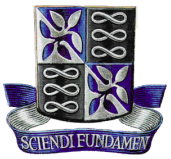
Universidade Federal da Bahia - UFBA
Instituto de Matemática - IM
Programa de Pós-Graduação em Matemática - PGMAT
Dissertação de Mestrado



Classificação de p-Grupos Finitos com Poucas Classes de Conjugação de Subgrupos Não-Normais

Ana Carolina Moura Teixeira

Salvador - Bahia
Março de 2015

Classificação de p-Grupos Finitos com Poucas Classes de Conjugação de Subgrupos Não-Normais

Ana Carolina Moura Teixeira

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Prof. Dr[a]. Carmela Sica.

Salvador - Bahia
Março de 2015

*T*266 Teixeira, Ana Carolina Moura.

Classificação de p-Grupos Finitos com Poucas Classes de Conjugação de Subgrupos Não-Normais/ Ana Carolina Moura Teixeira . – Salvador: UFBA - 2015.

50f. Orientador: Profª. Drª. Carmela Sica.

Dissertação (mestrado) – Universidade Federal da Bahia, Instituto de Matemática, Salvador, 2015.

1. Teoria de Grupos (Álgebra). 2. p-Grupos Finitos. 3. Grupos Nilpotentes. I. Carmela Sica. II. Universidade Federal da Bahia, Instituto de Matemática. III. Título.

CDD : 512

CDU : 512.54

Classificação de p-Grupos Finitos com Poucas Classes de Conjugação de Subgrupos Não-Normais

Ana Carolina Moura Teixeira

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 30 de Março de 2014.

Banca examinadora:

Prof. Dr[a]. Carmela Sica
UFBA

Prof. Dr[a]. Cristina Acciarri
UNB

Prof. Dr. Thierry Corrêa Petit Lobão
UFBA

Agradecimentos

Agradeço sobremaneira ao Senhor Deus e Pai, por todas bençãos e ajuda nesse período de estudo intenso e de grande aprendizado, que não se limitou ao mestrado. Agradeço à minha família pelo apoio e icentivo, mesmo com a distância permaneceram próximos. Aos meus amigos, àqueles que torceram por mim, estiveram comigo, oraram por mim, enfim, que me ajudaram de diversas maneiras durante esse período, que entenderam a ausência ou que me ajudaram dentro ou fora da matemática, em especial a Adriana que me aguentou por esses anos, convivendo diariamente com minhas chatices. Aos amigos que tive o previlégio de conhecer aqui em Salvador, foram poucos mas foram os melhores que pude encontrar: Lai, Moacyr e Maroca. Agradeço muitissíssimo à minha querida orientadora, pró Carmela, uma mulher incrível e uma profissional competente e muito responsável, agradeço a Deus por encontrá-la, pois sabia que Ele me daria o melhor que poderia encontrar aqui e ele me deu a senhora para me orientar, muito obrigada pela paciência, ajuda, icentivo e por todo aprendizado. À todos os professores, com os quais eu tive previlégio de aprender um pouco de matemática, em especial ao professor Ciro Russo, que me ensinou tanto de álgebra. Agradeço aos professores da UEFS pelo aprendizado e pelo icentivo, em especial ao professor Maurício, com quem dei meus primeiros passos em álgebra e com quem aprendi muito. Agradeço à minha turma e a todos os colegas da pós, aprendi muito com todos vocês. Agradeço ao Instituto de matemática e à todas as pessoas que direta e indiretamente contribuíram em todo o processo de mestrado. Agradeço ao Senhor por todos esses encontros e momentos, por tudo que vivi e aprendi, na certeza que a mão dEle nunca esteve longe de mim.

Finalmente, agradeço à CAPES pelo apoio financeiro concedido a mim durante todo o meu mestrado.

"A matemática é o alfabeto com qual DEUS escreveu o universo."

– Galileu Galilei.

Resumo

O objetivo deste trabalho é classificar os p-grupos finitos, que possuem poucas classes de conjugação de subgrupos não-normais. Seja $\nu(G)$ o número das classes de conjugação de subgrupos não-normais de um grupo G. É fácil observar que $\nu(G) = 0$ se, e somente se, G é um grupo de Dedekind. La Heye e Rhemtulla provaram que $\nu(G) \leq 1$ ou $\nu(G) \geq p$. Na dissertação serão classificados os p-grupos G com $\nu(G) \leq p+1$, p primo ímpar. Os grupos com $\nu(G) = 1$ e $\nu(G) = p + 1$ foram estudados por Brandl e o caso $\nu(G) = p$ foi estudado por Fernández-Alcober e Legarreta.

Palavras-chave: Teoria de grupos; p-grupos finitos; Grupos nilpotentes

Abstract

In this paper, the main goal is to classify the finite p-groups with few conjugacy classes of non-normal subgroups. Denote by $\nu(G)$ the number of conjugacy class of non-normal subgroups. It's easy to see that $\nu(G) = 0$ if, and only if, G is a Dedekind's group. La Heye and Rhemtulla have proved that either $\nu(G) \leq 1$ or $\nu(G) \geq p$. In this thesis, finite p-groups with $\nu(G) \leq p + 1$, where p is odd, will be classified. The study of groups with $\nu(G) = 1$ and $\nu(G) = p + 1$ were studied by Brandl, the case $\nu(G) = p$ was studied by Fernàndez-Alcober and Legarreta.
Keywords: Group Theory; finite p-groups; Nilpotent groups

Sumário

Introdução

Os grupos de Dedekind, grupos em que todos os subgrupos são normais, já foram estudados e a sua estrutura é bem conhecida na literatura, afirmando-se que um grupo com tal característica ele é abeliano ou produto direto de $Q_8 \times A \times B$, onde A é um 2-grupo abeliano elementar e B é um grupo que todos elementos têm ordem ímpar. Desse modo, decidiu-se estudar grupos próximos a grupos de Dedekind, por exemplo, grupos com "poucos" subgrupos não-normais. Assim, se H é um subgrupo de G não-normal, todos os seus conjugados são do mesmo tipo, faz sentido considerar os grupos com "poucas" classes de conjugação de subgrupos não normais. Denotando pelo $\nu(G)$ o número de classes de conjugação de subgrupos não-normais, o estudo começa por considerar os grupos G tal que $\nu(G) = 1$. Brandl, em 1995, estudou os p-grupos finitos com esta propriedade e mostrou que a única possibilidade é que o grupo seja isomorfo a: $M_p^n = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle$, onde $n \geq 3$ se $p > 2$, e $n \geq 4$ se $p = 2$. Por outro lado, La Haye e Rhemtulla mostraram que este número $\nu(G)$, se não for igual a 1, é necessariamente, igual ou superior a p. Então surge a pergunta: é possível dar uma descrição dos grupos com $\nu(G) = p$? Em 2010, Legarreta e Fernández-Alcober mostraram que é válido o questionamento acima e, para p ímpar, o grupo G tem a seguinte apresentação, com $n \leq 4$: $\langle a, b \mid a^{p^{n-2}} = b^{p^2} = 1, a^b = a^{1+p^{n-3}} \rangle$. Em 2013, Brandl também deu uma descrição dos grupos com $\nu(G) = p + 1$.

O objetivo deste trabalho é ilustrar as técnicas e os resultados obtidos para abordar o problema da classificação dos grupos com estas propriedades.

A dissertação está definida do seguinte modo: no primeiro capítulo, apresentamos algumas definições e resultados da Teoria de p-grupos de classe maximal e p grupo regular, bem como alguns resultados básicos de teoria de grupos. No segundo capítulo, será estudado o caso em que $\nu(G) = p$. No capítulo três, encontraremos o grupo quando $\nu(G) = p + 1$ e, finalmente, faremos a classificação de $\nu(G) \leq p + 1$ com $p \neq 2$ e primo.

Capítulo 1

Conceitos Iniciais

Neste capítulo, serão apresentados resultados fundamentais da teoria de p-grupos finitos, que serão necessários para o entendimento de todo o texto. Em todo trabalho serão preservadas as notações tradicionais. Caso haja necessidade de outras notações, estas serão devidamente introduzidas. Aqui, foram utilizadas como referências [FA00], [Ro82], bem como notas de aula da disciplina Tópicos de Álgebra, ministradas pela professora Drª. Carmela Sica, no curso de Mestrado em Matemática da Universidade Federal da Bahia.

1.1 Grupos Nilpotentes

Definição 1.1. *Um grupo G diz-se nilpotente se ele contém uma série de subgrupos*

$$\{1\} = G_0 \leq G_1 \leq ... \leq G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente $\frac{G_{i+1}}{G_i}$ está contido no centro de $\frac{G}{G_i}$, $\forall i \in \{0, \cdots, n-1\}$, ou seja, $\frac{G_{i+1}}{G_i} \leq Z\left(\frac{G}{G_i}\right)$.
Uma tal série de subgrupos de G diz-se uma série central de G.

Veremos, na próxima seção, que as propriedades de nilpotência podem ser caracterizadas em termos de duas diferentes séries de G, que são chamadas de Série Central Inferior e Série Central Superior.

1.1.1 Séries Centrais Superior e Inferior

Série Central Superior

Dado um grupo G, chamemos $Z_0(G) = \{1\}$ e $Z_1(G) = Z(G)$ e para todo $i > 1$ definimos $\frac{Z_i(G)}{Z_{i-1}(G)} = Z\left(\frac{G}{Z_{i-1}(G)}\right)$. Como $Z_i(G) \leq Z_{i+1}(G)$ temos a seguinte cadeia,

$$\{1\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_n(G) \leq \cdots$$

com a propriedade $\frac{Z_i(G)}{Z_{i-1}(G)} \leq Z\left(\frac{G}{Z_{i-1}(G)}\right)$.

É claro que, se existe $c \in \mathbb{N}$ tal que $Z_c(G) = G$, essa é uma série central e o grupo G é nilpotente.

Comutadores

Definição 1.2. *Para todo $x, y \in G$, definimos o comutador como $[x, y] = x^{-1}y^{-1}xy$.*

Desta forma, temos que x e y comutam se, e somente se, $[x, y] = 1$. Para comutadores de comprimento maior que 2, definiremos indutivamente:$[x, y, z] := [[x, y], z]$ e, para $n \geq 3$:

$$[x_1, x_2, \cdots, x_n] = [[x_1, \cdots, x_{n-1}], x_n].$$

O comutador simples de peso n.

Definimos, de modo mais geral, o comutador de dois subgrupos H e K de G como:

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

Definição 1.3. *Se G é um grupo e H um subgrupo de G tal que $\alpha(H) = H$, para todo automorfismo $\alpha : G \to G$, então H é subgrupo característico em G.*

Temos as seguintes propriedades, válidas para os comutadores:

Proposição 1.4. *Sejam G um grupo, $x, y, z \in G$ e um homomorfismo de grupos $\sigma : G \to H$ e $H, K, L \leq G$. Então, valem:*

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

(ii) $\sigma([x, y]) = [\sigma(x), \sigma(y)]$;

(iii) $[xy, z] = [x, z]^y[y, z] = y^{-1}[x, z]y[y, z]$ *e* $[x, yz] = [x, z][x, y]^z = [x, z]z^{-1}[x, y]z$;

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

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

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

Demonstração. (i) até (iii) são facilmente resolvidos pela definição de comutadores.

(iv) é consequência de (ii). Também, (v) vem de (iv) se considerarmos σ sendo o epimorfismo não trivial de G em G/N. Então falta provarmos só o item (vi). É claro que $[H, L][K, L] \leq [HK, L]$. Para inclusão inversa, primeiro vamos ver que $[H, L][K, L]$ é subgrupo. Observe que, para todo $k \in K$ e $l, l' \in L$,

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

por (iii). Logo L normaliza $[K, L]$. Portanto, como H normaliza L, $[H, L]$ também normaliza $[K, L]$ e, em particular, $[H, L][K, L]$ é um subgrupo. Para provar que $[HK, L]$ está contido neste subgrupo, é suficiente mostrar que o gerador $[hk, l]$ está lá. Como $[hk, l] = [h, l][h, l, k][k, l]$ e então, $[h, l, k] \in [H, L, K] \leq [L, K] = [K, L]$. Segue que $[HK, L] \leq [H, L][K, L]$. □

Proposição 1.5 (Identidade de Witt)**.** $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$

Demonstração. A identidade de Witt pode ser verificada utilizando a definição e propriedades dos comutadores. □

Definição 1.6. *Seja um grupo G, definimos o subgrupo derivado de G, denotado como G' como,*

$$G' = \langle [x, y]; x, y \in G \rangle.$$

Isto é, o subgrupo derivado é gerado pelos comutadores. Esse grupo tem propriedades importantes (das quais enuciaremos algumas), por isso é interessante estudá-lo. A proposição seguinte nos mostra que subgrupo nos fornece o maior quociente abeliano.

Proposição 1.7. *Sejam G grupo e H subgrupo normal de G. Então, o grupo quociente $\frac{G}{H}$ é abeliano, se e somente se, $G' \leq H$.*

Demonstração. ($\Rightarrow$) Para todo $x, y \in G$, $xG'yG' = xyG' = yx[x, y]G' = yxG' = yG'xG'$. Logo, $\frac{G}{G'}$ é abeliano. Como $H \triangleleft G$ e $\frac{G}{H}$ é abeliano, então $xHyH = xyH = yxH \Rightarrow x^{-1}y^{-1}xyH = H \Rightarrow x^{-1}y^{-1}xy \in H$, $\forall x, y \in G$. Logo, $G' \leq H$.

($\Leftarrow$) $G' \leq H \triangleleft G$ e $\frac{G}{G'}$ é abeliano. Pelo 1º Teorema do Isomorfismo, temos que $\frac{G}{H} \cong \frac{\frac{G}{G'}}{\frac{H}{G'}}$. Como $\frac{H}{G'} \leq \frac{G}{G'}$ então, $\frac{H}{G'}$ é abeliano. Logo, $\frac{G}{H}$ é abeliano. □

A seguir algumas propriedades de comutador:

Proposição 1.8. *$[H, K] \leq H$ se, e somente se, $K \leq N_G(H)$.*

Demonstração. $[h, k] \in H$ se, e somente se, $h^{-1}k^{-1}hk \in H$ se, e somente se, temos que $k^{-1}hk \in H$, para todo $k \in K$.

□

Proposição 1.9. *$[H, K] = 1$ se, e somente se, $H \leq C_G(K)$*

Demonstração. $[H, K] = 1$ se, e somente se, $H \leq C_G(K)$, pois: $h^{-1}k^{-1}hk = 1$ para todo $h \in H$ e $k \in K$ se, e somente se, $hk = kh$. □

Também podemos observar que,

Observação 1.10.

$$\frac{H_i}{H_{i-1}} \leq Z\left(\frac{G}{H_{i-1}}\right) \Leftrightarrow \left[\frac{H_i}{H_{i-1}}, \frac{G}{H_{i-1}}\right] = H_{i-1} \Leftrightarrow [H_i, G]H_{i-1} = H_{i-1} \Leftrightarrow [H_i, G] \leq H_{i-1}.$$

Definição 1.11 (Fecho Normal)**.** *Seja um grupo G e $X \leq G$. Definimos o Fecho Normal de X em G e denotamos por X^G como:*

$$X^G = \bigcap_{\substack{N \trianglelefteq G \\ X \subseteq N}} N = \langle g^{-1}xg |\ x \in X, g \in G \rangle.$$

Isto é, o menor subgrupo normal de G que contém X.

Lema 1.12. *Seja $G = \langle X \rangle$, então $G' = \langle [x,y] |\ x, y \in X \rangle^G$.*

Demonstração. Chamamos de $N = \langle [x,y] |\ x, y, \in X \rangle^G$, G/N é abeliano, pois todos os geradores comutam, segue que $G' \leq N$. Como obviamente $N \leq G'$, temos a igualdade. □

Definição 1.13. *Seja G um grupo nilpotente. Dizemos que G tem classe de nilpotência, $cl(G)$, igual a c se $c = min\{n |\ n$ é comprimento de uma série central$\}$.*

Teorema 1.14 (Lema dos três subgrupos)**.** *Sejam H, K e L subgrupos de $G \in N$ um subgrupo normal de G. Se $[H,K,L], [K,L,H] \leq N$ então, $[L,H,K] \leq N$.*

Demonstração. Vamos trabalhar com o grupo quociente G/N e assumir que $N = 1$, desse modo, $[H,K,L] = [K,L,H] = 1$ e então, pela identidade de Witt, temos que

$$[h, k^{-1}, l]^k [k, l^{-1}, h]^l [l, h^{-1}, k]^h = 1,$$

logo, $[l, h^{-1}, k] = 1$ para todo $l \in L$, $h \in H$ e $k \in K$. Isso implica que $[l,h,k] = 1$, como $[L,H] = \langle [l,h] \rangle$. Concluímos que $[L,H,K] = 1$. □

Definição 1.15. *Seja G um grupo. Definimos indutivamente:*
$\gamma_1(G) = G$
$\gamma_2(G) = [\gamma_1(G), G] = [G,G] = G'$
$\vdots$
$\gamma_i(G) = [\gamma_{i-1}(G), G]$.

