Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Wállef Januário Pereira da Silva

O Grupo $\nu(G)$ e Aplicações

Brasília, 01 de Março de 2018

Wállef Januário Pereira da Silva

O Grupo $\nu(G)$ e Aplicações

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

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Orientador: Prof. Dr. Raimundo de Araújo Bastos Júnior

Brasília

01 de Março de 2018

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

JW196g

Januário Pereira da Silva, Wállef
O Grupo $\nu(G)$ e Aplicações / Wállef Januário Pereira da Silva; orientador Raimundo de Araújo Bastos Júnior. -- Brasília, 2018.
84 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2018.

1. Grupos Finitos. 2. Condição de Finitude. 3. Quadrado Tensorial Não Abeliano de Grupos. I. de Araújo Bastos Júnior, Raimundo, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

O Grupo $\nu(G)$ e Aplicações

por

Wállef Januário Pereira da Silva*

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

MESTRE EM MATEMÁTICA

Brasília, 01 de março de 2018.

Comissão Examinadora:

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

Prof. Dr. Emerson Ferreira de Melo– MAT/UnB (Membro)

Prof. Dr. José Robério Rogério - UFC (Membro)

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

À Deus, fonte de toda sabedoria.
À família e amigos, base de toda felicidade.

Agradecimentos

"A gratidão é a virtude das almas nobres." - Esopo

Em uma palavra desejo expressar o amor, a paciência, o estresse, a perseverança, a raiva, a angústia, o desespero, o esforço, e demais sentimentos que me envolveram durante esses dois anos de mestrado.

Em primeiro lugar, quero agradecer ao meu Deus que esteve comigo em todos os momentos; que nas horas difíceis me ofereceu sua mão poderosa e seu Espírito consolador; que não me deixou desistir quando o desânimo me sufocou. Ao meu melhor amigo: Muito Obrigado!

Agradeço aos meus familiares pelo apoio de sempre. Em especial, aos meus pais João e Ivone; aos meus irmãos, Wellington, Williams e Jéssica; aos meus primos Silvio e Suelen. A ajuda de vocês foi essencial e determinante para essa conquista.

Agradeço aos meus colegas de curso, que com seus sorrisos e ombro amigo proporcionaram a cada dia uma alegria e paz diferente, um motivo para continuar. Em especial, agradeço ao Alancoc Alencar, que durante pouco mais de um ano suportou minhas diferenças ao dividir apartamento comigo. Aos demais colegas, Filipe Kelmer, Felipe Quintino, Wilson Murillo (Messi), Fabian Muñoz, Nathália Gonçalves, Marta Lizeth, Guillermo Villanueva, Welinton Gimarez, Alex Barros e todos os outros, levarei vocês em meu coração por toda a vida...

Agradeço aos professores Noraí Rocco, Luiz Miranda, Emerson Melo, Pedro Roitman, Ary Medino, por seu papel fundamental na minha formação acadêmica. Ao meu orientador Raimundo Bastos, pela pessoa bastante singular e agradável que é. Pela sua paciência, seus conselhos, ..., por sua ajuda para que eu chegasse até aqui. Aos professores Raimundo Bastos, José Robério e Emerson de Melo, pelas sugestões e correções para melhoria deste trabalho.

Aos meus professores de graduação. Em especial, Andreia Ribeiro e Tatiana Bertoldi, por sua torcida e conselhos.

Aos irmãos da igreja, por sua companhia e orações. Em especial, à Sarah Cirino e família, Hugo Robert e família, Daniel Guilardi e família, Nilton Cardoso e família, Marilene Paulino e família. Vocês foram essenciais!

Agradeço ao CNPq, pelo apoio financeiro.

Aos que estiveram na retaguarda, gritando bem baixinho: “Siga em frente!”, eu agradeço! Não somente com um obrigado momentâneo, mas com uma lembrança eterna em meu coração.

Mais uma vez, Obrigado!

"De onde, pois, vem a sabedoria, e onde está o lugar da inteligência?
Porque está encoberta aos olhos de todo vivente e oculta às aves do céu.
A perdição e a morte dizem: Ouvimos com os nossos ouvidos a sua fama.
Deus entende o seu caminho, e ele sabe o seu lugar.
Porque ele vê as extremidades da terra; e vê tudo o que há debaixo dos céus.
Quando deu peso ao vento e tomou a medida das águas;
quando prescreveu uma lei para a chuva
e caminho para o relâmpago dos trovões, então, a viu e a manifestou;
estabeleceu-a e também a esquadrinhou.
Mas disse ao homem:
- Eis que o temor do Senhor é a sabedoria, e apartar-se do mal é a inteligência."

Bíblia Sagrada, Jó 28, 20-28.

Resumo

Neste trabalho estudamos uma construção relacionada ao quadrado tensorial não abeliano de grupos ($G \otimes G$), a saber o grupo $\nu(G)$. Tal relação acontece pois $\nu(G)$ possui um subgrupo normal $[G, G^{\varphi}]$ isomorfo ao grupo $G \otimes G$. Além disso, olhando ν como operador na classe de grupos, apresentamos resultados que garantem que se G for nilpotente, ou solúvel, ou finito, então $\nu(G)$ também é nilpotente, ou solúvel, ou finito, respectivamente. Em particular, apresentamos aqui uma nova demonstração para a finitude de $\nu(G)$, quando G é finito. Usando técnicas semelhantes, também apresentamos uma demonstração para o caso em que G é localmente finito (ou π-grupo localmente finito), obtendo que $\nu(G)$ é localmente finito (ou π-grupo localmente finito), respectivamente.

Palavras-chave: 1) Grupos Finitos 2) Condição de Finitude 3) Quadrado Tensorial Não Abeliano de Grupos.

Abstract

In this work we study a construction related to the non-abelian tensor square of groups ($G \otimes G$), namely group $\nu(G)$. This relationship happens because $\nu(G)$ has a normal subgroup $[G, G^{\varphi}]$ isomorphic to group $G \otimes G$. In addition, looking at ν as operator in the class of groups, we present results that guarantee that if G is nilpotent, or soluble, or finite, then $\nu(G)$ is also nilpotent, or soluble, or finite, respectively. In special, we present here a new proof for the finiteness of $\nu(G)$, when G is finite. Using similar techniques, we present here a demonstration for the case where G is locally finite (or locally finite π-group), obtaining that $\nu(G)$ is locally finite (or locally finite π-group), respectively.

Keywords: 1) Finite Groups 2) Finiteness Conditions 3) Non-abelian Tensor Square of Groups.

Sumário

Lista de símbolos

$G, X, \cdots$	Conjunto, Grupo, Anel, etc.
$\alpha, \beta, f, \cdots$	Aplicações
$x, y, z, \cdots$	Elementos de um conjunto
$1, 1_G$	Elemento identidade de um grupo G
$\sigma(x)$, x^σ	Imagem de x por meio da aplicação σ
x^y	$y^{-1}xy$
$[x, y]$	$x^{-1}x^y$
$G \simeq H$	G é isomorfo a H
$H \leq G$	H é subgrupo do grupo G
$H < G$	H é subgrupo próprio de G
$H \trianglelefteq G$	H é subgrupo normal do grupo G
$\langle X \rangle$	Subgrupo gerado por X
$\langle X \mid R \rangle$	Grupo apresentado por geradores X e relatores R
G^n	Subgrupo gerado pelas n-ésimas potências de $g \in G$
$\|X\|$	Cardinalidade do conjunto X
$(G : H)$	Índice do subgrupo H em G
$o(g)$	Ordem do elemento g de um dado grupo G
H^G	Fecho normal de H em G
$G \oplus H$	Soma direta

$G \times H$	Produto cartesiano, produto direto
$N \rtimes H$	Produto semidireto de N por H
$G * H$	Produto livre
$G \otimes H$	Produto Tensorial
G'	Subgrupo derivado de G
G_{ab}	Quociente de G por G'
$G^{(i)}$	i-ésimo termo da série derivada de G
$\gamma_i(G)$	i-ésimo termo da série central inferior de G
$Z_i(G)$	i-ésimo termo da série central superior de G
$Z(G)$	Centro do grupo G
$\Phi(G)$	Frattini do grupo G
$\exp(G)$	Expoente de G
$G \twoheadrightarrow H$	Epimorfismo de G em H
id_G	Homomorfismo identidade de G em G
$C_n, \mathbb{Z}_n$	Grupo cíclico de ordem n

Introdução

Neste trabalho temos como objetivo estudar o artigo de N. Rocco *"On a Construction Related to the Non-abelian Tensor Square of a Group"* [21], e outros resultados relacionados. O assunto proposto neste artigo tem ínicio com a seguinte definição: sejam G e H grupos que agem um sobre o outro (à direita) e sobre si mesmos por conjugação. Nessas condições, dizemos que as ações

$$\begin{array}{rccc} \phi_1: & G \times H & \longrightarrow & G \\ & (g,h) & \longmapsto & \phi_1(g,h) = g^h \end{array} \quad , \quad \begin{array}{rccc} \phi_2: & H \times G & \longrightarrow & H \\ & (h,g) & \longmapsto & \phi_2(h,g) = h^g \end{array}$$

são *compatíveis* se satisfazerem

$$g^{\phi_2(h,g_1)} = g^{(h^{g_1})} = \left((g^{g_1^{-1}})^h\right)^{g_1} \quad e \quad h^{\phi_1(g,h_1)} = h^{(g^{h_1})} = \left((h^{h_1^{-1}})^g\right)^{h_1}, \tag{1}$$

para quaisquer que sejam $g, g_1 \in G,\ h, h_1 \in H$. Quando G e H agem um sobre o outro compativelmente, então o *produto tensorial não abeliano de G e H*, denotado por $G \otimes H$, é definido como sendo o grupo gerado pelos símbolos $g \otimes h$, para todos $g \in G, h \in H$, com as relações

$$gg_1 \otimes h = (g^{g_1} \otimes h^{g_1})(g_1 \otimes h), \quad g \otimes hh_1 = (g \otimes h_1)(g^{h_1} \otimes h^{h_1}),$$

para todos $g, g_1 \in G, h, h_1 \in H$. Como a ação por conjugação de G em si mesmo sempre é compatível, o *quadrado tensorial não abeliano de G*, denotado por $G \otimes G$, sempre poderá ser definido.

