Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Um estudo sobre p-grupos finitos powerful e potent

Nathália Nogueira Gonçalves

Brasília

2017

Nathália Nogueira Gonçalves

Um estudo sobre p-grupos finitos powerful e potent

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

Orientador:
Prof. Dr. Emerson Ferreira de Melo

Brasília

2017

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

Gonçalves, Nathália Nogueira
GG643e Um estudo sobre p-grupos finitos powerful e potent / Nathália Nogueira Gonçalves; orientador Emerson Ferreira de Melo. -- Brasília, 2017.
105 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2017.

1. p-grupos finitos. 2. powerful. 3. potent. I. Melo, Emerson Ferreira de, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de matemática

Um estudo sobre p-grupos finitos powerful e potent

por

Nathália Nogueira Gonçalves *

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

MESTRE EM MATEMÁTICA

Brasília, 24 de Fevereiro de 2017

Comissão Examinadora:

Emerson Ferreira de Melo
Dr. Emerson Ferreira de Melo (Orientador) - UnB

[illegible]
Dr. Raimundo de Araujo Bastos Júnior - UnB

Jhone Caldeira Silva
Dr. Jhone Caldeira Siva - UFG

*A autora foi bolsista do CNPq durante a elaboração deste trabalho.

"Nunca tenha certeza de nada, por que a sabedoria começa com a dúvida."
(Freud)

Agradecimentos

Primeiramente agradeço a Deus pela vitória alcançada.

Agradeço aos meus pais e às minhas irmãs pelo amor incondicional e por toda a ajuda nessa caminhada. Nenhuma palavra descreve minha gratidão e meu amor por vocês.

Ao meu amor, Rafael, por estar sempre comigo, por aguentar meus choros, aflições e mau humor durante esse tempo em Brasília. E por mais esse passo juntos.

À todos os meus familiares. Em especial, ao meu Avô, meus tios Sérgio, Jack e Renato, pelas orações e pelo exemplo de sempre. Aos meus primos, Gabriel e Benisa, que são meus irmãos de coração. Ao meu afilhado, Rafael, pela alegria.

Aos meus queridos amigos de Ouro Preto e do Colégio Sinapse por todo o carinho. Em especial, Su e Tiany, pela presença de sempre.

Aos meus professores da UFOP, que tanto me incentivaram. Em especial aos professores Sebastião Martins, Jamil Ferreira e Gustavo Souza por todo o incentivo.

Ao meu orientador Emerson Ferreira de Melo por todos os ensinamentos, paciência, disposição e dedicação. Obrigada também pelas ótimas conversas políticas e pessoais.

Agradeço aos professores participantes da banca Jhone Caldeira Silva e Raimundo de Araújo Bastos Júnior por aceitarem o convite e também pelas correções e sugestões.

Aos professores do Departamento de Matemática da UnB pelos conhecimentos transmitidos. Em especial os professores Cristina Acciarri, Daniela Amato, Emerson de Melo, Martino Garonzi e Noraí Rocco, por me mostrarem o quanto a Álgebra é fascinante.

Aos funcionários do Departamento de Matemática por todo o acolhimento e simpatia.

À todos os meus amigos do departamento, pelas várias conversas e risadas. Obrigada a todos os presentes na minha apresentação, pela força e torcida. Em especial, Alexandre, Ana Paula, Anna Carolina, Bruno, Christe, Lumena, Regiane, Sara e Welinton. Por estarem sempre ao meu lado durante esses dois anos.

Agradeço ao CNPq pelo apoio financeiro à este trabalho.

Enfim, agradeço a todos que de certa forma me ajudaram a chegar até aqui.

Resumo

Neste trabalho faremos um estudo sobre p-grupos finitos. Dentre as muitas propriedades que veremos, destacamos o estudo sobre a estrutura *power abelian* dos subgrupos normais de um p-grupo finito *potent*, que foi estudada através do artigo "*On the structure of normal subgroups of potent p-groups*". E também apresentamos uma caracterização para um p-grupo finito ser *powerful* obtida no artigo "*A characterization of powerful p-groups*".

Palavras-Chaves: p-grupos finitos; *powerful*; *potent*.

Abstract

In this work we will study finite p-groups. Among the properties, we highlight the power abelian structure of a normal subgroup of a finite potent p-group, which was studied in the paper "*On the structure of normal subgroups of potent p-groups*". We also present a characterization for a finite p-group to be a powerful p-group proved in the paper "*A characterization of powerful p-groups*".

Key-Words: finite p-group; powerful; potent.

Notações

$\lfloor r \rfloor$	O maior inteiro que é menor ou igual do que r.
$\lceil r \rceil$	O menor inteiro que é maior ou igual do que r.
$o(x)$	Ordem do elemento x.
x^y	$y^{-1}xy$.
$[x, y]$	$x^{-1}y^{-1}xy$.
$[x_1, \dots, x_n]$	$[[x_1, \dots, x_{n-1}], x_n]$.
$\|G\|$	Ordem do grupo G.
$d(G)$	Número mínimo de geradores do grupo G.
$H \leqslant G$	H um subgrupo do grupo G.
$\langle X \rangle$	Subgrupo gerado pelo conjunto X.
$[H_1, H_2]$	$\langle [x, y] \| x \in H_1, y \in H_2 \rangle$.
$[H_1, \dots, H_n]$	$[[H, \dots, H_{n-1}], H_n]$.
$[H_{1,k} H_2]$	$[H_1, H_2, \dots, H_2]$, H_2 aparece k vezes.
$N_G(H)$	Normalizador do subgrupo H no grupo G.
$C_G(H)$	Centralizador do subgrupo H no grupo G.
$Z(G)$	Centro do grupo G.
$\|G : H\|$	Índice do subgrupo H no grupo G.
$N \trianglelefteq G$	N um subgrupo normal do grupo G.
$\Phi(G)$	Subgrupo de Frattini do grupo G.
$\gamma_n(G)$	n-ésimo termo da série central inferior do grupo G.
$[G, G] = G'$	Subgrupo derivado do grupo G.
G^n	Subgrupo gerado pelas n-ésimas potências de elementos do grupo G.
$G^{\{n\}}$	Conjunto das n-ésimas potências de elementos do grupo G.
$\Omega_n(G)$	Subgrupo gerado pelos elementos do grupo G que possuem ordem menor ou igual a p^n.
$\Omega_{\{n\}}(G)$	Conjunto dos elementos do grupo G que possuem ordem menor ou igual a p^n.
$\mathbb{F}_p$	Corpo finito com p elementos.
$\mathbb{F}_p[t]$	Anel de polinômios na incógnita t e coeficientes em $\mathbb{F}_p$.
$Ann_M(t)$	$\{x \in M \mid tx = 0\}$, onde M é um módulo.

Sumário

Notações **1**

Introdução **4**

1 Preliminares **8**

1.1 Teoria de Grupos 8

1.1.1 Comutadores e subgrupos gerados por comutadores 8

1.1.2 Grupos nilpotentes 10

1.1.3 O subgrupo de Frattini 11

1.1.4 Fórmula de Compilação de Hall 12

1.2 Anéis e Módulos 13

2 Algumas famílias de p-grupos finitos **16**

2.1 Propriedades gerais 16

2.2 p-grupos regulares 22

2.3 p-grupos de classe maximal 29

2.4 p-grupos *powerful* 34

2.5 p-grupos *potent* 49

3 Resultados principais sobre p-grupos *potent* **56**

3.1 Subgrupos normais de um p-grupo *potent* 56

3.2 Estrutura de subgrupos normais de um p-grupo *potent* 72

4 Resultados principais sobre p-grupos *powerful* **81**

4.1 Grupos ω-maximal e palavras *interchangeable* 81

4.2 Resultados principais 87

5 Uma família de exemplos **92**

5.1 Preliminares para a construção da família 92

5.2 Família de exemplos 95

Bibliografia **98**

Introdução

Seja G um p-grupo abeliano, com p um primo. Usando o homomorfismo $\phi : G \to G$ dado por $\phi(g) = g^{p^i}$ é possível ver que para todo natural i valem os seguintes itens:

(i) $G^{p^i} = \{g^{p^i} | g \in G\}$;

(ii) $\Omega_i(G) = \{g \in G | g^{p^i} = 1\}$;

(iii) $|G : \Omega_i(G)| = |G^{p^i}|$.

No entanto, sabemos que não apenas os p-grupos abelianos satisfazem essas condições. Em [8], p-grupos satisfazendo esses três itens foram denominados de *power abelian*.

Dado G um grupo e elementos $x, y \in G$. A Fórmula de *Philip Hall* diz que existem elementos $c_i(x, y) \in \gamma_i(\langle x, y\rangle)$ tais que

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

para todo $n \in \mathbb{N}$, como podemos ver no Apêndice A de [4]. Um caso particular dessa fórmula é quando consideramos $n = p$ e isso é equivalente a dizer que $(xy)^p = x^p y^p z c_p$, onde $z \in \gamma_2(\langle x, y\rangle)^p$ e $c_p = c_p(x, y) \in \gamma_p(\langle x, y\rangle)$. Um p-grupo finito é dito ser *regular* quando $c_p(x, y) \in \gamma_2(\langle x, y\rangle)^p$. Os p-grupos regulares são exemplos de grupos que não são necessariamente abelianos mas possuem a estrutura *power abelian*, como podemos ver através do Teorema 2.10 de [5].

Em [20], publicado em 1987, *A. Lobotzky* e *A. Mann* desenvolveram a teoria sobre p-grupos finitos *powerful*. Dizemos que um p-grupo finito é *powerful* se $[G, G] \leqslant G^4$, para $p = 2$, ou $[G, G] \leqslant G^p$, para p ímpar. Eles observaram que a estrutura desses p-grupos é bastante semelhante à dos grupos abelianos. Nesse trabalho, foi provado que G^{p^i} é precisamente o conjunto das p^i-potências de elementos do grupo G. Recentemente, em 2002, *L. Wilson* [23], demonstrou em sua tese de doutorado que quando p é ímpar, $\Omega_i(G)$ é precisamente o conjuntos dos elementos de ordem menor ou igual a p^i. Em 2003, *L.*

Héthelyi e *L. Lévai* [12] provaram que $|\Omega_1(G)| = |G : G^p|$. O que seria o último passo para verificar que p-grupos *powerful* são *power abelian*.

Em [1], *D. Arganbright* mostrou que se G é um p-grupo, com p ímpar, que satisfaz $\gamma_{p-1}(G) \leqslant G^p$, então G^p é o conjunto das p-ésimas potências de G. Isso levou à definição dos p-grupos *potent*, que pode ser vista como uma generalização dos p-grupos *powerful*. Dizemos que um p-grupo finito é *potent* se $[G, G] \leqslant G^4$ para $p = 2$ ou $\gamma_{p-1}(G) \leqslant G^p$, para $p > 2$. Observe que para $p = 2$ e $p = 3$ ser *potent* é o mesmo que ser *powerful*. Em geral, qualquer p-grupo *powerful* é também *potent*. A estrutura dos p-grupos *potent* foi desenvolvida por *J. González-Sánchez* e *A. Jaikin-Zapirain* em [8] e os principais resultados que eles obtiveram estão reunidos no seguinte teorema.

Teorema (A). *Seja G um p-grupo finito potent.*

(*i*) *Se $p = 2$, então:*

  (*a*) *O expoente de $\Omega_i(G)$ é no máximo 2^{i+1} e, mais ainda, $[\Omega_i(G), G]^{2^i} = \Omega_i(G^2)^{2^i} = 1$;*

  (*b*) *A classe de nilpotência de $\Omega_i(G)$ é no máximo $\lfloor (i+2)/2 \rfloor$;*

  (*c*) *Se $N \trianglelefteq G$ e $N \leqslant G^2$ então N é power abelian;*

  (*d*) *Se $N \trianglelefteq G$ e $N \leqslant G^4$ então N é powerful.*

(*ii*) *Se $p > 2$, então:*

  (*a*) *O expoente de $\Omega_i(G)$ é no máximo p^i;*

  (*b*) *A classe de nilpotência de $\Omega_i(G)$ é no máximo $(p-2)i + 1$;*

  (*c*) *Se $N \trianglelefteq G$ então N é power abelian;*

  (*d*) *Se $N \trianglelefteq G$ e $N \leqslant G^p$ então N é powerful.*

Em particular, para p ímpar, vemos que um p-grupo *potent* é *power abelian*.

Seja G um p-grupo finito e $d(G)$ a quantidade mínima de geradores de G. Pelo Teorema da Base de Burnside, Teorema 1.6 de [5], temos que $|G : \Phi(G)| = p^{d(G)}$. Considerando G abeliano isso significa $|G : G^p| = p^{d(G)}$ e assim temos $d(G) = \log_p(|G : G^p|) = \log_p(|\Omega_1(G)|)$. Dessa forma é de se esperar a pergunta se em *powerful* isso ainda seria válido. Nesse sentido *B. Klopsch* e *I. Snopce*, [17], questionaram se, para um p-grupo finito G e p um primo ímpar, $d(G) = \log_p(|\Omega_1(G)|)$ é uma condição necessária e suficiente para o grupo ser *powerful*. Em [10], *J. González-Sánchez* e *A. Zugadi-Reizabal* mostraram que essa questão é verdadeira para $p \geq 5$, através do teorema a seguir, e construíram um contraexemplo para o primo $p = 3$.

Teorema (B). *Sejam $p \geq 5$ e G um p-grupo finito. Então as seguintes condições são equivalentes:*

(*i*) *G é powerful*

(*ii*) $d(G) = \log_p(|\Omega_1(G)|)$.

Como citamos acima em um p-grupo finito G, o número mínimo de geradores coincide com $\log_p(|G : \Phi(G)|) = \log_p(|G : G^p[G,G]|)$, lembrando que em p-grupos finitos $\Phi(G) = G^p[G,G]$. Portanto, podemos reescrever o Teorema (B) dizendo que $|\Omega_1(G)| = |G : G^p[G,G]|$ é uma condição necessária e suficiente para um p-grupo G ser *powerful*. Escrevendo dessa forma, o teorema a seguir se mostra como uma generalização do Teorema (B), o qual também inclui o caso em que $p = 3$.

Teorema (C). *Sejam p um primo ímpar, G um p-grupo finito e seja $k \leq p-2$ e $i \geq 1$ ou $k = p-1$ e $i \geq 2$. Então as seguintes condições são equivalentes:*

(*i*) $\gamma_k(G) \leqslant G^{p^i}$.

(*ii*) $|G : G^{p^i}\gamma_k(G)| = |\Omega_{\{i\}}(G)|$.

O Teorema (B) foi demonstrado em [10] como corolário do teorema anterior quando $k = 2$ e $i = 1$, para $p \geq 5$. Quando $k = p-1$ e $i = 1$ a equivalência do Teorema (C) não é satisfeita, como pode ser visto através do resultado a seguir. Lembre-se que um p-grupo finito G de ordem p^s, para algum $s \in \mathbb{N}$, é dito ser de classe maximal se G possui classe de nilpotência igual a $s-1$.

Teorema (D). *Sejam G um p-grupo, com p um primo ímpar e s um inteiro positivo, com $s \geq p+1$. Então existe um p-grupo finito tal que:*

(*i*) $|G| = p^s$.

(*ii*) *G é de classe maximal.*

(*iii*) $|G : G^p\gamma_{p-1}(G)| = |\Omega_1(G)|$.

(*iv*) $\gamma_{p-1}(G) \nleqslant G^p$.

O teorema anterior mostra, em particular, que para $p = 3$ o Teorema (B) não é válido, pois $\gamma_{p-1}(G) = \gamma_2(G) \nleqslant G$, ou seja, G não seria *powerful*.

Organizamos nosso trabalho em cinco capítulos e neles estaremos considerando que G é um p-grupo finito. No Capítulo 1 trazemos alguns dos pré-requisitos da Teoria de Grupos e de Anéis utilizados durante o desenvolvimento da dissertação. No Capítulo

2 apresentaremos as principais propriedades dos p-grupos regulares, de classe maximal *powerful* e *potent*.

No Capítulo 3 mostraremos a estrutura dos subgrupos normais de um p-grupo finito *potent* e demonstraremos o Teorema (A), que estudamos através do artigo *On the structure of normal subgroups of potent p-groups* de *J. González-Sánchez* e *A. Jaikin-Zapirain*. Esse artigo introduziu o conceito de p-grupo *potent*, e suas propriedades, na teoria dos p-grupos finitos.

No Capítulo 4 provaremos os Teoremas (B) e (C). Por fim, no Capítulo 5 construiremos a família de contraexemplos que demonstram o Teorema (D). Os resultados apresentados nesses últimos dois capítulos são do artigo *A characterization of powerful p-groups* de *J. González-Sánchez* e *A. Zugadi-Reizabal*. Esse artigo é muito interessante pois nele todas as famílias de p-grupos finitos definidas no Capítulo 2 são utilizadas e relacionadas.

Cabe ressaltar que a numeração utilizada para os teoremas nesta introdução é diferente da apresentada a eles ao longo da dissertação. Além do fato de que alguns deles estão divididos em dois ou mais teoremas.

Capítulo 1

Preliminares

Neste capítulo apresentaremos conceitos básicos e alguns resultados de Teoria de Grupos e Módulos que usaremos no nosso trabalho. Omitiremos as demonstrações dos resultados aqui apresentados, mas todos elas podem ser encontradas nas referências citadas.

1.1 Teoria de Grupos

O estudo sobre a Teoria de Grupos feita para este trabalho foi baseado principalmente nos livros *Finite Groups* [11], *Algebra-A Graduate Course* [15], *Analytic Pro-p Groups* [4], e no artigo [5]. Nosso estudo é bastante sucinto, por isso assumiremos como conhecidos muitos resultados, como por exemplo os Teoremas do Isomorfismo e o da Correspondência, dentre outros.

Dado um grupo G, denotaremos $o(g)$ pela ordem do elemento $g \in G$, $|G|$, como sendo a ordem do grupo G, $|G : H|$, o índice do subgrupo H no grupo G e $Z(G)$ o centro desse grupo. Demais notações serão definidas no seu devido tempo.

1.1.1 Comutadores e subgrupos gerados por comutadores

Seja G um grupo. O comutador de dois elementos x e y é definido por $[x, y] = x^{-1}y^{-1}xy$. Com isso temos que x e y comutam se, e somente se, $[x, y] = 1$.

Podemos definir comutador de qualquer comprimento natural da seguinte forma

$$[x_1, \dots, x_n] = [[x_1, \dots, x_{n-1}], x_n],$$

onde por convenção definimos $[x] = x$.

Teorema 1.1.1 ([5], Teorema 1.7)**.** *Seja G um grupo e considere x, y e z elementos de G. Então valem as seguintes propriedades de comutadores:*

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

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

(*iii*) $[xy, z] = [x, z]^{y}[y, z] = [x, z][x, z, y][y, z]$.

(*iv*) $[x, yz] = [x, z][x, y]^{z} = [x, z][x, y][x, y, z]$.

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

(*vi*) $yx = xy[y, x]$.

Teorema 1.1.2 ([4], Página 1 e 2)**.** *Seja G um grupo e x, y elementos de G. Para todo inteiro positivo n vale que:*

(*i*) $[x^{n}, y] = [x, y]^{x^{n-1}}[x, y]^{x^{n-2}} \cdots [x, y]^{x}[x, y]$.

(*ii*) $[x, y^{n}] = [x, y][x, y]^{y} \cdots [x, y]^{y^{n-1}}$.

Sejam H e K subgrupos de um grupo G. Também podemos definir o subgrupo comutador de H e K por $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$. De maneira análoga, definimos o subgrupo comutador de qualquer comprimento natural da seguinte forma $[H_1, \ldots, H_n] = [[H_1, \ldots, H_{n-1}], H_n]$, onde $H_1, \ldots, H_n$ são subgrupos de G.

Teorema 1.1.3 ([5], Teorema 1.7)**.** *Sejam G um grupo e H, K e L subgrupos G. Então:*

(*i*) $[H, K] = [K, H]$.

(*ii*) $H \leqslant N_G(K)$ *se, e somente se,* $[H, K] \leqslant K$.

(*iii*) $H \leqslant C_G(K)$ *se, e somente se,* $[H, K] = 1$.

(*iv*) $[H, K]^{\sigma} = [H^{\sigma}, K^{\sigma}]$, *para qualquer endomorfismo $\sigma : G \to G$. Em particular, o subgrupo comutador de dois subgrupos característicos (normais) de G é ainda é um subgrupo característico (normal).*

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

(*vi*) *Se H, K e L são subgrupos normais de G, então* $[HK, L] = [H, L][K, L]$.

O próximo resultado é muito útil quando se trata do subgrupo comutador. Pois, dado um grupo G e quatro subgrupos dele, sendo um deles normal, o lema nos mostra uma relação de pertinência entre o subgrupo comutador desses subgrupos e o normal. Esse resultado é conhecido como Lema dos Três Subgrupos.

Lema 1.1.4 ([5], Teorema 1.8)**.** ***(Lema dos Três Subgrupos)****Seja G um grupo, H, J e K subgrupos de G e N um subgrupo normal de G tal que $[H, J, K], [K, H, J] \leqslant N$. Então $[J, K, H] \leqslant N$.*

Em nosso trabalho também usaremos um caso particular desse teorema, onde se considerarmos $H = L$ e $J = N = K$, com L e N subgrupos normais, então $[N, N, L] \leqslant [L, N, N]$.

Usando a definição de comutadores, podemos definir uma sequência de subgrupos de um grupo G, denominada *série central inferior* de G, da seguinte forma:

$$\gamma_1(G) = G, \quad \gamma_2(G) = [G, G] = G', \quad \gamma_n(G) = [\gamma_{n-1}(G), G] \text{ para } n > 2.$$

Do modo como essa série é definida, facilmente podemos verificar que cada termo dela é característico em G. Além disso, ela satisfaz $\gamma_{i+1}(G) \leqslant \gamma_i(G)$, e isso acarreta que a série é central em G, ou seja, $\gamma_i(G)/\gamma_{i+1}(G) \leqslant Z(G/\gamma_{i+1}(G))$.

Os próximos dois teoremas são aplicações do Lema dos Três Subgrupos, onde o primeiro nos mostra uma relação muito útil da série central inferior.

Teorema 1.1.5 ([5], Teorema 1.9)**.** *Para qualquer grupo G, $[\gamma_i(G), \gamma_j(G)] \leqslant \gamma_{i+j}(G)$, para todo $i, j \geq 1$.*

Teorema 1.1.6 ([16], Lema 4.9)**.** *Seja G um grupo e N um subgrupo normal de G. Então $[\gamma_k(N), G] \leqslant [N, \gamma_k(G)]$, para todo $k \geq 1$.*

Outra propriedade da série central inferior, proveniente do Teorema 1.1.3, item (v), é o nosso próximo resultado, que de certa forma nos mostra como deve ser essa série no grupo quociente G/N, onde $N \trianglelefteq G$.

Teorema 1.1.7. *Sejam G um grupo e N um subgrupo normal de G. Então $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $i \geq 1$.*

1.1.2 Grupos nilpotentes

Dado G um grupo, dizemos que ele é nilpotente se existe $c \in \mathbb{N}$ tal que $\gamma_{c+1}(G) = 1$. O menor c que satisfaz essa condição é dito ser a classe de nilpotência de G. Observe que quando $c = 1$, temos $\gamma_2(G) = 1$ e isso significa que G é abeliano. Dessa forma os grupos nilpotentes de classe um são precisamente os abelianos.

A caracterização para um grupo G ser nilpotente também pode ser feita em termos de outra série, denominada *série central superior* de G. Recursivamente, ela é definida da forma $Z_0(G) = 1$, $Z_1(G) = Z(G)$ e, para $i > 1$, $Z_i(G)$ é a imagem inversa em G de $Z(G/Z_{i-1}(G))$, ou seja, satisfaz $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. O próximo teorema relaciona essa série com a central inferior e também justifica um pouco o fato delas serem chamadas inferior e a outra superior.

Teorema 1.1.8 ([5], Lema 1.12)**.** *Seja G um grupo nilpotente de classe c. Então $\gamma_{c+1-i}(G) \leqslant Z_i(G)$, para todo $0 \leq i \leq c$.*

Usando o resultado acima podemos caracterizar grupos nilpotentes considerando a série central superior, como veremos no teorema a seguir. Ele também nos mostra que a classe de nilpotência definida anteriormente é o comprimento de ambas as séries centrais, superior e inferior.

Teorema 1.1.9 ([5], Teorema 1.13)**.** *Um grupo G é nilpoente de classe c se, e somente se, $Z_c(G) = G$ e $Z_{c-1}(G) \neq G$.*

Grupos finitos nilpotentes também podem ser caracterizados através dos seus subgrupos de Sylow, sem depender de nenhuma série, como nos diz o próximo teorema.

Teorema 1.1.10 ([11], Teorema 3.5)**.** *Um grupo G é nilpotente se, e somente se, ele é produto direto de seus subgrupos de Sylow.*

1.1.3 O subgrupo de Frattini

Um subgrupo importante, que ainda é característico, em um grupo G é o denominado subgrupo de Frattini. Ele é denotado por $\Phi(G)$ e definido como sendo a interseção de todos os subgrupos maximais do G. Caso G, não possua nenhum maximal, definimos $\Phi(G) = G$.

Definição 1.1.11. *Sejam G um grupo e g um elemento de G. Dizemos que g é um não-gerador se quando $\langle X \cup g\rangle = G$, então temos que $\langle X\rangle = G$, para qualquer subconjunto $X \subseteq G$.*

Com essa definição de elementos não geradores em um grupo finito, pode-se mostrar que a definição de subgrupo de Frattini coincide com o conjunto dos elementos não-geradores de G.

Teorema 1.1.12 ([5], Teorema 1.5)**.** *Seja G um grupo finito e $x_1, \dots, x_n \in G$. Então temos que $G = \langle x_1, \dots, x_n\rangle$ se, e somente se, $G/\Phi(G) = \langle x_1\Phi(G), \dots, x_n\Phi(G)\rangle$.*

1.1.4 Fórmula de Compilação de Hall

Em qualquer grupo abeliano sabemos que vale $x^ny^n = (xy)^n$, mas isso não é válido em geral. A *Fórmula de Compilação de Philip Hall*, também conhecida por *Fórmula de Hall-Petrescu*, nos fornece um substituto para esse fato válido em qualquer grupo.

Sejam G um grupo, x, y elementos de G, e n um inteiro positivo. Então $(xy)^n$ e x^ny^n são iguais módulo G', dessa forma podemos escrever $x^ny^n = (xy)^nc$, para algum $c \in G'$. A fórmula de compilação estabelece uma expressão para c como um produto de comutadores.

Teorema 1.1.13 ([4], Apêndice A)**.** *Sejam x e y elementos de um grupo e n um inteiro positivo. Então*

$$x^ny^n = (xy)^nc_2^{\binom{n}{2}}\dots c_i^{\binom{n}{i}}\dots c_{n-1}^nc_n$$

onde $c_i \in \gamma_i(G)$ para cada i.

Podemos construir cada c_i igual a um produto de comutadores em x e y de comprimento pelo menos i. Dessa forma, a fórmula pode ser interpretada como uma identidade onde se considera $c_i = c_i(x, y) \in \gamma_i(\langle x, y\rangle)$, para cada i.

Um caso particular dessa fórmula é quando tomamos $n = p^k$ para algum inteiro positivo k. Como o coeficiente binomial $\binom{p^k}{i}$ é divisível por p^{k-j} para $p^j \leq i < p^{j+1}$, temos a seguinte reformulação.

Teorema 1.1.14 ([4], Lema 11.9)**.** *Seja G um grupo e x, y elementos de G. Então para todo $k \geq 0$ temos*

$$(xy)^{p^k} \equiv x^{p^k}y^{p^k}(\ mod\ \gamma_2(L)^{p^k}\gamma_p(L)^{p^{k-1}}\gamma_{p^2}(L)^{p^{k-2}}\gamma_{p^3}(L)^{p^{k-3}}\cdots\gamma_{p^k}(L)),$$

onde $L = \langle x, y\rangle$. Também temos que

$$[x, y]^{p^k} \equiv [x^{p^k}, y](\ mod\ \gamma_2(M)^{p^k}\gamma_p(M)^{p^{k-1}}\gamma_{p^2}(M)^{p^{k-2}}\dots\gamma_{p^k}(M)),$$

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

Um corolário simples da primeira parte desse teorema é quando tomamos uma quantidade finita de elementos do grupo G.

Corolário 1.1.15. *Seja G um grupo e $x_1, \dots, x_r$ elementos de G. Então*

$$(x_1\dots x_r)^{p^k} \equiv x_1^{p^k}\dots x_r^{p^k}(mod\ \gamma_2(L)^{p^k}\gamma_p(L)^{p^{k-1}}\gamma_{p^2}(L)^{p^{k-2}}\gamma_{p^3}(L)^{p^{k-3}}\dots\gamma_{p^k}(L)),$$

onde $L = \langle x_1, \dots, x_r\rangle$.

1.2 Anéis e Módulos

Nesta seção falaremos de alguns aspectos básicos da Teoria de Anéis e Módulos que podem ser encontrados em [7].

Definição 1.2.1. *Seja R um conjunto munido de duas operações: adição e multiplicação, denotadas usualmente por $'+'$ e pela justaposição, respectivamente. Dizemos que R é um anel se dados $r, s, t \in R$ as seguintes propriedades são satisfeitas:*

- *$(R, +)$ é um grupo abelino,*
- *$(rs)t = r(st)$,*
- *$r(s + t) = rs + rt$,*
- *$(s + t)r = sr + tr$.*

Se R possuir um elemento u que satisfaz $ur = r = ru$, para todo $r \in R$, esse elemento u é usualmente denotado por 1 e denominado unidade. Nesse caso, dizemos que R é um anel com unidade. Se além das quatro propriedades da definição acima, a operação de multiplicação for comutativa, então dizemos R é um anel comutativo.

Definição 1.2.2. *Seja M um grupo abeliano aditivo e R um anel. Suponha que para cada $m \in M$ e $r \in R$, seja definido um elemento de M, denotado por mr. Então M é um R-módulo à direita se para quaisquer $x, y \in M$ e $r, s \in R$ as seguintes condições valem:*

- *$(x + y)r = xr + yr$,*
- *$x(r + s) = xr + xs$,*
- *$x(rs) = (xr)s$,*
- *$x1 = x$.*

Também podemos definir um R-módulo à esquerda, onde existe um elemento de M que agora é denotado por rm e satisfaz propriedades análogas às citadas na definição de um R-módulo à direita.

Definição 1.2.3. *Um R-submódulo N de um R-módulo M é um subconjunto fechado para todas as operações de módulo, ou seja, N é um subgrupo aditivo de M e $nr \in N$, para todo $n \in N, r \in R$.*

Seja M um R-módulo, sejam $t \in \mathbb{N}$ e $m_1, \ldots, m_t$ elementos de M. Consideramos o seguinte subconjunto N de M:

$$N = m_1R + \cdots + m_tR = \{m_1r_1 + \cdots + m_tr_t \mid r_i \in R\}.$$

O conjunto N é um submódulo de M e é denominado submódulo gerado por $m_1, \ldots, m_t$. Dizemos que M é finitamente gerado se existe um número finito de elementos $m_1, \ldots, m_t$ de M tais que

$$M = m_1R + \cdots + m_tR.$$

Neste caso dizemos que $m_1, \ldots, m_t$ é um conjunto de geradores para o módulo M.

Um R-módulo que será utilizado posteriormente nesse trabalho será denotado por R^t, onde $t \in \mathbb{N}$. Definimos $R^t = \{(r_1, \ldots, r_t) \mid r_i \in R\}$ com a operação de adição coordenada a coordenada e a multiplicação por um elemento do anel atua em cada coordenada, ou seja, da seguinte forma

$$(r_1, \ldots, r_t) + (r'_1, \ldots, r'_t) := (r_1 + r'_1, \ldots, r_t + r'_t)$$

e

$$r(r_1, \ldots, r_t) := (rr_1, \ldots, rr_t).$$

O conjunto R^t é um R-módulo gerado pelos elementos $e_1, \ldots, e_t$, onde cada $e_i = (0, \ldots, 1_i, \ldots, 0)$ com $i \in \{1, \ldots, t\}$. Ou seja, R^t é um R-módulo finitamente gerado.

Definição 1.2.4. *Sejam R um anel e M um R-módulo. Seja N um R-submódulo de M. Então, em particular, $(N, +)$ é um subgrupo do grupo $(M, +)$ e podemos considerar o grupo quociente $(M/N, +_N)$, isto é, o conjunto $\{m + N \mid m \in M\}$ das classes laterais de N em M munido da adição*

$$\begin{aligned} +_N : M/N \times M/N &\longrightarrow M/N \\ (m_1 + N, m_2 + N) &\longmapsto (m_1 + m_2) + N. \end{aligned}$$

Sobre este grupo $(M/N, +_N)$, podemos considerar a seguinte multiplicação por escalar em R

$$\begin{aligned} R \times M/N &\longrightarrow M/N \\ (r, m + N) &\longmapsto mr + N. \end{aligned}$$

Essa operação está bem-definida e M/N é um R-módulo, denominado R-módulo quo-

ciente de M por N.

Definição 1.2.5. *Seja M um R-módulo. Dizemos que os elementos $m_1, \ldots, m_t$ de M são R-linearmente independentes quando, dados $r_i \in R$,para todo i vale*

$$\sum_{i=1}^{t} r_i m_i = 0 \Rightarrow r_i = 0.$$

Um R-módulo finitamente gerado M é dito ser livre se ele admite um conjunto finito de geradores $m_1, \ldots, m_t$ que são R-linearmente independentes, ou equivalentemente, se o módulo M é isomorfo a R^t.

Essa equivalência pode ser vista considerando-se o homomorfismo

$$\begin{aligned} \varphi : R^t &\longrightarrow M \\ (r_1, \ldots, r_t) &\longmapsto \sum_{i=1}^{t} m_i r_i. \end{aligned}$$

Neste caso dizemos que $\{m_1, \ldots, m_t\}$ é uma base para o módulo livre M. Observe ainda que $M = m_1 R \oplus \cdots \oplus m_t R$.

Teorema 1.2.6. *Sejam R um anel com unidade e M um R-módulo livre finitamente gerado. Então, todas as bases de M possuem o mesmo número de elementos.*

Com esse teorema podemos dizer que a quantidade de geradores de um R-módulo livre finitamente gerado está bem-definida, o que é normalmente denominado posto de M e denotaremos por $d_R(M)$.

A próxima e última definição dessa seção foi retirado do livro *The Structure of Groups of Prime Power Order*, [19, Capítulo 4, Página 93]. Ela será utilizada no Capítulo 5, para a construção de uma família de p-grupos finitos.

Definição 1.2.7. *Seja Λ um domínio de ideais principais. Uma Λ-lattice L é um módulo livre finitamente gerado sobre Λ.*

Capítulo

2

Algumas famílias de p-grupos finitos

Um grupo G no qual todo elemento tem como ordem uma potência de um certo primo p é dito ser um p-grupo. Quando se trata de um grupo finito G, essa definição significa que $|G| = p^n$, para algum $n \in \mathbb{N}$.

No capítulo anterior vimos algumas propriedades para grupos quaisquer, agora aprofundaremos nosso estudo em p-grupos finitos. Com esse intuito, primeiro faremos um estudo preliminar sobre suas propriedades e alguns de seus subgrupos, muito utilizados em nosso trabalho. Em seguida mostraremos algumas de suas famílias, bem como as principais características de cada uma.

A partir daqui, em alguns momentos omitiremos a especificação do p-grupo ser finito, mas tenha em mente que estamos considerando isso.

2.1 Propriedades gerais

No capítulo anterior definimos um grupo nilpotente. Uma característica, muito importante de um p-grupo finito é que eles são nilpotentes. Além disso, vale o teorema a seguir, que nos mostra, dentre outras coisas, uma limitação para a sua classe de nilpotência.

Teorema 2.1.1 ([5], Teorema 1.15). *Seja G um p-grupo finito de ordem $p^m \geq p^2$. Então:*

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

(ii) Se G tem classe de nilpotência c, então $|G : Z_{c-1}(G)| \geq p^2$.

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

Como corolário desse teorema, temos:

Corolário 2.1.2 ([5], Corolário 1.16)**.** *Sejam G um p-grupo finito e N um subgrupo normal de G com índice $p^i \geq p^2$. Então $\gamma_i(G) \leqslant N$.*

Em um p-grupo finito o subgrupo de Frattini, definido na Seção 1 do Capítulo 1, possui uma caracterização muito útil dentro dessa teoria, dada pelo seguinte teorema.

Teorema 2.1.3 ([5], Teorema 2.2)**.** *Seja G um p-grupo finito. Então $\Phi(G) = G^p[G,G]$.*

Outra informação muito importante que o subgrupo de Frattini nos mostra, quando se trata de p-grupos finitos, é sobre a quantidade mínima de geradores do grupo. Como veremos no próximo teorema, conhecido como Teorema da Base de Burnside. Denotamos $d(G)$ como sendo o número mínimo de geradores do grupo G e $\mathbb{F}_p$ como sendo um corpo finito com p elementos.

Teorema 2.1.4 ([5], Teorema 1.6)**.** *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 $\mathbb{F}_p$.*

(ii) *O conjunto $\{x_1, \ldots, x_d\}$ é um conjunto mínimo de geradores para G se, e somente se, $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ é uma base para $G/\Phi(G)$.*

(iii) *O número mínimo $d = d(G)$ de geradores do grupo G coincide com a dimensão de $G/\Phi(G)$ como um $\mathbb{F}_p-$espaço vetorial. Em outras palavras, $|G : \Phi(G)| = p^d$.*

Definimos o *expoente de um grupo G*, denotado por $exp(G)$, como sendo o mínimo múltiplo comum entre as ordens de seus elementos. Quando esse grupo é um p-grupo, o expoente será a maior ordem dos elementos de G. Isso significa que se G é um p-grupo finito, então $exp(G) = p^n$, para algum natural n.