Lema 1.16. *Seja G um grupo, então $\gamma_i(G)$ é um subgrupo característico em G para todo inteiro i com $i > 1$. Desse modo segue que a cadeia*

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_i(G) \geq \cdots$$

é uma série central e é dita série central inferior do grupo G.

Demonstração. Temos que cada termo $\gamma_i(G)$ é característico em G; em particular, $\gamma_i \trianglelefteq G$ para todo inteiro i. Desse modo, de $\gamma_i(G) = [\gamma_{i-1}(G), G]$, obtemos

$$\left[\frac{\gamma_{i-1}(G)}{\gamma_i(G)}, \frac{G}{\gamma_i(G)} \right] = \{1\}.$$

Logo,

$$\frac{\gamma_{i-1}(G)}{\gamma_i(G)} \leq Z\left(\frac{G}{\gamma_i(G)}\right),$$

para todo inteiro i, com $i \geq 1$. □

Teorema 1.17. *Sejam G um grupo e N um subgrupo normal de G. Então $\gamma_i(G/N) = \gamma_i(G)N/N$, para todo $i \geq 1$.*

Demonstração. Vamos fazer indução sobre i. Se $i = 1$, $\gamma_1(\frac{G}{N}) = \frac{G}{N} = \frac{\gamma_1(G)N}{N}$ e já é válido o resultado.

Supondo $i > 1$, hipótese de indução $\gamma_{i-1}(\frac{G}{N}) = \frac{\gamma_{i-1}(G)N}{N}$. Desse modo,

$$\begin{aligned}
\gamma_i\left(\frac{G}{N}\right) &:= \left[\gamma_{i-1}\left(\frac{G}{N}\right), \frac{G}{N}\right] \\
&= \left[\frac{\gamma_{i-1}(G)N}{N}, \frac{G}{N}\right] \\
&= \frac{[\gamma_{i-1}(G)N, G]N}{N} \\
&= \frac{[\gamma_{i-1}(G), G][N, G]N}{N} \\
&= \frac{\gamma_i(G)N}{N}.
\end{aligned}$$

□

Proposição 1.18. *Seja G um grupo de classe de nilpotência c. Então $\gamma_{c-i+1}(G) \leq Z_i(G)$ para todo $0 \leq i \leq c$.*

Demonstração. Esta prova é feita por indução em i. Se $i = 0$, então $\gamma_{c+1}(G) = 1 = Z_0(G)$ e é válido o resultado. Por outro lado, temos que,

$$[\gamma_{c+1-i}(G), G] = \gamma_{c+1-(i-1)}(G) \leq Z_{i-1}(G),$$

pela hipótese de indução, e consequentemente $\gamma_{c+1-i}(G) \leq Z_i(G)$. □

Teorema 1.19. *Para todo grupo G, $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.*

Demonstração. Vamos provar, fazendo indução sobre i. Se $i = 1$, então

$$[\gamma_1(G), \gamma_j(G)] \leq [G, \gamma_j(G)] = \gamma_{1+j}(G).$$

Para $i \geq 2$, por hipótese de indução temos que,

$$[\gamma_{i-1}(G), \gamma_j(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$$

e $[\gamma_j(G), G, \gamma_{i-1}(G)] \leq [\gamma_{j+1}(G), \gamma_{i-1}(G)] = \gamma_{i+j}(G)$. Logo, pelo lema dos três subgrupos, temos que, $[G, \gamma_{i-1}(G), \gamma_j(G)] = [\gamma_i(G), \gamma_j(G)] = [\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. □

Lema 1.20. *Se G é um grupo nilpotente, então $Z(G) \neq \{1\}$.*

Demonstração. Seja $1 = G_0 \lneqq G_1 \lneqq \cdots \lneqq G_n(G)$. Isto implica que $G_1 \neq \{1\}$ e

$$\frac{G_1}{\{1\}} \leq Z\left(\frac{G}{\{1\}}\right),$$

logo $G_1 \leq Z(G)$ e portanto $Z(G) \neq \{1\}$. □

Exemplo 1.21. *Todo grupo abeliano é nilpotente.*

Lema 1.22. *Seja G um grupo e $N \trianglelefteq G$. Se G/N é cíclico, então $G' = [G, G] = [G, N]$.*

Demonstração. Como G/N é cíclico, temos que $G/N = \langle xN \rangle$, logo $G = \langle x, N \rangle$. Seja $g_1 = x^r n_1$ e $g_2 = x^s n_2$, com $g_1, g_2 \in G$. Dessa forma,

$$\begin{aligned}
[g_1, g_2] &= [x^r n_1, x^s n_2] \\
&= [x^r, x^s n_2]^{n_1} [n_1, x^s n_2] \\
&= [x^r, n_2]^{n_1} [x^r, x^s]^{n_2 n_1} [n_1, x^s n_2] \\
&= [x^r, n_2]^{n_1} [n_1, x^s n_2] \in [G, N], \text{e obtemos o resultado desejado.}
\end{aligned}$$

□

Teorema 1.23. *Se G é nilpotente e N é um subgrupo não trivial de G, tal que $N \trianglelefteq G$ então $N \cap Z(G) \neq 1$.*

Agora vamos relembrar mais algumas propriedades de Teoria de Grupos.

Teorema 1.24. *Seja G um grupo periódico abeliano finitamente gerado, então*

$$G = \bigoplus_{i \in I} A_i.$$

Com A_i cíclico de ordem uma potência de primo.

Definição 1.25. *Seja G um grupo, definimos a classe de conjugação de um elemtento x, e denotamos por $[x]_{C_G}$, como $[x]_{C_G} = \{x^g |\ g \in G\}$, isto é, a órbita de um elemento $x \in G$ sob a ação de conjugação.*

Definição 1.26. *Sejam G um grupo e H tal que $H \leq G$. A classe de conjugação de H, denotado por $[H]_{C_G}$, é o conjunto de subgrupos $[H]_{C_G} = \{g^{-1} H g |\ g \in G\} = \{H^g |\ g \in G\}$, isto é, a órbita de um subgrupo H sob a ação de conjugação.*

Teorema 1.27 (Equação das Classes)**.** *Dado um grupo G:*

$$|G| = |Z(G)| + \sum_{\substack{[x]_{C_G} \in G/C_G \\ x \notin Z(G)}} |G : C_G(x)|.$$

Teorema 1.28. *Seja G um grupo, se $\frac{G}{Z(G)}$ é cíclico, então G é abeliano.*

Demonstração. Temos que $\frac{G}{Z(G)} = \langle xZ(G)\rangle$, logo, para todo $g \in G$, $g = x^n z$ com $n \in \mathbb{N}$ e $z \in Z(G)$. Dessa forma,

$g_1g_2 = (x^{n_1}z_1)(x^{n_2}z_2) = (x^{n_2}z_2)(x^{n_1}z_1) = g_2g_1$. Logo G é abeliano. □

Definição 1.29. *Seja G um grupo finito de ordem $|G| = p^n m$ onde p é primo e não divide m. Um subgrupo de G de ordem p^n chama-se um p-grupo de Sylow de G.*

1.2 p-Grupos finitos

Definição 1.30. *Seja G um grupo, dizemos que G é p-grupo se para todo $x \in G$, $|x| = p^\alpha$, $\alpha \in \mathbb{N} \cup \{0\}$ e p primo.*

Teorema 1.31 (Lema de Cauchy)**.** *Seja G um grupo finito e p um primo que divide $|G|$. Então, existe um elemento em G de ordem p.*

Demonstração. Ver [**?**] 1.6.17. □

Proposição 1.32. *G é um p-grupo finito se, e somente se, $|G| = p^\alpha, \alpha \in \mathbb{N}$.*

Demonstração. ($\Rightarrow$) Como G é um p-grupo finito, existe um primo q tal que $q\Big||G|$, pelo lema de Cauchy, existe $y \in G$ tal que $o(y) = q$ o que implica que $p = q$. Logo $|G| = p^\alpha$.

($\Leftarrow$) $o(x)\Big||G|$. □

Teorema 1.33. *Se G um p-grupo finito, então $Z(G) \neq 1$.*

Demonstração. De fato, suponha $Z(G) = 1$, pela equação das classes temos que

$$|G| = |Z(G)| + \sum_{\substack{[x]_{C_G} \in G/C_G \\ x \notin Z(G)}} |G : C_G(x)|.$$

Sabemos que $p\Big||G|$ e como $p\Big||G : C_G(x)|$, concluímos que $p\Big|Z(G)$. Logo $|Z(G)| \neq 1$. □

Corolário 1.34. *Seja G um p-grupo finito. Então todo subgrupo normal de G de ordem p é central em G.*

Demonstração. Decorre diretamente do fato que $Z(G) \neq \{1\}$. □

Corolário 1.35. *Seja p um primo. Então, todos os grupos de ordem p^2 são abelianos.*

Demonstração. Seja G tal que $|G| = p^2$, por 1.33, $|Z(G)| \neq 1$, então temos duas possibilidades para a ordem do centro de G, ou seja, $|Z(G)| = p$ ou $|Z(G)| = p^2$. Se $|Z(G)| = p$, então $|G : Z(G)| = p$. Logo $\frac{G}{Z(G)} \simeq C_p$ e pelo resultado anterior, temos que G é abeliano. Se $|Z(G)| = p^2$, então $Z(G) = G$. Portanto, G é abeliano. □

Definição 1.36. *Um p-grupo G é denominado p-grupo abeliano elementar se G for abeliano e $x^p = 1$, para todo $x \in G$.*

A seguinte proposição relaciona p-Grupos finitos com Grupos Nilpotentes:

Proposição 1.37. *Todo p-grupo finito é nilpotente.*

Demonstração. Suponha $G \neq \{1\}$, Sabemos por 1.33 que $Z(G) \neq 1$. Se existe i tal que $Z_i(G) = G$, então o grupo é nilpotente. Suponha $Z_i(G) \neq G$ e Como $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_{i-1}(G)}\right) \neq 1$ temos que $Z_i(G) \lneqq Z_{i+1}(G)$ e a série

$$\{1\} \lneqq Z(G) \lneqq Z_2(G) \lneqq \cdots$$

é estritamente crescente. Sendo G finito, temos que G é nilpotente. □

Teorema 1.38 (Teorema de Sylow)**.** *Seja G um grupo de ordem finita. Temos que:*

(i) *Se $p^\alpha \Big| |G|$, então existe $H \leq G$ tal que $|H| = p^\alpha$;*

(ii) *Se H, K p-subgrupos de Sylow, então existe $g \in G$ tal que $H = K^g = g^{-1}Kg$.*

Teorema 1.39. *Seja G um grupo finito, são equivalentes:*

(1) G é nilpotente;

(2) $H \leq G$, então existe uma série $K_0 = H \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_t = G$;

(3) Se $H \lneqq G$, então $H \lneqq N_G(H)$;

(4) Se $M \leq G$ maximal, então $M \trianglelefteq G$

(5) $G = \prod_{i \in \mathbb{N}}$, P_i P-subgrupo de Sylow.

Demonstração. (1) ⇒ (2) G é nilpotente de classe c, então $1 = Z_0 \leq Z_1 \leq \cdots \leq Z_c = G$, logo $H = HZ_0 \leq HZ_1 \leq \cdots \leq HZ_c = G$. Mostraremos que $HZ_i \trianglelefteq HZ_{i+1}$.

Temos que, dado $hz \in HZ_i$, para todo $h_1 \in H$, $(hz)^{h_1} = h^{h_1}z^{h_1} \leq HZ_i$, logo $H \leq N_G(HZ_i)$. Por outro lado,

$$[HZ_i, Z_{i+1}] \leq [G, Z_{i+1}] \leq Z_i \leq Z_iH,$$

isso implica que $Z_{i+1} \leq N_G(HZ_i)$. Logo, $HZ_{i+1} \leq N_G(HZ_i)$ e portanto, $HZ_i \trianglelefteq HZ_{i+1}$. E obtemos o resultado.

(2) ⇒(3). Sabemos que $H \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_c = G$, logo $K_1 \leq N_G(H)$. Se $H \lneqq G$, então $H \lneqq K_1 \leq N_G(H)$. Logo, $H \lneqq N_G(H)$.

(3) ⇒ (4). Seja $M \lessdot G$, por hipótese temos que, $M \lneqq N_G(M) \leq G$ então $N_G(M) = G$, logo $M \trianglelefteq G$.

(4) ⇒ (5). Se P é p-subgrupo de Sylow, mostraremos que $P \trianglelefteq G$.

Sabemos que se $N_G(P) = G$ então $P \trianglelefteq G$. Supondo $N_G(G) \neq G$, então existe M maximal, tal que $M \subsetneqq G$ e $N_G(P) \leq M$. Como $M \trianglelefteq G$ para todo $g \in G$ e $P \leq N_G(P) \leq M$, temos que $g^{-1}Pg \leq g^{-1}Mg = M$, já que $g^{-1}Pg$ é p-subgrupo de Sylow de M temos que existe $m \in M$ tal que $g^{-1}Pg = m^{-1}Pm$, logo, $mg^{-1}Pgm^{-1} = P$ e então, $gm^{-1} \in N_G(P) \leq M$ e $g \in M$, o que é uma contradição, logo P é normal em G. Como G é um grupo finito, digamos que $|G| = n$ com $n \in \mathbb{N}$ e $n = p_1^{\alpha} \cdots p_k^{\alpha}$ com cada p_k, primo, logo $|G| = p_1^{\alpha} \cdots p_k^{\alpha}$ e isto implica que $|G| = P_1 \cdots P_k$ e cada P_i é normal, temos que $G = P_1 \times \cdots \times P_k$.

(5) $\Rightarrow$ (1). Sabemos que todo p-grupo finito é nilpotente e produto direto finito de grupos nilpotentes é ainda nilpotente, logo G é nilpotente. □

Abaixo temos exemplos de grupos periódicos abelianos finitamente gerados:

Exemplo 1.40. *Seja G um grupo, tal que $|G| = p^k$, com $k \in \mathbb{N}$:*
Se $k = 1$, então $|G| = p$ e $G \simeq C_p$;
Se $k = 2$, então $|G| = p^2$ e $G \simeq C_{p^2}$ ou $G \simeq C_p \times C_p$;
Se $k = 3$, então $|G| = p^3$ e $G \simeq C_{p^3}$ ou $G \simeq C_p \times C_{p^2}$ ou $G \simeq C_p \times C_p \times C_p$

A próxima propriedade é muito importante e vai ser utilizada no decorrer do texto; a prova está em **[?]** p.141.

Proposição 1.41. *Um p-grupo finito tem exatamente um subgrupo de ordem p se, e somente se, G é cíclico, para $p \neq 2$ ou G é quatérnio generalizado.*

Definição 1.42. *Um subgrupo M de G é dito subgrupo maximal de G, se $M \neq G$ e não existe $H \leq G$ tal que $M < H < G$. De modo semelhante, $N \neq G$ é um subgrupo minimal de G se $N \neq 1$ e não existe subgrupo $K \leq G$ com $1 < K < N$.*

Teorema 1.43. *Seja G um p-grupo finito.*

(i) Se $H < G$ então $H < N_G(H)$. (A condição do Normalizador).

(ii) Se M é subgrupo maximal de G então M é normal em G e $|G : M| = p$.

Demonstração. (i) e (ii) decorrem de 1.39. □

Definição 1.44 (Subgrupo de Frattini)**.** *Dado G um grupo, definimos o sugbrupo de Frattini de G, como a interseção de todos os subgrupos maximais e o denotamos por* $\Phi(G) = \bigcap_{M \lessdot G} M$.

Veremos que um sugbrupo de Frattini de um grupo G é construído por elementos não geradores de G.

Definição 1.45. *Seja um grupo G, dizemos que $g \in G$ é não-gerador se, e somente se, $G = \langle X, g\rangle, X \subseteq G$, então $G = \langle X\rangle$.*

O resultado a seguir mostra que o subgrupo de Frattini é o conjunto dos não-geradores.

