Universidade de Brasília

Produto de comutadores em Grupos

Miguel Neto Hipólito

Orientador: Dr. Raimundo de Araújo Bastos Júnior

Departamento de Matemática
Universidade de Brasília

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

Brasília, 16 de julho de 2021

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de
Matemática

Produto de Comutadores em Grupos

Miguel Neto Hipolito *

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

MESTRE EM MATEMÁTICA

Brasília, 10 de novembro de 2022.

Comissão Examinadora:

Prof. Dr. Raimundo de Araújo Bastos Júnior - MAT/UnB (Orientador)

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

Prof. Dr. Csaba Schneider – UFMG (Membro)

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

Np

Neto Hipólito, Miguel
Produto de comutadores em Grupos / Miguel Neto Hipólito; orientador Raimundo de Araújo Bastos Júnior. -- Brasília, 2022.
66 p.

Tese(Mestrado em Matemática) -- Universidade de Brasília, 2022.

1. Grupos Finitos. 2. Largura de Grupos. 3. Produtos Entrelaçados. 4. Subgrupo Derivado. 5. Grupos de Matrizes. I. Bastos Júnior, Raimundo de Araújo, orient. II. Título.

Dedico esse trabalho aos meus famíliares, em especial a minha mãe Genilda Rita Hipólito e ao meu pai Manoel Eronaldo Neto.

Agradecimentos

Agradeço primeiramente à Deus por ter me dado forças e discernimento para enfrentar esse desafio.

À minha mãe Genilda Rita Hipólito, meu pai Manoel Eronaldo Neto e minha irmã Isabella Rita Hipólito pelo apoio em todas as etapas da minha vida, sempre me dando suporte em tudo que eu necessitei.

À meus primos Matheus, Mara, Marta, Lucas, Priscilla, Douglas, José Ivan, Sophia, Maria Clara, Rita Laraiane, Kaiky, Pedro Henrique, Taís, Márcio, por cada conselho e cada rolê que me proporcionaram. À minhas tias Marinalva, Maria do Socorro, Enói, por sempre me incentivarem.

Aos meus colegas de graduação Lilia, Eduarda, Maria Luiza por cada conversa, por sempre me ajudarem nas dificuldades da vida acadêmica.

Aos meus colegas de pós-graduação Paulo de Tarso, Caio, Tharles, Ayrton, Júlia pelos auxilios na elaboração da dissertação.

Ao meu orientador Raimundo de Araújo Bastos Júnior, eu agradeço por todos esses anos de trabalho juntos. Pela paciência e dedicação que teve comigo em cada trabalho que desenvolvemos, em especial esta dissertação de mestrado. Por cada conselho, cada puxão de orelha que me ajudaram a crescer profissionalmente e também como pessoa.

Aos membros da banca examinadora, Alex Carrazedo Dantas, Emerson Ferreira de Melo e Csaba Schneider, por todas as correções e sugestões.

Aos professores que contribuíram para a minha formação durante o mestrado, Alex Carrazedo Dantas, Willian Cintra, José Luis Teruel, Ary Vasconcelos, Emerson Ferreira de Melo.

À Capes pelo apoio financeiro para o desenvolvimento deste trabalho.

Resumo

O objetivo desse trabalho será estudar duas classes de problemas: critérios que garantem a existência de elementos não comutadores em determinados grupos; e numa perspectiva complementar, analisar critérios nos quais o subgrupo derivado coincide com o conjunto de comutadores.

Palavras-chave: Conjunto de Comutadores, Subgrupo Comutador, Largura de um grupo.

Abstract

The aim of this work will be to study two kind of problems: obtain sufficient conditions to guarantee the existence of non-commutator elements in certain groups; and in a complementary perspective, describe criteria in which the derived subgroup coincides with the set of all commutators.

Keywords: Set of Commutators, Commutator subgroup, Width of a group.

Conteúdo

Introdução

Os resultados aqui apresentados estão relacionados a teoria dos comutadores em grupos. Apresentamos dois tipos de resultados: condições suficientes para que o conjunto dos comutadores de um grupo coincida com o seu subgrupo derivado; e, numa direção oposta, construir grupos que possuem elementos no subgrupo derivado que não são comutadores. Todos os teoremas e exemplos aqui apresentados foram baseados nos trabalhos de P. J. Cassidy [1], M. Isaacs [6], R. M. Guralnick [4, 5], E. Spiegel [11]. Cabe ressaltar que fizemos uso do software livre GAP [2] e das notas de um minicurso do professor C. Schneider [10].

Definiremos/Fixaremos alguns termos para simplificar a leitura do texto. O conjunto dos comutadores e o subgrupo derivado (de um grupo G) são denotados e definidos como $\Gamma(G) = \{[x,y] \mid x,y \in G\}$ e é $G' = \langle \Gamma(G) \rangle$, respectivamente. Além disso, definimos a largura de um grupo G como

$$\lambda(G) = min\{n \in \mathbb{N} \mid \forall \alpha \in G' : \alpha = \prod_{i=1}^{m}[g_i,h_i],\ g_i,h_i \in G,\ m \leq n\}.$$

Ou seja, o menor inteiro positivo $n = n(G)$ para o qual todos os elementos do subgrupo derivado podem ser escritos como o produto de, no máximo, n comutadores. Em particular, $\lambda(G) = 1$ se, e somente se, $G' = \Gamma(G)$. Daí, a partir de agora, quando nos referirmos a grupos G com largura 1 podemos escrever $\lambda(G) = 1$ ou $\Gamma(G) = G'$.

Em 1951, Oystein Ore [7] escreveu a seguinte frase em seu artigo.

> "Em um grupo, o produto de dois comutadores não precisa ser necessariamente um comutador, consequentemente o subgrupo de comutadores de um dado grupo não pode ser definido como o conjunto de comutadores, mas apenas o grupo gerado por estes elementos."

Cabe ressaltar que tais questões já haviam sido investigadas por outros matemáticos. Em todo caso, no contexto da frase de Ore [7] duas perguntas se sobressaem:

Em quais condições podemos afirmar que em um grupo G vale $\Gamma(G) = G'$*?*

Quais critérios um grupo G deve ter para possuir $\lambda(G) > 1$?

E é em cima destes questionamentos, que neste trabalho estudaremos alguns artigos da literatura em que desenvolvem ferramentas para que consigamos responder se um dado grupo G possui alguma dessas propriedades.

Inicialmente, estudaremos uma condição suficiente para $G' = \Gamma(G)$. Para isso, definamos pra todo $x \in G$ o conjunto dos conjugados de x como $C_x = x^G = \{a^{-1}xa \mid a \in G\}$. E assim, definimos $B_x = \{st \mid s \in C_{x^{-1}},\ t \in C_x\}$. E com esse conjunto, baseados no trabalho de E. Spiegel [11], mostramos dois critérios que fazem com que o conjunto de comutadores seja igual ao subgrupo derivado. Mais precisamente,

Teorema A: *Seja x um elemento de um grupo G. Suponhamos que o subconjunto B_x é um subgrupo de G com $\Gamma(G) \subset B_x$. Então $\Gamma(G) = B_x = G'$.*

Teorema B: *Seja G um grupo. Se existe um subgrupo normal e abeliano N de G tal que G/N é um grupo cíclico gerado por xN, com $x \in G$, então $B_x = \Gamma(G) = G'$.*

Uma consequência (particular e) imediata do Teorema acima é o seguinte:

Corolário C: *Seja G um grupo metacíclico finito. Então $\lambda(G) = 1$.*

A partir de agora estaremos interessados em construir grupos nos quais $\lambda(G) > 1$. No artigo [5], R. M. Guralnick mostrou que se $|G| < 96$ ou $|G'| < 24$, então $\lambda(G) = 1$. Mais ainda, em [4], ele construiu explicitamente um grupo G de ordem 96 com $\lambda(G) = 2$. Aqui, com o auxílio do GAP e do artigo [4] mostramos:

Teorema D: *Seja G um grupo de ordem $\leqslant 96$.*

(i) *Se $|G| \leqslant 95$, então $\lambda(G) = 1$.*

(ii) *Existe, exatamente, dois grupos de ordem 96 com $\lambda(G) > 1$.*

Cabe destacar que a parte mais complicada do resultado acima é o item (i), pois envolve teoria de representações. Para contornar essa situação usamos uma rotina do GAP e verificamos que para todos os grupos com ordem até 95 o subgrupo derivado e conjuntos dos comutadores coincidem.

No trabalho [6], M. Isaacs usou produtos entrelaçados com o intuito de obter grupos da forma $G = U \wr H$ que possuem elementos não comutadores a partir de certas condições aritméticas e estruturais sobre os grupos envolvidos. Mais precisamente,

Teorema E: *Sejam U e H grupos finitos com U abeliano e H não abeliano. Consideremos $G = U \wr H$. Se*

$$\sum_{A \in \mathscr{A}} \left(\frac{1}{|U|} \right)^{|H:A|} < \frac{1}{|U|},$$

então $\lambda(G) > 1$, sendo que $\mathscr{A}$ é o conjunto dos subgrupos abelianos maximais de H.

A partir desses resultados construímos famílias de exemplos (cf. Exemplos 4.2.2, 4.2.3, e 4.2.4).

Até aqui os grupos envolvidos, em sua maioria, são finitos. Em particular, tais grupos tem largura finita. Agora, a partir do trabalho de P. J. Cassidy [1], construíremos grupos nilpotentes de classe 2 que possui largura infinita, ou seja $\lambda(G) = \infty$.

Seja $\mathbb{K}$ um corpo. Seja $\mathbb{K}[x,y]$ o anel dos polinômios em duas variaveis sobre o corpo $\mathbb{K}$. Em $\mathbb{K}[x,y]$, consideremos $\mathbb{K}[x]$, $\mathbb{K}[y]$ os subanéis dos polinômios nas variáveis x e y, respectivamente. Definamos,

$$G_{\mathbb{K}} = \left\{ \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \mid f \in \mathbb{K}[x], g \in \mathbb{K}[y], h \in \mathbb{K}[x,y] \right\}.$$

Teorema F: *Seja $\mathbb{K}$ um corpo. Então*

(i) *O grupo $G_{\mathbb{K}}$ é nilpotente de classe 2.*

(ii) $G'_{\mathbb{K}} = Z(G_{\mathbb{K}})$.

(iii) $\lambda(G_{\mathbb{K}}) = \infty$.

O trabalho está dividido em quatro Capítulos. Segue o que é feito em cada um deles:

No **Capítulo 1:** incluímos alguns resultados da Teoria de Grupos, no qual vemos propriedades necessárias para o desenvolvimento e entendimento dos capítulos subsequentes.

No **Capítulo 2:** Primeiramente, definiremos o conjunto dos conjugados de um elemento $x \in G$ dado pela forma $C_x = x^G = \{a^{-1}xa \mid a \in G\}$. E assim, definiremos $B_x = \{st \mid s \in C_{x^{-1}},\ t \in C_x\}$. Com esses objetos, iremos desenvolver o critério feito por Spiegel [11] no qual garante que os grupos em que o satisfaz possem $G' = \Gamma(G)$. Mais explicitamente, estudaremos as demonstrações dos resultados: Teoremas A, B e o Corolário C. E por fim, mostraremos diversos exemplos de aplicações desses resultados.

No **Capítulo 3:** Começaremos desenvolvendo um algoritmo no software livre GAP que nos dará a informação de Grupos nos quais $G' \neq \Gamma(G)$. Com este algoritmo, analisaremos os grupos de ordem até 96 e aos grupos em que tiver como característica o subgrupo derivado diferente do conjunto de comutadores, introduziremos a outro algoritmo desenvolvido para que visualizemos diversas propriedades sobre estes determinados grupos.

Logo após, estudaremos o método de construção criado pro Guralnick [4] em que justifica os grupos encontrados pelo algoritmo do software GAP terem $G' \neq \Gamma(G)$. E assim, veremos com o auxílio do GAP e a construção de Guralnick [4], a validade do Teorema D.

No **Capítulo 4:** Estudaremos um critério, desenvolvido por Isaacs [6], para a construção de Produtos entrelaçados no qual possuem $G' \neq \Gamma(G)$. Para isso, desenvolveremos a demonstração do Teorema E. Logo após, criaremos exemplos de famílias de Produtos Entrelaçados que possuem elementos não comutadores. E por fim, estudaremos um grupo construído por Cassidy [1], definido pela forma

$$G_{\mathbb{K}} = \left\{ \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \mid f \in \mathbb{K}[x], g \in \mathbb{K}[y], h \in \mathbb{K}[x,y] \right\},$$

no qual possui $\lambda(G) = \infty$. Mais especificamente, demonstraremos o Teorema F.

Capítulo 1

Preliminares

Assumimos que o leitor tem familiaridade com os conceitos básicos da Teoria de Grupos. Alguns teoremas como o Teorema de Lagrange e os Teoremas de Isomorfismo também são assumidos como conhecidos, podendo serem encontrados em vários referências, em particular em [3]. A construção deste capítulo foi baseada em [8, Capítulos 1, 5, 10 e 14].

1.1 Comutadores e Conjugados

Definição 1.1.1. *Seja G um grupo. Definimos como o conjugado de x por y o elemento da forma*

$$x^y = y^{-1}xy \in G$$

De maneira análoga, determinamos o conjugado de x^{-1} por y como

$$x^{-y} = y^{-1}x^{-1}y \in G.$$

Definição 1.1.2. *Sejam G um grupo e $x, y \in G$. Definimos o comutador de x e y como o elemento de G da forma*

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

Assim, o conjunto de todos os comutadores de G será denotado por

$$\Gamma(G) = \{[x,y] \mid x,y \in G\}.$$

Lema 1.1.3. *Se G é um grupo e $x,y,z \in G$, então*

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

(ii) $[xy,z] = y^{-1}[x,z]y[y,z]$;

(iii) Se x comuta com $[x,y]$, então $[x^k,y]=[x,y]^k$;

(iv) Se y comuta com $[x,y]$, então $[x,y^k]=[x,y]^k$.

Demonstração. Dados $x,y,z \in G$ e $k \in \mathbb{Z}$ temos

(i)

$$\begin{aligned}[x,yz] &= x^{-1}(yz)^{-1}x(yz) = x^{-1}z^{-1}y^{-1}xyz \\ &= x^{-1}z^{-1}(xzz^{-1}x^{-1})y^{-1}xyz \\ &= (x^{-1}z^{-1}xz)z^{-1}(x^{-1}y^{-1}xy)z = [x,z]z^{-1}[x,y]z.\end{aligned}$$

(ii)

$$\begin{aligned}[xy,z] &= (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz \\ &= y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz \\ &= y^{-1}(x^{-1}z^{-1}xz)y(y^{-1}z^{-1}yz) = y^{-1}[x,z]y[y,z].\end{aligned}$$

(iii) Por indução sobre k, quando $k \geq 0$. Para $k=0$, temos que

$$[x^0,y]=[1,y]=1^{-1}y^{-1}1y=1=[x,y]^0$$

Para $k=1$, segue que

$$[x^1,y]=[x,y]=[x,y]^1$$

Suponhamos que o resultado é válido para todo $i \leq j$ onde $j \in \mathbb{N}$. Primeiramente, repare que se x comuta com $[x,y]$ temos

$$x[x,y]=[x,y]x \Rightarrow x^{-1}x[x,y]x^{-1}=x^{-1}[x,y]xx^{-1} \Rightarrow [x,y]x^{-1}=x^{-1}[x,y]$$

ou seja, x^{-1} comuta com $[x,y]$ também. Com isso, segue que

$$\begin{aligned}
[x,y]^{k+1} &= [x,y]^k[x,y] \\
&= x^{-1}[x,y]^k y^{-1}xy \\
&= x^{-1}[x^k,y]y^{-1}xy \\
&= x^{-1}x^{-k}y^{-1}x^k yy^{-1}xy \\
&= x^{-(k+1)}y^{-1}x^{k+1}y \\
&= [x^{k+1},y].
\end{aligned}$$

Com isso, $[x,y]^k = [x^k,y]$ para todo $k \geq 0$. Agora, para $k \leq 0$, repare que por hipótese temos que $x[x,y] = [x,y]x$. Assim temos que $[y,x^{-1}] = [x,y]$ e $[x,y]^{-1} = [x^{-1},y]$. Além disso, com x^{-1} também comuta com $[x^{-1},y]$ temos que

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

Logo $[x,y]^k = [x^k,y]$ para todo $k \in \mathbb{Z}$.

(iv) Com a utilização do item anterior, segue que

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

logo $[x,y]^k = [x,y^k]$ para todo $k \in \mathbb{Z}$.

□

Definição 1.1.4. *Seja G um grupo. Definimos como subgrupo derivado G' o subgrupo gerado pelo conjunto de comutadores, ou seja*

$$G' = \langle \Gamma(G) \rangle$$

Nesse contexto é interessante incluir o conceito de largura de um grupo (não necessariamente finito) G.

Definição 1.1.5. *Chamamos de largura do grupo G, e denotamos por $\lambda(G)$, o menor inteiro n, caso exista, tal que todos os elementos de G' podem ser escritos como produto de n comutadores, ou seja,*

$$\lambda(G) = min\{n \in \mathbb{N} \mid \forall \alpha \in G' : \alpha = \prod_{i=1}^{m}[g_i,h_i],\ g_i,h_i \in G,\ m \leq n\}.$$

Denotaremos como $\lambda(G) = \infty$ quando para todo $n \in \mathbb{Z}$, existe um elemento $g \in G'$ tal que g não pode ser descrito como produto de n elementos.

