UNIVERSIDADE ESTADUAL DE MARINGÁ

CENTRO DE CIÊNCIAS EXATAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

(Mestrado)

Um estudo sobre cotas superiores para os expoentes de um p-grupo finito e seu multiplicador de Schur

Luís Miguel Rissi Fertunani

Orientadora: Profa. Dra. Irene Naomi Nakaoka

Maringá - PR

2024

[1]O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Um estudo sobre cotas superiores para os expoentes de um p-grupo finito e seu multiplicador de Schur

Luís Miguel Rissi Fertunani

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.
Área de concentração: Álgebra

Orientadora: Profa. Dra. Irene Naomi Nakaoka

Maringá - PR

2024

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

Fertunani, Luís Miguel Rissi
F411e Um estudo sobre cotas superiores para os expoentes de um p-grupo finito e seu multiplicador de Schur / Luís Miguel Rissi Fertunani. -- Maringá, 2024.
x, 85 f. : il.

Orientadora: Profª. Drª. Irene Naomi Nakaoka.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática – Área de Concentração: Álgebra, 2024.

1. Grupo finito. 2. Expoente. 3. Multiplicador de Schur. 4. Quadrado superior não abeliano. 5. Finite group. 6. Schur multiplier. 7. Non-abelian exterior square. I. Nakaoka, Irene Naomi, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemáica – Área de concentração: Álgebra. III. Título.

CDD 22.ed. 512.2
Edilson Damasio CRB9-1.123

LUÍS MIGUEL RISSI FERTUNANI

UM ESTUDO SOBRE COTAS SUPERIORES PARA OS EXPOENTES DE UM P-GRUPO FINITO E SEU MULTIPLICADOR DE SCHUR

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Profa. Dra. Irene Naomi Nakaoka - UEM (Presidente)

Prof. Dr. Noraí Romeu Rocco - UnB

Prof. Dr. Marcelo Escudeiro Hernandes - UEM

Aprovada em: 29 de fevereiro de 2024.

Local de defesa: Videoconferência – Google Meet (https://meet.google.com/nmy-zxca-dpv)

À minha família.

"O conhecimento nos torna humildes.
A ignorância nos torna arrogantes."

Confúcio.

AGRADECIMENTOS

Agradeço primeiramente à minha família por sempre me apoiar em meus estudos e serem a minha base durante a minha caminhada.

Agradeço principalmente à minha orientadora Profa. Dra. Irene Naomi Nakaoka, por seus ensinamentos e conselhos durante toda minha jornada, desde a graduação até a conclusão do mestrado.

À minha namorada Daniely Andrade Fonseca por sempre me apoiar e estar ao meu lado nos momentos mais desafiadores.

À todos os meus amigos que me apoiaram e me ajudaram com dúvidas e, principalmente, pelas palavras de incentivo.

À todos os professores que estiveram presentes em minha jornada acadêmica.

À CAPES, pelo auxílio financeiro, que foi essencial para que eu pudesse me dedicar exclusivamente aos estudos.

Aos professores doutores Noraí Romeu Rocco e Marcelo Escudeiro Hernandes por terem aceitado fazer parte da banca examinadora desta dissertação, e por contribuírem com sugestões para elaboração da versão final deste trabalho.

Meus sinceros agradecimentos a todos que de alguma forma passaram por minha vida durante essa jornada.

Por fim, agradeço à Deus por me possibilitar e dar forças para alcançar essa nova etapa em minha vida.

RESUMO

Este trabalho contém um breve estudo sobre expoentes de p-grupos finitos. Mais especificamente, apresentamos a demonstração de Antony, Komma e Thomas [2] de que se G é um p-grupo finito de classe de nilpotência no máximo $p+1$, então o expoente do subgrupo derivado de G é um divisor do expoente de $G/Z(G)$, onde $Z(G)$ denota o centro de G. Com base nesse resultado, estudamos algumas cotas superiores para os expoentes do quadrado exterior não abeliano e do multiplicador de Schur de um p-grupo finito que foram estabelecidas em [2, 25]. Além disso, apresentamos uma cota superior devida a Komma e Thomas para o expoente de um p-grupo finito G em função de sua classe de nilpotência e do expoente de um p-subgrupo de Sylow do grupo de automorfismos de G.

Palavras-chave: Grupo finito, Expoente, Multiplicador de Schur, Quadrado exterior não abeliano.

ABSTRACT

This work contains a brief study on exponents of finite p-groups. More specifically, we present Antony, Komma, and Thomas's proof [2] that suppose G is a finite p-group of nilpotency class at most $p+1$, and conclude the exponent of the derived subgroup of G is a divisor of the exponent of $G/Z(G)$, where $Z(G)$ denotes the center of G. Based on this result, we study some upper bounds for the exponents of the non-abelian exterior square and the Schur multiplier of a finite p-group that were established in [2, 25]. Additionally, we present an upper bound due to Komma and Thomas for the exponent of a finite p-group G in terms of its nilpotency class and the exponent of a Sylow p-subgroup of the automorphism group of G.

Keywords: Finite group, Exponent, Schur multiplier, Non-abelian exterior square.

Índice de Notações

$\varnothing$	conjunto vazio
$\mathbb{N}$	conjunto dos números naturais $\{0, 1, \dots\}$
$\mathbb{N}^*$	$\mathbb{N}\backslash\{0\} = \{1, \dots\}$
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Z}_n$	conjunto dos números inteiros módulo n
S_n	grupo simétrico de grau n
D_{2n}	grupo diedral de ordem $2n$
Q	grupo dos quatérnios
$\mathbb{C}^\times$	grupo multiplicativo $\mathbb{C}\backslash\{0\}$
I_n	$\{1, 2, \dots, n\}$
$X \subset Y$	X é um subconjunto de Y
$X \subsetneq Y$	X é um subconjunto próprio de X
$\|X\|$	cardinalidade do conjunto X
$\|g\|$	ordem de um elemento g
$X \times Y$	produto direto de X por Y
$X \setminus Y$	$\{x \in X \mid x \notin Y\}$
$H \leq G$	H é um subgrupo de G
$H < G$	H é um subgrupo próprio de G
$H \lhd G$	H é um subgrupo normal de G
$\langle X \rangle$	subgrupo gerado por X
$\langle X \rangle^G$	fecho normal de X
$G \cong H$	grupo G isomorfo ao grupo H
$Aut(G)$	grupo dos automorfismos de G
$Im(f)$	imagem da função f
$Ker(f)$	núcleo da função f
$C_G(x)$	centralizador de x em G
$C_G(H)$	centralizador de H em G, isto é, $\{g \in G;\ gh = hg,$ para todo $h \in H\}$
$Z(G)$	centro de um grupo G
$[x, y]$	comutador de x por y
$[X, Y]$	subgrupo comutador de X e Y
a^g	imagem da ação de g em a
a^G	classe de conjugação de a em G
$C_G(\phi)$	$\{x \in G : \phi(x) = x\}$, onde $\phi \in Aut(G)$
G'	subgrupo derivado

$H\ char\ G$	H é um subgrupo característico de G
$\frac{G}{H},\ G/H$	grupo quociente de G por um subgrupo normal H
Hg	$\{hg; h \in H\}$ classe lateral à esquerda de H em G
gH	$\{hg; h \in H\}$ classe lateral à direita de H em G
$G \otimes H$	produto tensorial não abeliano de G e H
$G * H$	produto livre de G e H
$K \rtimes Q$	produto semidireto de K por Q
mdc(m, n)	máximo divisor comum entre m e n
mmc(m, n)	mínimo múltiplo comum entre m e n
$\lceil n \rceil$	menor natural maior que n
$\lfloor n \rfloor$	maior natural menor que n
$\gamma_i(G)$	i-ésimo termo da série central inferior de G
$Z_i(G)$	i-ésimo termo da série central superior de G
$G^{(i)}$	i-ésimo termo da série derivada de G
$\Phi(G)$	subgrupo de Frattini de um grupo G
$Z^2(Q, K, \theta)$	conjunto composto por todos os 2-cociclos $f : Q \times Q \to K$
$B^2(Q, K, \theta)$	conjunto composto por todos os 2-cobordos $g : Q \times Q \to K$
$H^2(Q, K, \theta)$	$Z^2(Q, K, \theta)/B^2(Q, K, \theta)$
$H^2(Q, K)$	$H^2(Q, K, \theta)$ com $\theta : Q \to Aut(K)$ trivial
$M(Q)$	$H^2(Q, \mathbb{C}^\times)$

SUMÁRIO

Índice de Notações viii

Introdução 1

1 Preliminares 4

1.1 Cálculos com Comutadores 5

1.2 Grupos Solúveis e Nilpotentes 6

1.3 Apresentação de Grupo 10

1.4 Sequências Exatas 11

1.5 Multiplicador de Schur 12

2 Processo de Coleta 14

3 p-Grupos Finitos 32

3.1 p-Grupos *powerful* 32

3.2 p-Grupos Regulares 39

4 Produto Tensorial não Abeliano de Grupos 44

4.1 Definição e Propriedades 44

4.2 O Quadrado Tensorial Não Abeliano 49

4.3 Produto Exterior Não Abeliano de Grupos 55

5 Cotas superiores para os expoentes de um grupo e de seu multiplicador de Schur 62

5.1 Limites dependendo da classe nilpotência 62

5.2 Expoente de p-grupos metabelianos de classe $2p-1$ 76

Referências Bibliográficas 80

Índice Remissivo **84**

INTRODUÇÃO

Dado um grupo G, dizemos que um natural n é o expoente de G se for o menor natural não nulo tal que $g^n = 1$ para todo $g \in G$. Vamos denotar tal número por $\exp(G)$. Observamos que o expoente de um grupo nem sempre está definido , por exemplo, para grupos livres de torção. É possível mostrar que se o grupo G é finito, então $\exp(G) = \text{mmc}\{|g| \mid g \in G\}$, onde $|g|$ denota a ordem do elemento g em G. Para calcular o expoente de um grupo G, pode-se utilizar o sistema computacional GAP - Groups, Algorithms and Programming [17].

Muito se tem estudado sobre como certas propriedades de $G/Z(G)$ influenciam G', onde $Z(G)$ e G' denotam, respectivamente, o centro de G e o subgrupo derivado de G. Um teorema clássico de Schur [40] nos diz que se $G/Z(G)$ é finito, então G' também possui essa propriedade. Em [30], Mann provou que se G é um grupo com $G/Z(G)$ localmente finito de expoente n, então G' é um grupo localmente finito cujo expoente é finito e depende apenas de n. Seguindo nessa direção, em [2], Antony, Komma e Thomas demonstraram o seguinte resultado:

Teorema A. *Se p for um número primo e G um p-grupo finito com classe de nilpotência menor ou igual a $p+1$, então $\exp(G')$ é um divisor de $\exp(G/Z(G))$.*

Para p-grupos finitos de classe de nilpotência arbitrária c, Komma e Thomas [25] obtiveram a seguinte cota superior para $\exp(G')$:

Teorema B. *Se G é um p-grupo finito com classe de nilpotência $c \geq 1$, então:*

$$\exp(G') \,\Big|\, p^{\lceil \log_p c \rceil - 1} \cdot \exp\left(\frac{G}{Z(G)}\right).$$

Em [24], Khukhro e Shumyatsky limitaram o expoente de um grupo G com base em seu grupo dos automorfismos. Mais especificamente, se A é um grupo abeliano não cíclico de automorfismos de um grupo G, com $\text{mdc}(|A|, |G|) = 1$, e n o mínimo múltiplo comum dos expoentes dos centralizadores $C_G(a)$ para $a \in A \backslash \{1\}$, então Khukhro e Shumyatsky [24] provaram que o expoente de G é limitado em termos de n e q, em que q é o menor primo divisor de $|A|$ tal que o q-subgrupo de Sylow de A é não cíclico.

Komma e Thomas [25] apresentaram uma cota superior para o expoente de um p-grupo finito G em função da classe de nilpotência de G e do expoente de um p-subgrupo de Sylow do grupo de automorfismos de G, conforme abaixo:

Teorema C. *Sejam G um p-grupo finito de classe c e S um p-subgrupo de Sylow de $Aut(G)$, com $\exp(S) = q$. Então, $\exp(G)$ divide $p^{\lceil \log_p c \rceil} q^3$.*

Dado um grupo G com apresentação $\langle X \mid R \rangle$, seja F o grupo livre sobre X e R^F o fecho normal de R em F. Com isso em mente, usaremos o símbolo $M(G)$ para denotar o grupo $\left(F' \cap R^F\right) / \left[F, R^F\right]$ e o chamaremos de multiplicador de Schur de G. Foi conjecturado que $\exp(M(G)) \mid \exp(G)$ para um grupo finito G qualquer, porém isso não acontece para todo grupo, uma vez que Bayes, Kautsky e Wamsley [7] apresentaram um 2-grupo finito G com $\exp(G) = 4$ e $\exp(M(G)) = 8$. Recentemente, Vaughan-Lee [41] exibiu um 5-grupo finito com $\exp(G) = 5$ e $\exp(M(G)) = 25$. Muitos estudos vêm sendo feitos a fim de se determinar quais classes de grupos satisfazem $\exp(M(G)) \mid \exp(G)$. Por exemplo, já foi provado que isso acontece para p-grupos *powerful* [28], p-grupos metabelianos de expoente p [32], p-grupos metabelianos p-centrais [1] e grupos finitamente gerados G tais que $\exp(G/Z(G)) = 6$ [3].

Como uma consequência do Teorema A, Antony, Komma e Thomas mostraram que os p-grupos finitos de classe de nilpotência no máximo p também satisfazem $\exp(M(G)) | \exp(G)$.

Sendo $\gamma_{p+1}(G)$ o p-ésimo termo da série central inferior de um grupo G, Komma e Thomas [25] mostraram a veracidade do resultado abaixo.

Teorema D. *Seja G um p-grupo finito metabeliano com p um primo ímpar. Se a classe de nilpotência de G é menor ou igual a $2p-1$ e $\gamma_{p+1}(G) \leq [G^p, G]$, então $\exp(M(G)) | \exp(G)$.*

Esse teorema é uma consequência de cotas dos expoentes do segundo e terceiro termos da série central inferior de um grupo G, estabelecidos por Komma e Thomas em [25].

Neste trabalho estudamos cotas superiores para o expoente de um p-grupo finito, bem como para o multiplicador de Schur de p-grupos finitos, conforme os artigos [2] e [25].

Estruturamos este trabalho da seguinte forma.

O primeiro capítulo desta dissertação traz resultados importantes e amplamente conhecidos da Teoria dos Grupos que são necessários para os capítulos seguintes. Já no segundo capítulo, apresentamos um método chamado processo de coleta, que nos

permite concluir interessantes congruências módulo um subgrupo normal de um grupo G.

No Capítulo 3, introduzimos os conceitos de p-grupo *powerful* e de p-grupo regular e algumas de suas propriedades que são necessárias nos capítulos subsequentes.

O penúltimo capítulo apresenta um breve estudo sobre o produto tensorial não abeliano de grupos e o produto exterior não abeliano de grupos. Veremos neste capítulo uma relação entre o quadrado exterior não abeliano de um grupo finito G e uma determinada extensão central de $M(G)$ por G conhecida como grupo de recobrimento total de G. Essa relação será fundamental no estudo de expoentes de multiplicador de Schur que será realizada no Capítulo 5.

No último capítulo apresentamos cotas superiores para expoentes de p-grupos finitos e de alguns termos da série central inferior, bem como suas aplicações na estimativa de expoente de multiplicador de Schur. Em especial apresentamos as demonstrações dos Teoremas A a D.

CAPÍTULO 1

PRELIMINARES

Neste capítulo vamos fixar algumas notações e terminologias, bem como apresentar os conceitos e resultados que serão utilizados no decorrer deste trabalho. Assumiremos que o leitor esteja familiarizado com os conceitos e resultados que usualmente fazem parte de um primeiro curso de Teoria dos Grupos, por isso, omitiremos as demonstrações.

Para cada $n \in \mathbb{N}^*$, vamos denotar o conjunto $\{1, \ldots, n\}$ por I_n.

Se G é um grupo e $H \subset G$, usaremos a notação $H \leq G$ quando H for subgrupo de G e $H \lhd G$ quando H for um subgrupo normal em G. Denotaremos o elemento neutro de um grupo por 1 quando não precisarmos especificar o conjunto em que estamos lidando.

Para um subconjunto X de G, escreveremos $\langle X \rangle$ para denotar o subgrupo gerado por X e X^G para indicar o *fecho normal* de X em G, isto é, $X^G = \langle \{g^{-1}xg \mid x \in X, g \in G\} \rangle$, o qual tem a propriedade de ser o "menor" subgrupo normal de G que contém X. Além disso, o centro de G será representado por $Z(G)$.

Nesta dissertação as funções serão aplicadas à direita, isto é, dada uma função $\varphi : A \to B$ a $a \in A$, denotaremos por $(a)\varphi$ a imagem de a por φ. Além disso, para todo $U \leq A$, temos $(U)\varphi = \{(u)\varphi \mid u \in U\}$.

Dados um grupo G e $H \leq G$, para cada $g \in G$ seja $gH = \{g \cdot h \mid h \in H\}$. Se $H \lhd G$, então teremos um grupo $G/H = \{gH \mid g \in G\}$ munido da operação $*$ em que $(g_1H) * (g_2H) = (g_1g_2)H$ para quaisquer $g_1, g_2 \in G$. Com isso, podemos definir um homomorfismo de grupos:

$$\begin{array}{rccc} \pi : & G & \longrightarrow & \frac{G}{H} \\ & g & \longmapsto & gH \end{array},$$

que será chamado de *homomorfismo canônico* .

Dados um grupo G e um subgrupo H de G, dizemos que H é *característico* em G, e denotamos H char G, se para todo automorfismo $\varphi : G \to G$, temos que $(H)\varphi = H$.

Uma demonstração da próxima proposição pode ser vista em [38, pág. 104].

Proposição 1.1. *Sejam G um grupo e H, K subgrupos de G com $H \leq K$. Então,*

(i) *Se H char G, então $H \triangleleft G$;*

(ii) *Se H char K e K char G, então H char G;*

(iii) *Se H char G e $K \triangleleft G$, então $H \triangleleft G$.*

Dados um grupo G e $n \in \mathbb{N}$, denotamos por G^n o subgrupo $\langle g^n \mid g \in G \rangle$ de G. Não é difícil ver que G^n char G.

1.1 Cálculos com Comutadores

Nessa dissertação, faremos muitos cálculos envolvendo comutadores e, portanto, precisaremos usar algumas identidades que serão apresentadas nesta seção.

Para cada grupo G, dados $g, h \in G$, o *conjugado* de g por h é o elemento $g^h \coloneqq h^{-1}gh$. Além disso, o *comutador*de g e h é $[g, h] \coloneqq g^{-1}h^{-1}gh$. Para $g_1, \ldots, g_n \in G$, o *comutador simples* de peso $n \geq 2$ é definido recursivamente por $[g_1] = g_1$ e $[g_1, \ldots, g_{n-1}, g_n] \coloneqq [[g_1, \ldots, g_{n-1}], g_n]$. Usaremos também a notação $[g, {}_n h]$ para indicar $[g, h, \ldots, h]$ em que o símbolo h aparece n vezes.

Importantes propriedades de comutadores que serão usadas futuramente são apresentadas na proposição a seguir. Suas provas são feitas através de cálculos simples e serão omitidas.

Proposição 1.2. *Dados um grupo G e x, y, z elementos de G, as seguintes identidades são válidas:*

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

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

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

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

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

(vi) $[x, y, z^x][z, x, y^z][y, z, x^y] = 1$ *(Identidade de Jacobi);*

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

Dado um grupo G, se H, K são subgrupos de G, o subgrupo $\langle [h,k] \mid h \in H, k \in K \rangle$ será denotado por $[H,K]$. Ainda mais, considerando agora $H_1, \ldots, H_n$ subgrupos de G, definimos recursivamente $[H_1] = H_1$ e $[H_1, \ldots, H_{n-1}, H_n] \coloneqq [[H_1, \ldots, H_{n-1}], H_n]$. Usaremos $[H, {}_nK]$ para representar o grupo $[H, K, \ldots, K]$ em que o símbolo K aparece n vezes.

O subgrupo comutador $[G,G]$ de um grupo G é chamado *subgrupo derivado* de G e denotado por G'.

Com esses conceitos, se mostra facilmente o próximo resultado.

Proposição 1.3. *Dado um grupo G, se $H, K \leq G$ e $N \triangleleft G$, então:*

$$\left[\frac{HN}{N}, \frac{KN}{N}\right] = \frac{[H,K]N}{N}.$$

Além disso, temos que $G' \leq H$ se, e somente se, H é normal em G e G/H é abeliano.

1.2 Grupos Solúveis e Nilpotentes

Nesta seção introduzimos duas classes de grupos que são muito importantes na Teoria dos Grupos, a saber, a classe dos grupos solúveis e a de grupos nilpotentes.

Um grupo G é *solúvel* caso exista uma cadeia finita de subgrupos normais de G:

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G,$$

tal que G_{i+1}/G_i é abeliano para todo $i = 0, 1, \cdots, n-1$. Uma cadeia que satisfaz tais propriedades é chamada *série solúvel*.

Claramente todo grupo abeliano G é solúvel, bastando apenas tomar a cadeia $\{1\} \triangleleft G$. O grupo simétrico S_3 é também solúvel pois $\{1\} \triangleleft A_3 \triangleleft S_3$ é uma cadeia solúvel.

Definimos a *série derivada* de G:

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(m)} \geq \ldots,$$

indutivamente, como segue:

$$G^{(i)} = \begin{cases} G & \text{, se } i = 0 \\ \left[G^{(i-1)}, G^{(i-1)}\right] & \text{, se } i > 0 \end{cases}.$$

Note que $G^{(i)}/G^{(i+1)}$ é abeliano para todo $i \in \mathbb{N}$. Além disso, $G^{(i)}$ char G, para todo $i \geq 0$. Veja que se $G^{(i)} = \{1\}$ para algum $i \in \mathbb{N}$, temos que a série derivada de G é uma série solúvel, e portanto, G é solúvel. É possível verificar que a recíproca dessa afirmação é verdadeira, isto é, G é um grupo solúvel se, e somente se, $G^{(i)} = \{1\}$ para

algum $i \in \mathbb{N}$.

Agora, estudaremos uma nova classe de grupos que será muito importante no decorrer dessa dissertação.

Um grupo G é *nilpotente* caso exista uma cadeia finita de subgrupos normais de G:

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G,$$

tal que $G_{i+1}/G_i \leq Z\left(G/G_i\right)$ para todo $i = 0, 1, \cdots, n-1$. Uma cadeia que satisfaz tais propriedades é chamada *série central*. Se G é um grupo nilpotente, a quantidade de grupos em uma menor série central de G é chamada *classe de nilpotência* de G.

Note que todo grupo abeliano não trivial é nilpotente de classe 1. Basta tomar a cadeia $\{1\} \triangleleft G$. Além disso, todo p-grupo finito é nilpotente. Uma demonstração desse fato pode ser vista em [36].

Vamos ver agora duas cadeias que nos auxiliam a analisar se um grupo é nilpotente.

Seja $\gamma_i(G)$, para $i = 1, 2, \cdots$, definido indutivamente por:

$$\gamma_i(G) = \begin{cases} G & \text{, se } i = 1 \\ [\gamma_{i-1}(G), G] & \text{, se } i > 1 \end{cases}.$$

Cada $\gamma_i(G)$ é um subgrupo característico de G e, portanto, normal em G e satisfaz $\gamma_i(G) \geq \gamma_{i+1}(G)$, para todo $i \in \mathbb{N}^*$. A cadeia:

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots \gamma_m(G) \geq \ldots$$

é chamada *série central inferior de* G.

Além disso, a *série central superior* de G:

$$\{1\} = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_m(G) \leq \ldots,$$

é definida, indutivamente, como segue:

$$Z_i(G) = \begin{cases} \{1\} & \text{, se } i = 0 \\ \pi_{i-1}^{-1}\left(Z\left(\dfrac{G}{Z_{i-1}(G)}\right)\right) & \text{, se } i > 0 \end{cases},$$

onde $\pi_{i-1} : G \to G/Z_{i-1}(G)$ é o homomorfismo canônico. Então, para quaisquer $x \in G$ e $i \in \mathbb{N}$, temos a equivalência:

$$x \in Z_{i+1}(G) \iff (\forall y \in G)([x, y] \in Z_i(G)). \tag{1.1}$$

Usando a equivalência (1.1) e indução, não é difícil provar o lema a seguir.

Lema 1.4. *Sejam G um grupo e $i \in \mathbb{N}$. Se $g \in Z_i(G)$, então $[g, {}_j y] \in Z_{i-j}(G)$ para todo $y \in G$*

e $j \in \mathbb{N}$ *com* $j \leq i$. *Consequentemente,* $[g, {}_{i_1}a_1, {}_{i_2}a_2, \ldots, {}_{i_n}a_n] = 1$ *para todos* $g \in Z_i(G)$, $a_1, \ldots, a_n \in G$ *e* $i_1, \ldots, i_n \in \mathbb{N}$ *com* $i_1 + \cdots + i_n \geq i$.

É um resultado bem conhecido que um grupo G é nilpotente se, e somente se, existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$. Isso é equivalente a $\gamma_{n+1}(G) = \{1\}$. É possível também mostrar que a classe de nilpotência de G é o menor natural n tal que $\gamma_{n+1}(G) = \{1\}$ e $Z_n(G) = \{G\}$ (Veja, por exemplo, [36, pág. 125]).

Veremos no próximo resultado, que a partir de um grupo G, podemos obter outros grupos nilpotentes. Uma prova disto pode ser encontrada em [38].

Proposição 1.5. *Seja* G *um grupo nilpotente de classe* c. *Todo subgrupo* J *de* G *é nilpotente. Além disso, dado um subgrupo normal* H *de* G, *temos que* G/H *é nilpotente. Ainda mais,* J *e* G/H *tem classe de nilpotência no máximo* c.

Uma característica para grupos nilpotentes de classe no máximo 2 é dada a seguir.

Proposição 1.6. *Dado um grupo nilpotente* G *de classe no máximo* 2, *para quaisquer* $g, h, x \in G$ *e* $n \in \mathbb{N}$, *temos:*

(i) $[g, hx] = [g, h][g, x]$ *e* $[gx, h] = [g, h][x, h]$;

(ii) $[g, h^n] = [g, h]^n = [g^n, h]$;

(iii) $hg^n = g^n h[h, g]^n$;

(iv) $(gh)^n = g^n h^n [h, g]^{\frac{n(n-1)}{2}}$.

Demonstração.

(i) Note que, como $\gamma_2(G) \leq Z(G)$, temos:

$$[g, hx] = [g, x][g, h]^x = [g, x][g, h] = [g, h][g, x].$$

De modo análogo, mostramos a outra igualdade.

(ii) Segue de (i) por indução sobre k.

(iii) De (ii), temos $hg^n = g^n h[h, g^n] = g^n h[h, g]^n$.

(iv) Provaremos este item por indução sobre n. Para $n = 0$, é óbvio. Agora, assuma que o resultado é válido para um certo $n \in \mathbb{N}$. Com isso, usando o item (iii) e o fato que $G' \leq Z(G)$, temos:

$$(gh)^{n+1} = (gh)(gh)^n = g(hg^n)h^n[h, g]^{\frac{n(n-1)}{2}}$$

$$= gg^n hh^n [h,g]^n [h,g]^{\frac{n(n-1)}{2}} = g^{n+1} h^{n+1} [h,g]^{\frac{n(n+1)}{2}},$$

provando o desejado.

□

Dado $H \leq G$ com $[H,G] = H$, se prova por uma indução simples que $H \leq \gamma_i(G)$ para todo $i \in \mathbb{N}^*$. Uma consequência imediata deste fato é a proposição a seguir.

Proposição 1.7. *Se G é um grupo nilpotente e H é um subgrupo normal de G tal que $[H,G] = H$, então $H = \{1\}$.*

O resultado a seguir fornece um conjunto de geradores para $\gamma_i(G)$ a partir de um conjunto gerador de G. Uma demonstração de tal pode ser vista em [37, pág. 18].

Proposição 1.8. *Se um grupo G é gerado por um conjunto X, então $\gamma_i(G)$ é gerado pelos conjugados de comutadores simples de elementos de X com peso i, isto é,*

$$\gamma_i(G) = \langle [x_1, \ldots, x_i]^g \,|\, x_j \in X, j = 1, \ldots, i, g \in G \rangle .$$

Graças à Identidade de Witt-Hall, se prova facilmente o próximo resultado.

Proposição 1.9 (Lema dos Três Subgrupos)**.** *[36, 5.1.10, pág. 126] Sejam A, B e C subgrupos de um grupo G e N um subgrupo normal de G. Se $[A,B,C] \leq N$ e $[B,C,A] \leq N$, então $[C,A,B] \leq N$.*

Este resultado nos permite provar a seguinte proposição, que nos traz uma importante propriedade dos subgrupos $\gamma_i(G)$ de um grupo G.

Proposição 1.10. *Dado um grupo G, para todo $i, j \in \mathbb{N}^*$, temos que $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. Mais geralmente se $i_1, \ldots, i_n \in \mathbb{N}^*$, então $[\gamma_{i_1}(G), \ldots, \gamma_{i_n}(G)] \leq \gamma_{i_1+\cdots+i_n}(G)$.*

Ideia da demonstração. Vamos escrever $G_j = \{g \in G \mid [g, \gamma_i(G)] \leq \gamma_{i+j}(G), \forall i \in \mathbb{N}^*\}$ para cada $j \in \mathbb{N}^*$. Não é difícil ver que $G_j \leq G$. Dados $i, j, m \in \mathbb{N}$, cálculos simples nos mostram que:

$$[G_j, \gamma_i(G), G_m] \leq \gamma_{i+j+m}(G) \quad \text{e} \quad [\gamma_i(G), G_m, G_j] \leq \gamma_{i+j+m}(G).$$

Pelo Lema dos Três Subgrupos, temos $[G_m, G_j, \gamma_i(G)] \leq \gamma_{i+j+m}(G)$, para todo $i \in \mathbb{N}$, o que implica em $[G_j, G_m] \leq G_{j+m}$. Usando que $G_1 = G$, uma indução natural nos diz que $\gamma_i(G) \leq G_i$ para cada $i \in \mathbb{N}^*$. Logo, temos o desejado. □

Como consequência imediata das Proposições 1.8 e 1.10, segue:

Proposição 1.11. *Dados um grupo G, $x \in G$ e $i \in \mathbb{N}$ com $n \geq 2$, se $H = \langle x, G' \rangle$, então $\gamma_i(H) \leq \gamma_{i+1}(G)$.*

Outra importante propriedade dos termos da série central inferior é apresentada no próximo resultado, cuja demonstração pode ser encontrada em [37, pág. 16].

Proposição 1.12. *Dados um grupo G e $i, j \in \mathbb{N}^*$, temos que $\gamma_i(\gamma_j(G)) \leq \gamma_{i \cdot j}(G)$.*

1.3 Apresentação de Grupo

Nesse trabalho, alguns grupos serão definidos pelas suas apresentações. Portanto, o objetivo dessa seção é apresentar o conceito de grupos livres e apresentação de grupos, bem como alguns de seus resultados importantes.

Definição 1.13. Dados um grupo F e um subconjunto $X \subset F$, dizemos que F é um *grupo livre* sobre X se, para qualquer função $\theta : X \to G$, existe um único homomorfismo $\theta' : F \to G$ tal que $(x)\theta = (x)\theta'$ para todo $x \in X$.

É possível mostrar que se F é um grupo livre sobre $X \subset F$, então $F = \langle X \rangle$, como pode ser visto em [20, pág. 3]. A proposição a seguir nos mostra a importância de estudar tais grupos.

Proposição 1.14. *[20, pág. 7] Todo grupo é imagem homomórfica de algum grupo livre.*

Assim, consideremos G um grupo e $\varphi : F \to G$ um homomorfismo sobrejetor, em que F é um grupo livre sobre $X \subset F$. Então $G \cong F/N$ se considerarmos $N = Ker(\varphi)$. Tome $R \subset F$ de modo que $R^F = N$. Neste caso, escrevemos $G = \langle X \mid R \rangle$ e chamamos essa escrita de *apresentação livre* de G.