Definição 2.1.5. *Seja G um p-grupo finito. Para qualquer $i \geq 0$ definimos*

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

e

$$G^{p^i} = \langle x^{p^i} | x \in G \rangle.$$

Esses subgrupos são característicos em G. Pela definição de expoente, se $exp(G) = p^n$, então $x^{p^n} = 1$ para todo elemento x de G. Assim temos que $\Omega_n(G) = G$. Com isso, temos a seguinte série ascendente, denominada Ω-série de G

$$1 = \Omega_0(G) \leqslant \Omega_1(G) \leqslant \cdots \leqslant \Omega_{n-1}(G) \leqslant \Omega_n(G) = G.$$

Observe também que $G^{p^n} = \langle x^{p^n} \mid x \in G \rangle = 1$ e assim temos a série descendente, denominada G-série

$$G = G^{p^0} \geqslant G^{p^1} \geqslant \cdots \geqslant G^{p^{n-1}} \geqslant G^{p^n} = 1.$$

Como o subgrupo de Frattini é estrito temos que $G^{p^{i+1}} \leqslant (G^{p^i})^p \leqslant \Phi(G^{p^i}) < G^{p^i}$. Com isso a G-série de um p-grupo é estritamente decrescente. Então a G-série de um p-grupo de expoente p^n tem exatamente n passos.

Também definimos os seguintes subconjuntos:

Definição 2.1.6. *Seja G um p-grupo finito. Para qualquer $i \geq 0$ definimos*

$$\Omega_{\{i\}}(G) = \{x \in G \mid x^{p^i} = 1\}$$

e

$$G^{\{p^i\}} = \{g^{p^i} \mid g \in G\}.$$

Quando o grupo é abeliano, claramente, esses subconjuntos coincidem com os subgrupos definidos em 2.1.5, mas não apenas neles. O teorema a seguir nos mostra a igualdade desses subgrupos e uma relação do índice de $\Omega_i(G)$ em G e a ordem de G^{p^i}, onde G é um p-grupo abeliano.

Tentaremos deixar explícito, em cada caso, se estamos tratando deles como gerado ou como conjunto. No caso de coincidirem usaremos a notação da primeira definição.

Teorema 2.1.7 ([5], Teorema 2.3). *Seja G um p-grupo abeliano. Para qualquer $i \geq 0$ temos que:*

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

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

(iii) $|G : \Omega_i(G)| = |G^{p^i}|$ *(e consequentemente também* $|G : G^{p^i}| = |\Omega_i(G)|$*).*

Observe que o teorema anterior nos diz que se G é abeliano, então as três propriedades são satisfeitas. Mas, se elas são satisfeitas não podemos afirmar que G é abeliano. Quando um grupo satisfaz essas três propriedades, para todo i, um dos artigos trabalhados,[8], o denomina *power abelian*.

Ao longo do nosso trabalho veremos casos nos quais pediremos outras características, ao invés de abeliano, de modo que esse teorema ainda seja satisfeito.

O próximo teorema que veremos nos foi muito útil em várias demonstrações onde queríamos verificar a inclusão de certos subgrupos.

Teorema 2.1.8. *Sejam G um p-grupo finito e N, M subgrupos normais de G. Se $N \leqslant M[N,G]N^p$, então $N \leqslant M$.*

Demonstração. Considere M e N subgrupos normais de um p-grupo finito G. Vamos considerar que $M = 1$, então precisamos mostrar que $N = 1$.

Suponha por absurdo que $N \neq 1$. Como estamos em um p-grupo, existe um subgrupo normal K de G tal que $|N : K| = p$. Temos que $K, N \trianglelefteq G$ e $K < N$, então fazendo quociente por K, temos que $N/K \trianglelefteq G/K$.

Agora, como G/K é um p-grupo e $|N : K| = p$, então $N/K \cap Z(G/N) \neq 1$, e isso acarreta que $N/K \leqslant Z(G/N)$. Voltando para G, temos que $[N,G] \leqslant K$.

Também temos que $N^p \leqslant K$. De fato, como $|N/K| = p$, então todo elemento de N/K tem ordem p e, assim, $(nK)^p = n^pK = K$. Mas, $n^pK = K$ se, e somente se, $n^p \in K$. Logo, $N^p \leqslant K$.

Dessa forma, temos que $N^p \leqslant K$ e $[N,G] \leqslant K$, então $N^p[N,G] \leqslant K$. Mas isso é um absurdo, pois por hipótese $N \leqslant [N,G]N^p$ e $K < N$. Portanto, $N = 1$. □

No capítulo anterior vimos a Fórmula de Compilação de Hall. Agora veremos mais algumas consequências dessa fórmula utilizadas em nosso trabalho. A primeira é uma consequência do Corolário 1.1.15 e ela nos permite estabelecer uma relação de pertinência entre os termos da Ω-série do grupo com os elementos da série central inferior aplicadas nesses termos.

Corolário 2.1.9. *Seja G um p-grupo finito. Então temos que*

$$\Omega_i^{p^n}(G) \leqslant \Omega_{i-n}(G)\gamma_2(\Omega_i)^{p^n}\gamma_p(\Omega_i)^{p^{n-1}}\gamma_{p^2}(\Omega_i)^{p^{n-2}}\gamma_{p^3}(\Omega_i)^{p^{n-3}}\ldots\gamma_{p^n}(\Omega_i)$$

onde $\Omega_l = \Omega_l(G)$ para $l \leq 1$ e $\Omega_l = 1$ para $l \leq 0$.

Lembre-se que definimos subgrupo comutador de qualquer comprimento. Considerando N e H subgrupos de G vamos adotar a seguinte notação $[H,_k N]$ para o comutador $[H, N, \ldots, N]$, onde N aparece k vezes.

A outra consequência que ocorre no desenvolvimento da teoria em torno dessa fórmula, muito utilizada em nosso trabalho, é o seguinte teorema.

Teorema 2.1.10. *Sejam G um p-grupo finito e N, M subgrupos normais de G. Então, para um natural k,*

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

Demonstração. Considere $n \in N$ e $m \in M$, pelo Teorema 1.1.14, temos

$$[n^{p^k}, m] \equiv [n,m]^{p^k} (\mod \gamma_2(L)^{p^k}\gamma_p(L)^{p^{k-1}}\gamma_{p^2}(L)^{p^{k-2}}\dots\gamma_{p^k}(L)),$$

onde $L = \langle n, [n,m]\rangle$. Observe que $\gamma_2(L) = \langle [l_1, l_2] \mid l_1, l_2 \in L\rangle \leqslant [M,N,N]$. Dessa forma, temos a seguinte inclusão

$$\gamma_2(L)^{p^k} \leqslant ([M,N,N])^{p^k} \leqslant [M,N]^{p^k}$$

e, assim, $\gamma_{p^i}(L)^{p^{k-i}} = [\gamma_2(L),_{p^i-2}(L)]^{p^{k-i}} \leqslant [M,N,N,_{p^i-2}N]^{p^{k-i}} = [M,_{p^i}N]^{p^{k-i}}$, para os demais termos, com $i = 1,\dots,k$.

Com isso, por um lado, temos que

$$[n^{p^k}, m] \in [n,m]^{p^k}[N,M]^{p^k}\prod_{i=1}^{k}[M,_{p^i}N]^{p^{k-i}}.$$

Tomando todos os valores de M e N segue que

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

Por outro lado,

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

Vamos mostrar a outra inclusão por indução sobre a ordem de N. Se $|N| = 1$, então a inclusão é claramente válida. Para o passo de indução, lembre que $[N,M] \leqslant [N,G] < N$, então podemos aplicar a hipótese de indução em $[M,N]$ e isso acarreta

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

Consequentemente,

$$[N,M]^{p^k} \leqslant [N^{p^k}, M][M,N,N]^{p^k}\prod_{i=1}^{k}[M,_{p^i}N]^{p^{k-i}} \leqslant [N^{p^k}, M][[M,N]^{p^k},N]\prod_{i=1}^{k}[M,_{p^i}N]^{p^{k-i}}$$

$$[N,M]^{p^k} \leqslant [N^{p^k}, M][[N,M]^{p^k},G]\prod_{i=1}^{k}[M,_{p^i}N]^{p^{k-i}}.$$

Pelo Teorema 2.1.8, vale a inclusão desejada. Portanto, vale a congruência

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

$\square$

2.2 p-grupos regulares

A primeira família de p-grupos finitos que estudaremos será a dos p-grupos regulares, que foi fundamentalmente desenvolvida por P. Hall [13] e publicada em 1933. Essa teoria também pode ser encontrada no livro *Endliche Gruppen I* [14, Capítulo III].

Os aspectos dessa família que mostraremos nesse trabalho foram essencialmente estudadas através dos artigos [5] e [2]. Nesse segundo, é desenvolvida uma generalização da definição de regular.

A Fórmula de Compilação de Hall possui um significado especial quando usamos um primo p no expoente, já que os coeficientes binomiais $\binom{p}{i}$ são divisíveis por p para $1 \leq i \leq p-1$. Consequentemente, podemos escrever $x^p y^p = (xy)^p z c_p$ para algum elemento $z \in \gamma_2(\langle x, y\rangle)^p$ e $c_p = c_p(x,y) \in \gamma_p(\langle x, y\rangle)$. E isso sugere a definição de um grupo ser regular, que é a seguinte.

Definição 2.2.1. *Seja G um p-grupo finito. Dizemos que G é regular se, para todos $x, y \in G$,*

$$x^p y^p \equiv (xy)^p (mod\ \gamma_2(\langle x, y\rangle)^p).$$

Equivalentemente, se $c_p(x,y) \in \gamma_2(\langle x, y\rangle)^p$ para todos $x, y \in G$.

A condição dessa definição é local, ou seja, depende de cada par de elementos tomados em G. Com isso, se um p-grupo é regular, então seus subgrupos e grupos quocientes por um subgrupo normal são ainda regulares.

Claramente todos os p-grupos abelianos ou os que possuem expoente p são regulares. O problema dessa definição é que se precisarmos construir um p-grupo regular devemos checar a relação para todo par de elementos, o que em alguns casos pode ser um trabalho árduo de cálculo. O teorema a seguir nos mostra alguns casos em que podemos verificar outras propriedades, que podem ser mais simples, para concluir se o grupo é regular.

Teorema 2.2.2. *Seja G um p-grupo finito.*

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

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

(*iii*) *Um 2-grupo regular é abeliano.*

Demonstração. (*i*) Suponha que G tenha classe de nilpotência menor do que p. Então, pela definição da série central inferior, temos que $\gamma_p(G) = 1$ e, assim, $\gamma_p(\langle x, y\rangle) = 1$. Agora, pela Fórmula de Compilação de Hall, lembre que

$$(xy)^p \equiv x^p y^p (\text{mod } \gamma_2(\langle x, y\rangle)^p \gamma_p(\langle x, y\rangle)).$$

Então, $(xy)^p \equiv x^p y^p (\text{mod } \gamma_2(\langle x, y\rangle)^p)$, ou seja, G é regular.

Para a parte particular, observe que se G é um p-grupo de ordem menor ou igual a p^p, então temos que a classe de nilpotência de G é menor do que p, pois cada termo da série central inferior deve ser um p-grupo de ordem pelo menos p até chegar na identidade, e acabamos de ver que isso acarreta em G ser regular.

(*ii*) Suponha que $\gamma_{p-1}(G)$ seja cíclico. Se $p = 2$, então temos que $\gamma_1(G) = G$ é cíclico. E assim G é abeliano, mas nesse caso o resultado é trivialmente satisfeito.

Agora se $p > 2$, considere $x, y \in G$, arbitrários e seja $H = \langle x, y\rangle$. Temos que $\gamma_{p-1}(H) \leqslant \gamma_{p-1}(G)$, logo $\gamma_{p-1}(H)$ também é cíclico. Se $\gamma_{p-1}(H) \neq 1$, então temos que $\gamma_p(H) < \gamma_{p-1}(H)$, pela definição da série central inferior. Consequentemente, $\gamma_p(H) \leqslant \gamma_{p-1}(H)^p \leqslant \gamma_2(H)^p$. E neste caso $c_p(x, y) \in \gamma_2(H)^p$, ou seja, G é regular.

Por outro lado, se $\gamma_{p-1}(H) = 1$, então $c_p(x, y) \in \gamma_p(H) \leqslant \gamma_{p-1}(H) = 1$. E assim, também nesse caso, G é regular.

Agora, suponha que $p > 2$ e G' seja cíclico. Observe que se G' é cíclico, então $\gamma_{p-1}(G)$ também o é, pois $\gamma_{p-1}(G) \leqslant G'$. E, pelo que acabamos de ver, G é regular.

(*iii*) Suponha que G seja um 2-grupo regular e vamos mostrar que G é abeliano. Sejam $x, y \in G$ e escreva $H = \langle x, y\rangle$. Temos que $(xy)^2 = x^2y^2[y, x]^y$, donde $x^2y^2 = (xy)^2[x, y]^y$.

Por hipótese, G é regular. Assim $[x, y]^y \in \gamma_2(H)^2$. Observe que $\gamma_2(H)^2 \trianglelefteq H$, pois dados $\alpha = \alpha_1^2 \cdots \alpha_k^2 \in \gamma_2(H)^2$, onde $\alpha_i \in \gamma_2(H)$, $i = 1, \ldots, k$, e $g \in H$, temos que $\alpha^g = (\alpha_1^2 \cdots \alpha_k^2)^g = (\alpha_1^2)^g \cdots (\alpha_k^2)^g = (\alpha_1^g)^2 \cdots (\alpha_k^g)^2$ e, como $\gamma_2(H) \trianglelefteq H$, segue que $(\alpha_1^g)^2 \cdots (\alpha_k^g)^2 \in \gamma_2(H)^2$. Com isso $[x, y] \in \gamma_2(H)^2$. O que mostra que $H/\gamma_2(H)^2$ é abeliano e consequentemente $H' \leqslant (H')^2$.

Agora lembre que $\Phi(H') = (H')^2[H', H']$, donde $H' \leqslant \Phi(H')$. Mas isso ocorre apenas quando $H' = 1$, já que a outra inclusão é sempre verdadeira e estamos com H' finito. Dessa forma, dois quaisquer elementos de H comutam, consequentemente os de G. Portanto, G é abeliano.

□

Como comentado inicialmente, também estamos interessados numa generalização desse conceito, que denominamos k-regular e definimos da seguinte maneira:

Definição 2.2.3. *Seja G um p-grupo finito. Dizemos que G é k-regular se para todos $x, y \in G$ vale*

$$(xy)^{p^k} = x^{p^k} y^{p^k} \prod_i D_i^{p^k},$$

com D_i subgrupos adequados de $\gamma_2(\langle x, y\rangle)$ e $k \in \mathbb{N}$, $k > 0$.

Observe que quando $k = 1$ essas definições coincidem. A propriedade de ser k-regular também é estendida para seus subgrupos, assim como em regulares. Vamos verificar algumas propriedades para grupos k-regulares, que são muito conhecidas dentro da teoria de regulares.

Lema 2.2.4. *Seja G um p-grupo k-regular. Então*

(i) Se $x^{p^k} = y^{p^k} = e$, então $(xy)^{p^k} = e$.

(ii) Para todos $x, y \in G$, $x^{p^k} y^{p^k} = z^{p^k}$, para um certo $z \in G$ (que depende de x e y).

Demonstração. Vamos provar os dois itens por indução sobre a ordem de G. Para $|G| = 1$, em ambos os itens o resultado é trivialmente satisfeito. Então resta ver o passo de indução em cada item, podemos supor sem perda de generalidades que $G = \langle x, y\rangle$.

(i) Suponha que $x^{p^k} = y^{p^k} = e$. Considere $L = \langle x^g \mid g \in G\rangle$. Lembre que a regularidade se estende a subgrupos, então L é k-regular. Também temos que $|L| < |G|$, pois $y \notin L$. Aplicando a hipótese de indução em L, temos que todos os seus elementos têm ordem no máximo p^k. Observe que $[x, y] = x^{-1}x^y \in L$, pois $x, x^{-1}, x^y \in L$ e L é um subgrupo. Assim $[x, y]^{p^k} = e$.

Consideraremos que G não é abeliano, pois se fosse o teorema seria trivialmente satisfeito. Então $G' < G$, onde $G' = \langle [x, y]^g \mid g \in G\rangle$. Assim também podemos aplicar a hipótese de indução em G', logo $z^{p^k} = e$, para todo $z \in G'$, e com isso $exp(G') \leq p^k$.

Por hipótese, G é k-regular e $x^{p^k} = y^{p^k} = e$. Então, pela definição, $(xy)^{p^k} = x^{p^k} y^{p^k} \prod D_i^{p^k}$, com $D_i \leqslant G'$ para cada i. Logo, $D_i^{p^k} \leqslant (G')^{p^k} = e$, e assim $(xy)^{p^k} = e$, como queríamos.

(ii) Consideremos $L = \langle xy, G'\rangle$. Assim $L < G$, pois se fosse igual teríamos que G seria cíclico, logo abeliano, mas nesse caso o item é trivialmente satisfeito. Aplicando a hipótese de indução em L, temos, para todos $a, b \in L$, $a^{p^k} b^{p^k} = c^{p^k}$, para algum $c \in L$.

Por hipótese G é k-regular, então $x^{p^k} y^{p^k} = (xy)^{p^k} \prod D_i^{p^k}$, com $D_i \leqslant G'$, para cada i e assim $\prod D_i^{p^k} \leqslant (G')^{p^k}$. Isso nos diz que $x^{p^k} y^{p^k} = (xy)^{p^k} w^{p^k}$, com $w \in G'$. Veja que $xy \in L$ e $w \in L$, então pela hipótese de indução existe $z \in L < G$ tal que $(xy)^{p^k} w^{p^k} = z^{p^k}$. Portanto $x^{p^k} y^{p^k} = z^{p^k}$, para algum $z \in G$.

□

Como conclusão desse teorema temos que os subgrupos característicos $\Omega_k(G)$ e G^{p^k} de um p-grupo k-regular podem ser tomados como conjuntos ao invés do gerado, da mesma forma como em um grupo abeliano.

O próximo lema, assim como o anterior, são muitos conhecidos dentro da teoria de p-grupos regulares, aqui estamos mostrando que para p-grupos k-regulares eles também são válidos.

Lema 2.2.5. *Seja G um p-grupo k-regular e l-regular ou $k = 0$ ou $l = 0$. Então:*

(*i*) *Para quaisquer $x, y \in G$, $x^{p^k} = y^{p^k}$ se, e somente se, $(xy^{-1})^{p^k} = e$.*

(*ii*) *Para quaisquer $x, y \in G$, $[x^{p^k}, y^{p^l}] = e$ se, e somente se, $[x, y]^{p^{k+l}} = e$.*

Demonstração. (*i*) Primeiro observe que se $k = 0$, então a equivalência é clara. Assim vamos considerar $k \geq 1$ e provar por indução sobre $|G|$. Novamente usaremos que $G = \langle x, y \rangle$ e também consideraremos que G não é abeliano.

Suponha $x^{p^k} = y^{p^k}$ e considere $[x, y] = z$. Observe que $[x^{p^k}, y] = [y^{p^k}, y] = e$. Segue que

$$x^{p^k} = y^{-1} x^{p^k} y = (y^{-1} x y)^{p^k} = (x[x, y])^{p^k} = (xz)^{p^k}.$$

Considere $H = \langle x, z \rangle$, então $H \leqslant \langle x, G' \rangle \leqslant \langle x, \Phi(G) \rangle$ e este último é um subgrupo estrito de G, pois caso fosse igual teríamos que $G/\Phi(G)$ seria cíclico, e assim G também seria cíclico, e isso não pode ocorrer já que G não é abeliano.

Dessa forma $H < G$ e $x, xz \in H$, então pela hipótese de indução aplicada em H, temos que $e = (x(xz)^{-1})^{p^k} = (xz^{-1}x^{-1})^{p^k} = x(z^{p^k})^{-1}x^{-1}$ e assim $z^{p^k} = e$. Pelo item (*i*) do lema anterior, aplicado em $G' = \langle [x, y]^g \mid g \in G \rangle$, temos que $exp(G') \leq p^k$, pois colocamos $z = [x, y]$ e vimos que $z^{p^k} = e$. Agora, pela k-regularidade de G, $(xy^{-1})^{p^k} = x^{p^k}(y^{-1})^{p^k} \prod_i D_i^{p^k}$, com $D_i \leqslant G'$ para cada i, e então $(xy^{-1})^{p^k} = x^{p^k} y^{-p^k} = e$. Logo, $(xy^{-1})^{p^k} = e$.

Reciprocamente, suponha que $(xy^{-1})^{p^k} = e$. Observe que

$$(yx^{-1})^{p^k} = ((xy^{-1})^{-1})^{p^k} = e$$

e também

$$(xy^{-1})^{p^k} = e = yy^{-1} \Rightarrow y^{-1}(xy^{-1})^{p^k}y = e \Rightarrow (y^{-1}(xy^{-1})y)^{p^k} = e,$$

ou seja, $(y^{-1}x)^{p^k} = e$. Isso nos mostra que $(yx^{-1})^{p^k} = (y^{-1}x)^{p^k} = e$. Então, também, pelo item (i) do lema anterior temos que $e = (y^{-1}xyx^{-1})^{p^k} = [y, x^{-1}]^{p^k}$.

Sabemos que $[y, x^{-1}]$ e seus conjugados também geram G', então podemos ver que $exp(G') \leq p^k$. Agora, pela k-regularidade de G, temos

$$e = (xy^{-1})^{p^k} = x^{p^k}(y^{-1})^{p^k}\prod_i D_i^{p^k} = x^{p^k}(y^{-1})^{p^k},$$

ou seja, $x^{p^k}(y^{-1})^{p^k} = e$ Logo, $x^{p^k} = y^{p^k}$.

(ii) Suponha que $k = 0$. Então temos as seguintes equivalências

$$[x, y^{p^l}] = e \Leftrightarrow x^{-1}(y^{p^l})^{-1}xy^{p^l} = ((x^{-1}yx)^{p^l})^{-1}y^{p^l} = e \Leftrightarrow (x^{-1}yx)^{p^l} = y^{p^l}.$$

Como G é l-regular podemos aplicar o item anterior, então $((x^{-1}yx)^{-1}y)^{p^l} = e$, e isso é equivalente a $[x, y]^{p^l} = e$. De maneira totalmente análoga provamos o caso em que $l = 0$.

Vejamos o caso em que nenhum desses dois ocorre. Suponha que $[x^{p^k}, y^{p^l}] = e$. Então

$$e = (x^{p^k})^{-1}(y^{p^l})^{-1}x^{p^k}y^{p^k} = (x^{p^k})^{-1}((y^{p^l})^{-1}xy^{p^l})^{p^k},$$

ou seja, $((y^{p^l})^{-1}xy^{p^l})^{p^k} = x^{p^k}$. Pelo item anterior temos que isso é equivalente a $(x^{-1}(y^{p^l})^{-1}xy^{p^l})^{p^k} = e$.

Observe que $x^{-1}(y^{p^l})^{-1}xy^{p^l} = (x^{-1}y^{-1}x)^{p^l}y^{p^l}$ e assim $(x^{-1}y^{-1}x)^{p^l}y^{p^l} \in \Omega_k(G)$. Novamente pela aplicação do item anterior segue que $(x^{-1}y^{-1}xy)^{p^l} \in \Omega_k(G)$. Isso significa $((x^{-1}y^{-1}xy)^{p^l})^{p^k} = [x, y]^{p^{k+l}} = e$, como queríamos.

□

Lema 2.2.6. *Sejam G um p-grupo k-regular e l-regular e M e N subgrupos normais de G. Então $[M^{p^k}, N^{p^l}] = [M, N]^{p^{k+l}}$.*

Demonstração. Primeiro vejamos a inclusão $[M^{p^k}, N^{p^l}] \leqslant [M,N]^{p^{k+l}}$. Pelo Lema 2.2.4, item (ii), temos $M^{p^k} = \{m^{p^k} \mid m \in M\}$ e $N^{p^l} = \{n^{p^l} \mid n \in N\}$ e isso acarreta que $[M^{p^k}, N^{p^l}] = \langle [m^{p^k}, n^{p^l}] \mid m \in M, n \in N\rangle$ e $[M,N]^{p^{k+l}} = \langle [m,n]^{p^{k+l}} \mid [m,n] \in [M,N]\rangle$.

Dessa forma veja que $[m,n]^{p^{k+l}} \equiv e \pmod{[M,N]^{p^{k+l}}}$, agora pelo lema anterior, item (ii), também temos que $[m^{p^k}, n^{p^l}] \equiv e \pmod{[M,N]^{p^{k+l}}}$. Isso significa que cada gerador de $[M^{p^k}, N^{p^l}]$ pertence a $[M,N]^{p^{k+l}}$. Logo, a inclusão considerada é válida.

Por outro lado, temos que $[m^{p^k}, n^{p^l}] \equiv e \pmod{[M^{p^k}, N^{p^l}]}$ e pelo mesmo argumento que antes temos $[m,n]^{p^{k+l}} \equiv e \pmod{[M^{p^k}, N^{p^l}]}$. Mas, lembre que $[M,N] = \langle [m,n] \mid m \in M, n \in N\rangle$, então temos que $[M,N]/[M^{p^k}, N^{p^l}]$ é gerado por elementos cuja ordem é, no máximo, p^{k+l}.

Agora, pelo Lema 2.2.4 todo elemento de $[M,N]/[M^{p^k}, N^{p^l}]$ possui ordem, no máximo, p^{k+l}. Isso significa que $[M,N]^{p^{k+l}} \leqslant [M^{p^k}, N^{p^l}]$. Portanto, $[M,N]^{p^{k+l}} = [M^{p^k}, N^{p^l}]$. □

Quando consideramos um p-grupo finito que seja k-regular, esse p-grupo é também l-regular, para todo $l \geq k$, ou seja, a k-regularidade implica na $l-$regularidade. Como veremos no seguinte teorema.

Teorema 2.2.7. *Seja G um p-grupo k-regular. Então G é $(k+1)$-regular.*

Demonstração. Considere $x, y \in G$, arbitrários e defina $H = \langle x, y\rangle$. Por hipótese, G é um p-grupo k-regular. Então, pela definição, $(xy)^{p^k} = x^{p^k} y^{p^k} \prod_i D_i^{p^k}$, com $D_i \leqslant H'$.

Pelo item (ii), do Lema 2.2.4, aplicado a H', temos que existe um $D \in H'$ tal que $\prod_i D_i^{p^k} = D^{p^k}$. Dessa forma podemos reescrever a igualdade da definição como

$$(xy)^{p^k} = x^{p^k} y^{p^k} D^{p^k}. \tag{2.1}$$

Queremos mostrar que $(xy)^{p^{k+1}} \equiv x^{p^{k+1}} y^{p^{k+1}} \pmod{\gamma_2(H)^{p^{k+1}}}$. Provaremos por indução sobre l que

$$((xy)^{p^k})^l \equiv (x^{p^k})^l (y^{p^k})^l (D^{p^k})^l \pmod{\gamma_2(H)^{p^{k+1}}}. \tag{2.2}$$

para $l \geq 1$. Se $l = 1$, pela definição de ser k-regular segue que a equivalência 2.2 é válida.

Considere $l > 1$ e suponha por hipótese de indução que a equivalência 2.2 é válida para todo inteiro menor ou igual a $l-1$. Pela hipótese de indução e pelo primeiro passo temos que

$$((xy)^{p^k})^l = ((xy)^{p^k})^{l-1}(xy)^{p^k} \equiv (x^{p^k})^{l-1}(y^{p^k})^{l-1}(D^{p^k})^{l-1} x^{p^k} y^{p^k} D^{p^k} \pmod{\gamma_2(H)^{p^{k+1}}}$$

$$\equiv (x^{l-1})^{p^k}(y^{l-1})^{p^k}(D^{l-1})^{p^k} x^{p^k} y^{p^k} D^{p^k} \pmod{\gamma_2(H)^{p^{k+1}}}.$$

O Lema 2.2.6, aplicado a H, nos fornece que $[H^{p^k}, H^{p^k}] = [H, H]^{p^{2k}} \leqslant [H, H]^{p^{k+1}}$, onde $k \geq 1$ e com isso $H^{p^k}/\gamma_2(H)^{p^{k+1}}$ é abeliano. Então podemos reescrever a equivalência da seguinte forma:

$$((xy)^{p^k})^l \equiv (x^{l-1})^{p^k} x^{p^k} (y^{l-1})^{p^k} y^{p^k} (D^{l-1})^{p^k} D^{p^k} \pmod{\gamma_2(H)^{p^{k+1}}}.$$

E isso mostra que a equivalência 2.2 é válida para qualquer $l \geq 1$ e assim se considerarmos que $l = p$ temos que $(xy)^{p^{k+1}} \equiv x^{p^{k+1}} y^{p^{k+1}} D^{p^{k+1}} \pmod{\gamma_2(H)^{p^{k+1}}}$, ou seja, $(xy)^{p^{k+1}} \equiv x^{p^{k+1}} y^{p^{k+1}} \pmod{\gamma_2(H)^{p^{k+1}}}$. Sendo $x, y \in G$ arbitrários, temos que G é $(k+1)$-regular, como queríamos. $\square$

Para terminar nossa seção vamos demonstrar o teorema que relaciona o índice de $\Omega_k(G)$ em G com a ordem de G^{p^k} para um p-grupo k-regular, análogo ao Teorema 2.1.7 válido em abeliano. Assim vemos que p-grupos regulares gozam dessa estrutura.

Teorema 2.2.8. *Sejam G um p-grupo m-regular e $k \in \mathbb{N}$, com $k \geq m$. Então:*

(i) $\Omega_k(G) = \{x \in G \mid x^{p^k} = e\}$.

(ii) $G^{p^k} = \{x^{p^k} \mid x \in G\}$.

(iii) $|G : \Omega_k(G)| = |G^{p^k}|$.

Demonstração. (i) Pelo teorema anterior, temos que se G é m-regular, então G também é k-regular. E aplicando o Lema 2.2.4, item (i), podemos concluir que $\Omega_k(G)$ é exatamente o conjunto dos elementos de G que tem ordem no máximo p^k. Portanto, $\Omega_k(G) = \{x \in G \mid x^{p^k} = e\}$.

(ii) Pelo mesmo argumento do item anterior, temos que G é $k-$regular e pelo Lema 2.2.4, item (ii), temos que G^{p^k} é exatamente o conjunto das p^k-ésimas potências de G. Portanto, $G^{p^k} = \{g^{p^k} \mid g \in G\}$.

(iii) Primeiro observe que G é k-regular. Assim, considere a aplicação $\phi : G \to G^{p^k}$ dada por $x \mapsto x^{p^k}$. Temos ainda que ϕ é sobrejetivo, pois $G^{p^k} \leqslant G$ e $k \geq 1$. Observe que pelo Lema 2.2.5 temos que $x^{p^k} = y^{p^k}$ se, e somente se, $(xy^{-1})^{p^k} = e$. Agora, pela definição do subgrupo normal $\Omega_k(G)$ temos que $xy^{-1} \in \Omega_k(G)$. Considerando o grupo quociente $G/\Omega_k(G)$ temos que $xy^{-1} \in \Omega_k(G)$ se, e somente se, $x\Omega_k(G) = y\Omega_k(G)$. Como G^{p^k} é exatamente o conjunto das p^k-ésimas potências de G, temos a igualdade $|G/\Omega_k(G)| = |G^{p^k}|$ como cardinalidade de grupos. Portanto, $|G : \Omega_k(G)| = |G^{p^k}|$.

$\square$

2.3 p-grupos de classe maximal

Na primeira seção desse capítulo, vimos que a classe de nilpotência de um p-grupo finito de ordem p^m é no máximo $m-1$. Daí vem a definição da segunda família que estudaremos que são os de classe de nilpotência exatamente igual a $m-1$, denominados p-grupos de classe maximal.

A principal referência dessa teoria é o trabalho de *N. Blackburn* [3], publicado em 1958. Uma referência mais recente são as notas *An introduction to finite p-groups: regular p-groups and groups of maximal class* [5], de *Gustavo A. Fernandéz-Alcober*, através da qual realizamos nosso estudo. Primeiro vejamos a definição formal.

Definição 2.3.1. *Seja G um p-grupo de ordem $p^m \geq p^2$. Dizemos que G é de classe maximal quando sua classe de nilpotência é $m-1$.*

Os grupos de ordem p^2 são de classe maximal, pois são abelianos. Então $\gamma_2(G) = G' = \{e\}$ e assim eles possuem classe de nilpotência igual a 1.

Os grupos de ordem p^3 que não são abelianos, também são de classe maximal, pois existem apenas duas classes de isomorfismo e em ambas é possível verificar que a classe de nilpotência delas é 2.

Por exemplo, veja que para $p = 2$ essas duas classes de isomorfismos são do $D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, r^s = s^{-1} \rangle$ e do $Q_8 = \langle a, b \mid a^4 = 1, b^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle$, o diedral e o quatérnio de ordem 8, respectivamente. Eles não são abelianos, então a classe de nilpotência deles é maior do que 1, mas por serem p-grupos vale também que ela é menor ou igual a 2, logo deve ser 2.

Para um primo ímpar as duas classes de isomorfismos são as dos grupos $M_{p^3} = \langle a, b \mid a^{p^2} = b^p = 1, a^b = a^{1+p} \rangle$ (metacíclico) e $E_{p^3} = \langle a, b, c \mid a^p = b^p = c^p = 1, a^c = ab, [a, b] = [b, c] = 1 \rangle$. E de maneira análoga ao que fizemos antes, ambas possuem classe de nilpotência igual a 2.

Dessa forma podemos estudar apenas p-grupos de classe maximal de ordem maior ou igual a p^4, pois os menores já estão completamente classificados.

O primeiro resultado que mostraremos reuni as principais propriedades sobre os subgrupos normais de um p-grupo de classe maximal.

Teorema 2.3.2. *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* $2 \leq i \leq m-1$. *Consequentemente,* $|G : \gamma_i(G)| = p^i$ *para* $2 \leq i \leq m-1$.

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

(*iii*) *Os únicos subgrupos normais de G são $\gamma_i(G)$ e os subgrupos maximais de G. Mais precisamente, 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 $\geq p^2$, então G/N também é de classe maximal.*

(*v*) *$Z_i(G) = \gamma_{m-i}(G)$, para $0 \leq i \leq m-1$.*

Demonstração. (*i*) Seja G um p-grupo de classe maximal de ordem p^m. Então G tem classe de nilpotência igual a $m-1$. Isso nos mostra que a série central inferior tem comprimento $m-1$ e os termos até $m-1$ são estritos um no outro. Dessa forma, temos

$$p^m = |G| = \prod_{i=1}^{m-1} |\gamma_i(G) : \gamma_{i+1}(G)| = |G : G'| \prod_{i=2}^{m-1} |\gamma_i(G) : \gamma_{i+1}(G)|.$$

Agora, pelo Teorema 2.1.1 vale que $[G : G'] \geq p^2$. Sendo os termos da série central inferior estritos, também vale que $|\gamma_i(G) : \gamma_{i+1}(G)| \geq p$, quando $2 \leq i \leq m-1$. Com isso,

$$|G : G'| \prod_{i=2}^{m-1} |\gamma_i(G) : \gamma_{i+1}(G)| \geq p^2 \cdot p^{m-2} = p^m.$$

Como $|G| = p^m$, segue que essa desigualdade é exatamente igual a p^m. Assim $|\gamma_i(G) : \gamma_{i+1}(G)| = p$, para todo $2 \leq i \leq m-1$, e $|G : G'| = p^2$. Em particular, observe que

$$|G : \gamma_i(G)| = \prod_{j=1}^{i-1} |\gamma_j(G) : \gamma_{j+1}(G)| = |G : G'| \prod_{j=2}^{i-1} |\gamma_j(G) : \gamma_{j+1}(g)|.$$

Mas vimos que $|G : G'| = p^2$ e cada índice nesse produtório é p. Como temos $i-2$ fatores nesse produto, então $|G : \gamma_i(G)| = p^2 \cdot p^{i-2} = p^i$, para $2 \leq i \leq m-1$.

(*ii*) Como G é um p-grupo finito, pelo Teorema 2.1.3, $\Phi(G) = G'G^p$. Com isso, $G' \leqslant \Phi(G)$, logo $|G : \Phi(G)| \leq |G : G'| = p^2$.

Temos dois casos, se $|G : \Phi(G)| = p$, então $G/\Phi(G)$ é cíclico, logo é abeliano. Dessa forma, nesse caso temos que $G' = \{e\}$ e $|G : G'| = |G : \{e\}| = p^2$, ou seja, G será cíclico de ordem p^2.

Agora, se $|G : \Phi(G)| = p^2$, então pelo Teorema da Base de Burnside 2.1.4, temos que $d(G) = 2$ e ainda observe que $\Phi(G) = G'$, pois $|G : G'| = |G : \Phi(G)|$ e $G' \leqslant \Phi(G)$.

(iii) Seja N um subgrupo normal de G. Como N também é um p-grupo, então $|G : N| = p^i$ para algum $i = \{0, 1, \ldots, m-1\}$.

Observe que se $i = 0$, então $|G : N| = 1$ e isso acarreta que $N = G = \gamma_1(G)$. Se $i = 1$, então $|G : N| = p$ e assim N é maximal em G.

Por outro lado, se $i \geq 2$, pelo Corolário 2.1.2, temos que $\gamma_i(G) \leqslant N$. Pelo item (i), deste teorema temos que $|G : \gamma_i(G)| = p^i$.

Dessa forma, $|G : N| = p^i = |G : \gamma_i(G)|$ e $\gamma_i(G) \leqslant N$, logo $\gamma_i(G) = N$. Portanto, os únicos subgrupos normais de G são os maximais ou os termos da série central inferior.

(iv) Considere N um subgrupo normal de G de índice $p^i \geq p^2$. Pelo item anterior, temos que $N = \gamma_i(G)$ e por (i), segue que $|G : \gamma_i(G)| = p^i = |G : N|$.

Vimos que $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $j \geq 1$. Em particular, $\gamma_i(G/N) = \gamma_i(G)N/N = N/N = \{e\}$, logo $\gamma_i(G/N) = \{e\}$.

Como $\gamma_{i-1}(G)$ é um subgrupo próprio de $\gamma_i(G) = N$, $i-1$ é a classe de nilpotência de G/N, ou seja, o quociente também é de classe maximal.