Definição 1.1.6. *Seja G um grupo. Dizemos que $x \in G$ é um elemento não comutador se $x \in G' \setminus \Gamma(G)$.*

Proposição 1.1.7. *Seja G um grupo. O grupo G é abeliano se, e somente se, $\Gamma(G) = \{1\}$.*

Demonstração. De fato, se $\Gamma(G) = 1$, então $x^{-1}y^{-1}xy = 1$, assim $xy = yx$ para todo $x, y \in G$. Por outro lado, se G é abeliano temos para todo $x, y \in G$ que

$$x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = 1.$$

Logo, $\Gamma(G) = 1$. □

O resultado a seguir nos dá um critério bem conhecido para grupos com $\lambda(G) = 1$.

Proposição 1.1.8. *Seja G um grupo. Se $|G'| = p$, onde p é primo, então $\lambda(G) = 1$.*

Demonstração. De fato, para $|G'| = 2$, temos que existem $a, b \in G$ tais que $[a, b] \neq 1$. Logo, $G' = \{1, [a, b]\} = \Gamma(G)$, ou seja, $\lambda(G) = 1$. Para $|G'| = 3$, temos novamente que existem $a, b \in G$ tais que $[a, b] \neq 1$. Porém, $|\langle [a, b] \rangle| = 3$, logo $[b, a] = [a, b]^{-1} \neq [a, b]$ e assim $G' = \{1, [a, b], [b, a]\} = \Gamma(G)$, ou seja, $\lambda(G) = 1$. Agora para $p \geq 5$, suponhamos que $G' \not\subseteq Z(G)$, assim consideremos $1 \neq a \in G'$ e $b \in G$ de forma que $ab \neq ba$. Com isso, segue que existe $1 \leq n \leq p-2$ de modo que $[a, b] = a^n$, ja que $a^{-1}b^{-1}ab = [a, b] \neq a^{p-1}$ e $ab \neq ba$. Logo, $b^{-1}ab = a^{n+1}$. Tendo isso, tomemos $i, j \in |\{1, \ldots, |\langle a \rangle| - 1|$ com $i \leq j$ de forma que $[a^j, b] = [a^i, b]$. Assim,

$$\begin{aligned} [a^j, b] = [a^i, b] &\Rightarrow a^{-j}b^{-1}a^j b = a^{-i}b^{-1}a^i b \Rightarrow (b^{-1}ab)^j = a^{j-i}(b^{-1}ab)^i \\ &\Rightarrow a^{(n+1)j} = a^{j-i}a^{(n+1)i} \Rightarrow a^{n(j-i)} = 1. \end{aligned}$$

Assim, temos que $|\langle a \rangle| = p$, portanto $p \mid n$ ou $p \mid j - i$. Mas como $1 \leq n \leq p-2$, segue que $p \nmid n$, ou seja, $p \mid j - i$ e já que $0 \leq j - i \leq p - 1$, obtemos $i = j$, logo $\{[a^j, b] \mid 1 \leq j \leq o\} = |G'| = p$, isso implica que $\Gamma(G) = G'$, ou seja, $\lambda(G) = 1$. Agora, suponhamos o caso em $G' \subseteq Z(G)$. Temos que existem $a, b \in G$ tais que $[a, b] \neq 1$, caso contrário $G' = 1$. Com isso, como $|G'| = p$, temos que $G' = \langle [a, b] \rangle \subset Z(G)$ e a comuta com $[a, b]$. Dessa forma, $[a^j, b] = [a, b]^j$. Assim, $G' = \{[a, b]^j = [a^j, b] \mid 1 \leq j \leq p\} = \Gamma(G)$, ou seja, $\lambda(G) = 1$. □

Uma situação particularmente interessante ocorre no contexto de Grupos Metabelinos

Definição 1.1.9. *Dizemos que um grupo G é metabeliano se $G'' = 1$.*

Definição 1.1.10. *Sejam G um grupo e h um elemento do grupo de automorfismos de G. Dizemos que h age livre de ponto fixo em G se*

$$x^h = x \Longrightarrow x = 1.$$

Proposição 1.1.11. *Seja $G = K \rtimes H$ finito, onde K e H são abelianos. Suponha que $h \in H \backslash \{1\}$ age livre de ponto fixo em K, então $G' = K = \{[x,h] \mid x \in K\}$.*

Demonstração. De fato, $G' \leq K$, pois $G/K \cong H$ é abeliano. Mais ainda, tomemos

$$\begin{aligned} \Omega_h \colon K &\to K \\ x &\mapsto [x,h]. \end{aligned}$$

Temos que Ω_h é injetivo. Com efeito, dados $x, y \in K$ segue que

$$\begin{aligned} \Omega_h(x) = \Omega_h(y) &\Rightarrow x^{-1}x^h = y^{-1}y^h \\ &\Rightarrow yx^{-1}x^h = y^h \\ &\Rightarrow yx^{-1} = y^h x^{-h} = (yx^{-1})^h \\ &\Leftrightarrow yx^{-1} = 1 \Leftrightarrow y = x. \end{aligned}$$

Com isso, como Ω_h é injetivo e finito, então Ω_h é bijetivo. Portanto, $G' = K = \{[x,h] \mid x \in K\}$. $\square$

No próximo capítulo investigaremos uma situação análoga, sem levar em conta os elementos livres de pontos fixos, mas exigiremos que o grupo G possua um subgrupo normal e abeliano A tal que G/A é cíclico.

1.2 Grupos e Subgrupos

Para estes primeiros resultados apresentados iremos somente enuncia-los, porém, por questão de completude, segue a referência [8] para maiores detalhes.

Lema 1.2.1. *Seja p um primo. Se G é um grupo de ordem p ou p^2, então G é abeliano.*

Lema 1.2.2 (Teorema de Cauchy)**.** *Se G é um grupo finito cuja ordem é divisível por um primo p, então existe um $g \in G$ tal que $|\langle g \rangle| = p$.*

Definição 1.2.3. *Sejam G um grupo e $x \in G$. Definimos o centralizador de x em G como sendo*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Para um conjunto $X \subset G$ definimos

$$C_G(X) = \{g \in G \mid gx = xg, \ \forall\, x \in X\}.$$

Quando $X = G$, temos que o $C_G(G) = Z(G)$ denomidado centro de G.

Definição 1.2.4. *Sejam G um grupo e $X \subseteq G$. Definimos o normalizador do conjunto X em G da forma*

$$N_G(X) = \{g \in G \mid g^{-1}Xg = X\}.$$

Proposição 1.2.5. *Seja H um subgrupo de G. Então,*

(i) $C_G(H) \trianglelefteq N_G(H)$

(ii) $N_G(H)/C_G(H)$ *é isoformo a um subgrupo de* $Aut(H)$

Demonstração. De fato, mostraremos primeiramente que $C_G(H) \subset N_G(H)$. Ora, dado $g \in C_G(H)$ temos que

$$Hg = gH \Rightarrow g^{-1}Hg = H$$

ou seja, $g \in N_G(H)$. Agora, tome $g \in N_G(H)$, temos que a aplicação

$$\begin{aligned} \omega_g \colon H &\to H \\ h &\mapsto g^{-1}hg. \end{aligned}$$

é um automorfismo de H em H (chamado automorfismo interno). Assim, tomemos $Aut(H) = \{\omega_g \colon H \to H \mid \forall g \in N_G(H)\}$. E com isso, consideremos o homormorfismo

$$\begin{aligned} \theta \colon N_G(H) &\to Aut(H) \\ g &\mapsto \omega_g. \end{aligned}$$

temos que

$$\begin{aligned} Ker(\theta) = \{g \in N_G(H) \mid \theta(g) = Id\} &= \{g \in N_G(H) \mid g^{-1}hg = h, \ \forall h \in H\} \\ &= \{g \in N_G(H) \mid hg = gh, \ \forall h \in H\} \\ &= C_G(H) \end{aligned}$$

E pelo fato de $Ker(\theta) \trianglelefteq N_G(H)$, segue que $C_G(H) \trianglelefteq N_G(H)$ como queríamos demonstrar no item (i). E, pelo primeiro Teorema do Isomorfimo temos que

$$Aut(H) \supseteq Im(\theta) \cong \frac{N_G(H)}{Ker(\theta)} = \frac{N_G(H)}{C_G(H)}$$

como queríamos demonstrar no item (ii). □

Definição 1.2.6. *Seja G um grupo finito. Dizemos que um subgrupo H é um p-subgrupo de Sylow de G, quando a ordem de* $|H| = p^m$*, onde* p^m *é a maior potência de p que divide a ordem de G.*

Para o resultado a seguir faremos o enunciado sem a demonstração. Porém para critério de completude segue a referência [8] para maiores detalhes.

Proposição 1.2.7. *Sejam G um grupo finito e p o menor primo que divide a ordem de G. Se um subgrupo H tem índice p, então* $H \trianglelefteq G$

O resultado a seguir é o famoso Teorema de Sylow. É um resultado que aparece em qualquer curso de Intrrodução a Álgebra e sua prova será omitida. Por uma questão de completude deixamos a referência [8].

Teorema 1.2.8. *(Teorema de Sylow) Sejam G um grupo finito e p um primo. Suponhamos que* $|G| = p^m q$*, com* $m \geq 1$ *e* $mdc(p,q) = 1$*. Então:*

(a) Para cada inteiro positivo $n \leq m$*, existe um subgrupo H de ordem* p^n*. Além disso, se K é um p-subgrupo de Sylow de G, então existe um p-subgrupo P de G com ordem* p^m *tal que K é subgrupo de P.*

(b) Sejam P,Q p-subgrupos de Sylow, então existe um elemento $g \in G$ *tal que* $Q = g^{-1}Pg$*.*

(c) Seja n_p *o número de p-subgrupos de Sylow de G. Então*

$$\begin{cases} n_p \mid q \\ n_p \equiv 1 (mod p) \end{cases}$$

Proposição 1.2.9. *Sejam p e q primos distintos e G um grupo de ordem* $|G| = p^2 q$*. Então G contém um p-subgrupo de Sylow normal ou um q-subgrupo de Sylow normal.*

Demonstração. Consideremos primeiramente o caso em que $p > q$. Pelo Teorema de Sylow temos que

$$\begin{cases} n_p \mid q \\ n_p \equiv 1 (mod p) \end{cases} \Rightarrow n_p = 1 \text{ ou } n_p = q$$

mas como temos que $p > q$, segue que $n_p = q$ não pode acontecer, portanto $n_p = 1$ e com isso garantimos que neste caso existe um p-subgrupo de Sylow normal. Agora, suponhamos que $p < q$. Pelo Teorema de Sylow, temos que

$$\begin{cases} n_q \mid p^2 \\ n_q \equiv 1(modq) \end{cases} \Rightarrow n_q = 1 \; ou \; n_q = p \; ou \; n_q = p^2$$

se $n_q = p$, então $q \mid p-1$, absurdo, pois $q > p$. Agora, se $n_q = p^2$ temos que

$$\begin{aligned} q \mid p^2 - 1 &\Rightarrow q \mid (p-1)(p+1) \\ &\Rightarrow q \mid (p+1) \\ &\Rightarrow p < q \leq p+1 \end{aligned}$$

ou seja, p e q são primos consecutivos, e isso só acontece quando $p = 2$ e $q = 3$. Com isso, basta provarmos que G de ordem $|G| = 2^2.3 = 12$ possui um 2-subgrupo de Sylow ou 3-subgrupo de Sylow. De fato, observe que pelo Teorema de Sylow temos que

$$\begin{cases} n_3 \mid 4 \\ n_3 \equiv 1(mod3) \end{cases} \Rightarrow n_3 = 1 \; ou \; n_3 = 4 \qquad \begin{cases} n_2 \mid 3 \\ n_2 \equiv 1(mod2) \end{cases} \Rightarrow n_3 = 1 \; ou \; n_3 = 3$$

se $n_3 = 4$ e $n_2 = 3$ teriamos que existem $4.(3-1) = 8$ elementos de ordem 3 e $3.(4-1) = 9$ elementos de ordem 4, ou seja, teriamos 17 elementos distintos em um grupo de ordem 12, absurdo. Portanto, $n_2 = 1$ ou $n_3 = 1$, ou seja, existe um 2-subgrupo de Sylow normal ou um 3-subgrupo de Sylow normal. □

Definição 1.2.10. *(Produto Direto) Sejam $G_1, G_2, \ldots, G_n$ grupos. Definimos o produto direto de $G_1, G_2, \ldots, G_n$ como sendo o produto cartesinano $G_1 \times G_2 \times \ldots \times G_n$ com a operação coordenada a coordenada.*

O próximo resultado iremos ocultar sua demonstração, mas para maiores detalhes, segue a referência [3].

Proposição 1.2.11. *Dado um grupo G, dizemos que $G \simeq G_1 \times G_2 \times \ldots \times G_n$ se, e somente se, G possui subgrupos $H_1 \simeq G_1, \ldots, H_n \simeq G_n$ tais que*

(a) $G = H_1 H_2 \ldots H_n$

(b) $H_i \trianglelefteq G$, $\forall i = 1, \ldots, n$

(c) $H_i \cap \{H_1 \ldots H_{i-1} H_{i+1} \ldots H_n\} = \{e\}, \forall i = 1, \ldots, n$

Definição 1.2.12. *Seja $(G_i)_{i\in I}$ uma família de grupos. Definimos o produto direto dos grupos G_i com $i \in I$ da forma*

$$G = \bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} \mid g_i \in G_i \text{ e } g_i \neq 1_{G_i} \text{ para um número finito de índices}\}$$

cuja a operação é dada coordenada a coordenada.

1.3 Produtos Semidireto e Entrelaçado

1.3.1 Produto Semidireto

Definição 1.3.1. *Sejam N e H subgrupos de um grupo G. Chamamos de produto semidireto interno de N por H o grupo G se*

(a) $N \trianglelefteq G$ *e* $H \leq G$

(b) $G = NH$

(c) $N \cap H = 1$

Denominamos $G = N \rtimes H$ como notação para o produto semidireto.

Exemplo 1.3.2. *Consideremos $D_n = \langle a, b \mid a^n = 1\ ,\ b^2 = 1 \text{ e } b^{-1}ab = a^{-1}\rangle$ o grupo diedral de ordem $2n$. Tome $N = \langle a\rangle$ e $H = \langle b\rangle$, temos que $N \trianglelefteq D_n$ pois $|G : N| = 2$, além disso $H \leq G$. Pela definição do grupo diedral podemos reparar que $G = NH$ e como $N \cap H = 1$, segue que $G = N \rtimes H = \langle a\rangle \rtimes \langle b\rangle$.*

Lema 1.3.3. *Sejam N e H grupos. Então a aplicação*

$$\begin{array}{rccccccc} \phi & : & H & \longrightarrow & Aut(N) & & & \\ & & h & \longmapsto & \phi_h & : & N \longmapsto & N \\ & & & & & & n \longmapsto & h^{-1}nh \end{array}$$

é um homomorfismo.

Demonstração. Primeiro mostraremos que ϕ_h é um automorfismo de N. De fato, ϕ_h é a restrição de um automorfismo interno ao subgrupo normal N. Assim, concluímos que ϕ_h é um monorfismo. Agora é suficiente mostrar que ϕ_h é sobrejetivo. Com efeito, dado $n \in N$, $\phi_h(hnh^{-1}) = n$. Agora, provaremos que ϕ é um homomorfismo. De fato, dados $h_1, h_2 \in H$

temos que

$$\begin{aligned}\phi(h_1h_2) &= \phi_{h_1h_2}(n) = (h_1h_2)^{-1}n(h_1h_2)\\ &= h_2^{-1}h_1^{-1}nh_1h_2 = h_2^{-1}\phi_{h_1}(n)h_2\\ &= \phi_{h_2}(\phi_{h_1}(n)) = \phi(h_1)\phi(h_2)\end{aligned}$$

como $n \in N$ foi pego de forma arbitraria, segue que ϕ é um homomorfismo. $\square$

Teorema 1.3.4. *Sejam N e H grupos e $\phi : H \to Aut(N)$ um homomorfismo. Então o conjunto $G = \{(h,n) | h \in H$ e $n \in N\}$ munido da operação*

$$*_\phi : G \times G \to G$$

$$(h_1,n_1) *_\phi (h_2,n_2) \mapsto (h_1h_2, \phi_{h_2^{-1}}(n_1)n_2)$$

é um grupo. Mais ainda, temos as seguintes propriedades

(a) $N^* = \{(1,n) \mid n \in N\} \trianglelefteq G$.

(b) $H^* = \{(h,1) \mid h \in H\} \leq G$.

(c) $N^*H^* = G$ *e* $N^* \cap H^* = 1$.

(d) $N \cong N^*$ *e* $H \cong H^*$.