O produto tensorial não abeliano de grupos $G \otimes H$ foi introduzido por R. Brown e J. Loday em [8], generalizando o produto tensorial de $\mathbb{Z}$-módulos usual $G_{ab} \otimes_{\mathbb{Z}} H_{ab}$ de grupos abelianizados [8, Proposição 2.4]. Alguns casos especiais do produto tensorial já tinham aparecido em trabalhos anteriores, por exemplo, em [10], [16] e [26]. Por outro lado, devido a sua importância topológica, diversas pessoas começaram a estudar propriedades estruturais relacionadas à tais construções no contexto intrínseco de Teoria dos Grupos, por exemplo,

Proposição 1 [7, Proposição 5] *Se G é um grupo finito, então $G \otimes G$ é finito. Se, além disso, G é um p-grupo para algum primo p, então $G \otimes G$ é um p-grupo finito.*

Cabe mencionar também os seguintes trabalhos: [1], [2], [3], [5], [7], [13], [18] e [22].

Com o objetivo de estudar o quadrado tensorial não abeliano de um grupo G, N. Rocco introduziu, em [21], o grupo

$$\nu(G) := \langle G \cup G^{\varphi} \mid [g_1, g_2^{\varphi}]^{g_3} = [g_1^{g_3}, (g_2^{g_3})^{\varphi}] = [g_1, g_2^{\varphi}]^{g_3^{\varphi}}, \forall\, g_1, g_2, g_3 \in G \rangle,$$

como um quociente do produto livre $G * G^{\varphi}$, considerando dois grupos G e G^{φ}, onde G^{φ} é a imagem isomórfica de G através de um isomorfismo de grupos φ. Mais ainda, olhando ν como operador na classe de grupos, N. Rocco demonstrou que ele preserva propriedades do argumento G, tais como finitude, solubilidade, nilpotência e, para um grupo G finito, ν também preserva o conjunto de divisores primos da ordem de G. Nesse contexto, N. Rocco mostrou que existe um isomorfismo entre o grupo $G \otimes G$ e o subgrupo $[G, G^{\varphi}] \trianglelefteq \nu(G)$,

Proposição 2 [21, Proposição 2.6] *Seja G um grupo. Então, o quadrado tensorial $G \otimes G$ é isomorfo a $[G, G^{\varphi}]$. Mais ainda, a função*

$$\begin{array}{rccc} \tau: & G \otimes G & \longrightarrow & [G, G^{\varphi}] \\ & g_1 \otimes g_2 & \longmapsto & [g_1, g_2^{\varphi}] \end{array}$$

é um isomorfismo de grupos.

Este isomorfismo proporciona conhecer propriedades do quadrado tensorial não abeliano $G \otimes G$ por meio de cálculos de comutadores em $\nu(G)$, trazendo várias vantagens computacionais. Usando uma descrição do grupo $\nu(G)$, em [21], foi descrito as séries central inferior e derivada do grupo $\nu(G)$, a saber

Teorema 1 [21, Teorema 3.1] *Para $i \geq 2$ o i-ésimo termo da série central inferior de $\nu(G)$ é dado por*

$$\gamma_i(\nu(G)) = \gamma_i(G)\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G].$$

Teorema 2 [21, Teorema 3.3] *Para $i \geq 2$ o i-ésimo termo da série derivada de $\nu(G)$ é dado por*

$$\nu(G)_i = G_i G_i^{\varphi}[G_{i-1}, G_{i-1}^{\varphi}],$$

onde G_i denota o i-ésimo termo da série derivada de G.

Como corolários imediatos, foi demonstrado que, quando G for nilpotente de classe l, então $\nu(G)$ é nilpotente de classe no máximo $l+1$ [21, Corolário 3.2], e quando G for solúvel de comprimento derivado n, então $\nu(G)$ é solúvel de comprimento derivado no máximo $n+1$ [21, Corolário 3.4]. Dentre os resultados sobre a influência da estrutura do grupo G, foi dada uma descrição dos grupos $\nu(G)$ e $[G, G^{\varphi}]$ quando G é um produto semidireto:

Proposição 3 [21, Proposição 3.5] *Sejam G um grupo, $N \trianglelefteq G$ e $H \leq G$. Suponhamos que $G = N \rtimes H$ é um produto semidireto. Então,*
(i) $\nu(G) = \langle N, N^\varphi\rangle[N, H^\varphi][H, N^\varphi] \rtimes \langle H, H^\varphi\rangle$;
(ii) $\langle H, H^\varphi\rangle \simeq \nu(H)$.

Para mostrar a finitude do grupo $\nu(G)$, em [21], o autor utiliza resultados já conhecidos do grupo

$$\chi(G) := \langle G \cup G^\varphi \mid [g, g^\varphi] = 1, \text{ para todo } g \in G\rangle,$$

introduzido por S. Sidki em [25]. Entretanto, mais recentemente, N. Rocco sugeriu uma demonstração alternativa para este resultado, a qual apresentaremos aqui. Tal demonstração usa propriedades grupo teóricas e apenas a estrutura do grupo $\nu(G)$. A saber,

Teorema 3 *Sejam π um conjunto de primos e G um grupo. Se G é finito (ou π-grupo finito), então o quadrado tensorial não abeliano $[G, G^\varphi]$ é finito (ou π-grupo finito), respectivamente. Em particular, $\nu(G)$ é finito (π-grupo finito).*

Resultados semelhantes também são encontrados para o grupo $\chi(G)$ em [25].

Para finalizar, considerando G como sendo um p-grupo finito, N. Rocco conseguiu uma estimativa para a ordem de $G \otimes G$,

Corolário 1 [21, Corolário 3.12] *Sejam G um p-grupo finito, com $|G| = p^n$, $|G'| = p^m$, e d o número minimal de geradores de G. Então,*

$$p^{d^2} \leq |G \otimes G| \leq p^{n(n-m)}.$$

Além disso, tomando G como um grupo localmente finito (ou π-grupo localmente finito), usando ideias semelhantes às usadas para demonstrar o Teorema 3, N. Rocco sugeriu uma demonstração para mostrar que o grupo $\nu(G)$ também é localmente finito (ou π-grupo localmente finito), com π sendo um conjunto de primos, e tal demonstração é apresentada aqui. A saber,

Teorema 4 *Seja G um grupo localmente finito (ou π-grupo localmente finito). Então, $\nu(G)$ é localmente finito (ou π-grupo localmente finito), respectivamente.*

Este trabalho está dividido em três capítulos:

No capítulo 1, fizemos uma relação das principais definições que permeiam o tema deste trabalho. Alguns resultados e suas demonstrações também foram expostos. Neste capítulo, falamos de Grupos Nilpotentes e Solúveis, Homomorfismo Transfer e o Teorema de Schur, Grupos Livres e Apresentação de Grupos, Produto Livre de Grupos, Produto Tensorial de R-módulos e fizemos um breve apanhado de propriedades sobre o Produto Tensorial Não Abeliano de Grupos, encontradas em [7] e [8].

No capítulo 2, expomos os resultados encontrados no artigo [21], em particular, propriedades computacionais; descrições da estrutura de $\nu(G)$ para G sendo um produto direto, semidireto e nilpotente finito; a existência do isomorfismo entre $G \otimes G$ e $[G, G^{\varphi}]$, etc.

No capítulo 3, foi dada a atenção para o grupo $\nu(G)$ quando G é finito, π-grupo finito, e localmente finito (ou π-grupo localmente finito). Apresentamos uma demonstração para os Teoremas 3 e 4 citados anteriormente e apresentamos os demais resultados encontrados em [21] relacionados à ordem de $\nu(G)$ e $[G, G^{\varphi}]$.

Capítulo 1

Preliminares

Dedicamos este capítulo para apresentar ao leitor os conceitos necessários para o desenvolvimento deste trabalho. Usaremos a notação G para denotarmos um grupo, $Z(G)$ para o centro do grupo G, 1_G para o elemento neutro do grupo G, ou apenas 1, caso não haja possibilidade de confusão. Demais notações e definições elementares serão consideradas familiares ao leitor e, portanto, serão omitidas.

Observamos ainda que, em algumas demonstrações, incluiremos nas igualdades (desigualdades) referências de resultados anteriores a fim de facilitar o entendimento do raciocínio exposto. Para uma leitura mais detalhada sobre os assuntos aqui citados recomendamos [7], [8], [14], [15], [20] e [24].

1.1 Grupos Nilpotentes e Solúveis

O objetivo desta seção é introduzir os conceitos de grupo solúvel, grupo nilpotente e algumas propriedades relacionadas, assim como, as séries centrais e derivada de um grupo G qualquer. Além disso, apresentaremos o subgrupo de Frattini de um grupo G e o Teorema da Base de Burnside. A referência usada para esta seção foi [20].

Definição 1.1.1 *Um grupo G é dito ser **solúvel** se possuir uma série abeliana, isto é, uma série*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

em que cada quociente $\frac{G_{i+1}}{G_i}$ é abeliano para todo $i = 0, 1, \cdots, n-1$.

Naturalmente, todo grupo abeliano é solúvel, e o grupo simétrico

$$S_3 = \langle a, b \mid a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$$

é não abeliano e solúvel.

Definição 1.1.2 *Seja G um grupo. Dizemos que G é uma **extensão** de um grupo N por um grupo Q, se existe um subgrupo $M \trianglelefteq G$ tal que $N \simeq M$ e $\frac{G}{M} \simeq Q$.*

Proposição 1.1.1 [20, Proposição 5.2.1] *A classe de grupos solúveis é fechada para formação de subgrupos, imagens homomórficas e extensões.*

Definição 1.1.3 *Um grupo G é chamado **nilpotente** se possuir uma série central, ou seja, uma série normal*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

tal que cada quociente $\frac{G_{i+1}}{G_i}$ está no centro de $\frac{G}{G_i}$ para todo $i = 0, 1, \cdots, n-1$.