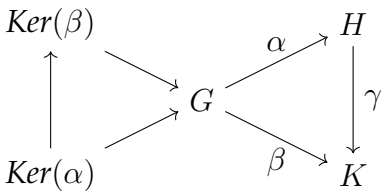
Caso X e R sejam finitos, dizemos que G é finitamente apresentado. O elementos de X são chamados de *geradores*, enquanto que os de R são *relatores*. É comum substituir R em $\langle X \mid R \rangle$, pelo conjunto de equações $R = 1$, isto é, $\{r = 1 \mid r \in R\}$. Este conjunto é chamado de conjunto de *relações definidoras* de G. Uma relação definidora pode assumir a forma "$u = v$"correspondente ao relator uv^{-1} e também à relação definidora $uv^{-1} = 1$. Por exemplo, tomando D_8 o grupo diedral de ordem 8, temos:

$$\begin{aligned} D_8 &= \left\langle \alpha, \beta \mid \alpha^4, \beta^2, \beta\alpha\beta\alpha \right\rangle \\ &= \left\langle \alpha, \beta \mid \alpha^4 = \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} \right\rangle \\ &= \left\langle a, b, c \mid a^2, c^2, b^2c^{-1}, c^{-1}a^{-1}ca, c^{-1}b^{-1}cb, b^{-1}a^{-1}bac^{-1} \right\rangle. \end{aligned}$$

Veja que isto também prova que a apresentação de um grupo não é única.

O resultado a seguir, é usado na demonstração do Teste da Substituição que apresentaremos mais adiante. Porém, por aplicarmos ele futuramente, trazemos seu enunciado nessa seção. Sua demonstração pode ser encontrada em [21, pág. 42].

Teorema 1.15. *Se G, H, K são grupos, $\alpha : G \longrightarrow H$ um epimorfismo e $\beta : G \longrightarrow K$ um homomorfismo tais que $Ker(\alpha) \leq Ker(\beta)$, então existe um homomorfismo $\gamma : H \longrightarrow K$ tal que $\alpha \circ \gamma = \beta$.*



Dada uma apresentação $G = \langle X \mid R \rangle$, uma função de X em um grupo H pode ser estendida para um homomorfismo de G em H? O resultado a seguir nos fornece uma condição necessária e suficiente para que isso ocorra.

Teorema 1.16 (Teste da Substituição)**.** *[20, Theorem 4, pág. 29] Sejam G um grupo com apresentação $\langle X \mid R \rangle$, H um grupo e $\theta : X \to H$ uma aplicação. Então, θ se estende a um homomorfismo $\theta' : G \to H$ se, e somente se, θ é consistente com todas as relações definidoras para G, isto é, se para todo $x \in X$ e $r \in R$, o resultado da substituição de x por $(x)\theta$ em R é a identidade de H.*

Dados dois grupos G e H com apresentações $\langle X \mid R \rangle$ e $\langle Y \mid S \rangle$, respectivamente, o *produto livre* de G e H é o grupo $G * H = \langle X \cup Y \mid R \cup S \rangle$. Assim, dados homomorfismos $\alpha : G \to J$ e $\beta : H \to J$, existe um único homomorfismo $\gamma : G * H \to J$ tal que $(g)\gamma = (g)\alpha$ e $(h)\gamma = (h)\beta$ para todos $g \in G$ e $h \in H$.

1.4 Sequências Exatas

Dados um grupo G e K um subgrupo normal de G, é possível provar que se K e G/K são p-grupos finitos, o mesmo pode-se dizer de G. O mesmo vale para grupos finitos, grupos solúveis e grupos periódicos. Com base nisso, trazemos a próxima definição e estudaremos um pouco sequências exatas curtas.

Definição 1.17. Uma sequência de grupos e homomorfismos

$$\cdots \longrightarrow G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} \cdots$$

é *exata* em G_n se $Im(f_{n-1}) = Ker(f_n)$. Dizemos que a sequência é *exata* se for exata em todo G_n.

Uma sequência exata da forma:

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\rho} Q \longrightarrow 1$$

é chamada de *sequência exata curta*. Neste caso, temos as seguintes propriedades:

(i) i é injetora e ρ é sobrejetora;

(ii) $Ker(\rho) = Im(i)$;

(iii) $\frac{G}{Ker(\rho)} \cong Im(\rho) = Q$, onde $Ker(\rho) \cong K$.

Além disso, uma sequência exata curta é dita *central* se $Im(i) \leq Z(G)$.

Agora, dados dois grupos K e G, vamos definir uma extensão de K por Q.

Definição 1.18. Sejam K e Q grupos. Uma *extensão* de K por Q é uma sequência exata curta da forma:

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\rho} Q \longrightarrow 1.$$

Neste caso, também dizemos que o grupo G é uma extensão de K por Q.

Notemos que duas extensões G_1 e G_2 de K por Q não precisam ser isomorfas. De fato, consideremos os grupos: S_3 e $\mathbb{Z}_6$. Não é difícil ver que tais grupos são extensões de $\mathbb{Z}_3$ por $\mathbb{Z}_2$ e claramente não são isomorfos. Também temos que se K é um subgrupo normal de um grupo G, então G é uma extensão de K por G/K.

Uma aplicação do conceito de sequência exatas é vista no lema a seguir.

Lema 1.19 (Lema dos Cinco)**.** *[36, pág. 421] Considere o seguinte diagrama comutativo:*

$$\begin{array}{ccccccccc} X_1 & \xrightarrow{\varphi_1} & X_2 & \xrightarrow{\varphi_2} & X_3 & \xrightarrow{\varphi_3} & X_4 & \xrightarrow{\varphi_4} & X_5 \\ \downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta_2} & & \downarrow{\scriptstyle \theta_3} & & \downarrow{\scriptstyle \theta_4} & & \downarrow{\scriptstyle \theta_5} \\ Y_1 & \xrightarrow{\psi_1} & Y_2 & \xrightarrow{\psi_2} & Y_3 & \xrightarrow{\psi_3} & Y_4 & \xrightarrow{\psi_4} & Y_5 \end{array},$$

em que cada linha é uma sequência exata de grupos e cada função é um homomorfismo. Se θ_1 é um epimorfismo, θ_5 é um monomorfismo e θ_2, θ_4 são isomorfismos, então θ_3 é um isomorfismo.

1.5 Multiplicador de Schur

Nesta seção apresentaremos algumas propriedades do multiplicador de Schur de um grupo G. Este grupo foi introduzido por Schur [40] para estudar representação projetiva de grupos.

Dado um grupo finito G, o multiplicador de Schur de G é o segundo grupo de cohomologia de G com coeficientes complexos e uma ação trivial de G. Porém, também pode ser definido como segue:

Definição 1.20. *Dado um grupo finito G, sejam F um grupo livre, $\varphi : F \to G$ um epimorfismo e R o núcleo de φ. Então, o multiplicador de Schur de G, denotado por $M(G)$, é o grupo:*

$$\frac{F' \cap R}{[F, R]}.$$

A equivalência entre as definições pode ser vista em [23]. O livro [38] traz alguns resultados sobre o multiplicador de Schur de um grupo G. Apresentamos a seguir dois destes.

Teorema 1.21. *Se Q é um grupo finito, então $M(Q)$ é um grupo finito abeliano e $exp(M(Q))$ divide $|Q|$.*

Corolário 1.22. *Se Q é um p-grupo finito, então $M(Q)$ é um p-grupo finito abeliano.*

Estamos agora interessados em um tipo especial de extensão central que será útil na obtenção de algumas propriedades importantes do produto exterior não abeliano de grupos, que veremos no Capítulo 4.

Definição 1.23. Dado um grupo Q, um grupo U que possui um subgrupo K tal que $K \leq Z(U) \cap U'$ e $U/K \cong Q$ é chamado um *grupo de recobrimento* de Q. Se, além disso, $K \cong M(Q)$, dizemos que U é um *grupo de recobrimento total* de Q.

Seja V o grupo de Klein. Em [38, Corollary 11.23] vemos que $M(V) \cong \mathbb{Z}_2$. Assim, se tomarmos U como sendo o grupo dos quatérnios Q ou o grupo diedral D_8, temos que U é um grupo de recobrimento de V. Porém, Q não é isomorfo à D_8. Isto prova que para um grupo Q, o grupo de recobrimento não é necessariamente único. Porém, se Q for finito e $Q' = Q$, o resultado [38, Corollary 11.12] nos diz que existe apenas um grupo de recobrimento de Q.

Teorema 1.24 (Schur, 1904)**.** *Todo grupo finito Q possui um grupo de recobrimento total.*

A partir da proposição a seguir, obtemos uma característica de um grupo de recobrimento U de Q quando Q é nilpotente.

Proposição 1.25. *Dados um grupo G e H um subgrupo central de G, se G/H é nilpotente de classe c, então G é nilpotente de classe no mínimo c e no máximo $c + 1$.*

Fonte da demonstração. Ver [35, pág. 46]. □

CAPÍTULO 2

PROCESSO DE COLETA

Dados um grupo G e $a, b \in G$, temos a identidade $ba = ab[b, a]$. Digamos que para $a_1, a_2, b_1, b_2 \in G$, tenhamos a expressão $a_1b_1a_2b_2$. Vamos usar a identidade acima para obter $a_1b_1a_2b_2 = a_1a_2b_1b_2c$, onde $c \in G$. Veja que:

$$a_1(b_1a_2)b_2 = a_1(a_2b_1[b_1, a_2])b_2 = a_1a_2b_1([b_1, a_2]b_2) = a_1a_2b_1b_2[b_1, a_2][[b_1, a_2], b_2].$$

Obtemos assim o desejado, bastando apenas tomar $c = [b_1, a_2][[b_1, a_2], b_2]$. Este processo é chamado *processo de coleta* e será amplamente usado nesta seção.

Dado um grupo G e $r \in \mathbb{N}^*$, vamos denotar por $C_r(G)$ o produto direto $G \times \cdots \times G$, em que que o termo G aparece r vezes. Usando indução simples podemos mostrar que a função:

$$\begin{array}{rccc} \alpha_r : & C_r(G) & \longrightarrow & \frac{G}{\gamma_{r+1}(G)} \\ & (g_1, \ldots, g_r) & \longmapsto & [g_1, \ldots, g_r]\,\gamma_{r+1}(G) \end{array},$$

é multilinear. Isso nos diz que qualquer comutador de peso r é multilinear, módulo $\gamma_{r+1}(G)$, ou seja,

$$[g_1, \ldots, g_ih_i, \ldots, g_r] \equiv [g_1, \ldots, g_i, \ldots g_r][g_1, \ldots, h_i, \ldots, g_r] \pmod{\gamma_{r+1}(G)},\ i = 1, \ldots, r.$$

Aqui, dado um subconjunto X de um grupo F, um *comutador formal* em X é um comutador que pode ser escrito por elementos de X. Por exemplo, para $x_1, x_2, x_3, x_4 \in X$, os elementos x_1, $[x_1, x_2, x_3, x_4]$ e $[x_1, [x_2, x_3], x_4]$ são comutadores formais em X. Desconsideramos aqui os comutadores triviais, como $[x_2, x_2]$ e $[x_3, [x_1, x_1]]$. Seja F um grupo livre de base X. Não é difícil ver que os comutadores formais de elementos de X são escritos de forma única.

Definição 2.1. Dado um grupo livre F sobre um conjunto ordenado X, os *comutadores formais básicos* em X, seus *pesos* e uma ordem $<$ nesses elementos são definidos indutivamente:

(i) Os elementos de X são comutadores formais básicos, possuem peso 1 e a ordem

segue a relação ordenada já definida em X;

(ii) Se os comutadores formais básicos de peso menor que n já foram definidos e ordenados, então $[u, v]$ é um comutador formal básico de peso n se:

- u e v são comutadores formais básicos e a soma dos pesos de u e v é n;
- $v < u$;
- Se $u = [r, s]$ com r e s comutadores formais básicos, então $s \leq v$.

Os comutadores formais básicos de peso n são maiores que os de peso menor que n. Dados $u = [w, a]$ e $v = [z, b]$ comutadores formais básicos de peso n, temos que $u < v$ se $w < z$ ou $w = z$ e $a < b$.

Denotaremos por $Y(X)$ o conjunto composto por todos os comutadores formais básicos. Para todo $g \in Y(X)$, representaremos o seu peso por $\omega(g)$.

Dado $n \in \mathbb{N}$, escrevamos $X = \{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ e consideramos a ordem em X definida por:

$$x_i < y_j, x_i < x_k, y_i < y_k, \text{ para quaisquer } i, j, k \in I_n \text{ com } i < k.$$

Assim, pelo conceito de peso definido,

$$\omega([x_1, x_2, x_3]) = \omega([x_1, x_2]) + \omega(x_3) = \omega(x_1) + \omega(x_2) + \omega(x_3) = 3.$$

Analogamente, $\omega([[x_1, x_2, x_3], [x_4, x_5]]) = 5$ e $\omega([[x_1, x_3], [x_2, x_4]]) = 4$.

Veja que $[x_1, x_2, x_3] > [x_4, x_5]$ pois $\omega([[x_1, x_2], x_3]) = 3$ e $\omega([x_4, x_5]) = 2$. Além disso, $[[x_1, x_2, x_3], [x_4, x_5]] < [[x_1, x_2, x_3, x_4], x_5]$ uma vez que $\omega([[x_1, x_2, x_3], [x_4, x_5]]) = 5 = \omega([[x_1, x_2, x_3, x_4], x_5])$ e $[x_1, x_2, x_3] < [x_1, x_2, x_3, x_4]$.

Sendo Z o conjunto dos comutadores formais de X, é fácil ver que Z é enumerável e $Y(X) \subset Z$. Agora, dada uma permutação $\varphi : I_n \to I_n$, podemos induzir uma permutação $\alpha_\varphi : Z \to Z$ em que, para $u \in Z$, temos que $(u)\alpha_\varphi$ tem a mesma estrutura que u mas com os índices trocados segundo φ. Por exemplo, tome $\varphi = (3\ 4)$ e $u = [x_1, y_2, x_3, y_4]$. Então:

$$(u)\alpha_\varphi = \left[x_{(1)\varphi}, y_{(2)\varphi}, x_{(3)\varphi}, y_{(4)\varphi}\right] = [x_1, y_2, x_4, y_3]\,.$$

Dado $u \in Y(X)$, dizemos que φ é *compatível* em relação à $u \in Y(X)$ se, ao aplicarmos φ aos índices dos elementos na escrita de u, a ordem desses índices é mantida, isto é, considerando o conjunto I composto pelos índices presentes na escrita de u, temos que $\varphi|_I$ é crescente. Assim, se $u \in Y(X)$ e φ é compatível com u, então $(u)\alpha_\varphi \in Y(X)$.

Por exemplo, para $\varphi = (1\ 2\ 3)$, se tomarmos $u = [y_1, x_3]$, os índices pertencentes a escrita de u são 1 e 3, cuja ordem é alterada por φ, já que $1 < 3$ mas $(1)\varphi > (3)\varphi$. Agora, caso tomemos $v = [x_4, x_1, y_5]$, os índices na escrita de v são 1, 4 e 5, cuja ordem é mantida por φ pois $1 < 4 < 5$ e $(1)\varphi < (4)\varphi < (5)\varphi$. Portanto, φ é compatível com v mas não é compatível com u.

Para elementos $\varphi \in S_n$, dizemos que φ é compatível com um número finito de elementos $u_1, \ldots, u_n \in Y(X)$ se φ não altera a ordem entre os índices de todos os elementos na escrita desses elementos. Por exemplo, tomemos a permutação $\varphi = (1\ 2)$. Se $u = [x_3, x_1]$ e $v = [x_2, x_4, x_5]$, os índices na escrita desses elementos são 1, 3 , 2, 4 e 5. A permutação φ não mantém a ordem desses índices, mais especificamente entre 1 e 2. Logo, φ não é compatível com u e v. Porém, tomando $r = [x_4, x_5, x_6]$, temos que φ é compatível com u e r, pois a ordem de 1, 3, 4, 5 e 6 é mantida.

É fácil ver que dados $u, v \in Y(X)$ com $u < v$ e $\varphi \in S_n$ compatível com u e v, então $(u)\alpha_\varphi < (v)\alpha_\varphi$. Tome por exemplo $u = [x_2, x_1]$ e $v = [x_3, x_1]$. Temos então que $\varphi = (2\ 3\ 4)$ é compatível com u e v. Assim, veja que $(u)\alpha_\varphi = [x_3, x_1]$ e $(v)\alpha_\varphi = [x_4, x_1]$. Com isso $v > u$ e $(v)\alpha_\varphi > (u)\alpha_\varphi$.

Seja $L(F)$ o fecho normal em F do conjunto de comutadores formais em X de peso no mínimo $n + 1$.

Para $n = 2$, tomando a expressão $x_1y_1x_2y_2$, pelos cálculos mostrados no início deste capítulo, teremos que:

$$x_1y_1x_2y_2 \equiv c_1c_2 \cdots c_m \pmod{L(F)},$$

para algum $m \in \mathbb{N}$, em que $c_1, \ldots, c_m \in Y(X)$ e estão escritos na ordem crescente segundo $<$. Para isso, basta tomar $m = 5$, $c_1 = x_1$, $c_2 = x_2$, $c_3 = y_1$, $c_4 = y_2$ e $c_5 = [y_1, x_2]$. Observe que não incluímos $[y_1, x_2, y_2]$ pois pertence a $L(F)$.

Fazendo esse mesmo processo para $n = 3$ e considerando a congruência módulo $L(F)$, obtemos:

$$\begin{aligned} x_1y_1x_2y_2x_3y_3 \equiv x_1x_2x_3y_1y_2y_3[y_1, x_2][y_1, x_3][y_2, x_3][y_1, x_2, x_3][y_1, x_2, y_2] \\ [y_1, x_2, y_3][y_1, x_3, y_2][y_1, x_3, y_3][y_2, x_3, y_3]. \end{aligned} \tag{2.1}$$

Observe que comutadores como $[[y_1, x_3], [y_1, x_2]]$ não estão na expressão pois pertencem a $L(F)$. Assim, temos um elemento congruente a $x_1y_1x_2y_2x_3y_3$, módulo $L(F)$, em que aparecem somente termos de $Y(X)$ e estão escritos na ordem crescente segundo a relação $<$.

Veja também que se tomarmos $u = [y_1, x_2]$, as únicas permutações em S_3 compatíveis

com u são $\varphi = Id$ (função identidade), $\psi = (1\ 2\ 3)$ e $\gamma = (2\ 3)$. Com isso, $(u)\alpha_\varphi = [y_1, x_2]$, $(u)\alpha_\psi = [y_2, x_3]$ e $(u)\alpha_\gamma = [y_1, x_3]$. Note que $(u)\alpha_\varphi$, $(u)\alpha_\psi$ e $(u)\alpha_\gamma$ pertencem a expressão obtida. Veremos a seguir que essa propriedade está presente em toda expressão obtida pelo processo de coleta.

Lema 2.2. *Nas descrições feitas acima, temos:*

$$x_1y_1 \cdots x_ny_n \equiv c_1c_2 \cdots c_m \pmod{L(F)}, \tag{2.2}$$

para algum $m \in \mathbb{N}$, em que $c_1, \ldots, c_m \in Y(X)$ e estão escritos na ordem crescente segundo a relação de ordem $<$. Além disso, se $u = c_i \in Y(X)$, para algum $i \in I_m$, e $\varphi \in S_n$ é compatível com u, então $(u)\alpha_\varphi = c_j$ para algum $j \in I_m$.

Demonstração. Vamos dividir a demonstração em três passos.

Passo 1: Primeiro vamos mostrar a congruência (2.2).

Para $n = 1$ é simples, já que x_1y_1 satisfaz o desejado. Então, supomos que $n > 1$. Aqui realizaremos o processo de coleta. Ou seja, estaremos reorganizando os elementos na decomposição obtida utilizando a identidade $ba = ab[b, a]$, para $a, b \in F$.

No primeiro passo, temos a expressão $x_1y_1x_2y_2 \cdots x_ny_n$, que será igual a:

$$x_1x_2y_1[y_1, x_2]y_2x_3y_3 \cdots x_ny_n.$$

Repetimos esse procedimento indutivamente, reorganizando os elementos de acordo com a ordem $>$. Note que o momento em que trocamos ba por $ab[b, a]$, foi realizada a coleta de a, com $a < b$.

Dessa forma, se $u, v \in Y(X)$ e realizamos o processo de coleta no qual surge o comutador $[u, v]$, isso significa que $u > v$. Além disso, se u tem a forma $[r, s] \in Y(X)$, então ele surgiu quando coletamos s, o que deve ter ocorrido antes de fazermos a troca de uv por $vu[u, v]$, ou seja, $s \leq v$, pois caso contrário, ainda não teríamos coletado s, e então u não estaria na expressão quando coletamos v. Assim, ocorreu como mostra a tabela a seguir.

Momento	Expressão
Antes da coleta de s	$\cdots r \cdots s \cdots v$
Coleta de s	$\cdots s \cdot r \cdot u \cdots v$
Coleta de v	$\cdots v \cdot u \cdot [u, v] \cdots$

Utilizaremos tabelas como essa para ilustrar o processo de coleta durante essa demonstração.

Assim, como os elementos da expressão inicial pertencem a $Y(X)$ e quando esse processo continua, só surgem elementos de $Y(X)$, mostramos que durante todo o procedimento, estamos trabalhando com elementos de $Y(X)$.

Repetimos o processo de coleta até que tenhamos passado por todos os elementos de peso até n. Assim, os elementos que não foram coletados serão comutadores formais básicos de peso maior que n, ou seja, estarão em $L(F)$.

Assim, considerando o módulo sobre $L(F)$, teremos que $x_1y_1 \cdots x_ny_n \equiv c_1c_2 \cdots c_m$ para algum $m \in \mathbb{N}$, em que $c_1, \ldots, c_m \in Y(X)$ e estão escritos na ordem crescente segundo $<$.

Agora, temos de provar que essa expressão satisfaz a segunda parte do enunciado.

Vamos separar o processo de coleta feito em etapas. Assim, para cada $i \in I_n$, a etapa i é quando coletamos todos os comutadores formais de peso i. Consideramos aqui como etapa 0 quando tomamos a expressão inicial. Assim, nosso processo teve $n+1$ etapas. O enunciado é obviamente válido para $i = 0$.

Passo 2: Vamos provar a seguinte afirmação:

Para $i \in \{0, \ldots, n\}$, ao fim da etapa i, para cada par de comutadores $u, v \in Y(X)$ na expressão obtida e $\varphi \in S_n$ compatível com u e v, se aparecem $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$ na expressão, então u e v têm a mesma posição relativa de $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$.

Veja que o afirmado vale na expressão inicial, ou seja, temos o desejado para $i = 0$. Assuma agora que para algum $i \in \{1, \ldots, n\}$, vale a afirmação para a etapa $i-1$ e vamos provar que o mesmo ocorre para a etapa i.

Sejam $u, v \in Y(X)$ que aparecem na expressão ao fim da etapa i e $\varphi \in S_n$ compatível com u e v tal que $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$ também aparecem na expressão. Vamos analisar três casos.

Caso 1: $\omega(u) \leq i$ e $\omega(v) \leq i$.

Neste caso, u, v, $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$ já terão sido coletados e, portanto, estarão respeitando a ordem $<$.

Caso 2: $\omega(u) > i$ e $\omega(v) \leq i$ ou $\omega(v) > i$ e $\omega(u) \leq i$.

Se $\omega(v) > i$ e $\omega(u) \leq i$, então u e $(u)\alpha_\varphi$ terão sido coletados, mas o mesmo não se diz de v e $(v)\alpha_\varphi$. Portanto, ao fim da etapa i, os comutadores u e $(u)\alpha_\varphi$ estarão à esquerda de v e $(v)\alpha_\varphi$. A análise para o caso $\omega(u) > i$ e $\omega(v) \leq i$ é análoga.

Caso 3: $\omega(u) > i$ e $\omega(v) > i$

Temos que $u = [w, a]$ e $v = [z, b]$ para $w, z, a, b \in Y(X)$, pois o peso de u e v é maior

que $i \geq 1$. Vamos dividir a análise desse caso em dois subcasos:

Caso 3.1: u e v já estavam na expressão ao fim da etapa $i-1$.

Então, $u = [w, a]$ e $v = [z, b]$ foram criados quando coletamos a e b com pesos menores ou iguais a $i-1$. Assim, já que $(u)\alpha_\varphi = [(w)\alpha_\varphi, (a)\alpha_\varphi]$ aparece na expressão ao fim da etapa i, ele foi criado na mesma etapa que u. Analogamente, $(v)\alpha_\varphi$ foi criado na mesma etapa que v. Portanto, $u, v, (u)\alpha_\varphi, (v)\alpha_\varphi$ já estavam na expressão ao fim da etapa $i-1$. Como não os coletamos na etapa i, suas posições relativas não se alteraram e, portanto, pela hipótese de indução, temos o desejado. Isso é ilustrado na tabela a seguir.

Momento	Expressão
Antes da coleta de a	$w \cdots a \cdots z \cdots b \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de a	$a \cdot w \cdot u \cdots z \cdots b \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$u \cdots z \cdots b \cdots (a)\alpha_\varphi \cdot (w)\alpha_\varphi \cdot (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de b	$u \cdots b \cdot z \cdot v \cdots (a)\alpha_\varphi \cdot (w)\alpha_\varphi \cdot (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$u \cdots v \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi$
Fim da etapa $i-1$	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$

Caso 3.2: u ou v foram criados na etapa i.

Digamos que v foi criado nessa etapa. Sendo k a soma dos pesos de u e v, vamos mostrar o desejado por indução sobre $k \in \mathbb{N}^*$.

Para $k \leq 2i+1$, já mostramos que se o peso de u ou v for menor ou igual a i temos o que queremos. Agora, tomemos $k \in \mathbb{N}^*$, com $k > 2i+1$, tal que o resultado é válido para todo natural menor que k. Temos os seguintes casos:

Caso 3.2.1: u não foi gerado na etapa i.

Como $v \in Y(X)$ e surgiu na etapa i, ele é da forma $[z, b]$ com $z, b \in Y(X)$, $z > b$ e b de peso i. Veja que z e $(z)\alpha_\varphi$ foram criados na mesma etapa.

• Se z e $(z)\alpha_\varphi$ foram criados antes da etapa i, temos que z e b apareciam na expressão ao fim da etapa $i-1$. Suponhamos sem perda de generalidade, que u estava à esquerda de z quando iniciamos a etapa i. Assim, como coletamos b antes de z (se z for coletado), temos que $v = [z, b]$ foi criado imediatamente à direita de z, ou seja, v foi criado à direita de u. Como não coletamos nenhum dos dois nesta etapa, u continuou à esquerda de v até o fim da etapa i. Veja que, como $(z)\alpha_\varphi$ aparecia ao fim da etapa $i-1$, pela hipótese de indução, ao fim da etapa $i-1$, $(u)\alpha_\varphi$ estava à esquerda de $(z)\alpha_\varphi$. Aplicando um raciocínio análogo, concluímos que $(u)\alpha_\varphi$ está à esquerda de $(v)\alpha_\varphi$ até o fim da etapa i.

Esse caso é ilustrado pela tabela a seguir.

Momento	Expressão
Começo da etapa i	$u \cdots z \cdots b \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de b	$u \cdots b \cdot zv \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$u \cdots v \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$

• Agora, digamos que z e $(z)\alpha_\varphi$ surgiram na etapa i. Pela hipótese de indução, u e z possuem a mesma posição relativa que $(u)\alpha_\varphi$ e $(z)\alpha_\varphi$ ao fim da etapa i. Como os pesos de u, $(u)\alpha_\varphi$, z e $(z)\alpha_\varphi$ são maiores que i, eles não foram coletados nesta etapa. Suponhamos que u finalizou a etapa i à esquerda de z e, então, assim estava desde a criação de z. Da mesma forma, $(u)\alpha_\varphi$ estava então à esquerda de $(z)\alpha_\varphi$. Quando coletamos b, criamos $v = [z, b]$ imediatamente à direita de z e, portanto, à direita de u. Analogamente, $(v)\alpha_\varphi$ estará à direita de $(u)\alpha_\varphi$ ao fim da etapa i. Assim, provamos o que queríamos quando v foi criado na etapa i mas u não. Para auxiliar o leitor, trazemos a próxima tabela ilustrando este caso.

Momento	Expressão
Começo da etapa i	$u \cdots b \cdots (u)\alpha_\varphi \cdots \alpha_\varphi(b)$
Criação de z	$u \cdots z \cdots b \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi$
Criação de $(z)\alpha_\varphi$	$u \cdots z \cdots b \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de b	$u \cdots b \cdot z \cdot v \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$b \cdots u \cdots v \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$

Caso 3.2.2: u e v foram criados na etapa i.

Portanto, $u = [w, a]$ e $v = [z, b]$, com $w > a$, $z > b$, além de que a e b possuem peso i. Notemos que, como $w > a$ e $z > b$, os pesos de w e z são maiores ou iguais a i. Podemos supor ainda que $a \leq b$. Vamos separar esse estudo em três subcasos.

Subcaso 1: $a = b$.

• Se z e w foram criados antes da etapa i, então, ao iniciar a etapa i, a posição relativa de z e w é a mesma que $(z)\alpha_\varphi$ e $(w)\alpha_\varphi$. Como $a < w$ e $a < z$, ao coletarmos a, não coletamos ainda w e z. Portanto, $u = [w, a]$ e $v = [z, a]$ ficarão com a mesma posição relativa que a posição relativa inicial de w e z. Essa posição relativa não será alterada nesta etapa, pois não coletaremos u nem v. Analogamente, $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$ ficarão com as

mesma posições relativas que $(w)\alpha_\varphi$ e $(z)\alpha_\varphi$ tinham na posição inicial. Logo, concluímos o desejado. A tabela abaixo mostra as fases dessa justificativa.

Momento	Expressão
Começo da etapa i	$w \cdots z \cdots a \cdots (w)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de a	$a \cdot w \cdot u \cdots z \cdot v \cdots (w)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$u \cdots v \cdots (a)\alpha_\varphi \cdot (w)\alpha_\varphi \cdot (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdot (v)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$

• Agora, caso z ou w tenha sido criado na etapa i, suponhamos, sem perda de generalidade, que z foi criado na etapa i. O mesmo pode-se dizer para $(z)\alpha_\varphi$. Digamos que u finalizou a etapa i à direita de z. Assim, pela hipótese de indução, $(u)\alpha_\varphi$ finalizou a etapa i à direita de $(z)\alpha_\varphi$. Como u e z tem pesos maiores que i, ao coletarmos a, criaremos $u = [w, a]$ à direita de z e, consequentemente, $v = [z, a]$ será criado à esquerda de u. Portanto, ao fim da etapa i, u estará à direita de v. Analogamente, $(u)\alpha_\varphi$ estará à direita de $(v)\alpha_\varphi$. A próxima tabela nos ajuda a compreender essa argumentação. Observe que as linhas não estão na ordem cronológica e algumas fases estão repetidas. Isto ocorre pelo fato da justificativa usar em conta as posições finais de $u, z, (u)\alpha_\varphi, (z)\alpha_\varphi$ a fim de determinar as posições finais de v e $\alpha_\varphi(v)$.

Momento	Expressão
Fim da etapa i	$z \cdots u \cdots (z)\alpha_\varphi \cdots (u)\alpha_\varphi$
Antes da coleta de a e $(a)\alpha_\varphi$	$z \cdots w \cdots a \cdots (z)\alpha_\varphi \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de a	$a \cdot z \cdot v \cdots w \cdot u \cdots (z)\alpha_\varphi \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$v \cdots u \cdots (a)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi \cdots (w)\alpha_\varphi \cdot (u)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (v)\alpha_\varphi \cdots (u)\alpha_\varphi$

Subcaso 2: Os pesos de z e w são i, mas $a < b$.

Assim, temos que $a < w$ e $a < b < z$. Novamente, como w e z foram criados antes da etapa i, ao iniciar a etapa i, a posição relativa de z e w é a mesma que $(z)\alpha_\varphi$ e $(w)\alpha_\varphi$. Suponhamos, sem perda de generalidade, que w está à direita de z na posição inicial e, consequentemente, $(w)\alpha_\varphi$ está à direita de $(z)\alpha_\varphi$. Assim, ao coletarmos a, $[w, a]$ ficará à direita de z. Portanto, ao coletarmos b, $[z, b]$ ficará à esquerda de $[w, a]$. Isto não se alterará nesta etapa já que não coletaremos u ou v. Analogamente, ao fim da etapa i, temos que $(v)\alpha_\varphi$ ficará à esquerda de $(u)\alpha_\varphi$.