Definimos este grupo G como Produto Semidireto Externo, e denominamos $G = N \rtimes_\phi H$. Além disso,

Demonstração. De fato, dados (h_1,n_1), (h_2,n_2), $(h_3,n_3) \in G$, temos que

$$\begin{aligned}((h_1,n_1) *_\phi (h_2,n_2)) *_\phi (h_3,n_3) &= (h_1h_2, \phi_{h_2^{-1}}(n_1)n_2) *_\phi (h_3,n_3)\\ &= ((h_1h_2)h_3, \phi_{h_3^{-1}}(\phi_{h_2^{-1}}(n_1)n_2))n_3)\\ &= (h_1(h_2h_3), \phi_{h_3^{-1}h_2^{-1}}(n_1)\phi_{h_3^{-1}}(n_2)n_3)\\ &= (h_1,n_1) *_\phi (h_2h_3, \phi_{h_3^{-1}}(n_2)n_3)\\ &= (h_1,n_1) *_\phi ((h_2,n_2) *_\phi (h_3,n_3))\end{aligned}$$

ou seja, G munido pela operação $*_\phi$ é associativo. Além disso, temos $(1,1) \in G$ como elemento neutro, pois dado $(h,n) \in G$ temos que

$$(1,1) *_\phi (h,n) = (1h, \phi_{h^{-1}}(1)n) = (h,n)$$

e

$$(h,n)*_\phi(1,1) = (h1, \phi_{1^{-1}}(n)1) = (h,n)$$

E por fim , dado $(h,n) \in G$ considerando $(h^{-1}, \phi_h(n^{-1})) \in G$ obtemos que

$$(h,n)*_\phi(h^{-1}, \phi_h(n^{-1})) = (hh^{-1}, \phi_h(n)\phi_h(n^{-1}) = (hh^{-1}, \phi_h(nn^{-1})) = (1,1)$$

e

$$(h^{-1}, \phi_h(n^{-1}))*_\phi(h,n) = (h^{-1}h, \phi_{h^{-1}}(\phi_h(n^{-1}))n) = (h^{-1}h, \phi_{h^{-1}h}(n^{-1}))n) = (h^{-1}h, n^{-1}n) = (1,1);$$

ou seja, $(h,n)^{-1} = (h^{-1}, \phi_h(n^{-1}))$ é o elemento inverso de (h,n). Com isso, concluímos que G munido da operação $*_\phi$ é um grupo.
Agora mostraremos as propriedades consequentes deste grupo

(a) De fato, dados $(1,n) \in N^*$ e $(h_1,n_1) \in G$ temos que

$$\begin{aligned}
(h_1,n_1)^{-1}*_\phi(1,n)*_\phi(h_1,n_1) &= (h_1^{-1}, \phi_{h_1}(n_1^{-1}))*_\phi(1,n)*_\phi(h_1,n_1)\\
&= (h_1^{-1}, \phi_{h_1}(n_1^{-1}))*_\phi(h_1, \phi_{h_1^{-1}}(n)n_1)\\
&= (h_1^{-1}h_1, \phi_{h_1^{-1}}(\phi_{h_1}(n_1^{-1}))\phi_{h_1^{-1}}(n)n_1)\\
&= (1, n_1^{-1}\phi_{h_1^{-1}}(n)n_1) \in N^*.
\end{aligned}$$

(b) Dados $(h_1,1),(h_2,1) \in H^*$ temos que

$$\begin{aligned}
(h_1,1)*_\phi(h_2,1)^{-1} &= (h_1,1)*_\phi(h_2^{-1}, \phi_h(1))\\
&= (h_1,1)*_\phi(h_2^{-1},1) = (h_1h_2^{-1},1) \in H^*.
\end{aligned}$$

(c) Por definição segue diretamente que $N^* \cap H^* = (1,1)$. Agora, notemos que para cada $h \in H$ e $n \in N$, temos

$$(h,1)*_\phi(1,n) = (h, \phi_1(1)n) = (h,n).$$

Logo, $G = H^*N^*$.

(d) Para mostrarmos que $N \cong N^*$ e $H \cong H^*$ basta considerarmos os seguintes isomorfismos:

$$\begin{aligned}
f_1 : H &\to H^*\\
h &\mapsto (h,1)
\end{aligned}$$

e

$$\begin{aligned} f_2 \colon K &\to K^* \\ k &\mapsto (1,k). \end{aligned}$$

□

Exemplo 1.3.5. *Sejam $C_2 = \langle a \rangle$ e $C_3 = \langle b \rangle$ grupos cíclicos de ordem 2 e 3 respectivamente. Repare que $Aut(C_3) = \{Id, \sigma\}$ onde*

$$\begin{aligned} \sigma : C_3 &\to C_3 \\ b^i &\mapsto b^{2i} \end{aligned}$$

para $i = 0, 1, 2$. Veja que para todo $b^i \in C_3$ temos que

$$\sigma^2(b^i) = \sigma(\sigma(b^i)) = \sigma(b^{2i}) = b^{4i} = b^i$$

ou seja, σ tem ordem 2, portanto existe um homomorfismo

$$\begin{aligned} \phi : C_2 &\to Aut(C_3) \\ a^i &\mapsto \sigma^i \end{aligned}$$

para $i = 0, 1$. Assim, definimos o grupo $G = C_2 \rtimes_\phi C_3 = \{(1,1), (1,b), (1,b^2), (a,1), (a,b), (a,b^2)\}$ como o produto semidireto de C_3 por C_2. Agora, repare que $|G| = 6$, além disso temos

$$\begin{aligned} (1,b)^3 &= (1,b) *_\phi (1,b) *_\phi (1,b) = (1, \phi_1(b)b) *_\phi (1,b) = (1,b^2) *_\phi (1,b) \\ &= (1, \phi_1(b)b^2) = (1,b^3) = (1,1) \end{aligned}$$

$$(a,1)^2 = (a,1) *_\phi (a,1) = (a^2, \phi_a(1)1) = (1,1)$$

$$\begin{aligned} (a,1) *_\phi (1,b) &= (a, \phi_1(1)b) = (a,b) = (a, \sigma(b^2)1) \\ &= (a, \phi_{a^{-1}}(b^2)1) = (1,b^2) *_\phi (a,1) = (1,b)^2 *_\phi (a,1) \end{aligned}$$

Com isso, a aplicação

$$\begin{aligned} f: \ G &\to S_3 \\ (a,1) &\mapsto (12) \\ (1,b) &\mapsto (123) \end{aligned}$$

é um isomorfismo, ou seja, $S_3 \cong C_2 \rtimes_\phi C_3$.

Exemplo 1.3.6. *Sejam* $N = C_3$ *e* $H = C_2 \times C_2$. *Temos que* $Aut(C_3) = \{Id, \sigma\}$, *onde*

$$\begin{aligned} \sigma : C_3 &\to C_3 \\ a^i &\mapsto a^{2i} \end{aligned}$$

para $i = 0,1,2$. *Veja que, como no exemplo acima, para todo* $b^i \in C_3$ *temos que*

$$\sigma^2(a^i) = \sigma(\sigma(a^i)) = \sigma(a^{2i}) = a^{4i} = a^i$$

ou seja, σ *tem ordem 2, portanto os homomorfismo de* $C_2 \times C_2$ *em* $Aut(C_3)$ *são*

$$\begin{array}{rcccc} \theta_{(1,1)} & : & C_2 \times C_2 & \longrightarrow & Aut(C_3) \\ & & (1,1) & \longmapsto & Id \\ & & (1,b) & \longmapsto & Id \\ & & (b,1) & \longmapsto & Id \\ & & (b,b) & \longmapsto & Id \end{array} \qquad \begin{array}{rcccc} \theta_{(1,b)} & : & C_2 \times C_2 & \longrightarrow & Aut(C_3) \\ & & (1,1) & \longmapsto & Id \\ & & (1,b) & \longmapsto & Id \\ & & (b,1) & \longmapsto & \sigma \\ & & (b,b) & \longmapsto & \sigma \end{array}$$

$$\begin{array}{rcccc} \theta_{(b,1)} & : & C_2 \times C_2 & \longrightarrow & Aut(C_3) \\ & & (1,1) & \longmapsto & Id \\ & & (1,b) & \longmapsto & \sigma \\ & & (b,1) & \longmapsto & Id \\ & & (b,b) & \longmapsto & \sigma \end{array} \qquad \begin{array}{rcccc} \theta_{(b,b)} & : & C_2 \times C_2 & \longrightarrow & Aut(C_3) \\ & & (1,1) & \longmapsto & Id \\ & & (1,b) & \longmapsto & \sigma \\ & & (b,1) & \longmapsto & \sigma \\ & & (b,b) & \longmapsto & Id \end{array}$$

com isso, definimos os grupos $G_i = (C_2 \times C_2) \rtimes_{\theta_i} C_3$, *onde* $i \in C_2 \times C_2$. *Para* $i = (1,1)$ *temos que* $G = (C_2 \times C_2) \times C_3$. *Agora, para* $i \neq (1,1)$, *mostraremos que* $(C_2 \times C_2) \rtimes_{\theta_i} C_3 \cong D_6$ *o grupo diedral de ordem* 12. *De fato, sem perda de generalidade, tomemos o homomorfismo* $\theta_{(b,b)}$ *(o resultado seguirá de forma análoga para os casos* $\theta_{(1,b)}$ *e* $\theta_{(b,1)}$*). Assim, definimos* $\alpha := ((b,b),a)$ *e* $\beta := ((1,b),a)$, *logo temos que*

$$
\begin{aligned}
\alpha^2 &= ((b,b),a) *_{\theta\ (b,b)} ((b,b),a)\\
&= ((b,b)(b,b), \theta_{(b,b)}((b,b))(a)a)\\
&= ((1,1), Id(a)a) = ((1,1),a^2)
\end{aligned}
$$

logo,

$$
\begin{aligned}
\alpha^6 &= ((1,1),a^2)^3\\
&= ((1,1),a^2) *_{\theta\ (b,b)} ((1,1),a^2) *_{\theta\ (b,b)} ((1,1),a^2)\\
&= ((1,1),a) *_{\theta\ (b,b)} ((1,1),a^2)\\
&= ((1,1),1)
\end{aligned}
$$

$$
\begin{aligned}
\beta^2 &= ((b,1),a) *_{\theta\ (b,b)} ((b,1),a)\\
&= ((b,1)(b,1), \theta_{(b,b)}((b,1))(a)a)\\
&= ((1,1), \sigma(a)a) = ((1,1),a^3) = ((1,1),1)
\end{aligned}
$$

$$
\begin{aligned}
\alpha\beta &= ((b,b),a) *_{\theta\ (b,b)} ((b,1),a)\\
&= ((b,b)(b,1), \theta_{(b,b)}((b,1))(a)a)\\
&= ((1,b), \sigma(a)a) = ((1,b),a^3) = ((1,b),1)
\end{aligned}
$$

$$
\begin{aligned}
\beta\alpha^5 &= \beta\alpha\alpha^2\alpha^2\\
&= ((b,1),a) *_{\theta\ (b,b)} ((b,b),a) *_{\theta\ (b,b)} ((1,1),a^2) *_{\theta\ (b,b)} ((1,1),a^2)\\
&= ((1,b),a^2) *_{\theta\ (b,b)} ((1,1),a^2) *_{\theta\ (b,b)} ((1,1),a^2)\\
&= ((1,b),a) *_{\theta\ (b,b)} ((1,1),a^2)\\
&= ((1,b),1).
\end{aligned}
$$

Assim, obtemos que $G_i = (C_2 \times C_2) \rtimes_{\theta_i} C_3 = \langle \alpha, \beta \rangle = D_6$ *para todo* $i \in C_2 \times C_2$ *tal que* $i \neq (1,1)$.

1.3.2 Produto entrelaçado

Sejam H e K grupos. Consideremos o seguinte conjunto associado

$$B = \{f\colon K \longrightarrow H; S_f < \infty\},$$

sendo que $S_f = \{x \in K \mid f(x) \neq 1\}$ é o suporte da função f. Definamos a seguinte operação em B: dados $f, g \in B$ e $x \in K$, definimos uma nova aplicação: fg dada por:

$$fg(x) = f(x)g(x).$$

Lema 1.3.7. *B é um grupo.*

Demonstração. 1. (Associatividade) Dados aplicações $f, g, h \in B$ e $x \in K$. Temos que

$$(fg)h(x) = fg(x)h(x) = f(x)g(x)h(x) = f(x)gh(x) = f(gh)(x)$$

2. (Elemento neutro) Consideremos $i\colon K \to H$ dada por $x \mapsto 1$ para todo $x \in K$. Se $f \in B$, então
$$fi(x) = f(x)i(x) = f(x) = i(x)f(x) = if(x).$$
Notação: Usaremos a notação 1 no lugar de i para denotar o elemento neutro do grupo B.

3. (Elemento inverso) Dado $f \in B$. Definamos $g \in B$ dado por $g(x) = (f(x))^{-1}$, para todo $x \in K$. Assim,
$$fg(x) = f(x)g(x) = f(x)(f(x))^{-1} = 1.$$

□

Dizemos que B é a base do conjunto de todas as aplicações $\{f\colon K \to H\}$.

Lema 1.3.8. *Sejam H e K grupos.*

1. *Se H é abeliano, então B é abeliano.*
2. *Se H é um p-grupo, então B é um p-grupo.*

Demonstração. 1. Dados $f, g \in B$ e $x \in K$. Temos:

$$fg(x) = f(x)g(x) = g(x)f(x) = gf(x).$$

2. Dado $f \in B$. Tomemos $S_f = \{x_1, \dots, x_l\}$ o suporte de f. Como H é um p-grupo, denotemos $m_i = |f(x_i)|$ e $m = m_1 \cdot \ldots \cdot m_l$. Assim, se $x \in K$, então

$$f^m(x) = \overbrace{f \dots f}^{m\ vezes}(x) = \underbrace{f(x) \dots f(x)}_{m\ vezes} = 1.$$

□

Definamos uma aplicação $\varphi \colon K \to Aut(B)$ dada por:

$$\begin{array}{rcccl} \varphi : & K & \longrightarrow & Aut(B) & \\ & k & \longmapsto & \varphi_k : & B \longmapsto B \\ & & & & f \longmapsto f_k \end{array}$$

sendo que $f_k(x) = f(xk)$.

Lema 1.3.9. *A aplicação φ como definida acima é um homomorfismo.*

Demonstração. Dado $k \in K$, mostraremos que $\varphi_k \in Aut(B)$.

1. (φ_k é um homomorfismo) Dados $f, g \in B$, por definição

$$\varphi_k(fg) = (fg)_k$$

ou seja, para cada $x \in K$ temos:

$$(fg)_k(x) = fg(xk) = f(xk)g(xk) = f_k(x)g_k(x) = f_k g_k(x).$$

Assim,

$$\varphi_k(fg) = \varphi_k(f)\varphi_k(g).$$

2. (φ_k é um monomorfismo) Se $f \in \ker(\varphi_k)$, então

$$1 = f_k(x) = f(xk),$$

para todo $x \in K$. Em particular,

$$1 = f(y),$$

para todo $y \in K$. Assim, $f = 1 \in B$.

3. (φ_k é um epimorfismo) Dado $f \in B$. Consideremos a aplicação $\tilde{f}\colon K \to H$ dada por $\tilde{f}(x) = f(xk^{-1})$. Temos que $\varphi_k(\tilde{f}) = \tilde{f}_k$ e

$$\tilde{f}_k(x) = \tilde{f}(xk) = f((xk)k^{-1}) = f(x).$$

Logo, φ_k é sobrejetivo e concluímos que $\varphi_k \in (B)$.

Dados $k, k_1 \in K$, mostraremos que φ é um homomorfismo. Ou seja, precisamos mostrar

$$\varphi_{kk_1} = \varphi_k \varphi_{k_1}.$$

Dado $f \in B$, temos que

$$\varphi_{kk_1}(f) = f_{kk_1}.$$

Daí,

$$f_{kk_1}(x) = f(xkk_1)$$

e

$$\varphi_k \varphi_{k_1}(f(x)) = f_{kk_1}(x) = f_{k_1}(xk) = f(xkk_1).$$

□

Agora estamos em condições de definir o produto entrelaçado.