O comprimento da menor série abeliana de um grupo G solúvel é chamado de *comprimento derivado* de G. O comprimento da menor série central de um grupo H nilpotente é chamado de *classe de nilpotência* de H. Um grupo G tem comprimento derivado (ou classe de nilpotência) $l = 0$ se, e somente se, ele tiver ordem 1. Caso $l \leq 1$, então G é um grupo *abeliano*. Um grupo nilpotente é sempre solúvel, enquanto o grupo simétrico S_3 é um grupo solúvel não nilpotente.

Proposição 1.1.2 [20, Proposição 5.1.4] *A classe de grupos nilpotentes é fechada para formação de subgrupos, imagens homomórficas e produto direto finito.*

A classe de grupos nilpotentes não é fechada para extensões, pois o grupo simétrico S_3 é uma extensão de seus subgrupos $\langle a \rangle$ por $\langle b \rangle$, que são cíclicos de ordens 3 e 2, respectivamente. Mas, S_3 não é nilpotente, pois tem centro trivial.

Definição 1.1.4 *Sejam G um grupo e π um conjunto não vazio de números primos. Um π**-número** é um inteiro positivo tal que todos os seus divisores primos pertencem ao conjunto π. Um elemento de G é chamado π**-elemento** se sua ordem é um π-número. Caso todo elemento de G seja um π-elemento, então dizemos que G é um π**-grupo**.*

Quando $\pi = \{p\}$, para algum primo p, e G é um π-grupo, é comum chamar G de p-grupo. Os p-subgrupos de Sylow de um grupo G finito, são exemplos de p-grupos (veja [23, cap. 4]).

Proposição 1.1.3 [20, Proposição 5.1.3] *Seja G um p-grupo finito. Então, G é nilpotente.*

Demonstração: A demonstração é feita por indução na ordem de G. Então, se $|G| = 2$ o resultado segue trivialmente. Agora, suponhamos que todo p-grupo com ordem menor que a ordem de G seja nilpotente. Então, como G é p-grupo, seu centro é não trivial. Logo, o grupo $\frac{G}{Z(G)}$ é um p-grupo com ordem menor que a ordem de G. Pela hipótese de indução, $\frac{G}{Z(G)}$ é nilpotente e possui uma série central

$$\frac{Z(G)}{Z(G)} = \frac{H_0}{Z(G)} \leq \frac{H_1}{Z(G)} \leq \frac{H_2}{Z(G)} \leq \cdots \leq \frac{H_n}{Z(G)} = \frac{G}{Z(G)}.$$

Então, pelo Teorema da Correspondência, existe uma série normal de G

$$1 \trianglelefteq H_0 = Z(G) \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

que também é central, pois para todo $i = 0, 1, 2, \cdots, n-1$,

$$\frac{H_{i+1}}{H_i} \simeq \frac{\frac{H_{i+1}}{Z(G)}}{\frac{H_i}{Z(G)}} \leq Z\left(\frac{\frac{G}{Z(G)}}{\frac{H_i}{Z(G)}}\right) \simeq Z\left(\frac{G}{H_i}\right).$$

Portanto, G é um grupo nilpotente. ■

1.2 Comutadores e Séries Centrais

Para $x, y, z \in G$, o *conjugado* de x por y é denotado por $x^y := y^{-1}xy$; o *comutador* de x e y, nesta ordem, é denotado por $[x, y] := x^{-1}x^y$, e nossos comutadores são calculados à esquerda, isto é, $[x, y, z] := [[x, y], z]$. Com isso, valem as seguintes propriedades:

Proposição 1.2.1 [20, Proposição 5.1.5] *Sejam G um grupo e $x, y, z \in G$. Então,*
(i) $[x, y]^{-1} = [y, x]$;
(ii) $[x, y] = [x, y^{-1}]^{-y} = [x^{-1}, y]^{-x}$, *onde* $[x, y]^{-c} := ([x, y]^c)^{-1}$, *para todo* $c \in G$;
(iii) $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$;
(iv) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$;
(v) (Identidade de Hall-Witt) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

Se H e K são subconjuntos não vazios de um grupo G, então o comutador de H por K é definido como sendo o subgrupo

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

observando que, pelo item (i) da proposição anterior, $[H, K] = [K, H]$. Mais geralmente, para $n \geq 2$, temos

$$[H_1, H_2, \cdots, H_n] := [[H_1, H_2, \cdots, H_{n-1}], H_n].$$

Quando $G = K = H$, dizemos que $[G, G] := G'$ é o *subgrupo derivado* de G. Analogamente ao conjugado de um elemento, introduzimos

$$H^K := \langle k^{-1}hk \mid h \in H, k \in K \rangle. \tag{1.1}$$

Proposição 1.2.2 [20, Proposição 5.1.6 e 5.1.7] *Sejam G um grupo, X um subconjunto e K um subgrupo de G. Se $K = \langle Y \rangle$, então $[X, K] = [X, Y]^K$. Em particular, se $H = \langle X \rangle$ é um subgrupo de G, então*

$$[H, K] = [X, Y]^{HK}.$$

Lema 1.2.1 [20, Teorema 5.2.8] *Se H, K e L são subgrupos normais de um grupo G, então*

$$[HK, L] = [H, L][K, L].$$

Definição 1.2.1 *Sejam G um grupo e $G' := [G, G]$ o subgrupo derivado de G. A série*

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} \geq \cdots$$

onde $G^{(n+1)} = (G^{(n)})'$ para todo $n \in \mathbb{N}$, é chamada de ***série derivada*** *de G.*

A série derivada de um grupo G pode não chegar até ao subgrupo trivial $\{1\}$, a não ser que o grupo seja solúvel, como mostra o próximo resultado. Na série derivada, cada quociente $\frac{G^{(n)}}{G^{(n+1)}}$ é abeliano e o primeiro deles, $\frac{G}{G'}$, é também denotado por G_{ab}.

Observação 1.1 Com o intuito de simplificar a notação acima para a série derivada de um grupo G, podemos escrever $G^{(i)} = G_{i+1}$, $i = 0, 1, 2, \cdots$. Esta notação será usada apenas na seção 2.3.

Proposição 1.2.3 [20, Proposição 5.1.8] *Seja G um grupo solúvel, com série abeliana*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

Então, $G^{(i)} \leq G_{n-i}$, para $i = 0, 1, \cdots, n$. Em particular, $G^{(n)} = 1$, isto é, o comprimento derivado de G é igual ao comprimento da série derivada de G.

Demonstração: Demonstraremos por indução em i. Logo, para $i = 0$, segue trivialmente. Suponhamos que para algum $i > 0$ tenhamos $G^{(i)} \leq G_{n-i}$. Então, como $\frac{G_{i+1}}{G_i}$ é abeliano para todo $i = 0, 1, \cdots, n-1$, segue que

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_{n-i}, G_{n-i}] \leq G_{n-i-1},$$

como queríamos. ∎

Definição 1.2.2 *Seja G um grupo. A série*

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

onde $\gamma_{n+1}(G) = [\gamma_n(G), G]$ para todo $n \in \mathbb{N}$, é chamada de ***série central inferior*** *de G.*

Uma consequência da definição $\gamma_{n+1}(G) = [\gamma_n(G), G]$, $n \in \mathbb{N}$, é que

$$\frac{\gamma_n(G)}{\gamma_{n+1}(G)} \leq Z\Big(\frac{G}{\gamma_{n+1}(G)}\Big),$$

onde $Z\Big(\frac{G}{\gamma_{n+1}(G)}\Big)$ é o centro do grupo $\frac{G}{\gamma_{n+1}(G)}$. Observe também que o primeiro termo da série derivada de G é $G^{(0)}$, enquanto o primeiro termo da série central inferior de G é $\gamma_1(G)$.

Definição 1.2.3 *Seja G um grupo. O* i***-ésimo centro*** *de G, denotado por $Z_i(G)$, é um subgrupo característico de G definido indutivamente como sendo a imagem inversa do centro de $\frac{G}{Z_{i-1}(G)}$ sob o homomorfismo canônico*

$$\begin{aligned} \psi_i : \quad G &\longrightarrow \frac{G}{Z_{i-1}(G)} \\ x &\longmapsto Z_{i-1}(G)x, \end{aligned}$$

para todo $i = 1, 2, \cdots$. Por convenção, $Z_0(G) = \{1\}$.

Definição 1.2.4 *A* ***série central superior*** *de um grupo G qualquer é a série*

$$\{1\} = Z_0(G) \leq Z_1(G) = Z(G) \leq \cdots \leq Z_i(G) \leq \cdots,$$

para todo $i \in \mathbb{N}$.

Assim como a série derivada, a série central inferior de um grupo G pode não chegar ao subgrupo trivial $\{1\}$ do grupo G. Também, a série central superior pode não chegar no grupo G. Um grupo que satisfaz todas essas afirmações é o grupo simétrico S_n, para todo $n \geq 5$. Porém, quando G é nilpotente, as séries centrais inferior e superior chegam na unidade do grupo e no grupo G, respectivamente, como mostra o resultado a seguir:

Proposição 1.2.4 [20, Proposição 5.1.9] *Seja*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

uma série central de um grupo G nilpotente. Temos as seguintes propriedades:
(i) $\gamma_j(G) \leq G_{n-j+1}$, para todo $j \geq 1$. Em particular, $\gamma_{n+1}(G) = \{1\}$;
(ii) $G_j \leq Z_j(G)$, com $j \geq 0$. Em particular, $Z_n(G) = G$;
(iii) se n é a classe de nilpotência de G, r é o comprimento da série central superior de G, e s é o comprimento da série central inferior de G, então $n = r = s$.

