma_i(G)$, com $i \geq n-1$. Como $\gamma_i(G)^p = \gamma_{i+D}(G) \geq \gamma_{i+n-1}(G) \geq [\gamma_i(G), \gamma_{n-1}(G)]$, para todo $i \geq n$, temos $\gamma_i(G)$ p.e. $\gamma_{n-1}(G)$, para todo $i \geq n$. Como $\gamma_{n-1}(G)$ não é fortemente hereditariamente *powerful* (pela definição de n), temos que $\gamma_{n-1}(G)$ não é *powerful*. Porém, como G age uniserialmente sobre $\gamma_{n-1}(G)$, temos $|\gamma n - 1 + d_{n-1}(G)| = |\Phi(\gamma_{n-1}(G))|$, donde:

$$\gamma n - 1 + d_{n-1}(G) = \Phi(\gamma_{n-1}(G)) > \gamma_{n-1}(G)^p \geq \gamma_n(G)^p = \gamma_{n-D}(G) \geq \gamma_{2n-1}(G).$$

Portanto, $d_{n-1} \leq n-1$, donde, pelo Lema 3.1.21, $\gamma_{n-1}(G)$ é *powerful*, o que é uma contradição. Logo, $m \geq n$.

□

Capítulo 4

p-Grupos *self-similar* com estabilizadores do primeiro nível abelianos

Neste capítulo, iniciamos nossos estudos acerca de endomorfismo virtuais e de p-grupos *self-similar*. Nosso objetivo principal é a demonstração do Teorema A, isto é, desejamos provar que um p-grupo finito que possui um subgrupo maximal abeliano é *self-similar* se, e somente se, o mesmo possui um subgrupo maximal abeliano elementar do qual ele é uma extensão cindida. Para provarmos este resultado, utilizaremos endomorfismos virtuais.

4.1 Endomorfismos virtuais e grupos de automorfismos de árvores

Nesta seção, temos como objetivo descrever a relação entre endomorfismos virtuais e ações *self-similar* sobre a árvore enraizada k-ária. Esta teoria pode ser encontrada em [19] e [22]. Iniciaremos com algumas definições básicas.

Definição 4.1.1. Dado um conjunto $X = \{0, 1, \cdots, k-1\}$, X^* denotará o conjunto das palavras formadas a partir do alfabeto X, incluindo a palavra vazia.

Definição 4.1.2. Um automorfismo de um grafo (V, A) (onde V denota o conjunto de vértices e A o de arestas) é uma permutação $g : V \to V$ tal que, dados dois vértices $x, y \in V$, existe uma aresta ligando x e y se, e somente se, existe uma aresta ligando $g(x)$ e $g(y)$.

A seguinte definição de árvore enraizada k-ária não é a usual, mas é a que será utilizada no decorrer de toda esta dissertação.

Definição 4.1.3. Seja $X = \{0, \cdots, k-1\}$. Definimos a árvore enraizada k-ária como o grafo de vértices no conjunto X^*, onde cada vértice u possui k filhos, os vértices ux, para cada $x \in X$. A palavra vazia é a raiz da árvore.

Dizemos que uma árvore é regular se ela é k-ária para algum inteiro k. Por vezes utilizaremos apenas X^* para nos referirmos à árvore enraizada k-ária.

Dado um automorfismo g da árvore k-ária X^*, existe uma permutação $\pi_g : X \to X$ tal que:

$$g = \pi_g(g|_0, g|_1, \cdots, g|_{k-1}),$$

onde $g|_i$ é, também, um automorfismo da árvore k-ária. Portanto, dada uma palavra qualquer xw, com $x \in X$ e $w \in X^*$, temos:

$$g(xw) = \pi_g(x)g|_x(w).$$

Dizemos que um grupo G age transitivamente no primeiro nível da árvore k-ária se, dados $x, y \in X$, existe $g \in G$ tal que $g(x) = y$. Continuamos, agora, com as definições de grupo de automorfismos *self-similar* e de ação *self-similar*.

Definição 4.1.4. Um grupo G de automorfismos da árvore enraizada k-ária é dito *self-similar* se ele age transitivamente no primeiro nível e se, dado $g \in G$, com $g = \pi_g(g|_0, g|_1, \cdots, g|_{k-1})$, temos $g|_i \in G$, para todo $i \in X$.

Definição 4.1.5. Uma ação de um grupo G sobre a árvore enraizada k-ária X^* é denominada *self-similar* se ela é transitiva no primeiro nível e se, para todo $g \in G$ e $x \in X$, existem $h \in G$ e $y \in X$ tais que $g(xw) = yh(w)$, para todo $w \in X^*$.

Se retirarmos das duas definições acima a transitividade no primeiro nível da árvore, teremos as definições de grupo de automorfismos fechado por estado e de ação fechada por estado. Vale ressaltar que, quando se tratando da árvore p-ária, um grupo de automorfismos ou uma ação são fechados por estado se, e somente se, eles são *self-similar*.

Se G age sobre X^*, podemos definir uma função $\varphi : G \to \mathrm{Aut}(X^*)$ tal que $\varphi(g)(w) = g(w)$, para todo $w \in X^*$. Ou seja, cada elemento de G pode ser visto como um automorfismo (não necessariamente distinto) da árvore enraizada k-ária. Desta forma, a ação de G sobre a árvore k-ária é *self-similar* se, e somente se, $\varphi(G)$ é um grupo de automorfismos *self-similar*. Além disso, G será isomorfo a um grupo de automorfismos da árvore se, e somente se, sua ação sobre ela for fiel.

Introduzimos, agora, o conceito de endomorfismo virtual.

Definição 4.1.6. Dado um grupo G, um endomorfismo virtual é um homomorfismo $\phi : H \to G$, onde H é um subgrupo de G de índice finito k.

Este homomorfismo é também chamado de $\frac{1}{k}$-endomorfismo de G e é denotado por $\phi : H \to_k G$.

Definição 4.1.7. O *core* de um endomorfismo virtual $\phi : H \to_k G$ é o maior subgrupo normal de G contido em H que é ϕ-invariante.

Definição 4.1.8. Um endomorfismo virtual é dito simples se seu *core* é trivial.

A seguir mostramos um exemplo de um $\frac{1}{p}$-endomorfismo virtual simples.

Exemplo 4.1.9. Seja $G = C_p^m$, onde p é um número primo. Tome $S = \{e_1, \cdots, e_m\}$ um conjunto gerador de G e seja $H = \langle e_2, \cdots, e_m \rangle$. Definimos, então, o endomorfismo virtual injetivo $\phi : H \to_k G$ por $\phi(e_2^{\varepsilon_2} e_3^{\varepsilon_3} \cdots e_m^{\varepsilon_m}) = e_1^{\varepsilon_2} e_2^{\varepsilon_3} \cdots e_{m-1}^{\varepsilon_m}$, onde $\varepsilon_2, \cdots, \varepsilon_m \in \{0, \cdots, p-1\}$

Perceba que o único subgrupo ϕ-invariante em H é o subgrupo trivial, donde ϕ é um endomorfismo virtual simples.

Agora que definimos tudo o que era necessário, podemos apresentar a relação entre ações *self-similar* sobre X^* e endomorfismos virtuais. Seja G um grupo *self-similar* de automorfismos da árvore enraizada k-ária X^* agindo transitivamente sobre o primeiro nível da árvore, e seja H o estabilizador do vértice 0. Podemos, então, definir o $\frac{1}{k}$-endomorfismo virtual $\phi : H \to_k G$ por $\phi(h) = h|_0$.