Momento	Expressão
Começo da etapa i	$z \cdots w \cdots a \cdots b \cdots (z)\alpha_\varphi \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de a	$a \cdot z \cdot [z,a] \cdots w \cdot u \cdots b \cdots (z)\alpha_\varphi \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$z \cdots u \cdots b \cdots (a)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot [(z)\alpha_\varphi, (a)\alpha_\varphi] \cdots (w)\alpha_\varphi \cdot (u)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de b	$b \cdot z \cdot v \cdots u \cdots (z)\alpha_\varphi \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$v \cdots u \cdots (b)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi \cdots (u)\alpha_\varphi$
Fim da etapa i	$v \cdots u \cdots (v)\alpha_\varphi \cdots (u)\alpha_\varphi$

Subcaso 3: O peso de z ou o peso de w é maior que i, além de que $a < b$.

• Vamos supor que o peso de z é maior do que i.

– Primeiro veremos o caso em que z e $(z)\alpha_\varphi$ não foram criados nesta etapa. Suponhamos, sem perda de generalidade, que ao fim da etapa i, u ficou à esquerda de z. Então, pela hipótese de indução, ao fim da etapa i, $(u)\alpha_\varphi$ ficou à esquerda de $(z)\alpha_\varphi$. Desde que u foi criado, a posição relativa entre ele e z não foi alterada. Logo, quando coletamos b e criamos $[z,b]$, ele foi criado imediatamente à direita de z. Portanto, u e v tem a mesma posição relativa que u e z. De modo análogo, $(u)\alpha_\varphi$ e $(v)\alpha_\varphi$ terão a mesma posição relativa que $(u)\alpha_\varphi$ e $(z)\alpha_\varphi$. Novamente traremos uma tabela para auxiliar na compreensão da justificativa e ela não estará na ordem cronológica.

Momento	Expressão
Fim da etapa i	$u \cdots z \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi$
Coleta de a	$a \cdot w \cdot u \cdots z \cdots b \cdots (w)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (a)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$u \cdots z \cdots b \cdots (a)\alpha_\varphi \cdot (w)\alpha_\varphi \cdot (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de b	$u \cdots b \cdot z \cdot v \cdots (u)\alpha_\varphi \cdots (z)\alpha_\varphi \cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$u \cdots v \cdots (u)\alpha_\varphi \cdots (b)\alpha_\varphi \cdot (z)\alpha_\varphi \cdot (v)\alpha_\varphi$
Fim da etapa i	$u \cdots v \cdots (u)\alpha_\varphi \cdots (v)\alpha_\varphi$

– Agora, veremos o que ocorre se z e $(z)\alpha_\varphi$ foram criados nesta etapa. Suponhamos sem perda de generalidade, que u terminou a etapa i à direita de z e, consequentemente, $(u)\alpha_\varphi$ terminou a etapa i à direita de $(z)\alpha_\varphi$. Digamos que u foi criado antes de z. Então, quando z foi criado, ele estava à esquerda de u, pois não coletamos nem u nem z nesta etapa. Assim, quando criamos v imediatamente à direita de z, chegamos que u terminou a etapa i à direita de v. Assim como a última tabela, esta não obedece a ordem cronológica.

Momento	Expressão
Fim da etapa i	$z \cdots u$
Criação de z	$z \cdots u \cdots b$
Coleta de b	$b \cdot z \cdot v \cdots u$
Fim da etapa i	$v \cdots u$

Agora, se z foi criado antes de u e, portanto, u foi criado à direita de z. No momento que criamos u, temos que z estava à esquerda de w, e z ficou à esquerda de u até o fim da etapa i. Além disso, quando criamos v, ele ficou imediatamente à direita de z. Logo, ao fim, v ficou à esquerda de u.

Momento	Expressão
Fim da etapa i	$z \cdots u$
Criação de u	$z \cdots a \cdot w \cdot u \cdots b$
Criação de v	$b \cdot z \cdot v \cdots u$
Fim da etapa i	$v \cdots u$

De modo análogo se prova que, independentemente se $(z)\alpha_\varphi$ foi criado antes ou depois de $(u)\alpha_\varphi$, temos que $(v)\alpha_\varphi$ finalizou a etapa i à esquerda de $(u)\alpha_\varphi$.

• Agora vamos analisar o caso em que o peso de w é maior que i e o peso de z é i. Podemos supor isto uma vez que já estudamos o caso $\omega(z) > i$. Como $v = [z, b] \in Y(X)$, é fato que $z > b$.

– Se w surgiu na etapa i, ele surgiu antes de v, pois surgiu antes de u. Da mesma forma, $(w)\alpha_\varphi$ surgiu antes de $(v)\alpha_\varphi$. Como u foi criado à direita de z, temos que w foi criado à direita de z. Suponha, sem perda de generalidade, que w terminou a etapa i à direita de v. Pela hipótese de indução, $(w)\alpha_\varphi$ terminou a etapa i a direita de $(v)\alpha_\varphi$. Logo, quando criamos v, ele foi criado à esquerda de w e portanto, z estava à esquerda de w, ou seja, w foi criado à direita de z. Assim, quando coletamos a, geramos u à direita de z. Consequentemente, ao coletarmos b, criamos v à esquerda de u. Mais uma vez precisaremos trazer uma tabela que não segue a ordem cronológica.

Momento	Expressão
Fim da etapa i	$v \cdots w$
Coleta de b	$b \cdot z \cdot v \cdots w$
Coleta de a	$z \cdots a \cdot w \cdot u \cdots b$
Coleta de b	$b \cdot z \cdot v \cdots u$
Fim da etapa i	$v \cdots u$

Analogamente se prova que $(v)\alpha_\varphi$ finalizou a etapa i à esquerda de $(u)\alpha_\varphi$.

– Agora, se w não foi criado na etapa i, suponhamos que no fim da etapa $i-1$, w estava à esquerda de z. Pela hipótese de indução, o mesmo se diz entre $(w)\alpha_\varphi$ e $(z)\alpha_\varphi$. Logo, ao surgir u, ele foi criado à esquerda de z. Assim v foi criado à direita de u. Analogamente, ao fim da etapa i, $(v)\alpha_\varphi$ estará à direita de $(u)\alpha_\varphi$.

Momento	Expressão
Começo da etapa i	$w\cdots z\cdots a\cdots b\cdots (w)\alpha_\varphi\cdots (z)\alpha_\varphi\cdots (a)\alpha_\varphi\cdots (b)\alpha_\varphi$
Coleta de a	$a\cdot w\cdot u\cdots z\cdot [z,a]\cdots b\cdots (w)\alpha_\varphi\cdots (z)\alpha_\varphi\cdots (a)\alpha_\varphi\cdots (b)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$u\cdots z\cdots b\cdots (a)\alpha_\varphi\cdot (w)\alpha_\varphi\cdot (u)\alpha_\varphi\cdots (z)\alpha_\varphi\cdot [(z)\alpha_\varphi,(a)\alpha_\varphi]\cdots (b)\alpha_\varphi$
Coleta de b	$u\cdots b\cdot z\cdot v\cdots (u)\alpha_\varphi\cdots (z)\alpha_\varphi\cdots (b)\alpha_\varphi$
Coleta de $(b)\alpha_\varphi$	$u\cdots v\cdots (u)\alpha_\varphi\cdots (b)\alpha_\varphi\cdot (z)\alpha_\varphi\cdot (v)\alpha_\varphi$
Fim da etapa i	$u\cdots v\cdots (u)\alpha_\varphi\cdots (v)\alpha_\varphi$

Com isso finalizamos a prova da afirmação.

Passo 3: Agora, vamos provar a seguinte afirmação:

Se $u\in Y(X)$ e aparece na expressão final, então $(u)\alpha_\varphi$ também aparece na expressão na mesma etapa em que u foi criada, para toda permutação φ compatível com u.

Se u tem peso 1, então pertence a X. Logo, u aparece na etapa 0, bem como os demais elementos de X, ou seja, $(u)\alpha_\varphi$ aparece na mesma etapa que u foi criado, para toda permutação φ compatível com u. Agora, seja $k\geq 2$ o peso de u e vamos assumir que a afirmação é verdadeira para todos os elementos de $Y(X)$ com peso menor que u que aparecem no final da coleta. Portanto, u é da forma $[w,a]$ para $w,a\in Y(X)$. Seja $\varphi\in S_n$ compatível com u. Então, φ é compatível com w e a. Como u foi gerado na coleta de a, temos que w e a aparecem na expressão ao fim da etapa i e u foi construído na etapa i, onde i é o peso de a. Vamos analisar dois casos:

Caso 1: w foi criado antes da etapa i.

Pela hipótese de indução, $(w)\alpha_\varphi$ foi criado na mesma etapa. Da mesma forma, a e $(a)\alpha_\varphi$ foram criadas antes da etapa i, pois nesta etapa só se criam comutadores com peso maior que i. Assim, ao fim da etapa $i-1$, pela afirmação provada no Passo 2, w e a estão com a mesma posição relativa que $(w)\alpha_\varphi$ e $(a)\alpha_\varphi$.

Como u foi gerado na etapa i, temos que w estava à esquerda de a no fim da etapa $i-1$. Assim, $(w)\alpha_\varphi$ satisfaz o mesmo em relação à $(a)\alpha_\varphi$. Portanto, na etapa i, foi gerado $[(w)\alpha_\varphi,(a)\alpha_\varphi]=(u)\alpha_\varphi$, como desejado.

Momento	Expressão
Começo da etapa i	$w \cdots a \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de a	$a \cdot w \cdot u \cdots (w)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(a)\alpha_\varphi$	$u \cdots (a)\alpha_\varphi \cdot (w)\alpha_\varphi \cdot (u)\alpha_\varphi$
Fim da etapa i	$u \cdots (u)\alpha_\varphi$

Caso 2: w foi gerado na etapa i.

Para podermos prosseguir, vamos provar a seguinte afirmação:

Dado $r \in Y(X)$, com r compatível com φ e peso menor que o peso de u, se r foi gerado na etapa i à esquerda de a, então $(r)\alpha_\varphi$ foi gerado à esquerda de $(a)\alpha_\varphi$ na mesma etapa.

Se $i = 0$ a afirmação é verdadeira. Suponha que $i \geq 1$. Dado um elemento que foi gerado na etapa i, seu peso mínimo é $2i$ pois é da forma $[c, d]$ com c e d de peso no mínimo i. Assim, sendo l o peso de r, vamos proceder por indução sobre $l \in \{2i, 2i + 1, \dots\}$. Para $l = 2i$, temos que $r = [c, d]$, com $c, d \in Y(X)$ de peso i. Assim, c e d não foram gerados nesta etapa. Além disso, r deve ter sido criado antes de coletarmos a e, portanto, $d < a$.

Já que o peso de a é i, temos que c, d e a tem pesos menores que u podendo assim ser aplicada a hipótese de indução. Logo, temos que $(c)\alpha_\varphi$, $(d)\alpha_\varphi$ e $(a)\alpha_\varphi$ aparecem na expressão ao fim da etapa $i - 1$ e nas mesmas respectivas posições relativas que c, d e a pela afirmação provada no Passo 2.

Como $r = [c, d]$, ele foi gerado imediatamente à direita de c e à esquerda de a por hipótese. Então, $(c)\alpha_\varphi$ estava à esquerda de $(d)\alpha_\varphi$ e $(a)\alpha_\varphi$ ao fim da etapa $i - 1$. Assim, quando coletamos $(d)\alpha_\varphi$, ainda não vamos ter coletado $(a)\alpha_\varphi$, pois $(d)\alpha_\varphi < (a)\alpha_\varphi$. Dessa forma, vamos criar $(r)\alpha_\varphi = [(c)\alpha_\varphi, (d)\alpha_\varphi]$ à esquerda de $(a)\alpha_\varphi$. Provamos assim o desejado para $k = 2i$.

Momento	Expressão
Começo da etapa i	$c \cdots d \cdots a \cdots (c)\alpha_\varphi \cdots (d)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(d)\alpha_\varphi$	$(d)\alpha_\varphi \cdot (c)\alpha_\varphi \cdot (r)\alpha_\varphi \cdots (a)\alpha_\varphi$

Agora, seja $l > 2i$ de modo que a afirmação é verdadeira para todo comutador de peso menor que l, compatível com φ e que foi gerado na etapa i à esquerda de a. Temos que $r = [c, d] \in Y(X)$, com d de peso i e $d < a$, pois r foi construído antes de coletarmos a. Como r foi criado imediatamente à direita de c, temos que c estava à esquerda de a quando criamos r.

• Se c foi criado antes da etapa i, pela hipótese de indução, $(c)\alpha_\varphi$ foi criada na mesma etapa que c. Assim, pela afirmação provada, ao fim da etapa $i-1$, temos que as posições relativas de c, d e a são, respectivamente, as mesmas de $(c)\alpha_\varphi$, $(d)\alpha_\varphi$ e $(a)\alpha_\varphi$. Além disso, como r foi criado à esquerda de a, temos que c estava à esquerda de a ao fim da etapa $i-1$. Logo, $(c)\alpha_\varphi$ estava à esquerda de $(a)\alpha_\varphi$ ao fim da mesma etapa. Portanto, ao coletarmos $(d)\alpha_\varphi$, criamos $(r)\alpha_\varphi = [(c)\alpha_\varphi, (d)\alpha_\varphi]$ à esquerda de a, como desejado.

Momento	Expressão
Começo da etapa i	$c \cdots d \cdots a \cdots (c)\alpha_\varphi \cdots (d)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(d)\alpha_\varphi$	$(d)\alpha_\varphi \cdot (c)\alpha_\varphi \cdot (r)\alpha_\varphi \cdots (a)\alpha_\varphi$

• Agora, se c foi criado na etapa i, temos que ele foi criado à esquerda de a, pois $[c, d]$ foi criado à esquerda de a. Assim, $(c)\alpha_\varphi$ foi criado à esquerda de $(a)\alpha_\varphi$ pela hipótese de indução. Logo, ao coletarmos $(d)\alpha_\varphi$, criaremos $(r)\alpha_\varphi = [(c)\alpha_\varphi, (d)\alpha_\varphi]$ à esquerda de $(a)\alpha_\varphi$. Provamos assim tal afirmação. Novamente apresentaremos uma tabela fora da ordem cronológica, já que precisamos antes buscar uma informação sobre o fim da etapa i.

Momento	Expressão
Fim da etapa i	$r \cdots a$
Coleta de d	$d \cdot c \cdot r \cdots a$
Criação de c	$c \cdots d \cdots a$
Criação de $(c)\alpha_\varphi$	$(c)\alpha_\varphi \cdots (d)\alpha_\varphi \cdots (a)\alpha_\varphi$
Coleta de $(d)\alpha_\varphi$	$(d)\alpha_\varphi \cdot (c)\alpha_\varphi \cdot (r)\alpha_\varphi \cdots (a)\alpha_\varphi$

Aplicando esta afirmação para w, temos que $(w)\alpha_\varphi$ foi gerado à esquerda de $(a)\alpha_\varphi$. Assim, ao coletarmos $(a)\alpha_\varphi$, aparecerá $(u)\alpha_\varphi = [(w)\alpha_\varphi, (a)\alpha_\varphi]$.

Momento	Expressão
Criação de w	$w \cdots a$
Coleta de a	$a \cdot w \cdot u$

Concluímos a demonstração do lema. □

Observação 2.3. Vamos fazer algumas considerações a respeito do processo de coleta realizado no Lema 2.2.

(I) Um processo de indução simples sobre o peso dos elementos de $Y(X)$ nos diz que cada um deles aparece no máximo uma vez na expressão obtida.

(II) Para cada $w \in Y(X)\backslash X$ que aparece no processo de coleta, o primeiro elemento na escrita de w é y_i, para algum $i \in \mathbb{N}$. De fato, provaremos essa afirmação por indução sobre $\omega(w)$. Vamos supor que o peso de w é 2. Se $w = [x_i, x_j]$, com $i, j \in \mathbb{N}$, então $i > j$. Mas $[x_i, x_j]$ não aparecerá no processo de coleta, pois quando formos coletar x_j, o elemento x_i estará à sua direita e então, não faremos a substituição $x_i x_j = x_j x_i [x_i, x_j]$. Observamos também que comutadores da forma $[x_i, y_j]$ não pertencem a $Y(X)$ pois $x_i < y_j$, para todos $i, j \in \mathbb{N}$. Assim, existem $i \in I_n$ e $z \in X$ tais que $w = [y_i, z]$.

Agora, seja $w \in Y(X)\backslash X$ de peso $k > 2$ e assuma que o resultado vale para todo elemento de $Y(X)\backslash X$ de peso menor que k que aparece no processo de coleta. Assim, w é da forma $[r, s]$ com $r, s \in Y(X)$ e $r > s$. Portanto, o peso de r é maior ou igual ao peso de s, fazendo com que $\omega(w) > \omega(r) \geq 2$. Assim, pela hipótese de indução, o primeiro elemento na escrita de r, e consequentemente de w, é da forma y_i.

(III) Calculemos neste momento o número de vezes que aparecem comutadores da forma $[[y_a, x_b, x_c], [y_d, x_e]]$ ao finalizarmos o processo descrito no Lema 2.2. Digamos que aparece um elemento dessa forma com $a < b < c < d < e$. Então, pela segunda parte do Lema 2.2, existem $\binom{n}{5}$ elementos na expressão obtida que satisfaz o desejado. Agora, se pedirmos $a = b < c < d < e$, existem $\binom{n}{4}$ elementos como dito. Seguindo o mesmo raciocínio, o número de elementos da forma $[[y_a, x_b, x_c], [y_d, x_e]]$ que aparecem na expressão final é da forma $m_1 \cdot \binom{n}{1} + m_2 \cdot \binom{n}{2} + \cdots + m_5 \cdot \binom{n}{5}$, em que $m_1, \ldots, m_5 \in \mathbb{N}$.

De forma semelhante, para cada forma estabelecida de elementos de $Y(X)$, o número de vezes que aparecem elementos dessa forma na expressão final é uma soma de múltiplos de elementos da forma $\binom{n}{m}$ em que m é um natural não nulo menor ou igual ao peso da forma dada.

(IV) Para cada $m \in \{2, \ldots, n\}$, o elemento $[y_1, x_2, \ldots, x_m]$ também aparece na expressão ao fim do processo de coleta. De fato, provaremos essa afirmação por indução sobre m. Para $m = 2$, note que ao coletarmos x_2, teremos:

$$x_1 y_1 x_2 y_2 x_3 y_3 \cdots x_n y_n = x_1 x_2 y_1 [y_1, x_2] y_2 x_3 y_3 \cdots x_n y_n,$$

satisfazendo o desejado.

Agora, assuma que $[y_1, x_2, \ldots, x_m]$ foi criado no processo de coleta para algum $m \in \{2, \ldots, n-1\}$. Escrevemos $u = [y_1, x_2 \ldots, x_{m-1}]$ se $m > 2$ e $u = y_1$ caso $m = 2$. Assim, $[y_1, x_2, \ldots, x_m] = [u, x_m]$. Veja que criamos $[u, x_m]$ ao coletarmos x_m e portanto u estava à esquerda de x_m quando começamos a coletar x_m. Por consequência, como x_{m+1} estava à direita de x_m na expressão inicial e ainda não coletamos x_m nem x_{m+1}, temos que u estava à esquerda de x_{m+1} e ao coletarmos x_m, criamos $[u, x_m]$ à esquerda de x_{m+1}. Assim, ao coletarmos x_{m+1}, criaremos $[u, x_m, x_{m+1}] = [y_1, x_2, \ldots, x_m, x_{m+1}]$. Provamos assim o afirmado.

(V) Dado um elemento u da forma $[y_{i_1}, x_{i_2}, \ldots, x_{i_m}]$ para algum $m \in \mathbb{N}$, se u aparece na escrita final obtida, temos que $[y_{i_1}, x_{i_2}]$ foi criado na primeira etapa e, portanto, na expressão inicial tínhamos que y_{i_1} estava à esquerda de x_{i_2}, ou seja, $i_1 < i_2$.

Como $[y_1, x_{i_2}, x_{i_3}]$ aparece na escrita, ele é um elemento de $Y(X)$. Portanto, $x_{i_2} \leq x_{i_3}$. Além disso, ao coletarmos x_{i_3}, temos que $[y_1, x_{i_2}]$ já deve ter sido criado, fazendo com que $x_{i_2} < x_{i_3}$. Repetindo este argumento teremos que $i_1 < i_2 < \cdots < i_m$.

(VI) Dado um comutador $u \in Y(X)$ construído no processo de coleta, temos que u não é da forma $[u_1, \ldots, [x_i, x_j], \ldots, u_m]$ ou $[u_1, \ldots, [y_i, y_j], \ldots, u_m]$ para $u_1, \ldots, u_m \in Y(X)$, $i, j \in I_n$ e $m \in \mathbb{N}$. De fato, note que os comutadores do tipo $[x_i, x_j]$ e $[y_i, y_j]$ não surgem no processo, pois os elementos $x_1, \ldots, x_n$ já estão ordenados entre si desde o início e o mesmo acontece com $y_1, \ldots, y_n$.

Tomemos um comutador $u \in Y(X)$ que possui apenas um elemento da forma y_i em sua escrita e surgiu no processo de coleta. Pelo item (II), este elemento é o primeiro da escrita de u. Além disso, o primeiro parágrafo deste item nos diz que u é do tipo $[y_{i_1}, x_{i_2}, \ldots, x_{i_l}]$ para algum $l \in I_n$.

Para o que segue, vamos necessitar do seguinte lema.

Lema 2.4. *Dado $i \in \mathbb{N}$ e p primo, com $1 \leq i \leq p^n$, se $i = p^r j$ com $mdc(p, j) = 1$, então p^{n-r} divide $\binom{p^n}{i}$.*

Ideia da demonstração. Alguns cálculos simples mostram que $p^{n-r}\binom{p^n-1}{i-1} = j\frac{p^n!}{i!(p^n-i)!} = j\binom{p^n}{i}$. Então, p^{n-r} divide $j\binom{p^n}{i}$, e como $\text{mdc}(p^{n-r}, j) = 1$, temos que p^{n-r} divide $\binom{p^n}{i}$. □

Dados um comutador u em um grupo G e $g \in G$, o peso de u em g é quantidade de vezes que g aparece na escrita de u. Por exemplo, para $x, y \in G$, o comutador $[x, y, y]$ tem peso dois em y.

Sejam G um p-grupo e x, y elementos de G. Para $a, b \in \langle x, y\rangle$ e r um natural não nulo, seja $K_r(a, b)$ o fecho normal em $\langle x, y\rangle$ do conjunto formado por:

- comutadores formais em $\{a, b\}$ de peso no mínimo p^r e peso no mínimo 2 em b;
- as p^{r-k+1}-ésimas potências de comutadores formais em $\{a, b\}$ de peso maior ou igual a p^{k-1} e menor que p^k e peso no mínimo 2 em b para $k \in I_r$.

Usando o Lema 2.2 e levando em consideração a Observação 2.3, podemos demonstrar a seguinte fórmula de coleta de Hall [26, Proposition 1.1.32].

Teorema 2.5 (Commutator collection formulae)**.** *Sejam G um grupo, $x, y \in G$, $r \in \mathbb{N}^*$ e p um primo. Então:*

(i) $(xy)^{p^r} \equiv x^{p^r} y^{p^r} \prod_{i=2}^{p^r} [y, {}_{i-1}x]^{\binom{p^r}{i}}$ *(mod* $K_r(x, y)$*);*

(ii) $\left[x^{p^r}, y\right] \equiv [x, y]^{p^r} \prod_{i=2}^{p^r} [x, y, {}_{i-1}x]^{\binom{p^r}{i}}$ *(mod* $K_r(x, [x, y])$*).*

Demonstração. Escrevendo $n = p^r$, sejam $X = \{x_1, x_2, \ldots, x_n, y_1, \ldots, y_n\}$ e F o grupo gerado livremente por X. Pelo Lema 2.2, sendo $L(F)$ o fecho normal em F do conjunto composto por elementos de $Y(X)$ de peso maior que n, temos que:

$$x_1 y_1 \cdots x_n y_n \equiv c_1 c_2 \cdots c_m \pmod{L(F)},$$

em que $c_1, \ldots, c_m \in Y(X)$ e estão escritos na ordem crescente segundo a relação de ordem $<$. Além disso, se $u = c_i \in Y(X)$ para algum $i \in I_m$ e $\varphi \in S_n$ é compatível com u, então $(u)\alpha_\varphi = c_j$ para algum $j \in I_m$.

Consideremos a função $\alpha_1 : X \to \langle x, y\rangle$ em que para cada $i \in I_n$ temos $(x_i)\alpha_1 = x$ e $(y_i)\alpha_1 = y$. Como F é livre em X, podemos tomar um homomorfismo $\alpha : F \to \langle x, y\rangle$ que estende α. Assim, temos as seguintes congruências módulo $(L(F))\alpha$.

$$(xy)^n \equiv (x_1 y_1 \cdots x_n y_n)\alpha \equiv (c_1 c_2 \cdots c_m)\alpha \equiv (c_1)\alpha \ldots (c_m)\alpha.$$

Pela Observação 2.3 (II), em todo comutador de peso no mínimo 2 que surgiu no processo de coleta, o primeiro elemento em sua escrita é y_i, para algum $i \in I_n$. Dado um comutador formal básico w em X de peso maior que n que surgiu na coleta e que apareça apenas um símbolo da forma y_i, pela Observação 2.3 (VI), o comutador w é um elemento da forma $[y_{i_1}, x_{i_2}, \ldots, x_{i_k}]$ e, pela Observação 2.3 (V), $i_1 < i_2 < \cdots < i_k$. Como $i_1, \ldots, i_k \in I_n$, temos que o peso de w é menor ou igual a n, o que é um absurdo. Logo, todo elemento de $Y(X)$ gerado no processo de coleta e de peso maior que n possui pelo menos dois elementos da forma y_i. Logo, $(L(F))\alpha \leq K(x, y)$.

Agora, dado um comutador do tipo $[y, {}_{l-1}x]$, temos que ele é imagem por α dos elementos da forma $[y_{i_1}, x_{i_2}, \ldots, x_{i_l}]$. Pela Observação 2.3 (IV) e (V) há pelo menos um comutador dessa forma na coleta feita, além de que satisfaz $i_1 < i_2 < \cdots < i_l$. Assim, para descobrirmos quantos elementos da forma $[y, {}_lx]$ teremos, basta sabermos quantos comutadores do tipo $[y_{i_1}, x_{i_2}, \ldots, x_{i_l}]$, com $i_1 < i_2 < \cdots < i_l$, obteremos no processo de coleta.

Veja que existe uma bijeção ψ entre $I_n \backslash \{1, \ldots, l\}$ e $I_n \backslash \{i_1, \ldots, i_l\}$, pois tais conjuntos tem a mesma cardinalidade. Pelo Lema 2.2, se $i_1 < i_2 < \cdots < i_l$, então $[y_{i_1}, x_{i_2}, \ldots, x_{i_l}]$ aparece na expressão, já que podemos considerar a permutação:

$$\begin{aligned} \varphi : \ I_n &\longrightarrow I_n \\ j &\longmapsto \begin{cases} i_j, & \text{se } j \in I_l \\ \psi(j), & \text{se } j \notin I_l \end{cases}, \end{aligned}$$

o qual é compatível com $u = [y_1, x_2, \ldots, x_l]$ que já surgiu na etapa 1 do processo de coleta. Logo, existem $\binom{n}{l}$ elementos da forma desejada na expressão de $(xy)^n$ e estes estarão em sequência. Além disso, lembremos que pela Observação 2.3 (VI), se um elemento u de $Y(X)$ foi construído no processo de coleta e possui apenas um elemento da forma y_i na sua escrita, então u é do tipo $[y_{i_1}, x_{i_2}, \ldots, x_{i_l}]$, com $i_1 < i_2 < \cdots < i_l$, para algum $l \in I_n$.

Agora, dado um comutador de $Y(X)$ de peso m que surge no processo de coleta e contém dois elementos do tipo y_i em sua escrita, pela Observação 2.3 (III), o número de vezes que aparece um comutador dessa mesma forma é uma soma de naturais como $\binom{n}{t}$ onde $t \leq m$.

Dado k tal que $p^{k-1} \leq m < p^k$, temos que $t = p^j a$ onde $j \leq k-1$ e $\text{mdc}(p, a) = 1$. Pelo Lema 2.4, temos que p^{r-k+1} divide $\binom{p^r}{t}$. Assim, p^{r-k+1} divide o número de vezes que comutadores da mesma forma que a dada aparece na expressão de $x_1 y_1 \ldots x_n y_n$. Além disso, tais elementos estarão em sequência. Logo, ao calcularmos α de tais, o produto de suas imagens estarão em $K(x, y)$. Logo, concluímos que:

$$(xy)^{p^r} \equiv x^{p^r} y^{p^r} \prod_{i=2}^{p^r} [y, {}_{i-1}x]^{\binom{p^r}{i}} \pmod{K_r(x, y)}.$$

Agora, provaremos o segundo item. Uma indução simples nos mostra que para todo $m \in \mathbb{N}$ temos que $[x^m, y] = x^{-m}(x[x, y])^m$. Agora, usando argumentos análogos aos utilizados no primeiro item, se prova que:

$$(x[x,y])^{p^r} \equiv x^{p^r}[x,y]^{p^r} \prod_{i=2}^{p^r} [[x,y],{}_{i-1}x]^{\binom{p^r}{i}} \pmod{K_r(x,[x,y])}.$$

Logo, considerando as congruências módulo $K(x,[x,y])$,

$$[x^{p^r},y] \equiv x^{-p^r}(x[x,y])^{p^r} \equiv x^{-p^r}x^{p^r}[x,y]^{p^r} \prod_{i=2}^{p^r} [[x,y],{}_{i-1}x]^{\binom{p^r}{i}} \equiv [x,y]^{p^r} \prod_{i=2}^{p^r} [x,y,{}_{i-1}x]^{\binom{p^r}{i}},$$

como desejado. □

Apresentaremos a seguir outras duas fórmulas devidas a P. Hall, conhecidas como "Fórmulas de coleta de Hall". A demonstração desse resultado será omitida, mas pode ser encontrada em [16, pág. 4].

Teorema 2.6. *Sejam G um grupo e $x, y \in G$. Então, para todo $k \in \mathbb{N}$:*

$$(xy)^{p^k} \equiv x^{p^k}y^{p^k} \left(mod\ \gamma_2(H)^{p^k}\gamma_p(H)^{p^{k-1}}\gamma_{p^2}(H)^{p^{k-2}}\cdots\gamma_{p^k}(H)\right), \tag{2.3}$$

onde $H = \langle x, y\rangle$. Além disso, escrevendo $L = \langle x, [x,y]\rangle$, temos:

$$[x,y]^{p^k} \equiv [x^{p^k},y] \left(mod\ \gamma_2(L)^{p^k}\gamma_p(L)^{p^{k-1}}\gamma_{p^2}(L)^{p^{k-2}}\cdots\gamma_{p^k}(L)\right). \tag{2.4}$$

Além das fórmulas de coleta de Hall, os próximos dois resultados têm se mostrado ferramentas importantes no estudo de expoente de grupos e serão aplicados no Capítulo 5 na obtenção de limitantes para expoente de termos da série central inferior de um p-grupo finito. Omitiremos suas provas que podem ser encontradas em [16, páginas 5 e 6].

Teorema 2.7. *Sejam G um p-grupo finito e M, N subgrupos normais de G. Então:*

$$\left[N^{p^k},M\right] \equiv [N,M]^{p^k} \left(mod\ \ [M,{}_pN]^{p^{k-1}}\,[M,{}_{p^2}N]^{p^{k-2}}\cdots\left[M,{}_{p^k}N\right]\right).$$

Teorema 2.8. *Sejam G um p-grupo finito e N um subgrupo normal de G. Então temos as seguintes congruências para todos inteiros k e l, com $k \geq 0$ e $l \geq 1$;*

(i) $\left[N^{p^k},{}_lG\right] \equiv [N,{}_lG]^{p^k} \left(mod\ \prod_{r=1}^{k}[N,{}_{p^r+l-1}G]^{p^{k-r}}\right)$;

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

CAPÍTULO 3

p-GRUPOS FINITOS

Neste capítulo apresentaremos um estudo sobre duas classes de grupos que serão abordados em capítulos futuros, a saber: p-grupos *powerful* e p-grupos regulares.

3.1 p-Grupos *powerful*

Veremos no último capítulo desta dissertação que se G é um p-grupo metabeliano de classe menor ou igual a $2p-1$, então G^p é *powerful*. Além disso, G^p ser *powerful* é uma de três condições suficientes para que $\exp(M(G))|\exp(G)$ (Veja Teorema 5.4). Assim, o objetivo desta seção é introduzir o conceito de p-grupo *powerful* e apresentar os resultados que são necessários no estudo de expoentes de grupos que faremos no Capítulo 5. Salvo menção contrária, os resultados desta seção podem ser encontrados em [28].