Proposição 1.46. *Em um grupo G, $\Phi(G) = \{g \in G |\ g$ é não gerador$\}$.*

Demonstração. ($\subseteq$) Seja $g \in \Phi(G)$ e $G = \langle X, g\rangle$. Suponha, por absurdo, que $G \neq \langle X\rangle$. Definamos o conjunto,

$$\Omega = \{H \leq G |\ \langle X\rangle \leq H, g \notin H\}.$$

Então,$(\Omega, \subseteq)$ é um conjunto ordenado. Seja $\Sigma \in \Omega$ totalmente ordenado, $\bigcup_{i\in\mathbb{N}} H_i \in \Omega$ e Σ possui cota superior em Ω, já que $H_i \leq G$ e $g \notin H_i$, para todo $i \in \mathbb{N}$. Logo, pelo lema de Zorn, existe elemento maximal M de Ω.

Suponha que exista L tal que $M \lneqq L \leq G$. Temos que $L \notin \Omega$ e $\langle X\rangle \leq M < L$, então $g \in L$ e $L = G = \langle X, g\rangle$. Logo M é maximal em G. Mas $g \in \Phi(G) \leq M$. Absurdo, pela definição de Ω. Donde $G = \langle X\rangle$ e g é não gerador.

($\supseteq$) Seja $g \in G$ tal que g é não gerador de G. Queremos mostrar que $g \notin \Phi(G)$. Então, existe um maximal M de G, $g \notin M$, logo segue que $M \neq \langle g, M\rangle$ e $G = \langle g, M\rangle$. mas isto implica que $G = M$, já que g é não gerador. Absurdo, pois M é maximal. □

Teorema 1.47. *Seja G um grupo finito e $x_1, \cdots, x_n \in G$. Então temos que $G = \langle x_1, \cdots, x_n\rangle$ se, e somente se, $\frac{G}{\Phi(G)} = \langle x_1\Phi(G), \cdots, x_n\Phi(G)\rangle$.*

Demonstração. ($\Rightarrow$) Sempre vale.

($\Leftarrow$) $G = \langle x_1, \cdots, x_n, \Phi(G)\rangle$, então $G = \langle x_1, \cdots, x_n\rangle$. □

Podemos observar que a implicação direta é sempre válida para qualquer que seja o grupo dado, todavia a implicação inversa não é garantida sempre, isto fica mais claro com o próximo exemplo:

Exemplo 1.48. *Consideremos o grupo D_8, diedral de ordem 8, que temo como apresentação:*

$$D_8 = \langle a, b |\ a^4 = b^2 = 1, a^b = a^{-1}\rangle.$$

Consideremos o subgrupo normal, $\langle a\rangle \leq D_8$, o subgrupo quociente $\frac{D_8}{\langle a\rangle}$ é gerado por $b\langle a\rangle$, mas $D_8 \neq \langle b\rangle$.

Teorema 1.49 (Teorema da base de Burnside)**.** *Seja G um p-grupo finito. Então:*

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

(ii) O conjunto $\{x_1, \cdots, x_m\}$ é um conjunto minimal de geradores de G se, e somente se $\{x_1\Phi(G), \cdots, x_n\Phi(G)\}$ é uma base de $\frac{G}{\Phi(G)}$, como espaço vetorial sobre $\mathbb{F}_p$.

(iii) O número minimal, d, de geradores do grupo G coincide com a dimensão de $\frac{G}{\Phi(G)}$ como um espaço vetorial sobre $\mathbb{F}_p$. Ou seja, $|G : \Phi(G)| = p^d$.

Demonstração.

(i) Precisamos mostrar que $x\Phi(G)y\Phi(G) = y\Phi(G)x\Phi(G)$ e $(x\Phi(G))^p = \Phi(G)$, para todo $x, y \in G$ ou seja, que $x^{-1}y^{-1}xy, x^p \in M$, para todo subgrupos maximal M de G. Mas como todo maximal é normal e $|G : M| = p, istobviopor 1.43$, para todo $M \leq G$, Maximal.

(ii) No teorema anterior vimos que $G = \langle x_1, \cdots, x_n \rangle$ se, e somente se,

$$\frac{G}{\Phi(G)} = \langle x_1\Phi(G), \cdots, x_n\Phi(G) \rangle.$$

Então temos que $\{x_1, \cdots, x_n\}$ é um cojunto minimal de geradores se, e somente se $\{x_1\Phi(G), \cdots, x_n\Phi(G)\}$ um conjunto minimal de $\frac{G}{\Phi(G)}$, o que equivale a dizer que o conjunto é uma base de $\frac{G}{\Phi(G)}$.

(iii) Se $\frac{G}{\Phi(G)}$ tem uma base com d elementos, então $\frac{G}{\Phi(G)} \simeq \mathbb{Z}_p^d$, logo $|G : \Phi(G)| = p^d$.

□

Isto é, observamos que, quando G é um p-grupo finito, podemos encontrar a quantidade mínima de geradores de G, através do subgrupo de Frattini.

Se G tem ordem p^m, o próximo teorema nos mostra que a classe de nilpotência de G é $< m$.

Teorema 1.50. *Seja G um p-grupo de ordem $p^m \geq p^2$ e $cl(G) = c$. Então:*

(i) G é nilpotente de classe até, no máximo, $m - 1$.

(ii) $|G : Z_{c-1}(G)| \geq p^2$.

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

Demonstração. Começaremos provando o item (ii).

Suponha, por contradição, que $|G : Z_{c-1}(G)| \leq p$, isso implica que $G/Z_{c-1}(G)$ é cíclico e portanto por 1.29

$$\frac{G}{Z_{c-1}(G)} \cong \frac{G/Z_{c-2}(G)}{Z_{c-1}(G)/Z_{c-2}(G)} = \frac{G/Z_{c-2}(G)}{Z(G/Z_{c-2}(G))},$$

isto implica que $\frac{G}{Z_{c-2}}$ é abeliano e $Z_{c-1}(G) = G$ absurdo. Então $|G : Z_{c-1}(G)| \geq p^2$. Para provar (iii), lembrando que $G' = \gamma_2(G)$, temos que

$$\gamma_i(G) \leq Z_{c-i+1}(G)$$

e então $\gamma_2(G) \leq Z_{c-1}(G)$ e $|G : G'| \geq p^2$.

Finalmente, a partir da série

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_{c-1}(G) \leq Z_c(G) = G,$$

sabemos que $|G| = \prod_{i=0}^{c-1} |Z_{i+1}(G) : Z_i(G)|$ e sendo $|G : Z_{c-1}(G)| \geq p^2$, temos, $|G| = p^m \geq p^{(c-1)+2}$ e isto implica que, $c \leq m-1$ e acontece (i). □

Corolário 1.51. *Seja G um p-grupo e seja N um subgrupo normal de G de índice $p^i \geq p^2$. Então $\gamma_i(G) \leq N$.*

Demonstração. O grupo G/N tem ordem p^i, com $i \geq 2$. Então, pelo teorema anterior,temos que $cl(G/N) \leq i-1$ e consequentemente $\gamma_i(G/N) = N$ e como $\gamma_i(G/N) = \gamma_i(G)N/N$, concluímos que $\gamma_i(G) \leq N$. □

Definição 1.52 (p-Grupos de Classe Maximal)**.** *Dizemos que um p-grupo de ordem p^m, com $m \geq 2$ é um p-grupo de classe maximal se $cl(G) = m-1$.*

Exemplos de p-grupos de classe maximal:

É claro que todo grupo de ordem p^2 é de classe maximal, também podemos observar que grupos não abelianos de ordem p^3 detém a mesma propriedade.

Os grupos de ordem p^3 são bem conhecidos. Há duas classes de isomorfismo de grupos não abelianos de ordem p^3:

Se $p \neq 2$, temos a classe correspondente a

$$M_{p^3} = \langle a, b |\ a^{p^2} = b^p = 1, a^b = a^{1+p} \rangle$$

e

$$E_{p^3} = \langle a, b, c |\ a^p = b^p = c^p = 1; [a,b] = [a,c] = 1 \rangle.$$

Como $cl(M_{p^3}) \leq 3-1$, temos que $cl(M_{p^3}) \leq 2$. Por outro lado, $cl(M_{p^3}) \geq 2$, já que $cl(M_{p^3}) \neq 1$. Portanto, $cl(M_{p^3}) = 2$ e M_{p^3} é de classe maximal. De igual modo, também podemos mostrar que E_{p^3} é de classe maximal. E temos as seguintes séries centrais de G, com $G = M_{p^3}$ ou $G = E_{p^3}$:

Série central superior:

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq Z_2(G) = G$$

e Série Central inferior:

$$G = \gamma_0(G) \geq G' = \gamma_1(G) \geq \gamma_3(G) = 1.$$

E $Z(G) = G'$.

Para $p = 2$, a classe de isomorfismo corresponde a

$$D_8 = \langle a, b |\ a^4 = a^2 = 1; a^b = a^{-1} \rangle$$

e

$$Q_8 = \langle a, b |\ a^4 = 1; b^2 = a^2; a^b = a^3 \rangle.$$

Estes grupos também são de classe maximal, pois, calculando a série central inferior de D_8, por exemplo, temos que:

Tomando $a, b \in D_8$,
$\gamma_2(G) = [a, b] = a^{-1}a^b = a^{-2}$, implica que $G' = \langle a^2 \rangle$
$\gamma_3(G) = \langle [a^2, b] \rangle^{G'} = \langle a^{-2}a^b \rangle = \langle a^{-3} \rangle = 1$, logo

$$\gamma_1(G) = G \geq \gamma_2(G) \geq \gamma_3(G) = 1.$$

Portanto, $cl(D_8) = 2$. Do mesmo modo, temos que Q_8 é de classe maximal. O resultado também é válido para D_{2^n} e Q_{2^n}, com $n \in \mathbb{N}$ e a prova é semelhante a que acabamos de ver.

Os grupos M_{p^3}, E_{p^3}, D_8 e Q_8 são chamados extra-especiais, pois $|G'| = |Z(G)| = p$.

O próximo resultado caracteriza p-grupos de classe maximal.

Teorema 1.53. *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* $2 \leq i \leq m$;

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

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

(iv) Se N é um subgrupo normal de G de índice $\geq p^2$, então G/N tem também classe maximal;

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

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

Mas, como $|\gamma_i(G) : \gamma_{i+1}(G)| \geq p$ e, pelo teorema 1.50, $|G : G'| \geq p^2$, segue o resultado.

(ii) Sabemos que $G' \leq \Phi(G)$ e pela parte (i), temos que $|G : \Phi(G)| \leq p^2$. Se $|G : \Phi(G)| = p$, então $G/\Phi(G)$ é cíclico e G é também cíclico de ordem p^2. Caso contrário, $|G : \Phi(G)| = p^2$ e, pelo Teorema da Base de Burnside, 1.49, $d(G) = 2$.

(iii) Seja N um subgrupo normal qualquer de G, e seja $|G : N| = p^i$, com $0 \leq i \leq m$. Daí, se $i = 0$ ou 1, então $N = \gamma_1(G)$ ou N é maximal em G. Para $i \geq 2$,

$\gamma_i(G) \leq N$, pelo corolário anterior. Como $|G : N| = p^i$, concluímos que $N = \gamma_i(G)$, pois, pela parte (i), $|G : \gamma_i(G)| = p^i$.

(iv) Isto é imediato de (ii) e (i), logo a classe de $\frac{G}{\gamma_i(G)}$ é $i-1$, para $2 \leq i \leq m$.

(v) Novamente, pelo teorema 1.50, $|G : Z_{m-2}(G)| \geq p^2$. Como $|Z_{i+1}(G) : Z_i(G)| \geq p$, para $0 \leq i \leq m-3$, e

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

então todas as desigualdades acima viram igualdades. Segue que, $|G : Z_i(G)| = p^{m-i}$, para $0 \leq i \leq m-1$, e, pela parte (iii), $Z_i(G) = \gamma_{m-i}(G)$.

□

1.3 p-Grupo Regular

Nesta seção, veremos um pouco de outra teoria sobre p-grupos finitos, que são os p-grupos Regulares. É uma teoria muito importante para o estudo da estrutura dos p-grupos. Os subgrupos dessa série serão definidos abaixo:

Definição 1.54. *Seja G um p-grupo finito, definimos $\Omega_i(G)$ como,*

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

para todo $i \geq 0$.

Definição 1.55. *Seja G um p-grupo finito, definimos $\mho_i(G)$ como,*

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

para todo $i \geq 0$.

Lemos o símbolo $\mho$ como "agemo". Note que a palavra agemo é formada pelas letras da palavra omega na ordem inversa

Podemos observar que $\Omega_i(G)$ e $\mho_i(G)$ são subgrupos característicos de G. Por outro lado, vimos em 1.49 que $G/\Phi(G)$ é um grupo abeliano elementar de G, consequentemente, $x^p \in \Phi(G)$, para todo $x \in G$. Portanto, $\mho_1(G) \leq \Phi(G)$. O próximo resultado deixa mais clara a relação entre $\Phi(G)$ e $\mho_1(G)$.

Teorema 1.56. *Seja G p-grupo finito. Então:*

(i) $\Phi(G)$ é o menor subgrupo de G tal que $G/\Phi(G)$ é abeliano elementar;

(ii) $\Phi(G) = G'\mho_1(G)$.

Demonstração.

(i) Já vimos em 1.49 que $G/\Phi(G)$ é abeliano elementar. Suponha que o quociente G/N é também abeliano elementar, logo G/N é um espaço vetorial sobre $\mathbb{F}_p$. Então a interseção dos subgrupos maximais é trivial, isto é, para todo vetor não-nulo v existe um subgrupo maximal não contendo v. Mas sabemos que um subgrupo maximal de G/N é da forma M/N, com M maximal em G, pois da interseção de subgrupos maximais de G contendo N é igual a N. Logo, $\Phi(G) \leq N$.

(ii) G/N é abeliano elementar se, e somente se, $[x, y] \in N$ para todo $x, y \in G$, isto é, se e somente se, $G'\mho_1(G) \leq N$. Segue de (i) que $\Phi(G) = G'\mho_1(G)$. □

Relembrando que o *expoente* de G, denotado por $exp(G)$ é o menor inteiro e tal que $x^e = 1$ para todo $x \in G$. No caso de um p-grupo, se $exp(G) = p^e$, então $x^{p^e} = 1$ para qualquer $x \in G$ e ainda podemos escrever $\Omega_e(G) = G$. Sendo assim, podemos construir a seguinte série ascendente, denominada Ω-série de G:

$$1 = \Omega_0(G) \leq \Omega_1(G) \leq \Omega_2(G) \leq \cdots \leq \Omega_e(G) = G.$$

De modo semelhante, $\mho_e(G) = 1$ e podemos construir a seguinte série descendente, denominada $\mho$-série de G:

$$G = \mho_0(G) \geq \mho_1(G) \geq \mho_2(G) \geq \cdots \geq \mho_e(G) = 1$$

Vamos agora indicar duas propriedades gerais dos subgrupos $\Omega_i(G)$ e $\mho_i(G)$.

Teorema 1.57. *Seja G um p-grupo finito:*

(i) Se $exp(G) = p^e$, então $\mho_i(G) \leq \Omega_{e-i}(G)$.

(ii) Para todo $N \trianglelefteq G$, $\mho_i(G/N) = \mho_i(G)N/N$.

Demonstração.

(i) Temos que qualquer gerador x^{p^i} de $\mho_i(G)$ possui ordem no máximo p^{e-i}, pois $exp(G) = p^e$. Logo segue que $\mho_i(G) \leq \Omega_{e-i}(G)$.

(ii) Usemos a notação $\overline{G} = G/N$. Então,

$$\mho_i(\overline{G}) = \langle \bar{x}^{p^i} | \bar{x} \in \overline{G} \rangle = \langle \overline{x^{p^i}} \in G \rangle = \overline{\mho_i(G)},$$

isto é, $\mho_i(G/N) = \mho_i N(G)/N$. □

1.3.1 Fórmula de Coleta de Phillip Hall

Sabemos que $x^n y^n = (xy)^n$ para qualquer grupo abeliano, mas, em geral, a igualdade não é válida. A fórmula de Phillip Hall, descrita a seguir, relaciona os termos

$x^n y^n$ e $(xy)^n$ em qualquer grupo, usando comutadores entre x e y. A construção da fórmula se dá indutivamente usando como base a relação $ab = ba[a, b]$.