A seguir, mostramos como é definida a ação *self-similar* de G sobre a árvore enraizada k-ária induzida por um $\frac{1}{k}$-endomorfismo virtual qualquer $\phi : H \to_k G$. Tome $T = \{t_o, t_1, \cdots, t_{k-1}\}$ um transversal de H em G tal que $t_0 = 1$. Dado $g \in G$, seja $\overline{g}$ o elemento de T tal que $gH = \overline{g}H$. Se G age sobre a árvore k-ária, podemos, através da função $\varphi : G \to \mathrm{Aut}(X^*)$, ver cada elemento $g \in G$ como um automorfismo $\varphi(g)$ de X^*. Como queremos definir uma ação *self-similar*, dado $g \in G$, devemos ter:

$$\varphi(g) = \pi_g(g|_0, g|_1, \cdots, g|_{k-1}),$$

onde π_g é uma permutação de X e, para todo $i \in X$, existe $g_i \in G$ tal que $\varphi(g_i) = g|_i$. Para definirmos a ação de G sobre a árvore k-ária, definiremos, primeiramente, o grupo de automorfismos $\varphi(G)$.

Defina $g|_x$ por $\varphi(\phi(\overline{gt_x}^{-1} g t_x))$ e $\pi_g : X \to X$ por $\pi_g(x) = y$, onde $\overline{gt_x} = t_y$. Desta forma, tomando $g(w) = \varphi(g)(w)$, para todo $w \in X^*$, definimos indutivamente uma ação *self-similar* de G sobre X^* tal que H é o estabilizador do vértice 0 e tal que G age transitivamente no primeiro nível.

Note que se a ação induzida por um endomorfismo virtual $\phi : H \to_k G$ é fiel, então G pode ser visto como um grupo *self-similar* de automorfismos da árvore enraizada k-ária. A seguinte proposição é de fundamental importância para a teoria, uma vez que ela fornece uma condição suficiente e necessária para que isso aconteça.

Proposição 4.1.10. A ação de G sobre a árvore enraizada k-ária induzida pelo endomorfismo virtual $\phi : H \to_k G$ é fiel se, e somente se, o endomorfismo virtual ϕ é simples.

Demonstração. Suponha que a ação induzida por $\phi : H \to_k G$ não é fiel, então existe $g \in G$, com $g \neq 1$, tal que $g(w) = w$, $\forall w \in X^*$. Note que $g \in G_0$, ou seja, $g \in H$. Seja $N = \bigcap_{w \in X^*} G_w$ e tome $g \in N$ qualquer. Temos, dado $x \in X$ qualquer:

$$xw = g(xw) = \pi_g(x)g|_x(w), \forall w \in X^*.$$

Donde $g|_x(w) = w$, $\forall w \in X^*$ e, portanto, $g|_x \in N$. Logo:

$$g|_x = \phi(\overline{gt_x}^{-1} g t_x) = \phi(t_x^{-1} g t_x) \in N, \forall x \in X.$$

Em particular, tomando $x = 0$, temos $g|_0 = \phi(g) \in N$. Logo, como g é qualquer, temos que N é ϕ-invariante. Sejam $z \in G$, $g \in N$ e $w \in X^*$ quaisquer, então:

$$\begin{aligned}(z^{-1}gz)(w) &= z^{-1}(g(z(w))) \\ &= z^{-1}(z(w)) \\ &= (z^{-1}z)(w) = w.\end{aligned}$$

Portanto $N \trianglelefteq G$. Por fim, como N é não trivial, temos que o endomorfismo virtual ϕ não é simples.

Suponha, agora, que a ação induzida por $\phi : H \to_k G$ é fiel, e tome $N \leq H$ um subgrupo normal em G que é ϕ-invariante. Queremos mostrar que $N = 1$. Sejam $g \in N$ e $x \in X$ quaisquer. Tome $g_1 \in N$ tal que $g_1 = g^{t_x}$. Logo:

$$\begin{aligned}&gt_xH = t_yH \\ \Rightarrow &t_x t_x^{-1} g t_x H = t_y H \\ \Rightarrow &t_x g_1 H = t_x H = t_y H.\end{aligned}$$

Portanto $t_x = t_y$. Temos então, para todo $x \in X$, $\overline{gt_x} = t_x$ e $\pi_g(x) = x$. Provaremos agora que $g(w) = w$, para todo $w \in X^*$ e $g \in N$. Para isso utilizaremos indução sobre o tamanho de w. O caso em que w tem tamanho 1 está demonstrado acima. Tome agora $xw \in X^*$ qualquer

e suponha que $g(w') = w'$, para todo $g \in N$ e toda palavra w' de tamanho igual ao de w. Tomando $g \in N$ qualquer, temos:

$$\begin{aligned} g(xw) &= \pi_g(x)g|_x(w) \\ &= x\phi(\overline{gt_x}^{-1}gt_x)(w) \\ &= x\phi(t_{\pi_g(x)}^{-1}gt_x)(w) \\ &= x\phi(g^{tx})(w). \end{aligned}$$

Mas N é ϕ-invariante e normal em G, donde $\phi(g^{tx}) \in N$ e, pela hipótese de indução, $g(xw) = x\phi(g^{tx})(w) = xw$. Por fim, pelo princípio de indução finito temos que N estabiliza toda palavra de X^*, donde, uma vez que a ação de G sobre a árvore k-ária é fiel, temos $N = 1$, como desejávamos.

□

Finalizamos esta seção com um exemplo no qual construímos uma ação *self-similar* sobre a árvore 3-ária a partir de um $\frac{1}{3}$-endomorfismo virtual.

Exemplo 4.1.11. Seja $H = C_3^4 = \langle b,c,d,e \mid b^3 = c^3 = d^3 = e^3 = 1\rangle$ e $G = H \rtimes \langle a\rangle = \langle a,b,c,d,e \mid a^3 = 1, b^a = b, c^a = bc, d^a = d, e^a = e\rangle$.

O automorfismo $\alpha : H \to H$ induzido por a nos dá a matriz:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Definimos ϕ a partir do mapeamento $b \mapsto d \mapsto e \mapsto a$ e $c \mapsto 1$ e tomamos $t_0 = 1$, $t_1 = a$ e $t_2 = a^2$ como o transversal de H. Por fim, a ação de G sobre a árvore ternária enraizada é dada por:

$$\begin{array}{rcll} a & = & (012) & (1,1,1) \\ b & = & (1) & (d,d,d) \\ c & = & (1) & (1,d,d^2) \\ d & = & (1) & (e,e,e) \\ e & = & (1) & (a,a,a) \end{array}$$

4.2 $\frac{1}{p}$-Endomorfismos virtuais

Seguiremos, agora, para o nosso objetivo principal, que é estudar $\frac{1}{p}$-endomorfismos virtuais de p-grupos finitos. A teoria apresentada nesta seção pode ser encontrada em [22].

Dado um endomorfismo virtual $\phi : H \to_p G$, temos que H é um subgrupo maximal de G e, portanto, é normal. Por este motivo, podemos verificar que, na ação sobre a árvore p-ária induzida por este endomorfismo, H é o estabilizador de todo o primeiro nível de X^*, não só do vértice 0.

Como nesta seção começaremos a trabalhar com $\frac{1}{p}$-endomorfismos, vale ressaltar que muitos grupos não podem ser fielmente representados como um grupo *self-similar* de automorfismos da árvore p-ária. Iniciamos com o seguinte exemplo:

Exemplo 4.2.1. Dizemos que um p-grupo é extra-especial se o seu subgrupo de Frattini e seu centro são iguais e têm ordem p. Todo p-grupo extra-especial tem ordem p^{2r+1}, para algum $r \geq 1$, e é o produto central de r p-grupos não abelianos de ordem p^3 (checar seção 5 do quinto capítulo de [9]). Desta forma, se G é um p-grupo extra-especial de ordem maior ou igual a p^5 e $H \leq G$ é um subgrupo maximal, então H não é abeliano, donde $[H,H] = [G,G] \neq 1$ e, portanto, não existem endomorfismos virtuais simples de domínio H.

A definição a seguir será utilizada em nosso próximo resultado.

Definição 4.2.2. Sejam K, G_1 e G_1 grupos.