Dado um p-grupo G, um subgrupo N de G é *powerfully embedded* em G caso:

$$\begin{cases} [N,G] \leq N^{p^2}, & \text{se } p=2 \\ [N,G] \leq N^p, & \text{se } p>2 \end{cases}.$$

O grupo G é dito *powerful* se G é *powerfully embedded* em si mesmo, ou seja,

$$\begin{cases} G' \leq G^{p^2}, & \text{se } p=2 \\ G' \leq G^p, & \text{se } p>2 \end{cases}.$$

Neste trabalho, estudaremos os p-grupos *powerful* com p-ímpar. É fácil ver que todo p-grupo abeliano é *powerful*. Também o centro de um p-grupo G é *powerfully embedded* em G.

Para simplificar, vamos escrever N $p.e.$ G quando N for um subgrupo *powerfully embedded* em G. Claramente, se N $p.e.$ G, então N é *powerful*. Além disso, N é normal em G, pois para todos $n \in N$ e $g \in G$ temos $n^g = n[n,g] \in NN^P = N$.

Para prosseguirmos o estudo, precisaremos do próximo lema.

Lema 3.1. *Sejam G um p-grupo finito e N um subgrupo normal de G tal que $N \neq \{1\}$. Existe $K \triangleleft G$ tal que $K \triangleleft N$, $(N : K) = p$ e $[G, N] \leq K$.*

Demonstração. Vamos provar por indução sobre a ordem de G. Se $|G| = p$, então $N = G$ pois $\{1\} < N$ e assim basta tomarmos $K = \{1\}$.

Agora, seja G um grupo com ordem p^α tal que o resultado é verdadeiro para todo p-grupo com ordem menor que p^α. Seja N um subgrupo normal de G, com $N \neq \{1\}$.

Se $[G, N] = \{1\}$, então $N \leq Z(G)$. Pelo Primeiro Teorema de Sylow, existe um subgrupo K de N, e portanto de G, tal que $(N : K) = p$, pois $\{1\} < N$ e N é p-grupo. Como $K \leq N \leq Z(G)$, temos que $K \triangleleft G$, concluindo o necessário.

Agora, suponha que $[G, N] > \{1\}$. Como $[G, N] \triangleleft G$, podemos considerar o grupo $G/[G, N]$ com ordem menor que $|G|$. Uma vez que G é nilpotente, por ser p-grupo, e $N \neq \{1\}$, a Proposição 1.7, nos diz que $[G, N] < N$. Desse modo, $\{1_{G/[G,N]}\} < N/[G, N]$ e, por hipótese de indução, existe $K/[G, N] \triangleleft N/[G, N]$ com $K/[G, N] \triangleleft G/[G, N]$ e $((N/[G, N]) : (K/[G, N])) = p$. Com isso, $K \triangleleft G$, $[G, N] \triangleleft K$ e:

$$(N : K) = \left(\frac{N}{[G, N]} : \frac{K}{[G, N]}\right) = p.$$

Concluímos assim que o resultado é válido para todo p-grupo finito G. □

O próximo lema se trata de uma afirmação provada durante a demonstração de [28, Theorem 1.1].

Lema 3.2. *Dados um p-grupo finito G com p um primo ímpar e K um subgrupo normal de G, se $[K, G] \leq K^p[K, G, G]$, então K $p.e.$ G.*

Demonstração. Vamos supor que $[K, G] \leq K^p[K, G, G]$ mas K não é *powerfully embedded* em G e deduzir uma contradição. Como $[K, G, G] \leq [K, G]$, temos:

$$[K, G] = [K, G, G]\,([K, G] \cap K^p)\,.$$

De $[K, G] \not\leq K^p$ resulta $[K, G] \cap K^p < [K, G]$. Assim, escrevendo $H = [K, G] \cap K^p$, é fato que $[K, G]/H$ é um subgrupo normal não trivial do p-grupo finito G/H. Pelo Lema 3.1, existe $L/H \triangleleft G/H$ com:

$$\frac{L}{H} \triangleleft \frac{[K, G]}{H}, \quad \left(\frac{[K, G]}{H} : \frac{L}{H}\right) = p \quad \text{e} \quad \left[\frac{G}{H}, \frac{[K, G]}{H}\right] \leq \frac{L}{H}.$$

Logo, $H \leq L$, $L \triangleleft G$, $L \triangleleft [K, G]$, $([K, G] : L) = p$ e $[K, G, G] = [G, [K, G]] \leq L$.

Dessa forma, $L \leq [K, G] = [K, G, G]H \leq L$, o que contradiz o fato de $([K, G] : L) = p$.

Concluímos assim que a afirmação é verdadeira para todo p-grupo finito G. □

O próximo teorema será aplicado muitas vezes nesta mesma seção.

Teorema 3.3. *[28, Theorem 1.1] Dado um p-grupo G com p um primo ímpar, se N $p.e.$ G, então N^p $p.e.$ G.*

Demonstração. Suponhamos que temos N $p.e.$ G. Sendo $K = N^p$, vamos primeiramente provar que se $[K, G, G] = \{1\}$, então $[K, G] \leq K^p$. Da hipótese segue que $[N, G, G, G] \leq [K, G, G] = \{1\}$. Agora, dados $n \in N$ e $g \in G$, pelo Teorema 2.6, é fato que se $L = \langle n, [n, g]\rangle$, então:

$$[n, g]^p \equiv [n^p, g] \,(\text{mod } \gamma_2(L)^p\gamma_p(L))\,.$$

Pela Proposição 1.8, temos:

$$\gamma_2(L) = \left\langle [n, n]^l, [n, [n, g]]^l, [[n, g], [n, g]]^l \middle| \, l \in L \right\rangle = \left\langle [n, [n, g]]^l \middle| \, l \in L \right\rangle \leq [N, G],$$

e de modo análogo, $\gamma_3(L) = \left\langle [a, b, c]^l \middle| \, a, b, c \in \{n, [n, g]\}, l \in L \right\rangle$. Não é difícil verificar que se $a, b, c \in \{n, [n, g]\}$, então $[a, b, c] \in [N, G, G, G] = \{1\}$, provando assim que $\gamma_3(L) = \{1\}$. Uma vez que $\gamma_p(L) \leq \gamma_3(L) = \{1\}$, concluímos que:

$$[n, g]^p \equiv [n^p, g] \,(\text{mod } [N, G]^p)\,.$$

Portanto, $[n^p, g] \in [N, G]^p$ para todos $n \in N$ e $g \in G$, provando que $[K, G] \leq [N, G]^p$. Logo, $[K, G] \leq K^p$, como desejado.

Agora, suponhamos $[K, G, G] \neq \{1\}$. Colocando $H = [K, G, G]$, vamos estudar o grupo $K/H \triangleleft G/H$. Assim,

$$\left[\frac{N}{H}, \frac{G}{H}\right] = \frac{[N, G]H}{H} \leq \frac{N^pH}{H} = \left(\frac{N}{H}\right)^p,$$

provando que N/H $p.e.$ G/H. Além disso,

$$\left(\frac{N}{H}\right)^p = \frac{N^pH}{H} = \frac{KH}{H} = \frac{K}{H}.$$

Uma vez que $[K/H, G/H, G/H] = ([K, G, G]H)/H = \{1\}$, segue da primeira parte,

$$\frac{[K, G]}{H} = \left[\frac{K}{H}, \frac{G}{H}\right] \leq \left(\frac{K}{H}\right)^p = \frac{K^pH}{H},$$

fazendo com que $[K, G] \leq K^pH = K^p[K, G, G]$. Agora, do Lema 3.2, concluímos que K $p.e.$ G. □

Agora, estamos aptos a provar o próximo teorema, que nos fornece uma importante característica dos p-grupos *powerful* finitos.

Teorema 3.4. *[28, pág. 487] Dado um p-grupo finito powerful G com p ímpar, para cada par $i, j \in \mathbb{N}$, temos que G^{p^j} $p.e.$ G e $\left(G^{p^j}\right)^{p^i} = G^{p^{i+j}}$.*

Demonstração. Primeiro provaremos o seguinte:

Afirmação 1: Dado um p-grupo finito, se j é um natural tal que $G^{p^{j+1}} = \{1\}$ e G^{p^j} $p.e.$ G, então $\left(G^{p^j}\right)^p = \{1\}$.

Faremos essa prova por indução sobre a ordem de G. Se $G = \{1\}$, é óbvio. Agora, seja G um p-grupo finito tal que a afirmação é verdadeira para todo p-grupo com ordem menor que $|G|$.

Se $G^{p^j} = \{1\}$, já temos o desejado. Supomos assim que $G^{p^j} \neq \{1\}$. Como G^{p^j} é um p-grupo, temos $Z\left(G^{p^j}\right) \neq \{1\}$ e $Z\left(G^{p^j}\right) \triangleleft G$ uma vez que $Z\left(G^{p^j}\right)$ char $G^{p^j} \triangleleft G$. Tomemos então $N = Z\left(G^{p^j}\right)$. Logo, $|N| \neq 1$. Assim, G/N é um grupo com ordem menor que $|G|$ e, portanto, o resultado é válido neste grupo. Veja que, como $G^{p^{j+1}} = \{1\}$ e G^{p^j} $p.e.$ G,

$$\left(\frac{G}{N}\right)^{p^{j+1}} = \frac{G^{p^{j+1}}N}{N} = \frac{N}{N},$$

e,

$$\left[\left(\frac{G}{N}\right)^{p^j}, \frac{G}{N}\right] = \left[\frac{G^{p^j}N}{N}, \frac{G}{N}\right] = \frac{\left[G^{p^j}N, G\right]N}{N} = \frac{\left[G^{p^j}, G\right][N, G]\,N}{N}$$
$$\leq \frac{\left((G)^{p^j}\right)^p N}{N} = \left(\frac{G^{p^j}}{N}\right)^p = \left(\left(\frac{G}{N}\right)^{p^j}\right)^p.$$

Agora, pela hipótese de indução, $\left((G/N)^{p^j}\right)^p = N/N$, ou seja,

$$\frac{N}{N} = \left(\frac{G^{p^j}N}{N}\right)^p = \left(\frac{G^{p^j}}{N}\right)^p = \frac{\left(G^{p^j}\right)^p N}{N},$$

nos permitindo concluir que $\left(G^{p^j}\right)^p \leq N$. Assim, já que G^{p^j} $p.e.$ G,

$$\left[G^{p^j}, G^{p^j}\right] \leq \left[G^{p^j}, G\right] \leq \left(G^{p^j}\right)^p \leq N.$$

Dessa forma, $\gamma_2\left(G^{p^j}\right) \leq N \leq Z\left(G^{p^j}\right)$ e consequentemente $\gamma_3\left(G^{p^j}\right) = \{1\}$, isto é, G^{p^j} é nilpotente de classe no máximo 2.

Vamos provar que para todo $t \in G^{p^j}$, temos $t^p = 1$. Dado $t \in G^{p^j}$, existem $g_1, \ldots, g_k \in G$ tais que $t = g_1^{p^j} \cdots g_k^{p^j}$. Mostraremos que $t^p = 1$ por indução sobre k.

Para $k = 1$, temos $\left(g_1^{p^j}\right)^p = g_1^{p^{j+1}} \in G^{p^{j+1}} = \{1\}$, ou seja, $t^p = 1$. Agora, tome $k \in \mathbb{N}^*$ tal que o resultado é válido para todo elemento que pode ser escrito como um produto de $k-1$ termos da forma g^{p^j}. Dado $t = g_1^{p^j} \cdots g_k^{p^j}$ com $g_1, \ldots, g_k \in G$, tomemos $s = g_1^{p^j} \cdots g_{k-1}^{p^j}$. Pela hipótese de indução e o caso $k = 1$, temos $s^p = 1$ e $\left(g_k^{p^j}\right)^p = 1$. Então, pela Proposição 1.6 e considerando que p é ímpar e $\gamma_2(G^{p^j}) \leq Z(G^{p^j})$, temos:

$$\begin{aligned} t^p &= \left(sg_k^{p^j}\right)^p = s^p \left(g_k^{p^j}\right)^p \left[g_k^{p^j}, s\right]^{\frac{p(p-1)}{2}} = \left[g_k^{p^j}, s\right]^{\frac{p(p-1)}{2}} \\ &= \left(\left[g_k^{p^j}, s\right]^p\right)^{\frac{p-1}{2}} = \left[g_k^{p^j}, s^p\right]^{\frac{p-1}{2}} = 1. \end{aligned}$$

Logo, provamos que $t = 1$. Portanto, por indução, podemos afirmar que $t^p = 1$ para todo $t \in G^{p^j}$. Logo, $\left(G^{p^j}\right)^p = \{1\}$, como desejado.

Agora vamos mostrar o seguinte:

Afirmação 2: Dados um p-grupo finito G e $j \in \mathbb{N}$, se $G^{p^j}\ p.e.\ G$, então $\left(G^{p^j}\right)^p = G^{p^{j+1}}$.

Coloquemos $H = G^{p^{j+1}}$ e consideramos o grupo G/H. Observamos que:

$$\left(\frac{G}{H}\right)^{p^{j+1}} = \frac{G^{p^{j+1}}H}{H} = \frac{H}{H}.$$

Além disso, como $H \leq G^{p^j}$ e $G^{p^j}\ p.e.\ G$,

$$\begin{aligned} \left[\left(\frac{G}{H}\right)^{p^j}, \frac{G}{H}\right] &= \left[\frac{G^{p^j}H}{H}, \frac{G}{H}\right] = \left[\frac{G^{p^j}}{H}, \frac{G}{H}\right] = \frac{\left[G^{p^j}, G\right]H}{H} \\ &\leq \frac{\left(G^{p^j}\right)^p H}{H} \cdot \frac{\left(G^{p^j}\right)^p H}{H} = \left(\frac{G^{p^j}}{H}\right)^p \\ &= \left(\left(\frac{G}{H}\right)^{p^j}\right)^p, \end{aligned}$$

provando que $(G/H)^{p^j}\ p.e.\ G/H$.

Assim, pela Afirmação 1, vemos que $\left((G/H)^{p^j}\right)^p = H/H$. Então, concluímos que $H/H = \left(\left(G^{p^j}\right)^p H\right)/H$, nos permitindo afirmar que $\left(G^{p^j}\right)^p \leq H = G^{p^{j+1}}$. É fácil ver que $G^{p^{j+1}} \leq \left(G^{p^j}\right)^p$ e, consequentemente, $G^{p^{j+1}} = \left(G^{p^j}\right)^p$, provando a afirmação.

Agora, estamos aptos a provar o resultado. Primeiro mostraremos por indução sobre $j \in \mathbb{N}$ que G^{p^j} é *powerfully embedded* em G. Para $j = 0$, é óbvio, uma vez que $G^{p^j} = G$. Agora, suponhamos que para algum $j \in \mathbb{N}$, temos que $G^{p^j}\ p.e.\ G$. Pela Afirmação 2,

é fato que $\left(G^{p^j}\right)^p = G^{p^{j+1}}$, e então G^{p^j} $p.e.$ G pelo Teorema 3.3. Provamos assim por indução que G^{p^j} $p.e.$ G, para todo $j \in \mathbb{N}$.

Agora, dado $j \in \mathbb{N}$, vamos provar por indução sobre $i \in \mathbb{N}$ que $\left(G^{p^j}\right)^{p^i} = G^{p^{i+j}}$. Para $i = 0$, o resultado é óbvio. Agora, suponhamos que o resultado é válido para algum $i \in \mathbb{N}$. Observamos que:

$$\left(G^{p^j}\right)^{p^{i+1}} \leq \left(\left(G^{p^j}\right)^{p^i}\right)^p = \left(G^{p^{i+j}}\right)^p,$$

e, como $G^{p^{i+j}}$ $p.e.$ G, pela Afirmação 2, vale $\left(G^{p^{i+j}}\right)^p = G^{p^{i+j+1}}$. Logo, $\left(G^{p^j}\right)^{p^{i+1}} \leq G^{p^{(i+1)+j}}$.

É fácil ver que $G^{p^{(i+1)+j}} \leq \left(G^{p^j}\right)^{p^{i+1}}$, nos permitindo concluir que $\left(G^{p^j}\right)^{p^{i+1}} = G^{p^{i+1+j}}$. Logo, por indução, provamos que para todo par $i, j \in \mathbb{N}$ a igualdade $\left(G^{p^j}\right)^{p^i} = G^{p^{i+j}}$ ocorre. □

O próximo lema analisa o grupo G/G^{p^2} quando G é um p-grupo *powerful* e utilizaremos tal estudo futuramente.

Lema 3.5. *Seja G um p-grupo finito powerful, com p ímpar. Então:*

(i) *G/G^{p^2} é nilpotente de classe no máximo 2;*

(ii) *$(g_1 \cdots g_n)^p G^{p^2} = g_1^p \cdots g_n^p G^{p^2}$, para todos $n \in \mathbb{N}^*$ e $g_1, \ldots, g_n \in G$.*

Demonstração. (i) Pelo Teorema 3.4,

$$[G, G, G] \leq [G^p, G] \leq (G^p)^p = G^{p^2},$$

e assim,

$$\left[\frac{G}{G^{p^2}}, \frac{G}{G^{p^2}}, \frac{G}{G^{p^2}}\right] = \frac{[G, G, G]\, G^{p^2}}{G^{p^2}} = \frac{G^{p^2}}{G^{p^2}}.$$

Portanto, G/G^{p^2} é nilpotente de classe no máximo 2.

(ii) Primeiro observamos que se $g, h \in G$, então $[h, g] \in G' \leq G^p$. Assim, como p é ímpar, pelo Teorema 3.4,

$$[h, g]^{\frac{p(p-1)}{2}} = \left([h, g]^{\frac{p-1}{2}}\right)^p \in (G^p)^p = G^{p^2}.$$

Logo, pela Proposição 1.6 (iv),

$$\begin{aligned}(gh)^p\, G^{p^2} &= \left(\left(gG^{p^2}\right)\left(hG^{p^2}\right)\right)^p = \left(gG^{p^2}\right)^p \left(hG^{p^2}\right)^p \left[hG^{p^2}, gG^{p^2}\right]^{\frac{p(p-1)}{2}} \\ &= \left(\left(g^p h^p\right) G^{p^2}\right)\left([h, g]^{\frac{p(p-1)}{2}} G^{p^2}\right) = \left(g^p h^p\right) G^{p^2},\end{aligned}$$

ou seja, $(gh)^p G^{p^2} = (g^p h^p) G^{p^2}$, para quaisquer $g, h \in G$. Agora, usando este fato, não é difícil mostrar, por indução sobre $n \geq 1$, que $(g_1 \cdots g_n)^p G^{p^2} = g_1^p \cdots g_n^p G^{p^2}$, para todos $g_1, \ldots, g_n \in G$.

□

Para o que segue, lembramos que o *subgrupo de Frattini* $\Phi(G)$ de um grupo finito G é a interseção de todos os subgrupos maximais de G. Além disso, $\Phi(G)$ consiste dos não-geradores de G e quando G é um p-grupo finito, podemos afirmar que $\Phi(G) = G'G^p$.

Proposição 3.6. *[28, pág. 488] Seja G um p-grupo finito powerful com p primo ímpar. Então $G^p = \{g^p \mid g \in G\}$.*

Demonstração. Vamos provar por indução sobre a ordem de G. Para $|G| = 1$, temos que é óbvio pois $G^p = \{1\}$. Agora, tomemos um p-grupo G *powerful* tal que o resultado é válido para todo grupo com ordem menor que $|G|$.

Dado $x \in G^p$, existem $g_1, \ldots, g_k \in G$ satisfazendo $x = g_1^p \cdots g_k^p$. Considerando $g = g_1 \ldots g_k$, pelo Lema 3.5, temos:

$$xG^{p^2} = (g_1^p \cdots g_k^p)\, G^{p^2} = (g_1 \cdots g_k)^p G^{p^2} = g^p G^{p^2},$$

ou seja, existe $a \in G^{p^2}$ tal que $x = g^p a$. Uma vez que, pelo Teorema 3.4, $G^{p^2} = (G^p)^p$, existem $b_1, \ldots, b_r \in G^p$ com $a = b_1^p \ldots b_r^p$.

Escrevendo $H = \langle g, G^p \rangle$, já que $x = g^p a = g^p b_1^p \ldots b_r^p$ teremos que $x \in H^p$. Vamos agora estudar dois casos complementares.

Se $H = G$, como G é um p-grupo finito e *powerful*, temos $\Phi(G) = G' \cdot G^p = G^p$. Logo, G^p é um grupo finito e seus elementos são não-geradores. Dessa forma, $G = \langle g \rangle$. Assim, a igualdade $G^p = \{a^p \mid a \in G\}$ é uma consequência do fato de G ser abeliano.

Agora, se $H < G$, vamos provar que H é *powerful*. Dados $u, v \in H = \langle g, G^p \rangle$, temos que $u = g^i s$ e $v = g^j t$ para $i, j \in \mathbb{Z}$ e $t, s \in G^p$. Pelo Teorema 3.4, é fato que $[G^p, G] \leq (G^p)^p \leq H^p$. Logo,

$$\begin{aligned}[u, v] &= \left[g^i s, g^j t\right] = \left[g^i, g^j t\right]^s \left[s, g^j t\right] = \left(\left[g^i, t\right] \left[g^i, g^j\right]^t\right)^s \left[s, g^j t\right] \\ &= \left[g^i, t\right]^s \left[s, g^j t\right] \in [G^p, G] \leq H^p.\end{aligned}$$

Pela arbitrariedade de $u, v \in H$, podemos afirmar que $H' \leq H^p$, isto é, H $p.e.$ G. Consequentemente, H é *powerful*. Além disso, como $|H| < |G|$, pela hipótese de indução,

$$H^p = \{h^p \mid h \in H\}.$$

Daí, de $x \in H^p$, existe $h \in H$ tal que $x = h^p$. Como tomamos qualquer $x \in G^p$, provamos o desejado.

Logo, em ambos os casos, o resultado é verdadeiro. □

A Proposição 3.6 pode ser estendida, como veremos a seguir.

Teorema 3.7. *Seja G um p-grupo finito powerful, com p um primo ímpar. Então, para cada $i \in \mathbb{N}$, temos que:*

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

Demonstração. Procederemos por indução sobre i. Para $i = 0$, é óbvio. Agora, vamos supor para algum $i \in \mathbb{N}$ temos $G^{p^i} = \{g^{p^i} \mid g \in G\}$.

Sendo G *powerful*, o Teorema 3.4 nos diz que G^{p^i} $p.e.$ G, ou seja, G^{p^i} é *powerful*. Com isso, pela Proposição 3.6, sabemos que:

$$G^{p^{i+1}} = \left(G^{p^i}\right)^p = \left\{y^p \;\middle|\; y \in G^{p^i}\right\} = \left\{\left(g^{p^i}\right)^p \;\middle|\; g \in G\right\} = \left\{g^{p^{i+1}} \;\middle|\; g \in G\right\},$$

como desejado. Provamos assim o que queríamos por indução sobre i. □

A seguir apresentaremos uma consequência imediata do último teorema.

Corolário 3.8. *Seja G um p-grupo finito powerful, com p um primo ímpar, e $exp(G) = p^n$. Para cada $k \in \mathbb{N}$, com $k \leq n$, temos que* $\exp\left(G^{p^k}\right) = p^{n-k}$.

3.2 p-Grupos Regulares

Nesta seção apresentaremos o conceito de p-grupo regular, bem como algumas de suas principais propriedades. Salvo menção contrária, os resultados desta seção podem ser encontrados no Capítulo 10 de [19].

Dado um p-grupo finito G com p primo, dizemos que G é *regular* se para quaisquer $a, b \in G$ existem $d_1, \ldots, d_k \in \gamma_2(\langle a, b\rangle)$ tais que:

$$(ab)^p = a^p b^p \prod_{i=1}^{k} d_i^p,$$

ou equivalentemente,

$$(ab)^p \equiv a^p b^p \pmod{\gamma_2(\langle x, y\rangle)^p}.$$

É fácil ver que todo subgrupo de um p-grupo finito regular G, é também regular. Além disso, se $H \triangleleft G$, então G/H também é regular.

Claramente todo p-grupo abeliano finito é regular, bem como os grupos finitos de expoente p. O resultado a seguir nos fornece uma outra classe de p-grupos regulares.

Lema 3.9. *Dado um p-grupo finito G, se a classe de nilpotência de G é menor que p, então G é regular.*

Ideia da demonstração. Basta usar o Teorema 2.6 junto com o fato de $\gamma_p(H) \leq \gamma_p(G) = \{1\}$. □

Dado um p-grupo G e $i \in \mathbb{N}$, vamos adotar a notação $\Omega_i(G)$ para representar o subgrupo $\left\langle g \in G \mid g^{p^i} = 1 \right\rangle$. Não é difícil verificar que esse subgrupo é característico em G e, portanto, normal.

Lema 3.10. *Seja G um p-grupo regular. Se $x, y \in G$ e $x^p = y^p = 1$, então $(xy)^p = 1$. Consequentemente, $\Omega_1(G) = \{g \in G \mid g^p = 1\}$.*

Demonstração. Vamos provar esse resultado por indução sobre $|G|$. Se $G = \{1\}$, já temos o desejado. Agora, seja G um p-grupo regular tal que o resultado é válido para todo grupo com ordem menor que $|G|$. Se G é abeliano, já temos o que queremos. Agora, se $\langle x, y\rangle < G$, basta aplicarmos a hipótese de indução. Assim, podemos assumir que G não é abeliano e $G = \langle x, y\rangle$.

Sejam $L = x^G = \langle x^g \mid g \in G\rangle$ e U um subgrupo maximal de G com $x \in U$. Notemos que tal grupo existe pelo Lema de Zorn, pois G é finito e $G \neq \langle x\rangle$ já que G não é abeliano. Como G é nilpotente, temos que $U \triangleleft G$, e assim $L \leq U < G$.

Como L também é regular, da hipótese de indução segue que $\Omega_1(L) = \{u \in L \mid u^p = 1\}$. Agora, de $x^g \in \Omega_1(L)$ para todo $g \in G$, resulta $L \leq \Omega_1(L)$, isto é, L tem expoente divisor de p. Uma vez que $[x, y] = x^{-1}x^y$ com x e x^y em L, temos $[x, y]^p = 1$. De acordo com a Proposição 1.8, o subgrupo derivado G' é gerado pelos conjugados $[x, y]^g$ de $[x, y]$, e todos eles têm ordem p. Devido a $G' < G$, pois G é nilpotente, temos $c^p = 1$ para todo c em G'. Agora, a regularidade de G nos diz que existem $d_1, \ldots, d_k \in G'$ tais que:

$$(xy)^p = x^p y^p \prod_{i=1}^{k} d_i^p = 1,$$

como queríamos demonstrar. □

O Lema 3.10 pode ser estendido para os demais termos da cadeia:

$$\{1\} = \Omega_0(G) \leq \Omega_1(G) \leq \cdots \leq \Omega_n(G) \leq \cdots,$$

conforme nos diz o próximo resultado.

Teorema 3.11. *Sejam G um p-grupo regular e $k \in \mathbb{N}$. Para todos $x, y \in G$, se $x^{p^k} = y^{p^k} = 1$, então $(xy)^{p^k} = 1$. Consequentemente, $\Omega_k(G) = \{g \in G \mid g^{p^k} = 1\}$.*

Demonstração. Provaremos esse resultado por indução sobre k. Para $k = 0$, o resultado é óbvio e para $k = 1$, segue diretamente do Lema 3.10.

Agora, tomemos $k \in \{2, 3, \dots\}$ de modo que o enunciado seja verdadeiro para todo natural menor que k. A partir de $x^{p^k} = y^{p^k} = 1$, segue que $x^p, y^p \in \Omega_{k-1}(G)$. Definindo $\overline{x} = x\Omega_{k-1}(G)$ e $\overline{y} = y\Omega_{k-1}(G)$, temos que $\overline{x}^p = \overline{y}^p = \overline{1}$. Aplicando o Lema 3.10 no grupo $\frac{G}{\Omega_{k-1}(G)}$, vemos que $(\overline{xy})^p = \overline{1}$. Isso implica que $(xy)^p \in \Omega_{k-1}(G)$ e, por indução, $\Omega_{k-1}(G) = \{g \in G \mid g^{p^{k-1}} = 1\}$. Assim, $(xy)^{p^k} = ((xy)^p)^{p^{k-1}} = 1$, como desejado. □

Dado um p-grupo regular G, o próximo lema nos mostra que o conjunto $\{g \in G \mid g^p = 1\}$ é um subgrupo de G.

Lema 3.12. *Seja G um p-grupo regular e $x, y \in G$. Então, $x^p = y^p$ se, e somente se, $(xy^{-1})^p = 1$.*

Demonstração. Vamos proceder por indução sobre $|G|$. Para $G = \{1\}$ é óbvio. Agora, seja G um p-grupo regular tal que o resultado acontece para todo p-grupo com ordem menor que $|G|$. Se G é abeliano, já temos o que queríamos. Agora, se $\langle x, y\rangle < G$, basta aplicarmos a hipótese de indução. Assim, podemos assumir que G não é abeliano e $G = \langle x, y\rangle$. Coloquemos $z = [x, y]$.

Primeiro vamos mostrar que se $x^p = y^p$, então $(xy^{-1})^p = 1$.

Como $x^p = y^p$, temos $[x^p, y] = [y^p, y] = 1$ e, então,

$$x^p = y^{-1}x^p y = \left(y^{-1}xy\right)^p = (xz)^p .$$

Se tivermos que $\langle x, G'\rangle = G$, então de $G' \leq G^pG' = \Phi(G)$, obtemos $G = \langle x\rangle$, contrariando o fato que G é não abeliano. Assim, $\langle x, z\rangle \leq \langle x, G'\rangle < G$. Pela hipótese de indução, como $x^p = (xz)^p$, segue que $(xzx^{-1})^p = 1$. Assim, $z^p = 1$.

Pela Proposição 1.8, os elementos z^g ($g \in G$) de ordem divisora de p geram todo G'. Assim, para todo $g \in G$, temos que $z^g \in \Omega_1(G')$, o que implica que $G' \leq \Omega_1(G')$, isto é $G' = \Omega_1(G')$. Portanto, G' tem expoente divisor de p.

Como G é regular, existem $d_1, \dots, d_k \in \gamma_2(\langle x, y^{-1}\rangle) = \gamma_2(\langle x, y\rangle)G'$ tais que:

$$\left(xy^{-1}\right)^p = x^p y^{-p} \prod_{i=1}^{k} d_i^p = x^p y^{-p} = 1.$$

Agora, vamos provar a recíproca.

Se $(xy^{-1})^p = 1$, então $(yx^{-1})^p = \left((xy^{-1})^{-1}\right)^p = 1$ e $(y^{-1}x)^p = y^{-1}(xy^{-1})^p y = 1$. Assim, o Teorema 3.11 nos diz que $[y, x^{-1}]^p = (y^{-1}xyx^{-1})^p = 1$. Como $G = \langle x, y\rangle = \langle x, y^{-1}\rangle$, a Proposição 1.8 nos assegura que G' é gerado pelos elementos da forma $[y, x^{-1}]^g$, com $g \in G$. Além disso, para todo $g \in G$, temos que $[y, x^{-1}]^g \in \Omega_1(G')$. Logo, $G' = \Omega_1(G') = \{g \in G' \mid g^p = 1\}$, fazendo com que o expoente de G' seja um divisor de p. Agora, sendo G regular, existem $d_1, \ldots, d_k \in \gamma_2(\langle x, y^{-1}\rangle) = G'$ com:

$$1 = \left(xy^{-1}\right)^p = x^p y^{-p} \prod_{i=1}^{k} d_i^p = x^p y^{-p},$$

ou equivalentemente, $x^p = y^p$.

Assim, provamos a equivalência desejada. □

Como veremos a seguir, podemos generalizar o último lema para um potência qualquer de p.

Proposição 3.13. *Sejam G um p-grupo regular, $k \in \mathbb{N}$ e $x, y \in G$. Então, $x^{p^k} = y^{p^k}$ se, e somente se, $(xy^{-1})^{p^k} = 1$.*

Demonstração. Procederemos por indução sobre k. Para $k = 0$, é óbvio. Se tomarmos $k = 1$, o resultado segue diretamente do Lema 3.12.