(v) Novamente pelo Teorema 2.1.1, temos que $|G : Z_{m-2}(G)| \geq p^2$. Vimos que a série central superior é crescente e que $\gamma_{c+1-i}(G) \leqslant Z_i(G)$, onde c é classe de nilpotência de G e $0 \leq i \leq c$.

No nosso caso, a classe de G é $m-1$, então $\gamma_{m-i}(G) \leqslant Z_i(G)$, para $0 \leq i \leq m-1$. Para concluirmos a outra inclusão, vamos verificar que esses dois subgrupos possuem o mesmo índice em G.

Observe que se $i = m-1$, temos que $\gamma_{m-(m-1)}(G) = \gamma_1(G) = G \leqslant Z_{m-1}(G)$. Porém $Z_{m-1(G)} \leqslant G$, logo $Z_{m-1}(G) = G$. Dessa forma o último termo da série central superior é $Z_{m-1}(G) = G$. Da mesma maneira que o item (i), pelo Teorema 2.1.1, temos que $|G : Z_{m-2}(G)| \geq p^2$.

Também teremos que $|Z_{i+1}(G) : Z_i(G)| \geq p$, para $0 \leq i \leq m-3$. Assim,

$$p^m = |G| = \prod_{i=0}^{m-2} |Z_{i+1}(G) : Z_i(G)| = |G : Z_{m-2}(G)| \prod_{i=0}^{m-3} |Z_{i+1}(G) : Z_i(G)| \geq p^2 \cdot p^{m-2}.$$

Onde este último também é igual a p^m. Dessa forma, $|Z_{i+1}(G) : Z_i(G)| = p$, para cada $0 \leq i \leq m-3$, e com isso $|Z_i(G)| = \prod_{j=0}^{i-1} |Z_{j+1}(G) : Z_j(G)| = p^i$, para $0 \leq i \leq m-2$. Então, $|G : Z_i(G)| = p^{m-1}$, para $0 \leq i \leq m-2$.

Mas, pelo item (i), temos que $p^{m-i} = |G : \gamma_{m-i}(G)|$, então $\gamma_{m-i}(G) = Z_i(G)$, para $0 \leq i \leq m-1$, como queríamos.

$\square$

Quando G for um p-grupo de classe maximal denotaremos $G_i = \gamma_i(G)$, para $i \geq 2$, e $G_0 = G$.

Definição 2.3.3. *Seja G um p-grupo de classe maximal de ordem $p^m \geq p^4$. Definimos $G_1 = C_G(G_2/G_4)$ (a ação de G sobre G_2/G_4 é induzida pela conjugação). Em outras palavras, G_1 é composto dos elementos $x \in G$ tais que $[x, G_2] \leqslant G_4$.*

Observe que se N é um subgrupo normal de G tal que $|G/N| \geq p^4$, então pela definição acima temos que $(G/N)_1 = G_1/N$.

Teorema 2.1. *Seja G um p-grupo de classe maximal. Então G_1 é um subgrupo maximal característico de G.*

Demonstração. Primeiro vamos mostrar que G_1 é característico. Considere $f \in Aut(G)$. Lembre que $G_2 = \gamma_2(G)$ e $G_4 = \gamma_4(G)$ são característicos em G. Então temos

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

Portanto, G_1 é característico em G.

Por outro lado, como G_1 é o núcleo da ação de G sobre G_2/G_4, o grupo quociente G/G_1 pode ser imerso em $Aut(G_2/G_4)$. Mas, $|G_2 : G_4| = p^2$, então G_2/G_4 é isomorfo a C_{p^2} ou $C_p \times C_p$.

No primeiro caso, sabemos que $|Aut(G_2/G_4)| = p(p-1)$, enquanto que no segundo $|Aut(G_2/G_4)| = |GL_2(p)| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$. Em ambos os casos a maior potência de p que divide $|Aut(G_2/G_4)|$ é p. Dessa forma, $|G : G_1| \leq p$.

Se $G_1 = G$, então $G_3 = [G, G_2] = [G_1, G_2] \leqslant G_4$, por definição de G_1. Mas, sendo a série decrescente, $G_3 \leqslant G_4$ só ocorre quando $G_3 = 1$, e isso contradiz o fato de $|G| \geq p^4$. Logo, $|G : G_1| = p$, ou seja, G_1 é maximal em G. $\square$

Com a notação introduzida temos que $|G_i : G_{i+1}| = p$, para $0 \leq i \leq m-1$ e $G_i = 1$, para $i \geq m$.

O teorema a seguir será de grande utilidade na construção da família de exemplos que será feita no Capítulo 5. Omitiremos a demonstração em nosso trabalho, mas ela pode ser encontrada através da referência [5], no Teorema 4.9.

Teorema 2.3.4. *Seja G um p-grupo de classe maximal de ordem $p^m \geq p^{p+2}$. Então valem os seguintes itens:*

(*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* $x \in G_i - G_{i+1}$, *então* $x^p \in G_{i+p-1} - G_{i+p}$.

Elementos uniformes de um p-grupo de classe maximal

Dado G um p-grupo de classe maximal de ordem p^m, também podemos definir outros centralizadores da mesma forma que definimos $G_1 = C_G(G_2/G_4)$, da seguinte forma $C_G(G_i/G_{i+2})$, para $1 \leq i \leq m-2$. Como acontece com G_1, todos esses subgrupos são característicos e maximais em G.

Definição 2.3.5. *Seja* G *um* p*-grupo de classe maximal de ordem* p^m. *Dizemos que* $s \in G$ *é um elemento uniforme se* $s \notin \cup_{i=2}^{m-2} C_G(G_i/G_{i+2})$.

A primeira pergunta que surge é se qualquer p-grupo de classe maximal possui elementos uniformes, ou seja, o p-grupo G é igual ou diferente de $\cup_{i=2}^{m-2} C_G(G_i/G_{i+2})$. *Blackburn* mostrou que p-grupos de classe maximal de ordem p^m possuem elementos uniformes, ou seja, vale que $G \neq \cup_{i=2}^{m-2} C_G(G_i/G_{i+2})$.

Em um p-grupo finito G de ordem maior ou igual a p^2, temos que $|C_G(x)| \geq p^2$, para qualquer $x \in G$. Mais ainda, dado um subgrupo normal N de G vale $|C_G(x)| \geq |C_{G/N}(xN)|$, para qualquer $x \in G$ (Exercício 1.2 de [5]). Com isso, podemos verificar que uma condição necessária e suficiente para um p-grupo ser de classe maximal é que exista um elemento $x \in G$ tal que seu centralizador tenha ordem p^2. Note que tais elementos são precisamente os elementos uniformes. Também verifica-se que dado um elemento uniforme s vemos que $s^p \in Z(G)$ (Teorema 3.15 de [5]). Essas afirmações são obtidas fazendo-se um estudo detalhado das notas *An introduction to finite p-groups: regular p-groups and groups of maximal class* [5], de *Gustavo A. Fernandéz-Alcober.*

2.4 p-grupos ***powerful***

A próxima família é a de p-grupos finitos *powerful*. O estudo sobre esse família foi essencialmente desenvolvida por *A. Lubotzky* e *A. Mann* [20], em 1987. Porém, em 1965, *M. Lazard* [18] também realizou um estudo sobre esses p-grupos.

Um fato importante nessa família é que a quantidade mínima de geradores dos subgrupos são sempre menores ou iguais à do grupo, e isso nem sempre vale em outros grupos. E isso mostra que p-grupos finitos *powerful* possuem posto igual à quantidade mínima de geradores do grupo, como será visto nessa seção no Teorema 2.4.12.

Outro fato importante que também veremos é como encontrar um subgrupo *powerful* de posto limitado contido em um p-grupo de posto finito, o que será visto no Teorema 2.4.16. Além disso verificaremos que p-grupos *powerful*, assim como os regulares, compartilham de algumas das características dos abelianos.

O estudo a cerca dessa família foi essencialmente baseado no livro *Analytic Pro-p Groups* [4]. Os livros *p-Automorphisms of Finite p-Groups* [16] e *The Structure of Groups of Prime Power Order* [19] também possuem seções sobre esses p-grupos, assim como o artigo [20], e foram eventualmente consultadas.

Definição 2.4.1. *Seja G um p-grupo finito. Dizemos que G é powerful se $[G, G] = G' \leq G^p$, se p é ímpar, ou se $G' \leq G^4$, se $p = 2$.*

Lembre que em um p-grupo finito vale $\Phi(G) = G^pG'$, com isso quando tivermos p ímpar, G será *powerful* se, e somente se, $G^p = \Phi(G)$.

Definição 2.4.2. *Um subgrupo N de um p-grupo finito G é dito powerfully embedded em G, onde denotaremos por N p.e. G, se $[N, G] \leqslant N^p$, se p é ímpar, ou $[N, G] \leqslant N^4$, se $p = 2$.*

Essa definição nos mostra que G é *powerful* se, e somente se, G *p.e.* G. E também pode-se verificar que se N *p.e.* G, então $N \trianglelefteq G$ e N é *powerful*. Todo p-grupo abeliano é *powerful* e todos os seus subgrupos serão *powerfully embedded*.

Um exemplo clássico de p-grupo que não é *powerful* é o D_8, o diedral de ordem 8. Considerando $D_8 = \langle r, s \mid r^4 = s^2 = e, r^s = r^{-1} \rangle$ pode-se verificar que $D_8' = \langle r^2 \rangle$ e que $D_8^4 = \{e\}$, então $D_8' \nleq D_8^4$.

No estudo de p-grupos regulares vimos que seus subgrupos são ainda regulares, porém isso não ocorre em p-grupos *powerful*. Vamos construir um exemplo de um p-grupo *powerful* que possui um subgrupo que não é. Como vimos que D_8 não é *powerful* consideraremos um grupo que irá conter uma cópia isomorfa do D_8 como subgrupo próprio.

Defina o grupo $G = D_8 \times C_8$, onde C_8 é um grupo cíclico de ordem 8 gerado por z e D_8 tem a apresentação citada anteriormente. Considere o seguinte subgrupo, que é normal, $N = \langle [r,s]^{-1}z^4 \rangle = \langle r^2 z^4 \rangle$ de G. Agora considere o grupo quociente $K = G/N = (D_8 \times C_8)/N$, temos que $[K,K] = [G/N, G/N] = [G,G]N/N = \langle r^2 N \rangle = \langle z^4 N \rangle \leqslant K^4$. Assim K é *powerful*, mas veja que $H = \langle rN, sN \rangle$ é uma cópia isomorfa a D_8, onde o isomorfismo é $\phi : D_8 \to H$, dado por $r \mapsto rN$ e $s \mapsto sN$, que não é *powerful*, e assim H também não.

Exemplos de subgrupos de um p-grupos *powerful* que não preservam a propriedade quando p ímpar, podem ser construídos de maneira semelhante e no livro *The Structure of Groups of Prime Power Order* [19], Capítulo 6, pode-se encontrar um roteiro para essa construção.

O próximo lema nos mostra algumas das principais características de p-grupos *powerful.*

Lema 2.4.3. *Seja G um p-grupo finito e sejam N, K e W subgrupos normais de G, com $N \leqslant W$. Então:*

(*i*) *Se N p.e. G então NK/K p.e. G/K.*

(*ii*) *Se $p > 2$ e $K \leqslant N^p$, ou, se $p = 2$ e $K \leqslant N^4$, 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 $\langle x, N \rangle$ é powerful.*

(*iv*) *Se N não é powerfully embedded em W, então existe um subgrupo normal J de G tal que*

- *Se $p > 2$: $N^p[N,W,W] \leqslant J < N^p[N,W]$ e $[N^p[N,W] : J] = p$.*
- *Se $p = 2$: $N^4[N,W]^2[N,W,W] \leqslant J < N^4[N,W]$ e $[N^4[N,W] : J] = 2$.*

Demonstração. (*i*) Suponha que N *p.e.* G. Considere inicialmente $p > 2$ e o homomorfismo canônico $\pi : G \to G/K$. Pelo Teorema da Correspondência temos que $\pi(N) = NK/K$. Assim $\pi(N^p) = N^pK/K$ e $(\pi(N))^p = (NK/K)^p$. Mas $(NK/K)^p = N^pK/K$, então $\pi(N^p) = (\pi(N))^p$.

Temos que $[N,G] \leqslant N^p$, então $\pi([N,G]) \leqslant \pi(N^p)$. Como π é um homomorfismo e N é um subgrupo normal de G, segue que $\pi([N,G]) = [\pi(N), \pi(G)] = [NK/K, G/K] = [N,G]K/K$. E assim $[NK/K, G/K] \leqslant N^pK/K = (NK/K)^p$.

Por outro lado suponha $p = 2$ e considere ainda o homomorfismo canônico π como acima. Também temos que $\pi(N^4) = (\pi(N))^4$, então $\pi([N,G]) = [\pi(N), \pi(G)] =$

$[NK/K, G/K] = [N, G]K/K \leqslant N^4K/K = (NK/K)^4$. Portanto em ambos os casos temos NK/K *p.e.* G/K.

(*ii*) Suponha que $K \leqslant N^p$, se $p > 2$, ou $K \leqslant N^4$, se $p = 2$. Por um lado, suponha ainda que N *p.e.* G. Observe que $K \leqslant N^p \leqslant N$ ou $K \leqslant N^4 \leqslant N$ e assim $NK/K = N/K$, em ambos os casos. Como vimos que NK/K *p.e.* G/K, segue que N/K *p.e.* G/K, como queríamos.

Reciprocamente, suponha N/K *p.e.* G/K. Pela definição,$[N/K, G/K] \leqslant (N/K)^p$, se $p > 2$, ou $[N/K, G/K] \leqslant (N/K)^4$, se $p = 2$. Agora, veja que $p > 2$, temos $K \leqslant N^p \leqslant N$ e assim

$$[N, G]K/K = [N/K, G/K] \leqslant (N/K)^p = (NK/K)^p = N^pK/K = N^p/K.$$

E da mesma forma temos que se $p = 2$, então $K \leqslant N^4 \leqslant N$ e assim

$$[N, G]K/K = [N/K, G/K] \leqslant (N/K)^4 = (NK/K)^4 = N^4K/K = N^4/K.$$

Pelo Teorema da Correspondência temos que $[N, G] \leqslant N^p$ ou $[N, G] \leqslant N^4$, em cada caso. Portanto, N *p.e.* G.

(*iii*) Suponha que N *p.e.* G e seja $x \in G$. Considere $H = \langle N, x\rangle$ e vejamos que H é *powerful*. Primeiro observe que $[H, H] = [N, H]$, vejamos que valem as duas inclusões. Por um lado, temos que $N \leqslant H$, então $[N, H] \leqslant [H, H]$. Por outro lado, tome $n_1x^i, n_2x^j \in H$, onde $n_1, n_2 \in N$, e veja que

$$[n_1x^i, n_2x^j] = [n_1, n_2x^j]^{x^i}[x^i, n_2x^j] = ([n_1, x^j][n_1, n_2]^{x^j})^{x^i}[x^i, x^j][x^i, n_2]^{x^j} =$$

$$= [n_1, x^j]^{x^i}([n_1, n_2]^{x^j})^{x^i}[x^i, n_2]^{x^j} = [n_1^{x^i}, x^j][n_1^{x^{i+j}}, n_2^{x^{i+j}}][x^i, n_2^{x^j}].$$

Como $N \trianglelefteq G$, cada um desses comutadores da última igualdade são elementos de $[N, H]$, então $[H, H] \leqslant [N, H]$ e temos a igualdade citada.

Agora veja que com isso temos $[H, H] = [N, H] \leqslant [N, G] \leqslant N^p \leqslant H^p$, se $p > 2$, ou $[H, H] = [N, H] \leqslant [N, G] \leqslant N^4 \leqslant H^4$, se $p = 2$. Ou seja, temos que H é *powerful* em ambos os casos, como queríamos.

(*iv*) Inicialmente suponha que $p > 2$. Por hipótese, N não é *powerfully embedded* em W, ou seja, $[N, W] \nleqslant N^p$. Então $N^p < N^p[N, W] = M$. Como G é um p-grupo e

M e N^p são subgrupos normais de G, então existe $J \trianglelefteq G$ tal que $N^p \leqslant J < M$ e $|M : J| = p$.

Observe que $M/J \trianglelefteq G/J$ e G/J é também um p-grupo, com isso $M/J \cap Z(G/J) \neq 1$. Mas $|M : J| = p$, então $|M/J| = p$, com isso $M/J \leqslant Z(G/J)$. Isso acarreta que $[M, G] \leqslant J$ e assim $[N^p[N, W], G] \leqslant J < M$.

Temos que $[N, W, W] \leqslant [[N, W], G] \leqslant [M, G] = [N^p[N, W], G] \leqslant J$, ou seja, $[N, W, W] \leqslant J$. Como $N^p \leqslant J$, segue que $N^p[N, W, W] \leqslant J$. E, portanto, nesse caso, existe um subgrupo normal J tal que $N^p[N, W, W] \leqslant J < N^p[N, W]$ e $|N^p[N, W] : J| = p$.

Agora, de maneira análoga suponha $p = 2$. Por hipótese N não é *powerfully embedded* em W, ou seja $[N, W] \nleqslant N^4$. Então $N^4 \leqslant N^4[N, W]$, onde denominaremos de M tal subgrupo. Da mesma forma que no caso anterior existe $J \trianglelefteq G$ tal que $N^4 \leqslant J < N^4[N, W] = M$ e $|M : J| = 2$.

Também de maneira totalmente análoga obtemos que $[M, G] \leqslant J$. E com isso $[N^4[N, W], G] \leqslant J < N^4[N, W]$. Observe que $N^4 \leqslant J$, $[N, W]^2 \leqslant J$ e que $[N, W, W] \leqslant [[N, W], G] \leqslant [M, G] = [N^4[N, W], G] \leqslant J$. Portanto, existe J tal que $N^4[N, W]^2[N, W, W] \leqslant J < N^4[N, W]$ e $|N^4[N, W] : J| = 2$.

□

Observação 2.4.1. *Observe que o último item desse lema, de certa forma, nos mostra uma maneira de verificar que N p.e. W, onde N e W são subgrupos normais de G, um p-grupo finito, com $N \leqslant W$. Para isso inicialmente supomos por contradição que N não é powerfully embedded em W e então poderemos "quocientar"por um subgrupo normal adequado J e assim reduzir o caso onde $N^p = 1$, se $p > 2$, ou $N^4 = 1$, se $p = 2$, supondo ainda que $[N, W]$ tem ordem p (e $[N, W]$ é central em G), dessa forma obteremos um absurdo.*

O próximo teorema nos mostra uma propriedade válida com subgrupos normais *powerfully embedded* em um p-grupo finito, que pode parecer simples, mas por se tratar de subgrupos gerados isso nem sempre é válido.

Teorema 2.4.4. *Sejam G um p-grupo finito e M e N subgrupos normais powerfully embedded em G. Então $[N^p, M] = [N, M]^p$.*

Demonstração. Vamos provar as duas inclusões. Suponhamos inicialmente que $p > 2$. Pela Fórmula de Hall, Teorema 2.1.10, temos que $[N^p, M] \equiv [N, M]^p \pmod{[M,_p N]}$ e usando hipótese que M *p.e.* G, vale que

$$[N^p, M] \leqslant [N, M]^p[M,_p N] \leqslant [N, M]^p[M, G,_{p-1} N] \leqslant [N, M]^p[M^p,_{p-1} N].$$

Como $p > 2$, então $p - 1 \geq 2$. Isso nos dá que $[M^p,_{p-1} N] \leqslant [M^p, N, N]$. Com isso, $[N^p, M] \leqslant [N, M]^p[M^p, N, N]$ e novamente pelo Teorema 2.1.10 temos que

$$[N^p, M] \leqslant [N, M]^p[M^p, N, N] \leqslant [N, M]^p[[M, N]^p[N,_p M], N] =$$

$$= [N, M]^p[[M, N]^p, N][N,_p M, N] \leqslant [N, M]^p[[M, N]^p, G][N, G,_{p-1} M, N].$$

Usando agora a hipótese de que N é *powerfully embedded* em G e $[M, N]^p \trianglelefteq G$, segue que

$$[N^p, M] \leqslant [N, M]^p[N, M]^p[N^p,_{p-1} M, N] \leqslant [N, M]^p[N^p, M, M, N] \leqslant [N, M]^p[N^p, M, G, G].$$

Assim, $[N^p, M] \leqslant [N, M]^p[[N^p, M], G]$. Aplicando o Teorema 2.1.8, concluímos que $[N^p, M] \leqslant [N, M]^p$.

Por outro lado, $[N, M]^p \leqslant [N^p, M][M,_p N]$ e usando a hipótese de que M é *powerfully embedded* em G temos que $[N, M]^p \leqslant [N^p, M][M^p,_{p-1} N] \leqslant [N^p, M][M^p, N, N]$.

Na primeira inclusão mostramos que $[M^p, N] \leqslant [M, N]^p$, dessa forma $[N, M]^p \leqslant [N^p, M][[M, N]^p, G]$. Portanto, se $p > 2$ vale que $[N^p, M] = [N, M]^p$.

Considerando $p = 2$, pelo Teorema 2.1.10, temos $[N^2, M] \equiv [N, M]^2 \pmod{[M,_2 N]}$ e usando o fato de M ser *powerfully embedded*, segue que

$$[N^2, M] \leqslant [N, M]^2[M,_2 N] \leqslant [N, M]^2[M, G, N] \leqslant [N, M]^2[M^4, N].$$

Novamente pelo Teorema 2.1.10, vale que $[M^4, N] \equiv [M, N]^4 (\mathrm{mod} [N,_2 M]^2[N,_4 M])$. Usando agora o fato de N ser *powerfully embedded* obtemos

$$[N^2, M] \leqslant [N, M]^2[M, N]^4[N,_2 M]^2[N,_4 M] \leqslant$$

$$\leqslant [N, M]^2[M, N]^4[N, M]^2[[N, G],_3 M] \leqslant [N, M]^2[[N^4, M], G].$$

Assim $[N^2, M] \leqslant [N, M]^2[[N^2, M], G]$ e pelo Teorema 2.1.8 segue que $[N^2, M] \leqslant [N, M]^2$.

Por outro lado, o Teorema 2.1.10 também nos dá $[N, M]^2 \leqslant [N^2, M][M,_2 N]$, e usando o fato que M é *powerfully embedded* em G temos:

$$[N, M]^2 \leqslant [N^2, M][M^4, N] \leqslant [N^2, M][M, N]^4[N,_2 M]^2[N,_4 M].$$

Como N também é *powerfully embedded* em G, segue que

$$[N, M]^2 \leqslant [N^2, M][M, N]^4[N^4, M]^2[N^4,_3 M] \leqslant [N^2, M]([N, M]^2)^2$$

E novamente pelo Teorema 2.1.8 obtemos $[N, M]^2 \leqslant [N^2, M]$. Portanto, se $p = 2$ também vale a igualdade $[N^p, M] = [N, M]^p$. □

Considerando G um p-grupo finito e N um subgrupo dele, tal que N *p.e.* G, certamente poderíamos perguntar se alguns dos principais subgrupos de N, como N^p, $[N, G]$, herdam essa propriedade. E se tivermos dois subgrupos de G com tal propriedade, o produto deles é ainda *powerfully embedded* em G? Os próximos dois teoremas tem por objetivo responder, e de maneira positiva, essas questões.

Teorema 2.4.5. *Seja G um p-grupo finito e $N \leqslant G$, tal que N é powerfully embedded em G, então N^p p.e. G.*

Demonstração. Primeiro suponha que $p > 2$. Pelo teorema anterior temos que $[N^p, G] = [N, G]^p \leqslant (N^p)^p$, pois por hipótese N é *powerfully embedded* em G. Dessa forma $[N^p, G] \leqslant (N^p)^p$, ou seja, N^p *p.e.* G.

Agora considere $p = 2$, pelo teorema anterior temos que $[N^2, G] = [N, G]^2 \leqslant (N^4)^2$, pois N *p.e.* G. Mas, pelo Corolário 1.1.15 vale que $(N^4)^2 \equiv N^8 \pmod{\gamma_2(N^4)^2\gamma_2(N^4)}$ e assim $(N^4)^2 \leqslant N^8[N^4, G]$. Pelo Teorema 2.1.10, temos $[N^4, G] \leqslant [(N^2)^2, G] \leqslant [N^2, G]^2[G,_2 N^2]$. Com isso,

$$[N^2, G] \leqslant (N^4)^2 \leqslant N^8[N^2, G]^2[G, G, N^2] \leqslant (N^2)^4[N^2, G]^2[N^2, G, G]$$

Assim, $[N^2, G] \leqslant (N^2)^4[N^2, G]^2[N^2, G, G]$. Pelo Teorema 2.1.8 segue que $[N^2, G] \leqslant (N^2)^4$. Portanto, N^p *p.e.* G. □

Teorema 2.4.6. *Sejam G um p-grupo e M, N subgrupos normais powerfully embedded em G. Então $[N, G]$ e MN são powerfully embedded em G.*

A demonstração desse teorema é uma simples verificação da definição usando a propriedade $[N^p, M] = [N, M]^p$.

Considere um p-grupo finito G e vamos definir a seguinte sequência de subgrupos:

$$P_1(G) = G; \quad P_{i+1}(G) = P_i(G)^p[P_i(G), G], \ i \geq 1.$$

Para simplificar a notação escreveremos $G_i = P_i(G)$ e denominaremos essa série por p-série. Observe que essa cadeia é decrescente de subgrupos normais em G e ainda é uma série central, já que $[P_i(G), G] \leqslant P_{i+1}(G)$. Temos também que $P_2(G) = \Phi(G)$.

Vamos verificar algumas propriedades que ocorrem nessa série quando G é um p-grupo finito *powerful*.

Lema 2.4.7. *Seja G um p-grupo powerful.*

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

(ii) Para cada i, a aplicação $x \longmapsto x^p$ induz um homomorfismo de G_i/G_{i+1} sobre G_{i+1}/G_{i+2}.

Demonstração. (i) Vamos provar por indução sobre i. Para $i = 1$, o resultado é trivial, já que G *p.e.* G. Vimos que $G_2 = \Phi(G) = \Phi(G_1)$ e como $[G, G] \leqslant G^p$, para qualquer primo p, segue que $\Phi(G) = G^p$. Assim vale o primeiro passo da indução.

Suponha por hipótese de indução que G_i *p.e.* G e que $G_{i+1} = G_i^p = \Phi(G_i)$. Vejamos ser válido para $i + 1$. Como $G_{i+1} = G_i^p$, então pelo Teorema 2.4.5, G_{i+1} *p.e.* G.

Pela definição da série temos que $G_{i+2} = G_{i+1}^p[G_{i+1}, G]$ e como acabamos de ver que G_{i+1} *p.e.* G, segue $G_{i+2} \leqslant G_{i+1}^p$. Mas já temos que $G_{i+1}^p \leqslant G_{i+2}$, assim segue a igualdade $G_{i+2} = G_{i+1}^p$.

Para a outra igualdade temos que $G_{i+1}^p \leqslant \Phi(G_{i+1})$ e $\Phi(G_{i+1}) = G_{i+1}^p[G_{i+1}, G_{i+1}]$, pelo Teorema 2.1.3. Assim $\Phi(G_{i+1}) \leqslant G_{i+1}^p[G_{i+1}, G] \leqslant G_{i+1}^p$. Dessa forma $\Phi(G_{i+1}) = G_{i+1}^p$. Como queríamos.

(ii) No item anterior vimos que G_i *p.e.* G, lembrando que $[G_i, G_i] \leqslant [G_i, G]$ segue que G_i é ainda *powerful*.

Observe que temos $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$, de fato, pela definição da série $P_2(G_i) = P_1(G_i)^p[P_1(G_i), G] = G_i^p[G_i, G] = G_{i+1}$, pelo item anterior, e da mesma forma $P_3(G_i) = G_{i+2}$.

Então, mudando a notação, podemos assumir que $i = 1$ e substituindo G por G/G^3, podemos assumir $G_3 = 1$. Veja que $[G, G] \leqslant G_2 = \Phi(G)$ e sabemos $[G_2, G] \leqslant G_3$, assim $G_2 \leqslant Z(G)$ e então $[G, G] \leqslant G_2 \leqslant Z(G)$.

Com isso, temos que $[[G, G], G] \leqslant [Z(G), G] = 1$, ou seja, $\gamma_3(G) = 1$. Lembre que dados $x, y \in G$ e $n \in \mathbb{N}$ temos $(xy)^n \equiv x^n y^n [y, x]^{\frac{n(n-1)}{2}} (\mathrm{mod}\ \gamma_3(G))$.

Considere p um primo ímpar, então temos $(xy)^p = x^p y^p [y, x]^{\frac{p(p-1)}{2}}$ e, nesse caso, p divide $\frac{p(p-1)}{2}$. Como $[y, x] \in G_2$, temos que $([y, x]^p)^{\frac{p-1}{2}} \in G_2^p = G_3 = 1$, pelo item anterior. Isso significa que $(xy)^p = x^p y^p$.

Agora, se $p = 2$, como G é *powerful*, então $[G, G] \leqslant G^4 \leqslant (G^2)^2 \leqslant (\Phi(G))^2 = G_2^2 = G_3 = 1$. Assim $(xy)^2 = x^2 y^2 [y, x] = x^2 y^2$, já que $[y, x] \in [G, G] \leqslant G_3 = 1$. Dessa forma, em qualquer caso temos $(xy)^p = x^p y^p$.

Como $G_2^p = G_3 = 1$ e $G^p = G_2$, temos que $x \longmapsto x^p$ induz um homomorfismo sobrejetivo de G/G_2 sobre G_2/G_3.

Observe que verificamos a validade do item para $i = 1$, os demais casos seguem o mesmo raciocínio já que G_i é *powerful*, para todo i. Portanto, o lema está demonstrado.

□

Lema 2.4.8. *Se $G = \langle a_1, \ldots, a_d \rangle$ é um p-grupo powerful, então $G^p = \langle a_1^p, \ldots, a_d^p \rangle$.*

Demonstração. Considere o homomorfismo sobrejetivo $\theta : G/G_2 \longrightarrow G_2/G_3$ do lema anterior. Por hipótese G é gerado por $\{a_1, \ldots, a_d\}$, então G/G_2 é gerado pelo conjunto $\{a_1G_2, \ldots a_dG_2\}$.

Pelo homomorfismo G_2/G_3 será gerado por $\{\theta(a_1G_2), \ldots, \theta(a_dG_2)\}$, sendo esse homomorfismo $x \longmapsto x^p$, teremos que $G_2 = \langle a_1^pG_2^p, \ldots, a_dG_2^p \rangle G_3 = \langle a_1^p, \ldots, a_d^p \rangle G_3$, pois $G_2^p = G_3$.

Agora temos que $G_2 = G^p$ e $G_3 = \Phi(G_2)$. Como o subgrupo Frattini é o composto pelos elementos não-geradores do grupo, temos que $G^p = \langle a_1^p, \ldots, a_d^p \rangle$, como queríamos. □

O próximo resultado é uma das características de *powerful* que é compartilhada com grupos abelianos.

Proposição 2.4.9. *Se G é um p-grupo powerful, então todo elemento de G^p é potência de um elemento de G.*

Demonstração. Vamos provar por indução sobre $|G|$. Se $|G| = 1$, o resultado é claro. Então suponha por hipótese de indução que o resultado seja válido para todo p-grupo *powerful* de ordem estritamente menor do que $|G|$.

Considere $g \in G^p$. Pelo Lema 2.4.7 temos um homomorfismo induzido $x \longmapsto x^p$ de $G/G_2 \longrightarrow G_2/G_3$ e $G_2 = G^p$, também por este lema, existem $x \in G$ e $y \in G_3$ tais que $g = x^p y$.

Defina $H = \langle G^p, x \rangle = \langle G_2, x \rangle$. Vimos que G_i *p.e.* G, para cada i, então, pelo Lema 2.4.3, H é *powerful*. Temos que $y \in G_3 = G_2^p$, então $g = x^p y \in \langle x^p, G_2^p \rangle = H^p$.

Agora temos dois casos, se $H \neq G$, então podemos aplicar hipótese de indução. Assim g é uma potência de um elemento de H, logo de G. E o teorema estaria satisfeito.

Se $H = G$, temos $G = \langle G_2, x \rangle = \langle \Phi(G), x \rangle = \langle x \rangle$, ou seja, G seria cíclico e, nesse caso, o teorema já é trivialmente satisfeito. □

Observe que essa última proposição é uma das características citadas no Teorema 2.1.7 para que um grupo seja dito *power abelian*. Em 2002, *L Wilson* [23], demonstrou em sua tese de doutordo que para p ímpar Ω_i é exatamente o conjunto das p^i-ésimas potência de elementos de G. No ano seguinte *L. Héthelyi* e *L. Lévai* [12], mostraram $|G : G^p| = |\Omega_1(G)|$, quando G é um p-grupo *powerful*. Dessa forma o fato de um p-grupo finito *powerful* ser *power abelian* é muito recente. Não entraremos em detalhes da demonstração desses resultados em nosso trabalho.

Juntando as características já apresentadas no Lema 2.4.7 com os últimos dois resultados demonstrados temos o próximo teorema que nos mostra um resumo das principais propriedades da p-série quando G é um p-grupo finito *powerful*.

Teorema 2.4.10. *Seja $G = \langle a_1, \ldots, a_d \rangle$ um p-grupo powerful, e coloque $G_i = P_i(G)$ para cada i.*

(*i*) *G_i p.e. G;*

(*ii*) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle$;*

(*iii*) *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$, para cada $k \geq 0$;*

(*iv*) *A aplicação $x \longmapsto x^{p^k}$ induz um homomorfismo de G_i/G_{i+1} sobre G_{i+k}/G_{i+k+1}, para cada i e k.*

Demonstração. (*i*) Esse item já foi mostrado no Lema 2.4.7.

(*ii*) Vamos provar por indução sobre i. Para $i = 1$, temos que $G_1 = G^{p^{1-1}} = \{x^{p^{1-1}} \mid x \in G\} = \langle a_1^{p^{1-1}}, \ldots, a_d^{p^{1-1}} \rangle = \langle a_1, \ldots, a_d \rangle = G$, assim o resultado é válido nesse caso.

Suponha por hipótese de indução que o resultado seja válido para todo inteiro j menor do que i, ou seja, $G_j = G^{p^{j-1}} = \{x^{p^{j-1}} \mid x \in G\} = \langle a_1^{p^{j-1}}, \ldots, a_d^{p^{j-1}} \rangle$. Pelo Lema 2.4.7, vimos que $G_{i+1} = G_i^p = P_2(G_i)$, para cada i, então sendo G_i *powerful* pela Proposição 2.4.9 segue que $G_{i+1} = G_i^p = \{x^p \mid x \in G_i\}$. Da mesma forma temos que $G_i = G_{i-1}^p = \{y^p \mid y \in G_{i-1}\}$.

Agora, por hipótese de indução $G_{i-1} = G^{p^{i-2}} = \{z^{p^{i-2}} \mid z \in G\} = \langle a_1^{p^{i-2}}, \ldots, a_d^{p^{i-2}} \rangle$. Assim temos $G_i = G_{i-1}^p = (G_{i-1})^p = (G^{p^{i-2}})^p = G^{p^{i-1}}$ e $G_{i-1}^p = \{y^p \mid y \in G_{i-1}\} = \{(z^{p^{i-2}})^p \mid z \in G\} = \{z^{p^{i-1}} \mid z \in G\} = G^{p^{i-1}}$.

Veja que $G_{i-1} = G^{p^{i-2}} = \langle a_1^{p^{i-2}}, \ldots, a_d^{p^{i-2}} \rangle$ e G_{i-1} é *powerful*, então pelo Lema 2.4.8 segue que $(G^{p^{i-2}})^p = \langle (a_1^{p^{i-2}})^p, \ldots, (a_d^{p^{i-2}})^p \rangle = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle = G^{p^{i-1}}$. Portanto, vale que $G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle$.

(*iii*) Juntando o item anterior com o item (*i*) do Lema 2.4.7, temos que $G_i = G_{i-1}^p = G^{p^{i-1}}$ e lembre que $G_i = P_i(G)$.

Fazendo $i = k + 1$ e sendo G_i *powerful* podemos colocar G_i no lugar de G, assim

$$P_{k+1}(G_i) = (G_i)_{k+1} = G_i^{p^k} = \{x^{p^k} \mid x \in G_i\} = \{(y^{p^{i-1}})^{p^k} \mid y \in G\} = \{y^{p^{k+i-1}} \mid y \in G\}.$$

E este último é igual a G_{k+i}. Portanto, $P_{k+1}(G_i) = G_i^{p^k} = G_{k+i}$, $k \geq 0$.

(iv) Vamos mostrar por indução sobre k. Para $k = 1$ é o Lema 2.4.7 aplicando $i = 1$. Então suponha que o resultado seja válido para um inteiro k e vejamos para $k + 1$.

Então por hipótese temos um homomorfismo de G_i/G_{i+1} sobre G_{i+k}/G_{i+k+1} induzido de $x \longmapsto x^{p^k}$. Agora pelo Lema 2.4.7 temos que $x \longmapsto x^p$ induz um homomorfismo sobrejetivo de G_{i+k}/G_{i+k+1} sobre G_{i+k+1}/G_{i+k+2}.

Considerando a composição desses dois homomorfismos temos que $x \longmapsto x^{p^{k+1}}$ induz um homomorfismo de G_i/G_{i+1} sobre G_{i+k+1}/G_{i+k+2}, como queríamos.

□

Corolário 2.4.11. *Se $G = \langle a_1, \ldots, a_d \rangle$ é um p-grupo powerful então $G = \langle a_1 \rangle \cdots \langle a_d \rangle$, ou seja, G é o produto de seus subgrupos cíclicos $\langle a_i \rangle$.*

Demonstração. Suponhamos que $G_l > G_{l+1} = 1$. Inicialmente vamos mostrar por indução sobre l que $G = \langle a_1 \rangle \cdots \langle a_d \rangle G_l$. Se $l = 1$, então $G = \langle a_1 \rangle \cdots \langle a_d \rangle G_1$ e $G_1 = G$, logo o resultado é trivial. Suponha por hipótese de indução que o resultado seja válido para $l - 1$, ou seja, que vale $G = \langle a_1 \rangle \cdots \langle a_d \rangle G_{l-1}$.