Teorema 1.58 (Fórmula de coleta de Hall)**.** *Seja G um grupo e $x, y \in G$. Então existe elementos $c_i = c_i(x, y) \in \gamma_i(\langle x, y\rangle)$, tal que*

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

para todo $n \in \mathbb{N}$

A fórmula de compilação de Hall tem grande importância quando a usamos com expoente primo p, uma vez que os coeficientes binomiais são divisíveis por p. Consequentemente, podemos escrever

$$x^p y^p = (xy)^p z c_p$$

para algum elemento $z \in \mathfrak{V}_1(\langle x, y\rangle')$. O que nos sugere a seguinte definição.

Definição 1.59. *Seja G um p-grupo finito. Dizemos que G é um p-grupo regular se $x^p y^p \equiv (xy)^p (mod \mathfrak{V}_1(\langle x, y\rangle'))$ para todo $x, y \in G$. (Equivalentemente, se $c_p(x, y) \in \mathfrak{V}_1(\langle x, y\rangle')$ para todo $x, y \in G$.)*

A condição na definição de um p-grupo regular é local, uma vez que só envolve o subgrupo gerado por x e y. Por isso todos subgrupos e grupos quocientes de p-grupos regular são ainda regulares. São exemplos de p-grupos regular: p-grupos abelianos, grupos de expoente p e p-grupos com classe de nilpotência menor que p. O próximo resultado mostra alguns desses resultados, fornecendo algumas condições para que um grupo seja regular e caracterizando os 2-grupo regulares.

Teorema 1.60. *Seja G um p-grupo finito.*

(i) Se a classe de nilpotência de G é menor que p então G é regular. Em particular, todo p-grupo de ordem $\leq p^p$ é regular.

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

(iii) Um 2-grupo regular é abeliano.

Demonstração.

(i) Se G tem classe menor que p, então $\gamma_p(G) = 1$. Dessa forma, $\gamma_p(\langle x, y\rangle) = 1$, para todo $x, y \in G$, e então $c_p(x, y) = 1$ para todo $x, y \in G$, o que nos prova que G é regular.

(ii) Assumiremos que $\gamma_{p-1}(G)$ é cíclico. Se $p = 2$, então $G = \gamma_1(G)$ é cíclico, logo abeliano e portanto regular. Suponhamos então que $p > 2$. Seja $x, y \in G$ e defina $H = \langle x, y\rangle$. Dessa forma, $\gamma_{p-1}(H) \leq \gamma_{p-1}(G)$ é cíclico. Se $\gamma_{p-1}(H) = 1$, temos que $cl(H) < p$, logo, H é regular. Por 1.3.1, se $\gamma_{p-1}(H) \neq 1$, então $\gamma_p(H) \lneqq \gamma_{p-1}(H)$. $c_p \in \gamma_p(H) \leq \mathfrak{V}_1(\gamma_{p-1}(H))$ e H é regular.

(iii) Seja $H = \langle x, y\rangle$. Então,

$$x^2y^2 = xxyy = xyx[x,y]y = xyxyy^{-1}[x,y]y = (xy)^2y^{-1}[x,y]y.$$

Se G é regular, temos $[x,y]^y \in \mho_1(H')$ e isto implica que $[x,y] \in \mho_1(H')$. Desse modo, $\frac{H}{\mho_1(H')}$ é abeliano e $H' \leq \mho_1(H') \leq \Phi(H') < H'$. Mas , se $\Phi(H') = H'$ então $H' = 1$. Portanto, cada dois elementos de G comuta e G é abeliano. □

No final desta seção, vamos provar algumas propriedades básicas de p-grupos regulares, as quais são similares as de p-grupos abelianos.

Lema 1.61. *Seja G um p-grupo regular e sejam $x, y \in G$. Então $x^p = y^p$ se, e somente se, $(x^{-1}y)^p = 1$.*

Demonstração. Como G é regular, temos que para todo $x, y \in G$, $x^{-p}y^p = (x^{-1}y)^pz$, com $z \in \mho_1(\langle x, y\rangle')$. Dessa forma, é suficiente mostrar que se $x^p = y^p$ ou $(x^{-1}y)^p = 1$ temos $\mho_1(\langle x, y\rangle') = 1$.

Supondo $x^p = y^p$ então, y e x^p comutam e então $(x^p)^y = 1 = (x^y)^p$, portanto H é não-cíclico. Vamos mostrar por indução, seja $H = \langle x, y\rangle$, existe um subgrupo maximal M de H contendo x. Mas, como M é normal em H, então se $x \in M$, $x^y \in M$. Logo, $\langle x, x^y\rangle \leq M$ e como $|M| \leq |H|$, temos que $(x^{-1}x^y)^p = 1$ e $[x,y]^p = 1$, e H' é gerado por elementos de ordem p. Como $|H'| < |H|$, por indução, $exp(H') = p$ e portanto $\mho_1(\langle x, y\rangle') = 1$.

Supondo agora que $(x^{-1}y)^p = 1$, então $x(x^{-1}y)^px^{-1} = 1$, isto implica que, $(yx^{-1})^p = 1$. Usando a implicação que acabamos de ver temos que $(xx^{-1}yx^{-1})^p = 1$, logo, temos: $((yx^{-1})^{-1}x^{-1}y)^p = 1 = (xy^{-1}x^{-1}y)^p = [x^{-1}, y]^p$ e como $H' = \langle [x^{-1}, y]^h |\ h \in H\rangle$, concluímos que $\mho_1(H') = 1$. □

Teorema 1.62. *Seja G um p-grupo regular. Então:*

(i) Para todo $x, y \in G$ e para todo $i \geq 0$, temos que $x^{p^i} = y^{p^i}$ se, e somente se, $(x^{-1}y)^{p^i} = 1$.

(ii) Para todo $i \geq 0$, $\Omega_i(G) = \{x \in G | x^{p^i} = 1\}$.

(iii) Para todo $i \geq 0$, $\mho_i(G) = \{x^{p^i} | x \in G\}$.

(iv) Para todo $i \geq 0$, $|G : \Omega_i(G)| = |\mho_i(G)|$ (Consequentemente também, $|G : \mho_i(G)| = |\Omega_i(G)|$).

Demonstração. Primeiramente, notemos que, se vale a propriedade (i), para um i fixado, então o conjunto $\{x \in G | x^{p^i} = 1\}$ é um subgrupo e consequentemente coincide com $\Omega_i(G)$. Portanto a prova do (ii) está condicionada a validade do primeiro item.

Para provar o primeiro item, vamos fazer indução sobre i. Se $i = 0$ já vale o resultado e se $i = 1$, o resultado foi provado no lema. Assumindo o resultado válido para

$i-1$, nós também temos que o segundo item também é válido para $i-1$ e $\Omega_{i-1}(G)$ consiste dos elementos que tem ordem divisível por p^{i-1}. Portanto, de $x^{p^i} = y^{p^i}$ temos $(x^p)^{p^{i-1}} = (y^p)^{p^{i-1}}$ e, por indução, $(x^{-p}y^p)^{p^{i-1}} = 1$, então $x^{-p}y^p \in \Omega_{i-1}(G)$ e $x^p\Omega_{i-1}(G) = y^p\Omega_{i-1}(G)$. Usando $i = 1$ isso implica que $(x^{-1}y\Omega_{i-1}(G))^p = \Omega_{i-1}(G)$, isto é, $(x^{-1}y)^p \in \Omega_{i-1}(G)$. Concluímos que $(x^{-1}y)^{p^i} = 1$.

(iii) Novamente esta prova será feita por indução sobre i. Provaremos que dados $x, y \in G$ quaisquer, existe $z \in G$ tal que $x^p y^p = z^p$. Para $i = 1$ já temos válido o resultado. Façamos agora, indução sobre $|G|$. Sejam, $H = \langle x, y\rangle$ e $K = \langle xy, \Phi(H)\rangle$. Se $K = H$, então H é cíclico, logo, regular e vale o resultado. Então podemos assumir que $K < H$. Como G é regular, temos que $x^p y^p = (xy)^p c$ para algum $c \in \mho_1(H') \leq \mho_1(K)$. Então $(xy)^p c$ é um produto de dois elementos em $\mho_1(K)$ e aplicando a hipótese de indução em K, pode ser escrito da forma z^p. Portanto $x^p y^p = (xy)^p = z^p$.

Para i em geral, observe que

$$\mho_1(\mho_{i-1}(G)) = \{x^p |\ x \in \mho_{i-1}(G)\} = \{x^{p^i} |\ x \in G\}$$

é um subgrupo de G. Então $\mho_i(G) = \{x^{p^i} |\ x \in G\}$.

(iv) Segue por (i) e (ii) que $x^{p^i} = y^{p^i}$ se, e somente se, $x^{-1}y \in \Omega_i(G)$, ou seja, $x\Omega_i(G) = y\Omega_i(G)$. Portanto, a aplicação $x\Omega_i(G) \in \frac{G}{\Omega_i(G)} \mapsto x^{p^i} \in \mho_i(G)$ está bem definida e é injetiva. Mas pela parte (iii) temos também que a aplicação é sobrejetiva, portanto bijetiva. Logo temos que $|G : \Omega_i(G)| = |\mho_i(G)|$. □

Proposição 1.63. *Se G é um p-grupo regular e $G = N \rtimes H$, então $\Omega_i(G) = \Omega_i(N)\Omega_i(H)$ e, $\mho_i(G) = \mho_i(N)\mho_i(H)$.*

Demonstração. Sabemos que $\Omega_i(N) \leq \Omega_i(G)$ e $\Omega_i(H) \leq \Omega_i(G)$, logo $\Omega_i(N)\Omega_i(H) \leq \Omega_i(G)$. Por outro lado,

$|\Omega_i(G)| = |G : \mho_i(G)| = \frac{|G|}{|\mho_i(G)|} = \frac{|N||H|}{|\mho_i(G)|} \leq \frac{|N||H|}{|\mho_i(N)\mho_i(H)|} = |\Omega_i(N)\Omega_i(H)|$. Logo, temos a igualdade desejada. De modo semelhante, temos que $\mho_i(G) = \mho_i(N)\mho_i(H)$. □

Capítulo 2

Caracterização dos Grupos com p Classes de Conjugação de Subgrupos Não-Normais

Neste capítulo, vamos provar os resultados principais contidos nos artigos [FALe10] e [Br95]; os mesmo foram utilizados aqui como referência de técnicas utilizadas na demonstração de tais resultados. Primeiramente, vamos ver alguns exemplos que nos ajudarão a entender o problema.

Denotaremos por $\nu(G)$ o número de classes de conjugação de subgrupos não-normais.

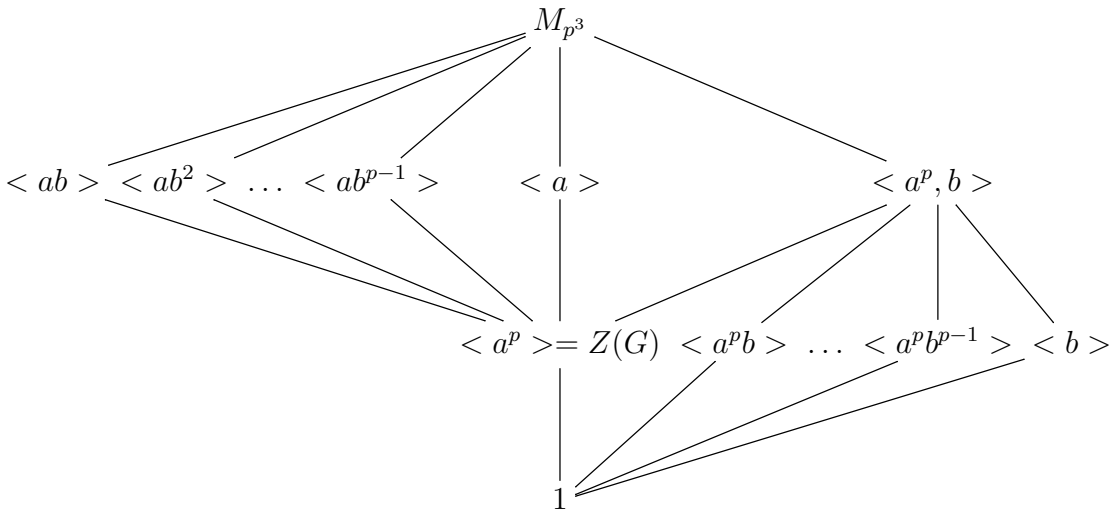
Os grupos em que todos os subgrupos são normais, sao chamados grupos de Dedekind. Esses grupos já foram estudados e o seguinte resultado, que se pode encontrar em [**?**], caracteriza tais grupos:

Teorema 2.1 (Dedekind, Baer)**.** *Todos os subgrupos de um grupo G são normais se e somente se G é abeliano ou o produto direto de um grupo quatérnio de ordem 8, um 2-grupo abeliano elementar e um grupo abeliano com todos elementos de ordem ímpar.*

Dessa forma, um grupo tem $\nu(G) = 0$ se e somente se G é grupo de Dedekind. O estudo começa por considerar os grupos G com $\nu(G) = 1$.

Exemplo 2.2. *Seja $M_{p^3} = \langle a, b \mid a^{p^2} = b^p = 1, a^b = a^{1+p} \rangle$, p primo ímpar. Temos que $|M(p^3)| = p^3$. Vamos mostrar que $\nu(M_{p^3}) = 1$.*

Demonstração. Se pode mostrar que os subgrupos $\langle b \rangle$, $\langle a^p \rangle = Z(G) = G'$ e $\langle a^p b^i \rangle$, para todo $i = 1, ..., p-1$, tem ordem p. Sendo M'_{p^3} cíclico, Pelo item(ii) de 1.60, temos que M_{p^3} é regular, e $(ab^i)^p = a^p b^{ip} z$, com $z \in \mho_1(M'_{p^3})$. Logo, $(ab^i)^p = a^p b^{ip} = a^p$ e então $(ab^i)^p = a^p$ e os subgrupos $\langle ab^i \rangle$, para todo $i = 0, ..., p-1$, têm ordem p^2. Também o subgrupo $\langle a^p, b \rangle$ tem ordem p^2. Então o reticulado dos subgrupos de $M(p^3)$ é o seguinte:



É claro que, se H é um subgrupo não normal de G ele tem ordem p, visto que os subgrupos de ordem p^2 são maximais, logo normais, conforme vimos na seção 1.2. Como $b^a = a^{-1}ba = bb^{-1}a^{-1}ba = b(b^{-1}ab)^{-1}a = ba^{-(p+1)}a = ba^{-p} \notin \langle b \rangle$, então $\langle b \rangle$ é não normal em G.

Como $|[\langle b \rangle]_{C_G}| = |G : N_G(\langle b \rangle)| = p$, portanto, a classe de conjugação de $\langle b \rangle$ contém p elementos: todos os subgrupos de ordem p que não estão contidos no centro. Logo, $\nu(G) = 1$. □

Brandl, em 1995, [Br95], classificou os p-grupos finitos com $\nu(G) = 1$, e mostrou que um tal grupo é uma generalização do exemplo 2.2(anterior). Através do seguinte resultado:

Teorema 2.3. *Seja G um p-grupo finito. Temos que $\nu(G) = 1$ se, e somente se, G é isomorfo a*

$$M_{p^r} = \langle a, b \mid a^{p^{r-1}} = b^p = 1, a^b = a^{1+p^{r-2}} \rangle,$$

onde $r \geq 3$ se $p > 2$, e $r \geq 4$ se $p = 2$.

Lema 2.4. *Seja G un p-grupo finito:*

Se N é um subgrupo normal de um grupo G, então $\nu(G/N) \leq \nu(G)$. Se $p \neq 2$ e $\nu(G/N) = \nu(G)$, então $N = 1$

Então surge a pergunta: é possível dar uma descrição dos grupos com $\nu(G) > 1$?

Na verdade $\nu(G)$ não pode ser um número qualquer, como La Haye e Rhemtula mostraram em **[?]** no seguinte resultado:

Lema 2.5. *Seja G um p-grupo finito com $\nu(G) > 0$. Então temos que $\nu(G) = 1$ ou $\nu(G) \geq p$.*

Então seria interessante descrever todos os grupos com $\nu(G) = p$. O exemplo abaixo é de um grupo que tem p classes de conjugação de subgrupos não-normais:

Exemplo 2.6. *Seja p um primo ímpar. Se consideramos o grupo:*

$$G = L_{p^4} := \langle a, b | a^{p^2} = b^{p^2} = 1, a^b = a^{1+p} \rangle,$$

então $\nu(G) = p$.