Demonstração: Nos itens (i) e (ii) a demonstração se faz por indução em j.
(i) O caso $j = 1$ segue trivialmente. Para algum $j > 1$, suponhamos que

$$\gamma_j(G) \leq G_{n-j+1}. \tag{1.2}$$

Dado que cada quociente $\frac{G_{i+1}}{G_i}$ está no centro de $\frac{G}{G_i}$, temos que $[G_{i+1}, G] \leq G_i$ para todo $i = 0, 1, \cdots, n-1$, e consequentemente,

$$\gamma_{j+1}(G) = [\gamma_j(G), G] \overset{(1.2)}{\leq} [G_{n-j+1}, G] \leq G_{n-j},$$

para todo j, como queríamos demonstrar.
(ii) O caso $j = 0$ segue trivialmente. Suponhamos para $j > 0$ que

$$G_j \leq Z_j(G). \tag{1.3}$$

Então, como cada quociente $\frac{G_{j+1}}{G_j}$ está no centro de $\frac{G}{G_j}$ para todo $j = 0, 1, \cdots, n-1$, temos que

$$[G_{j+1}, G] \leq G_j \overset{(1.3)}{\leq} Z_j(G).$$

Em particular,

$$G_{j+1} \leq Z_{j+1}(G).$$

Como queríamos demonstrar.
(iii) O item (iii) segue diretamente dos itens (i) e (ii). ■

A seguir veremos uma propriedade que relaciona as séries centrais de um grupo G.

Lema 1.2.2 [20, Lema 5.1.10, Proposição 5.1.11] *Sejam G um grupo qualquer, m e n inteiros positivos. Então,*
(i)(Lema dos Três Subgrupos) se H, K e L são subgrupos de G tais que dois dos subgrupos de comutadores

$$[H, K, L], [K, L, H], [L, H, K]$$

estão contidos em um subgrupo normal de G, então o terceiro também está.
(ii) $[\gamma_m(G), Z_n(G)] \leq Z_{n-m}(G)$, se $n \geq m$.

Demonstração: (i) Pela Proposição 1.2.2, para quaisquer $h \in H, k \in K, l \in L$, temos que

$$[H, K, L] = \langle [h, k^{-1}, l]^{x_1 l_1} \mid x_1 \in [H, K], l_1 \in L \rangle,$$

$$[K, L, H] = \langle [k, l^{-1}, h]^{x_2 h_1} \mid x_2 \in [K, L], h_1 \in H \rangle,$$

$$[L, H, K] = \langle [l, h^{-1}, k]^{x_3 k_1} \mid x_3 \in [H, K], k_1 \in L \rangle.$$

Suponhamos que

$$[K, L, H], [L, H, K] \subseteq N \trianglelefteq G.$$

Então, pela identidade de Hall-Witt,

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

Portanto,

$$[h, k^{-1}, l]^k = ([l, h^{-1}, k]^h)^{-1} \cdot ([k, l^{-1}, h]^l)^{-1} \in N.$$

Daí, pela normalidade de N, segue que $[H, K, L] \subseteq N$, como queríamos.
(ii) Para todo natural n fixado, iremos mostrar por indução em m, com $m \leq n$, que o resultado é válido. Assim, para $m = 1$, temos

$$[\gamma_1(G), Z_n(G)] = [G, Z_n(G)] \leq Z_{n-1}(G).$$

Considerando para algum m, com $1 < m < n$, que

$$[\gamma_m(G), Z_n(G)] \leq Z_{n-m}(G). \tag{1.4}$$

Pelo Lema dos Três Subgrupos podemos afirmar que

$$[\gamma_m(G), G, Z_n(G)] \leq [G, Z_n(G), \gamma_m(G)][Z_n(G), \gamma_m(G), G]. \tag{1.5}$$

Além disso, como

$$[G, Z_n(G), \gamma_m(G)] \leq [Z_{n-1}(G), \gamma_m(G)] \leq [Z_n(G), \gamma_m(G)] \overset{(1.4)}{\leq} Z_{n-m-1}(G),$$

$$[Z_n(G), \gamma_m(G), G] \overset{(1.4)}{\leq} [Z_{n-m}(G), G] \leq Z_{n-m-1}(G).$$

Consequentemente, por (1.5), temos

$$[\gamma_{m+1}(G), Z_n(G)] = [\gamma_m(G), G, Z_n(G)] \leq Z_{n-m-1}(G).$$

Portanto, a afirmação é verdadeira para todo $1 \leq m \leq n$, com $n \in \mathbb{N}$. ■

Proposição 1.2.5 [20, Lema 5.2.1] *Seja G um grupo nilpotente e $\{1\} \neq N \trianglelefteq G$. Então, $N \cap Z(G) \neq \{1\}$.*

Demonstração: Dado que G é nilpotente de classe c, existe um menor inteiro i tal que $N \cap Z_i(G) \neq \{1\}$. Mas, pela escolha sobre i,

$$[N \cap Z_i(G), G] \leq N \cap Z_{i-1}(G) = \{1\}.$$

Logo, $N \cap Z_i(G) \leq N \cap Z(G)$. Daí $N \cap Z(G) \neq \{1\}$, como queríamos. ■

Definição 1.2.5 *Sejam G um grupo e M um subgrupo próprio de G. Dizemos que M é um **subgrupo maximal** de G se não existir subgrupo L tal que $M < L < G$.*

A seguir, temos algumas caracterizações de grupos nilpotentes finitos.

Teorema 1.2.1 [20, Teorema 5.2.4] *Seja G um grupo finito. Então, as seguintes propriedades são equivalentes:*
(i) G é nilpotente;
(ii) Todo subgrupo maximal de G é normal;
(iii) G é o produto direto de seus subgrupos de Sylow.

Corolário 1.2.1 *Seja G um grupo nilpotente finito. Então, quaisquer dois elementos de ordens coprimas comutam.*

Demonstração: Seja

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

onde cada p_i é um número primo com $p_i \neq p_j$ sempre que $i \neq j$ e $\alpha_i \in \mathbb{N}$, $i = 1, 2, \cdots, n$. Dado que G é nilpotente, então pelo teorema anterior G é um produto direto de seus p_i-subgrupos de Sylow para $i = 1, 2, \cdots, n$. Portanto, se $a, b \in G$, temos que $a = a_1 a_2 \cdots a_n$ e

$b = b_1 b_2 \cdots b_n$, onde cada a_i, b_i são elementos de um p_i-subgrupo de Sylow de G. Denotando as ordens de a e b por $o(a)$ e $o(b)$, respectivamente, suponhamos que $mdc(o(a), o(b)) = 1$. Como $o(a) = mmc(o(a_1), o(a_2), \cdots, o(a_n))$ e $o(b) = mmc(o(b_1), o(b_2), \cdots, o(b_n))$, então se algum $a_i \neq 1$ para algum i, então p_i divide $o(a)$, consequentemente, p_i não divide $o(b)$ e $b_i = 1$. Analogamente, se $b_j \neq 1$, então $a_j = 1$ para algum j. Portanto, $G = Q_1 \times Q_2$ onde $a \in Q_1$ e $b \in Q_2$. Em particular, $ab = ba$. ■

Definição 1.2.6 *Seja G um grupo. O* ***subgrupo de Frattini*** *de G, denotado por $\Phi(G)$, é a interseção de todos os subgrupos maximais de G. Quando G não tem subgrupos maximais, então o Frattini de G é o próprio G.*

Definição 1.2.7 *Seja G um grupo. Dizemos que um elemento $g \in G$ é um* ***elemento não gerador*** *de G, quando $G = \langle g, X \rangle$ implicar que $G = \langle X \rangle$, onde X é um subconjunto de G.*

Lema 1.2.3 (G. Frattini) [20, Teorema 5.2.12] *Em qualquer grupo G, o Frattini de G é igual ao conjunto de todos os elementos não geradores de G.*

Demonstração: Denotaremos por H o conjunto de todos os elementos não geradores de G. Logo, queremos mostrar que $\Phi(G) = H$. Sendo assim, tomando $g \in H$ e supondo que $g \notin \Phi(G)$, existe um subgrupo M maximal de G tal que $g \notin M$. Em particular, $G = \langle g, M \rangle = \langle M \rangle = M$. Este absurdo implica que $g \in \Phi(G)$. Agora, seja $h \in \Phi(G)$ e suponhamos que $h \notin H$, isto é, $G = \langle h, X \rangle$ implica que $G \neq \langle X \rangle$ para algum subconjunto X de G. Em particular, $h \notin \langle X \rangle$. Pelo Lema de Zorn (veja [23, Apêndice IV]), existe um subgrupo M de G que é maximal com respeito a propriedade de que contém $\langle X \rangle$ e não contém h. Portanto, pela definição de M, se $M < K \leq G$, então $h \in K$ e, consequentemente, $K = G$. Segue que M é um subgrupo maximal de G que não contém h. Absurdo, pois $h \in \Phi(G)$. Portanto, $h \in H$, completando a demonstração. ■

Teorema 1.2.2 (Teorema da Base de Burnside) [20, Teorema 5.3.2] *Seja G um p-grupo finito. Então, $\Phi(G) = G'G^p$. Além disso, se $(G : \Phi(G)) = p^r$, todo conjunto de geradores de G tem um subconjunto de r elementos que geram G.*

Segue do Teorema da Base de Burnside que o quociente $\frac{G}{\Phi(G)}$ é um p-grupo abeliano elementar.

1.3 Homomorfismo Transfer e o Teorema de Schur

O objetivo desta seção é demonstrar um famoso teorema devido I. Schur sobre grupos cujo o centro tem índice finito. Este resultado será usado para dar um critério de finitude para o grupo $\nu(G)$. Para esta seção, tomamos [20] como referência.

Sejam G um grupo possivelmente infinito e H um subgrupo com índice n em G. Escolhendo um transversal à direita $\mathcal{T} = \{t_1, t_2, \cdots, t_n\}$ para H em G consideraremos a ação por multiplicação à direita de $g \in G$ no conjunto das classes laterais de H de modo que $Ht_ig = Ht_{(i)g}$ onde a função $i \mapsto (i)g$ é uma permutação do conjunto $\{1, 2, \cdots, n\}$. Portanto,

$$t_igt_{(i)g}^{-1} \in H, \forall\, g \in G.$$

Definição 1.3.1 *Sejam H um subgrupo de índice finito de um grupo G qualquer e A um grupo abeliano. Considere um homomorfismo $\theta : H \to A$. Então, o **transfer** de θ é a função*

$$\begin{array}{rccl} \theta^* : & G & \longrightarrow & A \\ & x & \longmapsto & \displaystyle\prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}, \end{array}$$

onde $\mathcal{T} = \{t_1, t_2, \cdots, t_n\}$ é um transversal à direita para H em G.