Definição 1.3.10. *Sejam H, K grupos. Definimos o produto entrelaçado como sendo o produto semidireto de $B \rtimes_\varphi K$, sendo que $B = \{f\colon K \to H \mid (f) < \infty\}$ e $\varphi\colon K \to Aut(B)$ é o homomorfismo como definido acima. Notação: $H \wr K$.*

Exemplo 1.3.11. *Sejam $H = C_2 = \langle a \rangle$ e $K = C_2 = \langle b \rangle$. Construiremos a estrutura do grupo $G = H \wr K = C_2 \wr C_2$. Ora, definamos o grupo base na forma $B = \langle a \rangle \times \langle a \rangle = \{(1,\ 1), (1,\ a), (a,\ 1), (a,\ a)\}$. E com isso, temos a aplicação*

$$\begin{array}{ccccccc}
\varphi & : & C_2 & \longrightarrow & Aut(C_2 \times C_2) & & \\
 & & b & \longmapsto & \varphi_b : & C_2 \times C_2 \longmapsto & C_2 \times C_2 \\
 & & & & & (1,1) \longmapsto & (1,1) \\
 & & & & & (1,a) \longmapsto & (a,1) \\
 & & & & & (a,1) \longmapsto & (1,a) \\
 & & & & & (a,a) \longmapsto & (a,a)
\end{array}$$

com isso, definimos o grupo $G = C_2 \wr C_2 = \langle b \rangle \rtimes_\varphi B$ um grupo de ordem 8. Agora, mostraremos que $C_2 \wr C_2 \cong D_4$. De fato, definamos $r := (b, (a,1))$ e $s := (b, (1,1))$, então

$$\begin{aligned}
r^2 &= (b,(a,1)) *_\varphi (b,(a,1)) \\
&= (b^2, \varphi(b)((a,1))(a,1)) \\
&= (1, \varphi_b((a,1))(a,1)) = (1,(1,a)(a,1)) = (1,(a,a)).
\end{aligned}$$

Logo,

$$\begin{aligned}
r^4 &= (1,(a,a))^2 \\
&= (1,(a,a)) *_\varphi (1,(a,a)) \\
&= (1, \varphi(1)((a,a))(a,a)) \\
&= (1, Id((a,a))(a,a)) = (1,(1,1))
\end{aligned}$$

$$\begin{aligned}
s^2 &= (b,(1,1)) *_\varphi (b,(1,1)) \\
&= (b^2, \varphi(b)((1,1))(1,1)) \\
&= (1, \varphi_b((1,1))(1,1)) = (1,(1,1)(1,1)) = (1,(1,1))
\end{aligned}$$

$$\begin{aligned}
s^{-1}rs &= (b,(1,1))^{-1} *_\varphi (b,(a,1)) *_\varphi (b,(1,1)) \\
&= (b,(1,1)) *_\varphi (b,(a,1)) *_\varphi (b,(1,1)) \\
&= (b^2, \varphi(b)((1,1))(a,1)) *_\varphi (b,(1,1)) \\
&= (1,(a,1)) *_\varphi (b,(1,1)) \\
&= (b, \varphi(b)((a,1))(1,1)) = (b,(1,a)) = r^{-1}
\end{aligned}$$

Portanto, $C_2 \wr C_2 \cong \langle r,\ s | r^4 = s^2 = 1 \text{ e } s^{-1}rs = s^{-1}\rangle = D_4$*, como queríamos mostrar.*

Capítulo 2

Grupos com largura $\lambda(G) = 1$

Nesse capítulo estudaremos o artigo de E. Spiegel [11]. Nele desenvolveremos dois teoremas que nos dão critérios para garantir quando o conjunto de todos os comutadores de um grupo G coincida com seu subgrupo derivado G'. Adicionalemnte, apresentamos exemplos de grupos que satisfazem as hipóteses dos resultados em questão.

2.1 Critérios para $\Gamma(G) = G'$

A seguir definimos dois subconjuntos (relacionados a classes de conjugação) que são fundamentais no entendimento dos resultados e exemplos desse capítulo.

Definição 2.1.1. *Seja G um grupo. Para $x \in G$ definimos*

$$C_x = x^G = \{a^{-1}xa \mid a \in G\}$$

como o conjunto dos conjugados de x (em G).

Definição 2.1.2. *Definimos B_x como o produto dos conjuntos C_x e $C_{x^{-1}}$, ou seja,*

$$B_x = \{st \mid s \in C_{x^{-1}},\, t \in C_x\}$$

O lema a seguir é técnico e será usado fortemente na demonstração dos Teoremas 2.1.4 e 2.1.5 (correspondem aos Teoremas A e B da introdução, respectivamente).

Lema 2.1.3. *Seja x um elemento de um grupo G. Então*

(a) $\Gamma(G) = \bigcup_{x \in G} B_x$;

(b) Se $y \in B_x$, então $C_y \subseteq B_x$;

(c) Se $y \in B_x$, então $y^{-1} \in B_x$;

(d) Se $y = cx'$ com $c \in Z(G)$ e $x' \in C_x$, então $B_x = B_y$.

Demonstração. De fato,

(a) Dados $x, y \in G$. Como $x \in C_x$ e $y^{-1}x^{-1}y \in C_{x^{-1}}$, segue que $y^{-1}x^{-1}yx \in B_x$. Portanto, $\Gamma(G) \subseteq \bigcup_{x \in G} B_x$. Por outro lado, repare que dado $k \in \bigcup_{x \in G} B_x$ existem $y, z \in G$ tais que

$$\begin{aligned} k &= (y^{-1}x^{-1}y)(z^{-1}xz) \\ &= (y^{-1}x^{-1}y)z^{-1}(yy^{-1})x(yy^{-1})z \\ &= (y^{-1}x^{-1}y)(z^{-1}y)(y^{-1}xy)(y^{-1}z) \\ &= (y^{-1}xy)^{-1}(y^{-1}z)^{-1}(y^{-1}xy)(y^{-1}z) = [y^{-1}xy, y^{-1}z] \end{aligned}$$

ou seja, $\bigcup_{x \in G} B_x \subseteq \Gamma(G)$. Portanto, $\Gamma(G) = \bigcup_{x \in G} B_x$.

(b) Como $y \in B_x$, então $y = ab$ com $a = v^{-1}x^{-1}v \in C_{x^{-1}}$ e $b = u^{-1}xu \in C_x$. Com isso, seja $w \in G$, então

$$\begin{aligned} w^{-1}yw &= w^{-1}abw \\ &= w^{-1}a(ww^{-1})bw \\ &= (w^{-1}aw)(w^{-1}bw) \\ &= (w^{-1}(v^{-1}x^{-1}v)w)(w^{-1}(u^{-1}xu)w) \\ &= ((vw)^{-1}x^{-1}(vw))((uw)^{-1}x(uw)) \end{aligned}$$

ou seja, $C_y \subset B_x$.

(c) Dado $y \in B_x$. Temos $y = (u^{-1}x^{-1}u)(v^{-1}xv)$ para $u, v \in G$. Portanto,

$$\begin{aligned} y^{-1} &= ((u^{-1}x^{-1}u)(v^{-1}xv))^{-1} \\ &= (v^{-1}xv)^{-1}(u^{-1}x^{-1}u)^{-1} \\ &= (v^{-1}x^{-1}v)(u^{-1}xu) \end{aligned}$$

que pertence a B_x.

(d) Como $x' \in C_x$, segue que $x' = w^{-1}xw$ para algum $w \in G$. Com isso, seja $k \in B_x$, então

$$\begin{aligned}
k &= (u^{-1}x^{-1}u)(v^{-1}xv) \\
&= (u^{-1}(w(x')^{-1}w^{-1})u)(v^{-1}(wx'w^{-1})v) \\
&= (u^{-1}(w(c^{-1}y)^{-1}w^{-1})u)(v^{-1}(w(c^{-1}y)w^{-1})v) \\
&= (u^{-1}(wy^{-1}w^{-1})u)(v^{-1}(wyw^{-1})v) \\
&= ((w^{-1}u)^{-1}y^{-1}(w^{-1}u))((w^{-1}v)^{-1}y(w^{-1}v))
\end{aligned}$$

ou seja, $B_x \subseteq B_y$. Por outro lado, seja $h \in B_y$, então

$$\begin{aligned}
h &= (r^{-1}y^{-1}r)(s^{-1}ys) \\
&= (r^{-1}(cx')^{-1}r)(s^{-1}(cx')s) \\
&= (r^{-1}(c(w^{-1}xw))^{-1}r)(s^{-1}(c(w^{-1}xw))s) \\
&= (r^{-1}(w^{-1}x^{-1}w)r)(s^{-1}(w^{-1}xw)s) \\
&= ((wr)^{-1}x^{-1}(wr))((ws)^{-1}x(ws))
\end{aligned}$$

ou seja, $B_y \subseteq B_x$. Logo, $B_x = B_y$.

□

Os dois próximos Teoremas correspondem aos Teoremas A e B da Introdução, respectivamente. Por uma questão de completude e simplificar a leitura, incluímos ambos os enunciados correspondentes.

Teorema 2.1.4. *Seja x um elemento de um grupo G. Suponhamos que o subconjunto B_x é um subgrupo de G com $\Gamma(G) \subseteq B_x$. Então $\Gamma(G) = B_x = G'$.*

Demonstração. Pelo item (a) do Lema 2.1.3 observamos que $\Gamma(G) = \bigcup_{x\in G} B_x \supset B_x$. Por outro lado, como $\Gamma(G) \subset B_x \leq G$, temos que o subgrupo derivado G' está contido em B_x. Compilando as inclusões acima temos:

$$B_x \subset \bigcup_{x\in G} B_x = \Gamma(G) \subset G' \subset B_x.$$

Logo, $\Gamma(G) = B_x = G'$. □

Teorema 2.1.5. *Seja G um grupo. Se existe um subgrupo normal e abeliano N de G tal que G/N é um grupo cíclico gerado por xN, com $x \in G$, então $B_x = \Gamma(G) = G'$*

Demonstração. Como G/N é cíclico, qualquer elemento $h \in G$ pode ser escrito da forma $h = ax^i$ para algum $a \in N$ e $i \in \mathbb{Z}$. Com isso, dado um $i \in \mathbb{Z}$, seja $u \in B_{x^i}$, ou seja,

$$u = r^{-1}x^{-i}rs^{-1}x^is \text{ , } \textit{para } r = x^ja \textit{ e } s = x^kb \textit{ com } a,b \in N \textit{ e } j,k \in \mathbb{Z}.$$

Pelo fato de N ser abeliano e normal em G, temos que

$$\begin{aligned}
u &= r^{-1}x^{-i}rs^{-1}x^is \\
&= (ax^j)^{-1}x^{-i}(ax^j)(bx^k)^{-1}x^i(bx^k) \\
&= (a^{-1}x^{-j})x^{-i}(ax^j)(b^{-1}x^{-k})x^i(bx^k) \\
&= a^{-1}x^{-j}x^{-i}(x^ja)b^{-1}x^{-k}x^i(x^kb) \\
&= a^{-1}(x^{-j}x^{-i}x^jab^{-1}x^{-k}x^ix^k)b \\
&= a^{-1}(x^{-i}ab^{-1}x^i)b \\
&= a^{-1}b(x^{-i}ab^{-1}x^i) \\
&= (ab^{-1})^{-1}x^{-i}(ab^{-1})x^i
\end{aligned}$$

Portanto, $B_{x^i} = \{c^{-1}x^{-i}cx^i | c \in N\}$. Com isso, seja $a^{-1}x^{-i}ax^i, b^{-1}x^{-i}bx^i \in B_{x^i}$ *com* $a,b \in N$, utilizando novamente o fato de que N é abeliano e normal em G, temos que

$$\begin{aligned}
a^{-1}x^{-i}ax^ib^{-1}x^{-i}bx^i &= a^{-1}(x^{-i}ax^i)b^{-1}(x^{-i}bx^i) \\
&= a^{-1}b^{-1}(x^{-i}ax^i)(x^{-i}bx^i) \\
&= (ab)^{-1}x^{-i}(ab)x^i,
\end{aligned}$$

ou seja, B_{x^i} é fechado para a operação de G, com isso, pelo item (c) do Lema 2.1.3 temos que B_{x^i} é um subgrupo de G e pelo item (b) do Lema 2.1.3 concluímos que B_{x^i} é um subgrupo normal de G. Assim, dado $a^{-1}x^{-i}ax^i \in B_{x^i}$ com $a \in N$, seja $a^{-1}x^{-1}ax \in B_x$, então

$$B_x\, a^{-1}x^{-1}ax = B_x \Rightarrow B_x\, a^{-1}x^{-1}a = B_x\, x^{-1}$$

como B_{x^i} é normal segue que

$$B_x\, a^{-1}x^{-i}a = B_x\, x^{-i} \Rightarrow B_x\, a^{-1}x^{-i}ax^i = B_x$$

ou seja, $B_{x^i} \subset B_x$. Agora com a utilização dos elementos demonstrados acima mostraremos que $\Gamma(G) \subset B_x$, pois com este resultado estaremos com as hipóteses do Teorema 2.1.4, e com isso concluiremos que $B_x = \Gamma(G) = G'$. De fato, dado $u, v \in G$, onde $u = ax^i$ e $v = bx^j$ com $a, b \in N$, $i, j \in \mathbb{Z}$, então

$$\begin{aligned}
u^{-1}v^{-1}uv &= (x^{-i}a^{-1})(x^{-j}b^{-1})(ax^i)(bx^j) \\
&= (x^{-i}a^{-1}x^{-j})b^{-1}a(x^ibx^j) \\
&= b^{-1}(x^{-i}a^{-1}x^{-j})(x^ibx^j)a \\
&= b^{-1}(x^{-i}a^{-1}x^{i})(x^{-j}bx^j)a \\
&= (b^{-1}x^{-j}bx^j)(ax^{-i}a^{-1}x^i)
\end{aligned}$$

que pertence a B_x pois é um subgrupo de G que contém B_{x^i} , B_{x^j} com vimos acima. Portanto, $\Gamma(G) \subset B_x$. □

2.2 Exemplos: Grupos de Spiegel

Em homenagem ao autor do artigo que estudamos para fazer esse capítulo incluímos o seu nome junto com os exemplos de grupos de largura 1 que satisfazem as hipóteses dos Teoremas 2.1.4 e 2.1.5.

Definição 2.2.1. *Dizemos que um grupo G é metacíclico se existe um subgrupo normal cíclico N para o qual G/N também é cíclico.*

Um corolário imediato do Teorema 2.1.5 nos garante que grupos metacíclicos tem $\lambda(G) = 1$.

Corolário 2.2.2. *Seja G um grupo metacíclico. Então $\lambda(G) = 1$.*

Demonstração. Chamemos N um subgrupo normal cíclico no qual G/N é cíclico. Temos que N é normal abeliano e $G/N = \langle xN \rangle$, para algum $x \in G \setminus N$. E, pelo Teorema 2.1.5, $G' = \Gamma(G)$. □

Por uma questão de completude, cabe destacar alguns grupos (algumas famílias) metacíclicos.

Exemplo 2.2.3. *Seja $D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ o grupo diedral de ordem $2n$. Mostraremos que $B_b = D_n'$. De fato, tome $N = \langle a \rangle$ é um subgrupo cíclico normal de D_n (em particular, N é abeliano). Com isso, temos que $D_n/N = \langle bN \rangle$. Logo, pelo Teorema 2.1.4 podemos concluir que $B_b = D_n'$ e, consequentemente, $\lambda(D_n) = 1$.*

Existe uma caracterização dos p-grupos finitos que possuem um subgrupo maximal que é cíclico. Em particular, tais grupos são metacíclicos. Por uma questão de completude incluímos o Exemplo a seguir com famílias infinitas de p-grupos (não abelianos) nos quais o conjunto de todos os comutadores formam um subgrupo (cf. [8] para mais detalhes).

Exemplo 2.2.4. *(i) (Diedrais de ordem 2^n) Seja $G = \langle x, a \mid a^{2^{n-1}} = 1 = x^2,\ x^{-1}ax = a^{-1}\rangle$ o grupo dos diedrais de ordem 2^n. Observe que $H = \langle a\rangle$ é maximal. Logo, pelo corolário 2.2.2, segue que $G' = \Gamma(G)$.*

(ii) (p-grupos) Dado $G = \langle x, a \mid x^p = 1 = a^{p^{n-1}},\ a^x = a^{1+p^{n-2}}\rangle$, onde $|G| = p^n$. Temos que o subgrupo $H = \langle a\rangle$ é maximal. Portanto, pelo Corolário 2.2.2, $G' = \Gamma(G)$.

(iii) (Quatérnions Generalizados de ordem 2^n) Dado

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1,, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1}\rangle$$

o grupo dos quarténios, cuja a ordem é igual a $|Q_{2^n}| = 2^n$, ou seja, um 2-grupo. Observe que $H = \langle x\rangle$ é um subgrupo cíclico maximal de Q_{2^n}. Logo, pelo Corolário 2.2.2, segue que $Q'_{2^n} = \Gamma(Q_{2^n})$.

(iv) (Semidiedrais) Dado $G = \langle x, a \mid x^2 = 1 = a^{2^{n-1}}\ ,\ a^x = a^{2^{n-2}-1}\rangle$ o grupo semidiedral de ordem 2^n. Temos que $H = \langle a\rangle$ o subgrupo de G é cíclico e maximal. Portanto, pelo corolário 2.2.2, segue que $G' = \Gamma(G)$.

Exemplo 2.2.5. *Seja $G = \mathrm{GL}(2,\mathbb{C})$ o grupo de matrizes complexas invertíveis 2×2 e $\mathrm{SL}(2,\mathbb{C})$ o subgrupo de G das matrizes com deteminantes iguais a 1. Repare que, dado $[X,Y] \in \Gamma(G)$ temos que*

$$\begin{aligned} det([X,Y]) &= det(X^{-1}Y^{-1}XY) = det(X^{-1})det(Y^{-1})det(X)det(Y) \\ &= det(X)^{-1}det(X)det(Y)^{-1}det(Y) = 1 \end{aligned}$$

Com isso, dado $A \in G'$ segue que

$$det(A) = det(\prod_{i,j}[X_i, Y_j]) = \prod_{i,j} det([X_i, Y_j]) = \prod_{i,j} 1 = 1$$

ou seja, $G' \subset \mathrm{SL}(2,\mathbb{C})$. Assim, mostraremos, com a utilização do Teorema 2.1.4 que

$$G' = B_X = \Gamma(G) \text{ com } X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Para isso, basta mostrarmos que $\Gamma(G) \subseteq B_X$.