Demonstração. Como $L'_{p^4} = \langle a^p \rangle$, temos que L_{p^4} é regular. Sendo $\mho_1(L'_{p^4}) = \{1\}$ temos $(a^i b^j)^p = a^{ip} b^{jp}$. Além disso, $\langle a \rangle \trianglelefteq L_{p^4}$, então $\langle a \rangle \cap Z(G) \neq \{1\}$. Isso implica que $\langle a^p \rangle \leq Z(L_{p^4})$ e $L'_{p^4} \leq Z(L_{p^4})$, ou seja, L_{p^4} tem classe de nilpotência 2. Segue que $[a, b^p] = [a, b]^p = 1$ e $b^p \in Z(L_{p^4})$. De $|L_{p^4} : \langle a^p, b^p \rangle| = p^2$ e $\langle a^p, b^p \rangle \leq Z(G)$, segue que $Z(G) = \langle a^p, b^p \rangle = \Omega_1(G)$.

Seja $H \leq G$. Se $|H| = p$, então $H = \langle a^i b^j \rangle$ e $(a^i b^j)^p = a^{ip} b^{jp} = 1$, ou seja, $p|i$ e $p|j$ e $a^i b^j \in Z(G)$, então $H \trianglelefteq G$. Se $|H| = p^2$ e H cíclico, então $H = \langle a^i b^j \rangle$ com $(a^i b^j)^{p^2} = 1$, então $p \nmid i$ ou $p \nmid j$. Por indução temos $(a^i b^j)^n = a^{in + \frac{n(n-1)}{2} ijp} b^{jn}$ para $n \geq 1$.

Sejam i, j, com $1 \leq i \leq p^2 - 1$ e $1 \leq j \leq p^2 - 1$. Como existe $\bar{n}$ tal que $\bar{n} j \equiv 1 (mod p^2)$, temos que $(a^i b^j)^{\bar{n}} = a^{in + \frac{\bar{n}(\bar{n}-1)}{2} ijp} b^{j\bar{n}} = a^{i\bar{n}} b$. Podemos supor que $H = \langle a^i b \rangle$, $0 \leq i \leq p^2 - 1$ ou $H = \langle a \rangle$. Claramente $\langle a \rangle$ é normal em G.

Seja $H = \langle a^i, b \rangle$, $0 \leq i \leq p^2 - 1$, observe que eles são todos distintos. Como:

$$(a^i b)^b = (a^i)^b = (a^b)^i b = a^{(1+p)i} b,$$

$$(a^i b)^{b^2} = (a^{(1+p)i})^b b = (a^{1+p})^{(1+p)i} b = a^{(1+2p)i}$$

$$[\langle a^i b \rangle] = \{\langle a^i b \rangle, \langle a^{(1+p)i} b \rangle, \cdots, \langle a^{(1+(p+1)p)i} b \rangle\}.$$

Temos que $\langle a^i b \rangle$ e $\langle a^j b \rangle$ não são conjugados se $i \neq j$ e $0 \leq i, j \leq p-1$, portanto $\nu(G) \geq p$.

Se H não é cíclico, $|H| = p^2$, então H tem expoente p e $H \leq \Omega_1(L_{p^4}) \leq Z(G)$ é um subgrupo normal . Claramente, se $|H| = p^3$, então H é normal em G e $\nu(G) = p$. □

Veremos agora um exemplo de um grupo G em que $\nu(G) = p + 1$.

Exemplo 2.7. *Seja p um primo, $p > 2$. Seja $G = E_{p^3} = \langle x, y \mid x^p = y^p = 1, [x, y]^x = [x, y] = [x, y]^y \rangle$ o subgrupo não abeliano de ordem p^3 e expoente p. Então $\nu(G) = p + 1$.*

Demonstração. Como um subgrupo de ordem p^2 é maximal, ele é normal, então temos que um subgrupo não normal de G tem ordem p. Sabemos que todo elemento de G tem ordem p, os subgrupos de ordem p serão $\dfrac{p^2 - 1}{p - 1} = p^2 + p + 1$ subgrupos de ordem p; entre eles existe um único subgrupo normal que é o centro. Se um subgrupo de ordem p for normal ele tem que estar contido no centro, então o centro é o único subgrupo normal de ordem p. Portanto G tem exatamente $p^2 + p$ subgrupos não normais. Além disso, se

H é um subgrupo não normal de G, a única possibilidade para o índice do normalizador de H em G é ser igual a p. Visto que $|[K]| = |G : N_G(K)| = p$, ou seja, que cada classe de conjugação tem p elementos, concluímos que o número de classes de conjugação de subgrupos não normais de G é $\frac{p^2+p}{p} = p + 1$. Então $\nu(G) = p + 1$. □

Em 2010, Legarreta e Fernández-Alcober caracterizaram os grupos com p classes de conjugação de subgrupos não normais, com p primo ímpar, provando o seguinte resultado:

Teorema 2.8 (Lagarreta, Fernandéz-Alcober)**.** *Seja G um p-grupo finito com ordem p^n, com $p > 2$. Então $\nu(G) = p$ se, e somente se, G tem a seguinte descrição, para $n \geq 4$:*

$$L_{p^n} = \langle a, b \mid a^{p^{n-2}} = b^{p^2} = 1, a^b = a^{1+p^{n-3}} \rangle.$$

Nessa prova precisaremos de duas propriedades sobre $\nu(G)$, as quais foram obtidas em [FALe08] e [FALe09], respectivamente, onde também estão devidamente provadas:

$(P1)$ Seja G um p-grupo finito não abeliano, com p primo ímpar. Se $|G'| = p^k$, então $\nu(G) \geq p(k-1) + 1$.

$(P2)$ Seja G um grupo de ordem p^n, com p primo ímpar. Definimos $\lambda(G) = n - s$, onde $exp(Z(G)) = p^s$. Se $|G'| = p$, então $\nu(G) \geq p^{\lambda(G)-2}$.

Um grupo diz-se minimal-não-abeliano se G não é abeliano e todo subgrupo de G é abeliano. Também vamos precisar da classificação de p-grupos finitos minimais-não-abeliano, encontrado em Miller e Moreno, [MM03], que diz que, para $p > 2$, existem duas possibilidades: (i) G é metacíclico, e

$$G = \langle a, b |\ a^{p^m} = b^{p^l} = 1, a^b = a^{1+p^{m-1}} \rangle,$$

para $m \geq 2$. (ii) G não é metacíclico, e

$$G = \langle a, b, c |\ a^{p^m} = b^{p^l} = c^p = 1, [a, b] = c, [a, c] = [b, c] = 1 \rangle.$$

Nesse último caso, notemos que o quociente $\frac{G}{\langle a^{p^{m-1}}, b^{p^{l-1}} \rangle}$ é isomorfo a E_{p^3}. Sabendo que $\nu(E_{p^3}) = p + 1$, segue que $\nu(G) \geq p + 1$.

Também para esta prova são necessários os seguintes resultados:

Teorema 2.9. *Seja V um espaço vetorial de dimensão n e seja f uma forma bilinear antisimétrica. Então existe uma base ordenada da forma $\{u_1, v_1, \cdots, u_k, v_k, w_1, \cdots, w_{n-2k}\}$, com $0 \leq 2k \leq n$ e $f(u_i, v_i) = 1 = -f(v_i, u_i)$ para todo $i = 1, \cdots, k$ e $f(a, b) = 0$ nos outros casos.*

A prova do resultado, pode ser vista em [Ro06].

Teorema 2.10. *Sejam G um p-grupo finito e $\frac{G}{Z(G)}$ p-grupo abeliano elementar e cíclico. Então, temos que, $\left|\frac{G}{Z(G)}\right| = p^{2k}$ com $k \in \mathbb{N}$.*

Demonstração. $G/Z(G)$ pode ser visto como espaço vetorial sobre $\mathbb{Z}_p$. Seja c um gerador de G'. Como $[x,y] \in G'$, então existe $f(x,u)$ tal que $[x,y] = c^{f(x,y)}$ e $f(x,y) \in \mathbb{Z}_p$. Então está bem definida a função

$$f : (xZ, yZ) \in \frac{G}{Z(G)} \times \frac{G}{Z(G)} \mapsto f(x,y) \in \mathbb{Z}_p.$$

f é uma forma bilinear antisimétrica e existe uma base $B = \{u_1Z, v_1Z, \cdots, w_1Z, \cdots, w_{n-2k}Z\}$. Se $n \neq 2k$, então existe w_1Z tal que $f(w_1, a) = 0$ para todo $aZ \in G/Z(G)$, isto implica $[w_1, a] = 1$ e $w_1 \in Z(G)$, mas isso é um absurdo. Então, $n = 2k$, como desejado.

□

Por fim, podemos provar o resultado.

Demonstração. ($\Leftarrow$) Seja $G = L_{p^n}$, vamos mostrar que $\nu(G) = p$. Sabemos que $\Omega_1(G) = \langle a^{p^{n-3}}, b^p \rangle$, vamos mostrar que $\Omega_1(G)$ é central. Para isso é suficiente que $a^{p^{n-3}}$ comute com b e b^p comute com a.De fato,

$$\begin{aligned} (a^{p^{n-3}})^b &= (a^b)^{p^{n-3}} \\ &= (a^{1+p^{n-3}})^{p^{n-3}} \\ &= a^{p^{n-3}+p^{2(n-3)}} \end{aligned}$$

Mas, se $n \geq 4$ temos que $2(n-3) \geq n-2$. Logo, para todo $n \geq 4$, temos que, $(a^{p^{n-3}})^b = a^{p^{n-3}}$ e $a^{p^{n-3}} \in Z(G)$. De modo análogo, temos que $b^a = a^{-1}ba = bb^{-1}a^{-1}ba = ba^{-1-p^{n-3}}a = ba^{-p^{n-3}}$. Logo, $(b^p)^a = (b^a)^p = (ba^{-p^{n-3}})^p$, agora sendo o grupo regular e $\mho_1(L'_{p^n}) = \{1\}$, temos $(ba^{-p^{n-2}})^p = b^p a^{-p^{(n-2)}} = b^p$ e $b^p \in Z(G)$.

Como $|\Omega_1(G)| = p^2$, com cada elemento de ordem p, $\Omega_1(G)$ é p-grupo abeliano elementar e, portanto, possui $p+1$ subgrupos, que chamaremos de $Z_i = \langle a^{p^{n-3}} b^{-ip} \rangle$, com $i = 1, \cdots, p-1$, $Z_p = \langle b^p \rangle$ e $Z_{p+1} = \langle a^{p^{n-3}} \rangle$.

Como, $[a,b] = a^{-1}a^b = a^{-1}a^{1+p^{n-3}} = a^{p^{n-3}}$. Podemos observar que $G' = \langle [a,b] \rangle^G = \langle a^{p^{n-3}} \rangle$ já que $\langle a^{p^{n-3}} \rangle$ é normal.

Afirmação 1: Todo subgrupo não normal de G contém pelo menos um dos subgrupos $Z_i, i = 1, \cdots, p+1$.

De fato, suponha $H \ntrianglelefteq G$, com $|H| = p^k$, $k < n$.

Como $p | p^k$, pelo Lema de Cauchy, existe $h \in H$ tal que $|h| = p$. Logo $h \in \Omega_1(G)$, dessa forma $H \cap \Omega_1(G) \neq 1$ e temos que $Z_i \leq H$.

Afirmação 2. Se H contém dois Z_i, $i = 1, \cdots, p+1$.. Então esse subgrupo contém $\Omega_1(G)$.

Vimos que se $H \ntrianglelefteq G$, então $Z_i \leq H$. Suponhamos que $Z_j \leq H$, $i \neq j$,

Como $\Omega_1(G)$ é um p-grupo abeliano elementar de ordem p^2, é gerado por dois elementos. Dessa forma, tomando $h_i \in Z_i$ e $h_j \in Z_j$, temos que $\Omega_1(G) = \langle h_i, h_j \rangle$, logo

$\Omega_1(G) \leq H$.

Dessa forma, temos que: Se $H \not\trianglelefteq G$ e $Z_i \leq H$, então $\frac{H}{Z_i} \not\trianglelefteq \frac{G}{Z_i}$, se $H \not\trianglelefteq G$ e $\Omega_1(G) \leq H$, temos que $\frac{H}{\Omega_1(G)} \not\trianglelefteq \frac{G}{\Omega_1(G)}$. Logo,

$$\nu(G) = \sum_{i=1}^{p+1} \nu\left(\frac{G}{Z_i}\right) - p\nu\left(\frac{G}{\Omega_1(G)}\right) = \sum_{i=1}^{p} \left(\frac{a}{Z_i}\right),$$

pois, para $i = p+1$, $\frac{G}{G'}$ é abeliano e $\nu\left(\frac{G}{G'}\right) = 0$; sendo $G' \leq \Omega_1(G)$, $\nu\left(\frac{G}{\Omega_1(G)}\right) = 0$. Também:

Vamos analisar o quociente $\frac{G}{Z_i}$, com $i = 1, \cdots, p$. Para $i = p$, temos que

$$\frac{L_{p^n}}{\langle b^p \rangle} = \langle \bar{a}, \bar{b} | \bar{a}^{p^{n-2}} = \bar{b}^p = 1, \bar{a}^{\bar{b}} = \bar{a}^{1+p^{n-3}} \rangle \cong M_{p^{n-1}}$$

e $\nu(M_{p^{n-1}}) = 1$.

para $i = 1, \cdots, p-1.$, Consideremos $L_{p^n} = \langle a, a^{p^{n-4}i}b \rangle$ e então,

$$\frac{L_{p^n}}{Z_i} = \langle aZ_i, a^{p^{n-4}i}bZ_i | \ |aZ_i| = p^{n-2}; |a^{p^{n-4}i}bZ_i| = p \rangle$$

e como L_{p^4} é regular:

$$(a^{p^{n-4}i}b)^p = a^{p^{n-3}i}b^p.$$

Dessa forma,

$$\frac{L_{p^n}}{Z_i} = \langle aZ_i, a^{p^{n-4}i}bZ_i | \ a^{p^{n-2}}Z_i = (a^{p^{n-4}i}b)^p Z_i = Z_i; \ (aZ_i)^{(a^{p^{n-4}i}b)Z_i} = a^{1+p^{n-3}}Z_i \rangle,$$

já que $(aZ_i)^{(a^{p^{n-4}i}b)Z_i} = (a^b)Z_i = a^{1+p^{n-3}}Z_i$. Portanto, temos que $\frac{L_{p^n}}{Z_i} \cong M_{p^{n-1}}$, Como $\nu(M_{p^{n-1}}) = 1$, concluímos que $\nu(L_{p^n}) = p$.

$\Rightarrow$ Seja G um grupo tal que $\nu(G) = p$. Pela propriedade (1), temos que: Tomando $|G'| = p^k$,

$$\begin{aligned} p = \nu(G) \geq p(k-1)+1 \ &\Rightarrow \ p \geq pk - p + 1 \\ &\Rightarrow \ 2p \geq pk + 1 \\ &\Rightarrow \ 2p - pk \geq 1 \\ &\Rightarrow \ p(2-k) \geq 1. \end{aligned}$$

Temos que $2 - k \geq 1/p$ e então $k \leq 2 - 1/p$ e $1 \leq k \lneq 2$. O que implica que $k = 1$ e portanto $|G'| = p$. Como consequência, temos que G é um grupo nilpotente de classe 2 e regular. Desta forma, Sabendo que $[x, y] \in G' \leq Z(G)$ para $x, y \in G$, temos,

$1 = [x, y]^p = [x^p, y]$, e então $x^p \in Z(G)$. Logo $xZ(G)$ tem ordem p, e $exp\left(\frac{G}{Z(G)}\right) =$

$exp(\Omega_1(G)) = p$ e $|\frac{G}{Z(G)}| = p^2$, logo, por 2.10, temos que $\left|\frac{G}{Z(G)}\right| = p^{2k}$. Por (P2) temos que $|G| = p^n$, $exp(Z(G)) = p^s$ e $\lambda(G) = n - s$. Se $|G'| = p$, então $\nu(G) \geq p^{\lambda(G)-2}$, segue que $p \geq p^{\lambda(G)-2}$ e isto implica $\lambda(G) - 2 \leq 1$, logo $\lambda(G) \leq 3$. Seja $|Z(G)| = p^r$, temos que $s \leq r$, daí $n - s \geq n - r$ e $n - r \leq 3$. Como $|G : Z(G)| = p^{n-r}$ temos que $|G : Z(G)| \leq p^3$, logo $|G : Z(G)| = p^2$. Portanto $\frac{G}{Z(G)} \cong C_p \times C_p$.