Nos resultados a seguir, estaremos considerando as mesmas informações descritas na definição anterior. Em particular, demonstraremos que θ^* é um homomorfismo que independe da escolha do transversal $\mathcal{T}$.

Lema 1.3.1 [20, Lema 10.1.1] *A função $\theta^* : G \to A$ é um homomorfismo de grupos que independe da escolha do transversal $\mathcal{T}$.*

Demonstração: Primeiramente, considere $\mathcal{T}' = \{t'_1, t'_2, \cdots, t'_n\}$ como sendo um outro transversal à direita para H em G, tal que $Ht_i = Ht'_i$ e $t'_i = h_it_i$ para algum $h_i \in H$, $i = 1, 2, \cdots, n$. Então, considerando a ação por multiplicação à direita de $x \in G$ no conjunto das classes laterais de H, de modo que $Ht'_ix = Ht'_{(i)x}$, onde a função $i \mapsto (i)x$ é uma permutação do conjunto $\{1, 2, \cdots, n\}$, temos que

$$t'_ixt'^{-1}_{(i)x} = h_it_ixt_{(i)x}^{-1}h_{(i)x}^{-1}.$$

Portanto, pela comutatividade em A,

$$\prod_{i=1}^{n}(t'_ixt'^{-1}_{(i)x})^{\theta} = \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}\prod_{i=1}^{n}(h_i)^{\theta}(h_{(i)x}^{-1})^{\theta} \tag{1.6}$$

Como i e $(i)x$ percorrem todo $\{1, 2, \cdots, n\}$, o segundo fator à direita em (1.6) é trivial. De modo que, θ^* independe da escolha do transversal. Agora, tomando $x, y \in G$ vemos que

$$\begin{aligned} (xy)^{\theta^*} &= \prod_{i=1}^{n}(t_ixyt_{(i)xy}^{-1})^{\theta} \\ &= \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}\prod_{i=1}^{n}(t_{(i)x}yt_{(i)xy}^{-1})^{\theta} \\ &= \prod_{i=1}^{n}(t_ixt_{(i)x}^{-1})^{\theta}\prod_{j=1}^{n}(t_jyt_{(j)y}^{-1})^{\theta} \\ &= x^{\theta^*}y^{\theta^*}. \end{aligned}$$

Assim, θ^* é um homomorfismo e a demonstração se conclui. ■

Com base no lema anterior podemos encontrar um outro transversal à direita de H em G a partir de um transversal dado, para facilitar o cálculo do valor de θ^* em $x \in G$. Isto é obtido por meio do seguinte resultado:

Lema 1.3.2 (Lema Técnico) [20, Lema 10.1.2] *Seja $\mathcal{T} = \{t_1, t_2, \cdots, t_n\}$ um transversal à direita de H em G. Então,*

$$(Hs_i, Hs_i x, \cdots, Hs_i x^{l_i}), \quad i = 1, \cdots, k,$$

são as $\langle x\rangle$-órbitas de um conjunto de classes laterais à direita de H em G, tal que, se $\theta : H \to A$ é um homomorfismo de H em um grupo abeliano A, então

$$x^{\theta^*} = \prod_{m=1}^{k} (s_m x^{l_m} s_m^{-1})^{\theta}.$$

Demonstração: Considere a permutação do conjunto das classes laterais $\{Ht_1, \cdots, Ht_n\}$ produzida pela multiplicação à direita por $x \in G$. Uma $\langle x\rangle$-órbita é dada por

$$(Ht_i, Ht_i x, \cdots, Ht_i x^{l_i - 1}),$$

onde $l_i - 1$ é o menor inteiro positivo tal que $Ht_i x^{l_i} = Ht_i$, com $i \in \{1, 2, \cdots, n\}$. Consequentemente, existem índices $\{i_1, i_2, \cdots, i_k\} \subseteq \{1, 2, \cdots, n\}$ tais que os conjuntos

$$\begin{aligned} \Omega_1 &= \{Ht_{i_1}, Ht_{i_1}x, \cdots, Ht_{i_1}x^{l_{i_1}-1}\}; \\ \Omega_2 &= \{Ht_{i_2}, Ht_{i_2}x, \cdots, Ht_{i_2}x^{l_{i_2}-1}\}; \\ &\vdots \\ \Omega_k &= \{Ht_{i_k}, Ht_{i_k}x, \cdots, Ht_{i_k}x^{l_{i_k}-1}\}, \end{aligned}$$

são dois a dois disjuntos sempre que $i_m \notin \{i_r, (i_r)x, \cdots, (i_r)x^{l_{i_r}-1}\}$, para todo $m \neq r$, com $i_r \mapsto (i_r)x$ sendo uma permutação. Observe que $\sum_{m=1}^{k} |\Omega_m| = n$ e que

$$\mathcal{K} := \biguplus_{m=1}^{k} \{t_{i_m}, t_{i_m}x, \cdots, t_{i_m}x^{l_{i_m}-1}\}$$

é um novo transversal à direita de H em G. Sendo assim, para calcular o transfer em x com o transversal $\mathcal{K}$, vejamos que a ação à direita de x em $\mathcal{K}$ faz com que

$$(Ht_{i_m}x^{j-1})x = Ht_{i_m}x^j, \quad \text{com} \;\; j = 1, 2, \cdots, l_{i_m}.$$

Portanto, denotando $s_m = t_{i_m}$, a contribuição de $\mathcal{K}$ para x^{θ^*} é

$$((s_m x)(s_m x)^{-1}(s_m x^2)(s_m x^2)^{-1} \cdots (s_m x^{l_m - 1})(s_m x^{l_m-1})^{-1}(s_m x^{l_m} s_m^{-1}))^{\theta},$$

que se reduz a $(s_m x^{l_m} s_m^{-1})^\theta$. Assim,

$$x^{\theta^*} = \prod_{m=1}^{k} (s_m x^{l_m} s_m^{-1})^\theta.$$

■

Um caso muito importante de transfer surge quando θ é um homomorfismo canônico de H para H_{ab}, isto é, $x^\theta = H'x$. Em particular, quando H é central em G, o transfer $\theta^* : G \to H_{ab}$ é um endomorfismo de G, como mostra o resultado a seguir.

Lema 1.3.3 (I. Schur) [20, Lema 10.1.3] *Seja H um subgrupo do centro de um grupo G. Se $(G : H) = n$, então o transfer θ^* de G em H é a função $x \mapsto x^n$. Consequentemente, esta função é um endomorfismo de G.*

Demonstração: Dado que $H \leq Z(G)$, podemos considerar θ como sendo o homomorfismo identidade

$$\begin{aligned} id_H : \quad H &\longrightarrow H \\ x &\longmapsto x. \end{aligned}$$

Portanto, usando a notação do Lema 1.3.2 vemos que $s_i x^{l_i} s_i^{-1} \in H \leq Z(G)$. Daí, $x^{l_i} \in Z(G)$ e, portanto, $s_i x^{l_i} s_i^{-1} = x^{l_i}$, $i = 1, 2, \cdots, k$. Consequentemente,

$$x^{\theta^*} = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1})^{id_H} = \prod_{i=1}^{k} s_i x^{l_i} s_i^{-1} = \prod_{i=1}^{k} x^{l_i} = x^n.$$

■

Antes de demonstrar o Teorema de Schur, mostraremos um lema que será usado em sua demonstração e também em outros resultados apresentados neste trabalho.

Lema 1.3.4 [20, Lema 1.6.11] *Seja H um subgrupo de índice finito em um grupo G finitamente gerado. Então, H é finitamente gerado.*

Demonstração: Seja X um conjunto finito de geradores de G e seja

$$\mathcal{T} = \{t_1 = 1_G, t_2, \cdots, t_n\}$$

um transversal de H em G. Se $g \in G$, então $Ht_j g = Ht_{(j)g}$ onde $j \mapsto (j)g$ é uma permutação de $\{1, 2, \cdots, n\}$. Logo,

$$t_j g = h(j, g) t_{(j)g}, \quad h(j, g) \in H. \tag{1.7}$$

Seja $a \in H$ e escreva $a = y_1 \cdots y_k$, $y_l \in X \cup X^{-1}$. Por (1.7), temos

$$\begin{aligned} a = t_1 a &= t_1 y_1 \cdots y_k \\ &= h(1, y_1)(t_{(1)y_1} y_2) y_3 \cdots y_k \\ &\vdots \\ &= h(1, y_1) h((1)y_1, y_2) \cdots h((1)y_1 y_2 \cdots y_{k-1}, y_k) t_{((1)y_1 \cdots y_{k-1})y_k} \\ &= h(1, y_1) h((1)y_1, y_2) \cdots h((1)y_1 y_2 \cdots y_{k-1}, y_k) t_{(1)a} \in Ht_{(1)a} \end{aligned}$$

Mas, $Ht_{(1)a} = Ht_1 a = H$ implica que

$$H = \langle h(j,y) \,|\, 1 \leq j \leq n,\, y \in X \cup X^{-1} \rangle,$$

como queríamos. ∎

Teorema 1.3.1 (I. Schur) [20, Teorema 10.1.4] *Seja G um grupo tal que $(G : Z(G)) = n$. Então, o subgrupo derivado G' é finito. Mais ainda, $\exp(G')$ divide n.*

Demonstração: Sejam $C := Z(G)$ e $\mathcal{T} = \{g_1, g_2, \cdots, g_n\}$ um transversal à direita de C em G. Como $\frac{G}{C} = \{Cg_1, Cg_2, \cdots, Cg_n\}$, para cada $x, y \in G$ podemos escrever $x = c_i g_i$ e $y = c_j g_j$, com $i, j \in \{1, \cdots, n\}$ e $c_i, c_j \in C$. Logo,

$$[x, y] = [c_i g_i, c_j g_j] = [g_i, g_j],$$

implica que

$$G' = \langle [g_i, g_j] \,|\, g_i, g_j \in \mathcal{T}, i, j \in \{1, \cdots, n\} \rangle.$$