Tomemos agora $k \in \{2, 3, \ldots\}$ tal que o resultado é válido para $k - 1$. Vamos mostrar a equivalência:

$$x^{p^k} = y^{p^k} \iff \left(xy^{-1}\right)^{p^k} = 1.$$

Se $x^{p^k} = y^{p^k}$, então $(x^p)^{p^{k-1}} = (y^p)^{p^{k-1}}$. Pela hipótese de indução, $(x^p y^{-p})^{p^{k-1}} = 1$, ou seja, $x^p y^{-p} \in \Omega_{k-1}(G)$. Em outras palavras $(x\Omega_{k-1}(G))^p = (y\Omega_{k-1}(G))^p$. Pelo Lema 3.12, como $G/\Omega_{k-1}(G)$ é regular, podemos afirmar que:

$$1\Omega_{k-1}(G) = \left((x\Omega_{k-1}(G))(y\Omega_{k-1}(G))^{-1}\right)^p = \left(xy^{-1}\right)^p \Omega_{k-1}(G).$$

Logo, pelo Teorema 3.11, $(xy^{-1})^p \in \Omega_{k-1}(G) = \{g \in G \mid g^{p^{k-1}} = 1\}$, ou seja,

$$\left(xy^{-1}\right)^{p^k} = \left(\left(xy^{-1}\right)^p\right)^{p^{k-1}} = 1. \tag{3.1}$$

Reciprocamente, se $\left((xy^{-1})^p\right)^{p^{k-1}} = (xy^{-1})^{p^k} = 1$, então $(xy^{-1})^p \in \Omega_{k-1}(G)$. Assim,

$$\left((x\Omega_{k-1}(G))(y\Omega_{k-1}(G))^{-1}\right)^p = \left(xy^{-1}\right)^p \Omega_{k-1}(G) = \Omega_{k-1}(G).$$

Portanto, aplicando o Lema 3.12 no grupo $\frac{G}{\Omega_{k-1}(G)}$, obtemos que $(x\Omega_{k-1}(G))^p = (y\Omega_{k-1}(G))^p$, isto é, $x^p y^{-p} \in \Omega_{k-1}(G)$. Pelo Teorema 3.11, sabemos que $\Omega_{k-1}(G) = \{g \in$

$G \mid g^{p^{k-1}} = 1\}$. Portanto, $(x^p y^{-p})^{p^{k-1}} = 1$. A hipótese de indução nos diz então que $(x^p)^{p^{k-1}} = (y^p)^{p^{k-1}}$, ou seja, $x^{p^k} = y^{p^k}$.

Provamos assim a equivalência desejada por indução sobre k. □

Embora não exigimos que G seja um p-grupo regular no próximo resultado, usaremos alguns resultados vistos acima em sua demonstração.

Teorema 3.14. *[29, pág, 370] Seja G um p-grupo finito de classe menor ou igual a p. Dados $x, y \in G$ e $n \in \mathbb{N}$, as seguintes afirmações são equivalentes:*

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

(ii) $[x, y]^{p^n} = 1$;

(iii) $[x, y^{p^n}] = 1$.

Demonstração. Primeiro provaremos a equivalência de (i) e (ii). Tomando $H = \langle x, G' \rangle$, pela Proposição 1.11, temos que $\gamma_c(H) \leq \gamma_{c+1}(G) = \{1\}$ fazendo com que H seja um p grupo com classe de nilpotência menor ou igual a $c - 1 \leq p - 1$. Portanto, pelo Lema 3.9, vemos que H é regular. Assim, pela Proposição 3.13, temos as equivalências:

$$\begin{aligned}
[x^{p^n}, y] = 1 &\iff x^{p^n} = y^{-1} x^{p^n} y \\
&\iff x^{p^n} = \left(y^{-1} x y\right)^{p^n} \\
&\iff \left(x \left(y^{-1} x y\right)^{-1}\right)^{p^n} = 1 \\
&\iff \left(x y^{-1} x^{-1} y\right)^{p^n} = 1 \\
&\iff [x^{-1}, y]^{p^n} = 1 \\
&\iff \left([x, y]^{x^{-1}}\right)^{-p^n} = 1 \\
&\iff \left([x, y]^{p^n}\right)^{-x^{-1}} = 1 \\
&\iff [x, y]^{p^n} = 1,
\end{aligned}$$

provando a equivalência desejada.

Falta agora vermos que (ii) é equivalente a (iii). Usando a equivalência já provada, temos:

$$[x, y^{p^n}] = 1 \iff [y^{p^n}, x] = 1 \iff [y, x]^{p^n} = 1 \iff [x, y]^{p^n} = 1,$$

como queríamos. Assim, provamos o desejado. □

CAPÍTULO 4

PRODUTO TENSORIAL NÃO ABELIANO DE GRUPOS

Neste capítulo apresentamos um breve estudo sobre produto tensorial não abeliano de grupos e, em especial, sobre o produto exterior não abeliano de grupos. Veremos aqui uma importante relação entre o quadrado exterior não abeliano de um grupo G e o subgrupo derivado de um grupo de recobrimento total de G (Teorema 4.17), a qual será fundamental na obtenção de cotas superiores para o multiplicador de Schur que será realizado no próximo capítulo.

4.1 Definição e Propriedades

Sejam G e H grupos nos quais cada um age à direita sobre o outro. Adicionalmente, considere as ações à direita de G e H sobre si mesmos por conjugação. Assim, temos uma ação à direita bem definida do produto livre $G * H$ sobre G e outra sobre H. Dizemos que as ações de G sobre H e de H sobre G são *compatíveis* se para quaisquer $a, b \in G$ e $x, y \in H$, tivermos:

$$a^{(x^b)} = \left(\left(a^{b^{-1}}\right)^x\right)^b, \tag{4.1}$$

$$x^{(a^y)} = \left(\left(x^{y^{-1}}\right)^a\right)^y. \tag{4.2}$$

Se dois grupos G e H agem um sobre o outro compativelmente, Brown e Loday [10, 11] definiram o *produto tensorial não abeliano* de G e H como sendo o grupo gerado por todos os elementos da forma $a \otimes x$, com $a \in G$ e $x \in H$, que satisfaz:

$$(ab) \otimes x = \left(a^b \otimes x^b\right)(b \otimes x) \quad \text{e} \quad a \otimes (xy) = (a \otimes y)\left(a^y \otimes x^y\right),$$

para arbitrários $a, b \in G$ e $x, y \in H$. Tal grupo será denotado por $G \otimes H$. Portanto,

$$G \otimes H = \langle \{a \otimes x \mid a \in G, x \in H\} \mid R \rangle,$$

em que:

$$R = \left\{ ((ab) \otimes x)^{-1} \left(a^b \otimes x^b\right) (b \otimes x), (a \otimes (xy))^{-1} (a \otimes y) (a^y \otimes x^y) \middle| a, b \in G \text{ e } x, y \in H \right\}.$$

Quando $G = H$ e todas as ações são tomadas como sendo a conjugação, então as ações são compatíveis. Assim, o produto tensorial $G \otimes G$ fica bem definido e o chamaremos de *quadrado tensorial não abeliano* de G.

Os geradores do produto tensorial não abeliano $G \otimes H$ podem ser vistos, de certa forma, como abstrações de comutadores, uma vez que em $G \otimes H$, valem as igualdades:

$$(ab) \otimes x = \left(a^b \otimes x^b\right) (b \otimes x), \tag{4.3}$$

$$a \otimes (xy) = (a \otimes y) (a^y \otimes x^y), \tag{4.4}$$

os quais lembram as identidades de comutadores:

$$[ab, x] = [a, x]^b [b, x] \quad \text{e} \quad [a, xy] = [a, y][a, x]^y.$$

Definição 4.1. Sejam G e H grupos agindo compativelmente um sobre o outro e L um grupo qualquer. Dizemos que uma aplicação $\theta : G \times H \to L$ é uma *biderivação* se para quaisquer $a, b \in G$ e $x, y \in H$ tivermos:

$$(ab, x)\theta = (a^b, x^b)\theta(b, x)\theta, \tag{4.5}$$

$$(a, xy)\theta = (a, y)\theta(a^y, x^y)\theta. \tag{4.6}$$

Usando as relações definidoras de $G \otimes H$, facilmente se verifica que se G e H são grupos agindo compativelmente um sobre o outro, então a aplicação:

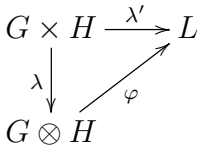
$$\begin{array}{rccc} \lambda : & G \times H & \longrightarrow & G \otimes H \\ & (a, x) & \longmapsto & a \otimes x \end{array},$$

é uma biderivação.

No que segue, salvo menção contrária, G e H são grupos que agem compativelmente um sobre o outro.

Usando o Teste da Substituição, podemos ver que para o produto tensorial não abeliano, a Propriedade Universal é verdadeira, mais especificamente, se L é um grupo e existe uma biderivação $\lambda' : G \times H \to L$, então existe um único homomorfismo

$\varphi : G \otimes H \to L$ que faz o diagrama



comutar, ou seja, tal que $(a \otimes x)\varphi = (a, x)\lambda'$, para todos $a \in G$, $x \in H$.

A seguir, apresentaremos alguns resultados devidos a R. Brown, D. L. Johnson e E. F. Robertson [9]. Suas provas serão omitidas, mas elas podem ser facilmente encontradas em outras dissertações, como [34], [35], [42], [27] e [12].

Proposição 4.2. *Os grupos G e H agem sobre $G \otimes H$ de maneira que para todos $a, b \in G$ e $x, y \in H$,*

$$(b \otimes x)^a = b^a \otimes x^a \text{ e } (a \otimes y)^x = a^x \otimes y^x.$$

Da Proposição 4.2, segue que temos uma ação do produto livre $G * H$ sobre $G \otimes H$ dada por:

$$(a \otimes x)^t = a^t \otimes x^t,$$

para qualquer $a \otimes x \in G \otimes H$ e $t \in G * H$.

Proposição 4.3. *Existe um único isomorfismo $\theta : G \otimes H \longrightarrow H \otimes G$ tal que para todos $a \in G$ e $x \in H$:*

$$(a \otimes x)\theta = (x \otimes a)^{-1}.$$

Na próxima proposição, veremos que sob certas condições, podemos a partir de homomorfismos de grupos $\alpha : G \to A$ e $\beta : H \to B$ construir um homomorfismo $\alpha \otimes \beta : G \otimes H \to A \otimes B$ em que $(a \otimes x)(\alpha \otimes \beta) = (a)\alpha \otimes (x)\beta$ para quaisquer $a \in G$ e $x \in H$.

Proposição 4.4. *Sejam A e B grupos que agem compativelmente um sobre o outro e suponha que $\alpha : G \to H$ e $\beta : H \to B$ são homomorfismos que preservam ações, no sentido de que $(x^a)\beta = ((x)\beta)^{(a)\alpha}$ e $(a^x)\alpha = ((a)\alpha)^{(x)\beta}$ para quaisquer $a \in G$ e $x \in H$. Então existe um único homomorfismo $\alpha \otimes \beta : G \otimes H \to A \otimes B$ tal que $(a \otimes x)\alpha \otimes \beta = (a)\alpha \otimes (b)\beta$ para todos $a \in G$ e $x \in H$. Ainda mais, se α e β forem sobrejetoras, então $\alpha \otimes \beta$ também será.*

No que segue, vamos escrever u^{-a} e u^{-x} para representar, respectivamente, $(u^{-1})^a = (u^a)^{-1}$ e $(u^{-1})^x = (u^x)^{-1}$, com $u \in G \cup H$ e $a, x \in G * H$.

Proposição 4.5. *Sejam G e H grupos que agem um sobre o outro compativelmente. Para quaisquer $a, b \in G$ e $x, y \in H$, as seguintes identidades são válidas:*

(i) $a \otimes 1_H = 1_{G\otimes H} = 1_G \otimes x$;

(ii) $(a^{-1} \otimes x)^a = (a \otimes x)^{-1} = (a \otimes x^{-1})^x$;

(iii) $(a \otimes x)^{-1}(b \otimes y)(a \otimes x) = (b \otimes y)^{[a,x]} = (b \otimes y)^{a^{-1}a^x} = (b \otimes y)^{x^{-a}x}$;

(iv) $(a \otimes x)(b \otimes y)(a \otimes x)^{-1} = (b \otimes y)^{[x,a]} = (b \otimes y)^{x^{-1}x^a} = (b \otimes y)^{a^{-x}a}$;

(v) $(a^{-1}a^x) \otimes y = (a \otimes x)^{-1}(a \otimes x)^y$;

(vi) $b \otimes (x^{-a}x) = (a \otimes x)^{-b}(a \otimes x)$;

(vii) $[a \otimes x, b \otimes y] = (a^{-1}a^x) \otimes \left(y^{-b}y\right)$;

$(viii)$ *Se* $x^a = x$, *então para todo* $n \in \mathbb{N}$, *temos que* $(a \otimes x)^n = a^n \otimes x$.

A Proposição 4.5 (ii) nos permite provar o seguinte lema que nos auxiliará em futuras demonstrações.

Lema 4.6. *Dados dois grupos G e H que agem um sobre o outro compativelmente, todo elemento de $G \otimes H$ pode ser escrito como produto de um número finito de elementos da forma $g \otimes h$, com $g \in G$ e $h \in H$.*

Demonstração. Pela definição de $G \otimes H$, dado $t \in G \otimes H$, existem $g_1, \ldots, g_k \in G$, $h_1, \ldots, h_k \in H$ e $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$ tais que $t = (g_1 \otimes h_1)^{\varepsilon_1} \cdots (g_k \otimes h_k)^{\varepsilon_k}$. Para cada $i \in I_k$, se $\varepsilon_i = -1$, note que:

$$(g_i \otimes h_i)^{\varepsilon_i} = (g_i \otimes h_i)^{-1} = \left(g_i^{-1} \otimes h_i\right)^{g_i} = \left(g_i^{-1}\right)^{g_i} \otimes h_i^{g_i},$$

e, portanto, trocando $(g_i \otimes h_i)^{\varepsilon_i}$ por $\left(g_i^{-1}\right)^{g_i} \otimes h_i^{g_i}$ na decomposição de t para todo $i \in I_k$ com $\varepsilon_i = -1$, temos t escrito na forma desejada. □

Definição 4.7. Sejam P e M grupos. Dizemos que um homomorfismo de grupos $\mu : M \longrightarrow P$ juntamente com uma ação de P sobre M é um *módulo cruzado* se as seguintes condições são satisfeitas:

$$(m^p)\mu = p^{-1}((m)\mu)p; \tag{4.7}$$

$$(m_1)^{(m)\mu} = m^{-1}m_1m, \tag{4.8}$$

para todos $p \in P$ e $m, m_1 \in M$.

Lema 4.8. *Sejam P e M grupos. Se $\mu : M \longrightarrow P$ é um módulo cruzado, então as seguintes afirmações são verdadeiras:*

(i) $Ker(\mu) \leq Z(M)$;

(ii) $Im(\mu) \triangleleft P$.

Demonstração. Dado $m \in Ker(\mu)$, para todo $x \in M$ vale:

$$m^{-1}xm = x^{(m)\mu} = x.$$

Pela arbitrariedade de $x \in M$, temos que $m \in Z(M)$. Como tomamos qualquer $m \in Ker(\mu)$, provamos que $Ker(\mu) \leq Z(G)$.

Agora, tomemos $r \in Im(\mu)$ e $s \in P$ quaisquer. Existe então $m \in M$ tal que $(m)\mu = r$. Assim,

$$(m^s)\,\mu = s^{-1}(m)\mu s = s^{-1}rs,$$

garantindo que $s^{-1}rs \in Im(\mu)$. Portanto, $Im(\mu) \triangleleft P$. □

Proposição 4.9. *[11] Sejam G e H grupos que agem compativelmente entre si. Então:*

(i) *Existem homomorfismos de grupos $\lambda : G \otimes H \to G$ e $\mu : G \otimes H \to H$ tais que $(g \otimes h)\lambda = g^{-1}g^h$ e $(g \otimes h)\mu = h^{-g}h$, para todos $g \in G$ e $h \in H$;*

(ii) *Os homomorfismos λ e μ, juntamente com as ações de G e H sobre $G \otimes H$, definidas na Proposição 4.2, são módulos cruzados;*

(iii) *Se $g \in G$, $h \in H$ e $t \in G \otimes H$, então $(t)\lambda \otimes h = t^{-1}t^h$ e $g \otimes (t)\mu = t^{-g}t$;*

(iv) *Para $t, s \in G \otimes H$, temos que $(t)\lambda \otimes (s)\mu = [t, s]$;*

(v) *As ações de G sobre $Ker(\mu)$ e de H sobre $Ker(\lambda)$ são triviais.*

Dados dois grupos G e H de modo que H age em G, tomamos o subgrupo $D_H(G) = \langle g^{-1}g^h \mid g \in G, h \in H \rangle$, o qual chamaremos de *subgrupo derivativo* de G sob a ação de H. Assim, se G e H agem entre si compativelmente, ao considerarmos os homomorfismos $\lambda : G \otimes H \to G$ e $\mu : G \otimes H \to H$, teremos que $D_H(G) = Im(\lambda)$ e $D_G(H) = Im(\mu)$.

Teorema 4.10. *[13, Pág. 402] Sejam G e H grupos que agem compativelmente um sobre o outro. Se $D_H(G)$ ou $D_G(H)$ é nilpotente de classe c, então $G \otimes H$ é nilpotente de classe no mínimo c e no máximo $c + 1$. Caso $D_H(G)$ ou $D_H(G)$ seja solúvel, então $G \otimes H$ também será solúvel.*

Demonstração. Suponha que $D_H(G)$ é nilpotente de classe c. Tomando $A = Ker(\lambda)$, temos a seguinte extensão central:

$$1 \longrightarrow A \xrightarrow{inc} G \otimes H \xrightarrow{\lambda} D_H(G) \longrightarrow 1\ .$$

Com isso,

$$\{1\} = \gamma_{c+1}(D_H(G)) \cong \gamma_{c+1}\left(\frac{G \otimes H}{A}\right) = \frac{\gamma_{c+1}(G \otimes H)A}{A},$$

fazendo com que $\gamma_{c+1}(G \otimes H) \leq A$. Logo,

$$\gamma_{c+2}(G \otimes H) = [\gamma_{c+1}(G \otimes H), G \otimes H] \leq [A, G \otimes H] = \{1\}.$$

Portanto, $G \otimes H$ é nilpotente de classe no máximo $c+1$. Se d é a classe de nilpotência de $G \otimes H$, temos:

$$\{1\} = \gamma_{d+1}\left(\frac{G \otimes H}{A}\right) \cong \gamma_{d+1}(D_H(G)),$$

e isso nos diz que $d \geq c$, como queríamos. A prova para o caso em que $D_G(H)$ é nilpotente, segue de forma análoga.

Agora, suponha sem perda de generalidade que $D_H(G)$ é solúvel, então $(G \otimes H)/A$ também será. Uma vez que A é abeliano, segue que $G \otimes H$ é solúvel. □

4.2 O Quadrado Tensorial Não Abeliano

Nesta seção apresentaremos o quadrado tensorial não abeliano definido por Brown, Johnson e Robertson em [9]. Uma importante característica desse grupo é sua relação com o multiplicador de Schur, que foi provada por Miller [31].

O quadrado tensorial não abeliano $G \otimes G$ de um grupo G é um caso particular do produto tensorial $G \otimes H$ de dois grupos G e H com $G = H$ e todas as ações como sendo a conjugação. Segue de imediato pelas propriedades dos comutadores que a seguinte aplicação é uma biderivação:

$$\begin{array}{rccc} [\cdot,\cdot]: & G \times G & \longrightarrow & G \\ & (g,h) & \longmapsto & [g,h] \end{array}.$$

Sendo $[\cdot,\cdot]$ uma biderivação, a Propriedade Universal garante a existência de um homomorfismo de grupos:

$$\begin{array}{rccc} \kappa: & G \otimes G & \longrightarrow & G \\ & g \otimes h & \longmapsto & [g,h] \end{array}.$$

Vamos denotar por $J_2(G)$ o núcleo do homomorfismo κ. Notemos que κ é um caso particular do homomorfismo λ definido na seção anterior (Veja Proposição 4.9 (i)). Com isso, temos as seguintes propriedades que seguem da Proposição 4.9.

Proposição 4.11. *Dado um grupo G, temos que $J_2(G)$ é um subgrupo central de $G \otimes G$ e G age trivialmente sobre $J_2(G)$.*

Em 1950, o matemático Whitehead introduziu em [43] um importante grupo para essa teoria, o qual é denotado por $\Gamma(G)$ e é chamado de *funtor quadrático de Whitehead*. Sua relevância é mostrada através de um homomorfismo que veremos no Teorema 4.13.

Definição 4.12. Dado um grupo abeliano (aditivo) A, $\Gamma(A)$ é o grupo gerado por todos os símbolos $\gamma(a)$ com $a \in A$ sujeito às seguintes relações:

$$\gamma(-a) = \gamma(a); \tag{4.9}$$

$$\gamma(a+b+c) + \gamma(a) + \gamma(b) + \gamma(c) = \gamma(a+b) + \gamma(b+c) + \gamma(a+c) \tag{4.10}$$

para todos os elementos $a, b, c \in A$.

Algumas propriedades seguem direto da definição, como por exemplo:

(i) $\gamma(0)$ é o elemento neutro de $\Gamma(A)$. Isso é obtido de (4.10) fazendo $a = b = c = 0$.

(ii) $\gamma(a) + \gamma(b) = \gamma(b) + \gamma(a)$, para todos $a, b \in A$.

Com efeito, colocando $c = 0$ em (4.10), obtemos:

$$\gamma(a+b+0) + \gamma(a) + \gamma(b) + \gamma(0) = \gamma(a+b) + \gamma(b+0) + \gamma(a+0),$$

implicando que $\gamma(a) + \gamma(b) = \gamma(b) + \gamma(a)$.

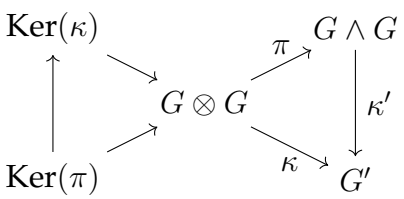
A observação (ii) nos diz que $\Gamma(A)$ é um grupo abeliano. A seguir, veremos que existe uma relação entre o funtor quadrático de Whitehead e o quadrado tensorial não abeliano.

Teorema 4.13. *[11, pág. 316] Existe um homomorfismo $\psi : \Gamma(G^{ab}) \longrightarrow G \otimes G$ tal que $(\gamma(\overline{g}))\psi = g \otimes g$, onde $\overline{g}$ denota a classe de g módulo G'.*

Fonte da demonstração. Ver [42, Proposição 3.17, pág. 46]. □

Notemos que a aplicação definida no Teorema 4.13 satisfaz $Im(\psi) \leq J_2(G)$ e, sendo $J_2(G)$ um subgrupo central de $G \otimes G$, $Im(\psi) \triangleleft G \otimes G$. Daí, o grupo quociente $\frac{G \otimes G}{Im(\psi)}$ faz sentido, o qual será chamado *quadrado exterior não abeliano* de G e denotado por $G \wedge G$.

Notemos que temos o seguinte diagrama:



Assim, pelo Teorema 1.15, existe um homomorfismo

$$\kappa' : G \wedge G \longrightarrow G'$$

tal que $\pi \circ \kappa' = \kappa$, onde $\pi : G \otimes G \longrightarrow G \wedge G$ é a projeção natural.

Com a notação acima, Miller mostrou em [31] a seguinte relação entre o quadrado exterior não abeliano e o multiplicador de Schur.

Teorema 4.14. $Ker(\kappa') \cong M(G)$.

Consideremos $i : J_2(G) \longrightarrow G \otimes G$ a aplicação inclusão e $\beta = i \circ \pi \circ \alpha^{-1}$, onde α é o isomorfismo de $M(G)$ sobre $Ker(\kappa')$. Não é difícil verificar que a aplicação β é sobrejetora. Com isso, temos o seguinte diagrama comutativo com linhas exatas e extensões centrais como colunas.

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
\Gamma(G^{ab}) & \xrightarrow{\psi} & J_2(G) & \xrightarrow{\beta} & M(G) & \longrightarrow & 1 \\
\| & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \alpha} & & \\
\Gamma(G^{ab}) & \xrightarrow{\psi} & G \otimes G & \xrightarrow{\pi} & G \wedge G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} & & \\
 & & G' & \xrightarrow[=]{} & G' & & \\
 & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & &
\end{array}$$

Whitehead [43] mostrou que se A é um grupo abeliano finito, então $\Gamma(A)$ também é finito. A demonstração desse fato também pode ser vista em [34, Corolário 7.10, pág. 21]

Dessa forma, se G é um grupo finito, então G', $\Gamma(G^{ab})$ e $M(G)$ são finitos. Assim, da segunda coluna do diagrama anterior segue a finitude de $G \wedge G$ e, com isso, da segunda linha do mesmo diagrama concluímos que $G \otimes G$ é finito. Observamos que, em [15], Ellis provou que dados grupos G e H finitos, temos que $G \otimes H$ é finito.

Existem grupos infinitos cujo produto tensorial não abeliano é finito. Assim, é interessante buscar propriedades de grupos que garantem que seu produto tensorial não abeliano é finito. Por exemplo, se considerarmos dois grupos G e H que agem compativelmente entre si, os matemáticos Donadze, Ladra e Thomas [13] provaram que se G é um grupo finitamente gerado, H é finito e H age trivialmente em G, então $G \otimes H$ é finito. Um estudo sobre condições de finitude para o produto tensorial não abeliano

de grupos também foi realizado por Bastos, Nakaoka e Rocco [6]. Eles mostraram que $G \otimes H$ é finito se, e somente se, o conjunto $\{g \otimes h \mid g \in G, h \in H\}$ é finito. Os autores ainda provaram que dados dois grupos finitamente gerados G e H que agem compativelmente um sobre o outro, se H é periódico e $D_G(H), D_H(G)$ são finitos, então $G \otimes H$ é finito.

A partir de agora, vamos ligar dois conceitos já estudados. Vamos ver uma relação entre um grupo de recobrimento total de um grupo G e o quadrado tensorial não abeliano $G \wedge G$. Mas, para isso, necessitamos dos seguintes dois resultados.

Proposição 4.15. *[9, pág. 182] Seja G um grupo e:*

$$1 \longrightarrow A \xrightarrow{i} K \xrightarrow{\pi} G \longrightarrow 1 \ ,$$

uma extensão central. Então, existe um homomorfismo $\xi : G \otimes G \to K$ tal que $\xi \circ \pi = \kappa$, onde κ é o homomorfismo definido na página 49.

Demonstração. Como π é um homomorfismo sobrejetor, para cada $g \in G$, existe $k_g \in K$ tal que $\pi(k_g) = g$. Considere a aplicação:

$$\begin{array}{rccc} \phi: & G \times G & \longrightarrow & K \\ & (g,h) & \longmapsto & [k_g, k_h] \end{array} ,$$

onde $(k_g)\pi = g$ e $(k_h)\pi = h$. Vamos mostrar que ϕ está bem definida. Dado $(g,h) \in G \times G$, tomemos $k_g^{(1)}, k_g^{(2)}, k_h^{(1)}, k_h^{(2)}$ tais que $\left(k_g^{(1)}\right)\pi = g = \left(k_g^{(2)}\right)\pi$ e $\left(k_h^{(1)}\right)\pi = h = \left(k_h^{(2)}\right)\pi$. Portanto, $k_g^{(1)}\left(k_g^{(2)}\right)^{-1} \in Ker(\pi)$, fazendo com que $k_g^{(2)}\left(k_g^{(1)}\right)^{-1} \in Z(K)$. De modo análogo, $k_h^{(2)}\left(k_h^{(1)}\right)^{-1} \in Z(K)$. Portanto,

$$\left[k_g^{(1)}, k_h^{(1)}\right] = \left[k_g^{(2)}\left(k_g^{(1)}\right)^{-1} k_g^{(1)}, k_h^{(2)}\left(k_h^{(1)}\right)^{-1} k_h^{(1)}\right] = \left[k_g^{(2)}, k_h^{(2)}\right],$$

provando que ϕ está bem definida.

Vamos mostrar agora que ϕ é uma biderivação. Dado $g, h, r \in G \times G$, sejam $k_g, k_h, k_r \in K$ tais que $(k_g)\pi = g$, $(k_h)\pi = h$ e $(k_r)\pi = r$. Logo, $(k_g k_h)\pi = gh$, $\left((k_g)^{k_h}\right)\pi = g^h$ e $\left((k_r)^{k_h}\right)\pi = r^h$. Assim,

$$(gh, r)\phi = [k_g k_h, k_r] = \left[k_g^{k_h}, k_r^{k_h}\right][k_h, k_r] = \left(g^h, r^h\right)\phi(h, r)\phi.$$

De modo análogo se prova que $(r, gh)\phi = (r, h)\phi\left(r^h, g^h\right)\phi$. Podemos afirmar então que ϕ é uma biderivação. Pela Propriedade Universal, existe então $\xi : G \otimes G \to K$ tal que $(g \otimes h)\xi = (g, h)\phi$ para todo $(g, h) \in G \times G$. Logo, dados $g, h \in G$:

$$(g \otimes h)\xi \circ \pi = ([k_g, k_h])\pi = [(k_g)\pi, (k_h)\pi] = [g, h] = (g \otimes h)\kappa.$$

Uma vez que $G \otimes H$ é gerado pelos elementos da forma $g \otimes h$, provamos que $\xi \circ \pi = \kappa$. □

Lema 4.16. *Seja M e N grupos em que M é abeliano finitamente gerado. Se $f : M \to N$ é um homomorfismo sobrejetor, então f é um isomorfismo.*

Demonstração. Para cada $n \in \mathbb{N}^*$, escreva $K_n = Ker(f^n) \subset M$. Dado $n \in \mathbb{N}^*$, tome $x \in K_n$. Então:

$$(x)f^{n+1} = ((x)f^n)f = (0)f = 0,$$

donde $x \in K_{n+1}$. Pela arbitrariedade de $x \in K_n$, provamos que $K_n \subset K_{n+1}$ para todo $n \in \mathbb{N}^*$.

Como M é finitamente gerado e abeliano, se trata de um $\mathbb{Z}$-módulo Noetheriano e portanto existe $m \in \mathbb{N}^*$ tal que $K_m = K_{m+i}$ para todo $i \in \mathbb{N}$. Para provar que f é injetor, vamos provar que $Ker(f) = \{0\}$. Dado $x \in Ker(f)$, como f é sobrejetor, temos que f^m também é sobrejetor. Assim, existe $y \in M$ tal que $(y)f^m = x$. Logo,

$$0 = (x)f = ((y)f^m)\, f = (y)f^{m+1}.$$

Assim, $y \in K_{m+1} = K_m$. Portanto, $x = (y)f^{m+1} = 0$, mostrando que f é injetora. Logo, concluímos que f é um isomorfismo. □

Teorema 4.17. *[9, pág. 183] Se U é um grupo de recobrimento total de um grupo finito G, então existe uma aplicação $\zeta : G \wedge G \to U'$ que é um isomorfismo.*

Demonstração. Tomemos uma extensão central:

$$1 \longrightarrow M(G) \xrightarrow{\ i\ } U \xrightarrow{\ \pi\ } G \longrightarrow 1\ ,$$

com $Im(i) \leq U' \cap Z(U)$.

Pela Proposição 4.15 existe $\xi : G \otimes G \to U$ tal que $\xi \circ \pi = \kappa$. Lembremos que, pela construção de ξ, para cada $g \otimes h \in G \otimes G$, temos $(g \otimes h)\xi = [u_g, u_h]$ onde $(u_g)\pi = g$ e $(u_h)\pi = h$. Assim, $Im(\xi) \leq U'$ e dados $g \otimes g \in G \otimes G$, temos que $(g \otimes g)\xi = 1_{G \otimes G}$. Portanto, ao tomarmos o homomorfismo $\psi : \Gamma(G^{ab}) \longrightarrow G \otimes G$ como construído na Proposição 4.13, teremos $Im(\psi) \leq Ker(\xi)$. Uma vez que $G \wedge G = (G \otimes G)/Im(\psi)$, está bem definido o homomorfismo:

$$\begin{array}{rccc} \zeta : & G \wedge G & \longrightarrow & U' \\ & r \cdot Im(\psi) & \longmapsto & (r)\xi \end{array}.$$

Dados $u_1, u_2 \in U$, sejam $g_1 = (u_1)\pi$ e $g_2 = (u_2)\pi$. Dessa forma, $(g_1 \wedge g_2)\zeta = (g_1 \otimes g_2)\xi = [u_1, u_2]$. Uma vez que tomamos quaisquer $u_1, u_2 \in G$, provamos que ζ é sobrejetora.