Observe que o grupo quociente G_{l-1}/G_l é abeliano, logo usando o teorema anterior, item (ii), temos que $G/G_l = \langle a_1 \rangle \cdots \langle a_d \rangle G_{l-1}/G_l = \langle a_1 \rangle \cdots \langle a_d \rangle \langle a_1^{p^{l-1}}, \ldots, a_d^{p^{l-1}} \rangle / G_l$.

Agora, por hipótese de indução temos que $G/G_l = \langle a_1 \rangle \cdots \langle a_d \rangle \langle a_1^{p^{l-1}} \rangle \cdots \langle a_d^{p^{l-1}} \rangle / G_l = \langle a_1 \rangle \cdots \langle a_d \rangle / G_l$. Dessa forma, podemos supor que $G = \langle a_1 \rangle \cdots \langle a_d \rangle G_l$.

Novamente pelo teorema anterior, item (ii), temos que $G_l = \langle a_1^{p^{l-1}}, \ldots, a_d^{p^{l-1}} \rangle$ e, pelo item (i), G_l *p.e.* G, isso significa que $[G_l, G] \leqslant G_l^p$. Mas lembre que $G_l^p = G_{l+1} = 1$, por hipótese, então $[G_l, G] = 1$. Isso significa que $G_l \leqslant Z(G)$ e então $G_l = \langle a_1^{p^{l-1}} \rangle \cdots \langle a_d^{p^{l-1}} \rangle$. Logo $G = \langle a_1 \rangle \cdots \langle a_d \rangle$, como queríamos. □

O corolário anterior é mais das características que os p-grupos *powerful* compartilham com p-grupos abelianos finitos. Assim como o teorema a seguir, que é um dos principais teoremas dessa seção.

Teorema 2.4.12. *Se G é um p-grupo powerful e $H \leqslant G$ então $d(H) \leq d(G)$.*

Demonstração. Vamos provar por indução sobre $|G|$. Se $|G| = 1$, o teorema é claro. Suponhamos por hipótese de indução que o resultado seja válido para todo p-grupo *powerful* de ordem estritamente menor do que a ordem de G. Seja $d(G) = d$ e $d(G_2) = m$, onde $G_2 = \Phi(G)$. Considere $H \leqslant G$.

Pelo Lema 2.4.7 temos que G_2 é *powerful*, então se considerarmos o subgrupo $K = H \cap G_2$, pela hipótese de indução temos que $d(K) \leq m = d(G_2)$. Agora, pelo item (ii) desse mesmo lema temos que a aplicação $\pi : G/G_2 \longrightarrow G_2/G_3$ dada por $x \longmapsto x^p$ é um epimorfismo. Como $G_2 = \Phi(G)$, segue que $d(G) = d = dim(G/G_2)$, como espaço vetorial sobre F_p.

Da mesma forma $G_3 = \Phi(G_2)$, assim $d(G_2) = m = dim(G_2/G_3)$. Com isso, pelo Teorema do Núcleo e da Imagem, $dim(Nuc(\pi)) = dim(G/G_2) - dim(G_2/G_3) = d - m$. Então $dim(Nuc(\pi) \cap HG_2/G_2) \leq d - m$.

Considerando a aplicação restrita $\pi' := \pi\big|_{HG_2/G_2} : HG_2/G_2 \longrightarrow \pi(HG_2/G_2)$ e aplicando novamente o Teorema do Núcleo e da Imagem, temos $dim(\pi(HG_2/G_2)) + dim(Nuc(\pi')) = dim(HG_2/G_2)$. Assim

$$dim(\pi(HG_2/G_2)) = dim(HG_2/G_2) - dim(Nuc(\pi) \cap HG_2/G_2) \geq e - (d-m) = m - (d-e),$$

onde $e = dim(HG_2/G_2)$.

Sejam $h_1, \ldots, h_e$ elementos de H tais que $HG_2 = \langle h_1, \ldots, h_e \rangle G_2$. Observe que $\Phi(K) \leqslant K^p$ e por definição $G_3 = \Phi(G_2) = G_2^p$, mas como $K = H \cap G_2$, temos $K \leqslant G_2$ e assim $K^p \leqslant G_2^p \leqslant \Phi(G_2) = G_3$. Logo $\Phi(K) \leqslant K^p \leqslant G_3$.

Desde que $\Phi(K) \leqslant K^p \leqslant G_3$, o subespaço de $K/\Phi(K)$ gerado pelas classes $h_1^p, \ldots, h_e^p$ tem dimensão pelo menos $dim(\pi(HG_2/G_2)) \geq m - (d-e)$. Pela hipótese de indução $d(K) \leq m$, então podemos encontrar $d - e$ elementos $y_1, \ldots, y_{d-e}$ de K tais que $K = \langle h_i^p, \ldots, h_e^p, y_1, \ldots, y_{d-e} \rangle \Phi(K)$. Então $K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{d-e} \rangle$ e assim

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

Lembre que a Regra de Dedekind nos diz que dados subgrupos A, B e C de um grupo G tais que $B \leqslant A$, então $A \cap (BC) = B(A \cap C)$. Como $H = H \cap HG_2$, aplicando essa regra temos

$$H = H \cap HG_2 = H \cap \langle h_1, \ldots, h_e \rangle G_2 = \langle h_1, \ldots, h_e \rangle (H \cap G_2) = \langle h_1, \ldots, h_e \rangle K.$$

Com isso, $H = \langle h_1, \ldots, h_e, y_1, \ldots, y_{d-e} \rangle$. Portanto, $d(H) \leq d(G)$. □

Agora vamos definir o posto de um grupo finito que é dado por

$$rk(G) = \sup\{d(H) \mid H \leqslant G\}.$$

O teorema anterior é muito importante no estudo da família de p-grupos finitos *powerful*, pois através dele e da definição de posto pode-se ver que $d(G) = rk(G)$.

O segundo teorema mais importante que discutiremos é uma espécie de recíproca para o teorema anterior, 2.4.12, pois nele veremos que em qualquer p-grupo de posto finito G, existe um subgrupo característico *powerful* de índice limitado em função do posto $rk(G)$. Antes precisaremos de uma preparação para essa "recíproca".

Definição 2.4.13. *Sejam G um p-grupo finito e r um inteiro positivo. Definimos $V(G,r)$ como sendo a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$.*

A imagem de qualquer homomorfismo de um p-grupo G aplicado em $GL_r(\mathbb{F}_p)$ é um p-grupo e todo p-subgrupo de $GL_r(\mathbb{F}_p)$ é conjugado a um subgrupo do grupo inferior uni-triangular $U_r(\mathbb{F}_p)$, esse grupo inferior uni-triangular é formado pelas matrizes A_{ij} de tamanho r e entradas em $\mathbb{F}_p$ que satisfazem $a_{ij} = 0$, se $j > i$, $a_{ij} = 1$, se $i = j$, e se $i > j$, a_{ij} pode ser qualquer elemento de $\mathbb{F}_p$. Dessa forma poderíamos igualmente definir $V(G,r)$ como sendo a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$.

Observe que um elemento g de G pertence a $V(G,r)$ se, e somente se, g age trivialmente em qualquer representação linear de G sobre qualquer $\mathbb{F}_p-$espaço vetorial de dimensão no máximo r.

Para $r \in \mathbb{N}$, defina o inteiro $\lambda(r)$ por

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

Lema 2.4.14. *(i) O grupo $U_r(\mathbb{F}_p)$ tem uma série, de comprimento $\lambda(r)$, de subgrupos normais, com quocientes abelianos elementares.*

(ii) Se G é um p-grupo finito, então $G/V(G,r)$ tem uma série com essas propriedade.

Demonstração. (i) Vamos provar por indução sobre r. Para $r = 1$, temos que $U_1(\mathbb{F}_p) = \mathbb{F}_p$ e $\lambda(1) = 1$, já que $\mathbb{F}_p$ é um p-grupo abeliano elementar. Assim o resultado é válido nesse caso.

Suponha por hipótese de indução que o resultado seja válido para qualquer $s < r$ e vejamos ser verdadeiro para r. Considere $s = \lfloor r/2 \rfloor$ e observe que dado $X \in U_r(\mathbb{F}_p)$ podemos reescrevê-lo da seguinte forma

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

com $A \in U_s(\mathbb{F}_p)$ e $C \in U_{r-s}(\mathbb{F}_p)$. Defina a aplicação, que é um homomorfismo, da seguinte forma

$$\begin{aligned}\varphi : U_r(\mathbb{F}_p) &\longrightarrow U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)\\ X &\longmapsto (A, C).\end{aligned}$$

Consideremos $K = Ker(\varphi)$ pela definição temos que $K = \{X \in U_r(\mathbb{F}_p) \mid \varphi(X) = (Id_s, Id_{r-s})\} = \{X \in U_r(\mathbb{F}_p) \mid A = Id_s \text{ e } C = Id_{r-s}\}$, com Id_s e Id_{r-s} são as matrizes identidades de tamanho s e $r-s$, respectivamente. Ou seja, os elementos de K são da forma

$$X = \begin{pmatrix} Id_s & 0 \\ B & Id_{r-s} \end{pmatrix}.$$

Com isso, temos que K é um p-grupo abeliano elementar. Pelo Primeiro Teorema do Isomorfismo $U_r(\mathbb{F}_p)/K \cong Im(\varphi) \leqslant U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)$.

Agora, pela hipótese de indução $U_s(\mathbb{F}_p)$ e $U_{r-s}(\mathbb{F}_p)$ possuem tais séries, então $Im(\varphi)$ também possui tal série. Pelo isomorfismo temos que $U_r(\mathbb{F}_p)/K$ possui uma série tal que seus quocientes são p-grupos abelianos elementares.

Vimos que K é um p-grupo abeliano elementar, dessa forma temos que $U_r(\mathbb{F}_p)$ possui uma série com essas propriedades, como queríamos.

(ii) Seja G um p-grupo finito e por definição $V(G, r)$ é a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$. Mas, sendo G finito, temos que essa intercessão é constituída por uma quantidade de núcleos, ou seja, $V(G, r) = \cap_{i=1}^{k} N_i$, onde $N_i = ker(\varphi_i)$ com $\varphi_i : G \to U_r(\mathbb{F}_p)$. E pelo Primeiro Teorema do Isomorfismo $G/N_i \cong Im(\varphi_i(G)) = H_i \leqslant U_r(\mathbb{F}_p)$.

Agora considere o homomorfismo

$$\begin{aligned}\psi : G &\longrightarrow G/N_1 \times \cdots \times G/N_k\\ g &\longmapsto (gN_1, \ldots, gN_k).\end{aligned}$$

Observe que $Ker(\psi) = \{g \in G \mid (gN_1, \ldots, gN_k) = (\overline{1}, \ldots, \overline{1})\} = \cap_{i=1}^{k} N_i = V(G, r)$. E, novamente pelo Primeiro Teorema do Isomorfismo temos que $G/V(G, r) \cong H_1 \times \cdots \times H_k \leqslant U_r(\mathbb{F}_p) \times \cdots \times U_r(\mathbb{F}_p)$.

Pelo item anterior temos que cada $U_r(\mathbb{F}_p)$ possui uma série de comprimento $\lambda(r)$ onde cada quociente é abeliano elementar, então, pelo isomorfismo, $G/V(G, r)$ também possui tal série.

$\square$

Proposição 2.4.15. *Sejam G um p-grupo finito e r um inteiro positivo. Coloque $V = V(G,r)$ e sejam $W = V$ se $p > 2$ ou $W = V^2$ se $p = 2$. Se $N \lhd G$, $d(N) \leq r$, e $N \leqslant W$, então N p.e. W.*

Demonstração. Vamos mostrar por indução sobre a ordem de N. Se $|N| = 1$, o resultado é claramente satisfeito. Suponha por hipótese de indução que o resultado seja válido para todo grupo de ordem estritamente menor do que $|N|$ e vejamos ser válido para a ordem de N.

Primeiro vamos supor que $p > 2$ e nesse caso $V = W$. Suponha por absurdo que $[N,V] \nleqslant N^p$. Pelo Lema 2.4.3, item (iv), podemos assumir que $N^p = 1$ e $|[N,V]| = p$. Como G é um p-grupo , então existe $M \lhd G$ tal que $[N,V] \leqslant M < N$ e $|N : M| = p$.

Sendo $N/[N,V]$ um p-grupo abeliano elementar, segue que $d(M/[N,V]) = d(N/[N,V]) - 1 \leq r - 1$, já que $|N : M| = p$ e $d(N) \leqslant r$. Também pelo fato de $[N,V]$ ter ordem p, temos que ele é cíclico, ou seja, possui apenas um gerador e isso acarreta que $d(M) \leq r$. Observe ainda que $M < N \leqslant V$, ou seja, $M < V$. Com isso, pela hipótese de indução aplicada a M, M *p.e.* V, ou seja, $[M,V] \leqslant M^p = 1$.

Assim $[M,N] \leqslant [M,V] = 1$ e isso significa que os elementos de M comutam com os de N, ou seja, $M \leqslant Z(N) \leqslant N$. Mas sendo N/M um grupo cíclico e $M \leqslant Z(N)$, temos que N é abeliano e assim é um $\mathbb{F}_p$−espaço vetorial de dimensão no máximo r.

Agora, observamos que $g \in V(G,r)$ se, e somente se, g age trivialmente em toda representação linear de G sobre qualquer $\mathbb{F}_p$−espaço vetorial de dimensão no máximo r. Em particular, age trivialmente em N. Então $[N,V] = 1$, o que é um absurdo, já que supomos $|[N,V]| = p$. Portanto, nesse caso, N *p.e.* $V = W$.

Para o outro caso, faremos de maneira análoga. Considere $p = 2$ e, assim, $W = V^2$. Suponha por absurdo que N não é *powerfully embedded* em W. Da mesma forma que antes, pelo Lema 2.4.3, podemos assumir que $N^4 = 1$ e $|[N,W]| = 2$.

Considerando $x, y \in N$, lembre que $(xy)^2 = x^2y^2[y,x]^y$. Como $N \leqslant W$, podemos dizer que qualquer produto de quadrados em N é congruente a um quadrado módulo $[N,W]$. Segue daí que $(N^2)^2 = 1$, pois se elevamos ao quadrado novamente teremos elementos de N^4 e $[N,W]^2$, mas ambos são triviais.

Veja que também ocorre $[x^2,y] = [x,y]^2[[x,y],x]$. Mas $[[x,y],x] = 1$, pois $[[N,W],N] < N$ e assim $|[[N,W],N]| = 1$. Então $[x^2,y] = [x,y]^2 \in [N,N]^2 \leqslant [N,W]^2 = 1$. Como $[x^2,y] \in [N^2,N]$ segue que $[N^2,N] = 1$, ou seja, $N^2 \leqslant Z(N)$.

Agora N/N^2 é um $\mathbb{F}_p$−espaço vetorial de dimensão no máximo r, pois nesse quociente todo elemento possui ordem 2 e isso o torna abeliano. Assim $dim(N/N^2) = dim(N/\Phi(N)) = d(N) \leq r$, por hipótese. Isso acarreta que $[N,V] \leqslant N^2$.

Consequentemente, para $a \in N$ e $v \in N$, podemos escrever $[a,v] = b$, para algum

$b \in N^2$ e com isso temos $a^v = ab$. Mas $(a^v)^2 = (a^2)^v = (ab)^2 = a^2b^2[b,a]$. Temos que $b^2 = 1$, pois $b \in N^2$ e $(N^2)^2 = 1$, e também $[b,a] = 1$, pois $N^2 \leqslant Z(N)$ e assim $[N^2, N] = 1$. Assim podemos reescrever essa igualdade da seguinte forma $(a^2)^v = a^2$, ou seja, $[a^2, v] = 1$. Isso acarreta que $[N^2, V] = 1$.

Dessa forma, observe que $[N, V, V] \leqslant [N^2, V] = 1$. Assim pela Fórmula de Compilação de Hall temos $[N, W] = [N, V^2] \leqslant [N, V]^2[N, V, V] \leqslant (N^2)^2[N, V, V] = 1$, pelo que vimos acima. Então $[N, W] = 1$, o que é um absurdo, já que supomos $|[N, W]| = |[N, V^2]| = 2$. Portanto, N *p.e.* $W = V^2$. □

Para terminar essa seção vamos demonstrar o outro teorema que citamos ser de suma importância, pois eles nos mostra qual subgrupo de um p-grupo de posto finito é *powerful*. Ou seja, uma maneira de encontrar um subgrupo *powerful*, que também veremos ser característico. Lembre-se que para um dado $r \in \mathbb{N}$ definimos o inteiro $\lambda(r)$ como sendo um inteiro que satisfaz $2^{\lambda(r)-1} < r \leq 2^{\lambda(r)}$.

Teorema 2.4.16. *Seja G um p-grupo finito de posto r. Então G possui um subgrupo powerful característico de índice no máximo $p^{r\lambda(r)}$, se p é ímpar ou $2^{r+r\lambda(r)}$ se $p = 2$.*

Demonstração. Considere $V = V(G, r)$. Pelo Lema 2.4.14, $G/V(G, r)$ possui uma série de subgrupos normais com comprimento no máximo $\lambda(r)$, onde os quocientes são abelianos elementares. Olhando agora para G temos uma série $V \leqslant N_1 \leqslant \ldots \leqslant N_s = G$, com $s \leq \lambda(r)$ e N_i/N_{i+1} é um p-grupo abeliano elementar.

Por hipótese G tem posto r, então cada um desses fatores tem ordem no máximo p^r, pois $d(N_i) \leq d(G) = r$. Com isso $|G : V| \leq p^{r\lambda(r)}$.

Para o caso em que $p > 2$, veja que pela definição de V, temos que ele é característico em G, logo $V \lhd G$. Pela hipótese de G ter posto r, temos que $d(V) \leq r$. Aplicando a proposição anterior temos que V *p.e.* V e isso significa que V é *powerful*. Portanto, se $p > 2$, V é um subgrupo caraterístico *powerful* de índice no máximo $p^{r\lambda(r)}$.

Agora suponha que $p = 2$. Primeiro observe que V^2 é característico em V, de fato, por definição $V^2 = \langle v^2 \mid v \in V \rangle$ e dado ϕ um automorfismo de V temos que $\phi(v^2) = (\phi(v))^2$ e este é um gerador em V^2, pois $\phi(v) \in V$. Com isso V^2 é característico em G e então $V^2 \lhd G$. Também temos que $d(V^2) \leq r$ e novamente pela proposição anterior temos que V^2 *p.e.* V^2, ou seja, V^2 é *powerful*.

Para terminar veja apenas que $|G : V^2| = |G : V||V^2 : V| \leq 2^{r\lambda(r)} \cdot 2^r = 2^{r+r\lambda(r)}$, pois $|V : V^2|$ também tem ordem no máximo 2^r. Portanto, nesse caso, o subgrupo característico *powerful* de índice no máximo $2^{r+r\lambda(r)}$ de G que existe é V^2. □

2.5 p-grupos *potent*

Em 1969, *D. Arganbright* publicou um trabalho, [1], onde ele demonstrou que se G é um p-grupo, com p ímpar, satisfazendo $\gamma_{p-1}(G) \leqslant G^p$, então o subgrupo G^p é precisamente o conjunto das $p-$ésimas potências de G.

Isso levou a se definir mais uma classe de p-grupos finitos denominada *potent*, que foi introduzida por *J. González-Sánchez* e *A. Jaikin-Zapirain* através do artigo *On the structure of normal subgroups of potent p-groups* [8], em 2004. Todo o estudo feito nessa seção foi baseado neste artigo e também através da referência [1].

Definição 2.5.1. *Seja G um p-grupo finito. Dizemos que G é potent se $\gamma_{p-1}(G) \leq G^p$, para p ímpar, ou se $G' \leq G^4$, para $p = 2$.*

Observe que para $p = 2$ ou $p = 3$ as definições de p-grupo *powerful* e *potent* coincidem. Veja ainda que se G é um p-grupo *powerful*, então G é também *potent*.

O próximo lema reuni algumas características básicas sobre essa nova família de p-grupos finitos. Umas dessas propriedades é o fato de G^p poder ser tomado como conjunto. Em [8] isso foi denominado *p-powered*.

Teorema 2.5.2. *Seja G um p-grupo potent. Então valem as seguintes propriedades:*

(i) *Se $p = 2$, então $\gamma_{k+1}(G) \leqslant \gamma_k(G)^4$ e se $p > 2$, então $\gamma_{p-1+k}(G) \leqslant \gamma_{k+1}(G)^p$;*

(ii) *$\gamma_k(G)$ é potent, para todo $k \in \mathbb{N}$;*

(iii) *$\langle x, [G, G]\rangle$ é potent, para todo $x \in G$;*

(iv) *G^p é precisamente o conjunto das $p-$ésimas potências de G;*

(v) *Se N é um subgrupo normal de G, então G/N é potent.*

Demonstração. Seja G um p-grupo finito *potent*.

(i) Suponha $p = 2$ e mostraremos por indução sobre k que $\gamma_{k+1}(G) \leqslant \gamma_k(G)^4$. O caso base, quando $k = 1$, é trivial, já que por hipótese G é *potent*.

Suponha por hipótese de indução que o resultado seja válido para inteiro menor ou igual k, e vejamos para $k+1$. Pela definição da série central inferior e pela hipótese de indução, segue que $\gamma_{k+2}(G) = [\gamma_{k+1}(G), G] \leqslant [\gamma_k(G)^4, G]$.

Pelo Teorema 2.1.10, temos que $[\gamma_k(G)^4, G] \leqslant [\gamma_k(G), G]^4[G,_2 \gamma_k(G)]^2[G,_4 \gamma_k(G)]$. Considerando $k > 1$, temos $k \geq 2$. Assim

$$[G,_2 \gamma_k(G)]^2 \leqslant [G, \gamma_k(G), \gamma_2(G)] \text{ e } [G,_4 \gamma_k(G)] \leqslant \gamma_{k+3}(G).$$

Dessa forma, reescrevemos $\gamma_{k+2}(G) \leqslant \gamma_{k+1}(G)^4\gamma_{k+3}(G)$. Pelo Teorema 2.1.8, segue que $\gamma_{k+1} \leqslant \gamma_k(G)^4$, como queríamos.

Agora, suponha que $p > 2$ e vamos mostrar que $\gamma_{p-1+k}(G) \leqslant \gamma_{k+1}(G)^p$. Para isso vamos usar indução sobre k. Para $k = 0$ temos que $\gamma_{p-1}(G) \leqslant \gamma_1(G)^p = G^p$ e isso é válido pelo fato de G ser um p-grupo *potent*.

Suponha por hipótese de indução que o resultado seja válido para todo natural menor do que ou igual a k e vejamos que vale para $k + 1$. Pela hipótese de indução e pelo Teorema 2.1.10, temos

$$\gamma_{p-1+k+1}(G) = [\gamma_{p-1+k}(G), G] \leqslant [\gamma_{k+1}(G)^p, G] \leqslant [\gamma_{k+1}(G), G]^p[G,_p \gamma_{k+1}(G)].$$

Daí, $\gamma_{p-1+k+1}(G) \leqslant \gamma_{k+2}(G)^p\gamma_{p(k+1)+1}(G)$. Agora observe que

$$p(k+1)+1 > (p-1)(k+1)+1 = (p-1)k+p-1+1 > k+p-1+1 = p-1+k+1.$$

Assim $p(k + 1) + 1 \geq p - 1 + k + 2$. Logo $\gamma_{p(k+1)+1}(G) \leqslant \gamma_{p-1+k+2}(G)$. Com isso,

$$\gamma_{p-1+k+1}(G) \leqslant \gamma_{k+2}(G)^p\gamma_{p-1+k+2}(G) = \gamma_{k+2}(G)^p[\gamma_{p-1+k+1}(G), G].$$

Portanto, pelo Teorema 2.1.8, $\gamma_{p-1+k+1}(G) \leqslant \gamma_{k+2}(G)^p$, para $p > 2$.

(ii) Suponha que $p = 2$. Temos que $[\gamma_k(G), \gamma_k(G)] \leqslant [\gamma_k(G), G] = \gamma_{k+1}(G)$. Pelo item anterior temos que $\gamma_{k+1}(G) \leqslant \gamma_k(G)^4$. Portanto, por definição, segue que $\gamma_k(G)$ é *potent*, para $k \in \mathbb{N}$.

Suponha agora que $p > 2$. Pelas propriedades da série central inferior $\gamma_{p-1}(\gamma_k(G)) \leqslant \gamma_{k(p-1)}(G)$. Observe que $p - 1 > 1$, assim $(p - 1)(k - 1) > k - 1$, isto é, $(p - 1)(k - 1) + 1 > k$. Dessa forma

$$\gamma_{p-1}(\gamma_k(G)) \leqslant \gamma_{k(p-1)}(G) = \gamma_{p-1+(k-1)(p-1)}(G) \leqslant \gamma_{(k-1)(p-1)+1}(G)^p \leqslant \gamma_k(G)^p.$$

Portanto, por definição, também segue que $\gamma_k(G)$ é *potent*, para $k \in \mathbb{N}$.

(iii) Seja $x \in G$ arbitrário e considere $H = \langle x, [G, G]\rangle$. Primeiro vamos mostrar que $\gamma_k(H) \leqslant \gamma_{k+1}(G)$, para $k \geq 2$. Vamos fazer indução sobre k. Se $k = 2$, temos que $\gamma_2(H) = \langle [h_1, h_2] \mid h_1, h_2 \in H\rangle$ e olhando nos geradores vemos que $\gamma_2(H) \leqslant \gamma_3(G)$.

Suponha por hipótese de indução que o resultado vale para todo inteiro menor do que ou igual a k e vejamos a validade para $k+1$. Temos

$$\gamma_{k+1}(H) = [\gamma_k(H), H] \leqslant [\gamma_{k+1}(G), H] \leqslant [\gamma_{k+1}(G), G] = \gamma_{k+2}(G).$$

Assim $\gamma_k(H) \leqslant \gamma_{k+1}(G)$, para $k \geq 2$.

Suponha agora que $p = 2$, usando o item (i) desse teorema, obtemos

$$\gamma_2(H) \leqslant \gamma_3(G) \leqslant \gamma_2(G)^4 = [G, G]^4 \leqslant H^4.$$

Então H é *potent*. Agora, suponha que $p > 2$ e também usando o item (i) desse teorema, temos:

$$\gamma_{p-1}(H) \leqslant \gamma_p(G) = \gamma_{p-1+1}(G) \leqslant \gamma_2(G)^p = [G, G]^p \leqslant H^p.$$

Portanto, também nesse caso, H é *potent*.

(iv) Vamos fazer apenas o caso em que $p > 2$, pois para $p = 2$ foi feito na seção de *powerful*. Suponha que G seja um p-grupo não abeliano, pois caso contrário o item é trivialmente satisfeito. Vamos provar por indução sobre a ordem de G. Suponha que o resultado seja válido para todo grupo de ordem estritamente menor do que a ordem G.

Pela Fórmula de Hall podemos escrever $(x_1 \cdots x_k)^p = x_1^p \cdots x_k^p g_1^p \cdots g_t^p g$, onde $g_i \in \gamma_2(G)$, para $1 \leq i \leq t$, e $g \in \gamma_p(G)$. Aplicando o item (i) desse teorema, temos que $\gamma_p(G) \leqslant \gamma_2(G)^p$. Assim existem elementos $g_{t+1}, \ldots, g_r \in \gamma_2(G)$ tais que $g = g_{t+1}^p \cdots g_r^p$.

Agora, $\gamma_2(G)$ é estrito em G, então, pela hipótese de indução aplicada nesse subgrupo, temos que $g_1^p \cdots g_t^p g_{t+1}^p \cdots g_r^p = y^p$ para algum $y \in \gamma_2(G)$. Logo, $x_1^p \cdots x_k^p = (x_1 \cdots x_k)^p s^p$, onde $s = y^{-1}$ é um elemento em $\gamma_2(G)$.

Defina $x = x_1 \cdots x_k$ e considere $H = \langle \gamma_2(G), x \rangle$. Pelo item (iii) desse teorema, temos que $\gamma_{p-1}(H) \leqslant H^p$. Como G não é abeliano, então H também é estrito em G. Dessa forma, podemos novamente aplicar a hipótese de indução, agora em H. Logo, existe $h \in H$ tal que $x^p s^p = h^p$. Portanto, $x_1^p \cdots x_k^p = h^p$, como queríamos.

(v) Seja N um subgrupo normal de G e considere o grupo quociente G/N. Suponha primeiro que $p = 2$. Usando propriedade de subgrupo normal do Teorema 1.1.3, item (v), e a hipótese de que G é *potent*, temos que $[G/N, G/N] \leqslant G^4N/N = (G/N)^4$. Portanto, nesse caso, G/N é *potent*.

Suponha agora que $p > 2$. No Teorema 1.1.7 vimos $\gamma_k(G/N) = \gamma_k(G)N/N$, com $k \geq 1$. Então temos que $\gamma_{p-1}(G/N) = \gamma_{p-1}(G)N/N \leqslant G^pN/N$, pois G é *potent*. Assim $\gamma_{p-1}(G/N) \leqslant G^pN/N = (G/N)^p$ e portanto G/N é *potent*.

□

Na família de p-grupos *powerful*, definimos o que seria um subgrupo ser *powerfully embedded* em um p-grupo finito. De maneira semelhante também definimos isso para a família de *potent*.

Definição 2.5.3. *Sejam G um p-grupo finito e N um subgrupo normal. Dizemos que N é potently embedded em G se $[N, G] \leq N^4$ se $p = 2$ e $[N,_{p-2} G] \leqslant N^p$, se $p > 2$.*

Observe que quando $p = 2$ ou $p = 3$ dizer que um subgrupo é *potently embedded* ou que ele é *powerfully embedded* significa a mesma coisa.

Utilizando apenas essa definição pode-se verificar que um p-grupo finito é *potent* se, e somente se, ele é *potently embedded* em si próprio. Da mesma maneira como ocorria em *powerful*.

Na seção de p-grupos *powerful* fizemos uma versão para o próximo teorema, dessa forma faremos aqui apenas o caso em que p é ímpar.

Teorema 2.5.4. *Sejam N e M subgrupos potently embedded em G, um p-grupo finito. Então $[N^p, M] = [N, M]^p$.*

Demonstração. Vamos mostrar as duas inclusões. Considere o caso em que $p > 2$. Pelo Teorema 2.1.10, temos que $[N^p, M] \equiv [N, M]^p \pmod{[M,_p N]}$. Então

$$[N^p, M] \leqslant [N, M]^p[M,_p N] \leqslant [N, M]^p[M,_{p-2} G, N, N] \leqslant [N, M]^p[M^p, N, N],$$

pois M é *potently embedded* em G. Aplicando o Teorema 2.1.10 novamente, temos $[M^p, N] \equiv [M, N]^p \pmod{[N,_p M]}$. Como N também é *potently embedded* segue que

$$[N^p, M] \leqslant [N, M]^p[[M, N]^p[N,_p M], N] = [N, M]^p[[M, N]^p, N][[N,_p M], N]$$

$$\leqslant [N, M]^p[M, N]^p[N,_p M] = [N, M]^p[N,_p M] \leqslant [N, M]^p[N,_{p-2} G, M, M].$$

Assim, $[N^p, M] \leqslant [N, M]^p[N^p, M, M]$. Utilizando o Teorema 2.1.8 obtemos $[N^p, M] \leqslant [N, M]^p$, como queríamos. Agora vejamos a inclusão contrária. Novamente pelo Teorema 2.1.10, obtemos que $[N, M]^p \leqslant [N^p, M][M,_p N]$. Utilizando a inclusão que já foi demonstrada, segue que

$$[N, M]^p \leqslant [N^p, M][M^p, N, N] \leqslant [N^p, M][[M, N]^p, N] \leqslant [N^p, M][[M, N]^p, G].$$

Logo pelo Teorema 2.1.8 segue que $[N,M]^p \leqslant [N^p,M]$. Portanto, $[N^p,M]=[N,M]^p$.

□

O próximo teorema nos mostra que a propriedade de um subgrupo ser *potently embedded* se estende para alguns de seus subgrupos.

Teorema 2.5.5. *Seja G um p-grupo e M, N subgrupos potently embedded de G. Então vale que:*

(i) *MN é potently embedded em G.*

(ii) *$[N,G]$ é potently embedded em G.*

(iii) *N^p é potently embedded em G.*

Demonstração. *(i)* Considere M e N subgrupos *potently embedded*, então vale que $[N,_{p-2}G] \leqslant N^p$ e $[M,_{p-2}G] \leqslant M^p$, se $p>2$, ou $[N,G] \leqslant N^4$ e $[M,G] \leqslant M^4$. Usando propriedades de comutadores temos que:

$$[NM,_{p-2}G]=[N,_{p-2}G][M,_{p-2}G] \leqslant N^pM^p \leqslant (NM)^p$$

e

$$[NM,G]=[N,G][M,G] \leqslant N^4M^4 \leqslant (NM)^4.$$

Observe que MN é um subgrupo normal de G, pois M e N o são. Portanto, MN é *potently embedded* em G.

(ii) Para $p>2$ temos que: $[[N,G],_{p-2}G]=[[N,_{p-2}G],G] \leqslant [N^p,G]=[N,G]^p$ pelo fato de G ser *potently embedded* em si próprio e usando o Teorema 2.5.4.

Para $p=2$ temos que $[[N,G],G] \leqslant [N^4,G]$, pois N é *potently embedded* em G. Pelo Teorema 2.1.10 temos que $[N^4,G] \equiv [N,G]^4(\operatorname{mod}[G,_2N]^2[G,_4N])$. Assim

$$[[N,G],G] \leqslant [N,G]^4[G,_4N][G,_2N]^2 \leqslant [N,G]^4[N,G,G,G][N,G,G]^2.$$

Pelo Teorema 2.1.8, segue que $[[N,G],G] \leqslant [N,G]^4$. Portanto $[N,G]$ é *potently embedded* em G.

(iii) Utilizando o Teorema 2.5.4 repetidas vezes obtemos que $[N^p,_{p-2}G] \leqslant [N,_{p-2}G]^p$. Como N é *potently embedded* temos que $[N^p,_{p-2}G] \leqslant (N^p)^p$. Portanto, N^p é *potently embedded* em G.

Agora considere $p = 2$, pelo Teorema 2.5.4 temos que $[N^2, G] = [N, G]^2 \leqslant (N^2)^4$, pois N é *potently embedded*. Portanto, N^2 é *potently embedded*.

$\square$

Subgrupos dimensão de G

Considerando G um p-grupo finito podemos definir recursivamente os *subgrupos de dimensão de* G dados por

$$D_1(G) = G, \quad D_i(G) = D^p_{\lceil i/p \rceil}[D_{i-1}, G], \ i \geq 2.$$

Para simplificar a notação escreveremos $D_i(G) = D_i$, para todo $i \geq 1$. Observe que dessa forma essa série é uma sequência decrescente de subgrupos normais e satisfaz as propriedades $D_i^p \leqslant D_{ip}$ e $[D_{i-1}, G] \leqslant D_i$. E observe ainda que $D_i^p \leqslant D^p_{\lceil i+1/p \rceil} \leqslant D_{i+1}$ e isso acarreta que o quociente D_i/D_{i+1} é um p-grupo abeliano elementar. O Capítulo 11, de [4], possui outros detalhes e propriedades a respeito desses subgrupos, onde considera-se G um grupo qualquer.

Considerando que G seja um p-grupo finito *potent*, pode-se mostrar, usando a definição da sequência e indução sobre i, que D_i é *potently embedded* em G.

A respeito desses subgrupos demonstraremos, nessa seção, o teorema a seguir. Ele nos mostra como os termos dessa sequência se comportam quando G é um p-grupo *potent*. Nele veremos que cada termo dessa série é reescrito como uma potência de outro termo. Porém, no próximo capítulo mostraremos mais alguns resultados preliminares sobre esses subgrupos em um p-grupo *potent*, que servirão de base para demonstração da definição de *power abelian* para essa família de p-grupos.

Teorema 2.5.6. *Suponha $n \in \mathbb{N}$ e $i = \lfloor \log_p n \rfloor$ e seja $1 \leq k \leq p$ tal que $(k-1)p^i < n \leq kp^i$. Se G é potent, então* $D_n = \begin{cases} D_k^{p^i}, 1 \leq k \leq p-2 \\ D_1^{p^{i+1}}, p-1 \leq k \leq p \end{cases}.$

Demonstração. Vamos mostrar por indução sobre n. Primeiro observe que para $n \in \mathbb{N}$, com $n \leq p-2$, o resultado é válido. De fato, se $n \leq p-2$, então $i = \lfloor \log_p n \rfloor = 0$ e seja $1 \leq k \leq p$ tal que $k-1 < n \leq k \Rightarrow n = k$. Como $i = 0$, então $p^i = 1$, assim $D_k^{p^i} = D_n^{p^0} = D_n$. Dessa forma o teorema vale para $n \leq p-2$.

Por indução sobre n, com $n \leq p$, é possível mostrar que $D_n = G^p\gamma_n(G)$. Usando isso, juntamente com a definição da série D_n e o fato de G ser *potent*, temos que $D_{p-1} = G^p = D_p$. Agora observe que se $n = p-1$, então $i = 0$ e $k = p-1$, assim vale o teorema já que $D_{p-1} = D_1^{p^{0+1}} = D_1^p = G^p$. E se $n = p$, então $i = 1$ e $k = 1$, assim $D_p = D_1^{p^1} = D_1^p = G^p$.

Dessa forma temos o teorema mostrado para todo natural $n \leq p$. Então tome $m \in \mathbb{N}$, com $m > p$ e suponha que o resultado seja válido para todo inteiro $n < m$. Vejamos sua validade para $n = m$.