(i) Dizemos que K é um produto subdireto de G_1 e G_2 se $K \leq G_1 \times G_2$ e as projeções de K sobre G_1 e G_2 são sobrejetivas.

(ii) K é dito subdiretamente irredutível se toda representação subdireta de K possui um grupo isomorfo a K como um dos fatores do produto.

Proposição 4.2.3. Seja $\phi : H \to_p G$ um endomorfismo virtual simples e não injetivo, onde G é um p-grupo não abeliano finito. Seja K o núcleo de ϕ. Então:

(i) K não contém nenhum subgrupo não trivial normal em G.

(ii) Dado $t \in G \backslash H$ e $i = 0, 1, \cdots, p-1$, temos que K^{t^i} é um subgrupo normal em H e $K \cap K^t \cap \cdots \cap K^{t^{p-1}} = 1$.

(iii) O grupo H é um produto subdireto não trivial de $H/K \times H/K^t \times \cdots \times H/K^{t^{p-1}}$.

Demonstração.

(i) Suponha $N \leq K$ com $N \trianglelefteq G$, então $\phi(N) = 1$, donde N é subgrupo ϕ-invariante de H normal em G. Portanto, como ϕ é simples, temos $N = 1$.

(ii) Primeiramente, tome $g \in G \backslash H$ qualquer. Como $H \trianglelefteq G$, temos que $K^g \leq H$. Além disso, dado $h \in H$:

$$\begin{aligned}(K^g)^h &= h^{-1}g^{-1}Kgh \\ &= g^{-1}(h^g)^{-1}Kh^g g \\ &= g^{-1}Kg.\end{aligned}$$

Logo, $K^g \trianglelefteq H$.

Temos $K \trianglelefteq H$ e $K \ntrianglelefteq G$ (pois K não é trivial), donde $H \leq N_G(K) < G$, mas H é maximal, logo $H = N_G(K)$. Portanto $[G : N_G(K)] = p$ é o número de conjugados de K em G. Mas se $K^{t^i} = K^{t^j}$, então $K^{t^{i-j}} = K$, donde $K \trianglelefteq \langle H, t^{i-j}\rangle \leq H$ e $t^{i-j} \in H$. Por fim, $i - j$ é um múltiplo de p, donde $K, K^t, \cdots, K^{t^{p-1}}$ são subgrupos distintos e, portanto, são os únicos conjugados de K.

Com isso, temos que $K \cap K^t \cap \cdots \cap K^{t^{p-1}} \leq K$ é normal em G. Portanto, pelo item anterior, temos $K \cap K^t \cap \cdots \cap K^{t^{p-1}} = 1$.

(iii) Como ϕ é não injetiva, temos $K = \ker\phi \neq 1$. Temos, então, que $K, K^t, \cdots, K^{t^{p-1}}$ são normais em H, são não triviais e possuem interseção trivial. Logo, podemos definir:

$$\begin{aligned}\theta : H &\to {}^{H}\!/_{K} \times {}^{H}\!/_{K^t} \times \cdots \times {}^{H}\!/_{K^{t^{p-1}}} \\ h &\mapsto (hK, hK^t, \cdots, hK^{t^{p-1}})\end{aligned}$$

Que é um homomorfismo com núcleo $K \cap K^t \cap \cdots \cap K^{t^{p-1}}$. Portanto $H \cong \mathrm{Im}\theta$, onde $\mathrm{Im}\theta$ é um subgrupo de ${}^{H}\!/_{K} \times {}^{H}\!/_{K^t} \times \cdots \times {}^{H}\!/_{K^{t^{p-1}}}$, cujas projeções são sobrejetivas.

□

Note que dado um endomorfismo virtual injetivo $\phi : H \to_p G$, onde G é um p-grupo, temos que H e $\phi(H)$ são subgrupos maximais isomorfos de G. A seguir, utilizamos a Proposição 4.2.3 para mostrar um exemplo de p-grupo que não admite nenhum $\frac{1}{p}$-endomorfismo virtual simples.

Exemplo 4.2.4. Considere o grupo diedral $D_{2^n} = \langle a, x \mid a^{2^{n-1}} = x^2 = 1, xax = a^{-1}\rangle$, com $n \geq 4$. Todos os subgrupos maximais deste grupo são subdiretamente irredutíveis, donde, pela Proposição 4.2.3, D_{2^n} não admite nenhum $\frac{1}{2}$-endomorfismo simples e não injetivo. Por

outro lado, os únicos dois subgrupos maximais isomorfos de D_{2^n} são $\langle a^2, x\rangle$ e $\langle a^2, ax\rangle$ e, dado um isomorfismo ϕ entre eles, podemos facilmente estender ϕ para um automorfismo de D_{2^n}. Porém, o subgrupo de Frattini de G é característico e está contido em $\langle a^2, x\rangle$ e em $\langle a^2, ax\rangle$, donde D_{2^n} também não admite nenhum $\frac{1}{2}$-endomorfismo simples e injetivo.

A seguir, apresentamos o Lema da Cisão (*Splitting Lemma*), que nos dá uma condição necessária para a existência de um $\frac{1}{p}$-endomorfismo virtual simples.

Lema 4.2.5 (Lema da Cisão)**.** Seja G um grupo tal que a seguinte sequência é uma sequência exata curta:

$$1 \to H \to G \to C_p \to 1.$$

Se $\phi : H \to_p G$ é um endomorfismo virtual simples e H contém elementos de ordem p, então $\phi(H)\backslash H$ também contém elementos de ordem p.

Além disso, G é uma extensão cindida de H.

Demonstração. Lembre-se que $\Omega_{\{1\}}(H) = \{x \in H \mid o(x) = p\}$. Sabemos que $\langle \Omega_{\{1\}}(H)\rangle = \Omega_1(H)$ é normal em G, portanto, como ϕ é simples, temos que $\Omega_1(H)$ não é ϕ-invariante. Logo, existe $x \in \Omega_{\{1\}}(H)$ tal que $\phi(x) \notin \Omega_1(H)$. Mas $o(\phi(x)) \mid p$, donde temos $o(\phi(x)) = p$. Além disso, temos $\phi(x) \notin \Omega_1(H)$, logo, $\phi(x) \notin H$. Temos, portanto, que $\phi(H)\backslash H$ possui elementos de ordem p.

Como H é maximal temos $G = \langle \phi(x)\rangle H$ com $\langle \phi(x)\rangle \cap H = 1$. Portanto, $\langle \phi(x)\rangle$ é um transversal de H e $\nu(\langle \phi(x)\rangle) = C_p$. Podemos, então, definir a cisão $\sigma : C_p \to G$ de tal forma que $\sigma(\nu(\phi(x)^n)) = \phi(x)^n$, para todo inteiro n. Portanto, G é um extensão cindida de H.

□

Para simplificar a nossa terminologia, finalizamos esta seção com a definição a seguir.

Definição 4.2.6. Dado um grupo G e um primo p, dizemos que G é *self-similar* para o primo p se o mesmo pode ser fielmente representado como um grupo *self-similar* de automorfismos da árvore enraizada p-ária.

4.3 $\frac{1}{p}$-Endomorfismo virtuais de p-grupos finitos com domínio abeliano

Uma pergunta que surge naturalmente no estudo de p-grupos *self-similar* é: quando um p-grupo possui um $\frac{1}{p}$-endomorfismo virtual simples? Nesta seção, trabalharemos com p-grupos que possuem um subgrupo maximal abeliano, e conseguiremos, no Teorema A, uma

resposta satisfatória para o problema neste caso. A teoria aqui presente pode ser encontrada em [22] e [1]. Iniciamos com a seguinte proposição:

Proposição 4.3.1. Seja G um grupo tal que a seguinte sequência é uma sequência exata curta:

$$1 \to H \to G \to C_p \to 1,$$

onde H é um p-grupo finito não-trivial.