Vamos supor que $Z(G)$ é cíclico. Sabemos que, $|\Omega_1(G) : \Omega_1 \cap Z(G)| \leq |G : Z(G)| = p^2$. E então, $|\Omega_1(G)| = |\Omega_1(G) : \Omega_1 \cap Z(G)|.|\Omega_1 \cap Z(G)| \leq p^3$, já que sendo o centro cíclico, ele possui um único subgrupo de ordem p. Portanto $|\Omega_1(G)| \leq p^3$. Se vale a igualdade, então $\left|\frac{\Omega_1(G)}{\Omega_1(G)\cap Z(G)}\right| = \left|\frac{G}{Z(G)}\right|$ e portanto $G = \Omega_1(G)Z(G)$. Consequentemente, $\Omega_1(G)$ é não abeliano, visto que G é não abeliano.

Vamos mostrar que dois subgrupos de $\Omega_1(G)$ são conjugados em G se, e somente se, eles são conjugados em $\Omega_1(G)$. De fato, sejam $H_1, H_2 \leq \Omega_1(G)$ conjugados, então existe $g \in G$ tal que $H_1 = H_2^g$. E temos que g é da forma cz, com $c \in \Omega_1(G)$ e $z \in Z(G)$. Assim, $H_1 = (H_2^{zc}) = (H_2^z)^c = (H_2)^c$. Portanto H_1 e H_2 são conjugados em $\Omega_1(G)$. Portanto, temos que $|\Omega_1(G)| = p^3$, $exp(\Omega_1(G)) = p$ e é não abeliano. Logo $\Omega_1(G) = E_{p^3}$.

Segue que $\nu(G) \geq \nu(\Omega_1(G)) = p+1$, o que é absurdo, pois $\nu(G) = p$ por hipótese. Portanto, $|\Omega_1(G) : \Omega_1(G) \cap Z(G)| \neq p^2$ e temos duas opções para este índice, ou seja:

$|\Omega_1(G) : \Omega_1(G) \cap Z(G)| = p$ ou $|\Omega_1(G) : \Omega_1(G) \cap Z(G)| = 1$.

Se $|\Omega_1(G) : \Omega_1(G) \cap Z(G)| = 1$ então, $|\Omega_1(G)| = |\Omega_1(G) \cap Z(G)| = p$. Isso implica G tem um único subgrupo de ordem p e, como $p \neq 2$, temos por 1.29 que G é cíclico e portanto abeliano. Absurdo!

Supondo agora que $|\Omega_1(G) : \Omega_1(G) \cap Z(G)| = p$, dessa forma $|\Omega_1(G)| = p^2$ e $\Omega_1(G)$ é um p-grupo abeliano elementar. Logo, como $\Omega_1(G) \cap Z(G) \subseteq \Omega_1(G)$, então existe um complemento T tal que, $\Omega_1(G) = T \times (\Omega_1(G) \cap Z(G))$. De modo análogo, como sabemos que $\frac{G}{Z(G)}$ é p-grupo abeliano elementar e $\left|\frac{\Omega_1(G)Z(G)}{Z(G)}\right| = p$. Então existe um complemento $\frac{M}{Z(G)} \leq \frac{G}{Z(G)}$ que não está contido em $\frac{\Omega_1(G)Z(G)}{Z(G)}$, tal que, $\frac{G}{Z(G)} = \frac{M}{Z(G)} \times \frac{\Omega_1(G)Z(G)}{Z(G)}$.

Logo, $G = M(\Omega_1(G)Z(G))$ e como $Z(G) \leq M$, temos que $G = M\Omega_1(G) = M(T \times (\Omega_1(G) \cap Z(G))) = MT$, pois $\Omega_1(G) \cap Z(G) \leq M$. E sabemos que $T \leq \Omega_1(G)$ e $\Omega_1(G) \cap M \leq Z(G)$, logo $T \cap M \leq Z(G)$ e, então, $T \cap M \leq T \cap Z(G) = 1$. Portanto, $G = M \rtimes T$.

Afirmação 3: $\Omega_1(M) = \Omega_1(G) \cap M$ tem ordem p.

De fato, como $\Omega_1(G) = \Omega_1(T)\Omega_1(M)$ e $|\Omega_1(G)| = p^2$, se $|\Omega_1(M)| = p^2$, então $|\Omega_1(T)| = 1$, o que é um absurdo. Por outro lado, também temos que $|\Omega_1(M)| \neq 1$. Logo, $|\Omega_1(M)| = p$.

Afirmação 4: Como $|G'| = p$, então $G \cong M_{p^n}$.

Sabemos que M é cíclico, então existe $m \in M$ tal que $M = \langle m \rangle$ e $|M| = p^n, n \in \mathbb{N}$. Sabemos também que $|T| = p$, logo, existe $t \in T$ para o qual $T = \langle t \rangle$. Então temos que

$G = \langle m, t \rangle$, com a seguinte apresentação:

$$G = \langle m, t | m^{p^n} = t^p = 1; m^t \in \langle m \rangle \rangle.$$

Precisamos saber como t age em m.

Sabemos que $M \trianglelefteq G$, logo $m^t = m^r$, com $r \in \mathbb{N}$ e $[m, t] = m^{-1+r}$. Como $|G'| = p$, $|m^{r-1}| = p$ e então $m^{r-1} \in \langle m^{p^{n-1}} \rangle$. Logo $[m, t] = (m^{p^{n-1}})^l$, com $p \nmid l$. Como $l \in \mathbb{Z}_p$, e existe $x \in \mathbb{Z}_p$ tal que $lx \equiv 1 \ mod p$. Portanto $[m, t^x] = [m, t]^x = (m^{p^{n-1}})^{lx} = m^{p^{n-1}}$ e concluímos então que,

$$G = \langle m, t^x | m^{p^n} = (t^p)^x = 1; (m^t)^x = m^{1+p^{n-1}} \rangle \cong M_{p^{n-1}}.$$

Absurdo, pois, por hipótese, $\nu(G) = p$.

Assumiremos agora que $Z(G)$ é não cíclico. Desta forma, como $|G'| = p$, podemos encontrar um subgrupo central $Z = \langle z \rangle$ de ordem p, tal que $\langle z \rangle \cap G' = 1$. Então, em 2.4, $\nu(G) > \nu(G/Z) \geq 1$, pois G/Z é não abeliano. Mas como sabemos que $\nu(G) = p$, necessariamente $\nu(G/Z) = 1$ e portanto $G/Z \cong M_{p^{n-1}}$ e G/Z é 2-gerado. Pondo $G/Z = \langle aZ, bZ \rangle$ temos que $G = \langle a, b \rangle Z$. Se escrevermos $H = \langle a, b \rangle$, então $G = HZ$. Se $H \cap Z = 1$, então $G = H \times Z$, o que implica, $H \cong G/Z$, logo $H \cong M_{p^{n-1}}$ e, como $Z = \mathbb{Z}_p$, $G = M_{p^{n-1}} \times \mathbb{Z}_p$. Então $\mathbb{Z}_p = \langle z \rangle$ e $M_{p^{n-1}} = \langle a, b \rangle$ com $\langle b \rangle \ntrianglelefteq M_{p^{n-1}}$, então temos que $\langle z^i b \rangle \ntrianglelefteq G$ para todo $i = \{0, \cdots, p-1\}$ e $\langle b, z \rangle \ntrianglelefteq G$ e temos que $\nu(G) \geq p + 1$, o que é impossível, pois por hipótese, temos que $\nu(G) = p$.

Se $H \cap Z \neq 1$, então $Z \leq H$ e $G = HZ = H$. Como $H = \langle a, b \rangle$ temos que $\left|\frac{G}{\phi(G)}\right| = p^2$ e como $\left|\frac{G}{Z(G)}\right| = p^2$ e $exp(\frac{G}{Z(G)}) = p$ e $\phi(G) \leq Z(G)$, isso implica que $\phi(G) = Z(G)$.

Seja M um subgrupo maximal de G, então $\phi(G) \leq M$ e $|M/\phi(G)| = p$. Logo $M/Z(G)$ é cíclico e portanto M é abeliano. Como M é arbitrário, temos que G é um grupo minimal não abeliano.

Se G não é metacíclico, por 2, $\nu(G) \geq p + 1$, absurdo. Então G é metacíclico e, por 2, temos que G tem a seguinte apresentação:

$$G = \langle a, b | a^{p^m} = b^{p^l} = 1; a^b = a^{1+p^{m-1}} \rangle.$$

Se $l = 1$, então $G \cong M_{p^m}$ e $\nu(G) = 1$, absurdo. Logo $l \geq 2$.

Seja $C = \langle b^{p^2} \rangle$, sabendo que $\exp(G/Z(G)) = p$, então $b^p \in Z(G)$ e logo $b^{p^n} \in Z(G)$ e C é central em G, portanto $C \trianglelefteq G$. Dessa forma,

$$G/C = \langle \bar{a}, \bar{b} | \bar{a}^{p^m} = \bar{b}^{p^2} = 1; a^b = a^{1+p^{m-1}} \rangle \cong L_{p^n}$$

e temos que $\nu(G/C) = p$.

Daí, sendo $\nu(G/C) = \nu(G) = p$, temos que $C = 1$.
Note que, $b^p \in Z$ e Z é cíclico de ordem p, então $b^{p^2} = 1$. Portanto,

$$G = \langle a, b | a^{p^m} = b^{p^2} = 1; a^b = a^{1+p^{m-1}} \rangle \cong L_{p^n},$$

como desejávamos.

□

O resultado acima mostra que os grupos com $\nu(G) = p$ são uma generalização do exemplo 2.6.

Capítulo 3

Caracterização de Grupos com $p+1$ Classes de Conjugação de Subgrupos Não-Normais

Neste capítulo, vamos provar o resultado principal contido no artigo [Br13], e que foi utilizado como referência das técnicas utilizadas na sua demonstração. Primeiramente, veremos alguns resultados importantes para o entendimento.

Definição 3.1 (Produto Central)**.** *Sejam H e K grupos, $M \leq Z(H)$ e θ um monomorfismo $\theta : M \to Z(K)$. Seja L o produto direto de H e K, isto é, $L = H \times K$. Definimos o conjunto $D = \{(m^{-1}, \theta(m)) |\ m \in M\}$, pode-se observar que D é subgrupo normal de L isomorfo a M. Definimos G o produto central de H e K amalgamado sobre M como o grupo quociente, $G := \frac{L}{D} = \frac{H \times K}{D}$. E escrevemos como*

$$G = H * K.$$

Temos que:
- $\frac{HD}{D} \simeq H$ e $\frac{KD}{D} \simeq K$ são subgrupos normais de G
- $\frac{HD}{D} \cap \frac{KD}{D} = \frac{MD}{D} = \frac{\theta(M)D}{D} \simeq M$
- $G = \langle \frac{HD}{D}, \frac{KD}{D} \rangle$

então, de fato G é produto central interno de $\frac{HD}{D}$ e $\frac{KD}{D}$:

$$G = \frac{HD}{D} * \frac{KD}{D}.$$

Em 2013, Brandl [Br13], mostrou que um p-grupo finito, p primo ímpar, com $\nu(G) = p + 1$ se pode construir a partir do exemplo 2.7, usando o produto central:

Teorema 3.2. *Sejam p um primo ímpar e $n \geq 3$. Seja H um grupo não abeliano de ordem p^3 e expoente p, $H \cong E_{p^3}$. Sejam $K \cong \mathbb{Z}_{p^{n-2}}$, o grupo cíclico de ordem p^{n-2} e $\Omega_1(K)$ o único subgrupo de K de ordem p. Seja $G = D_{p^n} := H * K$ onde $Z(H)$ e $\Omega_1(K)$ são amalgamados. Então $\nu(G) = p + 1$.*

Demonstração. Observemos que, como $H \cong E_{p^3}$, H é p-grupo de classe maximal, $Z(H) = H'$ de ordem p, pois sabemos que E_{p^3} é um p grupo extra-especial, como vimos no primeiro capítulo.

Como $|Z(H)| = p$ temos que $Z(H) \cong \mathbb{Z}_p$ e, por definição, $\Omega_1(K) \cong \mathbb{Z}_p$. Dessa forma, existe um isomorfismo

$$\theta : Z(H) \to \langle \Omega_1(K) \rangle$$

e $D = \{(z^{-1}, \theta(z)) |\ z \in \mathbb{Z}_p\}$. Portanto,

$$G = D_{p^r} \cong \frac{H \times K}{D} \cong \frac{E_{p^3} \times \mathbb{Z}_{p^{n-2}}}{D'}.$$

Obs.: Note que, quando dizemos que dois subgrupos são amalgamados, temos que no quociente os grupos são identificados através ds isomorfirmos θ.

Como $\Omega_1(K) \leq Z(G)$, temos que $G' = E'_{p^3}$. Isto implica que, $|G'| = p$ e portanto $cl(G) = 2$.

Seja S subgrupo de G não normal. Se $S' \neq 1$, então temos que $S' = G'$, já que $S' \leq G'$. Dessa forma, se $|G'| = p$ então $G' \leq Z(G)$ e $G' = S' \leq S$, logo $S \trianglelefteq G$, contradição. Portanto, S é abeliano e $\mho_1(S) \leq \mho_1(G) \leq Z(G)$.

Observemos que $Z(H \times K) = Z(H) \times K = \mathbb{Z}_p \times \mathbb{Z}_{p^{r-2}}$, então $Z(G) = \frac{Z(H) \times K}{D}$ é cíclico.

Se $\mho_1(S) \neq 1$, então $|\mho_1(S)| > p$ e $\mho_1(S) \leq Z(G)$, logo, $G' = \Omega_1(Z(G)) \leq \mho_1(S)$. Portanto, $G' \leq S$ e temos uma contradição, novamente. Logo $\mho_1(S) = 1$ e todo subgrupo não normal de G é abeliano elementar. Concluímos que $S \leq \Omega_1(G) = H$. Mas sabemos que $H = E_{p^3}$ contém $p+1$ classes de conjugação de subgrupos cíclicos que são não normais em G. Todos subgrupos de ordem p^2 de H contém G' e portanto são normais com G. Portanto $\nu(G) = p + 1$. □

Observe que para $n = 3$ o grupo D_{p^n} definido no teorema acima é exatamente o grupo do exemplo 2.7, E_{p^3}.

A inclusão inversa, ou seja, a parte que diz que, dado um grupo G tal que $\nu(G) = p + 1$, podemos concluir que $G \cong D_{p^r}$, com $p > 2$ e $r \geq 3$ será demonstrada no próximo capítulo, onde provaremos o resultado geral do artigo de R. Brandl [Br13], que é nosso objetivo geral.

Capítulo 4

Classificação de Grupos com até $p+1$ Classes de Conjugação de Subgrupos Não-Normais

À luz dos resultados vistos nos capítulos anteriores, temos que a classificação dos p-grupos finitos, p ímpar, com $\nu(G) \leq p+1$ pode ser resumida pelo seguinte teorema de [Br13]:

Teorema 4.1 (Brandl)**.** *Seja G um p-grupo de ordem p^r com $p > 2$. Se $\nu(G) \leq p+1$, então G possui uma das seguintes características:*
(i) G é abeliano;
(ii) $\nu(G) = 1$ e $G \cong M_{p^n} = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle, (n \geq 3)$;
(iii) $\nu(G) = p$ e $G \cong L_{p^n} = \langle a, b \mid a^{p^{n-2}} = b^{p^2} = 1, a^b = a^{1+p^{n-3}} \rangle$, $(n \geq 4)$;
(iv) $\nu(G) = p+1$ e $G \cong D_{p^n} = \langle x, y, y | x^p = y^p = z^{p^{n-2}} = [x, z] = [y, z] = 1; y^x = yz^{n-3}, (n \geq 3)$.

Observação 4.2. *Não existe um grupo G de ordem p^3 tal que $\nu(G) = p$.*

Antes de provar esse Teorema, vamos conhecer alguns resultados que serão essenciais para a demonstração.

Vimos que La Heye e Rhemtula provaram que: (também válido para $p = 2$) Se G é p-grupo então $\nu(G) \leq 1$ ou $\nu(G) \geq p$.