Sejam $i = \lfloor \log_p m \rfloor$ e $1 \leq k \leq p$ tal que $(k-1)p^i < m \leq kp^i$. Por definição, temos que $D_m = D^p_{\lceil m/p \rceil}[D_{m-1}, G]$. Observe que $(k-1)p^{i-1} < \lceil m/p \rceil \leq kp^{i-1}$ e $\lceil m/p \rceil < m$. Então, por hipótese de indução,

$$D_{\lceil m/p \rceil} = \begin{cases} D_k^{p^{i-1}}, 1 \leq k \leq p-2 \\ D_1^{p^i}, p-1 \leq k \leq p \end{cases}.$$

Temos que $m - 1 < m$, então também podemos aplicar a hipótese de indução e assim temos

$$D_{m-1} = \begin{cases} D_k^{p^i} \text{ ou } D_{k-1}^{p^i}, 1 \leq k \leq p-2 \\ D_1^{p^{i+1}}, p-1 \leq k \leq p \end{cases}.$$

Pela cadeia dos subgrupos dimensão, temos que $D_{k-1} \geqslant D_k$, logo $D_k^{p^i} \leqslant D_{k-1}^{p^i}$. Assim podemos escrever

$$D_{m-1} = \begin{cases} \leqslant D_{k-1}^{p^i}, 1 \leq k \leq p-2 \\ D_1^{p^{i-1}}, p-1 \leq k \leq p \end{cases}.$$

Então $[D_{m-1}, G] \leqslant [D_{k-1}^{p^i}, G]$, se $1 \leq k \leq p-2$, ou $[D_{m-1}, G] = [D_1^{p^{i+1}}, G]$, se $p - 1 \leq k \leq p$.

Sabemos que $[D_k, G] \leqslant D_{k+1}$, então $[D_{k-1}^{p^i}, G] = [D_{k-1}, G]^{p^i} \leqslant D_k^{p^i}$, pelo Teorema 2.5.4. Também temos que $[D_1^{p^{i+1}}, G] \leqslant D_1^{p^{i+1}}$. Dessa forma,

$$D_m = \begin{cases} \leqslant (D_k^{p^{i-1}})^p D_k^{p^i} = D_k^{p^i}, 1 \leq k \leq p-2 \\ \leqslant (D_1^{p^i})^p D_1^{p^{i+1}} = D_1^{p^{i+1}}, p-1 \leq k \leq p \end{cases}.$$

Assim temos,

$$D_m = \begin{cases} \leqslant D_k^{p^i}, 1 \leq k \leq p-2 \\ \leqslant D_1^{p^{i+1}}, p-1 \leq k \leq p \end{cases}.$$

Como já temos que $D_k^{p^i} \leqslant D_m$ e vimos que $D_{p-1} = G^p = D_1^p = D_p$, segue que

$$D_m = \begin{cases} D_k^{p^i}, 1 \leq k \leq p-2 \\ D_1^{p^{i+1}} = (D_1^p)^{p^i} = D_k^{p^i}, p-1 \leq k \leq p \end{cases}.$$

□

Capítulo 3

Resultados principais sobre p-grupos *potent*

No capítulo anterior vimos que os p-grupos finitos regulares e os *powerful* são *power abelian*. Com isso em mente, um dos principais objetivos desse capítulo é verificar que isso também vale na família dos p-grupos *potent*. Lembre que um p-grupo finito é dito ser *potent* quando $[G,G] \leqslant G^4$, se $p = 2$, ou $\gamma_{p-1}(G) \leqslant G^p$, se $p > 2$.

Além de verificar a propriedade de ser *power abelian* na família dos p-grupos *potent*, também mostraremos uma limitação para classe de nilpotência dos subgrupos característicos $\Omega_i(G)$ desse grupo. Também veremos que, sob certas condições, um p-grupo *potent* possui um subgrupo *powerful*.

Dessa forma, na primeira seção veremos alguns lemas técnicos para um subgrupo normal de um p-grupo *potent*, bem como os resultados citados no parágrafo anterior. E na segunda seção mostraremos que um subgrupo normal de um p-grupo *potent* possui a estrutura *power abelian*. Todos os resultados deste capítulo foram obtidos por *J. González-Sánchez* e *A. Jaikin-Zapirain* no artigo *On the structure of normal subgroups of potent p-groups* [8].

3.1 Subgrupos normais de um p-grupo *potent*

Nesta seção mostraremos algumas relações importantes que ocorrem quando consideramos um subgrupo normal N em um p-grupo finito *potent* G. O primeiro teorema nos mostra que ou esse subgrupo normal N está contido em um subgrupo próprio *potent* ou vale a relação $[G,G]^{p^n} \leqslant [N^{p^i}, G^{p^s}]^{p^t}$, onde $n = i + s + t$.

Teorema 3.1.1. *Sejam G um p-grupo finito potent e N um subgrupo normal de G. Então uma das seguintes condições valem:*

(*i*) *Sejam $i, s, t \geq 0$ tais que $n = i + s + t$. Se $n \geq 1$, para p é ímpar, ou se $n \geq 2$, quando $p = 2$, então $[G, G]^{p^n} \leqslant [N^{p^i}, G^{p^s}]^{p^t}$.*

(*ii*) *Existe um subgrupo próprio potent T de G tal que N está contido em T.*

Demonstração. Vamos dividir o teorema em dois casos, no primeiro vamos supor que $[G, G]^{\mathbf{p}} \leqslant [N, G^{\mathbf{p}}]$, onde $\mathbf{p} = 4$, se $p = 2$, e $\mathbf{p} = p$, se p é ímpar, e dele mostraremos que vale o item (*i*) do teorema. Depois vamos supor que $[G, G]^{\mathbf{p}} \nleqslant [N, G^{\mathbf{p}}]$ e mostraremos que vale o item (*ii*) do teorema. Como só ocorre um desses casos o teorema estará demonstrado.

Para o primeiro caso, inicialmente mostraremos que $[G, G]^{\mathbf{p}} \leqslant [N, G]^{\mathbf{p}}$. Se $p = 2$, $\mathbf{p} = 4$, estamos supondo que $[G, G]^4 \leqslant [N, G^4]$. Pelo Teorema 2.1.10 temos que $[N, G^4] \equiv [N, G]^4 \pmod{[N,_2 G]^2[N,_4 G]}$. Assim,

$$[G, G]^4 \leqslant [N, G^4] \leqslant [N, G]^4[N,_2 G]^2[N,_4 G] \leqslant [N, G]^4[G,_2 G]^2[G,_4 G].$$

Usando o Teorema 2.5.2, item (*i*), podemos reescrever essa inclusão de subgrupos por $[G, G]^4 \leqslant [N, G]^4[G, G, G]^2[G, G, G, G]^4 = [N, G]^4\gamma_3(G)^2\gamma_4(G)^4$. Como a série central inferior é decrescente, temos que $\gamma_4(G) \leqslant \gamma_3(G)$ e então $\gamma_4(G)^4 \leqslant \gamma_3(G)^4$. Também temos que $\gamma_3(G)^4 \leqslant \gamma_3(G)^2$, então $[G, G]^4 \leqslant [N, G]^4\gamma_3(G)^2$. Novamente pelo Teorema 2.5.2, item (*i*), temos $\gamma_3(G)^2 \leqslant (\gamma_2(G)^4)^2$. Dessa forma, $[G, G]^4 \leqslant [N, G]^4([G, G]^4)^2$. Segue do Teorema 2.1.8 que $[G, G]^4 \leqslant [N, G]^4$.

Agora se $\mathbf{p} = p$, temos $[G, G]^p \leqslant [N, G^p]$. Como consequência da Fórmula de Hall, temos que $[N, G^p] \equiv [N, G]^p \pmod{[N,_p G]}$. Assim,

$$[G, G]^p \leqslant [N, G^p] \leqslant [N, G]^p[N,_p G] \leqslant [N, G]^p[G,_p G] = [N, G]^p\gamma_{p+1}(G).$$

Aplicando o Teorema 2.5.2, item (*i*), para o caso em que p é ímpar, temos $\gamma_{p+1}(G) = \gamma_{p-1+2}(G) \leqslant \gamma_3(G)^p$. Com isso

$$[G, G]^p \leqslant [N, G]^p\gamma_3(G)^p = [N, G]^p[G, G, G]^p.$$

Como $[G, G]$ e G são *potently embedded* em G, podemos aplicar o Teorema 2.5.4 e assim $[G, G, G]^p = [[G, G]^p, G]$. Segue do Teorema 2.1.8 que $[G, G]^p \leqslant [N, G]^p$. Assim se $[G, G]^{\mathbf{p}} \leqslant [N, G^{\mathbf{p}}]$ então $[G, G]^{\mathbf{p}} \leqslant [N, G]^{\mathbf{p}}$ e isso mostra o primeiro passo de indução da afirmação $[G, G]^{p^n} \leqslant [N, G]^{p^n}$, quando $p^n \geq \mathbf{p}$.

Suponhamos por hipótese de indução que $[G,G]^{p^n} \leqslant [N,G]^{p^n}$ e mostraremos a validade dessa relação para $n+1$. Temos que $[G,G]^{p^{n+1}} = ([G,G]^{p^n})^p \leqslant ([N,G]^{p^n})^p$. Agora pelo Corolário 1.1.15 temos que $([N,G]^{p^n})^p \equiv [N,G]^{p^{n+1}} \pmod{\gamma_2([N,G]^{p^n})^p}$. Assim temos,

$$[G,G]^{p^{n+1}} \leqslant ([N,G]^{p^n})^p \leqslant [N,G]^{p^{n+1}}\gamma_2([N,G]^{p^n})^p \leqslant [N,G]^{p^{n+1}}\gamma_2([N,G]^{p^n}) \leqslant$$

$$\leqslant [N,G]^{p^{n+1}}\gamma_2([G,G]^{p^n}) = [N,G]^{p^{n+1}}[[G,G]^{p^n},[G,G]^{p^n}] \leqslant [N,G]^{p^{n+1}}[[G,G]^{p^n},[G,G]^p] =$$
$$= [N,G]^{p^{n+1}}[[G,G]^{p^n},[G,G]]^p = [N,G]^{p^{n+1}}[[G,G]^{p^{n+1}},[G,G]] \leqslant [N,G]^{p^{n+1}}[[G,G]^{p^{n+1}},G].$$

Assim, temos $[G,G]^{p^{n+1}} \leqslant [N,G]^{p^{n+1}}[[G,G]^{p^{n+1}},G]$ e do Teorema 2.1.8 segue que

$$[G,G]^{p^{n+1}} \leqslant [N,G]^{p^{n+1}}.$$

Feito isso, agora podemos demonstrar que nesse caso vale o item (i), então consideremos i,s,t inteiros não-negativos tais que $i+s+t=n\geq 1$, se p é ímpar e $n\geq 2$, se p é par. Primeiro mostraremos que $[G,G]^{p^i} \leqslant [N^{p^i},G]$.

Para $\mathbf{p}=p$, temos

$$[G,G]^{p^i} \leqslant [N,G]^{p^i} \leqslant [N^{p^i},G][G,_2 N]^{p^i}[G,_p N]^{p^{i-1}}\cdots[G,_{p^i} N] \leqslant$$

$$\leqslant [N^{p^i},G][G,_2 G]^{p^i}[G,_p G]^{p^{i-1}}\cdots[G,_{p^i} G] \leqslant [N^{p^i},G][G,_2 G]^{p^i} = [N^{p^i},G][[G,G]^{p^i},G].$$

Pelo Teorema 2.1.8 segue que $[G,G]^{p^i} \leqslant [N^{p^i},G]$, se p é ímpar.

Para $\mathbf{p}=4$, temos

$$[G,G]^{p^i} \leqslant [N,G]^{p^i} \leqslant [N^{p^i},G][G,_2 N]^{p^i}[G,_p N]^{p^{i-1}}\cdots[G,_{p^i} N] \leqslant$$

$$\leqslant [N^{p^i},G][G,_2 G]^{p^i}[G,_p G]^{p^{i-1}}\cdots[G,_{p^i} G] \leqslant [N^{p^i},G][G,G,G]^{p^{i-1}} \leqslant$$
$$\leqslant [N^{p^i},G]([G,G]^{p^{i-1}})^4 = [N^{p^i},G]([G,G]^{p^{i-1}})^{p^2} = [N^{p^i},G]([G,G]^{p^i})^p.$$

Segue do Teorema 2.1.8 que $[G,G]^{p^i} \leqslant [N^{p^i},G]$, se $p=2$. Dessa forma, temos que $[G,G]^{p^i} \leqslant [N^{p^i},G]$. Agora vejamos que $[G,G]^{p^{i+s}} \leqslant [N^{p^i},G^{p^s}]$. Observe que $[G,G]^{p^{i+s}} = ([G,G]^{p^i})^{p^s} \leqslant ([N^{p^i},G])^{p^s}$. Assim precisamos ver que $[N^{p^i},G]^{p^s} \leqslant [N^{p^i},G^{p^s}]$.

Para $\mathbf{p}=p$,

$$[N^{p^i},G]^{p^s} \leqslant [N^{p^i},G^{p^s}][N^{p^i},_2 G]^{p^s}[N^{p^i},_p G]^{p^{s-1}}\cdots[N^{p^i},_{p^i} G] \leqslant$$

$$\leqslant [N^{p^i},G^{p^s}][G^{p^i},_2 G]^{p^s}[G^{p^i},_p G]^{p^{s-1}}\cdots[G^{p^i},_{p^s} G] \leqslant$$

$$\leqslant [N^{p^i}, G^{p^s}][[G,G]^{p^i}, G]^{p^s}[[G,G]^{p^i},_{p-1} G]^{p^{s-1}} \cdots [[G,G]^{p^i},_{p^s-1} G] \leqslant$$

$$\leqslant [N^{p^i}, G^{p^s}][G,G,G]^{p^{i+s}}[\gamma_p(G), G]^{p^{i+s-1}} \cdots [\gamma_{p^s}(G), G]^{p^i} \leqslant [N^{p^i}, G^{p^s}][G,G,G]^{p^{i+s}}.$$

Dessa forma temos $[G,G]^{p^{i+s}} \leqslant [N^{p^i}, G]^{p^s} \leqslant [N^{p^i}, G^{p^s}][[G,G]^{p^{i+s}}, G]$ e pelo Teorema 2.1.8 segue que $[G,G]^{p^{i+s}} \leqslant [N^{p^i}, G^{p^s}]$.

Para $\mathbf{p} = 4$, temos

$$[G,G]^{p^{i+s}} \leqslant [N^{p^i}, G]^{p^s}[N^{p^i},_2 G]^{p^s}[N^{p^i},_2 G]^{p^{s-1}} \cdots [N^{p^i},_{p^s} G] \leqslant$$

$$\leqslant [N^{p^i}, G^{p^s}][G^{p^i},_2 G]^{p^s}[G^{p^i},_2 G]^{p^{s-1}}[G^{p^i},_{p^2} G]^{p^{s-2}} \cdots [G^{p^i},_{p^s} G] \leqslant$$

$$\leqslant [N^{p^i}, G^{p^s}][G,_2 G]^{p^{i+s}}[G,_2 G]^{p^{i+s-1}}[G,_{p^2} G]^{p^{i+s-2}} \cdots [G,_{p^s} G]^{p^i} \leqslant$$

$$\leqslant [N^{p^i}, G^{p^s}][G,G,G]^{p^{i+s}} \leqslant [N^{p^i}, G^{p^s}][[G,G]^{p^{i+s}}, G].$$

Dessa forma, temos que $[G,G]^{p^{i+s}} \leqslant [N^{p^i}, G^{p^s}]$ e assim, nesse caso, $[G,G]^{p^{i+s}} \leqslant [N^{p^i}, G^{p^s}]^{p^t}$. Observe que supomos $[G,G]^{\mathbf{p}} \leqslant [N, G^{\mathbf{p}}]$ e mostramos que o primeiro item do teorema é válido. Agora suponhamos que $[G,G]^{\mathbf{p}} \nleqslant [N, G^{\mathbf{p}}]$ e mostraremos a validade do segundo item. Primeiro veremos que $[G,G]^{\mathbf{p}} = [G, G^{\mathbf{p}}]$. De fato, temos que G é *potent*, então G e G^p são *potently embedded* em G. Assim se $\mathbf{p} = p$, pelo Teorema 2.5.4 vale $[G,G]^p = [G, G^p]$. E se $\mathbf{p} = 4$, temos que $[G,G]^4 = ([G,G]^2)^2 = [G,G^2]^2 = [G,(G^2)^2] = [G,G^4]$.

Lembrando da definição dos subgrupos dimensão, temos que para $k = 1$, vale $D_k^{\mathbf{p}} = D_1^{\mathbf{p}} = G^{\mathbf{p}}$. Com isso, se $[G,G]^{\mathbf{p}} = [G, G^{\mathbf{p}}] \nleqslant [N, G^{\mathbf{p}}]$, então existe $k \geq 1$ tal que $[G, D_k^{\mathbf{p}}] \nleqslant [N, G^{\mathbf{p}}]$ e $[G, D_{k+1}^{\mathbf{p}}] \leqslant [N, G^{\mathbf{p}}]$.

Agora considere o conjunto $T = \{g \in G \mid [g, D_k^{\mathbf{p}}] \leqslant [N, G^{\mathbf{p}}]\}$. Vamos mostrar que $N \leqslant T$ e T é *potent*. Observe que pela escolha de k temos que T é um subgrupo próprio de G, pois caso $T = G$ teríamos que $[G, D_k^{\mathbf{p}}] \leqslant [N, G^{\mathbf{p}}]$ e isso é um absurdo já que estamos no caso em que $[G, D_k^{\mathbf{p}}] \nleqslant [N, G^{\mathbf{p}}]$.

Também temos que $N \subseteq T$. De fato, temos que $N \trianglelefteq G$, então vale que $[n,g] \in [N,G] \leqslant N$, para todo $g \in G$ e $n \in N$. Em particular, $D_k^{\mathbf{p}} \leqslant G$. Assim, se $\alpha \in D_k^{\mathbf{p}}$ então $[n, \alpha] \in [N, D_k^{\mathbf{p}}] \leqslant [N, G] \leqslant N$. Mas, pela sequência dos subgrupos dimensão, temos que $D_k^{\mathbf{p}} \leqslant D_1^{\mathbf{p}} = G^{\mathbf{p}}$, pois $k \geq 1$. Dessa forma, $[n, \alpha] \in [N, D_k^{\mathbf{p}}] \leqslant [N, G^{\mathbf{p}}] \leqslant N$. Com isso, se $n \in N$, então $n \in T$. Logo, $N \leqslant T$.

Como $N \trianglelefteq G$, segue que $N \trianglelefteq T$. Veja ainda que T é um subgrupo normal de G. De fato, dado $\alpha \in T$ e $g \in G$, arbitrários, temos que

$$[\alpha^g, D_k^{\mathbf{p}}] = [\alpha^g, (D_k^{\mathbf{p}})^g] = [\alpha, D_k^{\mathbf{p}}]^g \leqslant [N, G^{\mathbf{p}}]^g = [N^g, (G^{\mathbf{p}})^g] = [N, G^{\mathbf{p}}].$$

Então $\alpha^g \in T$, para todo $g \in G$, e isso significa que $T \trianglelefteq G$.

Agora, para terminar, vejamos que T é *potent*. Tome $x \in [T,T]$, se $p = 2$, e $x \in \gamma_{p-1}(T)$, se p é ímpar. Como G é *potent*, temos que $[T,T] \leqslant [G,G] \leqslant G^4$, se $p = 2$, ou $\gamma_{p-1}(T) \leqslant \gamma_{p-1}(G) \leqslant G^p$. Com isso $x \in [T,T] \leqslant G^4$ ou $x \in \gamma_{p-1}(T) \leqslant G^p$, ou seja $x \in G^{\mathbf{p}}$. Pelo Teorema 2.5.2, item (iv), temos que cada elemento de G^p pode ser escrito como potência de algum elemento de G. Dessa forma podemos escrever $x = a^p$, para algum $a \in G$.

Primeiro vamos mostrar que $[a, D_k^{\mathbf{p}}] \leqslant [a, D_k]^{\mathbf{p}}[N, G^{\mathbf{p}}]$. Para $\mathbf{p} = 4$, temos

$$[a, D_k^4] \leqslant [a, D_k]^4[a,_2 D_k]^2[a,_4 G_k] \leqslant [a, D_k]^4[G, D_k, D_k]^2[G,_4 D_k] =$$

$$= [a, D_k]^4[[G, D_k]^2, D_k][G,_4 D_k] \leqslant [a, D_k]^4[[G, D_k]^2, D_k][D_{k+1},_2 D_k, D_k] \leqslant$$

$$\leqslant [a, D_k]^4[D_{k+1}^4, D_k] \leqslant [a, D_k]^4[D_{k+1}^4, G] \leqslant [a, D_k]^4[N, G^4].$$

E para $\mathbf{p} = p$,

$$[a, D_k^p] \leqslant [a, D_k]^p[a,_2 D_k]^p[a,_p D_k] \leqslant [a, D_k]^p[G,_2 D_k]^p[G,_p D_k] =$$

$$= [a, D_k]^p[[G, D_k]^p, D_k][G, D_k,_{p-2} D_k, D_k] \leqslant [a, D_k]^p[D_{k+1}^p, D_k][D_{k+1},_{p-2} D_k, D_k] \leqslant$$

$$\leqslant [a, D_k]^p[D_{k+1}^p, D_k] \leqslant [a, D_k]^p[D_{k+1}^p, G] \leqslant [a, D_k]^p[N, G^p].$$

Observe que também temos $[a, D_k]^{\mathbf{p}} \leqslant [a^{\mathbf{p}}, D_k][N, G^{\mathbf{p}}]$. De fato, para $\mathbf{p} = 4$,

$$[a, D_k]^4 \leqslant [a^4, D_k][D_k,_2 a]^2[D_k,_4 a] \leqslant [a^4, D_k][D_k,_2 G]^2[D_k,_4 G] \leqslant$$

$$\leqslant [a^4, D_k][[D_k, G]^2, G][D_{k+1},_2 G, G] \leqslant [a^4, D_k][D_{k+1}^4, G] \leqslant [a^4, D_k][N, G^4].$$

E para $\mathbf{p} = p$,

$$[a, D_k]^p \leqslant [a^p, D_k][D_k,_2 a]^p[D_k,_p a] \leqslant [a^p, D_k][D_k,_2 G]^p[D_k,_p G] \leqslant$$

$$\leqslant [a^p, D_k][[D_k, G]^p, G][D_{k+1},_{p-2} G, G] \leqslant [a^p, D_k][D_{k+1}^p, G] \leqslant [a^p, D_k][N, G^4].$$

Assim, até agora temos que $[a, D_k^{\mathbf{p}}] \leqslant [a, D_k]^{\mathbf{p}}[N, G^{\mathbf{p}}] \leqslant [a^{\mathbf{p}}, D_k][N, G^{\mathbf{p}}]$. Agora precisamos ver que $[a^{\mathbf{p}}, D_k] \leqslant [N, G^{\mathbf{p}}]$. Para $\mathbf{p} = 4$, lembre que $x = a^4 \in [T,T]$ e usando o Lema dos Três Subgrupos, Lema 1.1.4, temos

$$[a^4, D_k] \leqslant [[T,T], D_k] = [T, T, D_k] \leqslant [D_k, T, T] \leqslant [D_k, G, T] \leqslant [D_k^4, T] \leqslant [N, G^4].$$

Então $[a, D_k^4] \leqslant [a^4, D_k][N, G^4] \leqslant [N, G^4]$ e isso acarreta que $a \in T$, logo $a^4 \in T^4$. Dessa forma $[T, T] \leqslant T^4$ e isso significa que, nesse caso, T é *potent*.

Para $\mathbf{p} = p$, lembre que $x = a^p \in \gamma_{p-1}(T)$ e usando o Teorema 1.1.6 temos

$$[a^p, D_k] \leqslant [\gamma_{p-1}(T), D_k] \leqslant [D_{k,p-1} T] \leqslant [D_{k,p-2} G, T] \leqslant [D_k^p, T] \leqslant [N, G^p].$$

Então $[a, D_k^p] \leqslant [a^p, D^k][N, G^p] \leqslant [N, G^p]$ e assim $a \in T$. Logo $a^p \in T^p$. Dessa forma $\gamma_{p-1}(T) \leqslant T^p$, ou seja, T é *potent*. Com isso, vemos que se $[G, G]^{\mathbf{p}} \nleqslant [N, G^{\mathbf{p}}]$, existe um subgrupo potent T de G tal que $N \leqslant T$. Assim, nesse caso vale o segundo item do teorema. $\square$

Esse último teorema é muito importante, pois, de certa forma ele nos mostra uma boa localização para qualquer subgrupo normal de um p-grupo *potent*. Isso será muito útil para a limitação dos expoentes de qualquer subgrupo normal e, consequentemente, dos subgrupos $\Omega_i(G)$ do grupo G, que é um dos subgrupos que desejamos estudar. A primeira consequência desse teorema é o seguinte lema, onde verificamos que $N^{p^{i+1}} = (N^{p^i})^p$, para todo $i \geq 1$, considerando as mesmas condições do teorema anterior.

Lema 3.1.2. *Sejam G um p-grupo potent e N um subgrupo normal de G. Então $(N^{p^i})^p = N^{p^{i+1}}$, para todo $i \geq 1$.*

Demonstração. Pela definição dos subgrupos $(N^{p^i})^p$ e $N^{p^{i+1}}$, verificamos a validade da inclusão $N^{p^{i+1}} \leqslant (N^{p^i})^p$. Para a outra, provaremos por indução sobre a ordem de G. Se $|G| = 1$, nada temos a fazer. Suponha que o resultado seja válido em todo grupo *potent* de ordem estritamente menor do que a ordem de G. Pelo Teorema 3.1.1, supondo que vale o item (ii), teremos $N \leqslant T$, onde T é um subgrupo próprio *potent* de G. Logo, pela hipótese de indução em T, $(N^{p^i})^p \leqslant N^{p^{i+1}}$.

Dessa forma, podemos supor que vale o item (i) do Teorema 3.1.1. Pelo Corolário 1.1.15, temos $(N^{p^i})^p \equiv N^{p^{i+1}} \pmod{\gamma_2(N^{p^i})^p}$. Assim

$$(N^{p^i})^p \leqslant N^{p^{i+1}}[N^{p^i}, N^{p^i}]^p \leqslant N^{p^{i+1}}[N^{p^i}, N^{p^i}] \leqslant N^{p^{i+1}}[G^{p^i}, G^{p^i}]$$

$$(N^{p^i})^p \leqslant N^{p^{i+1}}[G^{p^i}, G^{p^i}] \leqslant N^{p^{i+1}}[G^{p^i}, G^p] = N^{p^{i+1}}[G, G]^{p^{i+1}}.$$

Usando o Teorema 3.1.1 temos que $[G, G]^{p^{i+1}} \leqslant [N, G]^{p^{i+1}} \leqslant N^{p^{i+1}}$. Com isso, $(N^{p^i})^p \leqslant N^{p^{i+1}}[G, G]^{p^{i+1}} \leqslant N^{p^{i+1}}$, ou seja, $(N^{p^i})^p \leqslant N^{p^{i+1}}$. Portanto $(N^{p^i})^p = N^{p^{i+1}}$, para todo $i \geq 1$. $\square$

Teorema 3.1.3. *Sejam G um p-grupo potent e N um subgrupo normal de G. Então:*

(*i*) *Se* $p = 2$*,* $\gamma_3(N) \leqslant [N,G]^4 \cap [N^4,G]$ *e* $\gamma_4(N) \leqslant [N^4,G]^4$*; se* $p > 2$*,* $\gamma_p(N) \leqslant [N,G]^p \cap [N^p,G]$*.*

(*ii*) *Se* p *é ímpar,* $[N^p,N^p] \leqslant [N,N]^{p^2}$ *e se* $p = 2$*,* $[N^2,N^2] \leqslant [N,N]^4[N,N,N]^2 \leqslant N^8$*. Em particular,* N^p *é um* p*-grupo powerful.*

(*iii*) *A classe de nilpotência de* N *é no máximo* $e(N)(p-1)+1$*, se* p *é ímpar e* $\lfloor (e(N)+2)/2 \rfloor$*, se* $p = 2$*, onde* $e(N) = \log_p(exp(N))$*.*

Demonstração. Vamos provar por indução sobre a ordem de G. Primeiro vamos supor que vale o item (i) do Teorema 3.1.1. Então $[G,G]^{p^n} \leqslant [N^{p^i}, G^{p^s}]^{p^t}$, para $n = i+s+t \geq 1$, se p é ímpar, e $n \geq 2$, se $p = 2$. Vamos considerar $p = 2$ e provar os três itens do teorema.

(*i*) Pelo Teorema 2.5.2, item (i), temos que $\gamma_{k+1}(G) \leqslant \gamma_k(G)^4$, $p = 2$. Então $\gamma_3(N) \leqslant \gamma_3(G) \leqslant \gamma_2(G)^4 = [G,G]^{2^2}$. Pelo Teorema 3.1.1, $[G,G]^4 \leqslant [N^4,G]$ e $[G,G]^4 \leqslant [N,G]^4$. Dessa forma, $\gamma_3(N) \leqslant [N^4,G]$ e $\gamma_3(N) \leqslant [N,G]^4$, ou seja, $\gamma_3(N) \leqslant [N^4,G] \cap [N,G]^4$. Analogamente, temos que $\gamma_4(N) \leqslant \gamma_4(G) \leqslant \gamma_3(G)^p \leqslant (\gamma_2(G)^4)^4$, ou seja, $\gamma_4(N) \leqslant ([G,G]^4)^4 \leqslant [G,G]^{16}$. Pelo Teorema 3.1.1, para $n = 4$, temos $\gamma_4(N) \leqslant [G,G]^{16} \leqslant [N^4,G]^4$. Portanto $\gamma_3(N) \leqslant [N^4,G] \cap [N,G]^4$ e $\gamma_4(N) \leqslant [N^4,G]^4$.

(*ii*) Primeiro vamos mostrar que $[N^2,N^2] \leqslant [N,N]^4[N,N,N]^2 \leqslant N^8$ e assim teremos que N^2 é *powerful*. Sem perdas de generalidades podemos supor que $[N,N]^4$ $[N,N,N]^2 = 1$. Vejamos que $[N^2,N^2] \leqslant [N,N]^4[N,N,N]^2 = 1$. Observe que pela Fórmula de Hall e pelo item anterior temos que

$$\gamma_4(N) = [\gamma_3(N),N] \leqslant [[N,G]^4,N] \leqslant [[N,G],N]^4[N,_2[N,G]]^2[N,_4[N,G]] \leqslant$$

$$\leqslant [N,N]^4[N,N,N]^2[N,_4N] = \gamma_5(N).$$

Logo $\gamma_4(N) \leqslant \gamma_5(N)$, ou seja, $\gamma_4(N) = \gamma_5(N)$ e isso significa que $\gamma_4(N) = 1$. Novamente pela Fórmula de Hall temos

$$[N^2,N^2] \leqslant [N,N^2]^2[N^2,N,N] = [N,N^2]^2[[N,N]^2[N,_2N],N] =$$

$$= [N,N^2]^2[[N,N]^2,N][[N,_2N],N] = [N,N^2]^2[[N,N]^2,N] =$$

$$= [N,N^2]^2[N,N,N]^2[N,_2[N,N]] = [N,N^2]^2[N,N,N]^2 = [N,N^2]^2.$$

Também temos: $[N,N^2]^2 \leqslant ([N,N]^2[N,N,N])^2 \leqslant [N,N]^4[N,N,N]^2\gamma_2(H)^2$, onde $H = \langle [N,N]^2, [N,N,N] \rangle$. Observe que $\gamma_2(H)^2 \leqslant \gamma_2(H) \leqslant \gamma_5(N) = 1$.

Dessa forma $[N,N^2]^2 \leqslant [N,N]^4[N,N,N]^2 = 1$. Agora, desde que $[N,N] \leqslant N^2$, pelo lema anterior temos que $[N,N]^4 \leqslant N^8$. No item (i), deste teorema, vimos que $\gamma_3(N) \leqslant [N,G]^4$, logo $\gamma_3(N)^2 = [N,N,N]^2 \leqslant [N,G]^8$. Com isso $[N^2,N^2] \leqslant [N,N]^4[N,N,N]^2 \leqslant N^8[N,G]^8 \leqslant N^8 = (N^2)^4$ e então N^2 é *powerful*.

(iii) Primeiro, por indução sobre n, mostraremos que $\gamma_{n+1}(N) \leqslant [G,N]^{4^{n-1}}$. Para $n=1$, essa afirmação é claramente satisfeita. Suponha que o seja válido para todo inteiro $i \leq n$ e vejamos que vale para $n+1$. Temos

$$\gamma_{n+2}(N) = [\gamma_{n+1}(N),N] \leqslant [[G,N]^{4^{n-1}},N] \leqslant [[G,G]^{4^{n-1}},G] = [\gamma_2(G)^{4^{n-1}},G] \leqslant$$

$$\leqslant [(G^4)^{4^{n-1}},G] = [G^{4^n},G] = [G,G]^{4^n} \leqslant [N,G]^{4^n}.$$

Agora provaremos que a classe de nilpotência de N é limitada por $\lfloor (e(N)+2)/2 \rfloor$, onde $e(N) = \log_2(exp(N))$. Temos que $N^{exp(N)} = 1$ e $[N,G] \leqslant N$, assim $\gamma_{n+1}(N) \leqslant [G,N]^{4^{n-1}} \leqslant N^{4^{n-1}}$ e então $4^{n-1} \leq exp(N)$. Dessa forma,

$$2^{2n-2} \leq exp(N) \Rightarrow 2n-2 \leq \log_2(exp(N)) \Rightarrow n \leq (e(N)+2)/2.$$

Portanto, a classe de nilpotência de N é limitada por $\lfloor (e(N)+2)/2 \rfloor$, onde $e(N) = \log_2(exp(N))$.

Agora vamos supor que p é ímpar.

(i) Por hipótese, G é *potent*, de onde $\gamma_{p-1}(G) \leqslant G^p$. Daí temos que $[\gamma_{p-1}(G),G] \leqslant [G^p,G] = [G,G]^p$. Aplicando o Teorema 3.1.1, item (i), temos que $[G,G]^p \leqslant [N^p,G] \cap [N,G]^p$. Com isso $\gamma_p(N) \leqslant \gamma_p(G) \leqslant [G,G]^p \leqslant [N^p,G] \cap [N,G]^p$, ou seja, $\gamma_p(N) \leqslant [N^p,G] \cap [N,G]^p$.

(ii) Vamos mostrar que $[N^p,N^p] \leqslant [N,N]^{p^2}$. Sem perdas de generalidades podemos supor que $[N^p,N^p,G] = 1$. Primeiro veja que pela Fórmula de Hall temos $[N^{p^2},N] \leqslant [N^p,N]^p[N,_p N^p]$. Como $p \geq 3$ e pela suposição de $[N^p,N^p,G] = 1$, temos que $[N,_p N^p] \leqslant [G,_p N^p] \leqslant [N^p,N^p,G] = 1$. Assim $[N^{p^2},N] \leqslant [N^p,N]^p$. Também temos que $[N^p,N^p] \leqslant [N^p,N]^p[N^p,_p N]$. Agora veja que

$$[N^p,_p N] \leqslant [G^p,_{p-1} G,N] \leqslant [[G^p,G^p],N] \leqslant [[G,G]^{p^2},N] \leqslant$$

$$\leqslant [[G^{p^2},N],N] \leqslant [[G,G]^{p^2},N] = [[G,G]^{p^2},N] \leqslant [[G,N]^{p^2},N].$$

Assim temos,

$$[N^p, N^p] \leqslant [N^p, N]^p [N^p,_p N] \leqslant [N^p, N]^p [[G^{p^2}, N], N] \leqslant [N^p, N]^p [[G, N]^{p^2}, N] \leqslant$$

$$\leqslant [N^p, N]^p [N^{p^2}, N] \leqslant [N^p, N]^p.$$

Segue que $[N^p, N^p] \leqslant [N^p, N]^p$. Também temos

$$[N^p, N] \leqslant [N, N]^p [N,_p N] \leqslant [N, N]^p [\gamma_p(G), N] \leqslant [N, N]^p [\gamma_2(G)^p, N] \leqslant$$

$$\leqslant [N, N]^p [[N, G]^p, N]$$

e

$$[[N, G]^p, N] \leqslant [[N, G], N]^p [N,_p [N, G]] \leqslant [N, N]^p [[G, G]^p, N, N] \leqslant$$

$$\leqslant [N, N]^p [[N, G]^p, N, N].$$

Pelo Teorema 2.1.8, segue que $[[N, G]^p, N] \leqslant [N, N]^p$. Com isso $[N^p, N^p] \leqslant [N^p, N]^p \leqslant ([N, N]^p)^p = [N, N]^{p^2}$. Veja também que $[N^p, N^p] \leqslant [N, N]^{p^2} \leqslant N^{p^2} = (N^p)^p$, ou seja, N^p é *powerful*.

(iii) Para terminar, vejamos que a classe de nilpotência é no máximo $e(N)(p-2)+1$. Inicialmente mostraremos que $\gamma_{e(N)(p-2)+2}(N) \leqslant [G, G]^{p^{e(N)}}$. Usando o Teorema 2.5.2, item (i), várias vezes temos

$$\gamma_{e(N)(p-2)+2}(N) \leqslant \gamma_{e(N)p-2e(N)+2}(G) = \gamma_{p-1+(e(N)-1)p-2e(N)+3}(G) \leqslant$$

$$\leqslant (\gamma_{(e(N)-1)p-2e(N)+4}(G))^p = (\gamma_{p-1+(e(N)-2)p-2e(N)+5}(G))^p \leqslant (\gamma_{(e(N)-2)p-2e(N)+6}(G))^{p^2} \leqslant$$

$$\leqslant (\gamma_{(e(N)-2)p-2e(N)+6}(G))^{p^2} = (\gamma_{p-1+(e(N)-3)p-2e(N)+7}(G))^{p^2} \leqslant$$

$$\leqslant (\gamma_{(e(N)-3)p-2e(N)+8}(G))^{p^3} \ldots.$$

Como existem $e(N)$ vezes o número p, podemos fazer isso até a última vez que aparece. Com isso temos a seguinte fórmula de recorrência para $i < e(N) = \log_p(exp(N))$

$$(\gamma_{p-1+(e(N)-i)p-2e(N)+2i+1}(G))^{p^{i-1}} \leqslant (\gamma_{(e(N)-i)p-2e(N)+2i+2}(G))^{p^i} =$$

$$= (\gamma_{p-1+[e(N)-(i+1)]p-2e(N)+2(i+1)+1}(G))^{p^i}.$$

Para o caso em que $i = 1$ já foi visto. Então suponha válido para todo $j \leq i$ e vejamos que vale para $j+1$. De fato, pelo Teorema 2.5.2, item (i), temos

$$(\gamma_{p-1+[e(N)-(i+1)]p-2e(N)+2(i+1)+1}(G))^{p^i} \leqslant ((\gamma_{[e(N)-(i+1)]p-2e(N)+2(i+1+2)}(G))^p)^{p^i} =$$

$$= (\gamma_{p-1+[e(N)-(i+2)]p-2e(N)+2(i+2)+1}(G))^{p^{i+1}}.$$

Observe que se fizermos $i = e(N)-1$, temos

$$(\gamma_{p-1+[(e(N)-e(N)+1)]p-2e(N)+2(i+1)+1}(G))^{p^i} = (\gamma_{p-1+p-1}(G))^{p^{e(N)-2}} \leqslant$$

$$\leqslant \gamma_p(G)^{p^{e(N)-1}} = \gamma_{p-1+1}(G)^{p^{e(N)-1}} \leqslant \gamma_2(G)^{p^{e(N)}} = [G,G]^{p^{e(N)}}.$$

Dessa forma $\gamma_{e(N)(p-2)+2}(N) \leqslant [G,G]^{p^{e(N)}}$. Agora, pelo Teorema 3.1.1, item (i), temos que $[G,G]^{p^{e(N)}} \leqslant [N,G]^{p^{e(N)}}$ já que $e(N) \geq 1$, pois caso fosse igual a zero teríamos que $N=1$. Como $[N,G]^{p^{e(N)}} \leqslant N^{p^{e(N)}} = 1$, vemos que $\gamma_{e(N)(p-2)+1+1}(N) \leqslant [N,G]^{p^{e(N)}} \leqslant N^{p^{e(N)}} = 1$. Isso acarreta que a classe de nilpotência de N será no máximo $e(N)(p-2)+1$, como queríamos.