Se existe um endomorfismo virtual simples $\phi : H \to_p G$ tal que $\phi(H)$ é um p-grupo regular, então G é um extensão cindida de H e o expoente de H é p.

Demonstração. Como H é um p-grupo não trivial e ϕ é simples, temos, pelo Lema 4.2.5, que G é um extensão cindida de H.

Seja $a \in \phi(H)\backslash H$ um elemento de ordem p (a existência de a é garantida, novamente, pelo Lema 4.2.5), então $G = \langle a \rangle H$. Além disso, como H é maximal em G e $\phi(H) \not\subseteq H$, temos $[\phi(H) : \phi(H) \cap H] = p$, donde $\phi(H) \cap H \trianglelefteq \phi(H)$ e $\phi(H) = \langle a \rangle (\phi(H) \cap H)$.

Logo, dado $h \in H$, existem $h_1 \in \phi(H) \cap H$ e $n \in \{0, \cdots, p-1\}$ tais que $\phi(h) = a^n h_1$. Note que $\langle a, h_1 \rangle' = \langle [a, h_1] \rangle = \langle (h_1^{-1})^a h^1 \rangle$, donde $\langle a, h_1 \rangle' \leq \phi(H) \cap H$. Por outro lado, temos, por hipótese, que $\phi(H)$ é regular, donde:

$$\phi(h^p) = \phi(h)^p = (a^n)^p h_1^p c^p = h_1^p c^p,$$

com $c \in \langle a, h_1 \rangle'$. Logo $\phi(h^p) \in H^p$ e, como o elemento h escolhido foi qualquer, $\phi(H^p) \leq H^p$. Mas $H^p \trianglelefteq G$, pois $H \trianglelefteq G$. Portanto, temos que H^p é um subgrupo ϕ-invariante normal em G e ϕ é um endomorfismo virtual simples, donde $H^p = 1$ e $\exp(H) = p$.

□

Com o próximo teorema, conseguimos dizer quando, dado um p-grupo G com um subgrupo maximal abeliano H, existe um endomorfismo virtual simples $\phi : H \to_p G$.

Teorema 4.3.2. Seja G um grupo tal que a seguinte sequência é uma sequência exata curta:

$$1 \to H \to G \to C_p \to 1,$$

onde H é p-grupo finito abeliano não trivial. Então existe um endomorfismo virtual simples $\phi : H \to_p G$ se, e somente se, G é uma extensão cindida de H e H é p-grupo abeliano elementar.

Demonstração.

($\Rightarrow$)

Note que, como H é abeliano, temos $\phi(H)$ é abeliano e, portanto, regular. Com isso, estamos nas hipóteses da Proposição 4.3.1, donde G é uma extensão cindida de H e $\exp(H) = p$.

($\Leftarrow$)

Por hipótese, temos que G é uma extensão cindida de H, portanto, H possui um complemento de ordem p. Seja $a \in G\backslash H$ um elemento de ordem p. Defina o automorfismo:

$$\begin{aligned} \alpha : H &\to H \\ h &\mapsto h^a \end{aligned}$$

Seja $d = d(H)$. Como H é abeliano elementar, podemos enxergá-lo como um espaço vetorial V de dimensão d sobre o corpo $\mathbb{F}_p$. Podemos, também, ver α como um elemento de ordem p de $GL(d,p)$. Como α tem ordem p, temos que o polinômio minimal de α divide $x^p - 1 = (x-1)^p$. Logo, o único autovalor de α é 1, donde cada bloco da matriz na forma canônica de Jordan tem tamanho menor ou igual a $p \times p$ e tem a forma:

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Sejam $s_1 \geq s_2 \geq \cdots \geq s_m$ os tamanhos dos blocos de Jordan e seja:

$$B = \{b_{1,1}, b_{1,2}, \cdots, b_{1,s_1}, b_{2,1}, b_{2,2}, \cdots, b_{2,s_2}, \cdots, b_{m,1}, b_{m,2}, \cdots, b_{m,s_m}\}$$

a base correspondente à matriz α na forma de Jordan, de modo que $E_1 = \langle b_{1,1}, b_{2,1}, \cdots, b_{m,1} \rangle$ é o espaço vetorial gerado pelos autovetores da matriz. Denotemos $K = \langle \{b_{i,j} \mid i = 1, \cdots, m; j = 2, \cdots, s_i\} \rangle$, donde $V = E_1 \oplus K$.

Definimos o endomorfismo virtual $\phi : H \to_p G$ a partir do mapeamento:

$$b_{1,1} \mapsto b_{2,1} \mapsto b_{3,1} \mapsto \cdots \mapsto b_{m-1,1} \mapsto b_{m,1} \mapsto b_{a,1},$$

para elementos da base de E_1, e do mapeamento:

$$b_{i,j} \mapsto 1,$$

para elementos da base de K. Lembremos que $\alpha(b_{i,1}) = 1b_{i,1}$, donde $b_{i,1}^a = b_{i,1}$, para todo $i = 1,2,\cdots,m$. Portanto, $\{b_{2,1}, b_{3,1}, \cdots, b_{m-1,1}, b_{m,1}, a\}$ comutam e o endomorfismo virtual ϕ está bem definido, de modo que $K = \ker(\phi)$.

Resta mostrar que ϕ é simples. Para isso, suponha $N \leq H$ ϕ-invariante e normal em G. Tome $x \in N$ qualquer, então, como H é abeliano, temos $x = vk$ para algum $v \in E_1$ e algum $k \in K$. Seja $v = b_{1,1}^{e_1} \cdots b_{m,1}^{e_m}$. Suponha por absurdo que $v \neq 1$ e seja e_i o expoente diferente de 0 tal que i é o maior possível. Então:

$$\phi^{m-i}(vk) = b_{m-i+1,1}^{e_1} \cdots b_{m,1}^{e_{i-1}} a^{e_i},$$

donde $\phi^{m-i}(x) \notin H$. Portanto, $\phi^{m-i}(x) \notin N$, o que é um contradição, pois N é ϕ-invariante. Logo, $v = 1$.

Suponha agora $k \neq 1$, então $k = z\, b_{i,j}^e$, para algum $z \in K$, com $j \neq 1$ o menor possível tal que $e \neq 0$. Note, porém, que $b_{i,j}^a = b_{i-1,j}\, b_{i,j}$, donde $k^{a^{i-1}} \notin K$, e, portanto, $k^{a^{i-1}} \notin N$, o que é uma contradição, pois $N \trianglelefteq G$. Logo, $v = k = 1$.

Por fim, concluímos que N é trivial, donde ϕ é um endomorfismo virtual simples.

□

Observação 4.3.3. Podemos estender a forma de enxergar a "volta"do Teorema 4.3.2.

Seja G um grupo tal que a seguinte sequência é uma sequência exata curta:

$$1 \to H \to G \to C_p \to 1,$$

onde H é p grupo finito não-trivial.

Defina E_1 como a intersecção de H com o maior p-grupo abeliano elementar contido em $Z(G)$. Uma vez que H é normal em G temos, pelo Teorema 1.2.1, que o grupo E_1 é não trivial. Todo subgrupo de H que é normal em G contém um elemento de E_1 (nesta observação E_1 realizará o mesmo papel que o auto-espaço E_1 realizou na prova do Teorema 4.3.2). Seja $\{b_1, b_2, \cdots, b_m\}$ uma base de E_1 e seja $a \in G \backslash H$ um elemento de ordem p. Como a comuta com $b_1, b_2, \cdots, b_m$ e tem ordem p, podemos definir o homomorfismo $\phi_0 : E_1 \to G$ a partir do mapeamento

$$b_1 \to b_2 \to \cdots \to b_m \to a.$$

Se pudermos estender ϕ_0 para um homomorfismo $\phi : H \to G$, então $\phi : H \to_p G$ será um endomorfismo virtual simples. Um dos casos em que podemos fazer isso é quando existe um subgrupo K normal em H tal que $H = K \rtimes E_1$.