De fato, repare primeiramente que $X = X^{-1}$, *já que*

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

Observe também que dado $A \in \mathrm{SL}(2,\mathbb{C})$, *então* A *é semelhante a uma matriz da forma*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ ou } \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \text{ para } \alpha \neq 0$$

Agora, dado um elemento $K \in C_X = \{M^{-1}XM \mid M \in G\}$ *temos que*

$$\begin{aligned} K &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} \frac{ad+bc}{ad-bc} & \frac{2bd}{ad-bc} \\ \frac{-2ac}{ad-bc} & \frac{-ad-bc}{ad-bc} \end{pmatrix} \end{aligned}$$

Assim, podemos afirmar que

$$tr(K) = \frac{ad+bc}{ad-bc} + \frac{-ad-bc}{ad-bc} = 0$$

e também que

$$det(K) = \begin{vmatrix} \frac{ad+bc}{ad-bc} & \frac{2bd}{ad-bc} \\ \frac{-2ac}{ad-bc} & \frac{-ad-bc}{ad-bc} \end{vmatrix} = \frac{-(ad-bc)^2}{(ad-bc)^2} = -1$$

E mais, temos que a recíproca desse resultado é verdadeira. De fato, dado $K \in \mathrm{SL}(2,\mathbb{C})$ *de forma que* $tr(K) = 0$ *e* $det(K) = -1$. *Denominando*

$$K = \begin{pmatrix} \alpha & \beta \\ \gamma & \varepsilon \end{pmatrix}$$

Temos que,

$$tr(K) = \alpha + \varepsilon = 0 \Rightarrow \alpha = -\varepsilon$$

e

$$det(K) = \alpha\varepsilon - \beta\gamma = -1$$

Ora, tomemos

$$\alpha = \frac{ad+bc}{ad-bc}\,; \beta = \frac{2bd}{ad-bc}\,; \gamma = \frac{-2ac}{ad-bc}\,; \varepsilon = \frac{-ad-bc}{ad-bc}$$

onde $a,b,c,d \in \mathbb{C}$

Repare agora que os elementos definidos dessa forma segue arbitrário e de acordo com a hipótese. Além disso, segue que

$$\begin{aligned} K &= \begin{pmatrix} \frac{ad+bc}{ad-bc} & \frac{2bd}{ad-bc} \\ \frac{-2ac}{ad-bc} & \frac{-ad-bc}{ad-bc} \end{pmatrix} \\ &= \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

ou seja, $K \in C_X$. *Agora, observe que dado* $A \in \Gamma(G)$ *temos que* $A \in B_X$ *se, e somente se,* $R^{-1}XRA = S^{-1}XS$ *onde* $R,S \in G$. *Mas isso vai significa que* $R^{-1}XRA \in C_X$ *no qual é equivalente dizer que* $tr(R^{-1}XRA) = 0$. *Logo, com esse raciocinio, segue que se* $A \in \Gamma(G)$, *então* $A \in B_X$. *De fato*

Se $A = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}$ *para algum* $\alpha \neq 0$, *tomemos* R *de forma que* $R^{-1}XR = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *assim*

$$tr(R^{-1}XRA) = tr\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}\right) = 0.$$

Se $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$*, tomemos R de forma que* $R^{-1}XR = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$*, assim*

$$tr(R^{-1}XRA) = tr\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = 0.$$

Se $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$*, tomemos R de forma que* $R^{-1}XR = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$*, assim*

$$tr(R^{-1}XRA) = tr\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\right) = 0.$$

Portanto, $\Gamma(G) \subset B_X$*, logo pelo teorema 2.1.4 segue que* $G' = B_X = \Gamma(G)$*.*

Exemplo 2.2.6 (Grupo de permutações S_n, para $n = 3,4$)**.** *Sejam* $G = S_n$ *o grupo de permutações com n elementos e* A_n *o subgrupo das permutações pares de* S_n*. Mostraremos que* $S_n' = A_n$*. Ora, temos que* $|S_n/A_n| = 2$*, ou seja,* $S_n/A_n \cong C_2$*, portanto* $S_n' \subseteq A_n$*. Por outro lado, temos que* A_n *é gerado por 3-ciclos, portanto dado* $\sigma \in A_n$*, temos que* $\sigma = a_1a_2\dots a_n$ *onde* a_i *são 3-ciclos para todo* $i \in \{1,2,\dots,n\}$*. Com isso, tomando* (abc) *um 3-ciclo arbitrário temos que*

$$(abc) = (ab)(ac)(ba)(ca) = (ba)^{-1}(ca)^{-1}(ba)(ca) \in S_n'$$

ou seja, $\sigma \in S_n'$ *e* $A_n \subseteq S_n'$*. Logo,* $S_n' = A_n$*. Agora, mostraremos a existência de um elemento* $x \in S_n$ *tal que* $B_x = \Gamma(S_n) = S_n'$ *para* $n = 3$ *e* 4*. Ora, com a utilização do Teorema 2.1.4, tomaremos um elemento específico x e mostraremos que* $\Gamma(S_n) \subseteq B_x$ *nos casos em que* $n = 3$ *e* 4*. De fato, para* $n = 3$*, tomemos* $x = (123)$*, então*

$$1 = (123)^{-1}(123)^{-1}(123)(123)^{-1}(123)(123) \in B_{(123)}$$

$$(123) = (132)^{-1}(123)^{-1}(132)(12)^{-1}(123)(12) \in B_{(123)}$$

$$(132) = (123)^{-1} \in B_{(123)} \ (Lema\ 2.1.3\ (iii)).$$

Logo, $\Gamma(S_3) \subseteq B_{(123)}$*, portanto, pelo Teorema 2.1.4, temos que* $B_{(123)} = \Gamma(S_3) = A_3 = S_3'$*. Agora para* $n = 4$*, tomemos* $x = (123)(4)$ *então*

$$1 = ((123(4))^{-1}((123)(4))^{-1}(123)(4)((123)(4))^{-1}(123)(4)(123)(4) \in B_{(123)(4)}$$

$$(123) = (132)^{-1}((123)(4))^{-1}(132)(12)^{-1}(123)(4)(12) \in B_{(123)(4)}$$

$$(142) = (124)^{-1}((123)(4))^{-1}(124)(14)^{-1}(123)(4)(14) \in B_{(123)(4)}$$

$$(134) = (124)^{-1}((123)(4))^{-1}(124)(24)^{-1}(123)(4)(24) \in B_{(123)(4)}$$

$$(243) = (124)^{-1}((123)(4))^{-1}(124)(13)^{-1}(123)(4)(13) \in B_{(123)(4)}$$

$$(12)(34) = (23)^{-1}((123)(4))^{-1}(23)(14)^{-1}(123)(4)(14) \in B_{(123)(4)}$$

$$(13)(24) = (124)^{-1}((123)(4))^{-1}(124)(234)^{-1}(123)(4)(234) \in B_{(123)(4)}$$

$$(14)(23) = (234)^{-1}((123)(4))^{-1}(234)((123))^{-1}(123)(4)(123) \in B_{(123)(4)}$$

e também, pelo Lema 2.1.3 segue que $(132), (124), (143), (234) \in B_{(123)(4)}$, *com isso segue que* $\Gamma(S_4) \subseteq B_{(123)(4)}$, *portanto, pelo Teorema 2.1.4, temos que* $B_{(123)(4)} = \Gamma(S_4) = A_4 = S_4'$. *Para* $n \geq 5$ *a existência de um* $x \in S_n$ *tal que* $\Gamma(S_n) \subseteq B_x$ *também é válida, porém a demostração desse fato foge do objetivo deste trabalho.*

Exemplo 2.2.7. *Neste exemplo mostraremos que é possivel ter um grupo G de forma que* $\Gamma(G) = G'$, *mas* $B_x \neq \Gamma(G)$ *para qualquer* $x \in G$. *De fato, para cada inteiro positivo i, associemos um grupo* G_i *não abeliano. Com isso, consideremos* $G = \bigoplus_{i=1}^{\infty} G_i$ *e tome* $x \in G$ *no qual pode ser pensado em uma sequência da forma* $x = \{x_i\}$ *onde* $x_i \in G_i$ *e* $x_i = e_i$, *em que* e_i *é o elemento identidade de* G_i, *se* $i > N(x)$ *onde* $N(x)$ *é um inteiro positivo dependente de x Se* $a \in B_x$ *e* $a = \{a_i\}$, *com* $a_i \in G_i$ *então* $a_i = e_i$ *se* $i > N(x)$. *Logo, se tomamos um elemento* $b \in \Gamma(G)$ *de forma que* $b_i \neq e_i$ *para algum* $i > N(x)$, *segue que* $b \notin B_x$, *e portanto* $B_x \not\subset \Gamma(G)$, *como x foi escolhido de forma arbitraria, segue que* $B_x \neq \Gamma(G)$. *Por outro lado, temos que* $G' = \bigoplus_{i=1}^{\infty} G_i'$ *e* $\Gamma(G) = \bigoplus_{i=1}^{\infty} \Gamma(G_i)$. *Portanto* $G' = \Gamma(G)$ *se, e somente se,* $G_i' = \Gamma(G_i)$. *Logo, para construirmos um grupo G de forma que* $\Gamma(G) = G'$, *mas* $B_x \neq \Gamma(G)$ *para qualquer* $x \in G$, *basta tomarmos* $G = \bigoplus_{i=1}^{\infty} G_i$ *de forma que* $\lambda(G_i) = 1$ *para todo* $i \in \mathbb{N}$.

Exemplo 2.2.8. *Sejam p e q primos. Iremos mostrar que dado um grupo G tal que a ordem seja* p^i *onde* $i = 1, 2, 3$ *ou* 4, *então* $\Gamma(G) = G'$.

De fato, se $|G| = p^i$ *com* $i = 1$ *ou* 2 *temos pelo lema 1.2.1 que G é abeliano. E pela proposição 1.1.7 segue que* $\Gamma(G) = 1$. *Logo,* $\Gamma(G) = G'$.

Para o caso $|G| = p^3$, *Teorema 1.2.8 garantimos que existe um subgrupo H de ordem* p^2. *Como pelo Lema 1.2.1 temos que H é abeliano e, sendo p o menor primo que divide a ordem de G, segue da Proposição 1.2.7 que H normal sobre G. Com isso, temos que* $|G/H| = p$ *e portanto um grupo ciclico, logo pelo Teorema 2.1.5 segue que* $\Gamma(G) = G'$.

Para $|G| = p^4$, *basta garantirmos que exista um subgrupo normal e abeliano de ordem* p^3. *De fato, consideremos um subgrupo normal de G com ordem* p^2, *denotemos este grupo por*

A. Com isso, consideremos $K = C_G(A)$, observe que pelo item (i) da Proposição 1.2.5 que $K \trianglelefteq N_G(A)$, mas como A é abeliano, temos que $K \trianglelefteq G$. Agora, pelo item (ii) da Proposição 1.2.5 segue que G/K é isomorfo a um subgrupo de $Aut(A)$, mas

$$\begin{aligned} A = C_{p^2} \text{ ou } A = C_p \times C_p \Rightarrow Aut(A) = Aut(C_{p^2}) \text{ ou } Aut(A) = Aut(C_p \times C_p) \\ \Rightarrow |Aut(C_{p^2})| = \phi(p^2) = p(p-1) \text{ ou } \\ |Aut(C_p \times C_p)| = |\ \mathrm{GL}(2,p)| = p(p-1)^2(p+1) \end{aligned}$$

como $|G/K| \mid\mid |Aut(A)|$, pelas combinações, a única possível nos garante que $|G/K| = p$, ou seja, $|K| = p^3$ e, além disso, G/K é cíclico. Com isso, agora basta provarmos que K é abeliano. De fato, repare que $A \subset Z(K)$, isso implica que K/A é cíclico e, portanto, K é abeliano. Logo, considerando K o subgrupo normal e abeliano de G, tal que G/K é cíclico, segue pelo Teorema 2.1.5 que $\Gamma(G) = G'$.

Exemplo 2.2.9. *No caso $|G| = pq$, suponhamos que $p < q$, pelo Teorema 1.2.8 observamos que $n_p = 1$, então H é normal a G, onde H é o p-subgrupo de Sylow de G, além disso, por ter ordem prima p temos que H é abeliano, logo existe o subgrupo quociente G/H no qual tem ordem prima q e consequentemente é cíclico. Assim, pelo Teorema 2.1.5 segue que $\Gamma(G) = G'$. De forma análoga para o caso $q < p$, chegamos ao mesmo resultado.*

Exemplo 2.2.10. *Para $|G| = p^2q$, pela Proposição 1.2.9 temos que existe um p-subgrupo de Sylow normal ou um q-subgrupo de Sylow normal. Se existe $H \trianglelefteq G$ tal que H é um p-subgrupo de Sylow, temos pelo Lema 1.2.1 que H é abeliano, e além disso, G/H tem ordem prima q e portanto é cíclico, portanto $\Gamma(G) = G'$. Agora, para o caso em que existe $H \trianglelefteq G$ tal que H é um q-subgrupo de Sylow de G, temos que $G' \subset H$, pois $|G/H| = p^2$, e com isso segue que $|G'| = q$, logo pela Proposição 1.1.8 segue de $\lambda(G) = 1$.*

Combinando os Exemplos 2.2.8, 2.2.9 e 2.2.10 podemos verificar a seguinte proposição:

Proposição 2.2.11. *Seja G um grupo finito de ordem < 30 (exceto para $|G| = 24$). Então $\Gamma(G) = G'$.*

Demonstração. Reapare que os grupos G de ordens 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29 são da forma p^i para algum $i = 1,2,3$ *ou* 4. Assim, pelo exemplo 2.2.8 temos que $\Gamma(G) = G'$. Da mesma forma, temos que os grupos G de ordens 6, 10, 14, 15, 21, 22, 26 são grupos da forma pq, em que p e q são primos, com isso, pelo exemplo 2.2.9 segue que $\Gamma(G) = G'$. E por ultimo, os grupos G de ordens 12, 18, 20, 28 tem formato p^2q onde p e q são primos. Logo, pelo exemplo 2.2.10 temos que os conjuntos de comutadores de G é igual ao subgrupo derivado também. Tendo essas observações, segue o resultado previsto. $\square$

Em vista da Proposição anterior, cabe ressaltar que o resultado acima não é o melhor possível. Nos trabalhos [4] e [5], Robert M. Guralnick mostrou que todos os grupos finitos G de ordem $|G| < 96$ tem $\lambda(G) = 1$. Mais ainda, ele apresentou um grupo de ordem 96 nos qual $\Gamma(G) \neq G'$. As técnicas empregadas no artigo [5] fazem uso de teoria de representações de grupos finitos e, nessa perspectiva, não será objeto de estudo dessa dissertação.

Observação 2.2.12. *No próximo capítulo, usaremos o software GAP para verficar que existem apenas dois grupos até ordem* 96 *para os quais temos* $\lambda(G) > 1$. *E, seguindo o artigo [4], construímos explicitamente um desses grupos.*

Capítulo 3

Exemplos Minimais com $\lambda(G) > 1$

Nesse capítulo temos três objetivos que foram distribuídos em três seções:

(1) Introduzir algumas rotinas do GAP, no qual foram necessária para a construção do algoritmo em que conseguimos identificar grupos com $\lambda(G) > 1$;

(2) Com este algoritmo construido no GAP mostraremos que todos os grupos G de ordem $\leqslant 95$ tem $\lambda(G) = 1$ e existem, exatamente, dois grupos de ordem 96 com $\lambda(G) > 1$;

(3) Baseados no artigo de R. M. Guralnick [4] construiremos um desses grupos em questão.

Aqui cabe destacar que o item (2) é consequência do artigo de R. M. Guralnick (cf. [5]), mas a demonstração originalmente apresentada envolve técnicas que fogem dos objetivos desse trabalho. Assim, optamos pelo uso direto do GAP para efetuar os cálculos até ordem 96.

3.1 GAP

Nessa seção apresentaremos as funções empregadas ao longo do nosso estudo com o GAP [2]. Pressupomos o conhecimento prévio de alguns fundamentos de programação, por exemplo: os comandos “for - do, print, if - then, ...”. Para maiores detalhes veja as referências [10] e [9, Capítulo 1–4].

3.1.1 Rotinas básicas do GAP

Para construir os algoritmos usados para encontrar os grupos usamos umas rotinas específicas do GAP, são elas:

1. AllSmallGroup(ord): Esta função é usada no proposito de analisar todos os grupos de uma determinada ordem;
2. SmallGroup(ord, pos): é usada para analisar um determinado grupo de uma ordem pré estabelecida;
3. IsSolvable(G): Nesta função analisa se determinado grupo G é soluvel;
4. DerivedLength(G): Caso o grupo G seja solúvel, com essa função podemos calcular o comprimento derivado de G;
5. IsNilpotent(G): Nesta função analisa se determinado grupo G é nilpotente;
6. DerivedSubgroup(G): Esta função calcula o subgrupo derivado (G') de determinado grupo G;
7. StructureDescription(G): Esta função retorna a estrutura de um grupo G pré determinado. Essa estrutura é feita com base nas definições do GAP. São diversas estruturas, mas para os grupos em que são apresentados neste trabalho necessitamos conhecer as seguintes
   (a) $G \times H$: Essa estrutura indica o produto direto de G e H;
   (b) $G : H$: Essa estrutura indica o produto semi direto de G por H.