Em particular, G' é finitamente gerado. Sendo

$$\frac{G'}{G' \cap C} \simeq \frac{G'C}{C} \leq \frac{G}{C},$$

então $(G' : G' \cap C) < \infty$. Logo, $G' \cap C$ é finitamente gerado [Lema 1.6.11]. Agora, usando o Lema 1.3.3, a função $\theta^* : G \to C$ dada por $x \mapsto x^n$ determina um homomorfismo para o qual

$$\frac{G}{\ker \theta^*} \simeq \operatorname{Im} \theta^* \leq C.$$

Logo,

$$G' \leq \ker \theta^* \text{ e, em particular, } (G')^n = 1. \tag{1.8}$$

Daí, $\exp(G')$ divide n. Além disso, se $h_1, h_2, \cdots, h_k$ são geradores do subgrupo abeliano finitamente gerado $G' \cap C$, temos que

$$\begin{aligned} G' \cap C &= \langle h_1, h_2, \cdots, h_k \rangle \\ &= \langle h_1 \rangle + \cdots + \langle h_k \rangle. \end{aligned}$$

Mas, por (1.8), temos que $|\langle h_l \rangle| < +\infty$, para todo $l = 1, 2, \cdots, k$. Portanto, $|G' \cap C| < +\infty$ e pelo Teorema de Lagrange,

$$|G'| = |G' \cap C|(G' : G' \cap C) < +\infty,$$

e, assim, concluímos a demonstração. ∎

1.4 Grupos Livres e Produtos Livres

Nesta seção, faremos uma introdução aos conceitos de Grupo Livre, Apresentações de Grupos e Produto Livre de Grupos. As referências utilizadas foram [14], [15] e [20].

Definição 1.4.1 *Sejam F um grupo, X um conjunto não vazio e $\sigma : X \to F$ uma função. Dizemos que F é **livre** em X, se para cada função $\alpha : X \to G$, onde G é um grupo, existe um único homomorfismo $\beta : F \to G$ tal que $\alpha = \beta\sigma$.*

A equação $\alpha = \beta\sigma$ expressa a comutatividade do diagrama

$$\begin{tikzcd} F \arrow[dr, dashed, "\beta"] & \\ X \arrow[u, "\sigma"] \arrow[r, "\alpha"'] & G. \end{tikzcd}$$

A função $\sigma : X \to F$ é necessariamente injetiva. De fato, se para $x_1, x_2 \in X$ tivermos $\sigma(x_1) = \sigma(x_2)$ com $x_1 \neq x_2$, então podemos escolher uma função $\alpha : X \to G$, onde G é um grupo com pelo menos dois elementos distintos g_1 e g_2, tal que $\alpha(x_1) = g_1$ e $\alpha(x_2) = g_2$. Mas, $\alpha = \beta\sigma$ implica que

$$g_1 = \alpha(x_1) = \beta\sigma(x_1) = \beta\sigma(x_2) = \alpha(x_2) = g_2.$$

Como isso, segue que $x_1 = x_2$.

Observe que a definição de grupos livres não nos garante a existência de tais grupos. Por isso, descreveremos na sequência uma maneira de construir grupos livres. Nesta construção, veremos que F será livre também sobre Im σ, com a função inclusão ι : Im $\sigma \to F$ fazendo o papel de σ na definição. Consequentemente, um grupo livre será sempre livre em um certo subconjunto. Além disso, a comutatividade do diagrama nos dirá que a restrição de β a X é α, de modo que β é a única extensão de α a F.

Seja X um conjunto não vazio, cujos elementos chamaremos de *símbolos*. Escolha um conjunto disjunto de X de mesma cardinalidade e denote-o por $X^{-1} = \{x^{-1} \mid x \in X\}$. Uma *palavra* w em X é uma sequência finita de símbolos de $X \cup X^{-1}$, escrita por convenção na forma

$$w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n},$$

onde cada $x_{i_j} \in X$, $\epsilon_j = \pm 1$, $n \geq 0$, $j = 1, 2, \cdots, n$. O inteiro n é chamado de *comprimento* da palavra w. No caso em que $n = 0$, chamamos w de *palavra vazia*, e será denotada por 1. Duas palavras são iguais se, e somente se, tiverem os mesmos símbolos em suas correspondentes posições. O *produto* de duas palavras é formado por justaposição, isto é, se $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n}$ e $v = x_{j_1}^{\delta_1} x_{j_2}^{\delta_2} \cdots x_{j_m}^{\delta_m}$ são palavras em X, então o produto de w e v é

$$wv = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n} x_{j_1}^{\delta_1} x_{j_2}^{\delta_2} \cdots x_{j_m}^{\delta_m}.$$

Por convenção, $w1 = w = 1w$. A *inversa* de w é a palavra

$$w^{-1} = x_{i_n}^{-\epsilon_n} x_{i_{n-1}}^{-\epsilon_{n-1}} \cdots x_{i_2}^{-\epsilon_2} x_{i_1}^{-\epsilon_1},$$

e $1^{-1} = 1$. Seja S o conjunto de todas as palavras em X. Definimos uma relação de equivalência $\sim$ em S da seguinte maneira: duas palavras w e $v \in S$ são ditas equivalentes se é possível obter uma palavra da outra inserindo ou retirando os símbolos xx^{-1}, ou $x^{-1}x$, com $x \in X$. Por exemplo, as palavras

$$w = x_1 x_2 x_2^{-1} \text{ e } v = x_1,$$

são equivalentes. Para mais detalhes veja [15].

Com base nessas informações, temos o seguinte resultado:

Proposição 1.4.1 [20, Proposição 2.1.1] *Seja X um conjunto não vazio. Então existe um grupo F e uma função $\sigma : X \to F$ tal que F é livre em X e $F = \langle Im\, \sigma \rangle$.*

Demonstração: Sejam X um conjunto não vazio, S o conjunto de todas as palavras em X e $\sim$ a relação de equivalência vista anteriormente. Definiremos F como o conjuntos de todas as classes de equivalência $[w]$, $w \in S$. Como o produto de palavras em X é feito por justaposição, vemos que $wv \sim w'v'$ sempre que $w \sim w'$ e $v \sim v'$. Assim, podemos definir uma operação produto em F de duas classes de equivalência da seguinte forma:

$$[w][v] = [wv].$$

Logo, $[w][1] = [w] = [1][w]$, $[w][w^{-1}] = [ww^{-1}] = [1]$. Além disso, como $(wv)u = w(vu)$, então

$$([w][v])[u] = [wv][u] = [(wv)u] = [w(vu)] = [w][vu] = [w]([v][u]).$$

Portanto, F é um grupo com o produto definido, onde $[1]$ é o elemento neutro de F, e $[w^{-1}]$ é o elemento inverso de cada classe $[w]$ de F. Agora, definiremos a função $\sigma : X \to F$ por $\sigma(x) = [x]$, e consideremos uma função qualquer $\alpha : X \to G$, onde G é um grupo. Estendendo linearmente a aplicação α, podemos construir uma outra aplicação $\alpha_2 : S \to G$ dada por $\alpha_2(w) = g_{i_1}^{\epsilon_1} g_{i_2}^{\epsilon_2} \cdots g_{i_n}^{\epsilon_n}$, onde $\alpha(x_{i_j}^{\epsilon_j}) = g_{i_j}^{\epsilon_j}$, $\epsilon_j = \pm 1$ e $j = 1, 2, \cdots, n$. Note que, $w \sim v$ implica que $\alpha_2(w) = \alpha_2(v)$, pois

$$\alpha_2(xx^{-1}) = \alpha(x)\alpha(x^{-1}) = gg^{-1} = 1_G = \alpha_2(x^{-1}x)$$

Isto nos permite estender α_2 para uma função bem definida $\beta : F \to G$ dada por $\beta([w]) = \alpha_2(w)$. Em particular, β é um homomorfismo, pois para quaisquer $[w], [v] \in F$,

$$\beta([w][v]) = \beta([wv]) = \alpha_2(wv) = \alpha_2(w)\alpha_2(v) = \beta([w])\beta([v]).$$

Além disso, para todo $x \in X$,

$$\beta\sigma(x) = \beta([x]) = \alpha_2(x) = \alpha(x).$$

Finalmente, se $\gamma : F \to G$ é outro homomorfismo tal que $\alpha = \gamma\sigma$, então $\gamma\sigma = \beta\sigma$, ou seja, β e γ coincidem em Im σ. Mas $F = \langle \text{Im } \sigma \rangle$ implica que $\beta = \gamma$ em todo o grupo F. ∎

A seguir, veremos uma caracterização de grupos livres, para isso precisamos definir os conceitos de palavra reduzida e forma normal. Assim, uma palavra w em X é chamada *reduzida* se ela não contém nenhum par de símbolos consecutivos da forma xx^{-1} ou $x^{-1}x$, $x \in X$. Por convenção, a palavra vazia é reduzida. Em particular, em cada classe de equivalência $[w] \in F$ existe uma única palavra reduzida, [20, Proposição 2.1.2]. Consequentemente, podemos considerar cada classe de equivalência $[w]$ de F, com $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n}$ sendo a única forma reduzida desta classe, $\epsilon_j = \pm 1$, $n \geq 0$ e $j = 1, 2, \cdots, n$. Pela definição de produto em F, temos que

$$[w] = [x_{i_1}]^{\epsilon_1} [x_{i_2}]^{\epsilon_2} \cdots [x_{i_n}]^{\epsilon_n}.$$

Multiplicando as classes consecutivas que são iguais, temos

$$[w] = [x_{j_1}]^{l_1} [x_{j_2}]^{l_2} \cdots [x_{j_m}]^{l_m},$$

onde cada l_k é um inteiro não nulo e $m \geq 0$ e $x_{j_k} \neq x_{j_{k+1}}$. Note que a palavra reduzida, pode ser novamente obtida a partir desta, logo, esta expressão é única. Para simplificar a notação, denotaremos a classe de equivalência $[w]$ por apenas w. Portanto, cada elemento w de F pode ser escrito unicamente da forma

$$w = x_{j_1}^{l_1} x_{j_2}^{l_2} \cdots x_{j_m}^{l_m}.$$

onde cada l_k é um inteiro não nulo, $m \geq 0$ e $x_{j_k} \neq x_{j_{k+1}}$. Esta forma é chamada de *forma normal* de w. Às vezes, é conveniente abreviá-la para $w = w(x_{j_1}, x_{j_2}, \cdots, x_{j_m})$ ou mesmo $w(x)$.