Podemos reescrever o Teorema 4.3.2 de uma outra forma utilizando a Proposição 4.1.10.

Teorema 4.3.4. Um p-grupo finito admite uma ação fiel e *self-similar* sobre a árvore enraizada p-ária tal que o estabilizador do primeiro nível é abeliano se, e somente se, ele é uma extensão cindida de um p-grupo abeliano elementar pelo grupo cíclico de ordem p.

O lema a seguir será utilizado na demonstração do Teorema 4.3.6, que responde a questão proposta no início desta seção.

Lema 4.3.5. Seja G um p-grupo finito que possui um subgrupo maximal abeliano A. Então:

(i) Para todo $g \in G\backslash A$, temos $G' = \{[g,a] \mid a \in A\}$. Consequentemente $|G'| = [A : C_A(g)]$.

(ii) Se G não é abeliano, então $[G : Z(G)] = p|G'|$.

Demonstração.

(i) Tome $g \in G\backslash A$ qualquer. Sabemos que $G = \langle g, A\rangle$, donde $G' = \langle [x,y] \mid x,y \in \{g\} \cup A\rangle$. Mas, se $x,y \in A$, então $[x,y] = 1$, uma vez que A é abeliano, e $[x,y] = [y,x]^{-1}$. Portanto, $G' = \langle [g,a] \mid a \in A\rangle$.

Porém, dados $a,b \in A$, temos $[g,a],[g,b] \in A$ (pois $A \trianglelefteq G$). Logo, $[g,a,b] = 1$, donde:

$$[g,a][g,b] = [g,a][g,b][g,a,b] = [g,ab].$$

Note também que $[g,a^{o(a)-1}] = [g,a]^{-1}$. Portanto, $[g,a][g,b],[g,a]^{-1} \in \{[g,a] \mid a \in A\}$ e $G' = \{[g,a] \mid a \in A\}$. Podemos, então, definir o homomorfismo:

$$\begin{aligned} \theta : A &\to G' \\ a &\mapsto [g,a] \end{aligned}$$

Note que $a \in \ker(\theta)$ se, e somente se, $[g,a] = 1$, donde $\ker(\theta) = C_A(g)$. Logo, $A/C_A(g) \cong \mathrm{Im}\theta = G'$ e $|G'| = [A : C_A(g)]$.

(ii) Como G não é abeliano e A é um subgrupo maximal abeliano, temos $g \notin Z(G)$, para todo $g \in G\backslash A$. Logo, $Z(G) \leq A$. Tome $a \in A$ e $g \in G\backslash A$ quaisquer, então $a \in Z(G)$ se, e somente se, $[g,a] = 1$. Portanto, $Z(G) = C_A(g)$, donde, pelo item anterior, $[G : Z(G)] = [G : A][A : C_A(g)] = p|G'|$.

□

Por fim, a seguir temos o Teorema A, com o qual conseguimos caracterizar os p-grupos *self-similar* que possuem um subgrupo maximal abeliano.

Teorema 4.3.6. Seja G um p-grupo finito que possui um subgrupo maximal abeliano. Então G é *self-similar* se, e somente se, G possui um subgrupo maximal abeliano elementar do qual G é uma extensão cindida.

Demonstração.

($\Leftarrow$)

Esta parte da demonstração é um resultado direto do Teorema 4.3.2.

($\Rightarrow$)

Suponha G um grupo *self-similar*, $\phi : H \to_p G$ um endomorfismo virtual simples e $A \leq G$ um subgrupo maximal abeliano. Note que, se mostrarmos que H é abeliano, poderemos aplicar novamente o Teorema 4.3.2.

Suponha, por contradição, que H não é abeliano. Então temos $H \neq A$, donde $A \cap H$ é um subgrupo maximal abeliano de H. Provaremos, agora, que ϕ é injetivo. Suponha que exista $x \in \ker(\phi)\backslash A$. Pelo Lema 4.3.5, temos $H' = [x, A \cap H]$, donde $\phi(H') = 1$. Porém, como H' é um subgrupo característico de H, temos $H' \trianglelefteq G$. Mas, como ϕ é simples, $H' = 1$, o que contradiz a suposição de H não ser abeliano. Logo, $\ker(\phi) \leq A$, donde $H \leq N_G(\ker(\phi))$ e $A \leq N_G(\ker(\phi))$. Mas $G = HA$ e, portanto, $\ker(\phi) \trianglelefteq G$ e $\ker(\phi) = 1$.

Seja $g \in H\backslash A$. Então, pelo Lema 4.3.5, temos $G' = [g, A] = [g, G]$ e $H' = [g, A \cap H] = [g, H]$. Suponha que exista $a \in C_A(g)\backslash H$. Desta forma, $G = \langle a \rangle H = \langle a \rangle (\langle g \rangle A \cap H)$, logo, $G' = [g, \langle a \rangle H] = [g, H] = H'$. Mas $\phi(H') \leq G'$, donde $H' = 1$, o que contradiz a suposição de que H é não abeliano. Portanto, não existe $a \in C_A(g)\backslash H$ e, portanto, $Z(G) \leq H$.

Temos, então, pelo Lema 4.3.5:

$$\begin{aligned} |G'| &= [G : C_A(g)] \\ &= [A : A \cap H][A \cap H : C_A(g)] \\ &= p[A \cap H : C_{A \cap H}(g)] \\ &= p|H'|. \end{aligned}$$

Porém, novamente pelo Lema 4.3.5, $[G : Z(G)] = p|G'|$ e $[H : Z(H)] = p|H'|$, donde $[G : Z(G)] = p[H : Z(H)] = [G : Z(H)]$ e, então, $Z(G) = Z(H)$. Como ϕ é injetiva, podemos definir um endomorfismo virtual injetivo $\theta : \phi(H) \to_p G$, tal que $\theta(\phi(h)) = h$. Como $\phi(H)$ não é abeliano, também temos que $Z(\phi(H)) = Z(G)$. Logo:

$$\phi(Z(G)) = \phi(Z(H)) = Z(\phi(H)) = Z(G),$$

o que é uma contradição, pois ϕ é simples. Temos, então, por fim, que H é abeliano.

□

Para o caso em que p é um primo ímpar, conseguimos um resultado ainda mais forte. Finalizamos este capítulo com o corolário a seguir.

Corolário 4.3.7. Seja G um p-grupo finito, sendo p um primo ímpar. Se G possui um subgrupo maximal abeliano A, então G é *self-similar* se, e somente se, A é abeliano elementar e G é uma extensão cindida de A.

Demonstração.

($\Leftarrow$)

Esta parte da demonstração é um resultado direto do Teorema 4.3.2.

($\Rightarrow$)

Pelo Teorema 4.3.6, existe $H \leq G$, um subgrupo maximal abeliano elementar, do qual G é uma extensão cindida. Caso $A = H$, não há mais o que provar. Tomemos, então, $H \neq A$. Temos $G = HA$, donde $H \cap A \leq Z(G)$ (uma vez que ambos são grupos abelianos) e, então, $[G : Z(G)] \leq p^2$. Note que $G' \leq Z(G)$, portanto, G tem classe de nilpotência menor ou igual a 2. Como $p \geq 3$, temos que G é regular (pelo Teorema 1.2.13).

Seja $\langle g \rangle$ um complemento de H em G, então $g = ah$, para algum $a \in A \backslash H$ e algum $h \in H$. Como $a = gh^{-1}$, temos $o(a) = p$ (pelo Teorema 1.2.14), uma vez que $o(h) \leq o(g) = p$ e G é regular. Mas $A = \langle a \rangle A \cap H$ é abeliano, portanto, A é abeliano elementar.

□

O resultado acima, porém, não é válido se $p = 2$. Um contra-exemplo para este caso é o grupo D_8, que é *self-similar* e possui um subgrupo maximal abeliano não-elementar.