3.1.2 Algoritmo para determinar elementos no derivado que não são comutadores

Com o seguinte algoritmo, conseguimos determinar os grupos nos quais o subgrupo derivado possui elementos que não são comutadores:

```
a := AllSmallGroups([1..ord]);;
for i in [1..Size(a)] do
g := a[i];;
e:=Elements(g);;
k:=DerivedSubgroup(g);;
k1:=[];;
for j in [1..Size(e)] do
for t in [1..Size(e)] do
Add(k1,Comm(e[j],e[t]));;
```

```
od;
od;
if  Size(Difference(k, Set(k1)))>1  then
Print(StructureDescription(g), ”\n”);
Print(i, "n");
fi;
od;
```

Com tais grupos em mãos e suas respectivas posições dentro da rotina SmallGroup, abstraímos certas propriedades algébricas para entender melhor a influência dos comutadores em sua estrutura. Por exemplo, Solubilidade, Nilpotência, os elementos pertencentes ao subgrupo derivado que não são comutadores, além da ordem do subgrupo derivado e o número de elementos do conjunto dos comutadores. Consideremos o seguinte algoritmo:

```
g:= SmallGroup(ord, pos);;
e:= Elements(g);;
k:= DerivedSubgroup(g);;
k1:= [];;
for j in [1..Size(e)] do
for t in[1..Size(e)] do
Add(k1, Comm(e[j], e[t]));;
od;
od;
Print(k, "\n");
Print(Set(k1), "\n");
Print("Temos ", Size(Difference(k, Set(k1)), "elementos não comutadores que estão no deri-
vado e eles são ", Set(Difference(k, Set(k1)) "n");
if IsSolvable(g) = true then
Print("G é soluvel e seu comprimento derivado é ", DerivedLength(g), ".", "\n");
else
Print("G não é soluvel.", "\n");
fi;
if IsNilpotent(g) = true then
Print("G é nilpotente.", "\n");
else
Print("G não é nilpotente.", "\n");
```

fi;

3.2 Grupos com ordem $\leqslant 96$ (via GAP)

Em [4], Guralnick mostrou que existe um grupo de ordem 96 com $\lambda(G) = 2$. Em seguida, em [5], ele provou que todos os grupos finitos G com ordem $\leqslant 95$ tem largura $\lambda(G) = 1$. Essa seção será devotada a ilustrar este resultado utilizando o software livre GAP, mostrando algumas características e propriedades destes grupos. E, na próxima seção, detalharemos a construção de um desses grupos de ordem 96.

Com a utilização do GAP, foi desenvolvido um algoritmo no qual ele acusa quando um grupo tem o conjunto de comutadores diferente do subgrupo derivado ($\Gamma(G) \neq G'$). Utilizando este algoritmo para grupos com ordem até 96 temos que ((C4 x C2) : C4) : C3 (SmallGroup(96,3)) e o (C2 x C2 x Q8) : C3 (SmallGroup(96,203)) são os únicos grupos no qual $\lambda(G) > 1$. E repare que ambos são de ordem 96, portanto vemos por meio computacional que o resultado descrito por Guralnick em [5] é ilustrado, já que os primeiros exemplos de grupos com $\lambda(G) > 1$ aparece somente na ordem 96, segue que os grupos de ordem $\leqslant 95$ tem $\lambda(G) = 1$.

Na ordem 96, temos dois exemplos de grupos com essas propriedades, são eles:

1. Usando o GAP, consideremos o grupo G que aparece na posição: SmallGroups(96,3). Usando o software GAP, temos que G é um grupo 6-gerado, solúvel com comprimento derivado 3 (e não nilpotente). Mais ainda, a ordem de seu subgrupo derivado $|G'| = 32$ e o conjunto de comutadores possui um total 29 elementos. Assim, existem 3 elementos neste grupo que estão contidos no subgrupo derivado e não são comutadores.

```
g:= SmallGroup(96,3);
<pc group of size 96 with 6 generators>
Print(StructureDescription(g));
((C4 x C2) : C4) : C3
e:= Elements(g);;
k:= DerivedSubgroup(g);;
k1:= [];;
for j in [1..Size(e)] do
for t in [1..Size(e)] do
Add(k1, Comm(e[j], e[t]));;
od;
od;
Print(Elements(DerivedSubgroup(g)), "\n");
[ <identity> of ..., f2, f3, f4, f5, f6, f2*f3, f2*f4, f2*f5, f2*f6, f3*f4,
  f3*f5, f3*f6, f4*f5, f4*f6, f5*f6, f2*f3*f4, f2*f3*f5, f2*f3*f6, f2*f4*f5,
  f2*f4*f6, f2*f5*f6, f3*f4*f5, f3*f4*f6, f3*f5*f6, f4*f5*f6, f2*f3*f4*f5,
  f2*f3*f4*f6, f2*f3*f5*f6, f2*f4*f5*f6, f3*f4*f5*f6, f2*f3*f4*f5*f6 ]
Print(Set(k1), "\n");
[ <identity> of ..., f2, f3, f5, f6, f2*f3, f2*f4, f2*f5, f2*f6, f3*f4,
  f3*f5, f3*f6, f4*f6, f2*f3*f4, f2*f3*f5, f2*f3*f6, f2*f4*f5, f2*f4*f6,
  f2*f5*f6, f3*f4*f5, f3*f4*f6, f3*f5*f6, f4*f5*f6, f2*f3*f4*f5, f2*f3*f4*f6,
  f2*f3*f5*f6, f2*f4*f5*f6, f3*f4*f5*f6, f2*f3*f4*f5*f6 ]
Print(Difference(k, Set(k1)), "\n");
[ f4, f4*f5, f5*f6 ]
if IsSolvable(g) = true then
h:= DerivedLength(g);;
Print("G é solúvel e seu comprimento derivado é ", h, ".", "\n");
fi;
G é solúvel e seu comprimento derivado é 3.
if IsNilpotent(g) = true then
Print ("G é Nilpotente.");
else
Print("G não é Nilpotente.");
fi;
G não é Nilpotente.
```

Figura 3.1 Algoritmo GAP: (C4 x C2) : C4) : C3

2. No GAP, o outro grupo G com as propriedades desejadas, aparece na posição: SmallGroup(96, 203). Usando o programa, temos que G é um grupo 6-gerado, solúvel com comprimento derivado 3 (e não nilpotente). Além disso, ordem de seu subgrupo derivado $|G'| = 32$ e o conjunto de comutadores possui um total 29 elementos. Então, como no caso anterior, existem 3 elementos neste grupo que estão contido no subgrupo derivado e não são comutadores.

```
g:= SmallGroup(96,203);
<pc group of size 96 with 6 generators>
Print(StructureDescription(g));
(C2 x C2 x Q8) : C3
e:= Elements(g);;
k:= DerivedSubgroup(g);;
k1:= [];;
for j in [1..Size(e)] do
for t in [1..Size(e)] do
Add(k1, Comm(e[j], e[t]));;
od;
od;
Print(Elements(DerivedSubgroup(g)), "\n");
[ <identity> of ..., f2, f3, f4, f5, f6, f2*f3, f2*f4, f2*f5, f2*f6, f3*f4,
  f3*f5, f3*f6, f4*f5, f4*f6, f5*f6, f2*f3*f4, f2*f3*f5, f2*f3*f6, f2*f4*f5,
  f2*f4*f6, f2*f5*f6, f3*f4*f5, f3*f4*f6, f3*f5*f6, f4*f5*f6, f2*f3*f4*f5,
  f2*f3*f4*f6, f2*f3*f5*f6, f2*f4*f5*f6, f3*f4*f5*f6, f2*f3*f4*f5*f6 ]
Print(Set(k1), "\n");
[ <identity> of ..., f2, f3, f4, f5, f6, f2*f3, f2*f4, f2*f5, f3*f4, f3*f5,
  f4*f5, f4*f6, f5*f6, f2*f3*f4, f2*f3*f5, f2*f4*f5, f2*f4*f6, f2*f5*f6,
  f3*f4*f5, f3*f4*f6, f3*f5*f6, f4*f5*f6, f2*f3*f4*f5, f2*f3*f4*f6,
  f2*f3*f5*f6, f2*f4*f5*f6, f3*f4*f5*f6, f2*f3*f4*f5*f6 ]
Print(Difference(k, Set(k1)), "\n");
[ f2*f6, f3*f6, f2*f3*f6 ]
if IsSolvable(g) = true then
h:= DerivedLength(g);;
Print("G é solúvel e seu comprimento derivado é ", h, ".", "\n");
fi;
G é solúvel e seu comprimento derivado é 3.
if IsNilpotent(g) = true then
Print ("G é Nilpotente.");
else
Print("G não é Nilpotente.");
fi;
G não é Nilpotente.
```

Figura 3.2 Algoritmo GAP: (C2 x C2 x Q8) : C3

3.3 Um grupo de ordem 96 com elementos não comutadores

Seguiremos o artigo [4] e construiremos, explicitamente, um grupo G que possui ordem 96 com $\lambda(G) > 1$.

Lema 3.3.1. *Sejam G um grupo com subgrupo H e um elemento $x \in G$ tal que $G' \subseteq H$ e $G = \langle H, x\rangle$. Se w é um comutador de G, então $w = [x^k a, b]$ para algum $k \in \mathbb{Z}$ e $a, b \in H$.*

Demonstração. Como $H \trianglelefteq G$, temos que para todo $g \in G$ podemos reescrevê-lo como $g = x^k h$, onde $h \in H$ e $k \in \mathbb{Z}$. Logo, um comutador w de G tem o seguinte formato:

$$w = [g_1, g_2] = [x^s h_1, x^t h_2].$$

Caso $t = 0$ não há nada a demonstrar, agora para $s = 0$, pelo Lema 1.1.3 temos que

$$[h_1, x^t h_2] = [(x^t h_2)h_1, x^t h_2] = [x^t h_2 h_1, (x^t h_2 h_1)^{-1} x^t h_2] = [x^t h_3, h_1^{-1}]$$

como desejamos. Faremos indução sobre $k = min\{|s|, |t|\}$. Para o caso $k = 0$ já foi verificado acima. Agora consideremos $w = [x^s h_1, x^t h_2]$, com $k > 0$ e também que o resultado seja válido para todos k' tal que $0 < k' < k$. Supondo $|s| \geq |t|$, sem perda de generalidade, pelo Algoritmo da Divisão temos que

$$w = [x^s h_1, x^t h_2] = [(x^t h_2)^{-q} x^s h_1, x^t h_2] = [x^{s-qt} h_3, x^t h_2].$$

Porém $k' = min\{|s - qt|, |t|\} < k$. Logo, por indução, segue o resultado. $\square$

Seja o grupo $Q_8 \rtimes C_3 = \langle a, b, x \mid a^4 = b^4 = x^3 = 1, xax^{-1} = b, xbx^{-1} = ab, a^2 = b^2, aba^{-1} = b^{-1}\rangle$, consideremos $H_1 = \langle a, b\rangle \cong Q_8$. Repare que, $H_1 \trianglelefteq G_1$, portanto $G_1' \subseteq H_1$. Por outro lado, pela propriedades de G_1, temos que $a = [x^{-1}, b^{-1}], ba^{-1} = [x^{-1}, a^{-1}] \in G_1'$, ou seja, $\langle a, b^{-1}\rangle \subseteq G_1'$. Portanto, $G_1' \cong H_1 = Q_8$.

Lema 3.3.2. *Se $u, v \in H_1$ e $[x^k u, v] = a^2$, então $3|k$.*

Demonstração. Suponha que $3 \not| k$, então $|\langle [x^k, v]\rangle| = 4$ ou $v = a^2$. Como $[x^k, v] \in H_1 \cong Q_8$, temos que $|\langle [x^k, v]\rangle| = 1, 2$ *ou* 4. Além disso, se $3 \not| k$ e $|\langle x\rangle| = 3$ é suficiente considerar $k = 1$ *ou* 2. Com isso, se $|\langle [x^k, v]\rangle| = 1$, para $k = 1$ teremos que $xv = vx$, portanto, se $v = a^i$ onde $0 \leq i \leq 3$, temos

$$xa^i = a^i x \Rightarrow xa^i x^{-1} = a^i \Rightarrow b^i = a^i \Rightarrow v \in \langle a^2\rangle.$$

Se $v = a^i b$ para $0 \leq i \leq 3$ temos que

$$xa^ib = a^ibx \Rightarrow xa^ibx^{-1} = a^ib \Rightarrow b^iab = a^ib \Rightarrow b^i = a^{i-1}$$

contradição, já que $a^i = b^k \in \langle a^2 \rangle$, teríamos i,k números pares e com isso $i \equiv k$ $(mod\ 4)$. Agora, se $|\langle [x^k,v] \rangle| = 2$, para $k = 1$, como $[x,v] \in H_1$ tem ordem 2, temos que $[x,v] = a^2$. Logo, se $v = a^i$ para $0 \leq i \leq 3$, então

$$x^{-1}a^{-i}xa^i = a^2 \Rightarrow a^{-i}xa^ix^{-1} = xa^2x^{-1} = a^2 \Rightarrow a^ib^i = a^2 \Rightarrow b^i = a^{i+2}$$

contradição, já que $i \equiv i+2$ $(mod 4)$. Agora, se $v = a^ib$ com $0 \leq i \leq 3$, temos que

$$x^{-1}b^{-1}a^{-i}xa^ib = a^2 \Rightarrow b^{-1}a^{-i}xa^ibx^{-1} = xa^2x^{-1} = a^2 \Rightarrow b^{-1}a^{-i}b^iab = a^2$$
$$\Rightarrow a^{-i}b^ia = a^2 \Rightarrow b^i = a^{i+1}$$

Novamente uma contradição, pois $i \equiv i+1 (mod\ 4)$. Para os casos em que $k = 2$ e $|\langle [x,v] \rangle| = 1$ *ou* 2 procedemos da mesma maneira que os anteriores. Mas, para $|\langle [x^k,v] \rangle| = 4$, teríamos

$$a^2 = [x^ku,v] = [x^k,v][u,v]$$

já que $H_1' = Z(H_1)$. E por outro lado, $|\langle [x^k,v] \rangle| = |\langle [x^k,v] \rangle||\langle [u,v] \rangle| = 4$, contradição pois $|\langle [x^k,v] \rangle| = 2$. Logo, $v \in \langle a^2 \rangle$, ou seja, $[x^ku,a^2] = a^2$ o que significa de $a = 1$, contradição, portanto segue que $k \equiv\ 0$ $(mod\ 3)$. □

Observação 3.3.3. *Consideremos $G_1 = Q_8 \rtimes C_3$ e G_2 um grupo não abeliano que tenha um subgrupo normal abeliano H_2 de índice 3. Tome $y \in G_2 \setminus H_2$, com isso consideremos o grupo $G = \langle H_1 \times H_2, (x,y) \rangle = (H_1 \times H_2)\langle (x,y) \rangle$, já que $G' \subseteq G_1' \times G_2' \subseteq H_1 \times H_2$.*

Teorema 3.3.4. *Seja G o grupo descrito na observação 3.3.3, temos que*

(i) $G' = G_1' \times G_2'$;

(ii) $|G| = 24|H_2|$;

(iii) $\lambda(G) > 1$

Demonstração. Faremos a demonstração de cada item individualmente.

(i) Já temos que $G' \subseteq G_1' \times G_2'$, pois $G \leq G_1 \times G_2$. Por outro lado, dado $\alpha_1 \in \Gamma(G_1)$, pelo Lema 3.3.1 temos que

$$(\alpha_1, 1_{G_2}) = [(x^kh, y^k), (h_1, 1)] \in G'.$$

De modo análogo, dado $\alpha_2 \in \Gamma(G_2)$ temos $(1_{G_1}, \alpha_2) \in G'$. Assim,

$$G_1' \times G_2' = \langle (\alpha_1, 1_{G_2}), (1_{G_1}, \alpha_2) | \alpha_i \in \Gamma(G_i), i = 1,2 \rangle \subseteq G'$$

Portanto, $G' = G_1' \times G_2'$.

(ii) Como $y \notin H_2$ e $H_2 \trianglelefteq G_2$, temos que $y^3 \in H_2$. Com isso,

$$(H_1 \times H_2) \cap \langle (x,y) \rangle = \langle (x,y)^3 \rangle = \langle (1,y^3) \rangle$$

Assim, $|\langle (x,y) \rangle : \langle (1,y^3) \rangle = 3$. Portanto,

$$|G| = \frac{|H_1 \times H_2||\langle (x,y) \rangle|}{|(H_1 \times H_2) \cap \langle (x,y) \rangle|} = \frac{8|H_2||\langle (x,y) \rangle|}{|\langle (1,y^3) \rangle|} = 24|H_2|.$$

(iii) Dado $c \in G_2' \backslash \{1\}$ e $w = (a^2, c)$. Suponhamos que w é um comutador e consideremos $H = H_1 \times H_2$, segue que $G = \langle H, (x,y) \rangle = H\langle (x,y) \rangle$. Pelo Lema 3.3.1 temos $(h_1, h_2), (k_1, k_2) \in H$ e $k \in \mathbb{Z}$ tais que

$$(a^2, c) = [(x^k, y^k)(h_1, h_2), (k_1, k_2)]$$

ou seja,

$$a^2 = [x^k h_1, k_1] \text{ e } c = [y^k h_2, k_2]$$

Pelo Lema 3.3.2, temos que $3|k$. Como $|\langle x \rangle| = 3$ e $|G_2 : H_2| = 3$, temos que $a^2 = [h_1, k_1]$ e $y^k \in H_2$, ou seja, $c = [h_2 y^k, k_2] \in H_2' = \{1\}$. Absurdo, pois $c \neq 1$.