Agora vamos supor que o item (ii) do Teorema 3.1.1. Assim existe um subgrupo próprio T *potent* de G tal que N está contido em T. Aplicando a hipótese de indução em T, temos que o primeiro item desse teorema é dado por $\gamma_3(N) \leqslant [N,T]^4 \cap [N^4,T]$ e $\gamma_4(N) \leqslant [N^4,T]^4$, para $p=2$.

E para p ímpar $\gamma_p(N) \leqslant [N,T]^p \cap [N^p,T]$. Como $T \leqslant G$, temos que o item (i) vale nesse caso.

Observe que a demonstração dos itens seguintes são baseadas no primeiro item desse teorema, na Fórmula de Hall e no Teorema 2.1.8. Dessa forma esses itens também são válidos quando supomos o item (ii) do Teorema 3.1.1. Portanto o teorema está demonstrado em qualquer caso. □

Teorema 3.1.4. *Seja G um p-grupo potent.*

(i) *Se p é ímpar, então o expoente de $\Omega_i(G)$ é no máximo p^i. Em particular, a classe de nilpotência de $\Omega_i(G)$ é limitada por $i(p-2)+2$.*

(ii) *Se $p=2$, então o expoente de $\Omega_i(G)$ é limitado por 2^{i+1} e $\gamma_2(\Omega_i(G))^{2^i} = 1$. Em particular, a classe de nilpotência de $\Omega_i(G)$ é menor ou igual a $\lfloor (i+2)/2 \rfloor$.*

Demonstração. Vamos demonstrar o teorema por indução sobre $|G|$. Para $|G|=1$, o resultado é claro. Suponhamos por hipótese de indução que para todo grupo de ordem estritamente menor do que $|G|$ tem-se que o expoente de $\Omega_i(G)$ é limitado. Lembre que

$\Omega_i(G) \trianglelefteq G$ e G é um p-grupo *potent*, aplicando o Teorema 3.1.1 temos duas possibilidades. Uma possibilidade é que existe um subgrupo próprio *potent* T de G tal que $\Omega_i(G) \leqslant T$. Com isso temos que $\Omega_i(\Omega_i(G)) \leqslant \Omega_i(T) \leqslant T \leqslant G$. Porém vale que $\Omega_i(\Omega_j(G)) = \Omega_k(G)$, onde $k = \min\{i,j\}$, logo $\Omega_i(\Omega_i(G)) = \Omega_i(G)$. Dessa forma, $\Omega_i(G) \leqslant \Omega_i(T)$ e assim $\Omega_i(G) = \Omega_i(T)$.

Agora, como T é um subgrupo próprio de G vale a hipótese de indução em $\Omega_i(T)$, isso acarreta que $\Omega_i(G)$ tem expoente limitado por p^i, se $p > 2$, ou por 2^{i+1}, se $p = 2$. E nesse caso a parte da nilpotência é apenas uma aplicação do teorema anterior. Portanto, considerando que item (ii) do Teorema 3.1.1 é satisfeito, o resultado está provado.

A outra possibilidade é que $[G,G]^{p^n} \leqslant [\Omega_i(G)^{p^l}, G^{p^s}]^{p^t}$ para qualquer $l,s,t \geq 0$ tais que $l+s+t = n \geq 1$ se p é ímpar e $n \geq 2$ se $p = 2$. Para essa parte vamos separar os casos em que $p = 2$ e $p > 2$. Suponha inicialmente que $p > 2$, pelo caso particular do Corolário 1.1.15 temos

$$\Omega_1(G)^p \leqslant \gamma_2(\Omega_1(G))^p \gamma_p(\Omega_1(G)) \leqslant [G,G]^p \gamma_p(G).$$

Pelo Teorema 2.5.2, item (i), temos que $\gamma_p(G) \leqslant \gamma_2(G)^p$, com isso

$$\Omega_1(G)^p \leqslant [G,G]^p \gamma_p(G) \leqslant [G,G]^p \leqslant [\Omega_1(G)^p, G].$$

Segue do Teorema 2.1.8 que $\Omega_1(G)^p = \{1\}$ e o resultado é válido para $i = 1$. Suponha por hipótese de indução que $\Omega_j(G)^{p^j} = 1$ para todo natural $j \leq i$ e vejamos ser válido para $i+1$. Temos que $\frac{\Omega_{i+1}(G)}{\Omega_i(G)} \leqslant \Omega_1(\frac{G}{\Omega_i(G)})$. Como quociente de *potent* por um subgrupo normal herda essa propriedade, segue que $\frac{G}{\Omega_i(G)}$ é *potent*. Aplicando o caso base da segunda hipótese de indução temos que $\Omega_1(\frac{G}{\Omega_i(G)})^p = \{1\}$ e então $(\frac{\Omega_{i+1}(G)}{\Omega_i(G)})^p = \{1\}$. E por definição temos $\frac{\Omega_{i+1}(G)^p \Omega_i(G)}{\Omega_i(G)} = \{1\}$ e isso acarreta que $\Omega_{i+1}(G)^p \leqslant \Omega_i(G)$.

Agora, por hipótese dessa segunda indução, temos que $\Omega_i(G)^{p^i} = 1$ e pelo Lema 3.1.2 obtemos que

$$\Omega_{i+1}(G)^{p^{i+1}} = (\Omega_{i+1}(G)^p)^{p^i} \leqslant (\Omega_i(G))^{p^i} = 1.$$

Dessa forma $\Omega_{i+1}(G)^{p^{i+1}} = 1$, como queríamos.

Suponha que $p = 2$. Como G é finito, existe j tal que $[\Omega_i(G), G]^{2^{j+1}} = 1$. Observe que se $j < i$, então vale que $[\Omega_i(G), G]^{2^i} = 1$, pois se $j < i$, então $j + 1 \leq i$ e com isso $[\Omega_i(G), G]^{2^i} \leqslant [\Omega_i(G), G]^{2^{j+1}} = 1$.

Vejamos então o que ocorre quando $j \geq i$. Primeiro mostraremos que a ordem dos elementos da forma $[x,g]$, com $x \in G$, tal que $x^{2^i} = 1$, e $g \in G$, é limitada por 2^j. De fato, como consequência da Fórmula de Hall temos

$$[x,g]^{2^j} \equiv [x^{2^j},g] \pmod{[G,_2 G]^{2^{j-1}}[G,_{2^2} G]^{2^{j-2}}\cdots[G,_{2^j} G]}$$

$$\Rightarrow [x,g]^{2^j} \equiv [x^{2^j},g] \pmod{\gamma_3(G)^{2^{j-1}}\gamma_5(G)^{2^{j-2}}\cdots\gamma_{2^j+1(G)}}.$$

Pelos Teoremas 2.5.2, item (i), e 3.1.1 temos $\gamma_3(G) \leqslant \gamma_2(G)^4 \leqslant [\Omega_i(G),G]^4$. Provaremos, por indução sobre k, que também vale $\gamma_{2^k+1}(G) \leqslant [\Omega_i(G),G]^{4^{2^k-1}}$, para $k>1$. De fato, para $k=2$, temos

$$\gamma_{2^2+1}(G) = \gamma_5(G) \leqslant \gamma_4(G)^4 \leqslant \gamma_3(G)^{4^2} \leqslant \gamma_2(G)^{4^3} = [G,G]^{4^3} \leqslant [\Omega_i(G),G]^{4^3}.$$

Assim, $\gamma_{2^2+1}(G) \leqslant [\Omega_i(G),G]^{4^3}$. Suponha que o esse resultado seja válido para todo inteiro $n \leq k$ e vejamos para $k+1$. Vamos utilizar o Teorema 2.5.2, item (i), repetidas vezes para encontrar uma fórmula de recorrência e verificar o passo de indução. Temos

$$\gamma_{2^{k+1}+1}(G) = \gamma_{2^k+2^k+1}(G) \leqslant \gamma_{2^k+2^k}(G)^4 = \gamma_{2^k+(2^k-1)+1}(G)^4 \leqslant \gamma_{2^k+(2^k-1)}(G)^{4^2} =$$

$$= \gamma_{2^k+(2^k-2)+1}(G)^{4^2} \leqslant \gamma_{2^k+2^k-2}(G)^{4^3}.$$

Considerando n como sendo o número de vezes que repetiremos o processo temos a seguinte fórmula de recorrência: $\gamma_{2^k-(n-1)+1}(G)^{4^{n-1}} \leqslant \gamma_{2^{k+1}-(n-1)}(G)^{4^n}$, para $n \geq 1$. Aplicando 2^k vezes, temos

$$\gamma_{2^{k+1}-(2^k-1)+1}(G)^{4^{2^k-1}} = \gamma_{2^k+2}(G)^{4^{2^k-1}} \leqslant \gamma_{2^{k+1}+1}(G)^{4^{2^k}} = \gamma_{2^{k+1}-2^k+1}(G)^{4^{2^k}}.$$

E por hipótese de indução, segue que $\gamma_{2^k+1}(G) \leqslant [\Omega_i(G),G]^{4^{2^k-1}}$, e, com isso,

$$\gamma_{2^{k+1}+1}(G) \leqslant \gamma_{2^k+1}(G)^{4^{2^k}} \leqslant ([\Omega_i(G),G]^{4^{2^k-2}})^{4^{2^k}} = [\Omega_i(G),G]^{4^{2^{k+1}-1}}.$$

Agora nossa equivalência pode ser reescrita da seguinte forma:

$$[x,g]^{2^j} \equiv [x^{2^j},g] \pmod{([\Omega_i(G),G]^4)^{2^{j-1}}([\Omega_i(G),G]^{4^3})^{2^{j-2}}\cdots[\Omega_i(G),G]^{4^{2^j-1}}}$$

$$[x,g]^{2^j} \equiv [x^{2^j},g] \pmod{[\Omega_i(G),G]^{2^{j+1}}([\Omega_i(G),G]^{2^{j+1}})^{2^3}\cdots[\Omega_i(G),G]^{2^{2^{j+1}-2}}}.$$

Observe que todos os termos do segundo membro estão contidos em $[\Omega_i(G),G]^{2^{j+1}}$, pois seus expoentes são maiores ou iguais a 2^{j+1}. Logo $[x,g]^{2^j} \equiv [x^{2^j},g] \pmod{[\Omega_i(G),G]^{2^{j+1}}}$. Temos que $x^{2^i}=1$ e $j \geq i$, então $x^{2^j}=1$, e assim $[x^{2^j},g]=1$. Como $[\Omega_i(G),G]^{2^{j+1}}=1$, temos que a última equivalência nos dá que $[x,g]^{2^j}=1$.

O conjunto $X = \{[x,g] \mid x,g \in G \text{ e } x^{2^i} = 1\}$ é um conjunto de geradores de $[\Omega_i(G),G] = \langle [\alpha,g] \mid \alpha \in \Omega_i(G), g \in G\rangle$. Mostraremos por indução sobre o comprimento de um elemento h, onde h é uma palavra em $[\Omega_i(G),G]$, que $h^{2^j} = 1$. Observe que acabamos de fazer acima o primeiro passo dessa indução, ou seja, se o comprimento de $h \in [\Omega_i(G),G]$ é 1, então esse elemento elevado a 2^j é a identidade.

Suponhamos que o resultado seja válido para todo h cujo comprimento seja menor ou igual a l. Consideremos $x,y \in [\Omega_i(G),G]$ tais que o comprimento de x seja l e o de y seja 1, com $x^{2^j} = 1$ e $y^{2^j} = 1$. Pela Fórmula de Hall, temos

$$(xy)^{2^j} \equiv x^{2^j}y^{2^j} \pmod{\gamma_2([\Omega_i(G),G])^{2^j}\gamma_2([\Omega_i(G),G])^{2^{j-1}}\gamma_4([\Omega_i(G),G]^{2^{j-2}})\cdots\gamma_{2^j}([\Omega_i(G),G])}$$

Assim,

$$(xy)^{2^j} \equiv x^{2^j}y^{2^j} \pmod{\gamma_2([\Omega_i(G),G])^{2^{j-1}}\gamma_4([\Omega_i(G),G]^{2^{j-2}})\cdots\gamma_{2^j}([\Omega_i(G),G])}.$$

Observe que $\gamma_{2^k+2}(G) \leqslant \gamma_{2^k+1}(G) \leqslant [\Omega_i(G),G]^{4^{2^k-1}}$, com $k > 1$. Dessa forma, podemos reescrever o segundo membro apenas com potências maiores ou iguais a 2^{j+2} de $[\Omega_i(G),G]$ e com isso todo esse produto estará contido em $[\Omega_i(G),G]^{2^{j+1}}$. Como $x^{2^j} = 1$ e $y^{2^j} = 1$, segue que a equivalência é reescrita da seguinte forma $(xy)^{2^j} \equiv 1 \pmod{[\Omega_i(G),G]^{2^{j+1}}}$, ou seja, temos $(xy)^{2^j} = 1$. Com isso, mostramos que para qualquer comprimento de $h \in [\Omega_i(G),G]$, temos que $h^{2^j} = 1$ e isso mostra que $[\Omega_i(G),G]^{2^j} = 1$, quando $j \geq i$. Em particular, vale para i, ou seja, $[\Omega_i(G),G]^{2^i} = 1$ e assim segue que $\gamma_2(\Omega_i(G))^{2^i} = 1$. Agora precisamos ver que $\Omega_i(G)^{2^{i+1}} = 1$. Pelo Corolário 2.1.9, temos

$$\Omega_i(G)^{2^{i+1}} \leqslant \gamma_2(\Omega_i(G))^{2^{i+1}}\gamma_2(\Omega_i(G))^{2^i}\gamma_4(\Omega_i(G))^{2^{i-1}}\cdots\gamma_{2^{i+1}}(\Omega_i(G)).$$

De onde obtemos

$$\Omega_i(G)^{2^{i+1}} \leqslant \gamma_2(\Omega_i(G))^{2^i}\gamma_4(\Omega_i(G))^{2^{i-1}}\cdots\gamma_{2^{i+1}}(\Omega_i(G)). \tag{3.1}$$

Observe que $\gamma_{2^k}(\Omega_i(G)) \leqslant [\Omega_i(G),G]^{4^{2^k-2}}$. Vejamos isso por indução sobre k. Para $k = 1$, temos $\gamma_2(\Omega_i(G)) \leqslant [\Omega_i(G),G] = [\Omega_i(G),G]^{4^{2^1-2}}$ e assim vale o resultado no passo inicial. Suponha que o resultado seja válido para todo inteiro menor ou igual a k. Utilizando o Teorema 2.5.2, temos

$$\gamma_{2^{k+1}}(\Omega_i(G)) \leqslant \gamma_{2^{k+1}}(G) \leqslant \gamma_{2^k+(2^k-1)}(G)^4 \leqslant \gamma_{2^k+(2^k-2)}(G)^{4^2}.$$

Considerando n o número de vezes que faremos isso, temos a seguinte relação de recorrência $\gamma_{2^k+2^k-n+1}(G)^{4^{n-1}} \leqslant \gamma_{2^k+2^k-n}(G)^{4^n}$.

Para $n = 2^k$ e usando $\gamma_{2^k+1}(G) \leqslant [\Omega_i(G), G]^{4^{2^k-1}}$, temos

$$\gamma_{2^k+2^k-2^k+1}(G)^{4^{2^k-1}} = \gamma_{2^k+1}(G)^{4^{2^k-1}} \leqslant ([\Omega_i(G), G]^{4^{2^k-1}})^{4^{2^k-1}} = [\Omega_i(G), G]^{4^{2^{k+1}-2}}.$$

Então $\gamma_{2^k}(\Omega_i(G)) \leqslant [\Omega_i(G), G]^{4^{2^k-2}}$. Com isso, podemos reescrever a desigualdade 3.1 da seguinte forma

$$\Omega_i(G)^{2^{i+1}} \leqslant [\Omega_i(G), G]^{2^i}([\Omega_i(G), G]^{4^2})^{2^{i-1}} \ldots [\Omega_i(G), G]^{4^{2^{i+1}-2}}.$$

Todos os expoentes do segundo membro da desigualdade são maiores ou iguais a 2^i, com isso todos os termos são subgrupos de $[\Omega_i(G), G]^{2^i}$ e vimos que esse subgrupo é a identidade. Logo $\Omega_i(G)^{2^{i+1}} = 1$. Também nesse caso a parte da classe de nilpotência é uma aplicação do teorema anterior. □

Esse último teorema nos mostra uma propriedade muito interessante dos subgrupos característicos $\Omega_i(G)$ quando G é um p-grupo *potent*, que é a limitação tanto do expoente quanto da classe de nilpotência desses subgrupos.

Corolário 3.1.5. *Seja G um p-grupo potent. Então $\Omega_1(G^p)$ é abeliano e $\Omega_i(G^p)$ tem expoente menor ou igual a p^i.*

Demonstração. Primeiro mostraremos que $\Omega_1(G^p)$ é um p-grupo abeliano elementar. Para isso observemos inicialmente que $\Omega_1(G^p) \leqslant \Omega_2(G)^p$. De fato, considere $a \in \Omega_1(G^p)$ arbitrário, então podemos escrever $a = x_1 \cdot x_2 \cdots x_k$, com $x_i \in G^p$ e $x_i^p = 1$, para todo $i \in \{1, \ldots, k\}$. Por hipótese, G é *potent* e, então, G^p é exatamente o conjunto das p-potências de elementos de G, ou seja, $G^p = \{g^p \mid g \in G\}$. Dessa forma para cada fator x_i de a, vale $x_i = g_i^p$ para algum $g \in G$. E, assim, $x_i^p = (g_i^p)^p = 1$, ou seja, $g_i^{p^2} = 1$ onde $g_i \in G$ para cada i. Então podemos escrever que $a = x_1 \cdots x_k = g_1^p \cdots g_k^p$, com $g_i \in G$ e $g_i^{p^2} = 1$, para todo $i \in \{1, \ldots, k\}$, e isto significa que $a \in \Omega_2(G)^p$. Logo $\Omega_1(G^p) \leqslant \Omega_2(G)^p$. Sabendo disso, pelo Teorema 3.1.3 temos

$$[\Omega_1(G^p), \Omega_1(G^p)] \leqslant [\Omega_2(G)^p, \Omega_2(G)^p] \leqslant \Omega_2(G)^{p^2}, \text{ se } p > 2$$

e

$$[\Omega_1(G^p), \Omega_1(G^p)] \leqslant [\Omega_2(G)^p, \Omega_2(G)^p] \leqslant \Omega_2(G)^8, \text{ se } p = 2.$$

Com isso, em ambos os casos $[\Omega_1(G^p), \Omega_1(G^p)] \leqslant \Omega_2(G)^{\mathbf{p}p}$, onde $\mathbf{p} = 4$, se $p = 2$ ou $\mathbf{p} = p$, se $p > 2$. Mas, aplicando o teorema anterior em $\Omega_2(G)$, temos que seu expoente é limitado por p^2, se $p > 2$, ou por 2^3, se $p = 2$. Isso acarreta que $\Omega_2(G)^{\mathbf{p}p} = 1$, em qualquer caso. Logo, $[\Omega_1(G^p), \Omega_1(G^p)] = 1$ e isso significa que $\Omega_1(G^p)$ é abeliano. Para ver que é elementar tomando $a = x_1 \cdots x_k$, como inicialmente, temos que $a^p = (x_1 \cdots x_k)^p = x_1^p \cdots x_k^p$. Porém, $x_i \in G^p$ e $x_i^p = 1$, então $a^p = 1$. Portanto $\Omega_1(G^p)$ é abelino elementar.

Agora provaremos por indução sobre i que $\Omega_i(G^p)^{p^i} = 1$. Para $i = 1$, acabamos de mostrar. Suponhamos por hipótese de indução que para todo inteiro $j \leq i$ tenhamos que $\Omega_i(G^p)^{p^i} = 1$, onde G é um p-grupo *potent*. Lembre que $\Omega_{i+1}(G^p)/\Omega_i(G^p) \leqslant \Omega_1(\frac{G^p}{\Omega_i(G^p)}) = \Omega_1((\frac{G}{\Omega_i(G^p)})^p)$, essa última igualdade ocorre pelo fato de $\Omega_i(G^p) \leqslant G^p$. Temos que $G/\Omega_i(G^p)$ é *potent*, pois G o é e $\Omega_i(G^p) \trianglelefteq G$. podemos aplicar o primeiro passo da indução nesse grupo e então temos que $\Omega_1(G^p/\Omega_i(G^p))^p = 1$. Dessa forma, $(\Omega_{i+1}(G^p)/\Omega_i(G^p))^p = 1$, logo $\Omega_{i+1}(G^p)^p \leqslant \Omega_i(G^p)$. Pela hipótese de indução, temos que $\Omega_i(G^p)^{p^i} = 1$. Assim $(\Omega_{i+1}(G^p)^p)^{p^i} \leqslant \Omega_i(G^p)^{p^i} = 1$, ou seja, $\Omega_{i+1}(G^p)^{p^{i+1}} = 1$, como queríamos. □

Algumas vezes desejamos verificar se dois elementos do grupo satisfazem $(xy)^p = x^p y^p$, ou sob que condições ela ocorre. Dessa forma, é de se esperar a pergunta se isso vale quando consideramos subgrupos ao invés de elementos, e quais suas condições, ou seja, quando temos $(NL)^p = N^p L^p$, com N e L subgrupos normais. O próximo teorema nos mostra sob que condições isso ocorre em um p-grupo *potent*.

Corolário 3.1.6. *Sejam G um p-grupo potent e $N, L \leqslant G^2$ subgrupos normais de G. Então $(NL)^p = N^p L^p$.*

Demonstração. Sejam $N, L \trianglelefteq G$. Temos que $N \leqslant NL$ e $L \leqslant NL$, e, assim, $N^p \leqslant (NL)^p$ e $L^p \leqslant (NL)^p$. Com isso, temos a inclusão $N^p L^p \leqslant (NL)^p$.

Reciprocamente, primeiro observe que $NL/N^pL^p \leqslant \Omega_1(G^2/N^pL^p)$. De fato, dado $\overline{x} = xN^pL^p \in NL/N^pL^p$, então $x = nl$, com $n \in N \leqslant G^2$ e $l \in L \leqslant G^2$, com isso $xN^pL^p = nlN^pL^p = (nN^pL^p)(lN^pL^p)$ e veja que $(nN^pL^p)^p = n^pN^pL^p = N^pL^p$ e $(lN^pL^p)^p = N^pL^p$. Dessa forma, temos que xN^pL^p é escrito como produto de geradores do subgrupo $\Omega_1(G^2/N^pL^p)$.

Agora vejamos que $\Omega_1(G^2/N^pL^p)$ tem expoente limitado por p. Se $p = 2$, então temos que $G^2/N^pL^p = (G/N^pL^p)^2$ e sendo esse quociente p-grupo *potent*, podemos aplicar o corolário anterior e assim $\Omega_1(G^2/N^pL^p)^p = 1$. Se $p > 2$, então temos que $G^2/N^pL^p = G/N^pL^p$ e podemos aplicar o Teorema 3.1.4, pois o quociente também é *potent*. Logo $\Omega_1(G/N^pL^p)^p = 1$. Com isso, $(NL/N^pL^p)^p \leqslant \Omega_1(G^2/N^pL^p)^p = 1$, ou seja, $(NL/N^pL^p)^p = 1$. Assim $(NL)^p \leqslant N^pL^p$. Portanto, $(NL)^p = N^pL^p$. □

Para terminar essa seção vejamos o próximo teorema e pela demonstração podemos ver uma maneira de encontrar um subgrupo *powerful* dentro de um p-grupo *potent*.

Corolário 3.1.7. *Sejam G um p-grupo potent e N um subgrupo normal de G tal que $N \leqslant G^{\mathbf{p}}$. Então N é powerful.*

Demonstração. Considere o conjunto $T = \langle x \in G^2 \mid x^p \in N \rangle$. Mostraremos que $T \trianglelefteq G$ e que $T^p = N$. E pelo Teorema 3.1.3, item (ii) concluiremos que N será *powerful*, pois nesse teorema verificamos que se G é um p-grupo *potent* e N um subgrupo normal qualquer de G, então N^p é *powerful*.

Primeiro vejamos que $T \trianglelefteq G$. Dado $\alpha \in T$, podemos escrever $\alpha = x_1 \cdots x_k$, onde $x_i \in G^2$ e $x_i^p \in N$, para todo $i \in \{1, \ldots, k\}$. Considere $g \in G$, temos $\alpha^g = (x_1 \cdots x_k)^g = x_1^g \cdots x_k^g$. Observe que $x_i^g \in G^2$ e $(x_i^g)^p = (x_i^p)^g \in N$, pois ambos são subgrupos normais de G. Logo $\alpha^g \in T$ e, assim, $T \trianglelefteq G$.

Observe também que $T/N = \Omega_1(G^2/N)$. De fato, tome $\overline{\alpha} = \alpha N = x_1 \cdots x_k N = x_1 N \cdots x_k N$, com $x_i \in G^2$ e $x_i^p \in N$. Com isso, cada fator é um gerador de $\Omega_1(G^2/N)$ e obtemos a inclusão $T/N \leqslant \Omega_1(G^2/N)$. Por outro lado, tome $\overline{\alpha} \in \Omega_1(G^2/N)$. Podemos escrever $\overline{\alpha} = \overline{\alpha}_1 \cdots \overline{\alpha}_k$, de tal forma que $\overline{\alpha}_i = \alpha_i N \in G^2/N$ e $(\alpha_i N)^p = \overline{1}$, ou seja, $\alpha_i \in G^2$ e $\alpha_i^p \in N$. Assim $\overline{\alpha} = \overline{\alpha}_1 \cdots \overline{\alpha}_k = \alpha_1 \cdots \alpha_k N$, onde para cada i temos $\alpha_i \in T$, logo $\alpha = \alpha_1 \cdots \alpha_k \in T$ e então $\overline{\alpha} = \alpha N \in T/N$. Dessa forma, temos a outra inclusão. Logo $T/N = \Omega_1(G^2/N)$.

Pelas propriedades de p-grupos *potent* temos que G/N é ainda *potent*. Sabendo-se disso podemos mostrar que $\Omega_1(G^2/N)$ tem expoente no máximo p. De fato, se $p > 2$, então $G^2 = G$, assim $G^2/N = G/N$ e pelo Teorema 3.1.4 temos que $\Omega_1(G/N)^p = 1$. E se $p = 2$, temos que $G^2/N = (G/N)^2$ e pelo Corolário 3.1.5 temos que $\Omega_1((G/N)^p)^p = 1$. Com isso, $\Omega_1(G^2/N)$ tem expoente no máximo p, em ambos os casos.

Lembrando que vimos $T/N = \Omega_1(G^2/N)$, obtemos que $(T/N)^p \leqslant \Omega_1(G^2/N)^p = 1$. Assim $T^p \leqslant N$. Para ver a outra inclusão, tome $n \in N$, arbitrário. Como G é *potent*, então G^p é precisamente o conjunto das p-potências de G. Lembre que por hipótese $N \leqslant G^{\mathbf{p}}$. Com isso, se $p > 2$ existe $x \in G$ tal que $n = x^p \in N \leqslant G^p$. Como nesse caso $G^2 = G$, segue que $x \in T$ e logo $n = x^p \in T^p$, ou seja, $N \leqslant T^p$.

Caso $p = 2$, então $N \leqslant G^4 \leqslant G^2$ e assim existe $x \in G^2$ tal que $n = x^2 \in N$. Com isso, temos que $x \in T$, logo $n = x^2 \in T^2$, ou seja, $N \leqslant T^2$. Portanto $N = T^p$ e T^p é *powerful*, logo N é *powerful*. $\square$

3.2 Estrutura de subgrupos normais de um p-grupo *potent*

Nesta seção mostraremos que um p-grupo finito *potent* compartilha com os abelianos, regulares e *powerful* a propriedade de ser *power abelian*. Lembre que ela significa que nesses grupos são válidos os seguintes três itens, para todo inteiro i:

(i) $G^{p^i} = \{g^{p^i} \mid g \in G\}$;

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

(iii) $|G^{p^i}| = |G : \Omega_i(G)|$.

O primeiro teorema dessa seção nos mostra que subgrupos normais de um p-grupo *potent* é *p-powered*, ou seja, N^{p^i} é exatamente o conjunto das p^i-ésimas potências dos elementos de G, para todo $i \geq 0$.

Teorema 3.2.1. *Sejam G um p-grupo potent e $N \leqslant G^2$ um subgrupo normal de G. Então $N^{p^i} = \{n^{p^i} | n \in N\}$, para todo inteiro $i \geq 0$.*

Demonstração. Vamos provar por indução sobre as ordens de N e de G. Se $|N| = |G| = 1$, então o resultado é válido. Suponha por hipótese de indução que o teorema seja válido para todo grupo de ordem estritamente menor do que a ordem de N e de G. Considere $x, y \in N$. Se $p > 2$, temos que $x^p y^p \equiv (xy)^p \pmod{\gamma_2(N)^p \gamma_p(N)}$. Mas, vimos no Teorema 3.1.3, que $\gamma_p(G) \leqslant [N, G]^p$. Como $\gamma_2(N)^p \leqslant [N, G]^p$, segue que $x^p y^p \equiv (xy)^p \pmod{[N, G]^p}$.

Se $p = 2$, temos que $x^2 y^2 \equiv (xy)^2 \pmod{\gamma_2(N)^2 \gamma_2(N)}$. Seja $T = \langle g \in G \mid g^2 \in N \rangle$. Observe que $T/N = \Omega_1(G/N)$ e, pelo Teorema 3.1.4, $\Omega_1(G/N)$ possui expoente no máximo $2^2 = 4$, já que G/N é *potent*. Com isso, $(T/N)^4 = \Omega_1(G/N)^4 = 1$. Logo $T^4 \leqslant N$.

Temos também que $N \leqslant T^2$. De fato, tome $n \in N$, então $n \in G^2$, pois $N \leqslant G^2$. Mas, sendo G um p-grupo *potent*, segue que G^2 é exatamente o conjunto das 2-potências de G. Isso significa que existe $g \in G$ tal que $n = g^2 \in N$. Então $g \in T$ e assim $g^2 = n \in T^2$, ou seja, $N \leqslant T^2$. Por consequência da Fórmula de Hall, temos

$$[N, N] \leqslant [N, T^2] \leqslant [N, T]^2 [N,_2 T] \leqslant [N, T]^2 [T^2, T, T]. \tag{3.2}$$

E também

$$[T^2, T, T] \leqslant [[T, T]^2 \gamma_3(T), T] = [[T, T]^2, T] \gamma_4(T) \leqslant [T, T, T]^2 [T,_2 [T, T]] \gamma_4(T) \leqslant$$

$$\leqslant [T,T,T]^2\gamma_5(T)\gamma_4(T) = [T,T,T]^2\gamma_4(T).$$

Substituindo na desigualdade 3.2, segue que $[N,N] \leqslant [N,T]^2[T,T,T]^2\gamma_4(T)$. Aplicando o Teorema 3.1.3, item (i), temos $\gamma_3(T) \leqslant [T^4,G] \leqslant [N,G]$ e $\gamma_4(T) \leqslant [T^4,G]^4 \leqslant [N,G]^4$. Assim $[N,N] \leqslant [N,G]^2[N,G]^2[N,G]^4 = [N,G]^2$. Logo $x^2y^2 \equiv (xy)^2 \pmod{[N,G]^2}$. E, portanto, para qualquer primo, vale que $x^py^p \equiv (xy)^p \pmod{[N,G]^p}$.

Observe $[N,G]$ é um subgrupo estrito em N e também é subgrupo de G^2, então por hipótese de indução $[N,G]$ satisfaz o teorema. Isso nos dá que existe $c \in [N,G]$ tal que $x^py^p = (xy)^pc^p$.

Agora tome $H = \langle xy, [G,G]\rangle$. Temos dois casos possíveis para H, o primeiro é H ser um grupo cíclico e o segundo é ser um p-grupo *potent* estrito em G. Se H for um grupo cíclico, então H será abeliano e logo também satisfará o teorema.

Pelo Teorema 2.5.2, item (iii), temos H é *potent*. Com isso podemos ter que $H = G$ ou $H < G$. Se tivéssemos $H = G$, teríamos que $G/\Phi(G) = \langle xy, [G,G]\rangle/\Phi(G) \cong \langle xy\rangle$. Isso nos daria que $G/\Phi(G)$ seria cíclico, logo G também e assim seria abeliano. Porém estamos supondo que G não é abelino, pois caso fosse o teorema seria trivialmente satisfeito. Dessa forma, $H < G$.

Pela definição de H, $xy \in H$ e pelo fato de $x, y \in N$, com $N \trianglelefteq G$, obtemos que $xy \in N \cap H$. Também temos que $c \in N \cap H$, pois $c \in [N,G] \leqslant N$ e $[N,G] \leqslant [G,G] \leqslant H$. Como $N \cap H$ é um subgrupo normal H, que é um p-grupo *potent*, podemos aplicar a hipótese de indução e com isso o teorema também é aplicável a H. Então existe $z \in N \cap H$ tal que $(xy)^pc^p = z^p$. Dessa forma temos que $x^py^p = (xy)^pc^p = z^p$, onde $z \in N$ e assim $N^p = \{n^p \mid n \in N\}$. Vimos, no Teorema 3.1.3, que N^p é *powerful* e em grupos desse tipo vale que $N^{p^i} = \{n^{p^i} \mid n \in N\}$, para todo inteiro $i \geq 0$. Portanto o teorema está demonstrado. $\square$

Lema 3.2.2. *Sejam G um p-grupo potent e $x \in D_i$ tal que $x^p \in D_{ip+1}$. Então existe $w \in D_i$ tal que $w^p = 1$ e $xD_{i+1} = wD_{i+1}$.*

Demonstração. Vamos separar em dois casos, um quando $p > 2$ e o outro $p = 2$. Para o primeiro caso, considere $x \in D_i$ tal que $x^p \in D_{ip+1}$. Pela definição da série D_i, temos que $D_{i+1} \leqslant D_i$. Com isso, se $x \in D_{i+1}$, então podemos tomar $w = 1 \in D_i$, então $w^p = 1$ e $xD_{i+1} = D_{i+1} = wD_{i+1}$, como queríamos.

Suponhamos que $x \notin D_{i+1}$. Temos que $x^p \in D_{ip+1}$. Aplicando o Teorema 2.5.6 em D_{ip+1}, temos que $\lfloor \log_p(ip+1) \rfloor \leqslant i+1$, então existirá $j \geq i+1$ tal que $D_{ip+1} \leqslant D_j^p$. Assim $x^p \in D_j^p$ para algum $j \geq i+1$.

Mostraremos por indução inversa sobre j que o resultado é válido. Se j é grande o suficiente temos que $x^p = 1$, pois $D_j^p = 1$ e então poderíamos tomar $w = x \in D_i$ tal que

$w^p = x^p = 1$ e $xD_{i+1} = wD_{i+1}$. Suponhamos por hipótese de indução que se $z^p \in D^p_{j+1}$, então existe $w \in D_j$ tal que $w^p = 1$ e $zD_{j+1} = wD_{j+1}$. Temos que D_j é um subgrupo normal de G e ainda temos que $G^2 = G$, então vale o Teorema 3.2.1 aplicado a D_j. Com isso, existe $s \in D_j$ tal que $x^p = s^p$.

Por consequência da Fórmula de Hall, temos $(xs^{-1})^p \equiv x^p s^{-p} \pmod{\gamma_2(L)^p \gamma_p(L)}$, onde $L = \langle x, s \rangle$. Observe que $\gamma_2(L) = \langle [l_1, l_2] \mid l_1, l_2 \in L \rangle \leqslant [D_i, D_j]$ e $\gamma_p(L) \leqslant [[D_j, D_i],_{p-2} G] \leqslant [D_j,_{p-1} G]$.

Lembre que $x^p = s^p$, então $x^p s^{-p} = 1$. Assim a equivalência é reescrita da seguinte forma: $(xs^{-1})^p \equiv 1 \pmod{[D_i, D_j]^p [D_j,_{p-1} G]}$. Como D_j é *potently embedded* em G, segue que $[D_j,_{p-1} G] \leqslant [D^p_j, G]$, com isso temos a equivalência da seguinte forma $(xs^{-1})^p \equiv 1 \pmod{[D_j, G]^p [D^p_j, G]}$, assim $(xs^{-1})^p \equiv 1 \pmod{[D_j, G]^p}$. Agora, pela definição da série D_i, $[D_j, G] \leqslant D^p_{j+1}$ e isso nos dá que $(xs^{-1})^p \in D^p_{j+1}$.