Pelo Teorema 4.14, existe um isomorfismo $\varphi_1 : M(G) \to Ker(\kappa')$. Seja, então, $\varphi : M(G) \to G \wedge G$ a extensão no contradomínio de φ_1. Assim, para todo $m \in M(G)$, temos que $(m)\varphi \in Ker(\kappa')$, ou seja, $(m)\varphi \circ \kappa' = 1$ para todo $m \in M(G)$.

Como $Im(i) \leq U'$, podemos tomar $i^* : M(G) \to U'$ como a contração de i no contradomínio e, consequentemente, i^* é um homomorfismo injetor. Por outro lado, temos que $(U')\pi = ((U)\pi)' = G'$ já que π é sobrejetor. Logo, podemos tomar a aplicação $\pi^* : U' \to G'$ que é a restrição de π no domínio e contradomínio. Dessa forma, π^* é um homomorfismo sobrejetor. Note ainda que:

$$Ker(\pi^*) = Ker(\pi) \cap U' = Im(i) \cap U' = Im(i) = Im(i^*).$$

Assim, temos a sequência exata:

$$1 \longrightarrow M(G) \xrightarrow{i^*} U' \xrightarrow{\pi^*} G' \longrightarrow 1 \ .$$

Agora, note que dado $r \wedge s = (r \otimes s)Im(\psi) \in G \wedge G$, sejam u_r, u_s os elementos de U tais que $(u_r)\pi = r$ e $(u_s)\pi = s$. Dessa forma,

$$\begin{aligned}(r \wedge s)\zeta \circ \pi^* &= ((r \wedge s)\zeta)\,\pi^* = ((r \otimes s)\xi)\,\pi^* = ([u_r, u_s])\pi^* \\ &= ([u_r, u_s])\pi = [(u_r)\pi, (u_s)\pi] = [r, s] = (r \wedge s)\kappa'.\end{aligned}$$

Uma vez que $G \wedge G$ é gerado pelos elementos da forma $r \wedge s \in G \wedge G$, provamos que $\zeta \circ \pi^* = \kappa'$. Assim, para todo $m \in M(G)$, temos $(m)\varphi \circ \zeta \circ \pi^* = (m)\varphi \circ \kappa' = 1$, ou seja, $(m)\varphi \circ \zeta \in Ker(\pi^*) = Im(i^*)$. Como i é injetor, existe um único $v_m \in M(G)$ tal que $(v_m)i^* = (m)\varphi \circ \zeta$. Podemos assim tomar a função:

$$\begin{array}{rccc} \alpha : & M(G) & \longrightarrow & M(G) \\ & m & \longmapsto & v_m \end{array},$$

onde $v_m \in M(G)$ satisfaz $(v_m)i^* = (m)\varphi \circ \zeta$. Não é difícil verificar que α é um homomorfismo.

Agora, dado $v \in M(G)$, temos que $(v)i^* \in U'$. Como ζ é sobrejetora, existe $n \in G \wedge G$ tal que $(n)\zeta = (v)i^*$. Além disso, é certo que $(v)i^* \in Im(i^*) = Ker(\pi^*)$. Dessa forma, pelo que já provamos,

$$(n)\kappa' = (n)\zeta \circ \pi^* = ((v)i^*)\pi^* = 1,$$

ou seja, $n \in Ker(\kappa')$.

Uma vez que $\varphi_1 : M(G) \to Ker(\kappa')$ é um isomorfismo, existe $m \in M(G)$ tal que $(m)\varphi_1 = n$, ou seja, $(m)\varphi = n$. Logo, $(m)\varphi \circ \zeta = (n)\zeta = (v)i^*$, concluindo que $v = (m)\alpha$.

Já que tomamos qualquer $v \in M(G)$, podemos afirmar que α é um homomorfismo sobrejetor.

Como G é finito, então $M(G)$ é finito. Logo, o Lema 4.16 nos diz que α é um isomorfismo. Além disso, para qualquer $m \in M(G)$, temos que $((m)\alpha)i^* = (m)\varphi \circ \zeta$, ou seja, $\alpha \circ i^* = \varphi \circ \zeta$. Logo, considerando $Id_{\{1\}}$ e $Id_{G'}$ as funções identidades em $\{1\}$ e G', respectivamente, temos o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & M(G) & \xrightarrow{\varphi} & G \wedge G & \xrightarrow{\kappa'} & G' & \longrightarrow & \{1\} \\ {\scriptstyle Id_{\{1\}}}\downarrow & & {\scriptstyle \alpha}\downarrow & & {\scriptstyle \zeta}\downarrow & & {\scriptstyle Id_{G'}}\downarrow & & {\scriptstyle Id_{\{1\}}}\downarrow \\ \{1\} & \longrightarrow & M(G) & \xrightarrow{i^*} & U' & \xrightarrow{\pi^*} & G' & \longrightarrow & \{1\} \end{array} .$$

Como $Im(\varphi) = Im(\varphi_1) = Ker(\kappa')$, podemos aplicar o Lema 1.19 e obter que ζ é um isomorfismo. □

Segue dos Teoremas 1.24 e 4.17 que se G é um grupo finito, então existe um grupo de recobrimento total U de G e $U' \cong G \wedge G$.

4.3 Produto Exterior Não Abeliano de Grupos

Nesta seção, estudaremos o produto tensorial não abeliano $M \otimes N$ para subgrupos normais M e N de um grupo G em que todas as ações tomadas serão conjugações. Observemos que $M \otimes N$ pode não ser isomorfo ao subgrupo $\langle m \otimes n \mid m \in M, n \in N \rangle$ de $G \otimes G$. De fato, vamos mostrar a seguir um exemplo em que tais não são isomorfos.

Tomemos $G = D_8 = \langle \alpha, \beta \mid \alpha^4 = 1, \beta^2 = 1, \beta\alpha\beta = \alpha^{-1} \rangle$. Sendo $M = N = \langle \alpha^2 \rangle$, veremos primeiramente que $J = \langle m \otimes n \mid m, n \in \{1, \alpha^2\} \rangle = \{1\}$. Os geradores de J são $1 \otimes 1, 1 \otimes \alpha^2, \alpha^2 \otimes 1, \alpha^2 \otimes \alpha^2$. Assim, basta analisarmos $\alpha^2 \otimes \alpha^2$. Agora,

$$\alpha^2 \otimes \alpha^2 = (\alpha \otimes \alpha^2)^2 = (\alpha \otimes \alpha)^4 = \alpha^4 \otimes \alpha = 1_{D_8 \otimes D_8}.$$

Portanto, $|J| = 1$.

Agora, vamos analisar o grupo $\langle \alpha^2 \rangle \otimes \langle \alpha^2 \rangle$. Tomemos a função:

$$\begin{array}{rccc} f: & \langle \alpha^2 \rangle \times \langle \alpha^2 \rangle & \longrightarrow & \mathbb{Z}_2 \\ & (\alpha^{2i}, \alpha^{2j}) & \longmapsto & \overline{i \cdot j} \end{array} .$$

É fácil verificar que f está bem definida e é uma biderivação. Com isso, existe um homomorfismo $g : \langle \alpha^2 \rangle \otimes \langle \alpha^2 \rangle \to \mathbb{Z}_2$ tal que $(\alpha^{2i} \otimes \alpha^{2j})g = (\alpha^{2i}, \alpha^{2j})f = \overline{i \cdot j}$. Uma vez que g é sobrejetora, temos que $| \langle \alpha^2 \rangle \otimes \langle \alpha^2 \rangle | \geq 2$. Portanto, $\langle \alpha^2 \rangle \otimes \langle \alpha^2 \rangle \ncong J$.

Também apresentaremos nesta seção o conceito de produto exterior não abeliano

$M \wedge N$ e uma sequência exata com essa construção. Obteremos então um corolário interessante a respeito do expoente de $N \wedge G$.

Proposição 4.18. *Dados um grupo G e subgrupos normais M e N de G, sejam $m \in M$ e $n \in N$. Consideremos o grupo $M \otimes N$ em que as ações são as conjugações. Se $[m,n,n] = 1$, então para todo $t \in \mathbb{N}$, temos:*

$$(m \otimes n^t) = (m \otimes n)^t \left([m,n]^{\frac{t(t-1)}{2}} \otimes n \right) \tag{4.11}$$

Demonstração. Sejam $m \in M$, $n \in N$ e suponha que $[m,n,n] = 1$. Para todo $a \otimes x \in M \otimes N$, é certo que:

$$[a \otimes x, [m,n] \otimes n] = (a^{-1}a^x) \otimes (n^{-[m,n]}n) = [a,x] \otimes [[m,n],n] = [a,x] \otimes 1_N = 1_{M \otimes N},$$

ou seja, $[m,n] \otimes n \in Z(M \otimes N)$.

Agora, demonstraremos (4.11) por indução sobre t. Naturalmente vale para $t = 0$. Suponha agora que o resultado é verdadeiro para um certo $t \in \mathbb{N}$. Veja primeiramente que:

$$(m \otimes n)^{[m,n]} = (m \otimes n)^{m^{-1}m^n} = (m \otimes n)^{-1}(m \otimes n)(m \otimes n) = m \otimes n.$$

Logo,

$$(m \otimes n)^n = (m^n \otimes n^n) = (m[m,n]) \otimes n = (m \otimes n)^{[m,n]}([m,n] \otimes n) = (m \otimes n)([m,n] \otimes n). \tag{4.12}$$

Como $n^{[m,n]} = n$, pela Proposição 4.5 (viii), temos que $[m,n]^k \otimes n = ([m,n] \otimes n)^k$ para todo $k \in \mathbb{N}$. Assim,

$$\begin{aligned}
m \otimes n^{t+1} &= m \otimes (n^t n) \\
&= (m \otimes n)(m \otimes n^t)^n \\
&= (m \otimes n) \left[(m \otimes n)^t \left([m,n]^{\frac{t(t-1)}{2}} \otimes n \right) \right]^n \\
&= (m \otimes n) \left((m \otimes n)^t \right)^n \left([m,n]^{\frac{t(t-1)}{2}} \otimes n \right)^n \\
&= (m \otimes n) \left((m \otimes n)^n \right)^t \left(\left([m,n]^{\frac{t(t-1)}{2}} \right)^n \otimes n^n \right) \\
&= (m \otimes n) \left((m \otimes n)([m,n] \otimes n) \right)^t \left([m,n] \otimes n \right)^{\frac{t(t-1)}{2}}, \text{ por (4.12)} \\
&= (m \otimes n)(m \otimes n)^t ([m,n] \otimes n)^t \left([m,n] \otimes n \right)^{\frac{t(t-1)}{2}}, \text{ pois } [m,n] \otimes n \text{ é central} \\
&= (m \otimes n)^{t+1} ([m,n] \otimes n)^{t + \frac{t(t-1)}{2}} \\
&= (m \otimes n)^{t+1} \left([m,n]^{t + \frac{t(t-1)}{2}} \otimes n \right) \\
&= (m \otimes n)^{t+1} \left([m,n]^{\frac{t(t+1)}{2}} \otimes n \right).
\end{aligned}$$

Isso conclui a prova. □

Dado um grupo G e $N, M \triangleleft G$, se N é abeliano, observe que $[[G,N],N] \leq [N,N] = \{1\}$. Assim, podemos aplicar as propriedades vistas na última proposição para obter o seguinte limitante superior para $\exp(M \otimes N)$.

Lema 4.19. *[2, pág. 259] Sejam G um grupo e $N, M \triangleleft G$, com N abeliano. Então $\exp(M \otimes N)$ divide r em que*

$$r = \begin{cases} \exp(N), & \text{se } \exp(N) \text{ for ímpar} \\ 2\exp(N), & \text{se } \exp(N) \text{ for par} \end{cases}. \tag{4.13}$$

Demonstração. Uma vez que N é abeliano e normal em G, temos $[g,n,n] = 1$ para todos $g \in G$ e $n \in N$. Seja r como em (4.13). Dados $n \in N$ e $m \in M$, note que $n^r = 1$, independente da paridade de $\exp(N)$. Além disso, se $\exp(N)$ for ímpar, vemos que:

$$\frac{r(r-1)}{2} = \frac{\exp(N)(\exp(N)-1)}{2} = \exp(N)\frac{\exp(N)-1}{2},$$

ou seja, $\exp(N) \left| \frac{r(r-1)}{2} \right.$. Da mesma forma, podemos concluir que se $\exp(N)$ é par também temos $\exp(N) \left| \frac{r(r-1)}{2} \right.$. Logo, para todos $m \in M$ e $n \in N$, temos $[m,n]^{\frac{r(r-1)}{2}} = 1$ e, como $r = 1$, pela Proposição 4.18, obtemos

$$1 = (m \otimes n^r) = (m \otimes n)^r \left([m,n]^{\binom{r}{2}} \otimes n \right) = (m \otimes n)^r (1 \otimes n) = (m \otimes n)^r.$$

Vamos provar que para todo $t \in M \otimes N$, vale $t^r = 1$. Pelo Lema 4.6, para um certo $k \in \mathbb{N}^*$, podemos escrever t como produto finito de k elementos da forma $m \otimes n$, com $m \in M$ e $n \in N$. Provaremos o enunciado por indução sobre k.

Para $k = 1$, temos que $t = m \otimes n$ para certos $m \in M$ e $n \in N$. Logo, pelo que provamos, $t^r = 1$. Agora, assuma que o resultado é válido para algum $k \in \mathbb{N}^*$ e escrevamos:

$$t = (m_1 \otimes n_1) \cdots (m_k \otimes n_k)(m_{k+1} \otimes n_{k+1}).$$

Fazendo $s = (m_1 \otimes n_1) \cdots (m_k \otimes n_k)$, temos $t = s(m_{k+1} \otimes n_{k+1})$ e, pela hipótese de indução, $s^r = 1$. Além disso, como N é abeliano, o subgrupo $D_M(N)$ também possui essa propriedade. Logo, $D_M(N)$ é nilpotente de classe no máximo 1 e o Teorema 4.10 nos diz que $M \otimes N$ é nilpotente de classe no máximo 2. Portanto, pela Proposição 1.6 (iv),

$$t^r = [s(m_{k+1} \otimes n_{k+1})]^r = s^r (m_{k+1} \otimes n_{k+1})^r \, [m_{k+1} \otimes n_{k+1}, s]^{\frac{r(r-1)}{2}} = [m_{k+1} \otimes n_{k+1}, s]^{\frac{r(r-1)}{2}}.$$

Agora, pelas Proposições 1.6 (i) e 4.5 (vii), lembrando que $\gamma_2(M \otimes N) \leq Z(M \otimes N)$, temos:

$$\begin{aligned}[m_{k+1} \otimes n_{k+1}, s]^{\frac{r(r-1)}{2}} &= [m_{k+1} \otimes n_{k+1}, (m_1 \otimes n_1) \cdots (m_k \otimes n_k)]^{\frac{r(r-1)}{2}} \\ &= [m_{k+1} \otimes n_{k+1}, m_1 \otimes n_1]^{\frac{r(r-1)}{2}} \cdots [m_{k+1} \otimes n_{k+1}, m_k \otimes n_k]^{\frac{r(r-1)}{2}} \\ &= ([m_{k+1}, n_{k+1}] \otimes [m_1, n_1])^{\frac{r(r-1)}{2}} \cdots ([m_{k+1}, n_{k+1}] \otimes [m_k, n_k])^{\frac{(r-1)}{2}}.\end{aligned}$$

Para cada $i \in I_k$, temos $[m_i, n_i]^{[m_{k+1}, n_{k+1}]} = 1$, pois N é abeliano. Portanto, pela Proposição 4.5 (viii) e usando o fato que $\exp(N) \left| \frac{r(r-1)}{2} \right.$, obtemos:

$$([m_{k+1}, n_{k+1}] \otimes [m_i, n_i])^{\frac{r(r-1)}{2}} = [m_{k+1}, n_{k+1}]^{\frac{r(r-1)}{2}} \otimes [m_i, n_i] = 1 \otimes [m_i, n_i] = 1_{M \otimes N}.$$

Portanto, concluímos que $t^r = [m_{k+1} \otimes n_{k+1}, s]^{\frac{r(r-1)}{2}} = 1_{M \otimes N}$, como queríamos. □

Sejam M e N subgrupos normais de um grupo G agindo um sobre o outro por conjugação em G e consideremos o produto tensorial $M \otimes N$. Seguindo Brown e Loday [10], o *produto exterior não abeliano* $M \wedge N$ é o grupo obtido de $M \otimes N$ impondo as relações adicionais $x \otimes x = 1$ para todo $x \in M \cap N$. Para $m \in M$ e $n \in N$, vamos denotar a imagem de $m \otimes n$ em $M \wedge N$ por $m \wedge n$.

Assim, o produto exterior não abeliano $M \wedge N$ pode ser visto como o grupo gerado por todos os símbolos $m \wedge n$, com $m \in M$ e $n \in N$, satisfazendo as seguintes relações:

$$(ab) \wedge x = \left(a^b \wedge x^b\right)(b \wedge x),\ a \wedge (xy) = (a \wedge y)\,(a^y \wedge x^y) \text{ e } u \wedge u = 1,$$

em que $a, b \in M$, $x, y \in N$ e $u \in M \cap N$.

Proposição 4.20. *[14, pág. 4228] Se M e N são subgrupos normais de um grupo G com $M \leq N$, então existe uma sequência exata:*

$$M \wedge G \longrightarrow N \wedge G \longrightarrow \frac{N}{M} \wedge \frac{G}{M} \longrightarrow \{1\}.$$

Demonstração. Uma vez que $M, N \triangleleft G$ com $M \leq N$, não é difícil verificar que existem homomorfismos $i : M \wedge G \to N \wedge G$ e $\pi : N \wedge G \to (N/M) \wedge (G/M)$ satisfazendo $(m \wedge g)i = m \wedge g$ e $(n \wedge g)\pi = nM \wedge gM$, para todos $m \in M$, $n \in N$ e $g \in G$. Claramente, π é sobrejetora. Vamos então provar que $Im(i) = Ker(\pi)$.

Dados $m \in M$ e $g \in G$, veja que:

$$(m \wedge g)i \circ \pi = (m \wedge g)\pi = mM \wedge gM = 1_{\frac{G}{M}} \wedge gM,$$

provando que $Im(i) \leq Ker(\pi)$.

Além disso, $Im(i) \triangleleft N \wedge G$, pois da definição de $N \wedge G$ e Proposição 4.5 (iii), para

todos $m \in M$, $g, h \in G$ e $n \in N$, temos:

$$(n \wedge g)^{-1}(m \wedge h)(n \wedge g) = (m \wedge h)^{[n,g]} = m^{[n,g]} \wedge h^{[n,g]} = \left(m^{[n,g]} \wedge g^{[n,g]}\right) i \in Im(i).$$

Ainda mais, já que $Im(i) \leq Ker(\pi)$, podemos tomar o homomorfismo:

$$\begin{array}{rccc} \alpha: & \frac{N \wedge G}{Im(i)} & \longrightarrow & \frac{N}{M} \wedge \frac{G}{M} \\ & t \cdot Im(i) & \longmapsto & (t)\pi \end{array}.$$

Vamos provar que para quaisquer $m \in M$ e $n \in N$, temos $n \wedge m \in Im(i)$. Note que:

$$\begin{aligned} 1_{N \wedge G} &= (nm) \wedge (nm) = (n \wedge (nm))^m (m \wedge (nm)) \\ &= \left((n \wedge m)(n \wedge n)^m\right)^m (m \wedge m)(m \wedge n)^m = (n \wedge m)^m (m \wedge n)^m \\ &= \left((n \wedge m)(m \wedge n)\right)^m. \end{aligned}$$

Logo, $(n \wedge m)(m \wedge n) = 1_{N \wedge G}$ e, consequentemente, $n \wedge m = ((m \wedge n)i)^{-1} \in Im(i)$, como desejado.

Para facilitar, vamos escrever $\bar{t}$ para representar $t \cdot Im(i) \in (N \wedge G)/Im(i)$ com $t \in N \wedge G$. Consideremos a aplicação:

$$\begin{array}{rccc} \rho_1: & \frac{N}{M} \times \frac{G}{M} & \longrightarrow & \frac{N \wedge G}{Im(i)} \\ & (nM, gM) & \longmapsto & \overline{n \wedge g} \end{array}.$$

Vamos provar que ρ_1 está bem definida. Para isso, sejam $n, n' \in N$ e $g, g' \in G$ com $nM = n'M$ e $gM = g'M$. Existem então $m_1, m_2 \in M$ tais que $n = m_1 n'$ e $g = m_1 g'$. Assim,

$$\begin{aligned} \overline{n \wedge g} &= \overline{(m_1 n') \wedge (m_2 g')} = \overline{(m_1 \wedge (m_2 g'))^{n'} (n' \wedge (m_2 g'))} \\ &= \overline{m_1^{n'} \wedge (m_2 g')^{n'}}\ \overline{(n' \wedge g')(n' \wedge m_2)^{g'}} \\ &= \overline{m_1^{n'} \wedge (m_2 g')^{n'}}\ \overline{n' \wedge g'}\ \overline{(n')^{g'} \wedge m_2^{g'}} = \overline{n' \wedge g'}, \end{aligned}$$

uma vez que $m_1^{n'} \wedge (m_2 g')^{n'}, (n')^{g'} \wedge m_2^{g'} \in Im(i)$. Assim, ρ_1 está bem definida. Cálculos simples nos mostram que ρ_1 é uma biderivação. Assim, existe o homomorfismo $\rho_2 : (N/M) \otimes (G/M) \to (N \wedge G)/Im(i)$ tal que $\rho_2(nM \otimes gM) = \overline{n \wedge g}$ para quaisquer $n \in N$ e $g \in G$. Além disso, para $nM \in N/M$, temos $(nM \otimes nM)\rho_2 = \overline{n \wedge n} = \overline{1_{N \wedge G}} = 1_{(N \wedge G)/Im(i)}$, ou seja, $\Delta(N/M, G/M) \leq Ker(\rho_2)$. Assim, ρ_2 induz o homomorfismo $\rho : N/M \wedge G/M \to (N \wedge G)/Im(i)$ que satisfaz $(nM \wedge gM)\rho = \overline{n \wedge g}$, para todos $m \in G$ e $g \in G$.

Agora, para $n \in N$ e $g \in G$,

$$\left(\overline{n \wedge g}\right) \alpha \circ \rho = \left(\left(\overline{n \wedge g}\right) \alpha\right) \rho = \left((n \wedge g)\pi\right) \rho = (nM \wedge gM)\, \rho = \overline{n \wedge g},$$

e,

$$(nM \wedge gM)\rho \circ \alpha = (\overline{n \wedge g})\,\alpha = (n \wedge g)\pi = nM \wedge gM.$$

Provamos assim que ρ é a função inversa de α. Logo, α é um isomorfismo e isso nos diz que $Ker(\pi) \leq Im(i)$ e, consequentemente, $Ker(\pi) = Im(i)$. Assim, temos a sequência exata:

$$\{1\} \longrightarrow M \wedge G \xrightarrow{\ i\ } N \wedge G \xrightarrow{\ \pi\ } \tfrac{N}{M} \wedge \tfrac{G}{M} \longrightarrow \{1\}\ ,$$

e portanto o resultado é verdadeiro. □

Como uma consequência imediata da Proposição 4.20 temos o seguinte:

Corolário 4.21. *Se M e N são subgrupos normais de um grupo G finito, com $M \leq N$, então*

$$\exp(N \wedge G) \,\Big|\, \exp\left(\frac{N}{M} \wedge \frac{G}{M}\right) \cdot \exp(M \wedge G)\ .$$

No caso em que G é um p-grupo finito (p ímpar) e N é um subgrupo normal de G *powerful*, Antony, Komma e Thomas apresentaram o seguinte limitante superior para $\exp(N \wedge G)$.

Proposição 4.22. *[2, pág. 259] Sejam G um p-grupo finito com p um primo ímpar e $N \triangleleft G$. Se N é powerful, então $\exp(N \wedge G) | \exp(N)$. Em particular, se G é powerful, $\exp(G \wedge G) | \exp(G)$ e, consequentemente, $\exp(M(G)) | \exp(G)$.*

Demonstração. Como N é um p-grupo, existe $\varepsilon \in \mathbb{N}$ tal que $\exp(N) = p^{\varepsilon}$. Vamos provar o resultado por indução sobre ε. Para $\varepsilon = 0$, temos $N = \{1\}$ e portanto $N \wedge G = \{1\}$, ou seja, $\exp(N \wedge G) = \{1\}$.

Agora, suponhamos que o resultado é válido para todo subgrupo normal de G *powerful* com expoente p^{ε}. Seja N um subgrupo normal de G *powerful* tal que $\exp(N) = p^{\varepsilon+1}$.

Como N é *powerful*, temos $N' \leq N^p$ e, portanto, N/N^p é abeliano. Além disso, N^p char $N \triangleleft G$, isto é, $N^p \triangleleft G$. Dessa forma, podemos considerar o grupo $(N/N^p) \wedge (G/N^p)$. Pelo Corolário 4.21,

$$\exp(N \wedge G) \,\Big|\, \exp\left(\frac{N}{N^p} \wedge \frac{G}{N^p}\right) \cdot \exp\left(N^p \wedge G\right)\ . \tag{4.14}$$

Visto que $p^{\varepsilon+1}$ é ímpar e $\exp\left((N/N^p) \wedge (G/N^p)\right) | \exp\left((N/N^p) \otimes (G/N^p)\right)$, o Lema 4.19 nos diz que $\exp\left((N/N^p) \wedge (G/N^p)\right)$ divide $\exp\left(N/N^p\right)$. Não é difícil ver que $\exp\left(N/N^p\right) | p$ e, assim, $\exp\left((N/N^p) \wedge (G/N^p)\right) | p$.

Agora, pelo Teorema 3.4, podemos afirmar que $N^p = G^p$ é *powerfully embedded* em N e, consequentemente, N^p é *powerful*. Ainda mais, pelo Corolário 3.8, temos que $\exp(N^p) = p^{\varepsilon+1-1} = p^\varepsilon$. Assim, pela hipótese de indução, $\exp(N^p \wedge G) \mid p^\varepsilon$.

Logo, de (4.14) concluímos que $\exp(N \wedge G) | p \cdot p^\varepsilon$, ou seja, $\exp(N \wedge G) \mid \exp(N)$, provando assim o desejado por indução sobre ε. □

CAPÍTULO 5

COTAS SUPERIORES PARA OS EXPOENTES DE UM GRUPO E DE SEU MULTIPLICADOR DE SCHUR

Dado um grupo finito G, este capítulo tem como objetivo apresentar cotas superiores para os expoentes dos grupos G e $M(G)$ estabelecidos por Antony, Komma e Thomas em [2] e [25]. Muitos estudos já foram feitos a fim de se determinar sob quais hipóteses temos que $\exp(M(G))$ é um divisor de $\exp(G)$. Já foi provado que isto ocorre, por exemplo, para p-grupos *powerful* [28], p-grupos metabelianos de expoente no máximo p [32] e grupos metabelianos p-centrais [1]. Veremos que o mesmo acontece com os p-grupos finitos de classe no máximo p (Corolário 5.3) e com os p-grupos metabelianos finitos de classe no máximo $2p-1$ e p ímpar (Teorema 5.22). Também, quando G é um p-grupo finito de classe c, apresentaremos uma cota superior para $\exp(G)$ em função de p, c e do expoente de um p-subgrupo de Sylow do grupo de automorfismos de G (Teorema 5.12).

5.1 Limites dependendo da classe nilpotência

Usando o Teorema 2.5, Antony, Komma e Thomas [2] estabeleceram o seguinte resultado o qual foi aplicado no estudo que eles realizaram sobre o expoente do subgrupo derivado de um p-grupo de classe no máximo $p+1$ que veremos mais adiante.

Lema 5.1. *[2, pág. 255] Seja G um p-grupo. Se x e y são elementos de G tais que $\langle x, y\rangle$ possui classe de nilpotência no máximo $p+1$, então:*

(i) $[g, {}_p x]^{-1} = [x, g, {}_{p-1}x]$, *para todo* $g \in \langle x, y\rangle$;

(ii) *Dado* $n \in \mathbb{N}$, *se* $\left[x^{p^n}, y\right] = 1$, *então* $[x, y]^{p^n} = [y, {}_p x]^{\binom{p^n}{p}}$.

Demonstração. Consideremos aqui $H = \langle x, y\rangle$ que será um p-grupo com $\gamma_{p+2}(H) = \{1\}$.

(i) Para $i \in I_{p+1}$ e $h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_{p+1}, u, v \in H$, temos:

$$[h_1, \ldots, h_{i-1}, uv, h_{i+1}, \ldots, h_{p+1}] \\ = [h_1, \ldots, h_{i-1}, u, h_{i+1}, \ldots, h_{p+1}] \cdot [h_1, \ldots, h_{i-1}, v, h_{i+1}, \ldots, h_{p+1}].$$

Uma vez que $\gamma_{p+1}(H) \leq Z(H)$, temos:

$$1 = [xy, xy, {}_{p-1}x] = [x, x, {}_{p-1}x][x, y, {}_{p-1}x][y, x, {}_{p-1}x][y, y, {}_{p-1}x] = [x, y, {}_{p-1}x][y, {}_{p}x],$$

provando que $[y, {}_{p}x]^{-1} = [x, y, {}_{p-1}x]$.

Dado $g \in H$, existem $\varepsilon_1, \ldots, \varepsilon_k, \delta_1, \ldots, \delta_k \in \mathbb{Z}$ tais que $g = x^{\varepsilon_1} y^{\delta_1} \cdots x^{\varepsilon_k} y^{\delta_k}$. Assim, pela multilinearidade de comutadores de peso $p+1$ e como $[y, {}_{p}x]^{-1} = [x, y, {}_{p-1}x]$ e $[x, {}_{p}x]^{-1} = [x, x, {}_{p-1}x]$,

$$\begin{aligned} [g, {}_{p}x]^{-1} &= \left[x^{\varepsilon_1} y^{\delta_1} \cdots x^{\varepsilon_k} y^{\delta_k}, {}_{p}x\right]^{-1} = [x, {}_{p}x]^{-\varepsilon_1} [y, {}_{p}x]^{-\delta_1} \cdots [x, {}_{p}x]^{-\varepsilon_k} [y, {}_{p}x]^{-\delta_k} \\ &= [x, x, {}_{p-1}x]^{\varepsilon_1} [x, y, {}_{p-1}x]^{\delta_1} \cdots [x, x, {}_{p-1}x]^{\varepsilon_k} [x, y, {}_{p-1}x]^{\delta_k} \\ &= \left[x, x^{\varepsilon_1} y^{\delta_1} \cdots x^{\varepsilon_k} y^{\delta_k}, {}_{p-1}x\right] = [x, g, {}_{p-1}x], \end{aligned}$$

como queríamos provar.

(ii) Agora, suponhamos que $\left[x^{p^n}, y\right] = 1$ e seja $J = \langle x, [x, y] \rangle$. Pelo Teorema 2.5,

$$\left[x^{p^n}, y\right] \equiv [x, y]^{p^n} \prod_{i=2}^{p^n} [x, y, {}_{i-1}x]^{\binom{p^n}{i}} \pmod{K_n(x, [x, y])}, \tag{5.1}$$

onde $K_n(x, [x, y])$ é o fecho normal em J do conjunto formado por:

- comutadores formais em $\{x, [x, y]\}$ de peso no mínimo p^n e cujo peso em $[x, y]$ é no mínimo 2;
- as p^{n-k+1}-ésimas potências de comutadores formais em $\{x, [x, y]\}$ de peso maior ou igual a p^{k-1} e menor que p^k e cujo peso em $[x, y]$ é no mínimo 2, para $k \in I_n$.

Primeiro analisemos o caso $p = 2$. Veja que $K_n(x, [x, y])$ é gerado por conjugados de potência de comutadores simples cujo peso em $[x, y]$ é no mínimo 2. Pelo Lema 1.10, temos:

$$K_n(x, [x, y]) \leq [\gamma_2(H), \gamma_2(H)] \leq \gamma_4(H) = \{1\}.$$

Assim, de (5.1), segue a igualdade:

$$[x, y]^{2^n} = \left(\prod_{i=2}^{2^n} [x, y, {}_{i-1}x]^{\binom{2^n}{i}} \right)^{-1}.$$

Para $i \in \{3, \dots, 2^n\}$, vemos que $[x, y, {}_{i-1}x] \in \gamma_{i+1}(H) \leq \gamma_4(H) = \{1\}$. Com isso, pelo primeiro item, $[x, y]^{2^n} = ([x, y, {}_{2-1}x]^{-1})^{\binom{2^n}{2}} = [y, {}_2x]^{\binom{2^n}{2}}$, como queríamos.