Este próximo resultado classifica p-grupos finitos que tem um subgrupo cíclico maximal e pode ser encontrado em [Ro06]:

Lema 4.3. *Um grupo de ordem p^r tem um subgrupo cíclio maximal se, e somente se, é algum dos seguintes:*

(i) Um grupo cíclico de ordem p^r;

(ii) Um produto direto de um grupo cíclico de ordem p^{r-1} e outro de ordem p;

(iii) $\langle a, b |\ a^{p^{r-1}} = 1 = b^p, a^b = a^{1+p^{r-2}} \rangle = M_{p^r}$;

(iv) O grupo diedral D_{2^n} *e* $n \geq 3$*;*

(v) O grupo quatérnio generalizado $Q_{2^n}, n \geq 3$;

(vi) O grupo semi diedral $\langle a, b |\ a^{2^{n-1}} = 1 = b^2; a^b = a^{2^{n-2}-1} \rangle, n \geq 3$.

O resultado seguinte está devidamente provado no livro do Huppert [BH67]:

Lema 4.4. *Seja* G *um* p*-grupo não abeliano de ordem* p^n*,* $p > 3$*. Suponha que todo subgrupo minimal abeliano de* G *pode ser gerado com no máximo dois elementos. Então* G *pertence a uma dos três seguintes classes:*

(i) G *é metacíclico;*

(ii) $G = \langle x, y, y | x^p = y^p = z^{p^{n-2}} = [x, z] = [y, z] = 1; y^x = yz^{n-3} \rangle \cong D_{p^n}$; G *é também o produto central de um grupo não abeliano de ordem* p^3 *e expoente* p*,* $E_{p^3} = \langle x, y \rangle$*. E* $k = \langle z \rangle$*,* $|k| = p^{n-2}$ *e os subgrupos* E'_{p^3} *e* $\Omega_1(k)$ *são identificados.*

(iii) $G = \langle x, y, z | x^p = y^p = z^{p^{n-2}} = [y, z] = 1; y^x = yz^{sp^{n-3}}, z^x = yz \rangle$*. Com* $n \geq 4$ *e* $s = 1$ *ou* s *não quadrado mod* p*.*

Observação 4.5. *[BH67], (pág.*346; 12.5*) Para* $p = 3$*, além dos grupos da lista do teorema 4.4, temos que adicionar alguns grupos de classe maximal.*

Lema 4.6. *Seja* G *um grupo de ordem* p^r*,* $r \geq 3$ *e* p *primo ímpar. Suponha que todo quociente próprio de* G *é abeliano. Então* G *é abeliano,* $G \cong M_{p^r}$*,* $G \cong D_{p^r}$ *ou* $\nu(G) \geq p + 2$*.*

Demonstração. Se G é abeliano, já obtemos o resultado. Vamos assumir que G é não abeliano e para todo $M \trianglelefteq G$, G/M é abeliano e então $G' \leq M$. Se $G' \neq 1$, então $G' \trianglelefteq G$. Como $G' \leq M$, temos que G' é normal minimalem G e, portanto, $G' \leq Z(G)$. e $|G'| = p$.

Como G' é o único subgrupo normal minimal de G, temos que $Z(G)$ só tem um subgrupo de ordem p, logo $Z(G)$ é cíclico. Sendo $[x^p, y] = [x, y]^p$, temos que $\mho_1(G) \leq Z(G)$.

Por outro lado, como o derivado é cíclico, temos que G é p-grupo regular e vale $|\mho_1(G)| = |G : \Omega_1(G)|$, por 1.62. Seja $|\Omega_1(G)| = p^e$. Primeiro se $e = 1$, G é cíclico. Seja $e = 2$, pela propriedade dos p-grupos regulares citada anteriormente, temos que, $|\mho_1(G)| = |G : \Omega_1(G)| = p^{r-2}$.

Sabemos que se $|G : Z(G)| = p$, então $G/Z(G)$ é cíclico e G é abeliano por 1.29. Como $|G : \mho_1(G)| = p^2$, e $\mho_1(G) \leq Z(G)$ temos que $\mho_1(G) = Z(G)$. Como $Z(G)$ é cíclico, temos que $\mho_1(G) = \langle g^p \rangle$, para algum $g \in G$.

Daí, como $o(g^p) = p^{r-2}$ temos $o(g) = p^{r-1}$, e então G contém um subgrupo cíclico de índice p e pelo Lema 2.3, $G \cong M_{p^r}$.

Agora, seja $e \geq 3$. Se G contém um subgrupo abeliano elementar normal T de ordem p^3, então T possui p^2+p+1 subgrupos de ordem p, mas como $G' \leq T$ é normal em G, então p^2+p subgrupos de T são não normais em G. Seja $H \leq T$, com $|H| = p$ e $H \ntrianglelefteq G$. Para todo $g \in G$, $H^g \leq T^g = T$.

Seja $x \in G$, então $|[x]_{C_G}| = \{g^{-1}xg|\ g \in G\} = \{x[x,g]|g \in G\} \leq |G'| = p$. Logo $|[\langle x\rangle]_{C_G}| = p$ e temos, $\frac{p^2+p}{p} = p+1$ classes de conjugação de comprimento p. Se todos os subgrupos de T de ordem p^2 fossem normais em G, teríamos que as todas interseções também seríam normais em G. Então todos subgrupos de ordem p seriam normais. Segue que existe um subgrupo não normal de ordem p^2. Logo $\nu(G) \geq p+1+1 = p+2$.

Dessa forma podemos supor que, todo subgrupo normal abeliano de G será gerado por 2 elementos. E, pelo Lema 4.4, para $p > 3$, temos três possibilidades:

Primeiro, se G é metacíclico, então existe um subgrupo cíclico $H = \langle h\rangle$ de G tal que G/H é cíclico. Então, $G' \leq H$ e como G' é cíclico, temos que G é regular, isto implica $|\Omega_1(G)| = |G : \mho_1(G)|$. Como $G/H = \langle gH\rangle$, temos que $G = \langle g, h\rangle$ e $\frac{G}{\mho_1(G)}$ é 2-gerado de expoente p e sendo $G' \leq \Omega_1(G)$, abeliano. Portanto $|\frac{G}{\mho_1(G)}| = p^2$, então $|\Omega_1(G)| = p^2$. Neste caso, $e = 2$ e já vimos este caso anteriormente.

Segundo, temos que $G = \langle x, y, z | x^p = y^p = z^{p^{n-2}} = [y,z] = 1; y^x = y.z^{sp^{n-3}}; z^x = yz\rangle$, ou seja $G = (\langle y\rangle \times \langle z\rangle) \rtimes \langle x\rangle$. Dessa forma, $G' = \langle [y,x],[z,x]\rangle^G = \langle z^{sp^{n-3}}, y\rangle$ não é cíclico, e isto contradiz a hipótese.

Logo, $G = \langle x, y, z | x^p = y^p = z^{p^{n-2}} = [x,z] = [y,z] = 1; y^x = yz^{p^{n-3}}\rangle$, isto é, $G = (\langle y\rangle \times \langle z\rangle) \rtimes \langle x\rangle$. Como $\langle z\rangle \leq Z(G)$, concluímos que $G = D_{p^r}$.

Se $p = 3$, pela Observação 4.5, temos que adicionar alguns grupos de classe maximal à lista anterior, mas como G tem classe 2 a única possibilidade é que $|G| = p^3$. Então $G \cong E_{p^3}$ ou $G \cong M_{p^3}$. □

Este teorema encontra-se em [Br10], bem como sua prova.

Lema 4.7. *Seja p primo, seja $H = M_{p^{r-1}}$ onde $r \geq 4$, se $p > 2$ e $n \geq 5$ se $p = 2$. Além disso, seja $G = H \times C$, sendo $C = \langle c\rangle$ o grupo cíclico de ordem p, então $\nu(G) = 2p$.*

Demonstração. Seja $H = \langle a, b|\ a^{p^{r-2}} = b^p = 1,\ a^b = a^{1+p^{r-3}}\rangle$. Como, para todo $K \leq G$, temos que $\mho_1(K) \leq \mho_1(G) \leq \langle a^p\rangle$ se $\mho_1(K) \neq \{1\}$, sendo $G' = \langle a^{p^{r-2}}\rangle$, então $K \cap G' \neq \{1\}$, $G' \leq K$ e $K \trianglelefteq G$. Se $K \ntrianglelefteq G$, então $K^p = 1$, isto implica, $K \leq \Omega_1(G) = \langle a^{p^{r-2}}, b, c\rangle = \langle a^{p^{r-2}}\rangle \times \langle b\rangle \times \langle c\rangle$, $|\Omega_1(G)| = p^3$ e $\Omega_1(G)$ tem p^2+p+1 subgrupos de ordem p.

Se $H \leq \Omega_1(G)$, com $|H| = p$, então $H \trianglelefteq G$ se, e somente se, $H \leq Z(G) = \langle a^{p^{r-1}}\rangle \times \langle c\rangle$, logo $H \leq Z(G) \cap \Omega_1(G) = \Omega_1(Z(G))$. Em $\Omega_1(G)$ temos $p+1$ subgrupos centrais , logo normais, e p^2 subgrupos não normais.

Suponhamos agora que $H \ntrianglelefteq G$. Como $N_G(H) \geq \langle H, Z(G)\rangle$ e $H \cap Z(G) = 1$,logo

$$|H \times Z(G)| = p^{r-1} \leq |N_G(H)| < p^r,$$

donde $|G : N_G(H)| = p$ e cada subgrupo não normal tem p conjugados. Assim, temos $\frac{p^2}{p}$ classes de conjugação.

Seja $|K| = p^2$, tal que $K \leq \Omega_1(G) = \langle a^{p^{r-2}} \rangle \times \langle b \rangle \times \langle c \rangle$. Suponha $K \trianglelefteq G$, então $K \cap Z(G) \neq 1$, $K \cap \Omega_1(Z(G)) \neq 1$ e $\Omega_1(Z(G)) = \langle a^{p^{r-2}} \rangle \times \langle c \rangle$. Dessa forma, temos que $K \cap \Omega_1(G) = \langle a^{p^{r-2}i}c \rangle$ com, $0 \leq i \leq p-1$ ou $K \cap Z(G) = \langle a^{p^{r-2}} \rangle = G'$. Se $K \cap Z(G) = \langle a^{p^{r-2}i}c \rangle$ temos $a^{p^{r-2}i}(K \cap Z(G) = c^{-1}(K \cap Z(G))$ e $\langle c(K \cap Z(G)) \rangle = \langle a^{p^{r-2}i}(K \cap Z(G)) \rangle$. Então $\frac{G}{K \cap Z(G)} = \langle \bar{a}, \bar{b} | \bar{a}^{p^{r-1}} = \bar{b}^p = 1, \bar{a}^{\bar{b}} = \bar{a}^{1+p^{r-2}} \rangle \cong M_{p^{r-1}}$, e $\frac{K}{K \cap Z(G)} \trianglelefteq \frac{G}{K \cap Z(G)}$ se, e somente se, $\frac{K}{K \cap Z(G)} = \langle a^{p^{r-2}}(K \cap Z(G)) \rangle$ e $K = \langle a^{p^{r-2}}, ca^{p^{r-2}i} \rangle = \langle a^{p^{r-2}}, c \rangle$, segue que $G' \leq K$. Como os subgrupos de $\Omega_1(G)$ que contém G' são $p+1$ e temos p^2+p+1 subgrupos de ordem p^2, então $p^2+p+1-p-1 = p^2$ são não-normais.

Agora, $N_G(K) \geq \langle K, Z(G) \rangle \gneqq Z(G)$, implica, $|G : N_G(K)| \leq p$, logo $|G : N_G(K)| = p$ e cada classe tem p elementos. Então são p^2/p classes. Portanto, temos p classes de ordem p e p classes de ordem p^2 e concluímos que $\nu(G) = 2p$. □

Lema 4.8. *Seja G um grupo de ordem p^r, com $r \geq 4$, $p > 2$. Assuma que $\nu(G/M) < p$, para todo subgrupo normal minimal M de G, e existe um subgrupo normal minimal $N \leq G$ tal que $G/N \cong M_{p^{r-1}}$. Então $G \cong L_{p^r}$ ou $\nu(G) = 2p$.*

Demonstração. Seja $G/N = \langle aN \rangle \rtimes \langle bN \rangle \cong M_{p^{r-1}}$, onde $o(aN) = p^{r-2}$ e $o(bN) = p$, temos $a^{p^{r-2}} \in N$ e $a^{p^{n-1}} = 1$. Se $o(a) = p^{r-1}$, então G contém um subgrupo de índice p, isto é, possui um subgrupo cíclico maximal e então, pela classificação de tal grupo, apresentada anteriormente, temos que $G \cong M_{p^r}$, e isso é uma contradição, pois todo quociente de M_{p^r} é abeliano.

Dessa forma, $o(a) = p^{r-2}$. Como $a^{p^{n-3}} \notin N$, segue que $\langle a \rangle \cap N = \{1\}$. Dessa forma, definamos $A = \langle N, a \rangle = N \times \langle a \rangle$ e $A_o = A^{p^{r-3}} = \langle a^{p^{r-3}} \rangle$. Como A é normal em G, temos que A_o também é normal em G e $|A_o| = p$.

Vamos estudar os casos em que $\langle a \rangle$ é normal e o caso em que não é normal.

Primeiro, assumindo que $\langle a \rangle$ não é normal em G, temos então que $\frac{\langle a \rangle}{A_o}$ é também não-normal em $\frac{G}{A_o}$, logo $\frac{G}{A_o}$ não é abeliano e como $\nu(\frac{G}{A_o}) < p$, concluímos que $\nu(\frac{G}{A_o}) = 1$ e portanto $\frac{G}{A_o} \cong M_{p^{r-1}}$ e isto implica $\frac{\langle a \rangle}{A_o}$ ter ordem p, logo $o(a) = p^2$, mas, como vimos, $o(a) = p^{r-2}$, logo $|G| = p^r = p^4$ e, pela classificação de grupos de ordem p^4, em [BH67], temos que $G \cong L_{p^4}$.

Agora, considerando $\langle a \rangle$ normal em G. Seja $H = \langle a, b \rangle$, então $G = \langle a, b, N \rangle = HN$, sendo $N \leq Z(G)$. Se $H \cap N = 1$, temos que $G = H \times N$, como $\frac{G}{N} \cong M_{p^{r-1}}$, concluímos que $\frac{G}{N} \cong H \cong M_{p^{r-1}}$ e, como $N \cong C_p$, pelo lema 4.7 temos que $\nu(G) = 2p$.

Se $H \cap N = N$, então $H = G$ e $G = \langle a, b \rangle = \langle a \rangle \langle b \rangle$. Como $|G| = p^r$, $|a| = p^{r-2}$ e $|b| \leq p^2$, se $|\langle a \rangle \cap \langle b \rangle| \geq p$ teríamos que $|G| < p^r$. Logo $|b| = p^2$ e $G = \langle a \rangle \rtimes \langle b \rangle$.

Vamos olhar a ação de a sobre b.

Sabemos que $\frac{G}{N} = \langle aN \rangle \rtimes \langle bN \rangle$ e $(aN)^{bN} = (aN)^{1+p^{r-3}}$. Então existe um $n \in N$ tal que $a^b = a^{1+p^{r-3}}n \in \langle a \rangle$, implica que $n \in N \cap \langle a \rangle = \{1\}$, então $a^b = a^{1+p^{r-3}}$ e

$G \cong L_{p^r}$. □

Lema 4.9. *Seja G um p-grupo metacíclico, com $p > 2$.*

(i) Se $|\Omega_2(G)| = p^3$, então $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{r-1}}$ ou $G \cong M_{p^r}$;

(ii) Se $|\Omega_2(G)| = p^4$, então, para todo elemento $x \in G$ com $o(x) = p$, existe $y \in G$ com $x = y^p$.

Demonstração.

(i) Como G é metacíclico, com $p \neq 2$, temos que, G' é cíclico e então G é regular e $|\Omega_1(G)| = p^2$. Sabemos que $\Omega_1(\frac{G}{\Omega_1(G)}) = \frac{\Omega_2(G)}{\Omega_1(G)}$, e $|\Omega_2(G)| = p^3$, logo $\Omega_1(\frac{G}{\Omega_1(G)})$ tem ordem p.

Como $p \neq 2$, isto implica $G/\Omega_1(G)$ ser cíclico, Seja $b\Omega_1(G)$ um gerador. Seja $|G| = p^r$, dessa forma, $o(b) \geq p^{r-2}$. Se $o(b) = p^{r-2}$,então $\langle b\rangle \cap \Omega_1(G) = \{1\}$, que é absurdo! Portanto $o(b) = p^{r-1}$ e, pelo Lema 4.3, $G = \langle a, b\rangle$ com $o(a) = p$. Logo, $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{r-1}}$ se G é abeliano ou $G \cong M_{p^r}$ se G não é abeliano.