Capítulo 5

p-Grupos *self-similar* de determinada coclasse

Provaremos, agora, alguns resultados de p-grupos *self-similar* utilizando seus postos ou suas coclasses. Mostraremos os resultados do artigo "*On self-similar p-groups*" ([1]), de A. Babai, K. Fathalikhani, G. A. Fernández-Alcober e M. Vannacci. O objetivo principal deste capítulo é a demonstração dos Teoremas B e C, presentes na introdução desta dissertação. Para isso, utilizaremos endomorfismos virtuais.

5.1 p-Grupos *self-similar* de determinado posto

O primeiro resultado desta seção é, também, o mais importante, uma vez que todos os demais são consequências dele. O teorema ao qual nos referimos é o Teorema B, que nos diz que existe somente uma quantidade finita de p-grupos finitos *self-similar* de um determinado posto (definimos posto na Definição 1.1.9). Com este resultado, conseguiremos provar que existem apenas finitos p-grupos *self-similar* de uma determinada coclasse (Corolário 5.1.2) e apenas finitos p-grupos *self-similar* de determinada classe de nilpotência e número de geradores mínimo fixado (Corolário 5.1.3).

Dados $n_1, n_2, \cdots, n_m$ variáveis inteiras, dizemos que uma outra variável inteira é $(n_1, \cdots, n_m)$-limitada se a mesma é limitada superiormente por uma função de $n_1, n_2, \cdots, n_m$. Lembre-se que, ao tratarmos de uma base $\{a_1, \cdots, a_d\}$ de um grupo, sempre assumiremos $o(a_1) \geq \cdots \geq o(a_d)$. A demonstração do resultado a seguir se baseia na teoria de p-grupos *powerful*.

Teorema 5.1.1. Seja G um p-grupo finito *self-similar* de posto r. Então a ordem de G é (p, r)-limitada.

Demonstração. Seja $\phi : H \to_p G$ um endomorfismo virtual simples de G, sendo H um subgrupo maximal de G. Pelo Teorema 2.2.5, existe $W \trianglelefteq G$ (com $W = V(G,r)$, se p é ímpar, e $W = V(G,r)^2$, se $p = 2$) tal que, pela Proposição 2.2.4, todo subgrupo normal de G contido em W é *powerfully embedded* em W. Temos também que $[G : W]$ é (p,r)-limitado. Tome $N = (W \cap H)^2$, então $[W \cap H : N] \leq 2^r$, donde $[G : N] \leq 2^r[G : W \cap H] \leq 2^r[G : W][G : H] = 2^r p[G : W]$ e, portanto, o índice de N é (p,r)-limitado. Mostraremos que a ordem de N é, também, (p,r)-limitada.

Seja $\{a_1, \cdots, a_d\}$ uma base do p-grupo *powerful* N (pela Proposição 2.3.7 garante a sua existência), onde $d = d(N) \leq r$. Defina $m_i = o(a_i)$, para $i = 1, \cdots, d$, e $m_{d+1} = 1$, e seja e o exponente de G/N. Afirmamos que $m_i \leq em_{i+1}$, para todo $i = 1, \cdots, d$. Suponha, por contradição, que $m_{j-1} > em_j$ para algum j com $2 \leq j \leq d+1$. Então:

$$\phi(\Omega_1(N^{em_j})) \leq \Omega_1(G^{em_j}) \leq \Omega_1((G^e)^{m_j}) \leq \Omega_1(N^{m_j}).$$

Temos, porém, pelo Teorema 2.1.11:

$$N^{m_j} = \langle a_1^{m_j} \rangle \cdots \langle a_d^{m_j} \rangle = \langle a_1^{m_j} \rangle \cdots \langle a_{j-1}^{m_j} \rangle.$$

sendo $\{a_1^{m_j}, \cdots, a_{j-1}^{m_j}\}$ uma base de N^{m_j}. Como $o(a_i) \geq o(a_{j-1}) \geq em_j$, para $i \geq j-1$, temos, analogamente, que $\{a_1^{em_j}, \cdots, a_{j-1}^{em_j}\}$ é uma base de N^{em_j}. Pelo Lema 2.3.8 , temos:

$$\Omega_1(N^{m_j}) = \langle a_1^{m_1/p}, \cdots a_{j-1}^{m_j/p} \rangle = \Omega_1(N^{em_j}).$$

Mas $\phi(\Omega_1(N^{em_j})) \leq \Omega_1(N^{m_j})$, donde, como ϕ é simples, temos $\Omega_1(N^{em_j}) = 1$, o que é uma contradição, pois $m_{j-1} > em_j$.

Temos, então, $m_i \leq em_{i-1}$, para todo $i = 1, \cdots, d$. Logo:

$$m_i \leq em_{i-1} \leq e^2 m_{i-2} \leq \cdots \leq e^{d-i+1}.$$

Portanto:

$$|N| = |\langle a_1 \rangle| \cdots |\langle a_d \rangle| = m_1 \cdots m_d \leq e^{\frac{d(d+1)}{2}}.$$

Como $d \leq r$ e $e \leq |G/N| = [G : N]$, temos que a ordem de N é (p,r)-limitada. Portanto, a ordem de G é, também, (p,r)-limitada.

□

Corolário 5.1.2. Seja G um p-grupo finito *self-similar* de coclasse s. Então a ordem de G é (p,s)-limitada.

Demonstração. Seja c a classe de nilpotência de G e seja $m = (p-1)p^{s-1}$, se p é ímpar, e $m = 2^{s+2}$, se $p = 2$. Os grupos G tais que $c \leq 2p^{s+2}$, obviamente, tem a ordem limitada por $p^{s+2p^{s+2}}$. Se G é um grupo tal que $c > 2p^{s+2}$, então, pelos Teoremas 3.3.9 e 3.3.10, temos que G age uniserialmente sobre o subgrupo $\gamma_m(G)$, donde $|\gamma_m(G)| = p^{c+1-m}$. Desta forma, $[G : \gamma_m(G)] = p^{c+s}/p^{c+1-m} = p^{s+m-1}$. Além disso, por esses mesmos teoremas, temos $d(\gamma_m(G)) \leq m$ e, pelo Corolário 3.3.3, temos que $\gamma_m(G)$ é *powerful*. Portanto, o posto de $\gamma_m(G)$ é (p,s)-limitado e o índice $[G : \gamma_m(G)]$ é (p,s)-limitado, donde o posto de G é, também, (p,s)-limitado. Portanto, pelo Teorema 5.1.1, temos que a ordem de G é (p,s)-limitada.

□

Corolário 5.1.3. Seja G um p-grupo *self-similar* d-gerado de classe de nilpotência c. Então a ordem de G é (p,d,c)-limitada.

Demonstração. Pelo Corolário 1.1.11, temos que o posto de G é (d,c)-limitado, donde, pelo Teorema 5.1.1, temos que a ordem de G é (p,d,c)-limitada.

□

Finalizaremos esta seção com o Corolário 5.1.6, que tem sua demonstração em grande parte contida na prova do Teorema 5.1.1 e que julgamos poder ser de interesse independente dos demais resultados. A definição a seguir nos servirá para formular a hipótese deste corolário.

Definição 5.1.4. Um p-grupo finito é dito uniformemente *powerful* se:

(i) G é *powerful*;

(ii) Para todo i tal que $G^{p^i} \neq 1$, temos $[G^{p^i} : G^{p^{i+1}}] = [G : G^p]$.

Diremos que um p-grupo é uniforme se ele é uniformemente *powerful*. O lema a seguir nos fornece uma ferramenta que nos será útil para provarmos o último resultado desta seção.

Lema 5.1.5. Se G é um p-grupo uniforme, então, para todo i tal que $G^{p^i} \neq 1$, temos $d(G^{p^i}) = d(G)$.