$\square$

Observação 3.3.5. *Observe que agora podemos construir diversos grupos G com $\lambda(G) > 1$. De fato, seja G_2 um grupo não abeliano que contenha um subgrupo normal abeliano H_2 tal que $|G_2 : H_2| = 3$, segue da utilização do grupo G_1 definido na observação 3.3.3 e do Teorema 3.3.4 que teremos um grupo G de ordem $24|H_2|$ tal que $G' = Q_8 \times G_2'$ e $\lambda(G) > 1$.*

Exemplo 3.3.6. *Tomemos $G_2 = A_4$. Como $A_4' = K$, onde K é o grupo de Klein. Pelos resultados vistos acima obtemos um grupo G de ordem 96 tal que $G' \cong Q_8 \times K$ e $\lambda(G) > 1$.*

Exemplo 3.3.7. *Tomemos G_2 como um grupo não abeliano de ordem 27 e $H_2 \trianglelefteq G_2$ tal que $|H_2| = 9$. Observe que $|G_2'| = 3$. Portanto, temos um grupo G de ordem 216 tal que $G' \cong Q_8 \times C_3$ e $\Gamma(G) \neq G'$.*

Capítulo 4

Construindo grupos com $\lambda(G) > 1$

Nesse capítulo estudamos os trabalhos [1] e [6] nos quais são construídos grupos de largura $\lambda(G) > 1$. Em [6] M. Isaacs constrói um critério para a criação de grupos com $\Gamma(G) \neq G'$ sendo que G é um produto entrelaçado, $G = U \wr H$ (Teorema E da Introdução). Neste critério, toma-se como base características dos grupos U e H, o que nos proporciona diversas famílias de grupos nos quais $\lambda(G) > 1$. Enquanto isso, a partir de P. J. Cassidy [1], construímos grupos nilpotentes (de classe 2) com largura infinita (Teorema F da Introdução).

4.1 Produtos entrelaçados e elementos não comutadores

O objetivo desta seção é investigar exemplos de produtos entrelaçados de grupos (finitos) nos quais contém elementos não comutadores. Tais exemplos são baseados num artigo do M. Isaacs [6].

Lema 4.1.1. *Sejam G um grupo, H um subgrupo de G e $A \trianglelefteq G$ abeliano de forma que $G = AH$ com $A \cap H = 1$. Se $[x,y] \in A$ com $x,y \in G$, então $[x,y] \in [A,K]$ para algum $K \subseteq H$ abeliano.*

Demonstração. De fato, dados $x,y \in G$ temos que existem $a,b \in A$ e $h,k \in H$ tal que $x = ah$ $y = bk$. Por hipótese $[x,y] \in A$, portanto

$$\begin{aligned} [x,y]A = A &\Rightarrow x^{-1}y^{-1}xyA = A \\ &\Rightarrow xyA = yxA \end{aligned}$$

ou seja, x e y comutam em G/A. Mais ainda, se

$$\begin{aligned} xyA = yxA &\Rightarrow ahbkA = bkahA \\ &\Rightarrow hkA = khA \\ &\Rightarrow [h,k]A = A \\ &\Rightarrow [h,k] \in A. \end{aligned}$$

Ora, mas como $A \cap H = 1$, segue que $[h,k] = 1$, ou seja, $hk = kh$. Com isso, definamos $K = \langle h,k \rangle$, podemos afirmar que K é abeliano pois dados $m,n \in K$, temos que $m = h^i k^i$ e $n = h^j k^j$ com $i, j \in \mathbb{Z}$, assim

$$mn = h^i k^i h^j k^j = h^j k^j h^i k^i = nm.$$

Com isso, consideremos $[A,K]$, o grupo gerado pelos comutadores dos elementos de A com os elementos de K. Repare que $A,K \leq N_G([A,K])$, já que dados $a_1,a_2 \in A$ e $k_1,k_2 \in K$, temos que

$$[a_1a_2,k_1] = a_2^{-1}[a_1,k_1]a_2[a_2,k_1] \Rightarrow a_2^{-1}[a_1,k_1]a_2 = [a_1a_2,k_1][a_2,k_1]^{-1} \in [A,K]$$

e de forma análoga

$$[a_1,k_1k_2] = [a_1,k_2]k_2^{-1}[a_1,k_1]k_2 \Rightarrow k_2^{-1}[a_1,k_1]k_2 = [a_1,k_2]^{-1}[a_1,k_1k_2] \in [A,K]$$

ou seja, $A,K \leq N_G([A,K])$ e portanto, $AK \leq N_G([A,K])$, logo podemos concluir que $[A,K] \trianglelefteq AK$. Assim, as imagens de A e K em $AK/[A,K]$ são abeliano e centralizam umas a outras, portanto $AK/[A,K]$ é abeliano. Logo, $[x,y] \in (AK)' \subseteq [A,K]$. $\square$

Lema 4.1.2. *Sejam $G = U \wr H$ onde U é abeliano e G é finito. Sejam B o grupo base de G e $K \subseteq H$. Consideremos $n = |H : K|$, $\Omega = \{t_1,\dots,t_n\}$ o transversal de K em H e a aplicação*

$$\theta_{t_i} : B \to U$$
$$\theta_{t_i}(f) = \prod_{k \in K} f(t_i k).$$

Temos as seguintes afirmações:

(i) θ_{t_i} *é homomorfismo;*

(ii) θ_{t_i} *é sobrejetivo.*

Demonstração. :

(i) Reparamos que θ_{t_i} é um homomorfismo, pois dados $f, g \in B$ segue que

$$\begin{aligned}\theta_{t_i}(fg) &= \prod_{k\in K} fg(t_ik) \\ &= \prod_{k\in K} f(t_ik)g(t_ik) \\ &= \prod_{k\in K} f(t_ik)\prod_{k\in K} g(t_ik) \\ &= \theta_{t_i}(f)\theta_{t_i}(g).\end{aligned}$$

E, com isso, temos que

$$\theta_{t_i}(k^{-1}fk) = \theta_{t_i}(k^{-1})\theta_{t_i}(f)\theta_{t_i}(k) = \theta_{t_i}^{-1}(k)\theta_{t_i}(f)\theta_{t_i}(k) = \theta_{t_i}(f)$$

para $f \in B$ e $k \in K \subseteq H$, já que temos U abeliano.

(ii) Temos que θ_{t_i} é uma função sobrejetora, onde $t_i \in \Omega$, basta observar que para todo $u \in U$ existe um $f_{u,t_i} \in B$ tal que

$$f_{u,t_i} : H \to U$$
$$f_{u,t_i}(h) = \begin{cases} u\ ,\ h = t_i \\ 1\ ,\ h \neq t_i \end{cases}$$

portanto, $\theta_{t_i}(f_{u,t_i}) = \prod_{k\in K} f_{u,t_i}(t_ik) = u$.

□

Lema 4.1.3. *Sejam $G = U \wr H$ onde U é abeliano e G é finito. Sejam B o grupo base de G e $K \subseteq H$. Então $|[B,K]| = |U|^{|H|-|H:K|}$.*

Demonstração. Chamemos $n = |H : K|$, consideremos $\Omega = \{t_1, \ldots, t_n\}$ o transversal de K em H e tomemos $U_i \cong U$ para $1 \leq i \leq n$. Consideremos a seguinte aplicação $\psi = \theta_{t_1} \times \ldots \times \theta_{t_n}$ dada por

$$\begin{aligned}\psi : B &\to U_1 \times \ldots \times U_n \\ f &\mapsto \left(\prod_{k\in K} f(t_1k), \ldots, \prod_{k\in K} f(t_nk)\right)\end{aligned}$$

Pelo lema 4.1.2, θ_{t_i} é homomorfismo. Daí, segue na utilização desse fato coordenada a coordenada que ψ é um homomorfismo. Além disso,

$$\psi(\{f_{u,t_i} \mid u \in U\}) = U_1 \times \{1\} \times \ldots \times \{1\},$$

pois $\{\psi(f_{u,t_1} \mid u \in U\} = U_1 \times \{1\} \times \ldots \times \{1\} \in Im(\psi)$. De modo análogo, $\{\psi(f_{u,t_j} \mid u \in U\} = \{1\} \times \ldots \times U_j \times \ldots \times \{1\} \in Im(\psi)$. Assim, $U_1 \times U_2 \times \ldots \times U_n = Im(\psi)$, ou seja, ψ é sobrejetora. Com isso, $Ker(\psi) = C = \bigcap_{i=1}^{n} Ker(\theta_{t_i})$. Então, pelo Primeiro Teorema dos Isormorfismos, segue que

$$\begin{aligned} B/C \cong |U|^n &\Longrightarrow \frac{|B|}{|C|} = |U|^n = |U|^{|H:K|} \\ &\Longrightarrow \frac{|U|^{|H|}}{|C|} = |U|^{|H:K|} \\ &\Longrightarrow |C| = |U|^{|H|-|H:K|}. \end{aligned}$$

Assim, basta mostrarmos que $[B,K] = C$. De fato

- $[B,K] \subseteq C$:
  Dados $f \in B$ e $k \in K$, então

  $$\theta_t([f,k]) = \theta_t(f^{-1})\theta_t(k^{-1})\theta_t(f)\theta_t(k) = \theta_t^{-1}(f)\theta_t^{-1}(k)\theta_t(f)\theta_t(k) = 1.$$

  Portanto, $[f,k] \in C$ e assim $[B,K] \subseteq C$.

- $C \subseteq [B,K]$:
  De fato, consideremos o homomorfismo canônico

  $$\tau : B \to B/[B,K]$$

  e observe que
  $$\tau(k^{-1}fk) = \tau^{-1}(k)\tau(f)\tau(k) = \tau(f)$$

  para todo $f \in B$. Assim, sejam $c \in C$ e $k \in K$, definamos $c_k \in B$ por

  $$c_k = \begin{cases} c(x) \text{ , } xk \in T \\ 1 \text{ , } xk \notin T. \end{cases}$$

  Segue que $c = \prod_{k \in K} c_k$. Com isso, consideremos $b = \prod_{k \in K} (c_k)^k$, como $\tau(f) = \tau(f^k)$ temos $\tau(c) = \tau(b)$. Consideremos, sem perda de generalidade, que $b = 1$, assim se $x \notin T$, então $(c_k)^k(x) = c_k(xk^{-1}) = 1$ para todo k e $b(x) = 1$. Agora, se $x \in T$, então

  $$(c_k)^k(x) = c_k(xk^{-1}) = c(xk^{-1})$$

portanto

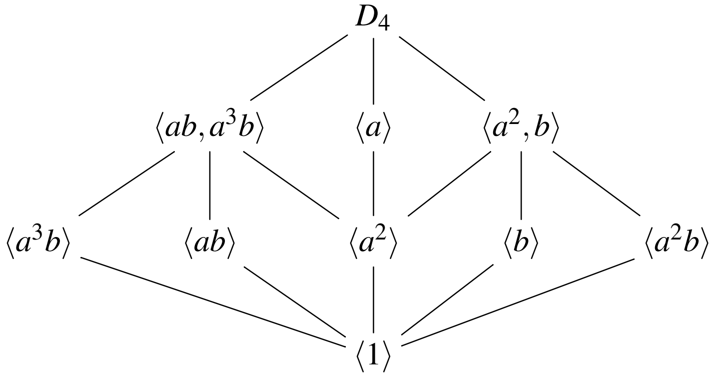
$$b(x) = \prod_k c(xk^{-1}) = \theta_x(c) = 1$$

Logo, $\tau(c) = 1$ e portanto, $C \subseteq [B,K]$ como queriamos demonstrar.

$\square$

Definição 4.1.4. *Seja G um grupo não abeliano. Dizemos que H é um subgrupo abeliano maximal de G se para todo subgrupo K de G abeliano, tal que $H \leq K \leq G$, temos $H = K$.*

Exemplo 4.1.5. *Consideremos a ilustração abaixo do retículado do grupo $D_4 = \langle a,b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$:*



Reparem que, todos os subgrupos de D_4 são abelianos, porém os abelianos maximais são somente os $\langle ab, a^3b \rangle, \langle a \rangle, \langle a^2, b \rangle$, já que $\langle a^3b \rangle, \langle ab \rangle, \langle a^2 \rangle, \langle b \rangle, \langle a^2b \rangle$ são subgrupos próprios de outro subgrupo abeliano de D_4.

Teorema 4.1.6. *Sejam U e H grupos finitos com U abeliano e H não abeliano. Consideremos $G = U \wr H$. Se*

$$\sum_{A \in \mathscr{A}} \left(\frac{1}{|U|} \right)^{|H:A|} < \frac{1}{|U|},$$

então $\lambda(G) > 1$, sendo que $\mathscr{A}$ é o conjunto dos subgrupos abelianos maximais de H.

Demonstração. Suponha que todos os elementos de $[B:H]$ são comutadores. Daí, pelo lema 4.1.1, temos que

$$[B,H] = \bigcup_{A \in \mathscr{A}} [B,A].$$

Como, pelo lema 4.1.3, temos $|[B,A]| = |U|^{|H|-|H:A|}$ segue que

$$|U|^{|H|-1} = |[B,H]| \leq \sum_{A \in \mathscr{A}} |[B,A]| = \sum_{A \in \mathscr{A}} |U|^{|H|-|H:A|}$$

$$\Rightarrow \frac{1}{|U|} \leq \sum_{A \in \mathscr{A}} \left(\frac{1}{|U|} \right)^{|H:A|}$$

uma contradição. Logo, G' possui um elemento não comutador. $\square$

Corolário 4.1.7. *Sejam U e H grupos finitos com U abeliano e H não abeliano. Consideremos $G = U \wr H$. Se*

$$|\mathscr{A}| < |U|,$$

então $\lambda(G) > 1$, sendo que $\mathscr{A}$ é o conjunto dos subgrupos abelianos maximais de H.

Demonstração. Seja $\mathscr{A} = \{A_1, A_2, \ldots, A_n\}$ o conjunto de subgrupos abelianos maximais de H. Repare que A_i é subgrupo proprio de H, para todo $i = 1, 2, \ldots, n$ portanto consideremos sem perda de generalidade que

$$2 \leq |H : A_1| \leq |H : A_2| \leq \ldots \leq |H : A_n|$$

Assim, temos que

$$\begin{aligned}
\sum_{A \in \mathscr{A}} \left(\frac{1}{|U|}\right)^{|H:A|} &= \left(\frac{1}{|U|}\right)^{|H:A_1|} + \left(\frac{1}{|U|}\right)^{|H:A_2|} + \ldots + \left(\frac{1}{|U|}\right)^{|H:A_n|} \\
&= \frac{1}{|U|^{|H:A_1|}} + \frac{1}{|U|^{|H:A_2|}} + \ldots + \frac{1}{|U|^{|H:A_n|}} \\
&\leq \frac{|\mathscr{A}|}{|U|^{|H:A_1|}} \leq \frac{|\mathscr{A}|}{|U|^2} < \frac{|U|}{|U|^2} = \frac{1}{|U|}
\end{aligned}$$

Pelo Teorema 4.1.6, existem elementos não comutadores (em G). $\square$

4.2 Exemplos

Com a utilização do Teorema 4.1.6 e Corolário 4.1.7 podemos obter famílias de grupos nas quais existem pelo menos um elemento não comutador.

4.2.1 Exemplos com H de ordem "baixa"

A seguir desenvolveremos as famílias nas quais considaramos H como sendo um dos grupos no seguinte conjunto $\{S_3\ , D_4, Q_8\}$.

Exemplo 4.2.1. *Consideremos $H = S_3$, temos que os subgrupos abelianos maximais de S_3 são $A_1 = \langle(12)\rangle$, $A_2 = \langle(13)\rangle$, $A_3 = \langle(23)\rangle$ e $A_4 = \langle(123)\rangle$, onde esses subgrupos tem ordem 2,2,2 e 3 respectivamente. Com isso, Tomando $U = C_3$ o grupo cíclico de ordem 3, segue que*

$$\sum_{A\in\mathscr{A}}\left(\frac{1}{|U|}\right)^{|H:A|} = \left(\frac{1}{|U|}\right)^{|H:A_1|} + \left(\frac{1}{|U|}\right)^{|H:A_2|} + \left(\frac{1}{|U|}\right)^{|H:A_3|} + \left(\frac{1}{|U|}\right)^{|H:A_4|}$$
$$= \left(\frac{1}{3}\right)^{3} + \left(\frac{1}{3}\right)^{3} + \left(\frac{1}{3}\right)^{3} + \left(\frac{1}{3}\right)^{2}$$
$$= \frac{1}{27} + \frac{1}{27} + \frac{1}{27} + \frac{1}{9} = \frac{2}{9} < \frac{1}{3} = \frac{1}{|U|}$$

ou seja, as condições do Teorema 4.1.6 são verificadas. Daí, o grupo $G = C_3 \wr S_3$ contém elementos não comutadores.