(ii) Por hipótese, o grupo $K = \Omega_2(G)$ tem ordem p^4. Sendo G regular e $exp(K) = p^2$.

Como K é metacíclico, existe $\langle a\rangle \trianglelefteq K$, tal que $K/\langle a\rangle$ é cíclico. Então $K/\langle a\rangle = \langle b\langle a\rangle\rangle$, logo, $K = \langle a, b\rangle$. Por outro lado, se $|\langle a\rangle \cap \langle b\rangle| > 1$, temos $|K| < p^4$. Portanto, $|\langle a\rangle \cap \langle b\rangle| = \{1\}$ e $K = \langle a\rangle \rtimes \langle b\rangle$, ambos elementos a, b com ordem p^2, e, pela caractericação de grupos de ordem p^4 encontrada em [BH67]: $K \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ ou $K \cong L_{p^2}$.

Se $K \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} = \langle a\rangle \times \langle b\rangle$ e $\Omega_1(K) = \{(a^r b^m)^p |\ m, n \in \{0, \cdots, p-1\}\}$ e então, para todo $g \in \Omega_1(G)$, existe x^p tal que $y = x^p$.

Se $K \cong L_{p^2} = \langle a, b |\ a^{p^2} = b^{p^2} = 1; a^b = a^{1+p}\rangle$, temos que $\Omega_1(G) = \Omega_1(\langle a\rangle)\Omega_1(\langle b\rangle) = \langle a^p\rangle\langle b^p\rangle = \langle a^p b^p\rangle = \{(a^n b^m)^p |\ m, n \in \{0, \cdots, p-1\}\}$. E obtemos o resultado.

□

Lema 4.10. *Seja $|G| = p^r$, com $r \geq 5$ e $p > 2$. Assuma que $\nu(G/M) \leq p$, para todo subgrupo normal minimal $M \leq G$ e que existe um subgrupo normal minimal $N \leq G$ com $G/N \cong L_{p^{r-1}}$. Então $\nu(G) \geq p + 2$.*

Demonstração. $G/N \cong L_{p^{r-1}} = \langle aN\rangle \times \langle bN\rangle$, com $o(aN) = p^{r-3}$ e $o(bN) = p^2$. Sejam $H_1/N, \cdots, H_p/N$ representantes para as classes de conjugação de subgrupos não normais de G/N. Pela estrutura de G/N, temos que $|H_i| = p^3$, para todo $i = \{1, \cdots, p\}$.

Vamos analisar dois casos: quando $\langle a\rangle$ é normal em G e quando $\langle a\rangle$ é não normal em G.

Caso 1: Suponha $\langle a\rangle$ normal em G.

Seja $H = \langle a, b\rangle$, então $G = \langle a, b, N\rangle = HN$. Se $H \neq G$, então $H \cap N = 1$ e $G = H \times N$, com $H \cong G/N \cong L_{p^{r-1}}$. Logo, $G \cong L_{p^{r-1}} \times \mathbb{Z}_p$.

Sejam $C_1, \cdots, C_p$ subgrupos não-normais e não conjugados de H. Então

$$C_1, \cdots, C_p, C_1 \times N, \cdots, C_p \times N$$

são dois a dois não-normais e não conjugados, pois C_i e C_j não são conjugados, para $i \neq j$, pois $|C_i| = p^2$ e $|C_j \times N| = p^3$ logo C_i não é conjugado com $C_j \times N$, para todo i, j, portanto $\nu(G) \geq 2p$.

Se $G = H = \langle a, b\rangle$, com $\langle a\rangle \trianglelefteq G$, temos que G é metacíclico e $\Omega_2(G) = p^3$ ou p^4. Suponha que G possui subgrupos não-normais de ordem p e existe T subgrupo cíclico de ordem p^2 tal que $S \leq T$, isto é, $S = T^p$. Como $S \ntrianglelefteq G$, então $T \ntrianglelefteq G$, temos que S e T não são conjugados com H_i, visto que $|H_i| = p^3$. Portanto, temos que $S, T, H_1, \cdots, H_p$ são subgrupos não-normais e não conjugados e então $\nu(G) \geq p + 2$. Se S não está contido em um subgrupo cíclico de ordem p^2, pelo Lema 4.9, temos que $G \cong M_{p^r}$, mas isto não pode ocorrer, já que estamos supondo que existe um subgrupo normal minimal N, tal que $\nu(G/N) \cong L_{p^{r-1}}$.

Então todo S de ordem p é normal em G. Temos que, $S \leq Z(G)$ e isto implica que $\Omega_1(G) \leq Z(G)$. Como G é metacíclico, temos que $G' \leq \langle a\rangle$, logo G' é cíclico. Mas $\Omega_1(G)$ não é cíclico então podemos escolher um subgrupo normal minimal $M \leq G$ tal que $G' \cap M = \{1\}$.

Sabemos que $\nu(G/M) \leq p$, temos que $\nu(G/M) = 0, 1, p$.

Se $\nu(G/M) = 0$, então $(G/M)' = \{1\}$

Se $\nu(G/M) = 1$, então $G/M \cong M_{p^r}$ e $|(G/M)'| = p$

E, se $\nu(G/M) = p$, temos que $G/M \cong L_{P^r}$ e $|(G/M)'| = p$. Log, $|(G/M)'| \leq p$; isto implica $|\frac{G'M}{M}| \leq p$ e, então, $|\frac{G'}{M\cap G'}| = |G'/\{1\}| = |G'| = p$. Portanto, $|G'| = p$.

Seja S um subgrupo não cíclico de G. Então $|\Omega_1(S)| \geq p^2$. Como $|\Omega_1(G)| = p^2$, temos que $\Omega_1(S) = \Omega_1(G)$ e $G' \leq \Omega_1(G) = \Omega_1(S)$ implica $G' \leq S$ e $S \trianglelefteq G$. Por outro lado, temos que $\Omega_1(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ e $\Omega_1(G)$ possui $p + 1$ subgrupos. Como $G' \leq \Omega_1(G)$ e $N \leq \Omega_1(G)$, chamaremos os $p - 1$ restantes como Z_i, $i = 2, \cdots, p$. Para $i = \{2, \cdots, p\}$, escolhamos $\frac{S_i}{Z_i} \leq \frac{G}{Z_i}$. Como G/Z_i é não abeliano, então existe $\frac{S_i}{Z_i} \ntrianglelefteq G/Z_i$.

Se S_i não é cíclico, então $S_i \ntrianglelefteq G$, contradição. Então, S_i é cíclico, para todo $i = \{2, \cdots, p\}$ e Z_i é o único subgrupo de ordem p, para i fixado. Se $S_i = S_j^g$, então $Z_1 = Z_2$, contradizendo o que vimos. Logo $[S_i]_{C_G} \neq [S_j]_{C_G}$, com $i \neq j$, com $i = 2, \cdots, p$ e temos $p - 1$ classes. Lembrando que temos $H_1 \cdots H_p$ não conjugados com $S_1 \cdots S_p$, segue $\nu(G) \geq p + p - 1 = 2p - 1 \geq p + 2$, para $p > 2$.

Caso2: $\langle a\rangle$ é não-normal em G.

Sabemos que $\langle aN\rangle \trianglelefteq G/N$ e $H_1/N, \cdots, H_p/N$ são representantes das classes de subgrupos não normais de G/N, logo $\langle aN\rangle \notin [H_i/N]_{C_{G/N}}$ para todo i, e isto implica que, $\langle a\rangle \notin [H_i]_{cG}$ e então $\nu(G) \geq p + 1$.

Suponha que exista j tal que H_j não é cíclico. Para todo $y \in H_j$, se $\langle y\rangle \trianglelefteq G$, temos que $H_j \trianglelefteq G$, então existe um cíclico $C \ntrianglelefteq G$, com $C \leq H_j$. Como $C \lneqq H_j$, temos que $|c| \neq |H_j|$. Logo, $\nu(G) \geq p + 1 + 1 = p + 2$.

Se H_i é cíclico para todo i e se existe S, com $|S| = p$ tal que $S \ntrianglelefteq G$ e, como $|H_i| = p^3$, $|\langle a\rangle| \geq p^2$ e $|S| = p$ não são conjugados, então $\nu(G) \geq p+2$. Se todos S de ordem p são

normais em G, então $\Omega_1(G) \leq Z(G)$. Sejam $Z_1, \cdots, Z_{p+1}$ subgrupos normais minimais de G. Se existe $i \neq j$ tal que G/Z_i e G/Z_j são abelianos, temos $G' \leq Z_i \cap Z_j = \{1\}$ e G abeliano, que é uma contradição. Isto implica no máximo existir j tal que G/Z_j é abeliano e, para todo $i \neq j$ G/Z_j é não-abeliano. Como $p > 2$, temos que $p + 1 > 3$ e podemos escolher um subgrupo normal $Z \in G$ tal que $Z \in \{Z_1, \cdots, Z_{p+1}\} \setminus \{Z_j, N, \Omega_1(\langle a \rangle)\}\}$.

Como G/Z é não abeliano existe $U/Z \nleq G/Z$ com $U \nleq G$. Sabemos que H_i é cíclico, isto implica N ser o único subgrupo de H_i de ordem p. Então $Z \nleq H_i$ e $Z \nleq H_i^g$. Como $Z \leq U$ e U não é conjugado com H_i, do mesmo modo, como $\langle a \rangle$ é cíclico, temos que $\Omega_1(\langle a \rangle)$ é o único subgrupo de ordem p de $\langle a \rangle$ e $Z \neq \Omega_1(\langle a \rangle)$. Se U fosse conjugado com $\langle a \rangle$, então teríamos $Z \leq \langle a \rangle$, o que é absurdo! Então $U, \langle a \rangle, H_i$ não são conjugados, para todo, $i = 1, \cdots, p$. Portanto $\nu(G) \geq p + 2$.

□

Finalmente, agora estamos aptos para provar nosso teorema de classificação de todos os grupos G com ordem $\nu(G) \leq p + 1$, onde p denota um número primo.

Teorema 4.11 (Brandl)**.** *Seja G um p-grupo de ordem p^r com $p > 2$. Se $\nu(G) \leq p + 1$, então G possui uma das seguintes características:*
(i) G é abeliano;
(ii) $\nu(G) = 1$ e $G \cong M(p^n) = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle, (n \geq 3)$;
(iii) $\nu(G) = p$ e $G \cong L(p^n) = \langle a, b \mid a^{p^{n-2}} = b^{p^2} = 1, a^b = a^{1+p^{n-3}} \rangle$, $(n \geq 4)$;
(iv) $\nu(G) = p + 1$ e $G \cong D(p^n) = \langle x, y, y | x^p = y^p = z^{p^{n-2}} = [x, z] = [y, z] = 1; y^x = yz^{n-3}, (n \geq 3)$.

Demonstração. Faremos indução sobre r. Se $r \leq 2$, G é abeliano. Se $r = 3$, então G é abeliano, $G \cong M_{p^3}$ ou $G \cong E_{p^3} = D_{p^3}$. Então, assumiremos $r \geq 4$.

Seja N um subgrupo normal minimal de G, então temos que $\nu(G/N) \leq p + 1$ e, por indução, G/N é um dos tipos $(i), (ii), (iii)$ ou (iv).

Suponha por absurdo que $\nu(G/N) = p + 1$, então como $\nu(G) = p + 1$, podemos observar que todos subgrupos não normais de G contém N. Logo, todos subgrupos não normais de G tem intersseção não trivial. Por 2.4, temos $p = 2$, o que contradiz nossa hipótese. Portanto, nós temos que $\nu(G/N) \leq p$ e $G/N \ncong D_{p^{r-1}}$. Então um dos seguintes casos pode ocorrer:

Caso 1: Todo quociente próprio G/N é abeliano;

Caso 2: Existe quociente próprio não abeliano e para todo $M \trianglelefteq G$, minimal, temos que $\nu(G/N) < p$;

Caso 3 Existe quociente próprio não abeliano e existe $N \trianglelefteq G$, minimal, tal que $\nu(G/N) = p$ e $\left|\frac{G}{N}\right| \geq p^4$ e $|G| \geq p^5$.

No caso 1, pelo lema em 4.6, temos que G é abeliano, $G \cong M_{p^r}$ ou $G \cong D_{p^r}$. No caso 2, usando o lema 4.8 que $G \cong L_{p^r}$. Se $r = 4$, o caso 3 não acontece porque não

existe um grupo de ordem p^3 e $\nu(G) = p$. Se $r \geq 5$ o lema 4.10 afirma que o caso 3 não acontece. Desta forma, completamos a demonstração. □

A tabela abaixo resume o que foi feito, até o momento, de pesquisas nesta área.

Hipóteses	Autor e Ano	Resultado
$\nu(G) = 0$	Dedekind; Baer	G abeliano, $G \cong Q_8 \times A \times B$
$\nu(G) = 1$	Brandl R.; 95	$G \cong M_{p^n}$
$\nu(G) = p$ e $p > 2$	Fernandéz A.; Leire L.; 10	$G \cong L_{p^n}$ $n \geq 4$
$\nu(G) = p + 1$ e $p > 2$	Brandl R.; 2013	$G \cong D_{p^n}$ $n \geq 3$

Desse modo, o caso em que $\nu(G) \geq p + 1$ ainda não é conhecida uma caracterização, tampouco se existe alguma 'salto' no número das classes de conjugação de subgrupos não-normais. Restando assim, muito ainda para ser pesquisado.

Considerações Finais

O objetivo geral deste trabalho foi classificar os p-grupos finitos que possuem "poucas"classes de conjugação de subgrupos que não são normais, isto é, quando $\nu(G) \leq p+1$, e sendo p um primo ímpar. O caso em que $p = 2$ ainda está em aberto e fica com uma sugestão para trabalhos futuros. O estudo de classificação de p-grupos finitos com poucas classes de conjugação de subgrupos não-normais requer detalhes de todos os casos prováveis para que possa ser tirada uma conclusão geral, por isso, é um estudo muito complexo que possui ainda muitas coisas a serem descobertas. Também temos como sugestão a caracterização do grupo G quando $\nu(G) = p+2$.

Referências

[BH67] Huppert B. *Endliche Gruppen I.* Springer-Verlag, Berlin Heidelberg, Nova York 1967.

[Bn66] Blackburn N. *Finite groups in which the nonnoemal subgroups have nontrivial intersection.*Journal of Algebra **3**(1966), 30–37.

[Br95] Brandl R. *Groups with few non-normal subgroups.* Comm. Algebra **23** (1995), no. 6, 2091–2098.

[Br10] Brandl R. *Conjugacy Ccass of subgroups of finite p-groups: The first gap.* Proccedings of Ischia Group Theori 2010, World Scientific Publishing, Singapore, 2010, pp. 39–44.

[Br13] Brandl R. *Conjugacy Classes of non-normal subgroups of finite p- groups.* Israel Journal of Mathematics **195** (2013), 473–479;

[FA00] Fernandéz-Alcober G. *An introduction to finite p-groups: regular p-groups and groups of maximal class.* XXI Brazilian Algebra Meeting. (2000).

[FALe08] Fernández-Alcober G. e Legarreta L., *Conjugacy classes of non-normal subgroups in finite nilpotent groups.* Journal of Group Theory **11** (2008), 381–397.

[FALe09] Fernández-Alcober G. e Legarreta L.,*Bounds for the number of conjugacy classes of non-normal subgroups.* Journal of Group Theory **37** (2009), 41–63.

[FALe10] Fernández-Alcober G. e Legarreta L. *The finite p-groups with p conjugacy classes of non-normal subgroups.* Israel J. Math. **180** (2010), no. 11, 189–192.

[LHRh99] La Haye R.; Rhemtulla A. *Groups with a bounded number of conjugacy classes of non-normal subgroups.* J. Algebra **214** (1999), no. 1, 41–63.

[LL07] Legarreta L., *Conjugacy Classes of subgroups in Finite p-Groups.*PhD Thesis, Bilbao, 2007. J. Algebra **214** (1999), no. 1, 41–63.

[MM03] Miller G. A. e Moreno H. C.*Non-abelian groups in which every subgroups is abelian.* Transactions of the American Mathematical Society **4**(1903), 398–404.

[Ro82] Robinson D. J. S., *A Course in the Theory of Groups.* Springer-Verlag (1982).

[Ro06] Robinson D. J. S., *A Course in Linear Algebra with Aplications.* World Scientific (2006).