Por hipótese de indução, existe $w \in D_j \leqslant D_{i+1} \leqslant D_i$, pois $j \geq i + 1$, tal que $w^p = 1$ e $xs^{-1}D_{j+1} = wD_{j+1}$. Observe que $s \in D_j \leqslant D_{i+1} \leqslant D_i$, então a igualdade é dada por $xs^{-1}D_{i+1} = wDi + 1$ e assim $xD_{i+1} = wD_{i+1}$. Portanto, nesse caso, existe $w \in D_i$ tal que $w^p = 1$ e $wD_{i+1} = xD_{i+1}$.

O caso em que $p = 2$ está demonstrado no Lema 3 de [12], já que nesse caso as definições de ser *powerful* e *potent* coincidem.

□

Proposição 3.2.3. *Sejam G um p-grupo potent e $N \leqslant G^2$ um subgrupo normal de G tal que $\Omega_1(G^2) \leqslant N$. Então $N^p \cap D_{pi} = (N \cap D_i)^p$ para cada inteiro $i \geq 1$.*

Demonstração. Verificaremos as duas inclusões. Por um lado, tome $\alpha \in (N \cap D_i)^p$. Observe que $N \cap D_i \leqslant N \leqslant G^2$. Assim, pelo Teorema 3.2.1, existe $\beta \in N \cap D_i$ tal que $\alpha = \beta^p$. Com isso, se $\beta \in N \cap D_i$, temos que $\alpha = \beta^p \in N^p$ e $\beta^p \in D^p_i \leqslant D_{pi}$. Logo, $\alpha \in N^p \cap D_{pi}$, ou seja, vale $(N \cap D_i)^p \leqslant N^p \cap D_{ip}$.

Reciprocamente, vejamos a outra inclusão por indução inversa sobre i. Pela hipótese de indução, podemos assumir que $N^p \cap D_{p(i+1)} \leqslant (N \cap D_{i+1})^p$. Seja $x \in N^p \cap D_{pi}$ e mostremos que $x \in (N \cap D_i)^p$. Por hipótese $N \leqslant G^2$, pelo Teorema 3.2.1, existe $y \in N$ tal que $x = y^p$. Vejamos que $x = y^p \in (N \cap D_i)^p$. Lembre que $x = y^p \in D_{pi}$.

Seja $j \leq i - 1$ tal que $y \in D_{i-j}$. Se $j \leq 0$, então $i - j \geq i$ e assim $D_{i-j} \leqslant D_i$, logo $y \in D_i$. Dessa forma $y \in N \cap D_i$ e, com isso, $y^p \in (N \cap D_i)^p$, como queríamos.

Agora, se $j \geq 1$, provaremos por indução sobre j. Assim assumiremos que se $y \in N \cap D_{i-(j-1)}$, então existirá $z \in N \cap D_i$ tal que $z^p = y^p$. Observe que $pi \geq p(i - j) + 1$. De fato, como $j \geq 1$ e $p \geq 2$, segue que

$$-jp \leq -2 \Rightarrow ip - jp + 1 \leq -2 + ip + 1 \Rightarrow p(i - j) + 1 \leqslant ip - 1 < ip \Rightarrow p(i - j) + 1 < ip.$$

Com isso, $y \in D_{i-j}$ tal que $y^p \in D_{ip} \leqslant D_{p(i-j)+1}$. Pelo lema anterior existe $w \in D_{i-j}$ tal que $w^p = 1$ e $yD_{i-j+1} = wD_{i-j+1}$. Mas, pela igualdade de classes temos que $y \in wD_{i-j+1}$ e assim existe $g \in D_{i-j+1}$ tal que $y = wg$.

Vejamos que $w \in N$. Se $p > 2$, temos que $G^2 = G$ e assim $\Omega_1(G^2) = \Omega_1(G)$. Como $w \in D_{i-j} \leqslant G$ e $w^p = 1$, segue que $w \in \Omega_1(G) \leqslant N$, por hipótese. Agora, se $p = 2$, primeiro veja que $w \in G^2$, pois $w = yg^{-1}$ e $y \in N \leqslant G^2$ e, também, $g \in D_{i-j+1} \leqslant D_2 = \Phi(G) = G^2$, já que $i - j + 1 \geq 2$. Como $w^p = 1$, segue que $w \in \Omega_1(G^2) \leqslant N$. Dessa forma, w e y são elementos de N. Logo $g \in N$.

Agora, vejamos que para qualquer primo p temos $y^p \equiv g^p \pmod{N^p \cap D_{i+1}^p}$. Primeiro suponhamos $p > 2$ e seja L o fecho normal de G gerado por w e y. Observe que $LD_{pi}/D_{pi} \leqslant \Omega_1(G/D_{pi})$. De fato, tome $\overline{\alpha} = \alpha D_{pi} \in LD_{pi}/D_{pi}$, com $\alpha \in LD_{pi}$. Assim podemos escrever $\alpha = ld$, onde $l \in L$ e $d \in D_{pi}$, e então $\alpha D_{pi} = ldD_{pi} = lD_{pi}$. Mas, como $l \in L$, segue que l é um produtório de elementos y e w, e possivelmente conjugados.

Lembre que $y^p \in D_{pi}$ e $w^p = 1 \in D_{pi}$. Então cada fator $\widetilde{l}$ de l satisfaz $(\widetilde{l}D_{pi})^p = \widetilde{l}^pD_{pi} = D_{pi}$. Dessa forma, lD_{pi} é um produtório de elementos $\widetilde{l}D_{pi} \in G/D_{pi}$ tal que $(\widetilde{l}D_{pi})^p = \overline{1}$. Logo $lD_{pi} \in \Omega_1(G/D_{pi})$.

Observe também que G/D_{pi} é *potent* e, pelo Teorema 3.1.4, $\Omega_1(G/D_{pi})$ tem expoente no máximo p. Assim $(LD_{pi}/D_{pi})^p \leqslant (\Omega_1(G/D_{pi}))^p$ e então $(LD_{pi})^p \leqslant D_{pi}$. Como $L^p \leqslant (LD_{pi})^p$, segue $L^p \leqslant D_{pi}$.

Pela Fórmula de Hall, $y^p = (wg)^p \equiv w^pg^p \pmod{\gamma_2(L)^p\gamma_p(L)}$. Mas $w^p = 1$, assim $y^p \equiv g^p \pmod{\gamma_2(L)^p\gamma_p(L)}$. Usando o Teorema 3.1.3 temos $\gamma_2(L)^p \leqslant [L^p, G]$ e $\gamma_p(L) \leqslant [L^p, G]$.

Observe que $[L^p, G] \leqslant N^p \cap D_{i+1}^p$, pois $[L^p, G] \leqslant L^p \leqslant N^P$, já que $L \trianglelefteq N$, e $[L^p, G] \leqslant [D_{pi}, G]$. Assim, nesse caso, $y^p \equiv g^p \pmod{N^p \cap D_{i+1}^p}$. Para o caso em que $p = 2$, veja que $y^2 = (wg)^2 = wwg[g, w]g = w^2g^2g^{-1}[g, w]g = g^2[g, w]^g$, ou seja, $y^2 = g^2[g, w]^g$. Porém, g^2 e $[g, w]$ são elementos de N^2, pois $g \in N$, logo $g^2 \in N^2$, e $[g, w] \in [N, N] \leqslant N^2$. Sendo $[N, N]$ um subgrupo normal, segue que $[g, w]^g \in N^2$. Temos ainda que $[g, w] \in D_{i+1}^2$. Dessa forma, $y^2 \equiv g^2 \pmod{N^2 \cap D_{i+1}^2}$.

Com isso, $y^p \equiv g^p \pmod{N^p \cap D_{i+1}^p}$, para qualquer primo p. Pelas propriedades da série D_i, temos que $D_{i+1}^p \leqslant D_{p(i+1)}$. Assim $y^p \equiv g^p \pmod{N^p \cap D_{p(i+1)}}$. Pela primeira hipótese de indução, temos que $N^p \cap D_{p(i+1)} \leqslant (N \cap D_{i+1})^p$. Como $N \cap D_{i+1}$ satisfaz o Teorema 3.2.1, existe $c \in N \cap D_{i+1}$ tal que $y^p = g^pc^p$.

Já vimos que $g \in N \cap D_{i-j+1}$ e também temos $c \in N \cap D_{i-j+1}$, pois $i - j + 1 \leq i + 1$ e assim $D_{i+1} \leqslant D_{i-j+1}$. Observe que o Teorema 3.2.1 também é aplicável a $N \cap D_{i-j+1}$. Logo, existe $y_1 \in N \cap D_{i-j+1}$ tal que $g^pc^p = y_1^p$. Como $y_1 \in N \cap D_{i-j+1}$, pela hipótese da segunda indução existe $z \in N \cap D_i$ tal que $z^p = y_1^p$. Dessa forma, temos $x = y^p = g^pc^p =$

$y_1^p = z^p$, com $z \in N \cap D_i$. Logo $x = z^p \in (N \cap D_i)^p$, ou seja, $N^p \cap D_{pi} \leqslant (N \cap D_i)^p$. Portanto, $N^p \cap D_{pi} = (N \cap D_i)^p$, para cada inteiro $i \geq 1$. □

O primeiro teorema visto nessa seção, Teorema 3.2.1, nos mostrou a validade do item (i) para um p-grupo *potent* ser *power abelian*, os próximos resultados que iremos demonstrar é o primeiro passo para verificar a validade do item (iii) dessa definição.

No primeiro capítulo definimos o que significa um conjunto possuir uma estrutura de R-módulo, onde R é uma anel. No próximo resultado usaremos essa estrutura para verificar que $|\Omega_1(N)| = |N : N^p|$, com N um subgrupo normal do p-grupo *potent* G contido em G^2, e nesse caso utilizaremos anel como sendo $\mathbb{F}_p[t]$.

Corolário 3.2.4. *Sejam G um p-grupo potent e $N \leqslant G^2$ um subgrupo normal de G tal que $\Omega_1(G^2) \leqslant N$. Então $|\Omega_1(N)| = |N/N^p|$.*

Demonstração. Primeiro lembre que consideramos a série D_i e vimos que D_i/D_{i_1} é um abeliano elementar. Com isso vamos considerar o seguinte grupo, que também é abeliano $L(G) = D_1/D_2 \oplus D_2/D_3 \oplus D_3/D_4 \oplus \cdots = \bigoplus_{i=1}^n D_i/D_{i+1}$, para algum $n \in \mathbb{N}$. Observe que tal n existe pelo fato de G ser finito e também pelo fato de que em algum momento $D_i = 1$.

Vamos definir a estrutura de $\mathbb{F}_p[t]-$módulo sobre $L(G)$, onde a operação é dada por $t(xD_{i+1}) = x^p D_{ip+1}$, com $x \in D_i$. Essa operação é estendida por linearidade para os demais elementos de $\mathbb{F}_p[t]$ da seguinte forma, dado um elemento $f(t) = \sum_{j=0}^n a_j t^j \in \mathbb{F}_p[t]$, onde cada $a_j \in \mathbb{F}_p$,

$$\begin{aligned} f(t)(xD_{i+1}) &= a_0(xD_{i+1}) + a_1 t(xD_{i+1}) + a_2 t^2(xD_{i+1}) + \cdots + a_n t^n(xD_{i+1}) \\ &= a_0 xD_{i+1} + a_1 x^p D_{ip+1} + a_2 t x^p D_{ip+1} + \cdots + a_n t^{n-1} x^p D_{ip+1} \\ &\vdots \\ &= a_0 xD_{i+1} + a_1 x^p D_{ip+1} + a_2 x^{p^2} D_{ip^2+1} + \cdots + a_n x^{p^n} D_{ip^n+1}, \end{aligned}$$

em cada entrada da soma direta. Observe que a relação $t(xD_{i+1}) \mapsto x^p D_{ip+1}$, com $x \in D_i$, está bem definida no sentido de $x^p D_{ip+1} \in D_{ip}/D_{ip+1}$, já que $x^p \in D_i^p \leqslant D_{ip}$.

Lembre que definimos que se M é um módulo finitamente gerado, $d_{\mathbb{F}_p[t]}(M)$ é o número mínimo de geradores de M, sobre o anel $\mathbb{F}_p[t]$. Usando o fato de ser finitamente gerado e a existência de uma base para M, pode-se mostrar que se $t^k M = 0$, para alguma k então valem as seguintes igualdades

$$d_{\mathbb{F}_p[t]}(M) = \log_p |M/tM| = \log_p |Ann_M(t)| = d_{\mathbb{F}_p[t]}(Ann_M(t)), \tag{3.3}$$

onde $Ann_M(t) = \{x \in M | tx = 0\}$. Veja que o $\mathbb{F}_p[t]-$módulo sobre $L(G)$ que definimos acima satisfaz essas igualdades, pois sendo G finito, teremos que $L(G)$ é finitamente gerado e assim qualquer submódulo também. Com isso, seja $K \trianglelefteq G$, arbitrário, e defina o seguinte submódulo

$$L(K) = (KD_2)/D_2 \oplus (KD_3) \cap D_2/D_3 \oplus (KD_4) \cap D_3/D_4 \oplus \cdots = \bigoplus_{i=0}^{l} (KD_{i+1}) \cap D_i/D_{i+1},$$

para algum natural $l \leq n$.

O subgrupo $\Omega_1(G^2)$ é normal em G. Assim podemos considerar o submódulo dado por $L(\Omega_1(G^2)) = \bigoplus(\Omega_1(G^2)D_{i+1}) \cap D_i/D_{i+1}$. Através das duas inclusões verifica-se que $L(\Omega_1(G^2)) = Ann_{L(G^2)}(t)$, onde $Ann_{L(G^2)}(t) = \{x \in L(G^2) \mid tx = 0\}$. De fato, considere $\widetilde{\alpha} \in L(G^2)$ tal que $t\widetilde{\alpha} = 0$, então $t\widetilde{\alpha} = t(\alpha_1 D_2, \ldots, \alpha_n D_{n+1}) = (\overline{1}, \ldots, \overline{1})$.

Em cada entrada temos $t\alpha_i D_{i+1} := \alpha_i^p D_{ip+1} = D_{ip+1}$, ou seja, $\alpha_i^p \in D_{ip+1}$. Com isso, $\alpha_i \in D_i$ tal que $\alpha_i^p \in D_{ip+1}$. Logo, pelo Lema 3.2.2, existe $w_i \in D_i$ tal que $w^p = 1$ e $\alpha_i D_{i+1} = w_i D_{i+1}$. Dessa forma, em cada entrada temos $w_i \in D_i$, $w_i^p = 1$ e $w_i \in G^2$, ou seja, $w_i \in (\Omega_1(G^2)D_{i+1}) \cap D_i$. Assim, cada entrada de $\widetilde{\alpha}$ satisfaz $\alpha_i D_{i+1} = w_i D_{i+1} \in (\Omega_1(G^2)D_{i+1}) \cap D_i/D_{i+1}$ e isso nos dá que $\widetilde{\alpha} \in L(\Omega_1(G^2))$. Logo $Ann_{L(G^2)}(t) \leqslant L(\Omega_1(G^2))$.

Por outro lado, dado $\widetilde{\alpha} = (\alpha_1 D_2, \ldots, \alpha_n D_{n+1}) \in L(\Omega_1(G^2))$, com $\alpha_i \in (\Omega_1(G^2)D_{i+1}) \cap D_i$, existem $x_i \in \Omega_1(G^2)$ e $g_i \in D_{i+1}$ tais que $\alpha_i = x_i g_i \in D_i$. Veja que $\alpha_i D_{i+1} = x_i g_i D_{i+1} = x_i D_{i+1}$ e assim $t\alpha_i D_{i+1} = tx_i D_{i+1} := x_i^p D_{ip+1}$. Agora, pelo Corolário 3.1.5, para $p = 2$ e pelo Teorema 3.1.4, para $p > 2$, temos $\Omega_1(G^2)$ tem expoente no máximo p, então $x_i^p = 1$. Como isso ocorre em cada entrada temos $t(\alpha_i D_{i+1}) = \overline{1}$ e isso acarreta que $t\widetilde{\alpha} = 0$, ou seja, $\widetilde{\alpha} \in Ann_{L(G^2)}(t)$. Logo, temos a inclusão contrária e assim vale a igualdade $L(\Omega_1(G^2)) = Ann_{L(G^2)}(t)$.

Por hipótese $\Omega_1(G^2) \leqslant N \leqslant G^2$, então também vale a inclusão dos respectivos submódulos, ou seja, $L(\Omega_1(G^2)) \leqslant L(N) \leqslant L(G^2)$, e ainda todos são $\mathbb{F}_p[t]-$submódulos finitamente gerados. Pela igualdade que acabamos de verificar e usando as igualdades dadas em 3.3 temos

$$d_{\mathbb{F}_p[t]}(L(\Omega_1(G^2))) \leq d_{\mathbb{F}_p[t]}(L(N)) \leq d_{\mathbb{F}_p[t]}(L(G^2)) = d_{\mathbb{F}_p[t]}(Ann_{L(G^2)}(t)) = d_{\mathbb{F}_p[t]}(L(\Omega_1(G^2))).$$

Ou seja, $d_{\mathbb{F}_p[t]}(L(N)) = d_{\mathbb{F}_p[t]}(L(G^2))$.

Observe que também vale a igualdade $tL(N) = L(N^p)$. De fato, pela definição dos submódulos temos que $L(N^p) = \bigoplus(N^p D_{i+1}) \cap D_i/D_{i+1}$ e $L(N) = \bigoplus(ND_{i+1}) \cap D_i/D_{i+1}$. Dado $\widetilde{a} = (a_1 D_2, \ldots, a_n D_{n+1}) \in L(N)$, com $a_i \in (ND_{i+1}) \cap D_i$, existem $n_i \in N$ e $d_i \in D_{i+1}$, tais que $a_i = n_i d_i \in D_i$. Veja que $t\widetilde{a}$ é aplicada em cada entrada e assim

$t(a_iD_{i+1}) = t(n_id_iD_{i+1}) = t(n_iD_{i+1}) := n_i^pD_{ip+1}$. Mas, $n_i^p \in N^p \leqslant N^pD_{ip+1}$ e $n_i^p \in D_i^p \leqslant D_{ip}$, ou seja, cada entrada satisfaz $ta_iD_{i+1} = n^pD_{ip+1} \in (N^pD_{ip+1}) \cap D_{ip}/D_{ip+1}$. Logo, $tL(N) \leqslant L(N^p)$.

Por outro lado, considere $\widetilde{a} = (a_1D_2, \dots, a_nD_{n+1}) \in L(N^p)$, com $a_i \in (N^pD_{i+1}) \cap D_i$. Tomemos uma entrada arbitrária $a_{ip} \in (N^pD_{ip+1}) \cap D_{ip}$. Como podemos aplicar o Teorema 3.2.1 em N, temos que existe $n_i \in N$, tal que $n_i^p \in N^p$. Assim $a_i = n_i^pd_i \in D_{ip}$, onde $d_i \in D_{ip+1}$. Dessa forma, em cada entrada $a_{ip}D_{ip+1} = n_i^pd_iD_{ip+1} = n_i^pD_{ip+1}$ e veja que $n_i^p \in N^p \cap D_{ip}$. Na Proposição 3.2.3 vimos que $N^p \cap D_{ip} = (N \cap D_i)^p$, para cada $i \geq 1$, então $n_i^p \in (N \cap D_i)^p$. Dessa forma em cada entrada temos que $t(n_iD_i) := n_i^pD_{ip+1} = a_{ip}D_{ip+1}$. Isso acarreta que $\widetilde{a} \in tL(N)$, então vale a outra inclusão. Logo, $tL(N) = L(N^p)$.

Observe que $\Omega_1(G^2) \leqslant \Omega(N)$, pois por hipótese $\Omega_1(G^2) \leqslant N$ e $\Omega_(G^2) = \Omega_1(\Omega_1(G^2)) \leqslant \Omega_1(N)$. Como a outra inclusão é válida por definição, segue que $\Omega_1(N) = \Omega_1(G^2)$. Com isso temos as seguintes igualdades

$$|\Omega_1(N)| = |\Omega_1(G^2)| = |L(\Omega_1(G^2))| = |Ann_{L(G^2)}(t)| = p^{d_{\mathbb{F}_p[t]}(L(G^2))} =$$

$$= p^{d_{\mathbb{F}_p[t]}(L(N))} = |L(N)/tL(N)| = |L(N)/L(N^p)| = |N/N^p|.$$

Portanto, $|\Omega_1(N) = |N/N^p| = |N : N^p|$. $\square$

Teorema 3.2.5. *Sejam G um p-grupo potent e $N \leqslant G^2$ um subgrupo normal de G. Então $|\Omega_1(N)| = |N/N^p|$.*

Demonstração. Considere G um p-grupo *potent* e $N \leqslant G^2$ um subgrupo normal de G. Lembre que $\Omega_1(G^2) \leqslant G^2$ e também é um subgrupo normal de G. Então, pelo Corolário 3.1.6 segue que $(\Omega_1(G^2)N)^p = \Omega_1(G^2)^pN^p$. Usando os Teoremas 2.5.5 e 2.5.4, quando $p = 2$, ou lembrando que $G^2 = G$, caso $p > 2$, temos que G^2 é *potent*. E assim podemos aplicar o Corolário 3.1.5, no primeiro caso, ou o Teorema 3.1.4, no segundo, de modo que o expoente de $\Omega_1(G^2)$ seja no máximo p, ou seja, $\Omega_1(G^2)^p = 1$. Com isso $(\Omega_1(G^2)N)^p = N^p$.

Por outro lado, como $N \leqslant G^2$, temos que $\Omega_1(N) = \Omega_1(G^2) \cap N$ e lembre que

$$|\Omega_1(G^2)N| = \frac{|\Omega_1(G^2)||N|}{|\Omega_1(G^2) \cap N|}.$$

Observe que $N \leqslant G^2$ e $\Omega_1(G^2) \leqslant G^2$. Logo $\Omega_1(G^2)N \leqslant G^2$ é um subgrupo normal de G e ainda temos $\Omega_1(G^2) \leqslant \Omega_1(G^2)N$. Com isso temos todas as hipóteses do corolário anterior considerando o subgrupo normal como sendo $\Omega_1(G^2)N$. Então

$$|\Omega_1(\Omega_1(G^2)N)| = \Big|\frac{\Omega_1(G^2)N}{(\Omega_1(G^2)N)^p}\Big|.$$

Fazendo as duas inclusões temos que $\Omega_1(G^2) = \Omega_1(\Omega_1(G^2)N)$. Juntando todas essas informações temos que

$$|\Omega_1(G^2)| = |\Omega_1(\Omega_1(G^2)N)| = \frac{|\Omega_1(G^2)N|}{|(\Omega_1(G^2)N)^p|} = \frac{|\Omega_1(G^2)||N|}{|\Omega_1(N)||N^p|}.$$

Portanto, $|\Omega_1(N)| = |N/N^p|$. □

Observe que o teorema anterior tem por objetivo retirar do Corolário 3.2.4 a hipótese de que $\Omega_1(G^2) \leqslant N$ e isso nos dá uma liberdade maior ao resultado. Dessa forma estamos prontos para terminar de verificar a estrutura *power abelian* de um subgrupo normal em p-grupo *potent*. Mas agora resta uma pequena parte, que é a generalização para qualquer inteiro $i \geq 0$, ou seja, que $|\Omega_i(N)| = |N : N^{p^i}|$.

Teorema 3.2.6. *Sejam G um p-grupo potent e $N \leqslant G^2$ um subgrupo normal de G. Então N possui estrutura power abelian.*

Demonstração. Precisamos verificar que dado um subgrupo normal N de G com as condições citadas de hipótese, ele satisfaz as três condições para o que denominamos possuir uma estrutura *power abelian*. O item (i) verificamos através do Teorema 3.2.1 e o item (ii) pelo Corolário 3.1.5. Dessa forma resta verificar que satisfaz o item (iii), o qual faremos por indução sobre i. O primeiro passo foi o que mostramos no teorema anterior.

Suponhamos por hipótese de indução que $|N^{p^i}| = |N : \Omega_i(N)|$ e vejamos ser válido para $i+1$. Pelo Lema 3.1.2, temos que $N^{p^{i+1}} = (N^p)^{p^i}$ e como N^p satisfaz as condições necessárias para aplicar a hipótese de indução, temos $|N^{p^{i+1}}| = |(N^p)^{p^i}| = |N^p : \Omega_i(N^p)|$.

Veja que $N^p \leqslant N \leqslant G^2$ e $N^p \trianglelefteq G^2$, então, através das duas inclusões pode-se verificar que $\Omega_i(N^p) = \Omega_i(N) \cap N^p$. Assim, pelo Segundo Teorema do Isomorfismo, temos

$$\frac{N^p}{\Omega_i(N) \cap N^p} \cong \frac{N^p\Omega_i(N)}{\Omega_i(N)} = \Big(\frac{N}{\Omega_i(N)}\Big)^p.$$

Dessa forma, até agora temos que $|N^{p^{i+1}}| = |N^p : (\Omega_i(N) \cap N^p)| = |(N/\Omega_i(N))^p|$. Por hipótese $N \leqslant G^2$ e como $\Omega_1(N) \trianglelefteq N \trianglelefteq G$, temos que $G/\Omega_i(N)$ é um p-grupo *potent*. E pelo Teorema de Correspondência temos

$$\frac{N}{\Omega_i(N)} \trianglelefteq \frac{G}{\Omega_i(N)} \quad \text{e} \quad \frac{N}{\Omega_i(N)} \leqslant \frac{G^2}{\Omega_i(N)}.$$

Isso nos dá que $N/\Omega_i(N)$ satisfaz as hipóteses do teorema anterior, logo

$$\Big|\Big(\frac{N}{\Omega_i(N)}\Big)^p\Big| = \Big|\frac{N}{\Omega_i(N)} : \Omega_1\Big(\frac{N}{\Omega_i(N)}\Big)\Big|.$$

Agora lembre que sempre vale

$$\frac{\Omega_{1+i}(N)}{\Omega_i(N)} \leqslant \Omega_1\Big(\frac{N}{\Omega_i(N)}\Big).$$

Usando o fato que N satisfaz o item (ii) da condição de ser *power abelian* é possível verificar que a outra inclusão também é válida, de modo que temos a igualdade desses grupos. Com isso, temos

$$|N^{p^{i+1}}| = \Big|\Big(\frac{N}{\Omega_i(N)}\Big)^p\Big| = \Big|\frac{N}{\Omega_i(N)} : \Omega_1\Big(\frac{N}{\Omega_i(N)}\Big)\Big| = \Big|\frac{N}{\Omega_i(N)} : \frac{\Omega_{i+1}}{\Omega_i(N)}\Big|.$$

Assim,

$$|N^{p^{i+1}}| = \frac{|N|}{|\Omega_i(N)|}\frac{|\Omega_i(N)|}{|\Omega_{i+1}(N)|}.$$

Portanto, $|N^{p^{i+1}}| = |N : \Omega_{i+1}(N)|$ e o resultado do teorema segue. □

Para terminar o capítulo, ressaltaremos que neste último teorema verificamos a validade da definição de *power abelian* para um subgrupo normal N de G, um p-grupo *potent*, com $N \leqslant G^2$. Observe que se primo p for ímpar, temos que $G^2 = G$ e, dessa forma, o próprio G possui a estrutura *power abelian*.

Capítulo

4

Resultados principais sobre p-grupos *powerful*

Este capítulo tem como objetivo demonstrar os resultados principais obtidos no artigo "*A characterization of powerful p-groups*". Demonstraremos que dado G um p-grupo finito, com p ímpar, uma condição necessária e suficiente para G ser *powerful* é que $d(G) = \log_p(|\Omega_1(G)|)$. Esse resultado será obtido como consequência do seguinte teorema.

Teorema 4.1. *Sejam p um primo ímpar, G um p-grupo finito e seja $k \leq p-2$ e $i \geq 1$ ou $k = p-1$ e $i \geq 2$. Então as seguintes condições são equivalentes:*

(*i*) $\gamma_k(G) \leqslant G^{p^i}$.

(*ii*) $|G : G^{p^i}\gamma_k(G)| = |\Omega_{\{i\}}(G)|$.

O ingrediente principal para demonstrar esse teorema são os chamados grupos ω-maximais e as palavras *interchangeable*, eles foram estudados por *J. González-Sánchez* e *B. Klopsch*, em [9].

Dessa forma, na primeira seção faremos um estudo bem sucinto sobre grupos ω-maximais, veremos certos tipos de palavras que possuem a características de serem *interchangeable* e por fim relacionar esses dois conceitos. E na segunda seção demonstraremos a caracterização para um p-grupo ser *powerful* e o Teorema 4.1.

4.1 Grupos ω-maximal e palavras *interchangeable*

Uma palavra é um elemento não trivial do grupo livre $F(X)$, onde X é um conjunto de geradores livres $\{x_1, x_2, \ldots\}$. Considere $\omega = \omega(x_1, \ldots, x_n)$ uma palavra, podemos escrever

$\omega = x_{i_1}^{s_1} \cdots x_{i_k}^{s_k}$, onde s_j é um número inteiro e $i_j \in \{1, \ldots, n\}$, para $j = 1, \ldots, k$. Todas as palavras aqui tomadas serão na forma reduzida.

Sejam $\omega = \omega(x_1, \ldots, x_n)$ uma palavra e G um grupo. Podemos associar a seguinte aplicação de $G \times \cdots \times G$ (n vezes) em G

$$\begin{aligned} \varphi_\omega : \underbrace{G \times \cdots \times G}_{n \text{ vezes}} &\longrightarrow G \\ (g_1, \ldots, g_n) &\longmapsto \omega(g_1, \ldots, g_n). \end{aligned}$$

Ou seja, dados os elementos $g_1, \ldots, g_n \in G$ e uma palavra $\omega = \omega(x_1, \ldots, x_n)$, a imagem de $(g_1, \ldots, g_n)$ através de φ_ω é dada por $\omega(g_1, \ldots, g_n) \in G$.

Dados $\omega = \omega(x_1, \ldots, x_n)$ uma palavra e G um grupo. Definimos o subgrupo verbal, denotado por $\omega(G)$, como sendo o subgrupo gerado pelo subconjunto $\{\omega(g_1 \ldots, g_n) \mid g_1, \ldots, g_n \in G\}$. Como exemplo, se considerarmos um grupo livre $F(x, y)$ o comutador $[x, y] = x^{-1}y^{-1}xy$ é uma palavra e o derivado seria o subgrupo verbal.

Definição 4.1.1. *Seja G um grupo finito e ω um palavra em G. Dizemos que G é ω-maximal quando todo subgrupo próprio H de G satisfaz $|H : \omega(H)| < |G : \omega(G)|$.*

Não entraremos em detalhes nas propriedades e características desses grupos, por não ser um dos objetivos do trabalho, porém um pouco mais de detalhes dessa teoria pode ser encontradas no artigo [9]. O próximo passo nesta seção é definir uma classe de palavras denominadas *interchangeable* e alguns de seus representantes.

Definição 4.1.2. *Sejam G um grupo e ω uma palavra de um subgrupo verbal $\omega(G)$. Dizemos que ω é interchangeable em G, se para cada subgrupo normal N de G vale*

$$[\omega(N), G] \leqslant [N, \omega(G)][\omega(G), G]^p[\omega(G), G, G].$$

Definimos esse conceito com o intuito principal de estudar certos tipos de palavras, como as do seguinte lema.

Lema 4.1.3. *Sejam p um primo ímpar e G um p-grupo finito. Se ω é igual a uma das seguintes palavras*

(i) $x^{p^i}[y_1, \ldots, y_k]$ *para algum* $i, k \in \mathbb{N}$ *com* $k \leq p - 1$,

(ii) $x^{p^i}[y_1, \ldots, y_{p-1}]^{p^{i-1}}[z_1, \ldots, z_p]$ *para algum* $i \in \mathbb{N}$ *com* $i \geq 2$,

então ω é interchangeable em G.

Demonstração. Considere N um subgrupo normal de G.

(i) Suponha que $\omega = x^{p^i}[y_1, \dots, y_k]$ para algum $i, k \in \mathbb{N}$, com $k \leq p-1$. Pela Fórmula de Hall temos que $[N^{p^i}, G] \equiv [N, G^{p^i}] \pmod{\gamma_{p+1}(G)}$. Isso acarreta que $[N^{p^i}, G] \leqslant [N, G^{p^i}]\gamma_{p+1}(G)$.

Observe que $k < p-1 \Rightarrow k+2 < p+1$, então $\gamma_{p+1}(G) \leqslant \gamma_{k+2}(G)$. Assim $[N^{p^i}, G] \leqslant [N, G^{p^i}]\gamma_{k+2}(G)$. Sabendo que N^{p^i} e $\gamma_k(G)$ são subgrupos normais de G, temos

$$[N^{p^i}\gamma_k(N), G] = [N^{p^i}, G][\gamma_k(N), G] \leqslant [N, G^{p^i}][N, \gamma_k(G)]\gamma_{k+2}(G) =$$

$$= [N, G^{p^i}\gamma_k(G)][\gamma_k(G), G, G] \leqslant [N, G^{p^i}\gamma_k(G)][G^{p^i}\gamma_k(G), G, G].$$

Assim, $[\omega(N), G] \leqslant [N, \omega(G)][\omega(G), G, G]$. Portanto ω é *interchangeable* em G.

(ii) Suponha que $\omega = x^{p^i}[y_1, \dots, y_{p-1}]^{p^{i-1}}[z_1, \dots, z_p]$ para algum $i \in \mathbb{N}$ com $i \geq 2$. Podemos considerar $\omega(G) = G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)$. Queremos mostrar que

$$[\omega(N), G] \leqslant [N, \omega_G][\omega(G), G]^p[\omega(G), G, G].$$

Porém primeiro vejamos que

$$[\omega(G), G]^p[\omega(G), G, G] = [G, G]^{p^{i+1}}[G, G, G]^{p^i}\gamma_{p+1}(G)^p\gamma_{p+2}(G).$$

Pela Fórmula de Hall temos

$$[G^{p^i}, G] \equiv [G, G]^{p^i} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}$$

e

$$[\gamma_{p-1}(G)^{p^{i-1}}, G] \equiv [\gamma_{p-1}(G), G] \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}.$$

Observe que

$$[\omega(G), G] = [G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G), G] = [G^{p^i}, G][\gamma_{p-1}(G)^{p^{i-1}}, G][\gamma_p(G), G].$$

Assim temos $[\omega(G), G] \equiv [G, G]^{p^i}\gamma_p(G)^{p^{i-1}}\gamma_{p+1}(G) \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}$. Então

$$[\omega(G), G]^p \equiv [G, G]^{p^{i+1}}\gamma_p(G)^{p^i} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}. \tag{4.1}$$

Também temos que

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

Aplicando a Fórmula de Hall, novamente, temos

$$[[G^{p^i}, G], G] \equiv [[G, G]^{p^i}, G] \equiv [G, G, G]^{p^i} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}$$

e

$$[[\gamma_{p-1}(G)^{p^{i-1}}, G], G] \equiv [\gamma_p(G)^{p^{i-1}}, G] \equiv [\gamma_p(G), G]^{p^{i-1}} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}.$$

Com isso, $[\omega(G), G, G] \equiv [G, G, G]^{p^i}\gamma_{p+1}(G)^{p^{i-1}}\gamma_{p+2}$ (mod $gamma_{p+1}(G)^p\gamma_{p+2}(G))$. Mas, como $\gamma_{p+1}(G)^{p^{i-1}} \leqslant \gamma_{p+1}(G)^p$, para todo $i \geq 2$, segue que

$$[\omega(G), G, G] \equiv [G, G, G]^{p^i} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}} \tag{4.2}$$

Dessa forma, pelas equivalências 4.1 e 4.2, temos

$$[\omega(G), G]^p[\omega(G), G, G] \equiv [G, G]^{p^{i+1}}\gamma_p(G)^{p^i}[G, G, G]^{p^i} \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}. \tag{4.3}$$

Observe que $p \geq 3$ então $\gamma_p(G)^{p^i} \leqslant \gamma_3(G)^{p^i}$ e temos que $\gamma_p(G) \leqslant \omega(G)$ então $\gamma_{p+1}(G)^p\gamma_{p+2}(G) \leqslant [\omega(G), G]^p[\omega(G), G, G]$. Com isso, podemos reescrever a equivalência 4.3 como sendo a seguinte igualdade

$$[\omega(G), G]^p[\omega(G), G, G] = [G, G]^{p^{p+1}}[G, G, G]^{p^i}\gamma_{p+1}(G)^p\gamma_{p+2}(G).$$

Agora consideremos $\omega(N) = N^{p^i}\gamma_{p-1}(N)^{p^{i-1}}\gamma_p(N)$. Assim

$$[\omega(N), G] = [N^{p^i}, G][\gamma_{p-1}(N)^{p^{i-1}}, G][\gamma_p(N), G].$$

Pelo Teorema 2.1.10 temos que $[N^{p^i}, G] \equiv [N, G]^{p^i} \equiv [N, G^{p^i}] \pmod{\gamma_{p+1}(G)^p\gamma_{p+2}(G)}$. Então

$$[\omega(N), G] \leqslant [N, G^{p^i}][\gamma_{p-1}(N), G]^{p^{i-1}}[\gamma_p(N), G]\gamma_{p+1}(G)^p\gamma_{p+2}(G).$$

Usando o Teorema 1.1.6, obtemos

$$[\omega(N), G] \leqslant [N, G^{p^i}][N, \gamma_{p-1}(G)^{p^{i-1}}][N, \gamma_p(G)]\gamma_{p+1}(G)^p\gamma_{p+2}(G)$$

Ou seja, $[\omega(N), G] \leqslant [N, G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)]\gamma_{p+1}(G)^p\gamma_{p+2}(G)$. Logo, $[\omega(N), G] \leqslant [N, \omega(G)][\omega(G), G]^p[\omega(G), G, G]$. Portanto, ω é *interchangeable* em G.

□

O próximo teorema é o principal resultado desta seção. Ele será utilizado durante a demonstração do Teorema 4.1, que será apresentada na próxima seção.