Demonstração. Suponha i qualquer tal que $G^{p^i} \neq 1$. Temos $G^{p^{i+1}} = \Phi(G^{p^i})$, donde, como G é uniforme, temos $|G^{p^i}/\Phi(G^{p^i})| = |G/\Phi(G)|$. Desta forma, como ambos os grupos são abelianos elementares, temos $d(G^{p^i}/\Phi(G^{p^i})) = d(G/\Phi(G))$ e, portanto, $d(G^{p^i}) = d(G)$.

□

Corolário 5.1.6. Seja G um p-grupo finito *self-similar* e $\phi : H \to_p G$ um endomorfismo virtual simples. Se $U \subseteq H$ é um subgrupo normal uniforme de G, então $\exp(U) \leq \exp(G/U)$ se p é ímpar, e $\exp(U) \leq 4\exp(G/U)$ se $p = 2$.

Demonstração. Tome $N = U^2$. Utilizaremos as mesmas notações da prova do Teorema 5.1.1. Pelo Lema 5.1.5, temos $m_i = m_d$, para todo $i = 1, \cdots, d$, donde, como $N^{p^i} = \langle a_1^{p^i}, \cdots, a_d^{p^i} \rangle$, temos $\exp(N) = m_d$. Pela demonstração do Teorema 5.1.1, porém, sabemos que $\exp(G/N) \geq m_d$, logo, $\exp(G/N) \geq \exp(N)$. Caso p seja ímpar, já temos o resultado desejado. Caso $p = 2$, temos $\exp(U) = 2\exp(U^2) \leq 2\exp(G/U^2) \leq 4\exp(G/U)$.

□

5.2 p-Grupos *self-similar* de classe maximal

Trabalharemos, agora, com p-grupos *self-similar* de classe maximal, isto é, de coclasse igual a 1. Nesta seção, demonstraremos o Teorema C, ou seja, daremos uma caracterização completa destes p-grupos (Teorema 5.2.5), além de darmos a melhor cota possível para a ordem dos mesmos (Corolário 5.2.4).

Resgataremos, agora, as notações utilizadas na terceira seção do nosso primeiro capítulo e, assim como nela, trabalharemos somente com p-grupos de ordem maior ou igual a p^4. Relembrando, dado um p-grupo de classe maximal G, consideramos $G_0 = G$, $G_1 = C_G(G_2/G_4)$ e $G_i = \gamma_i(G)$, para $i \geq 2$.

Iniciamos com dois resultados a respeito de p-grupos de classe maximal.

Lema 5.2.1. Seja G um p-grupo de classe maximal de ordem $p^n \geq p^4$, e seja K um subgrupo de G que contém um elemento uniforme. Se existe um elemento x em K tal que $x \in G_t \setminus G_{t+1}$, então $G_t \leq K$.

Demonstração. Seja $s \in K$ um elemento uniforme de G, então $[x,s] \in G_{t+1} \setminus G_{t+2}$, $[x,s,s] \in G_{t+2} \setminus G_{t+3}$, e assim por diante, até temos $[x,\ {}_{n-1-t}\ s] \in G_{n-1} \setminus G_n$. Como G_{n-1} é um subgrupo central de ordem p, temos $G_{n-1} \leq K$, donde, uma vez que $[G_{n-1}, G_{n-2}] = p$, temos $G_{n-1} = [x,\ {}_{n-2-t}\ s]G_{n-2} \leq K$. Utilizando este argumento recursivamente, concluímos que $G_t \leq K$.

□

Proposição 5.2.2. Seja G um p-grupo de classe maximal e ordem $p^n \geq p^4$, e seja K um subgrupo de G que contém um elemento uniforme s. Se $|K| = p^{n-t}$, então $K = \langle s, G_{t+1} \rangle$.

Demonstração. Como $G = \langle s \rangle G_1$ e $s \in K$, temos $K = \langle s \rangle (K \cap G)$, donde $|K \cap G_1| = p^{n-t-1}$. Se $t = n-1$, temos $G_{t+1} = 1$ e $|K| = p$, donde temos o resultado. Suponha, agora, $t \leq n-2$,

ou seja, $K \cap G_1 \neq 1$. Considere $j = \min\{i \mid 1 \leq i \leq n-1, K \cap (G_i \backslash G_{i+1}) \neq \emptyset\}$. Portanto, pelo Lema 5.2.1, $K \cap G_1 = G_j$, pois $G_j \leq K \cap G_1$ e, se $x \in K \cap G_1$, então $x \in G_i \backslash G_{i+1}$, para algum i, donde, pela definição de j, $x \in G_j$. Como $|G_j| = p^{n-j}$, temos $j = t+1$. Logo, $K = \langle s, G_{t+1} \rangle$.

□

Com estes dois resultados, conseguimos provar a próxima proposição, que já nos diz bastante sobre os endomorfismos virtuais simples de um p-grupo de classe maximal.

Proposição 5.2.3. Seja G um p-grupo de classe maximal de ordem maior ou igual a p^4, e seja H um subgrupo maximal de G diferente de G_1. Então não existe endomorfismo virtual simples de H em G.

Demonstração. Como G/H é abeliano, temos $G_2 \leq H$. Além disso, temos $[G : G_2] = p^2$, donde $[H, G_2] = p$ e H/G_2 é cíclico. Portanto, $H' = [H, G_2]$. Como $[H, G_2] \trianglelefteq G$ e $[H, G_2]$ é um subgrupo próprio de G_2, temos $[H, G_2] = G_i$, para algum $i \geq 3$. Temos, também, que $[H, G_2] \not\leq G_4$, pois $H \neq G_1$. Logo, $[H, G_2] = G_3$.

Suponha, por absurdo, que $\phi : H \to_p G$ é um endomorfismo virtual simples. Sabemos que $\phi(H)$ é um subgrupo próprio de G, donde podemos considerar M um subgrupo maximal de G contendo $\phi(H)$. Logo, temos:

$$\phi(H') = \phi(H)' \leq M' = [M, G_2] \leq G_3 = H'.$$

O que é um absurdo, pois ϕ é simples e $H' = G_3 \neq 1$.

□

Com este resultado, provamos o seguinte corolário, que nos dá uma cota para a ordem dos p-grupos *self-similar* de classe maximal.

Corolário 5.2.4. Seja G um p-grupo de classe maximal. Se G é *self-similar*, então $|G| \leq p^{p+1}$.

Demonstração. Suponha que G é um p-grupo de classe maximal cuja ordem é maior que p^{p+1}. Pelo Teorema 1.3.18, temos $G_1^p = G_p$. Como $s^p \leq Z(G)$ (Teorema 1.3.10) e (uma vez que $G_p \neq 1$) $Z(G) \leq G_p$, temos $G^p = G_1^p$. Suponha, agora, por absurdo, que $\phi : H \to_p G$ é um endomorfismo virtual simples de G. Pela Proposição 5.2.3, temos $H = G_1$, donde, $\phi(H^p) \leq G^p = H^p$, o que é uma contradição. Portanto, G não é *self-similar* e temos o resultado desejado.

□

O resultado acima é o melhor possível, uma vez que o produto entrelaçado $C_p \wr C_p = C_p^p \rtimes C_p$ tem ordem p^{p+1}. É fácil ver que este grupo é *self-similar*, pois C_p^p é um subgrupo maximal abeliano elementar do qual $C_p \wr C_p$ é uma extensão cindida.

Caracterizamos, a seguir, os p-grupos *self-similar* de classe maximal.

Teorema 5.2.5. Seja G um p-grupo de classe maximal de ordem maior ou igual a p^4. Então G é *self-similar* se, e somente se, G_1 é abeliano elementar e G é uma extensão cindida de G_1.

Demonstração. Se G_1 é abeliano elementar e G é uma extensão cindida de G_1, então, pelo Teorema 4.3.2, G é *self-similar*.