A partir do Corolário 4.1.7, é possível generalizar o exemplo acima das seguintes formas:

Exemplo 4.2.2. *Tomando $H = S_3$ e U um grupo abeliano com $|U| \geq 4$. Pelo Corolário 4.1.7, o grupo $G = U \wr S_3$ possui elementos não comutadores. Consequentemente, temos uma família (infinita) de grupos $\mathscr{F} = \{C_n \wr S_3 | n \geq 4\}$, cuja ordens são $n^6 \cdot 6$ e tem largura $\lambda(C_n \wr S_3) > 1$, para todo $n \geq 4$.*

Exemplo 4.2.3. *Consideremos $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ o grupo dos quartérnios e U um grupo abeliano com ordem $|U| \geqslant 4$. Temos que o conjunto dos subgrupos maximais de Q_8 são $\mathscr{A} = \{\langle i\rangle, \langle j\rangle, \langle k\rangle\}$. Pelo Corolário 4.1.7 temos que o produto entrelaçado $G = U \wr Q_8$ tem largura $\lambda(G) > 1$.*

Exemplo 4.2.4. *Sejam p, q primos com $q < p$ e H um grupo não abeliano de ordem $p \cdot q$. Se $n > p+1$, então $\lambda(C_n \wr H) > 1$.*

4.2.2 Construindo p-grupos de largura maior do que 1

Aqui construiremos um 2-grupo com elementos não comutadores.

Exemplo 4.2.5. *Tomemos $H = D_4 = \langle a,b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1}\rangle$ o grupo diedral de ordem 8. Repare que, os subgrupos abelianos maximais de H são $\mathscr{A} = \{\langle a\rangle, \langle a^2, ab\rangle, \langle a^2, b\rangle\}$, ou seja, $|\mathscr{A}| = 3$. Com isso, pelo Corolário 4.1.7, considerando $U = C_2 \times C_2$, segue que o grupo $G = (C_2 \times C_2) \wr D_4$ contém elementos não comutadores.*

Podemos construir outros 2-grupos apenas modificando o subgrupo U. Mais, precisamente,

Observação 4.2.6. *Tomemos $U = C_2 \times C_2 \times \ldots \times C_2$ (n vezes) para $n \geqslant 2$ e $H = D_4$. Com isso, pelo Corolário 4.1.7, o produto entrelaçado $G = (C_2 \times C_2 \times \ldots \times C_2) \wr D_4$ contém elementos não comutadores.*

Seja p primo ímpar. Podemos construir p-grupos com largura $\lambda(G) > 1$.

Exemplo 4.2.7. *Sejam p um primo ímpar, H um p-grupo de ordem p^3 não abeliano e $U = C_p \times C_p \times \ldots \times C_p$ (n vezes). Então o número de subgrupos abelianos maximais (de H) é o mesmo número de subgrupos maximais de H e esse número é, exatamente, $p+1$. Assim, o produto entrelaçado $G = U \wr H$ possui elementos não comutadores.*

4.2.3 Construindo grupos não solúveis de largura maior do que 1

Todos os exemplos acima construídos são solúveis. Agora, podemos utilizar o Corolário 4.1.7 para construir famílias de grupo não solúveis com largura $\lambda(G) > 1$.

Exemplo 4.2.8. *Seja H um grupo não solúvel. Consideremos $X = \{K \subseteq H \mid K \leq H\}$, temos que $X \subseteq \mathbb{P}(H)$ o conjunto das partes do grupo H. Ora, como $\mathscr{A} \subseteq X$, segue que $|\mathscr{A}| \leq |X| \leq |\mathbb{P}(H)| = 2^{|H|}$. Assim, tomemos U um grupo abeliano tal que $|U| > 2^{|H|}$. Logo, pelo Corolário 4.1.7, segue que o grupo não solúvel $G = U \wr H$ possui $\lambda(G) > 1$.*

4.3 Grupos nilpotentes de classe 2 de largura infinita

O objetivo dessa seção será obter exemplos de grupos G com largura infinita, e denotaremos por $\lambda(G) = \infty$. Mais precisamente, para cada $n \in \mathbb{N}$ existe um elemento no derivado que não pode ser escrito como o produto de n comutadores.

Mostraremos que para todo corpo $\mathbb{K}$ existirá um grupo $G_{\mathbb{K}}$, tal que $\lambda(G_{\mathbb{K}}) = \infty$. Essa classe de exemplos foi construída pelo matemático P. J. Cassidy (cf. [1]) e para fazer referência, chamaremos tal grupo $G_{\mathbb{K}}$ de grupo de Cassidy.

Consideremos $\mathbb{K}$ um corpo. Seja $\mathbb{K}[x,y]$ o anel dos polinômios em duas variáveis sobre o corpo $\mathbb{K}$. Em $\mathbb{K}[x,y]$, consideremos $\mathbb{K}[x]$, $\mathbb{K}[y]$ os subanéis dos polinômios nas variáveis x e y, respectivamente. Definamos,

$$G_{\mathbb{K}} = \left\{ \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \mid f \in \mathbb{K}[x], g \in \mathbb{K}[y], h \in \mathbb{K}[x,y] \right\}.$$

Com o intuito de simplificar as notações, denotaremos

$$\begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} = M(f,g,h).$$

Como veremos a seguir, tal notação será útil para simplificar os cálculos que efetuaremos.

Lema 4.3.1. *O conjunto $G_{\mathbb{K}}$ munido da operação produto de matrizes é um grupo.*

Demonstração. Dados $f_1, f_2 \in \mathbb{K}[x]$, $g_1, g_2 \in \mathbb{K}[y]$ e $h_1, h_2 \in \mathbb{K}[x,y]$, temos que

$$\begin{aligned} M(f_1,g_1,h_1)M(f_2,g_2,h_2) &= \begin{pmatrix} 1 & f_1 & h_1 \\ 0 & 1 & g_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f_2 & h_2 \\ 0 & 1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & f_1+f_2 & h_1+h_2+f_1g_2 \\ 0 & 1 & g_1+g_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= M(f_1+f_2, g_1+g_2, h_1+h_2+f_1g_2). \end{aligned}$$

O que implica que o conjunto $G_{\mathbb{K}}$ é fechado para a produto de matrizes. Além disso, temos que $1_{G_{\mathbb{K}}} = M(0,0,0) \in G_{\mathbb{K}}$, pois

$$M(0,0,0)M(f,g,h) = M(f,g,h) = M(f,g,h)M(0,0,0)$$

para todo $M(f,g,h) \in G_{\mathbb{K}}$. E também temos que para todo $M(f,g,h) \in G_{\mathbb{K}}$ existe $M(f,g,h,)^{-1} = M(-f,-g,fg-h) \in G_{\mathbb{K}}$, tal que

$$M(f,g,h)M(-f,-g,fg-h) = M(0,0,0)$$

E já que a associatividade é herdada do anel de matrizes, segue que $G_{\mathbb{K}}$ munido da operação produto de matrizes é um grupo. □

Lema 4.3.2. *Seja $\mathbb{K}$ um corpo. Então, $G'_{\mathbb{K}} = Z(G_{\mathbb{K}}) = \{M(0,0,h) \mid h \in \mathbb{K}[x,y]\}$.*

Demonstração. Consideremos $H = \{M(0,0,h) \mid h \in \mathbb{K}[x,y]\}$. Dividiremos esta demonstração em duas partes, onde compararemos $G'_{\mathbb{K}}$ e $Z(G_{\mathbb{K}})$ com H.

1. $Z(G_{\mathbb{K}}) = H$

   Sejam $M(f,g,h)$ e $M(0,0,k) \in G_{\mathbb{K}}$, temos que

   $$M(f,g,h)M(0,0,k) = M(f,g,h+k) = M(0,0,k)M(f,g,h)$$

   ou seja, $M(0,0,k) \in Z(G_{\mathbb{K}})$, e portanto $H \subseteq Z(G_{\mathbb{K}})$.

   Por outro lado, seja $M(f_0,g_0,h_0) \in Z(G_{\mathbb{K}})$, temos que para todo $M(f,g,h)$, segue que

   $$M(f_0,g_0,h_0)M(f,g,h) = M(f,g,h)M(f_0,g_0,h_0)$$

isso implica que

$$M(f_0+f, g_0+g, h_0+h+f_0g) = M(f+f_0, g+g_0, h+h_0+fg_0)$$

Logo, temos que $fg_o = f_0g$, $\forall f \in \mathbb{K}[x]$ *e* $g \in \mathbb{K}[y]$, queremos mostrar que $f_0 = 0 = g_0$. Ora, suponhamos que $f_0 \neq 0$ e peguemos $g \neq 0$ e $f = 0$, assim temos que $0 \neq f_0g = fg_0 = 0$, absurdo. Logo, $f_0 = 0$, e de forma analoga vemos que $g_0 = 0$ o que implica que $M(f_0, g_0, h_0) = M(0, 0, h_0) \in H$ e portanto $Z(G_{\mathbb{K}}) \subseteq H$. Nisto está provado que $H = Z(G_{\mathbb{K}})$.

2. $H = G'_{\mathbb{K}}$

   Vamos mostrar que $G'_{\mathbb{K}} \subseteq H$. O comutador de dois elementos $M(f_1, g_1, h_1), M(f_2, g_2, h_2) \in G_{\mathbb{K}}$ é dado por

$$\begin{aligned}
[M(f_1,g_1,h_1), M(f_2,g_2,h_2)] &= [M(f_1,g_1,)M(0,0,h_1), M(f_2,g_2,0)M(0,0,h_1)] \\
&= [M(f_1,g_1,0), M(f_2,g_2,0)],\ \textit{pois } Z(G_{\mathbb{K}}) \\
&= M(f_1,g_1,0)^{-1}M(f_2,g_2,0)^{-1}M(f_1,g_1,0)M(f_2,g_2,0) \\
&= M(-f_1,-g_1,f_1g_1)M(-f_2,-g_2,f_2g_2)M(f_1,g_1,0)M(f_2,g_2,0) \\
&= M(-f_1-f_2,-g_1-g_2,f_1g_1+f_2g_2+f_1g_2) \\
&\quad .M(f_1+f_2,g_1+g_2,f_1g_2) \\
&= M(0,0,f_1g_1+f_2g_2+f_1g_2+f_1g_2-f_1g_1-f_1g_2-f_2g_1-f_2g_2) \\
&= M(0,0,f_1g_2-f_2g_1)
\end{aligned}$$

Segue por definição de $G'_{\mathbb{K}}$ que

$$\begin{aligned}
G'_{\mathbb{K}} &\leq \langle [M(f_1,g_1,h_1), M(f_2,g_2,h_2)] \mid M(f_1,g_1,h_1), M(f_2,g_2,h_2) \in G_{\mathbb{K}} \rangle \\
&\leq \langle [M(f_1,g_1,0), M(f_2,g_2,0)] \mid M(f_1,g_1,0), M(f_2,g_2,0) \in G_{\mathbb{K}} \rangle \\
&\leq \langle M(0,0,f_1g_2-f_2g_1) \rangle \ \subseteq H
\end{aligned}$$

A outra inclusão é garantida pelo seguinte, se $h = \sum_{i,j} a_{ij}x^iy^j$, então

$$\begin{aligned}
M(0,0,h) &= M(0,0,\sum_{i,j} a_{ij}x^iy^j) = \prod_{i,j} M(0,0,a_{ij}x^iy^j) \\
&= \prod_{i,j} [M(a_{ij}x^i,0,0)M(0,y^j,0)] \subseteq G'_{\mathbb{K}}
\end{aligned}$$

Logo, $H = G'_{\mathbb{K}}$

$\square$

Lema 4.3.3. *O grupo $G_{\mathbb{K}}$ é nilpotente de classe 2.*

Demonstração. Para provarmos que $G_{\mathbb{K}}$ é nilpotente de classe 2, basta mostrarmos que

$$[[M(f_1,g_1,h_1),M(f_2,g_2,h_2)],M(f_3,g_3,h_3)] = 1$$

para todo $M(f_1,g_1,h_1),M(f_2,g_2,h_2),M(f_3,g_3,h_3) \in G_{\mathbb{K}}$

Ora, sejam $M(f_1,g_1,h_1),M(f_2,g_2,h_2),M(f_3,g_3,h_3) \in G_{\mathbb{K}}$, segue que

$$\begin{aligned}
[[M(f_1,g_1,h_1),M(f_2,g_2,h_2)],M(f_3,g_3,h_3)] &= [[M(f_1,g_1,0),M(f_2,g_2,0)],M(f_3,g_3,0)] \\
&= [M(0,0,f_1g_2-f_2g_1),M(f_3,g_3,0)] \\
&= M(0,0,0) = 1_{G_{\mathbb{K}}}
\end{aligned}$$

$\square$

Teorema 4.3.4. *Seja $\mathbb{K}$ um corpo. Então $\lambda(G_{\mathbb{K}}) = \infty$.*

Demonstração. Seja $n \in \mathbb{N}$. Consideremos $h = \sum_{i=0}^{2n} x^i y^{2n-i}$ e $M(0,0,h) \in G_{\mathbb{K}}$. Vamos mostrar que $M(0,0,h)$ não pode ser escrito como produto de n comutadores.

Suponhamos que $M(0,0,h) \in K_n(G_{\mathbb{K}})$, onde $K_n(G_{\mathbb{K}}) = \{M(0,0,k) \in G'_{\mathbb{K}} \mid M(0,0,k) = \prod_{i=1}^{n}[M(f_i,g_i,h_i),M(x_i,y_i,z_i)]\}$. Como $H = Z(G_{\mathbb{K}})$, existem $s_j,u_j \in \mathbb{K}[x]$ e $t_j,v_j \in \mathbb{K}[y]$, com $1 \leq j \leq n$, tal que

$$\begin{aligned}
M(0,0,h) &= \prod_{j=1}^{n}[M(s_j,t_j,0),M(u_j,v_j,0)] \\
&= \prod_{j=1}^{n} M(0,0,s_jv_j - t_ju_j) \\
&= M(0,0,\sum_{j=1}^{n} s_jv_j - t_ju_j)
\end{aligned}$$

Portanto $h = \sum_{j=1}^{n} s_jv_j - t_ju_j$.

Chamemos $s_j = \sum_i a_{ij}x^i$ e $u_j = \sum_i b_{ij}x^i$, onde $a_{ij}, bij \in \mathbb{K}$, e $1 \leq j \leq n$. Por outro lado,

$$\begin{aligned}\sum_{i=0}^{2n} x^i y^{2n-i} &= \sum_{j=1}^{n} (\sum_i a_{ij}x^i)v_j - (\sum_i b_{ij}x^i)t_j \\ &= \sum_{j=1}^{n} \sum_i (a_{ij}v_j - b_{ij}t_j)x^i \\ &= \sum_i \sum_{j=1}^{n} (a_{ij}v_j - b_{ij}t_j)x^i\end{aligned}$$

Com isso,

$$y^{2n-i} = \sum_{j=1}^{n} (a_{ij}v_j - b_{ij}t_j), \; para\ cada\ 0 \leq i \leq 2n$$

Desta forma, o subespaço $\mathbb{V}$ gerado pelo conjunto de polinômios $\{1, y, \ldots, y^{2n}\}$ está contido no subespaço $\mathbb{W}$ gerado pelo conjunto $\{t_1, t_2, \ldots, t_n, v_1, v_2, \ldots, v_n\}$, absurdo, pois teriamos

$$2n + 1 = dim_{\mathbb{K}}(\mathbb{V}) \leq dim_{\mathbb{K}}(\mathbb{W}) = 2n$$

Assim $\forall n \in \mathbb{N}$ existe $M(0, 0, \sum_{i=0}^{2n} x^i y^{2n-i}) \notin K_n(G_{\mathbb{K}})$, portanto, $\lambda(G_{\mathbb{K}}) = \infty$. $\square$

Bibliografia

[1] Cassidy, P. J. (1979). Products of commutators are not always commutators: an example. *The American Mathematical Monthly*, 86(9):772–772.

[2] GAP (2020). *GAP – Groups, Algorithms, and Programming, Version 4.11.0*. The GAP Group.

[3] Gonçalves, A. (1979). *Introdução à álgebra*. Projeto Euclides, Impa.

[4] Guralnick, R. M. (1980). Expressing group elements as commutators. *Rocky Mountain J. Math.*, 10(3):651–654.

[5] Guralnick, R. M. (1982). Commutators and commutator subgroups. *Adv. in Math.*, 45(3):319–330.

[6] Isaacs, I. M. (1977). Commutators and the commutator subgroup. *Amer. Math. Monthly*, 84(9):720–722.

[7] Ore, O. (1951). Some remarks on commutators. *Proc. Amer. Math. Soc.*, 2:307–314.

[8] Robinson, D. J. S. (1996). *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition.

[9] Rocco, N. R. (1997). *Uma breve introdução ao sistema GAP*.

[10] Schneider, C. (2014). *Notas do minicurso: Uma introdução à álgebra computacional com GAP, Escola de Álgebra, Maringá*.

[11] Spiegel, E. (1976). Calculating commutators in groups. *Math. Mag.*, 49(4):192–194.