Proposição 1.4.2 [20, Proposição 2.1.3] *Sejam G um grupo e X um subconjunto de G. Suponhamos que cada elemento $g \in G$ tem uma única expressão da forma*

$$g = x_{j_1}^{l_1} x_{j_2}^{l_2} \cdots x_{j_m}^{l_m},$$

onde $x_{j_k} \in X$, l_k é um inteiro não nulo, $m \geq 0$ e $x_{j_k} \neq x_{j_{k+1}}$, $k = 1, 2, \cdots, m$. Então, G é livre em X.

Demonstração: Seja F um grupo livre em X. Mostraremos que $F \simeq G$. De fato, dado que F é livre em X com a função injetiva $\sigma : X \to F$ associada, existe para cada função $\alpha : X \to G$, um único homomorfismo $\beta : F \to G$ tal que $\alpha = \beta\sigma$. Em particular, podemos considerar α como sendo a função inclusão. Dado que $G = \langle X \rangle$, segue que β é sobrejetivo. Além disso, β é injetivo pela unicidade da forma normal. ∎

Proposição 1.4.3 [20, Proposição 2.1.5] *Sejam G um grupo gerado por um subconjunto X e F um grupo livre em um conjunto Y. Se $\alpha : Y \to X$ é sobrejetiva, então $\beta : F \to G$*

é um epimorfismo que estende α. Em particular, todo grupo é uma imagem de um grupo livre.

Demonstração: Sejam X um conjunto não vazio, $G = \langle X \rangle$ um grupo gerado por X e F um grupo livre em um conjunto Y, com $\sigma : Y \to F$ sendo a função injetiva associada. Pela hipótese de F ser livre em Y, para a função sobrejetiva $\alpha : Y \to X$ existe um único homomorfismo $\beta : F \to G$ tal que $\alpha = \beta\sigma$. Mas, como α é sobrejetiva, segue que β é um epimorfismo, pois $G = \langle X \rangle$. ∎

Definição 1.4.2 *Uma **apresentação livre** de um grupo G é um epimorfismo $\pi : F \twoheadrightarrow G$ de um grupo livre F para o grupo G. Se R é o núcleo de π, então os elementos de R são chamados de **relatores** da apresentação.*

Dada uma apresentação $\pi : F \twoheadrightarrow G$, escolha um conjunto Y de geradores livres de F e um subconjunto S de F tal que o fecho normal S^F de S em F é o $\ker \pi$. Note que a imagem de π restrita a Y é um conjunto de geradores de G. Além disso, vemos que $r \in F$ é um relator de π se, e somente se,

$$r = (s_{j_1}^{\varepsilon_1})^{f_{j_1}} (s_{j_2}^{\varepsilon_2})^{f_{j_2}} \cdots (s_{j_k}^{\varepsilon_k})^{f_{j_k}}, \qquad \text{onde } s_{j_i} \in S, f_{j_i} \in F \text{ e } \varepsilon_i = \pm 1, i = 1, 2 \cdots, k.$$

A apresentação π, junto com as escolhas de Y e S determinam um *conjunto de geradores* e *relatores definidores* para G. Em símbolos,

$$G = \langle Y \mid S \rangle. \tag{1.9}$$

É mais frequente listar os geradores de G e a *relações definidoras* $s(x) = 1$, $s \in S$, nos geradores X. Portanto,

$$G = \langle X \mid s(x) = 1, s \in S \rangle. \tag{1.10}$$

Às vezes, faremos referência a (1.9) ou (1.10) como uma apresentação de G. O resultado a seguir nos mostra o que acontece quando os relatores de uma apresentação de um grupo G são também relatores de uma apresentação de um grupo H.

Teorema 1.4.1 (von Dyck) [20, Teorema 2.2.1] *Sejam G e H grupos com apresentações $\varepsilon : F \twoheadrightarrow G$ e $\delta : F \twoheadrightarrow H$ tais que cada relator de ε é também um relator de δ. Então, a função*

$$\begin{aligned} \psi : \quad G &\longrightarrow H \\ \varepsilon(f) &\longmapsto \delta(f) \end{aligned}$$

é um epimorfismo bem definido de G em H.

Demonstração: A condição de que cada relator de ε é também relator de δ significa que $\ker \varepsilon \subseteq \ker \delta$. Agora, para mostrar que a aplicação ψ é bem definida, note que se $\varepsilon(f) = \varepsilon(f_1)$ então, $f = kf_1$, onde $k \in \ker \varepsilon \subseteq \ker \delta$. Consequentemente, $\delta(f) = \delta(k)\delta(f_1) = \delta(f_1)$, de modo que ψ está bem definida. Como ε e δ são epimorfismos, então ψ é um homomorfismo. Em particular, para todo $\delta(f) \in H$ existe $g \in G$ tal que $\varepsilon(f) = g$, logo, ψ também é um epimorfismo. ∎

Vejamos alguns exemplos de apresentações de grupos:

Exemplos 1.1 (1) O grupo diedral infinito D_∞ possui uma apresentação

$$D_\infty = \langle x, y \,|\, x^2 = 1, y^2 = 1 \rangle.$$

(2) O grupo diedral D_{2n} de ordem $2n$, com $n \geq 2$ tem uma apresentação

$$D_{2n} = \langle x, y \,|\, x^2 = y^n = 1, x^{-1}yx = y^{-1} \rangle.$$

Vejamos alguns resultados sobre homomorfismos induzidos.

Lema 1.4.1 [14, Lema 1] *Sejam F, G, H grupos e $\upsilon : F \to G$, $\alpha : F \to H$ homomorfismos tais que Im $\upsilon = G$ e $\ker \upsilon \subseteq \ker \alpha$. Então, existe um homomorfismo $\alpha' : G \to H$ tal que $\alpha'\upsilon = \alpha$.*

Demonstração: Dado que Im $\upsilon = G$, então para todo $g \in G$ existe $f \in F$ tal que $\upsilon(f) = g$. Com isso, definiremos $\alpha' : G \to H$ por $\alpha'(g) = \alpha(f)$. Em particular, α' é bem definida, pois tomando f e f' em F tais que $\upsilon(f) = \upsilon(f')$, temos que $f = kf'$, com $k \in \ker \upsilon \subseteq \ker \alpha$. Consequentemente, $\alpha(f) = \alpha(f')$. Portanto, o valor de $\alpha(f)$ independe da escolha de $f \in \mathrm{Im}^{-1}(g)$. Além disso, α' é um homomorfismo, pois se $\upsilon(f) = g$ e $\upsilon(f') = g'$ são elementos quaisquer de G, então dado que υ é um homomorfismo, temos $gg' = \upsilon(ff')$. Sendo assim, usando o fato de que α é homomorfismo, segue da definição de α' que

$$\alpha'(gg') = \alpha(ff') = \alpha(f)\alpha(f') = \alpha'(g)\alpha'(g').$$

Nos resta mostrar que $\alpha'\upsilon = \alpha$. Mas isto segue do fato que $f \in \mathrm{Im}^{-1}(\upsilon(f))$, para todo $f \in F$. Assim, $\alpha'(\upsilon(f)) = \alpha(f)$ para todo $f \in F$. ∎

Proposição 1.4.4 (Teste da Substituição) [14, Proposição 3] *Sejam $G = \langle X \,|\, R \rangle$ uma apresentação de um grupo G, H um grupo e $\theta : X \to H$ uma função. Então, θ estende para um homomorfismo $\alpha' : G \to H$ se, e somente se, para todo $x \in X$ e todo $r \in R$, o resultado da substituição de x por $\theta(x)$ em r nos dá a identidade de H.*

Demonstração: ($\Leftarrow$) Dado que $G = \langle X \,|\, R \rangle$ é uma apresentação de G, existe um grupo livre F em X e um epimorfismo $\upsilon : F \twoheadrightarrow G$ cujo o núcleo é o fecho normal de R em F. Além disso, pela definição, para a função $\theta : X \to H$ existe um único homomorfismo $\alpha : F \to H$

que estende θ. Suponhamos que o resultado da substituição de x por $\theta(x)$ em $r \in R$ nos dá o elemento identidade de H. Então, $R \subseteq \ker \alpha$, consequentemente, $\ker \upsilon \subseteq \ker \alpha$, pois $\ker \upsilon = R^F$ e $\ker \alpha \trianglelefteq F$. Logo, pelo lema anterior, existe um homomorfismo $\alpha' : G \to H$ induzido por α, estendendo θ.
($\Rightarrow$) Reciprocamente, suponhamos que existe um homomorfismo $\alpha' : G \to H$ que estende $\theta : X \to H$. Então,

$$R \subseteq R^F = \ker \upsilon \subseteq \ker \alpha' \upsilon = \ker \alpha.$$

■

Dado que G é gerado por X, então α' é único, quando existir. Além disso, se H é gerado por Im θ, então, α' é um epimorfismo.