Teorema 4.1.4. *Sejam ω uma palavra e G um p-grupo ω-maximal finito tal que ω é interchangeable em G. Então $\omega(G) \leqslant Z(G)$.*

Demonstração. Suponha por contradição que $\omega(G) \nleqslant Z(G)$. Assuma que G seja um contraexemplo minimal, ou seja, que G seja o grupo de menor ordem no qual temos $\omega(G) \nleqslant Z(G)$. Primeiro vejamos que $[\omega(G), G]$ é cíclico de ordem p e está contido no centro $Z(G)$, ou seja, $[\omega(G), G]$ é cíclico e $[\omega(G), G]^p[\omega(G), G, G] = 1$. De fato, temos que $\omega(G) \trianglelefteq G$ e assim $[\omega(G), G] \trianglelefteq G$. Sabemos que $[Z(G), G] = 1$, como $\omega(G) \nleqslant Z(G)$, temos que $[\omega(G), G] \neq 1$. Veja também que $|[\omega(G), G]| = p$, pois caso fosse estritamente maior do que p teríamos um subgrupo normal N de G de índice p que estaria contido em $[\omega(G), G]$ e isso contraria a minimalidade de G. Isso nos dá que $[\omega(G), G]$ é cíclico de ordem p.

Sendo $[\omega(G), G] \trianglelefteq G$, $[\omega(G), G] \neq 1$ e G um p-grupo finito, temos que $[\omega(G), G] \cap Z(G) \neq 1$. Mas, $|[\omega(G), G]| = p$, assim $[\omega(G), G] \leqslant Z(G)$. Com isso, obtemos que $[\omega(G), G, G] \leqslant [Z(G), G] = 1$. Dessa forma, temos que $[\omega(G), G]$ é cíclico de ordem p e $[\omega(G), G]^p[\omega(G), G, G] = 1$.

Agora considere os seguintes subgrupos de G, $N_1 = \{x \in G \mid [x, \omega(G)] = 1\}$ e $N_2 = \{x \in \omega(G) \mid [x, G] = 1\}$. Utilizando-se a definição desses grupos pode-se mostrar que $N_1 = C_G(\omega(G))$ e $N_2 = Z(G) \cap \omega(G) \leqslant N_1$. Mais ainda, verifica-se que ambos são característicos em G e que $\omega(N_1) \leqslant N_2$.

Como ω é *interchangeable*, se considerarmos o subgrupo normal como sendo N_1 e usar que $[\omega(G), G]^p[\omega(G), G, G] = 1$, obtemos que $[\omega(N_1), G] \leqslant [N_1, \omega(G)] = 1$, pela definição de N_1. Assim $[\omega(N_1), G] = 1$, isso acarreta que $\omega(N_1) \leqslant Z(G)$. Considerando $x \in G$ e $y \in \omega(G)$ defina a aplicação

$$\begin{aligned} \langle\ ,\ \rangle : G/N_1 \times \omega(G)/N_2 &\longrightarrow [\omega(G), G] \\ (xN_1, yN_2) &\longmapsto \langle xN_1, yN_2\rangle := [x, y]. \end{aligned}$$

Usando propriedades de comutadores e o fato que $[\omega(G), G]$ é central, verifica-se que essa aplicação está bem-definida. Vimos que N_1 e N_2 são característicos em G, logo são normais. Com isso os quocientes estão bem-definidos como grupo e observe ainda que são abelianos. De fato, dados $x, y, g \in G$ e $a, b, \alpha \in \omega(G)$ e lembrando que

$$xN_1yN_1 = yN_1xN_1 \Leftrightarrow [x,y] \in N_1 \quad \text{e} \quad aN_2bN_2 = bN_2aN_2 \Leftrightarrow [a,b] \in N_2.$$

Pela definição de N_1 temos $[[y,\alpha],x] = [1,x] = 1$ e $[[\alpha,x],y] = [1,y] = 1$. Usando a igualdade de Hall-Witt, temos que $[[x,y],\alpha] = 1$ e isso significa que $[x,y] \in N_1$. Ou seja, N_1 é abeliano. Por outro lado pela definição de N_2 temos que $[[b,g],a] = [1,a] = 1$ e $[[g,a],b] = [1,b] = 1$, e também pela igualdade de *Hall-Witt* $[[a,b],g] = 1$ e então $[a,b] \in N_2$, ou seja N_2 é abeliano.

Usando contagem das classes dos quocientes junto com a definição da aplicação entre p-grupos abelianos, obtemos que $|G : N_1| = |\omega(G) : N_2|$. Isso acarreta que $|G : \omega(G)| = |N_1 : N_2|$. Mas lembre que $\omega(N_1) \leqslant N_2 \leqslant N_1$, então $|N_1 : \omega(N_1)| \geqslant |N_1 : N_2| = |G : \omega(G)|$, o que é um absurdo, pois por hipótese G é ω-maximal.

Portanto, $\omega(G) \leqslant Z(G)$. $\square$

4.2 Resultados principais

Separaremos o Teorema 4.1 em dois. No primeiro teorema consideraremos o caso em que $k \leq p-2$ e $i \geq 1$ e no segundo consideraremos $k = p-1$ e $i \geq 2$. Isso se dará pelo fato de que na demonstração utilizaremos técnicas semelhantes, mas resultados preliminares diferentes.

Teorema 4.2.1. *Sejam $p \geq 5$, $i \geq 1$, $k \leq p-2$ e G um p-grupo finito. Então as seguintes condições são equivalentes:*

(*i*) $\gamma_k(G) \leqslant G^{p^i}$,

(*ii*) $|G : G^{p^i}\gamma_k(G)| = |\Omega_{\{i\}}(G)|$.

Demonstração. Suponha que $\gamma_k(G) \leqslant G^{p^i}$, de onde $G^{p^i}\gamma_k(G) = G^{p^i}$. Assim devemos mostrar que $|G : G^{p^i}| = |\Omega_{\{i\}}(G)|$. Observe que $k \leq p-2 \Rightarrow k+1 \leq p-1$ e então $\gamma_{p-1}(G) \leqslant \gamma_{k+1}(G) \leqslant \gamma_k(G)$. Temos ainda que $i \geq 1$, pois para $i = 0$ o teorema é trivialmente válido, logo $G^{p^i} \leqslant G^p$.

Dessa forma, o item (i) significa $\gamma_{p-1}(G) \leqslant G^p$, ou seja, G é um p-grupo finito *potent* G. No Teorema 3.2.5 vimos que o $|N : N^p| = |\Omega_1(N)|$, com $N \leqslant G^2$ um subgrupo normal do p-grupo *potent*. No nosso caso, p é ímpar e isso acarreta que $G^2 = G$, então o resultado será válido para qualquer subgrupo normal, em particular para o próprio G. O Teorema 3.2.6 nos mostra a validade dessa relação para todo $i \geq 0$. Logo, essa implicação está provada.

Reciprocamente, suponha que $|G : G^{p^i}\gamma_k(G)| = |\Omega_{\{i\}}(G)|$. Considere a seguinte conjunto de subgrupos $C = \{H \leqslant G \mid |H : H^{p^i}\gamma_{k+1}(H)| \geq |G : G^{p^i}\gamma_{k+1}(G)|\}$. Observe que $H^{p^i}\gamma_{k+1}(H)$ é o subgrupo de H formado por palavras do tipo $\omega = x^{p^i}[y_1, \ldots, y_{k+1}]$ com $x, y_j \in H$, $1 \leq j \leq k+1$. Assim podemos escrever $\omega(H) = H^{p^i}\gamma_{k+1}(H)$ e da mesma forma temos $\omega(G) = G^{p^i}\gamma_{k+1}(G)$.

O conjunto C é diferente de vazio, pois pelo menos o próprio grupo G pertence a C. Dessa forma, considere $M \leqslant G$, o elemento mínimo com relação à inclusão pertencente à C. Observe que qualquer subgrupo H de M, em particular para subgrupos próprios vale que $|H : \omega(H)| < |M : \omega(M)|$. Pois, caso houvesse algum subgrupo T de M, tal que $|T : \omega(T)| \geq |M : \omega(M)|$, teríamos que $T \in C$ e isso contraria a minimalidade de M.

Agora, se $|H : \omega(H)| < |M : \omega(M)|$, para todo $H < M$, então M é um subgrupo ω-maximal para palavras da forma $\omega = x^{p^i}[y_1, \ldots, y_{k+1}]$. Mas, pelo Lema 4.1.3, item (i), vimos que essa palavra é *interchangeable* em M. Então temos todas as hipóteses do Teorema 4.1.4 satisfeitas para o subgrupo M, então $M^{p^i}\gamma_{k+1}(M) = \omega(M) \leqslant Z(M)$.

Assim, $\gamma_{k+1}(M) \leqslant Z(M)$, então $\gamma_{k+2}(M) \leqslant [Z(M), M] = 1$, ou seja, $\gamma_{k+2}(M) = 1$. Portanto, a classe de nilpotência de M é no máximo $k+1 \leq p-1 < p$. Aplicando o Teorema 2.2.2 temos que M é regular. Dessa forma temos que M é um p-grupo regular, então, pelo Teorema 2.2.8, item (iii), temos que $|M : M^{p^i}| = |\Omega_i(M)| = |\Omega_{\{i\}}(M)|$. Com isso, temos as seguintes desigualdades

$$\begin{aligned} |G : G^{p^i}\gamma_{k+1}(G)| &\leq |M : M^{p^i}\gamma_{k+1}(M)| \leq |M : M^{p^i}| = |\Omega_{\{i\}}(M)| \\ &\leq |\Omega_{\{i\}}(G)| = |G : G^{p^i}\gamma_k(G)| \leq |G : G^{p^i}\gamma_{k+1}(G)|. \end{aligned}$$

Então temos que $|G : G^{p^i}\gamma_k(G)| = |G : G^{p^i}\gamma_{k+1}(G)|$. Como $G^{p^i}\gamma_{k+1}(G) \leqslant G^{p^i}\gamma_k(G)$, segue que $G^{p^i}\gamma_k(G) = G^{p^i}\gamma_{k+1}(G)$. Essa igualdade nos dá que $\gamma_k(G) \leqslant G^{p^i}[\gamma_k(G), G]$ e o resultado segue ao aplicarmos o Teorema 2.1.8. Portanto vale a outra implicação. □

Em [17], uma das questões levantados por *B. Klopsch* e *I. Snopce* foi a respeito de uma condição necessária e suficiente para um p-grupo finito G, com p ímpar, ser *powerful*. E essa condição era a relação $d(G) = \log_p(|\Omega_1(G)|)$.

Para $p \geq 5$, *J. González-Sánchez* e *A. Zugadi-Reizabel* obtiveram, em [10], uma resposta positiva para essa questão como consequência do teorema anterior. Quando $p = 3$, eles construíram, nesse mesmo trabalho, uma família de p-grupos finitos que mostram que a caracterização proposta não é válida, como veremos no próximo capítulo.

Corolário 4.2.2. *Sejam $p \geq 5$ e G um p-grupo finito. Então as seguintes condições são equivalentes:*

(i) G é powerful,

(ii) $d(G) = log_p(|\Omega_1(G)|)$.

Demonstração. Suponha que G seja um p-grupo *powerful*, com $p > 5$, de onde $G' \leqslant G^p$ e $\Phi(G) = G'G^p = G^p$. Agora, pelo Teorema da Base de Burnside $|G : \Phi(G)| = |G : G^p| = p^{d(G)}$, onde $d(G)$ é o número mínimo de geradores de G. Considerando $k = 2$ e $i = 1$, no teorema anterior temos que se G é *powerful*, então $|G : G^p| = |\Omega_{\{1\}}(G)|$. Mas, em p-grupos *powerful* vale que $\Omega_1(G) = \Omega_{\{1\}}(G)$. Assim $p^{d(G)} = |G : G^p| = |\Omega_1(G)|$. Logo, $d(G) = \log_p(|\Omega_1(G)|)$.

Reciprocamente, suponha que $d(G) = \log_p(|\Omega_1(G)|)$, ou seja, $|\Omega_1(G)| = p^{d(G)}$. Novamente por Burnside, $|G : \Phi(G)| = p^{d(G)}$ e assim $|G : G'G^p| = |\Omega_1(G)|$. Mas, isso acarreta que $|\Omega_1(G)| = |\Omega_{\{1\}}(G)|$. Então $|G : G'G^p| = |\Omega_{\{1\}}(G)|$. Pelo teorema anterior, quando $k = 2$ e $i = 1$, se isso ocorre, segue que $\gamma_2(G) \leqslant G^p$. Portanto, G é *powerful*. □

Para provar o caso em que $k = p-1$ precisaremos da definição de p-grupo k-regular dada no Capítulo 2, e ela nos diz que para quaisquer $x, y \in G$, $(xy)^{p^k} = x^{p^k} y^{p^k} \prod_i D_i^{p^k}$ para certos $D_i \in \gamma_2(\langle x, y\rangle)$, para todo i. Então podemos considerar $D_i = \gamma_2(\langle x, y\rangle)$ e assim nossa definição fica $(xy)^{p^k} = x^{p^k} y^{p^k} \gamma_2(\langle x, y\rangle)^{p^k}$. Com esse caso particular da definição, demonstraremos o próximo lema, que será de grande utilidade quando considerarmos o caso em que $k = p-1$ e $i \geq 2$ no Teorema 4.1.

Lema 4.2.3. *Sejam G um p-grupo finito e $\omega = x^{p^i}[y_1, \ldots, y_{p-1}]^{p^{i-1}}[z_1, \ldots, z_p]$, para algum $i \in \mathbb{N}$ com $i \geq 2$. Se G é um p-grupo ω-maximal, então $|G : G^{p^i}| = |\Omega_{\{i\}}(G)|$.*

Demonstração. Primeiro observe que no Lema 4.1.3 vimos que ω é *interchangeable* em G. Como G é um p-grupo finito ω-maximal, pelo Teorema 4.1.4, segue que $\omega(G) \leqslant Z(G)$. Assim, $[\omega(G), G] \leqslant [Z(G), G] = 1$ e isso acarreta que

$$[G^{p^i}, G][\gamma_{p-1}(G)^{p^{i-1}}, G][\gamma_p(G), G] = 1. \tag{4.4}$$

Vamos analisar cada parte dessa relação. Pelo Teorema 2.1.10,

$$[G^{p^i}, G] \equiv [G, G]^{p^i} \pmod{[G,_p G]^{p^{i-1}}[G,_{p^2} G]^{p^{i-2}} \cdots [G,_{p^i} G]}.$$

Como todos os termos da congruência são subgrupos de $\gamma_{p+1}(G)$, podemos reescrever essa congruência da seguinte forma $[G^{p^i}, G] \equiv [G, G]^{p^i} \pmod{\gamma_{p+1}(G)}$. Novamente pelo Teorema 2.1.10, temos

$$[\gamma_{p-1}(G)^{p^{i-1}}, G] \equiv \gamma_p(G)^{p^{i-1}} \pmod{[G,_p \gamma_{p-1}(G)]^{p^{i-2}}[G,_{p^2} \gamma_{p-1}(G)]^{p^{i-3}} \cdots [G,_{p^{i-1}} \gamma_{p-1}(G)]}.$$

De maneira análoga, ao analisado acima, todos os termos da equivalência são subgrupos de $\gamma_{p+1}(G)$ e assim podemos reescrevê-la da seguinte forma $[\gamma_{p-1}(G)^{p^{i-1}}, G] \equiv \gamma_p(G)^{p^{i-1}} \pmod{\gamma_{p+1}(G)}$. Com isso, a igualdade 4.4 é dada por

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

Considere $x, y \in G$ e $H = \langle x, y\rangle$, pela Fórmula de Compilação de Hall, Teorema 1.1.14, temos

$$(xy)^{p^i} \equiv x^{p^i} y^{p^i} (\bmod\ \gamma_2(H)^{p^i}\gamma_p(H)^{p^{i-1}}\gamma_{p^2}(H)^{p^{i-2}} \ldots \gamma_{p^k}(H))$$

Assim, $(xy)^{p^i} \equiv x^{p^i} y^{p^i} \pmod{\gamma_2(G)^{p^i}\gamma_p(G)^{p^{i-1}}\gamma_{p^2}(G)^{p^{i-2}} \cdots \gamma_{p^k}(G)}$. Porém, pelo mesmo argumento que antes, todos os termos a partir de $\gamma_{p^2}(G)^{p^{i-1}}$ são subgrupos de $\gamma_{p+1}(G)$.

Assim, reescrevemos essa última congruência da seguinte forma

$$(xy)^{p^i} \equiv x^{p^i} y^{p^i} \pmod{\gamma_2(G)^{p^i}\gamma_p(G)^{p^{i-1}}\gamma_{p+1(G)}}.$$

E isso acarreta que $(xy)^{p^i} = x^{p^i}y^{p^i} = x^{p^i}y^{p^i}\gamma_2(G)^{p^i}$, pois $1 \in \gamma_2(G)^{p^i}$. Sendo x e y arbitrários, segue que G é $i-$regular. Aplicando o Teorema 2.2.8, item (iii), segue que $|G : G^{p^i}| = |\Omega_i(G)| = |\Omega_{\{i\}}(G)|$, como queríamos. □

Teorema 4.2.4. *Sejam p um primo ímpar, $i \geq 2$ e G um p-grupo finito. Então as seguintes condições são equivalentes:*

(i) $\gamma_{p-1} \leq G^{p^i}$,

(ii) $|G : G^{p^i}\gamma_{p-1}(G)| = |\Omega_{\{i\}}(G)|$.

Demonstração. Suponha $|G : G^{p^i}\gamma_{p-1}(G)| = |\Omega_{\{i\}}(G)|$. Considere agora a palavra $\omega = x^{p^i}[y_1,\ldots,y_{p-1}]^{p^{i-1}}[z_1,\ldots,z_p]$ e defina o conjunto de subgrupos $C = \{H \leqslant G \mid |H : \omega(H)| \geq |G : \omega(G)|\}$. Observe que esse conjunto é não vazio, pois $G \in C$. Com isso, podemos tomar o elemento mínimo em C, com respeito à inclusão, seja M tal minimal. Dessa forma, para todo subgrupo H de M vale que $|M : \omega(M)| > |H : \omega(H)|$, pois M é minimal. Com isso o subgrupo M é ω-maximal.

Pelo Lema 4.1.3, item (ii), vimos que palavras dessa forma são *interchangeable* no grupo ambiente. Então todas as hipóteses do lema anterior aplicado ao subgrupo M são satisfeitas. Assim $|M : M^{p^i}| = |\Omega_{\{i\}}(M)|$. Como $M^{p^i} \leqslant \omega(M)$, temos que $|G : \omega(G)| \leq |M : \omega(M)| \leq |M : M^{p^i}|$. Então

$$|G : \omega(G)| \leq |M : M^{p^i}| = |\Omega_{\{i\}}(M)| \leq |\Omega_{\{i\}}(G)| = |G : G^{p^i}\gamma_{p-1}(G)|.$$

Agora, veja que $\omega(G) = G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)$, $\gamma_p(G) \leqslant \gamma_{p-1}(G)$ e $\gamma_{p-1}(G)^{p^{i-1}} \leqslant \gamma_{p-1}(G)$, então $\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G) \leqslant \gamma_{p-1}(G)$. Assim

$$G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G) \leqslant G^{p^i}\gamma_{p-1}(G). \tag{4.5}$$

Dessa forma, $|G : G^{p^i}\gamma_{p-1}(G)| \leq |G : G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)| = |G : \omega(G)]$. Logo $|G : \omega(G)| \leq |G : G^{p^i}\gamma_{p-1}(G)| \leq |G : \omega(G)|$, ou seja,

$$|G : \omega(G)| = |G : G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)| = |G : G^{p^i}\gamma_{p-1}(G)|. \tag{4.6}$$

Juntando a inclusão de subgrupos dada em 4.5 e a igualdade de índices dada em 4.6, obtemos que $G^{p^i}\gamma_{p-1}(G) = G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)$. Isso acarreta que $\gamma_{p-1}(G) \leqslant$

$G^{p^i}\gamma_{p-1}(G)^{p^{i-1}}\gamma_p(G)$. Assim, $\gamma_{p-1}(G) \leqslant G^{p^i}\gamma_{p-1}(G)\gamma_p(G) \leqslant G^{p^i}\gamma_{p-1}(G)^p\gamma_p(G)$, pois $p^{i-1} \geq p$ e $i \geq 2$. Aplicando o Teorema 2.1.8, segue que $\gamma_{p-1}(G) \leqslant G^{p^i}$, como queríamos.

Reciprocamente, suponha que $\gamma_{p-1}(G) \leqslant G^{p^i}$. Temos que $i \geq 2$ e $G^{p^i} \leqslant G^p$, para todo $i \geq 1$, então $\gamma_{p-1}(G) \leqslant G^{p^i} \leqslant G^p$. Sendo p um primo ímpar, segue que essa condição nos dá que G é um p-grupo *potent*. Agora se $\gamma_{p-1}(G) \leqslant G^{p^i}$ então vale que $|G : G^{p^i}\gamma_{p-1}(G)| = |G : G^{p^i}|$. Com isso precisamos mostrar que $|G : G^{p^i}| = |\Omega_{\{i\}}(G)|$ com G um p-grupo *potent*, para $p \geq 3$, como, comentado no Teorema 4.2.1 isso é válido nessa classe de p-grupo. Portanto, o teorema está provado. $\square$

Capítulo 5

Uma família de exemplos

Neste capítulo construiremos uma família de p-grupos que provam a validade do teorema a seguir. Essa família também servirá de contraexemplo para o caso em que $k = p-1$ e $i = 1$ no Teorema 4.1. Essa construção foi feita por *J. González-Sánchez* e *A. Zugadi-Reizabel* no artigo "*A characterization of powerful p-groups*"[10], com o principal intuito de mostrar que a caracterização para um p-grupo finito ser *powerful*, dada no capítulo anterior, não é válida quando $p = 3$.

Teorema 5.1. *Sejam p um primo ímpar e s um inteiro positivo $s \geq p+1$. Então existe um p-grupo finito G tal que:*

(i) $|G| = p^s$;

(ii) *G é de classe maximal;*

(iii) $|G : G^p\gamma_{p-1}(G)| = |\Omega_1(G)|$;

(iv) $\gamma_{p-1}(G) \nleq G^p$.

5.1 Preliminares para a construção da família

Nesta seção apresentaremos, principalmente, conceitos utilizados na construção da família de p-grupos que demonstram o Teorema 5.1. Utilizamos os livros *Profinite Groups* [22], *The Structure of Groups of Prime Power Order* [19] e *Endliche Gruppen I* [14].

Inicialmente relembremos a definição de espaço topológico e de aplicação contínua, para em seguida definir grupos topológicos.

Definição 5.1.1. *Um espaço topológico é um conjunto X junto com uma família de subconjuntos, denominados conjuntos abertos, satisfazendo as seguintes condições:*

(*i*) *Os conjuntos $\emptyset$ e X são ambos abertos;*

(*ii*) *A interseção de quaisquer dois conjuntos abertos é ainda um conjunto aberto;*

(*iii*) *A união de qualquer coleção de subconjuntos abertos é também um conjunto aberto.*

Sejam X e Y espaços topológicos. A aplicação $f : X \to Y$ é dita ser contínua se para cada conjunto aberto U de Y o conjunto $f^{-1}(U) = \{x \in X \mid f(x) \in U\}$ é também aberto em X. Outros definições e algumas propriedades a cerca de espaços topológicos podem ser encontradas em [22], bem como as próximas definições, que são agora relacionadas a grupos topológicos e homomorfismo contínuo.

Um grupo topológico é um conjunto G que é, ao mesmo tempo, um grupo e um espaço topológico e para o qual a aplicação $(x, y) \mapsto xy^{-1}$ de $G \times G$, com o produto topológico, em G é contínua. Um homomorfismo contínuo é uma aplicação, entre dois grupos topológicos, contínua que também é um homomorfismo de grupos.

Um conjunto direto é um conjunto I parcialmente ordenado tal que para todo $i_1, i_2 \in I$ existe um elemento $j \in I$ para o qual $i_1 \leq j$ e $i_2 \leq j$.

Definição 5.1.2. *Um sistema inverso (X_i, φ_{ij}) de um espaço topológico indexado por um conjunto direto I consiste de uma família $(X_i \mid i \in I)$ de espaços topológicos e uma família $(\varphi_{ij} : X_j \to X_i \mid i, j \in I,\ i \leq j)$ de aplicações contínuas tais que φ_{ii} é aplicação identidade Id_{X_i}, para cada i, e $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ sempre que $i \leq j \leq k$.*

Se cada X_i é um grupo topológico e cada φ_{ij} é um homomorfismo contínuo, dizemos que (X_i, φ_{ij}) é um sistema inverso de grupos topológicos. De maneira similar definimos um sistema inverso de anéis topológicos.

Definição 5.1.3. *Um limite inverso (X, φ_i) de um sistema inverso (X_i, φ_{ij}) de um espaço topológico é um espaço topológico X junto com uma família compatível $(\varphi_i : X \to X_i)$ de aplicações contínuas com a seguinte propriedade universal: sempre que $(\psi_i : Y \to X_i)$ é uma família compatível de aplicações contínuas do espaço Y existe uma única aplicação contínua $\psi : Y \to X$ tal que $\varphi_i \psi = \psi_i$, para cada i.*

Caso o sistema inverso considerado seja de grupos topológicos junto com uma família de homomorfismos contínuos temos um limite inverso de grupos topológicos. E de forma semelhante definimos o limite inverso de anéis topológicos.

Definição 5.1.4. *Seja C uma classe de grupos finitos. Dizemos que um grupo F é um C-grupo se $F \in C$ e G é um grupo pro-C se ele é um limite inverso de C-grupos. Observe que C-grupos são grupos pro-C.*

Algumas classes importantes são: a classe de todos os grupos finitos, a classe de p-grupos finitos, onde p é um primo fixado, e a classe de todos os grupos cíclicos finitos. Um limite inverso de grupos finitos é chamado de grupo profinito, o de p-grupos finitos é chamado grupo *pro-p* e o de grupos cíclicos finitos é dito grupo *procíclico*.

Fixado um primo p, consideraremos $\mathbb{Z}_p$ como sendo o conjunto de somas infinitas da forma

$$\sum_{j=0}^{\infty} a_j p^j,$$

com $0 \leq a_j < p$ para cada j, em cada caso essa expressão é unicamente determinada. Uma definição alternativa de $\mathbb{Z}_p$ é como limite inverso do sistema de anéis $(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{Z}}$. É possível definir operações estendidas através das usualmente definidas em $\mathbb{Z}$, e assim $\mathbb{Z}_p$ será um anel *pro-p*, denominado anel dos inteiros p-ádicos, e considerado dessa forma, $\mathbb{Z}_p$ é também um domínio de integridade. A construção pode ser encontrada em detalhes nos livros *Analytic pro-p groups*, [4], e *Profinite Groups*,[22], ambos no Capítulo 1.

Considere N um grupo e $\alpha \in Aut(N)$, onde $Aut(N)$ é o grupo dos automorfismos de N, dizemos que o subgrupo H de N é α-invariante se $\alpha(H) = H$. Definimos o subgrupo $[N, \alpha] = \langle [n, \alpha] = n^{-1}\alpha(n) | n \in N \rangle$ e recursivamente colocamos $N_1 = N$ e $N_i = [N_{i-1}, \alpha]$, para todo $i > 1$. Note que todos esses subgrupos são normais em N e α-invariantes.

Quando N é um p-grupo finito e $\alpha \in Aut(N)$, um automorfismo for de ordem p, teremos que para algum inteiro natural m vale $H_m = \langle 1 \rangle$. Assim esses subgrupos formam uma série estritamente decrescente de subgrupos α-invariantes de H.

Definição 5.1.5. *Considere N um p-grupo finito e $\alpha \in Aut(N)$ um automorfismo de ordem p agindo sobre N. Dizemos que α age uniserially sobre N se $[H, \alpha]$ possui índice p em H para todo subgrupo H de N não trivial e α-invariante.*

Outro conceito que necessitaremos é o de extensão.

Definição 5.1.6. *Sejam N e G grupos. Uma extensão de N por G é uma sequência exata curta*

$$1 \to N \xrightarrow{i} E \xrightarrow{\pi} G \to 1,$$

onde π é sobrejetiva, i é injetiva e a imagem de i é o núcleo de π.

Um exemplo típico de extensão é quando consideramos N um subgrupo normal de E e $G = E/N$, assim i será a aplicação inclusão e π a projeção natural.

Dado N um subgrupo de G, dizemos que G é uma extensão *split* de N, quando $N \trianglelefteq G$ e existe $H \leqslant G$ tal que $G = NH$ e $N \cap H = \{e\}$. Nesse caso G é o produto semidireto $H \ltimes N$. Caso exista $H \leqslant G$ com $G = NH$, mas com $N \cap H \neq \{e\}$, então G é dito ser uma extensão não-*split*.

O seguinte teorema é mais uma identidade entre comutadores, de grande utilidade em nosso exemplo. Sua demonstração pode ser encontrada em [14, Capítulo 3, Lema 10.9], ou através do Exercício 2.2 de [5].

Teorema 5.2. *Seja U um subgrupo normal abeliano em um grupo arbitrário G.*

(i) Para todos $x, y \in U$ e todo $g \in G$ vale $[xy, g] = [x, g][y, g]$.

(ii) Para $x \in U$, $g \in G$ e todo número natural n vale

$$(gx)^n = g^n x^n \prod_{i=2}^{n} [x,_{i-1} g]^{\binom{n}{i}}.$$

5.2 Família de exemplos

Considere a $\mathbb{Z}_p$−*lattice* M gerada por $(x_1, \ldots, x_{p-1})$ de posto $p-1$ e o seguinte automorfismo α de M

$$\begin{aligned} \alpha(x_i) &= x_{i+1}, \text{ se } i \leq p-2 \\ \alpha(x_{p-1}) &= x_1^{-1} \cdots x_{p-1}^{-1}. \end{aligned}$$

Aplicando-se esse automorfismo várias vezes é possível ver que ele possui ordem p. Além disso, podemos mostrar que α age *uniserially* sobre M, ou seja, que $[H, \alpha]$ possui índice p em H para todo subgrupo H não trivial α−invariante de M.

Pela maneira como definimos o homomorfismo α, qualquer subgrupo H que tomarmos em M de modo que também seja α−invariante, terá ainda posto $p-1$. Pois, se o elemento básico $x_i \in H$, então ainda temos $\alpha(x_i) \in H$, o que ocorrerá para qualquer $i = 1, \ldots, p-1$. Ou seja, o fato de α levar um elemento da base no próximo elemento básico ou em uma combinação de todos eles, no caso em que $i = p-2$, acarreta que todos os elementos da base devem estar em H, para que ele seja α-invariante. Grosseiramente podemos dizer que qualquer subgrupo α-invariante de M será apenas uma restrição nos "coeficientes", que são elementos de $\mathbb{Z}_p$.

Coloque $M_1 = M$ e $M_r = [M_{r-1}, \alpha]$. Dessa forma temos uma sequência decrescente de subgrupos $\alpha-$invariantes, onde um tem índice p no anterior:

$$M > [M, \alpha] > [M, \alpha, \alpha] > \cdots > [M,_{r-1} \alpha] \cdots$$

O produto semidireto $H = \langle \alpha \rangle \ltimes M$ é um grupo *pro-p*, pois os grupos quocientes são p-grupos finitos. Além disso, H/M_r, com $r > 2$, é um p-grupo de classe maximal e α é um elemento uniforme. Como M é abeliano, temos que $|C_{H/M_r}(\alpha)| = |C_{H/M_r}(\alpha^j x)|$, para $x \in M$ e $j = 1, \ldots, p-1$. Dessa forma, todos os elementos de $H \setminus M_r$ são uniformes.

Lema 5.2.1. *Seja $H = \langle \alpha \rangle \ltimes M$, como definido acima. Então os elementos de $H \setminus M$ possuem ordem p.*

Demonstração. Seja $s \in H \setminus M$ e considere $H_r = H/M_r$. Pelo parágrafo anterior temos que $\overline{s}$ é um elemento uniforme de H_r. Sendo assim $\overline{s}^p \in Z(H_r) = M_{r-1}/M_r$. Com isso $s^p \in M_{r-1}$, para todo $r \geq 2$. Ou seja, $s^p \in \cap_{r=2}^{\infty} M_r = \{1\}$. □

Os elementos de $H \setminus M$ são da forma $\alpha^j x$, com $x \in M$ e para $j = 1, \ldots, p-1$. Então considerando um elemento desses, pelo Teorema 5.2, temos que:

$$1 = (\alpha^j x)^p = (\alpha^j)^p x^p \sum_{i=2}^{p} [x,_i \alpha^j]^{\binom{p}{i}}.$$

Como α possui ordem p, temos que

$$x^p \sum_{i=2}^{p} [x,_i \alpha^j]^{\binom{p}{i}} = 1. \tag{5.1}$$

Denotemos $N_r = M/M_r$, ou seja, estamos "quocientando"toda a série que definimos anteriormente por M_r, isso acarreta que os termos contidos em M_r passam a ser a identidade no quociente. Lembre que cada termo da série tinha índice p no anterior, então seja z um gerador M_{r-1}/M_r. Agora considere G_r a extensão não-split

$$1 \longrightarrow N_r \longrightarrow G_r \longrightarrow C_p \longrightarrow 1,$$

onde $C_p = \langle y \rangle$ e a extensão é definida pela identidade $y^p = z$ e a ação de y em N_r é dada por α. Dessa maneira podemos escrever que $G_r = \langle y \rangle N_r = \langle y \rangle M/M_r$, onde $N_r \trianglelefteq G_r$, $G_r/N_r = \langle y \rangle$, $y^p = z$ e $\langle y \rangle \cap N_r = z \neq e$.

Observe que, para cada r, G_r é um p-grupo de classe maximal e os elementos de $G_r \setminus N_r$ são elementos uniformes.

Lema 5.2.2. *Seja $G_r = \langle y \rangle N_r$, como definido acima. Então os elementos de $G_r \setminus N_r$ possuem ordem p^2.*

Demonstração. Considere um elemento em $x \in N_r$ e $j = 1, \ldots, p-1$, pela identidade 5.1 e pelo Teorema 5.2 temos que

$$(y^j x)^p = y^{jp} x^p \sum_{i=2}^{p} [x,_i y^j]^{\binom{p}{i}} = z^j \neq 1.$$

Veja que $(y^j x)^{p^2} = ((y^j x)^p)^p = (z^j)^p = 1$, pois $z^p = 1$. □

Isso significa que os elementos de $G_r \setminus N_r$ não possuem ordem p, então os elementos que vão gerar $\Omega_1(G_r)$ estão em N_r, logo $\Omega_1(G_r) = \Omega_1(N_r) = \Omega_1(M/M_r)$.

Em particular, se $r \geq p$, pelo Teorema 2.3.4, segue que $|\Omega_1(G_r)| = p^{p-1}$. Agora por outro lado, como G_r é de classe maximal, então G_r possui apenas os normais da série central inferior. E pelo Teorema 2.3.4, temos que $G_r^p = \gamma_p(G_r)$. Assim $G_r^p \gamma_{p-1}(G_r) = \gamma_p(G)\gamma_{p-1}(G_r) = \gamma_{p-1}(G_r)$. Como α age *uniserially* sobre M, temos que $|G_r : G_r^p \gamma_{p-1}(G_r)| = p^{p-1}$. Mas claramente, o grupo G_r não satisfaz a inclusão $\gamma_{p-1}(G_r) \leqslant G_r^p$.

Referências Bibliográficas

[1] D. E. Arganbright. The power-commutator structure of finite p-groups. Pacific Journal of Mathematics **29** (1969), 11–17.

[2] W. Bannuscher, *Eine verallgemeinerung des regularittsbegriffes bei p-gruppen.* Beiträge zur Algebra und Geometrie **11** (1981), 51–63.

[3] N. Blackburn, *On a special class of p-groups.* Acta Math **100** (1958), 45–92.

[4] J. D. Dixon; M. P. F. Du Sautoy; A. Mann; D. Segal. *Analytic pro-p groups.* 2ª Edição. Cambridge University Press, 1999.

[5] G. A. Fernández-Alcober. *An introduction to finite p-groups: regular p-groups and groups of maximal class.* Matemática Contemporânea **20** (2001), 155–226.

[6] G. Fernández-Alcober; J. González-Sánchez; A. Jaikin-Zapirain. *Omega subgroups of pro-p groups.* Israel Journal of Mathematics **166** (2008), 393–410.

[7] A. Garcia; Y. Lequain. *Elementos de álgebra.* Rio de Janeiro: IMPA, 2013.

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

[9] J. González-Sánchez; B. Klopsch. *On $\omega-$maximal groups.* Journal of Algebra **328** (2011), 155–166.

[10] J. González-Sánchez. A. Zugadi-Reizabal. *A characterization of powerful p-groups.* Israel Journal of Mathematics **202** (2014), 321–329.

[11] D. Gorenstein. *Finite Groups.* New York: Chelsea Publishing Company, 1980.

[12] L. Héthelyi; L. Lévai. *On elements of order p in powerful p-groups.* Journal of Algebra **270** (2003), 1–6.

[13] P. Hall. *A contribution to the theory of groups of prime power order*. London Mathematical Society **36** (1933), 29–95.

[14] B. Huppert, *Endliche Gruppen I*. Berlin-New York: Die Grundlehren der Mathematischen Wissenschaften, 1967.

[15] I. M. Isaacs. *Algebra-A Graduate Course*. American Mathematical Society, 2009.

[16] E. I. Khukhro. *p-Automorphisms of Finite p-Groups*. Cambridge University Press, 1998.

[17] B. Klopsch; I. Snopce. *A characterization of uniform pro-p groups*. arXiv: 1210.4965. (2012).

[18] M. Lazard. *Grupes analytiques p-adiques*. Puclications Mathématiques de I'I.H.É.S. **26** (1965), 5–219.

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

[20] L. Lubotzky; A. Mann. *Powerful p-groups. I. Finite groups*. Journal of Algebra **105** (1987), 484–505.

[21] J. C. L. Souza. *Involuções e seus Centralizadores em Grupos Finitos*. 2016. 76 f. Dissertação (Mestrado em Matemática), Universidade de Brasília, Brasília.

[22] J. S. Wilson. *Profinite Groups*. Oxford University Press, 1997.

[23] L. Wilson, PhD thesis. Chicago, 2002.