Agora, provaremos que o mesmo vale quando $p > 2$. Observamos que os geradores de $K_n(x, [x, y])$ são todos conjugados de potências de comutadores com peso em $[x, y]$ no mínimo 2. Dado um comutador t com essa propriedade e peso no mínimo p, pelo Lema 1.10,

$$\begin{aligned} t &\in [H, \dots, H, \gamma_2(H), H, \dots, H, \gamma_2(H), H, \dots, H] \\ &= [\gamma_1(H), \dots, \gamma_1(H), \gamma_2(H), \gamma_1(H), \dots, \gamma_1(H), \gamma_2(H), \gamma_1(H), \dots, \gamma_1(H)] \\ &\leq \gamma_{p+2}(H) = \{1\}, \end{aligned}$$

o que implica em $t = 1$. Portanto, $K_n(x, [x, y])$ é o fecho normal em J de p^n-ésimas potências de comutadores formais em $\{x, [x, y]\}$ de peso no máximo $p - 1$ e peso em $[x, y]$ no mínimo 2. Pela Proposição 1.11 ,

$$\gamma_{p+1}(J) \leq \gamma_{p+1}(\langle x, H' \rangle) \leq \gamma_{p+2}(H) = \{1\},$$

e, portanto, J tem classe de nilpotência no máximo p e $x^{p^n} \in Z(J)$ por hipótese.

Mostraremos agora que dado $u \in H'$ um comutador formal básico em $\{x, [x, y]\}$, se $\omega(u) \geq 2$ e o peso de u em x é maior ou igual a 1, então $u^{p^n} = 1$. Provaremos isso por indução sobre tal escrita de u. Se tiver peso 2, então é da forma $[x, h]$ ou $[h, x] = [x, h]^{-1}$ com $h \in \langle x, y \rangle$. Assim, basta provarmos que $[x, h]^{p^n} = 1$. Porém, isso é direto do Teorema 3.14, já que $[x^{p^n}, h] = 1$. Assim, provamos o desejado para u de peso 2.

Agora, seja $k > 2$ o peso de u segundo a escrita dada e suponhamos que o resultado é válido para elementos com escrita de peso menor que k. Assim, $u = [r, s]$, onde x aparece na escrita de r ou s. Podemos supor, sem perda de generalidade que o peso de r em x é maior ou igual a 1. Assim, pela hipótese de indução, $r^{p^n} = 1$. Portanto, como $r, s \in J$, pelo Teorema 3.14, temos que $[r^{p^n}, s] = 1$, implica que $u^{p^n} = [r, s]^{p^n} = 1$. Portanto, provamos o desejado.

Assim, dado um comutador formal básico t em $\{x, [x, y]\}$ de peso menor que p e cujo peso em b é no mínimo 2, pela afirmação, temos $t^{p^n} = 1$. Provamos assim que $K_n(x, [x, y]) = \{1\}$ e, portanto, de (5.1),

$$\left[x^{p^n}, y\right] = [x, y]^{p^n} \prod_{i=2}^{p^n} [x, y, {}_{i-1}x]^{\binom{p^n}{i}}. \tag{5.2}$$

Agora, dado $i \in \{2, \dots, p^n\}$, se $i > p$, temos $[x, y, {}_{i-1}x] \in \gamma_{p+1}(J) = \{1\}$, ou seja, $[x, y, {}_{i-1}x] = 1$. Agora, se $i < p$, então, pelo Lema 2.4, $p^n \left| \binom{p^n}{i} \right.$. Portanto, pela

afirmação provada, $[x, y, {}_{i-1}x]^{\binom{p^n}{i}} = 1$.

Logo, de (5.2), decorre que:

$$1 = [x^{p^n}, y] = [x, y]^{p^n}[x, y, {}_{p-1}x]^{\binom{p^n}{p}}.$$

Assim,

$$[x, y]^{p^n} = [x, y, {}_{p-1}x]^{-\binom{p^n}{p}} = [y, {}_p x]^{\binom{p^n}{p}},$$

como queríamos.

□

Antony, Komma e Thomas estabeleceram uma condição suficiente para que se tenha $\exp(\gamma_2(G))$ divisor de $\exp(G/Z(G))$, conforme veremos a seguir:

Teorema 5.2. *[2, pág. 252] Se p for um número primo e G um p-grupo finito com classe de nilpotência menor ou igual a $p+1$, então $\exp(\gamma_2(G))\,|\exp(G/Z(G))$.*

Demonstração. Consideremos $p^n = \exp(G/Z(G))$. De acordo com a Proposição 1.12, temos $\gamma_p(\gamma_2(G)) \leq \gamma_{2p}(G) = \{1\}$. Logo, o Lema 3.9 nos diz que G' é regular. Vamos inicialmente mostrar que $[x, y]^{p^n} = 1$ para quaisquer $x, y \in G$. Do Lema 5.1, segue a igualdade:

$$[x, y]^{p^n} = [y, {}_p x]^{\binom{p^n}{p}}. \tag{5.3}$$

Se $p = 2$, como $[x, y]^{2^n} \in Z(G)$, temos:

$$[xy, y]^{2^n} = ([x, y]^y[y, y])^{2^n} = \left([x, y]^{2^n}\right)^y = [x, y]^{2^n}.$$

Portanto, de (5.3) e Lema 5.1 (ii),

$$[y, xy, xy]^{\binom{2^n}{2}} = [xy, y]^{2^n} = [x, y]^{2^n} = [y, x, x]^{\binom{2^n}{2}}.$$

Uma vez que $\gamma_4(G) = \{1\}$:

$$[y, xy, xy] = [y, x, x][y, x, y][y, y, x][y, y, y] = [y, x, x][y, x, y].$$

Logo,

$$[y, x, x]^{\binom{2^n}{2}} = [y, xy, xy]^{\binom{2^n}{2}} = ([y, x, x][y, x, y])^{\binom{2^n}{2}} = [y, x, x]^{\binom{2^n}{2}}[y, x, y]^{\binom{2^n}{2}},$$

fazendo com que, pelo Lema 5.1 (i) e (5.3):

$$1 = [y, x, y]^{\binom{2^n}{2}} = [x, {}_2 y]^{-\binom{2^n}{2}} = [y, x]^{-2^n} = [x, y]^{2^n},$$

como queríamos.

Vamos agora estudar o caso $p > 2$. Dados $a, b \in G$, denotemos por $S(a,b)$ o conjunto dos comutadores da forma $[b, a, c_1, \ldots, c_{p-1}]$ com $c_1, \ldots, c_{p-1} \in \{a, b\}$. Como $\gamma_{p+2}(G) = \{1\}$, vemos que os elementos de $S(a,b)$ são centrais em G. Para cada $r \in \{0, \ldots, p-1\}$, escrevemos $T_r(a,b)$ para representar o conjunto composto por todos os comutadores em $S(a,b)$ com peso $r+1$ em b, isto é, exatamente r elementos de $\{c_1, \ldots, c_{p-1}\}$ satisfazem $c_i = b$. Assim, escrevemos para cada $r \in \{0, \ldots, p-1\}$:

$$e_r(a,b) = \prod_{c \in T_r(a,b)} c.$$

Observe que esse produto está bem definido pois $T_r(a,b)$ é um conjunto finito e está contido em $Z(G)$.

Veja que, dados $x, y \in G$, pela linearidade dos comutadores de peso $p+1$, todo elemento de $S(xy,y)$ pode ser escrito como um produto de elementos de $S(x,y)$. Tomemos $c = [y, xy, c_1, \ldots, c_{p-1}] \in S(xy,y)$ de peso $t+1$ em y. Dado $d = [y, x, d_1, \ldots, d_{p-1}]$ em $S(x,y)$ com peso $s+1$ em y, existem $p-1-s$ índices i em I_{p-1} tais que $d_i = x$. Digamos que tais índices são $i_1, \ldots, i_{p-1-s}$. Portanto, ao escrever c como produto de elementos de $S(x,y)$, temos que d é um fator se, e somente se, $c_{i_1} = \cdots = c_{i_{p-1-s}} = xy$. Porém isto ocorre somente se existem t índices em $I_{p-1} \backslash \{i_1, \ldots, i_{p-1-s}\}$ tais que $c_i = y$, fazendo com que $t \leq s$. Logo, d aparece na escrita de $\binom{s}{t}$ elementos de $S(xy,y)$ com peso $t+1$ em y, além de que aparece apenas uma vez em cada expressão.

Pelo último parágrafo, para cada $t \in \{0, 1, \ldots, p-1\}$, escrevendo $e_t(xy,y)$ como produto de elementos de $S(x,y)$, obtemos:

$$e_t(xy,y) = \prod_{s=t}^{p-1} e_s(x,y)^{\binom{s}{t}}. \tag{5.4}$$

Considerando o conjunto $T = \{(m,h) \in \mathbb{N}^* \times \mathbb{N}^* \mid h \geq m\}$, podemos definir uma aplicação $\alpha : T \to \mathbb{N}^*$ por:

- $(1,h)\alpha = 1$ para todo $h \in \mathbb{N}^*$;
- $(m+1,h)\alpha = \sum_{k=m}^{h-1} \binom{h}{k} (m,k)\alpha$, para todo $(m+1,h) \in \mathbb{N}^* \times \mathbb{N}^*$ com $h \geq m+1$.

Vamos provar primeiramente por indução sobre m que $(m,m)\alpha = m!$. Para $m = 1$, temos que $(1,1)\alpha = 1 = 1!$. Agora, assuma que isso é verdade para um certo $m \in \mathbb{N}^*$. Assim,

$$(m+1,m+1)\alpha = \sum_{k=m}^{m} \binom{m+1}{k} (m,k)\alpha = \binom{m+1}{m} (m,m)\alpha = (m+1) \cdot m! = (m+1)!,$$

como queríamos.

Provaremos que para todos $x, y \in G$ e $m \in I_{p-1}$, temos $\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha\binom{p^n}{p}} = 1$. Mostraremos isso por indução sobre m. Para $m = 1$, como $x^{p^n} \in Z(G)$, pelo Lema 5.1 (ii),

$$e_0(x,y)^{\binom{p^n}{p}} = [y, {}_p x]^{\binom{p^n}{p}} = [x,y]^{p^n} = [x,xy]^{p^n} = [xy, {}_p x]^{\binom{p^n}{p}} = e_0(xy,y)^{\binom{p^n}{p}},$$

pois $x^{p^n} \in Z(G)$. Logo, por (5.4),

$$e_0(xy,y)^{\binom{p^n}{p}} = e_0(x,y)^{\binom{0}{0}\cdot\binom{p^n}{p}} \cdot \prod_{s=1}^{p-1} e_s(x,y)^{\binom{s}{0}\cdot\binom{p^n}{p}}$$

e, daí, $1 = \prod_{s=1}^{p-1} e_s(x,y)^{(1,s)\alpha\binom{p^n}{p}}$, provando o desejado para $m = 1$. Agora, assuma que para um certo $m \in I_{p-2}$, tenhamos $\prod_{t=m}^{p-1} e_t(a,b)^{(m,t)\alpha\binom{p^n}{p}} = 1$, para todos $a, b \in G$. Dados $x, y \in G$, por (5.4),

$$\begin{aligned}
\prod_{t=m}^{p-1} e_t(xy,y)^{(m,t)\alpha} &= \prod_{t=m}^{p-1}\prod_{s=t}^{p-1} e_s(x,y)^{\binom{s}{t}(m,t)\alpha} \\
&= \left(\prod_{t=m}^{p-1} e_t(x,y)^{\binom{t}{t}\cdot(m,t)\alpha}\right)\left(\prod_{t=m}^{p-1}\prod_{s=t+1}^{p-1} e_s(x,y)^{\binom{s}{t}(m,t)\alpha}\right) \\
&= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha}\right)\left(\prod_{t=m}^{p-2}\prod_{s=t+1}^{p-1} e_s(x,y)^{\binom{s}{t}(m,t)\alpha}\right).
\end{aligned}$$

Para $t, s \in \mathbb{N}$, temos a equivalência:

$$(m \le t \le p-2) \wedge (t+1 \le s \le p-1) \iff (m \le t \le s-1) \wedge (m+1 \le s \le p-1).$$

Assim,

$$\begin{aligned}
\prod_{t=m}^{p-1} e_t(xy,y)^{(m,t)\alpha} &= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha}\right)\left(\prod_{t=m}^{p-2}\prod_{s=t+1}^{p-1} e_s(x,y)^{\binom{s}{t}(m,t)\alpha}\right) \\
&= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha}\right)\left(\prod_{s=m+1}^{p-1}\prod_{t=m}^{s-1} e_s(x,y)^{\binom{s}{t}(m,t)\alpha}\right) \\
&= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha}\right)\left(\prod_{s=m+1}^{p-1} e_s(x,y)^{\sum_{t=m}^{s-1}\binom{s}{t}(m,t)\alpha}\right) \\
&= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha}\right)\left(\prod_{s=m+1}^{p-1} e_s(x,y)^{(m+1,s)\alpha}\right).
\end{aligned}$$

Logo, pela hipótese de indução,

$$\begin{aligned}1 &= \prod_{t=m}^{p-1} e_t(xy,y)^{(m,t)\alpha\binom{p^n}{p}} \\ &= \left(\prod_{t=m}^{p-1} e_t(x,y)^{(m,t)\alpha\binom{p^n}{p}}\right)\left(\prod_{s=m+1}^{p-1} e_s(x,y)^{(m+1,s)\alpha\binom{p^n}{p}}\right) \\ &= \prod_{s=m+1}^{p-1} e_s(x,y)^{(m+1,s)\alpha\binom{p^n}{p}},\end{aligned}$$

provando o desejado.

Pela afirmação provada, $1 = \prod_{t=p-1}^{p-1} e_t(x,y)^{(p-1,t)\alpha\binom{p^n}{p}} = e_{p-1}(x,y)^{(p-1,p-1)\alpha\binom{p^n}{p}}$.

Veja que $(p-1,p-1)\alpha = (p-1)!$, provando que $\operatorname{mdc}((p-1,p-1)\alpha, p) = 1$. Como G é um p-grupo, temos que $\left|e_{p-1}(x,y)^{\binom{p^n}{p}}\right|$ é uma potência de p. Logo, $e_{p-1}(x,y)^{\binom{p^n}{p}} = 1$. Como $e_{p-1}(x,y) = [y,x,{}_{p-1}y]$, pelo Lema 5.1,

$$1 = [y,x,{}_{p-1}y]^{\binom{p^n}{p}} = [x,{}_p y]^{-\binom{p^n}{p}} = [y,x]^{-p^n} = [x,y]^{p^n}.$$

Assim, em todo caso, para todos $x, y \in G$, temos $[x,y]^{p^n} = 1$, ou seja, $[x,y] \in \Omega_{p^n}(G')$. Logo, pelo Teorema 3.11, $G' \leq \Omega_{p^n}(G') = \left\{g \in G' \,\middle|\, g^{p^n} = 1\right\}$. Portanto, $\exp(G') | p^n$. □

Dado um p-grupo finito G, vimos que G possui um grupo de recobrimento total U e que $G \wedge G \cong U'$. Usando este fato, como uma consequência do Teorema 5.2, temos o resultado a seguir.

Corolário 5.3. *[2, pág. 257] Se G é um p-grupo finito com classe de nilpotência no máximo p, então $\exp(G \wedge G) | \exp(G)$ e, consequentemente, $\exp(M(G)) | \exp(G)$.*

Demonstração. Pelo Teorema 1.24, existe um grupo de recobrimento total U de G. Seja K um subgrupo de $U' \cap Z(U)$ tal que $K \cong M(G)$ e $U/K \cong G$. O Teorema 1.21 nos diz que $M(G)$ é um p-grupo finito e, portanto, pelo Teorema 4.17, temos $U' \cong G \wedge G$. Além disso, como $U/K \cong G$, podemos afirmar que U é um p-grupo finito.

Pela Proposição 1.25, como $K \leq Z(U)$ e $\gamma_{p+1}(G) = \{1\}$, vemos que U tem classe de nilpotência no máximo $p+1$. Logo o Teorema 5.2 nos diz que $\exp(U') \,|\exp\left(U/Z(U)\right)$.

Como $K \leq Z(U)$, dado $uZ(U) \in U/Z(U)$, se escrevermos $n = \exp\left(U/K\right)$, de $K = u^n K$, obtemos $u^n \in K \leq Z(U)$ e, então, $(uZ(U))^n = u^n Z(U) = Z(U)$. Logo, $\exp\left(U/Z(U)\right) | n$. Além disso, já que $U/K \cong G$, vemos que $n = \exp\left(U/K\right) = \exp\left(G\right)$. Portanto, concluímos que $\exp(G \wedge G)$ divide $\exp(G)$. □

Veremos a seguir mais uma aplicação do conceito de p-grupo *powerful* no cálculo do limite de $\exp(G \wedge G)$ e, consequentemente, de $\exp(M(G))$.

Teorema 5.4. *[2, pág. 259] Seja G um p-grupo finito com p um primo ímpar e $\exp(G) = p^n$, com $n \geq 1$. Se as seguintes três condições são satisfeitas:*

- *G^p é powerful;*
- *$\exp(G^p) = p^{n-1}$;*
- *$\gamma_{p+1}(G) \leq G^p$;*

então, $\exp(G \wedge G) | \exp(G)$ e, em particular, $\exp(M(G)) | \exp(G)$.

Demonstração. O Corolário 4.21 nos diz que $\exp(G \wedge G)$ divide $\exp\left((G/G^p) \wedge (G/G^p)\right) \cdot \exp(G^p \wedge G)$. A Proposição 4.22 nos diz que $\exp(G^p \wedge G)$ divide $\exp(G^p)$. Além disso, podemos afirmar pelo Corolário 5.3, que $\exp\left((G/G^p) \wedge (G/G^p)\right)$ divide $\exp\left(G/G^p\right)$. É fácil ver que $\exp\left(G/G^p\right) | \, p$ e, consequentemente, temos $\exp(G \wedge G) \, | p \cdot \exp(G^p)$. Logo, $\exp(G \wedge G) \, | p^n$, como queríamos demonstrar. □

Dado um p-grupo finito G, com p ímpar, dizemos que G é *potent* se $\gamma_{p-1}(G) \leq G^p$. Note que todo p-grupo *powerful*, com p ímpar, é *potent*. Moravec [33] provou que $\exp(M(G)) | \exp(G)$ para todo p-grupo *potent* finito. Porém, no próximo parágrafo, apresentaremos uma outra prova para este fato usando o Teorema 5.4.

Seja G um p-grupo *potent* finito, com p ímpar e expoente p^n. Observamos que $\gamma_{p+1}(G) \leq \gamma_{p-1}(G) \leq G^p$. Além disso, por [18, Corolário 4.7], temos que G^p é *powerful*. Por fim, [4, Teorema 2] nos assegura que $G^p = \{g^p \mid g \in G\}$ e, consequentemente, $\exp(G^p) = p^{n-1}$. Portanto, pelo Teorema 5.4, podemos afirmar que $\exp(M(G)) | \exp(G)$.

Observamos que dado um número real x, os símbolos $\lceil x \rceil$ e $\lfloor x \rfloor$ denotam, respectivamente, o teto e piso de x.

A demonstração do resultado a seguir é uma parte da prova do Teorema 3.1 de [25].

Teorema 5.5. *Sejam p um primo e G um p-grupo finito com classe de nilpotência c. Então, para cada $i \in I_c$ temos:*

$$\exp(\gamma_{i+1}(G)) \left| p^{\lceil \log_p \frac{c}{i} \rceil - 1} \cdot \exp\left(\frac{G}{Z(G)}\right) \right. . \tag{5.5}$$

Demonstração. Podemos escrever $\exp\left(G/Z(G)\right) = p^n$ para algum $n \in \mathbb{N}$. Assim, vamos provar que para $i \in I_c$, vale $\exp(\gamma_{i+1}(G)) \left| p^{\lceil \log_p \frac{c}{i} \rceil - 1 + n} \right.$.

Se $c \leq p+1$, uma vez que $\gamma_{i+1}(G) \leq \gamma_2(G)$, o Teorema 5.2 nos diz que para qualquer $i \in I_c$, vale $\exp(\gamma_{i+1}(G)) | p^n$ e, então (5.5) acontece para este caso.

Portanto, nos preocuparemos agora com o caso $c \geq p+2$. Coloquemos $m = \left\lceil \frac{c}{p} \right\rceil$, fazendo com que $c > m$ e $pm \geq c$. Dessa forma, $\gamma_{pm+1}(G) \leq \gamma_{c+1}(G) = \{1\}$ e, portanto,

$\gamma_{pm+1}(G) = \{1\}$. Pelo Teorema 2.7,

$$\left[\gamma_m(G)^{p^n}, G\right] \equiv [\gamma_m(G), G]^{p^n} \left(\mathrm{mod} \prod_{j=1}^{n} [G, {}_{p^j}\gamma_m(G)]^{p^{n-j}}\right).$$

Do Lema 1.10 segue que para cada $j \in I_n$:

$$[G, {}_{p^j}\gamma_m(G)] \leq \gamma_{mp^j+1}(G) \leq \gamma_{mp+1}(G) = \{1\},$$

provando que $[G, {}_{p^j}\gamma_m(G)] = \{1\}$ para todo $j \in I_n$. Logo, $\prod_{j=1}^{n} [G, {}_{p^j}\gamma_m(G)]^{p^{n-j}} = \{1\}$, implicando em $\left[\gamma_m(G)^{p^n}, G\right] = [\gamma_m(G), G]^{p^n} = (\gamma_{m+1}(G))^{p^n}$. Já que $\exp(G/Z(G)) = p^n$, é certo que $\gamma_m(G)^{p^n} \leq Z(G)$, ou seja, $\left[\gamma_m(G)^{p^n}, G\right] = \{1\}$. Portanto, $(\gamma_{m+1}(G))^{p^n} = \{1\}$, isto é, $\exp(\gamma_{m+1}(G)) | p^n$. Assim, para todo $i \in I_c$ com $i \geq m$, temos $\exp(\gamma_{i+1}(G)) \, | p^n$, ou seja, $\exp(\gamma_{i+1}(G)) \left| p^{\lceil \log_p \frac{c}{i} \rceil - 1 + n} \right.$.

Provaremos por indução sobre $j \in \{0, \cdots, m-1\}$ que para cada $i \in I_c$, com $i \geq m-j$, temos:

$$\exp(\gamma_{i+1}(G)) \left| p^{\lceil \log_p \frac{c}{i} \rceil - 1 + n} \right. .$$

Com isso, para $j = m-1$, teremos o resultado desejado. Observamos que o caso $j = 0$ foi feito acima.

Agora, assuma que para um certo $j \in I_{m-1}$ o resultado é válido para todo $i \in I_c$ com $i \geq m-(j-1) = m-j+1$. Sendo $l = m-j$, para facilitar os cálculos, escrevemos $k = n + \lceil \log_p \frac{c}{l} \rceil - 1$ e então, pelo Teorema 2.7:

$$[\gamma_l(G), G]^{p^k} \equiv \left[\gamma_l(G)^{p^k}, G\right] \left(\mathrm{mod} \prod_{r=1}^{k} [G, {}_{p^r}\gamma_l(G)]^{p^{k-r}}\right). \tag{5.6}$$

Dado $r \in I_k$, vamos mostrar que $[G, {}_{p^r}\gamma_l(G)]^{p^{k-r}} = \{1\}$. Para $r \geq \lceil \log_p \frac{c}{l} \rceil$, temos que:

$$lp^r \geq lp^{\log_p \frac{c}{l}} = l\frac{c}{l} = c,$$

e, portanto, novamente pela Proposição 1.10,

$$\begin{aligned}[G, {}_{p^r}\gamma_l(G)]^{p^{k-r}} &= [G, \gamma_l(G), {}_{p^r-1}\gamma_l(G)]^{p^{k-r}} = [\gamma_{l+1}(G), {}_{p^r-1}\gamma_l(G)]^{p^{k-r}} \\ &\leq (\gamma_{l+1+(p^r-1)l}(G))^{p^{k-r}} = (\gamma_{lp^r+1}(G))^{p^{k-r}} \leq (\gamma_{c+1}(G))^{p^{k-r}} = \{1\}.\end{aligned}$$

Agora, para $r \leq \lceil \log_p \frac{c}{l} \rceil - 1$, é certo que $r < \log_p \frac{c}{l}$ e, assim, $lp^r < c$, ou seja, $lp^r \in I_c$. Além disso,

$$n + \left\lceil \log_p \frac{c}{lp^r} \right\rceil - 1 = n + \left\lceil \left(\log_p \frac{c}{l}\right) - (\log_p p^r) \right\rceil - 1 = k - r. \tag{5.7}$$

Agora, veja que $lp^r \geq l+1 \geq m-j+1$. Assim, pela hipótese de indução,

$\exp(\gamma_{lp^r+1}) \left| p^{\lceil \log_p \frac{c}{lp^r} \rceil -1+n}\right.$. Daí, de (5.7) obtemos $\exp(\gamma_{lp^r+1}) \left| p^{k-r}\right.$. Portanto,

$$\begin{aligned}[G, {}_{p^r}\gamma_l(G)]^{p^{k-r}} &= [G, \gamma_l(G), {}_{p^r-1}\gamma_l(G)]^{p^{k-r}} = [\gamma_{l+1}(G), {}_{p^r-1}\gamma_l(G)]^{p^{k-r}} \\ &\leq (\gamma_{l+1+(p^r-1)l}(G))^{p^{k-r}} = (\gamma_{lp^r+1}(G))^{p^{k-r}} = \{1\}.\end{aligned}$$

Mostramos assim que $[G, {}_{p^r}\gamma_l(G)]^{p^{k-r}} = \{1\}$ para todo $r \in I_k$. Desta forma, por (5.6), podemos afirmar que:

$$\gamma_{l+1}(G)^{p^k} = [\gamma_l(G), G]^{p^k} = \left[\gamma_l(G)^{p^k}, G\right].$$

Como $l = m - j$ e $j \in I_{m-1}$, temos que $l < m < c$ implicando em $l < c$ e, consequentemente, $\lceil \log_p \frac{c}{l} \rceil \geq 1$. Assim,

$$\gamma_l(G)^{p^k} = \gamma_l(G)^{p^{n+\lceil \log_p \frac{c}{l} \rceil -1}} \leq \left(\gamma_l(G)^{p^n}\right)^{p^{\lceil \log_p \frac{c}{l} \rceil -1}} \leq \gamma_l(G)^{p^n}.$$

Com isso em mente, lembrando que $\exp(G/Z(G)) = p^n$, temos que:

$$\left[\gamma_l(G)^{p^k}, G\right] \leq \left[\gamma_l(G)^{p^n}, G\right] = \{1\}.$$

Dessa forma, $\gamma_{l+1}(G)^{p^k} = \{1\}$, provando que $\exp(\gamma_{l+1}(G))$ divide $p^{n+\lceil \log_p \frac{c}{l} \rceil -1}$.

Provamos assim que para todo $i \in I_c$, com $i \geq m - j$, temos $\exp(\gamma_{i+1}(G))$ divide $p^{\lceil \log_p \frac{c}{i} \rceil -1+n}$. Dessa forma, provamos a afirmação por indução sobre $j \in \{0, \ldots, m-1\}$. Para $j = m - 1$, temos o resultado desejado. □

Fazendo $i = 1$ no Teorema 5.5, obtemos o seguinte.

Corolário 5.6. *Se G é um p-grupo finito com classe de nilpotência $c \geq 1$, então,*

$$\exp(\gamma_2(G)) \left| p^{\lceil \log_p c \rceil -1} \cdot \exp\left(\frac{G}{Z(G)}\right)\right. .$$

Na literatura encontramos cotas superiores para o expoente do quadrado exterior não abeliano de um p-grupo finito em função da sua classe de nilpotência. Por exemplo, se p é ímpar e c a classe de nilpotência de G, Sambonet [39, Theorem 1.1] provou que $\exp(G \wedge G) \mid \exp(G)^{\lfloor \log_{p-1} c \rfloor +1}$. Caso $c \geq p$, Antony, Komma e Thomas [2, Theorem 4.2] mostraram que $\exp(G \wedge G)$ divide $\exp(G)^k$, em que $k = \left\lceil \log_{p-1}\left(\frac{c+1}{p+1}\right)\right\rceil + 1$. Além disso, Bastos, Melo, Gonçalves e Monetta [5, Therem 1.4] estabeleceram que $\exp(G \wedge G)$ divide $\exp(G)^{\lceil \log_p(c+1)\rceil}$.

Como uma aplicação do Corolário 5.6, obtém-se a seguinte cota superior para o expoente de $G \wedge G$, o qual melhora alguns resultados prévios.

Teorema 5.7. *[25, pág. 5] Sejam p um primo e G um p-grupo finito. Se a classe de nilpotência*

de G é c, então $\exp(G \wedge G) \,|p^{n-1}\exp(G)$, *onde* $n = \lceil \log_p(c+1) \rceil$. *Em particular,* $\exp(M(G))$ *divide* $p^{n-1}\exp(G)$.

Demonstração. Pelo Teorema 1.21, é certo que $M(G)$ é um p-grupo finito, e portanto, finitamente gerado. Seja U um grupo de recobrimento de G. Então, U é um p-grupo, pois G e $M(G)$ satisfazem essa propriedade, e U tem classe de nilpotência d, com $d \leq c+1$. Além disso, pelo Teorema 4.17, temos $G \wedge G \cong U'$. Assim, do Corolário 5.6, obtemos:

$$\exp(G \wedge G) \,\Big|\, p^{\lceil \log_p d \rceil - 1} \cdot \exp\left(\frac{U}{Z(U)}\right). \tag{5.8}$$

Agora, $p^{\lceil \log_p d \rceil - 1}$ divide $p^{\lceil \log_p c+1 \rceil - 1}$ pois $d \leq c+1$. Ainda mais, sabemos que $U/K_1 \cong G$ para algum subgrupo K_1 de U tal que $K_1 \cong M(G)$ e $K_1 \leq U' \cap Z(U)$. Dessa forma, sendo $m = \exp(G)$, teremos $\exp\left(U/Z(U)\right) | \, m$.

Portanto, de (5.8) segue que $\exp(G \wedge G) \,\Big|\, p^{\lceil \log_p (c+1) \rceil - 1} \cdot \exp\left(G\right)$. □

Como uma aplicação do Teorema 5.7, temos o seguinte.

Corolário 5.8. *Sejam p um primo ímpar e G um p-grupo finito. Se a classe de nilpotência de G é menor ou igual a p^2-1, então* $\exp(G \wedge G) \,|p \exp(G)$. *Em particular,* $\exp(M(G)) \,|p \exp(G)$.

Demonstração. Note que, se c é a classe de nilpotência de G, do Teorema 5.7 segue que $\exp(G \wedge G) \,|p^{\lceil \log_p (c+1) \rceil - 1} \exp(G)$ Além disso, como $c \leq p^2-1$, temos que:

$$\lceil \log_p(c+1) \rceil \leq \lceil \log_p \left(p^2 - 1 + 1\right) \rceil = \lceil \log_p \left(p^2\right) \rceil = 2,$$

garantindo que $p^{\lceil \log_p (c+1) \rceil - 1}$ divide $p^{2-1} = p$. Portanto, $\exp(G \wedge G) \,|p \exp(G)$. □

Em [41], Vaughan-Lee apresentou um grupo que atinge o limite fornecido pelo Corolário 5.8. Neste texto, é exibido um 5-grupo finito G de classe de nilpotência 9, com $\exp(G) = 5$ e $\exp(M(G)) = 25$.

Do Corolário 5.8, segue que:

Corolário 5.9. *Sejam p um primo ímpar e G um p-grupo finito. Se a classe de nilpotência de G é menor ou igual a 8, então* $\exp(G \wedge G) \,|p \exp(G)$. *Em particular,* $\exp(M(G)) \,|p \exp(G)$.

Demonstração. É uma consequência direta do Corolário 5.8 uma vez que $8 \leq p^2 - 1$ para todo primo p ímpar. □

Nosso objetivo agora é, a partir de um p-grupo finito G, limitar seu expoente em função de $\exp(G')$ e do expoente de um p-subgrupo de Sylow de $Aut(G)$. Para tanto, necessitamos do seguinte resultado.

Teorema 5.10. *[8, Theorem 150.1, pág. 59] Sejam G um p-grupo finito e S um p-subgrupo de Sylow de $Aut(G)$. Se $\exp(S) = q$, então $\exp(Z(G))|q$ ou $\exp(G/G')|pq^2$.*

Demonstração. Primeiro notemos que como S é um p-grupo finito, temos que $q = p^n$ para algum $n \in \mathbb{N}$. Faremos a prova por contrapositiva. Assim, suponha que $\exp(Z(G))$ não divide p^n e $\exp(G/G')$ não divide pq^2.