Suponha que G é *self-similar* e seja $\phi : H \to_p G$ um endomorfismo virtual simples. Pela Proposição 5.2.3, $H = G_1$. Seja $|G| = p^n$. Primeiramente, provaremos o caso em que $l(G) \geq 1$. Como ϕ é simples, temos $\phi(G_1) \not\subseteq G_1$. Seja $s \in \phi(G_1) \backslash G_1$. Como $l(G) \geq 1$, G_1 é o único centralizador de 2-passos em G (Proposição 1.3.21), donde s é um elemento uniforme. Portanto, pela Proposição 5.2.2, temos $\phi(G_1) = \langle s, G_{t+1} \rangle$, para algum inteiro t.

Mostraremos que $|\phi(G_1)| = p$ ou p^2, para isso, suponha por absurdo $|\phi(G_1)| \geq p^3$. Pelo Teorema 1.3.10, temos que $\phi(G_1)$ é de classe maximal, donde $|Z(\phi(G_1))| = p$ e, portanto, $Z(\phi(G_1)) = Z(G)$. Por outro lado, $Z(G_1) \trianglelefteq G$, donde $Z(G) \leq Z(G_1)$. Consequentemente:

$$\phi(Z(G_1)) \leq Z(\phi(G_1)) = Z(G) \leq Z(G_1),$$

o que é um absurdo, pois ϕ é simples. Portanto, $|\phi(G_1)| = p$ ou p^2. Temos, então, que $\phi(G_1') = \phi(G_1)' = 1$. Com isso, temos $\phi(G_1') \leq G_1'$, donde, como ϕ é simples, temos que G_1 é abeliano. Logo, pelo Teorema 4.3.2, temos que G_1 é abeliano elementar e que G é uma extensão cindida de G_1.

Tratemos, agora, do cado em que $l(G) = 0$. Como $Z(G_1)$ é normal em G, temos que $Z(G_1) = G_i$, para algum inteiro i. Temos $[G_1, G_{n-2}] \neq 1$, pois, pela Proposição 1.3.21, $G_1 \neq C_G(G_{n-2})$, portanto, $G_{n-2} \not\subseteq Z(G_1)$. Com isso, temos $Z(G_1) = G_{n-1}$ e $|Z(G_1)| = p$. Se ϕ é não injetivo, então temos $Z(G_1) \leq \ker\phi$ (pois $\ker\phi \trianglelefteq G_1$), o que é uma contradição, pois ϕ é simples. Portanto, ϕ é injetivo e, consequentemente, $\phi(G_1)$ é um subgrupo maximal de G. Podemos, então, definir o seguinte $\frac{1}{p}$-endomorfismo virtual:

$$\begin{aligned} \varphi : \phi(G_1) &\to G \\ x \quad &\mapsto \phi^{-1}(x) \end{aligned}$$

Este endomorfismo virtual é simples, pois, se $\varphi(N) \leq N$, então $\phi(\varphi(N)) \leq N$. Portanto, pela Proposição 5.2.3, temos $\phi(G_1) = G_1$, o que é uma contradição, uma vez que ϕ é simples. Desta forma, temos $l(G) \neq 0$, o que conclui a prova.

□

Se G é um p-grupo de classe maximal no qual G_1 é abeliano elementar, não podemos garantir que G é *self-similar*. Isto acontece pois não necessariamente G_1 terá um complemento em G (todos os elementos uniformes de G podem ter ordem p^2). Porém, nestas hipóteses, apresentamos o corolário a seguir, que finaliza esta seção.

Corolário 5.2.6. Seja G um p-grupo de classe maximal de ordem menor ou igual a p^{p+1} tal que G_1 é abeliano. Então $G/Z(G)$ é um p-grupo *self-similar*.

Demonstração. Pelo Teorema 1.3.1, temos que $G/Z(G)$ é de classe maximal e, pelo Teorema 1.3.16, temos $\exp(G/Z(G)) = p$. Logo, temos que $(G/Z(G))_1 = G_1/Z(G)$ é abeliano elementar. Além disso, como todo elemento uniforme de $G/Z(G)$ tem ordem p, temos que $G/Z(G)$ é uma extensão cindida de $(G/Z(G))_1$. Portanto, pelo Teorema 5.2.5, $G/Z(G)$ é um p-grupo *self-similar*.

□

Bibliografia

[1] Babai, A., Fathalikhani, K., Fernandez-Alcober, G., and Vannacci, M. (2016). On self-similar finite p-groups. *ArXiv*.

[2] Bartholdi, L. and Šunik, Z. (2006). Some solvable automaton groups. *Contemporary Mathematics*, 394:11–29.

[3] Bartholdi, L. and Virág, B. (2005). Amenability via random walks. *Duke Math. J.*, 130(1):39–56.

[4] Berlatto, A. and Sidki, S. (2007). Virtual endomorphisms of nilpotent groups. *Groups, Geometry, and Dynamics*, 1(1):21–46.

[5] Brunner, A. and Sidki, S. (2010). Abelian state-closed subgroups of automorphisms of m-ary trees. *Groups, geometry and dynamics*, 4(3):455–472.

[6] Dixon, J. D., Du Sautoy, M. P. F., Mann, A., and Segal, D. (1999). *Analytic Pro-p Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition.

[7] Fernández-Alcober, G. A. (2001). An introduction to finite p-groups: regular p-groups and groups of maximal class. *Matemática Contemporânea*, 20:156–226.

[8] Fernández-Alcober, G. A. (2007). Omega subgroups of powerful p-groups. *Israel Journal of Mathematics*, 162(1):75–79.

[9] Gorenstein, D. (2007). *Finite Groups*. AMS Chelsea Publishing Series. American Mathematical Society.

[10] Grigorchuk, R. and Zuk, A. (2002). On a torsion-free weakly branch group defined by a three state automaton. *IJAC*, 12:223–245.

[11] Grigorchuk, R. I. (1980). On burnside's problem on periodic groups. *Funktsional. Anal. i Prilozhen.*, 14(1):53–54.

[12] Gupta, N. and Sidki, S. (1983a). On the burnside problem for periodic groups. *Mathematische Zeitschrift*, 182:385–388.

[13] Gupta, N. and Sidki, S. (1983b). Some infinite p-groups. *Algebra and Logic*, 22:421–424.

[14] Johnson, D. L. (1997). *Presentations of Groups*. London Mathematical Society Student Texts. Cambridge University Press, 2 edition.

[15] Khukhro, E. (2011). *Nilpotent Groups and their Automorphisms*. De Gruyter Expositions in Mathematics. De Gruyter.

[16] Khukhro, E. I. (1998). *p-Automorphisms of Finite p-Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press.

[17] Leedham-Green, C., McKay, S., and Society, L. M. (2002). *The Structure of Groups of Prime Power Order*. London Mathematical Society monographs. Oxford University Press.

[18] Lubotzky, A. and Mann, A. (1987). Powerful p-groups. i: Finite groups. *Journal of Algebra*, 105.

[19] Nekrashevych, V. (2002). Virtual endomorphisms of groups. *Algebra and Discrete Mathematics*, 2002.

[20] Nekrashevych, V. and Sidki, S. (2004). Automorphisms of the binary tree: State-closed subgroups and dynamics of 1/2-endomorphisms. *Groups: Topological, Combinatorial and Arithmetic Aspects*, 311.

[21] Steinberg, B., Vorobets, M., and Vorobets, Y. (2006). Automata over a binary alphabet generating free groups of even rank. *International Journal of Algebra and Computation*, 21.

[22] Šunić, Z. (2010). Finite self-similar p-groups with abelian first level stabilizers. *International Journal of Algebra and Computation*, 21.

[23] Vorobets, M. and Vorobets, Y. (2007). On a free group of transformations defined by an automaton. *Geometriae Dedicata*, 124:237–249.

[24] Vorobets, M. and Vorobets, Y. (2010). On a series of finite automata defining free transformation groups. *Groups, Geometry, and Dynamics*, 4(2):377–405.