Como $\exp(Z(G))$ e $\exp(G/G')$ são potências de base p, segue que $\exp(Z(G)) > p^n$ e $\exp(G/G') > p^{2n+1}$, ou seja, $\exp(Z(G)) \geq p^{n+1}$ e $\exp(G/G') \geq p^{2n+2}$.

Uma vez que G/G' é um grupo abeliano e finito, pelo Teorema Fundamental do Grupo Abeliano Finitamente Gerado, existem inteiros positivos $i_1, \ldots, i_k$ satisfazendo $G/G' \cong \mathbb{Z}_{i_1} \times \cdots \times \mathbb{Z}_{i_k}$ e $i_j | i_{j+1}$ para cada $j \in I_{k-1}$. Segue, assim, que $\exp(G/G') = i_k$ e, consequentemente, $i_k \geq p^{2n+2}$.

Escrevendo $A = \mathbb{Z}_{i_1} \times \cdots \times \mathbb{Z}_{i_{k-1}}$, existe um isomorfismo $\psi : G/G' \to A \times \mathbb{Z}_{i_k}$. Usaremos a notação aditiva quando nos referirmos às operações em A e $\mathbb{Z}_{i_j}$.

Agora, como $\exp(Z(G)) \geq p^{n+1}$, existe $y \in Z(G)$ tal que $|y| \geq p^{n+1}$, ou seja, $|y| = p^m$ para algum natural $m \geq n+1$. Consideremos o elemento central $z = p^{m-n+1}$, o qual satisfaz $|z| = p^{n+1}$ e a função:

$$\begin{array}{rccc} \alpha: & A \times \mathbb{Z}_{i_k} & \longrightarrow & \langle z \rangle \\ & (a, \overline{r}) & \longmapsto & z^r \end{array}.$$

Primeiramente vamos mostrar que α está bem definida. Sejam $(a, \overline{r}), (b, \overline{s}) \in A \times \mathbb{Z}_{i_k}$ com $(a, \overline{r}) = (b, \overline{s})$. Então, $a = b$ e $\overline{r} = \overline{s}$. Assim, $i_k | (r - s)$. Lembramos que i_k é uma potência de base p com $i_k \geq p^{2n+2}$ e, então, $p^{n+1} | \, i_k$. Logo, $p^{n+1} | \, (r - s)$, fazendo com que $z^{r-s} = 1$. Portanto, $z^r = z^s$. Assim, provamos que α está bem definida e é fácil ver que α é um homomorfismo.

Podemos, assim, tomar o homomorfismo $\beta = \pi \circ \psi \circ \alpha : G \to \langle z \rangle$ onde $\pi : G \to \frac{G}{G'}$ é o homomorfismo canônico. Se $g \in G$ é tal que $g^{p^{n+1}} = 1$ e $(a, \overline{r}) = (g)\pi \circ \psi \in A \times \mathbb{Z}_{i_k}$, temos:

$$\left(p^{n+1}a, p^{n+1}\overline{r}\right) = p^{n+1}(a, \overline{r}) = p^{n+1}((g)\pi \circ \psi) = \left(g^{p^{n+1}}\right)\pi \circ \psi = (1_G)\pi \circ \psi = (0_A, \overline{0}).$$

Assim, $\overline{p^{n+1}r} = \overline{0}$, fazendo com que $i_k | p^{n+1}r$. Como i_k é uma potência de base p e $i_k \geq p^{2n+2}$, é certo que $p^{2n+2} | \, i_k$ e, consequentemente, $p^{2n+2} | \, p^{n+1}r$. Portanto, $p^{n+1} | \, r$, o que implica em $z^r = 1$. Dessa forma,

$$(g)\beta = (g)\pi \circ \psi \circ \alpha = (a, \overline{r})\alpha = z^r = 1.$$

Logo, $g \in Ker(\beta)$ para todo $g \in G$ com $g^{p^{n+1}} = 1$. Uma vez que $|\langle z \rangle| = p^{n+1}$, é fato

que $\langle z\rangle \leq Ker(\beta)$.

Tomemos a aplicação:

$$\begin{array}{rccc} \sigma: & G & \longrightarrow & G \\ & g & \longmapsto & g\cdot(g)\beta \end{array}.$$

Vejamos que σ é um homomorfismo. Dados $g, h \in G$, veja que $(g)\beta, (h)\beta \in \langle z\rangle \leq Z(G)$. Assim,

$$(gh)\sigma = (gh)(gh)\beta = gh(g)\beta(h)\beta = g(g)\beta h(h)\beta = (g)\sigma(h)\sigma,$$

provando que σ é um homomorfismo.

Vamos mostrar por indução sobre $j \in \mathbb{N}^*$ que $(g)\sigma^j = g((g)\beta)^j$, para todo $g \in G$. Para $j = 1$, é óbvio. Suponhamos que a afirmação é verdadeira para algum $j \in \mathbb{N}^*$. Então,

$$(g)\sigma^{j+1} = \left((g)\sigma^j\right)\sigma = \left(g((g)\beta)^j\right)\sigma = \left(g((g)\beta)^j\right)\left(g((g)\beta)^j\right)\beta = g((g)\beta)^{j+1}\left(((g)\beta)^j\right)\beta.$$

De $Im(\beta) \leq \langle z\rangle$ e $\langle z\rangle \leq Ker(\beta)$, resulta que $(g)\sigma^{j+1} = g((g)\beta)^{j+1}$, provando o desejado por indução.

Além disso, para todo $g \in G$, temos que $|(g)\beta|$ divide p^{n+1} pois $(g)\beta \in \langle z\rangle$. Portanto, para todo $g \in G$, $(g)\sigma^{p^{n+1}} = g((g)\beta)^{p^{n+1}} = g$, de onde segue que $\sigma \circ \sigma^{p^{n+1}-1}$ e $\sigma^{p^{n+1}-1} \circ \sigma$ são a identidade em G, provando que σ é um isomorfismo.

Se $hG' = (0_A, \overline{1})\psi^{-1}$, onde 0_A é o elemento neutro de A, temos $(h)\beta = (h)\psi \circ \alpha = (0_A, \overline{1})\alpha = z$. Já provamos que $\sigma^{p^{n+1}} = Id_G$, onde Id_G representa o automorfismo identidade em G. Vamos provar que $|\sigma| = p^{n+1}$. Para cada $j \in \mathbb{N}^*$ com $j < p^{n+1}$, temos que $z^j \neq 1$ pois $|z| = p^{n+1}$. Assim,

$$(h)\sigma^j = h((h)\beta)^j = hz^j \neq h,$$

provando que $|\sigma| \neq j$. Logo, $|\sigma| = p^{n+1}$.

Como $\sigma \in Aut(G)$ e $|\sigma| = p^{n+1}$, podemos tomar um p-subgrupo de Sylow T de $Aut(G)$ tal que $\sigma \in T$. Logo, $\exp(T) \geq p^{n+1}$. Pelo Teorema de Sylow, é certo que S e T são conjugados, fazendo com que $\exp(S) = \exp(T) \geq p^{n+1}$, o que é uma contradição, já que $\exp(S) = q = p^n$. Isso conclui a prova do resultado. □

Dado um p-grupo finito G, temos que todo p-subgrupo de Sylow de $Aut(G)$ é um p-grupo finito. Com isso, provaremos o próximo teorema que nos dá limitantes para $\exp(G/Z(G))$ e $\exp(G)$. A sua demonstração pode também ser vista em [8, pág. 59].

Teorema 5.11. *Dado um p-grupo finito G, se S é um p-subgrupo de Sylow de $Aut(G)$, com*

$\exp(S) = q$, *então:*

$$\exp\left(\frac{G}{Z(G)}\right) \Big| q \quad e \quad \exp(G) \,|pq^2 \exp(G') \,.$$

Demonstração. Note que $G/Z(G) \cong \text{Inn}(G) \leq \text{Aut}(G)$, onde $\text{Inn}(G)$ denota o grupo de todos os automorfismos internos de G. Dessa forma, $\text{Inn}(G)$ é um p-grupo e, portanto, está contido em algum p-subgrupo de Sylow de $\text{Aut}(G)$, que será denotado por S_1.

Pelo Teorema de Sylow, é certo que S e S_1 são conjugados e, consequentemente, são isomorfos. Logo, $\exp(S_1) = \exp(S) = q$. Uma vez que $G/Z(G) \cong \text{Inn}(G) \leq S_1$, podemos afirmar que $\exp\left(G/Z(G)\right) | \, q$.

Pelo Teorema 5.10, temos que $\exp(Z(G))|q$ ou $\exp\left(G/G'\right) | \, pq^2$. Se $\exp(Z(G))|q$, é fácil ver que:

$$\exp(G) \left| \exp\left(\frac{G}{Z(G)}\right) \exp(Z(G)), \right.$$

o que implica em $\exp(G) \,|q^2$.

Agora, caso $\exp\left(G/G'\right) | \, pq^2$, de $\exp(G) \,|\exp\left(G/G'\right) \exp(G')$, obtemos $\exp(G)$ divide $pq^2 \exp(G')$. Logo, de todo modo, podemos afirmar que $\exp(G) \,|pq^2 \exp(G')$. □

O último teorema e o Corolário 5.6 permitiram que Komma e Thomas estabelecessem o seguinte limitante superior para $\exp(G)$.

Teorema 5.12. *[25, pág. 6] Sejam G um p-grupo finito de classe c e S um p-subgrupo de Sylow de $Aut(G)$, com $\exp(S) = q$. Então, $\exp(G)$ divide $p^{\lceil \log_p c \rceil} q^3$.*

Demonstração. Pelo Corolário 5.6, é certo que $\exp(G') \left| p^{\lceil \log_p c \rceil - 1} \cdot \exp\left(G/Z(G)\right) \right.$. Novamente, pelo Teorema 5.11, podemos afirmar que $\exp\left(G/Z(G)\right) | \, q$ e $\exp(G) \,|pq^2 \exp(G')$. Logo, $\exp(G') \left| p^{\lceil \log_p c \rceil - 1} \cdot q \right.$, fazendo com que $\exp(G) \left| pq^2 p^{\lceil \log_p c \rceil - 1} \cdot q \right.$, ou seja, $\exp(G)$ divide $p^{\lceil \log_p c \rceil} q^3$, como queríamos. □

A cota superior para $\exp(G)$ no Teorema 5.12 é para p-grupos finitos, mas pode ser estendida para grupos finitos de ordens arbitrárias fazendo uso do seguinte resultado:

Teorema 5.13. *Dado um grupo finito G, sejam $p_1, \ldots, p_k$ os primos divisores de $|G|$. Para cada $i \in I_k$, seja S_i um p_i-subgrupo de Sylow de G. Então, $\exp(G) = \prod_{i=1}^{k} \exp(S_i)$.*

Demonstração. Para cada $g \in G$, sejam $\varepsilon_g^{(1)}, \ldots, \varepsilon_g^{(k)} \in \mathbb{N}$ tais que $|g| = p_1^{\varepsilon_g^{(1)}} \cdots p_k^{\varepsilon_g^{(k)}}$. Para cada $i \in I_k$, coloquemos $\varepsilon^{(i)} = \max\left\{ \varepsilon_g^{(i)} \Big| \, g \in G \right\}$. Desse modo,

$$\exp(G) = \text{mmc}\{|g| \mid g \in G\} = \text{mmc}\left\{ p_1^{\varepsilon_g^{(1)}} \cdots p_k^{\varepsilon_g^{(k)}} \Big| \, g \in G \right\} = p_1^{\varepsilon^{(1)}} \cdots p_k^{\varepsilon^{(k)}}.$$

Assim, basta mostrarmos que $\exp(S_i) = p_i^{\varepsilon^{(i)}}$, para todo $i \in I_k$.

Dado $i \in I_k$, tome $g \in S_i$. Então $|g| = p^n$ para algum $n \in \mathbb{N}$. Dessa forma, $\varepsilon_g^{(i)} = n$ e $\varepsilon_g^{(j)} = 0$ para todo $j \in I_k \backslash \{i\}$. Pela forma com que tomamos $\varepsilon^{(i)}$, é fato que $n \leq \varepsilon^{(i)}$ e, daí, $g^{p^{\varepsilon^{(i)}}} = 1$. Assim, $g^{p^{\varepsilon^{(i)}}} = 1$ para todo $g \in S_i$, provando que $\exp(S_i) \leq p_i^{\varepsilon^{(i)}}$.

Agora, pela forma com que tomamos $\varepsilon^{(i)}$, existe $g \in G$ tal que $\varepsilon_g^{(i)} = \varepsilon^{(i)}$. Com isso, considerando $\delta = p_1^{\varepsilon_g^{(1)}} \cdots p_{i-1}^{\varepsilon_g^{(i-1)}} p_{i+1}^{\varepsilon_g^{(i+1)}} \cdots p_k^{\varepsilon_g^{(k)}}$, temos que $|g| = p_i^{\varepsilon^{(i)}}\delta$, ou seja, $\left|g^{\delta}\right| = p_i^{\varepsilon^{(i)}}$. Para facilitar os cálculos, escrevemos $h = g^{\delta} \in G$. Como a ordem de h é uma potência de p_i, é fato que h pertence a algum p_i-subgrupo de Sylow de G, que denotaremos por T_i. Como $|h| = p_i^{\varepsilon^{(i)}}$, teremos que $\exp(T_i) \geq \varepsilon^{(i)}$.

Uma vez que T_i e S_i são p_i-subgrupos de Sylow de G, pelo Teorema de Sylow, é fato que T_i e S_i são conjugados e portanto possuem o mesmo expoente. Logo, $\exp(S_i) \geq \varepsilon^{(i)}$. Provamos assim que $\exp(S_i) = \varepsilon^{(i)}$ e consequentemente, temos o resultado desejado. □

Assim, combinando os Teoremas 5.12 e 5.13, obtemos o seguinte:

Teorema 5.14. *[25, pág. 6] Sejam G um grupo finito e $p_1, \ldots, p_k$ os primos divisores de $|G|$. Para cada $i \in I_k$, sejam P_i um p_i-subgrupo de Sylow de G de classe c_i e S_i um p_i-subgrupo de Sylow de $Aut(P_i)$ com $\exp(S_i) = q_i$. Então:*

$$\exp(G) \left| \prod_{i=1}^{k} p_i^{\lceil \log_{p_i} c_i \rceil} q_i^3 \right. .$$

Demonstração. Pelo Teorema 5.12, é fato que para todo $i \in I_k$, vale $\exp(P_i) \left| p_i^{\lceil \log_{p_i} c_i \rceil} q_i^3 \right.$. Então $\prod_{i=1}^{k} \exp(P_i) \left| \prod_{i=1}^{k} p_i q_i^3 \right.$. Portanto, pelo Teorema 5.13, temos que $\exp(G)$ divide $\prod_{i=1}^{k} p_i^{\lceil \log_{p_i} c_i \rceil} q_i^3$. □

5.2 Expoente de p-grupos metabelianos de classe $2p-1$

Lembramos que um grupo é metabeliano se seu subgrupo derivado é abeliano. Do Teorema 5.7, segue que se G é um p-grupo finito de classe no máximo $2p-1$, então $\exp(G \wedge G) | p \exp(G)$. Entretanto, no caso em que G é um p-grupo metabeliano finito, Komma e Thommas [25] mostraram que essa cota superior para $\exp(G \wedge G)$ pode ser reduzida para $\exp(G)$ (veja Teorema 5.20 e Observação 5.21). O objetivo nesta seção é apresentar a demonstração deste fato.

Inicialmente, vamos apresentar algumas identidades de comutadores que são válidas em um grupo metabeliano. Suas provas são feitas através de cálculos rotineiros usando o Teorema 1.2 e serão omitidas.

Proposição 5.15. *Seja G um grupo metabeliano G. Para todos $x, y \in G'$, $a, b, c, d \in G$ e $n \in \mathbb{N}^*$, as seguintes identidades são válidas:*

(i) $[xy, a] = [x, a][y, a]$;

(ii) $[x, a^b] = [x, a]$;

(iii) $[x, a, b] = [x, b, a]$;

(iv) $[a, b, c]^{-1} = [b, a, c]$;

(v) $[a, b^n] = \prod_{i=1}^{n} [a, {}_i b]^{\binom{n}{i}}$;

(vi) $[ab, {}_n c] = [a, {}_n c]^b [b, {}_n c]$;

(vii) $[a[b, c], d] = [a, d][b, c, d]$.

Lema 5.16. *Sejam p um primo e G um p-grupo finito metabeliano de classe menor ou igual a $2p-1$ tal que $\gamma_{p+1}(G) \leq [G^p, G]$. Então, $[G^p, G^p] \leq [G^p, G]^p$.*

Demonstração. Pelo Teorema 2.7, temos:

$$[G^p, G^p] \leq [G^p, G]^p \, [G^p, {}_p G] \, . \tag{5.9}$$

Agora, usando o Teorema 2.8 e o fato que $\gamma_{2p}(G) = \{1\}$, obtemos:

$$[G^p, {}_p G] \leq [G, {}_p G]^p \, [G, {}_{2p-1} G]^{p^{1-r}} = [G, {}_p G]^p \gamma_{2p}(G)^{p^{1-r}} = [G, {}_p G]^p.$$

Assim, de (5.9) e pela hipótese, segue que:

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

como queríamos. □

Lema 5.17. *Dados um p-grupo metabeliano G e subgrupos normais N e M de G, com $N \leq G'$, para todo $k \in \mathbb{N}$, temos $\left[N^k, M\right] = [N, M]^k$.*

Demonstração. Como G é metabeliano e $N \leq G'$, para todos $m \in M$ e $n \in N$, temos $\left[n^k, m\right] = [n, m]^k$. Além disso, pelo fato de N e $[N^k, M]$ serem subgrupos abelianos de G, é fato que:

$$[N^k, M] = \left\langle [n^k, m] \mid n \in N, m \in M \right\rangle = \left\langle [n, m]^k \mid n \in N, m \in M \right\rangle = [N, M]^k,$$

como queríamos. □

O próximo resultado provado por Komma e Thomas, fornece cotas superiores para os expoentes de $\gamma_2(G)$ e $\gamma_3(G)$ para um p-grupo metabeliano G de classe de nilpotência menor ou igual a $2p-1$.

Proposição 5.18. *[25] Sejam p um primo e G um p-grupo finito metabeliano de classe de nilpotência menor ou igual a $2p-1$ tal que $\gamma_{p+1}(G) \leq [G^p, G]$. Se $\exp(G) = p^n$, com $n \geq 2$, então:*

(i) $\exp(\gamma_2(G^p)) \mid p^{n-1}$;

(ii) $\exp(\gamma_3(G^p)) \mid p^{n-2}$.

Demonstração. Como $\exp(G) = p^n$ e G é metabeliano, pelo Lema 5.16,

$$(\gamma_2(G^p))^{p^{n-1}} = [G^p, G^p]^{p^{n-1}} \leq ([G^p, G]^p)^{p^{n-1}} = \{1\},$$

provando o primeiro item.

Agora, pelos Lemas 5.16 e 5.17, é certo que:

$$[G^p, G^p, G^p] \leq [[G^p, G]^p, G^p] = [G^p, G, G^p]^p \leq [G^p, G^p]^p = (\gamma_2(G^p))^p.$$

Logo, como $\gamma_2(G^p)$ é abeliano:

$$(\gamma_3(G^p))^{p^{n-2}} \leq [(\gamma_2(G^p))^p]^{p^{n-2}} = (\gamma_2(G^p))^{p^{n-1}} = \{1\},$$

e isto prova o segundo item. □

Corolário 5.19. *Sejam p um primo ímpar e G um p-grupo metabeliano finito de classe menor ou igual a $2p-1$ tal que $\gamma_{p+1}(G) \leq [G^p, G]$. Se $\exp(G) = p^n$, com $n \geq 1$, então $\exp(G^p) = p^{n-1}$.*

Demonstração. Se $n = 1$, então $\exp(G) = p$ e, daí, certamente $\exp(G^p) = 1$.

Agora, suponhamos que $n \geq 2$. Se $m = n-2$, temos que $m+1 = n-1$ e, como $\exp(G) = p^n$, existe $x \in G$ tal que $x^{p^{m+1}} \neq 1$, ou seja, $(x^p)^{p^m} \neq 1$ fazendo com que $\exp(G^p) \geq p^{n-1}$.

Portanto, basta provarmos que $x^{p^{n-1}} = 1$ para todo $x \in G^p$. Para cada $x \in G^p \backslash \{1\}$, existem $x_1, \ldots, x_k \in G$ tais que $x = x_1^p \cdots x_k^p$. Se $k = 1$, então $x^{p^{n-1}} = (x_1^p)^{p^{n-1}} = x^{p^n} = 1$ pois $\exp(G) = p^n$. Por outro lado, se $k \geq 2$, pelo Teorema 2.6, é certo que:

$$(x_1^p \cdots x_k^p)^{p^{n-1}} \equiv x_1^{p^n} \cdots x_k^{p^n} \left(\mathrm{mod}\ \gamma_2(G^p)^{p^{n-1}} \left(\prod_{i=1}^{n-1} \gamma_{p^i}(G^p)^{p^{n-1-i}} \right) \right).$$

Para $i \geq 2$, temos que $\gamma_{p^i}(G^p) = \{1\}$ pois G é nilpotente de classe menor ou igual a $2p-1$ e $p^i \geq p^2 \geq 2p$. Além disso, pela Proposição 5.18, é fato que $\gamma_2(G^p)^{p^{n-1}} = \{1\} =$

$\gamma_3(G^p)^{p^{n-2}}$. Uma vez que $p \geq 3$, temos que $\gamma_p^{p^{n-2}}(G^p) \leq \gamma_3^{p^{n-2}}(G^p)$ e, portanto:

$$(x_1^p \cdots x_k^p)^{p^{n-1}} \equiv x_1^{p^n} \cdots x_k^{p^n} \pmod{\{1\}},$$

isto é, $x^{p^{n-1}} = (x_1^p \cdots x_k^p)^{p^{n-1}} = x_1^{p^n} \cdots x_k^{p^n} = 1$, já que $\exp(G) = p^n$. Dessa forma, $x^{p^{n-1}} = 1$ para todo $x \in G^p$ fazendo com que $\exp(G^p) \leq p^{n-1}$. Concluímos assim que $\exp(G^p) = p^{n-1}$. □

Komma e Thomas provaram o próximo resultado em [25], fornecendo outra classe de grupos G que satisfazem $\exp(M(G)) | \exp(G)$.

Teorema 5.20. *[25] Seja G um p-grupo finito metabeliano com p um primo ímpar. Se a classe de nilpotência de G é menor ou igual a $2p-1$ e $\gamma_{p+1}(G) \leq [G^p, G]$, então $\exp(G \wedge G) | \exp(G)$. Consequentemente $\exp(M(G)) | \exp(G)$.*

Demonstração. Podemos escrever $\exp(G) = p^n$, para algum $n \in \mathbb{N}$. Se $n = 0$, ou seja, G é o grupo trivial, então, $G \otimes G$ é o subgrupo trivial. Dessa forma, o resultado vale quando $n = 0$.

Agora, para $n \geq 1$, basta provarmos que as três condições do Teorema 5.4 se verificam. Pelo Lema 5.16, temos que $\gamma_2(G^p) \leq [G^p, G]^p \leq (G^p)^p$, provando que G^p é *powerful*. Do Corolário 5.19, segue que $\exp(G^p) = p^{n-1}$. Da hipótese, temos $\gamma_{p+1}(G) \leq [G, G^p] \leq G^p$. Assim, o Teorema 5.4 nos permite afirmar que $\exp(G \wedge G) | \exp(G)$ e $\exp(M(G)) | \exp(G)$. □

Observação 5.21. Seja G um p-grupo metabeliano finito. Kappe e Morse [22] mostraram que $G^p \leq Z(G)$ se, e somente se, $\exp(G') \mid p$ e G tem classe de nilpotência no máximo p. Não é difícil ver que o p-grupo metabeliano $G/[G, G^p]$ satisfaz:

$$\left(\frac{G}{[G, G^p]}\right)^p \leq Z\left(\frac{G}{[G, G^p]}\right).$$

Logo, $\gamma_{p+1}(G/[G, G^p]) = \{1\}$ e isso nos diz que:

$$\gamma_{p+1}(G) \leq [G, G^p]. \tag{5.10}$$

Desta forma, a condição (5.10) pode ser retirada da hipótese de todos os resultados desta seção, conforme fizeram Komma e Thomas em [25] e o Teorema 5.20 pode ser reenunciado da seguinte forma:

Teorema 5.22. *[25] Seja G um p-grupo finito metabeliano com p um primo ímpar. Se a classe de nilpotência de G é menor ou igual a $2p-1$, então $\exp(G \wedge G) | \exp(G)$. Consequentemente $\exp(M(G)) | \exp(G)$.*

REFERÊNCIAS BIBLIOGRÁFICAS

[1] A. E. Antony, P. Komma, and V. Z. Thomas. On the exponent conjecture of Schur. *arXiv preprint arXiv:1906.09585*, 2020.

[2] A. E. Antony, P. Komma, and V. Z. Thomas. A property of p-groups of nilpotency class p+ 1 related to a theorem of Schur. *Israel Journal of Mathematics*, pages 251–267, 2022.

[3] A. E. Antony and V. Z. Thomas. On the exponent conjectures. *arXiv preprint arXiv:2005.11513*, 2020.

[4] D. Arganbright. The power-commutator structure of finite p-groups. *Pacific Journal of Mathematics*, 29(1):11–17, 1969.

[5] R. Bastos, E. de Melo, N. Gonçalves, and C. Monetta. The exponent of the non-abelian tensor square and related constructions of p-groups. *Mathematische Nachrichten*, 295(7):1264–1278, June 2022.

[6] R. Bastos, I. N. Nakaoka, and N. R. Rocco. Finiteness conditions for the non-abelian tensor product of groups. *Monatshefte für Mathematik*, 187:603–615, 2018.

[7] A. J. Bayes, J. Kautsky, and J. W. Wamsley. Computation in nilpotent groups (application). In M. F. Newman, editor, *Proceedings of the Second International Conference on the Theory of Groups*, pages 82–89, Berlin, Heidelberg, 1974. Springer Berlin Heidelberg.

[8] Y. Berkovich and Z. Janko. *Groups of Prime Power Order*, volume 4. de Gruyter, 2008.

[9] R. Brown, D. L. Johnson, and E. F. Robertson. Some computations of non-abelian tensor products of groups. *Journal of Algebra*, 111(1):177–202, 1987.

[10] R. Brown and J. L. Loday. Excision homotopique en basse dimension. *CR Acad. Sci. Paris SI Math*, 298(15):353–356, 1984.

[11] R. Brown and J. L. Loday. Van kampen theorems for diagrams of spaces. *Topology*, 26(3):311–335, 1987.

[12] C. B. da Cunha. Ações nilpotentes em produtos tensoriais não abeliano de grupos. *Dissertação (Mestrado em Matemática) - Universidade de Brasília*, 2023.

[13] G. Donadze, M. Ladra, and V. Z. Thomas. On some closure properties of the non-abelian tensor product. *Journal of Algebra*, 472:399–413, 2017.

[14] G. Ellis. On the relation between upper central quotients and lower central series of a group. *Transactions of the American Mathematical Society*, 353(10):4219–4234, 2001.

[15] G. J. Ellis. Non-abelian exterior products of groups and exact sequences in the homology of groups. *Glasgow Mathematical Journal*, 29(1):13–19, 1987.

[16] G. A. Fernández-Alcober, J. González-Sánchez, and A. Jaikin-Zapirain. Omega subgroups of pro-p groups. *Israel Journal of Mathematics*, 166(1):393–412, 2008.

[17] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.

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

[19] B. Huppert. *Endliche gruppen I*, volume 134. Springer-verlag, 2013.

[20] D. L. Johnson. *Topics in the theory of group presentations*, volume 42. Cambridge University Press, 1980.

[21] D. L. Johnson. *Presentations of Groups*. London Mathematical Society Student Texts. Cambridge University Press, 2 edition, 1997.

[22] L. C. Kappe and R. F. Morse. Levi-properties in metabelian groups. *Contemp. Math*, 109:59–72, 1990.

[23] G. Karpilovsky. *The Schur multiplier*. Oxford University Press, Inc., 1987.

[24] E. I. Khukhro and P. Shumyatsky. Bounding the exponent of a finite group with automorphisms. *Journal of Algebra*, 212(1):363–374, 1999.

[25] P. Komma and V. Z. Thomas. Bounding the exponent of a finite group by the exponent of the automorphism group and a theorem of Schur. *arXiv preprint arXiv:2112.01024*, 2021.

[26] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*. Number 27 in London Mathematical Society Monographs. Oxford University Press, 2002.

[27] M. D. Lima. Sobre a invariância do produto tensorial não abeliano de grupos. *Dissertação (Mestrado em Matemática) - Universidade Federal de Goiás*, 2015.

[28] A. Lubotzky and A. Mann. Powerful p-groups. i. finite groups. *Journal of Algebra*, 105(2):484–505, 1987.

[29] A. Mann. Groups with few class sizes and the centraliser equality subgroup. *Israel Journal of Mathematics*, 142:367–380, 2004.

[30] A. Mann. The exponents of central factor and commutator groups. *Journal of Group Theory*, 10(4):435–436, 2007.

[31] C. Miller. The second homology group of a group; relations among commutators. *Proceedings of the American Mathematical Society*, 3(4):588–595, 1952.

[32] P. Moravec. Schur multipliers and power endomorphisms of groups. *Journal of Algebra*, 308(1):12–25, 2007.

[33] P. Moravec. On pro-p groups with potent filtrations. *Journal of Algebra*, 322(1):254–258, 2009.

[34] I. N. Nakaoka. Sobre o produto tensorial não abeliano de grupos. *Dissertação (Mestrado em Matemática) - Universidade Estadual de Campinas*, 1994.

[35] G. R. Ortega. Propriedades de fecho e condições de finitude para o produto tensorial não abeliano de grupos. *Dissertação (Mestrado em Matemática) - Universidade Estadual de Maringá*, 2021.

[36] D. J. S. Robinson. *A Course in the Theory of Groups*. Springer Science & Business Media, 2 edition, 2012.

[37] N. R. Rocco. Métodos de Lie em teoria dos grupos. In S. N. Sidki, editor, *ATAS DA IX ESCOLA DE ALGEBRA*, volume 2, pages 129–213, Brasília, 1987. SBM.

[38] J. J. Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.

[39] N. Sambonet. Bounds for the exponent of the Schur multiplier. *Journal of Pure and Applied Algebra*, 221(8):2053–2063, 2017.

[40] I. Schur. Über die darstellung der endlichen gruppen durch gebrochen lineare substitutionen. *Journal für die reine und angewandte Mathematik*, 127:20 – 50, 1904.

[41] M. Vaughan-Lee. Schur's exponent conjecture – counterexamples of exponent 5 and exponent 9. *arXiv preprint arXiv:2008.06848*, 2020.

[42] P. V. Vitor. Produto tensorial nao abeliano de grupos. *Dissertação (Mestrado em Matemática) - Universidade Estadual de Maringá*, 2015.

[43] J. H. C. Whitehead. A certain exact sequence. *Annals of Mathematics*, pages 51–110, 1950.

Índice Remissivo

apresentação livre, 10
ações compatíveis, 44

biderivação, 45

classe de nilpotência, 7
commutator collection formulae, 29
comutador, 5
    formal, 14
        básico, 14
    simples, 5
conjugado, 5

extensão, 12

fecho normal, 4
funtor quadrático de Whitehead, 50

geradores, 10
grupo
    de recobrimento, 13
        total, 13
    livre, 10
    nilpotente, 7
    potent, 69
    powerful, 32
    regular, 39
    solúvel, 6

homomorfismo canônico, 4

Identidade
    de Hall-Witt, 5
    de Jacobi, 5

lema
    dos cinco, 12
    dos três subgrupos, 9

multiplicador de Schur, 13
módulo cruzado, 47

permutação compatível, 15
peso, 14
processo de coleta, 14
produto
    exterior não abeliano, 58
    livre, 11
    tensorial não abeliano, 44
propriedade universal, 45

quadrado
    exterior não abeliano, 50
    tensorial não abeliano, 45

relatores, 10
relações definidoras, 10

sequência exata, 11
    curta, 12
        central, 12
subgrupo
    característico, 4
    de Frattini, 38
    derivado, 6

derivativo, 48
powerfully embedded, 32
série
central, 7
inferior, 7
superior, 7
derivada, 6
solúvel, 6

teste da substituição, 11