Definição 1.4.3 *Seja $\{G_\lambda \,|\, \lambda \in \mathit{\Lambda}\}$ uma família não vazia de grupos. Um* ***produto livre*** *dos grupos G_λ é um grupo G e uma coleção de homomorfismos $\iota_\lambda : G_\lambda \to G$ com a seguinte propriedade: dado um conjunto de homomorfismos $\varphi_\lambda : G_\lambda \to H$ sobre qualquer grupo H, existe um único homomorfismo $\varphi : G \to H$ tal que $\varphi \iota_\lambda = \varphi_\lambda$, isto é, fazendo todos os diagramas abaixo comutarem.*

$$\begin{tikzcd} G_\lambda \arrow[r, "\iota_\lambda"] \arrow[d, "\varphi_\lambda"'] & G \arrow[dl, dashed, "\varphi"] \\ H & \end{tikzcd}$$

Os grupos G_λ's são chamados de *fatores livres* de G. Quando Λ é um conjunto finito $\{\lambda_1, \lambda_2, \cdots, \lambda_n\}$, denotamos G por

$$G := G_{\lambda_1} * G_{\lambda_2} * \cdots * G_{\lambda_n}.$$

As funções ι_λ são injetivas. De fato, se H é algum G_λ e $\varphi_\lambda = id_{G_\lambda}$ é o homomorfismo identidade de G_λ e φ_μ é o homomorfismo trivial $\varphi_\mu(x) = 1_H$ para todo $\mu \neq \lambda$ e $x \in G_\mu$, então, por definição, existe um único homomorfismo $\varphi : G \to G_\lambda$ tal que $\varphi \iota_\lambda = id_{G_\lambda}$, de modo que ι_λ é injetiva para todo $\lambda \in \Lambda$.

Dado uma família não vazia de grupos $\{G_\lambda \,|\, \lambda \in \mathit{\Lambda}\}$ o produto livre dos grupos G_λ existe e é único.

Proposição 1.4.5 [20, Proposição 6.2.1] *Sejam G_1 e G_2 produtos livres do conjunto $\{G_\lambda \,|\, \lambda \in \Lambda\}$. Então, G_1 e G_2 são isomorfos.*

Proposição 1.4.6 [20, Proposição 6.2.2] *Para toda família não vazia de grupos $\{G_\lambda \,|\, \lambda \in \Lambda\}$ existe um correspondente produto livre.*

Proposição 1.4.7 [15, pág. 196] *Seja $G = H * K$ um produto livre de grupos H e K. Então, $[H, K]$ é um subgrupo livre, normal em G, gerado livremente pelos símbolos $[h, k] = h^{-1}k^{-1}hk$ onde $1 \neq h \in H$ e $1 \neq k \in K$.*

1.5 Produto Tensorial de R-módulos

Nesta seção temos como objetivo introduzir alguns resultados relacionados ao produto tensorial de R-módulos, onde R é um anel com unidade qualquer. A referência utilizada para esta seção foi [24].

Definição 1.5.1 *Um R-**módulo à esquerda**, denotado por ${}_RM$, onde R é um anel com unidade, é um grupo abeliano (com notação aditiva) M possuindo uma multiplicação por escalar $R \times M \to M$, dada por $(r, m) \mapsto rm$, satisfazendo,*
(i) $r(m + m') = rm + rm'$;
(ii) $(r + r')m = rm + r'm$;
(iii) $(rr')m = r(r'm)$;
(iv) $1m = m$, *para todo* $m, m' \in M$ *e* $r, r' \in R$.

Exemplos 1.2 (1) Seja $\mathbb{Z}$ o anel dos números inteiros. Todo grupo abeliano pode ser visto como um $\mathbb{Z}$-módulo à esquerda.
(2) Todo anel R pode ser visto como um R-módulo à esquerda se definirmos uma multiplicação por escalar $R \times R \to R$ como sendo a multiplicação de elementos de R.
(3) Se S é um subanel de um anel R, então R pode ser visto como um S-módulo à esquerda onde a multiplicação por escalar $S \times R \to R$ é dada por $(s, r) \mapsto sr$. Em particular, tomando o centro de um anel R

$$Z(R) = \{a \in R \,|\, ar = ra, \text{ para todo}\, r \in R\},$$

podemos ver R como um $Z(R)$-módulo.

Definição 1.5.2 *Se M e N são R-módulos à esquerda, então um R-**homomorfismo** (ou uma R-**função**) é uma aplicação $f : M \to N$ tal que, para todos $m, m' \in M$ e $r \in R$,*
(i) $f(m + m') = f(m) + f(m')$;
(ii) $f(rm) = rf(m)$;

Um R-*isomorfismo* é um R-homomorfismo bijetivo.

Exemplo 1.1 Todo homomorfismo de grupos abelianos é uma $\mathbb{Z}$-função.

As definições de R-módulo à direita, denotado por M_R, e de R-homomorfismo de R-módulos à direita são análogas às definições 1.5.1 e 1.5.2, respectivamente. O *núcleo* e a *imagem* de uma R-função $f : M \to N$ entre R-módulos são definidos, respectivamente, como

$$\ker f = \{m \in M \,|\, f(m) = 0\}, \;\; \mathrm{Im}\, f = \{f(m) \in N \,|\, m \in M\}.$$

Definição 1.5.3 *Se M é um R-módulo à esquerda, então um **submódulo** N de M, denotado por $N \subseteq M$, é um subgrupo (com notação aditiva) N de M fechado sob a* *multiplicação por escalar* $rn \in N$*, sempre que* $n \in N$ *e* $r \in R$*. Similarmente, um submódulo* K *de um* R*-módulo à direita* L *é um subgrupo (com notação aditiva) de* L *fechado sob a multiplicação por escalar,* $kr \in K$*, sempre que* $k \in K$ *e* $r \in R$*.*

Exemplos 1.3 (1) Seja G um grupo abeliano com notação aditiva. Como $\mathbb{Z}$-módulo, os submódulos de G são seus subgrupos.
(2) Seja X um subconjunto de um R-módulo M à esquerda, então o conjunto de todas as R-combinações lineares de elementos em X, dado por

$$\langle X\rangle = \Big\{\sum_i r_i x_i \,|\, r_i \in R, x_i \in X\Big\},$$

é um submódulo chamado *submódulo gerado por* X. Um R-módulo M é chamado *cíclico* se existe $m \in M$, tal que

$$M = \{rm \,|\, r \in R\}.$$

Se M é um R-módulo e $m \in M$, então um *submódulo cíclico gerado por* m, denotado por $\langle m\rangle$, é

$$\langle m\rangle = \{rm \,|\, r \in R\}.$$

Definição 1.5.4 *Se* N *é um submódulo de um* R*-módulo à esquerda, então o* ***R-módulo quociente*** *é o grupo quociente* $\frac{M}{N}$ *com multiplicação por escalar dada por*

$$r(m + N) = rm + N. \tag{1.11}$$

A função natural

$$\begin{array}{rrcl} g: & M & \longrightarrow & \dfrac{M}{N} \\ & m & \longmapsto & m + N \end{array}$$

é uma R-função. Além disso, a multiplicação por escalar (1.11) está bem definida, pois, se $m + N = m' + N$, então $m - m' \in N$. Logo, $r(m - m') = rm - rm' \in N$, pois N é submódulo. Portanto, $rm + N = rm' + N$.

Definição 1.5.5 *Sejam* M *um* R*-módulo à esquerda e* $S_1, S_2, \cdots, S_n$ *submódulos de* M*. Dizemos que* M *é uma* ***soma direta*** *(interna) de* S_i*, denotada por*

$$M = S_1 \oplus \cdots \oplus S_n = \bigoplus_{i=1}^{n} S_i,$$

se cada $m \in M$ *tem uma única expressão da forma* $m = s_1 + \cdots + s_n$*, onde* $s_i \in S_i$ *para todo* $i = 1, 2, \cdots, n$*. Mais ainda, dizemos que* M *é uma soma direta de uma família* $\{S_i \,|\, i \in I\}$ *de submódulos, denotamos por*

$$M = \bigoplus_{i \in I} S_i,$$

se M consiste de todas as i-tuplas (s_i) onde cada i-ésima coordenada s_i pertence ao submódulo S_i, para todo i, tendo somente um número finito de coordenadas não nulas. Neste caso, cada elemento $m \in \bigoplus_{i\in I} S_i$ tem uma única expressão da forma

$$m = \sum_{i\in I} \mu_i s_i,$$

onde $\mu_i s_i : I \to \bigcup_{i\in I} S_i$ é uma aplicação dada por $\mu_i s_i(i) = s_i \in S_i$ e $\mu_i s_i(j) = 0 \in S_j$ para todo $i, j \in I$ e $j \neq i$.

Definição 1.5.6 *Um R-módulo à esquerda F é um **R-módulo à esquerda livre** se F é isomorfo a uma soma direta de cópias de R, isto é, existe um conjunto B de índices (possivelmente infinito) com $F = \bigoplus_{b\in B} R_b$, onde $R_b = \langle b\rangle \simeq R$ para todo $b \in B$. Chamamos B de **base** de F.*

Note que, pela definição de soma direta interna de R-módulos, cada elemento $m \in F$ tem uma única expressão da forma

$$m = \sum_{b\in B} r_b b,$$

onde $r_b \in R$ e quase todos r_b's são nulos. Assim, $F = \langle B\rangle$.

Um $\mathbb{Z}$-módulo livre é também chamado de *grupo abeliano livre* (veja também [23, pág. 312]). Todo anel R, quando considerado como um módulo à esquerda sobre si mesmo é um R-módulo livre.

Proposição 1.5.1 [24, Proposição 2.33] *Seja R um anel. Dado qualquer conjunto B, existe um R-módulo à esquerda livre F com base B.*

Proposição 1.5.2 (Extensão por Linearidade) [24, Proposição 2.34] *Sejam R um anel, F um R-módulo à esquerda livre com base X e M um R-módulo à esquerda. Se $f : X \to M$ é qualquer função, então existe uma única R-função $\tilde{f} : F \to M$ com $\tilde{f}\mu = f$, onde $\mu : X \to F$ é a inclusão, isto é, $\tilde{f}(x) = f(x)$ para todo $x \in X$. Assim, $\tilde{f}$ estende f.*

$$\begin{tikzcd} F \arrow[dr, dashed, "\tilde{f}"] & \\ X \arrow[u, "\mu"] \arrow[r, "f"'] & M \end{tikzcd}$$

Demonstração: Dado que F é um R-módulo à esquerda livre com base X, por definição, cada elemento $u \in F$ tem uma única expressão da forma

$$u = \sum_{x\in X} r_x x,$$

onde $r_x \in R$ e quase todos r_x's são nulos. Como candidata para a R-função $\tilde{f} : F \to M$ que estende $f : X \to M$, tomaremos

$$\begin{aligned} \tilde{f} : \quad F &\longrightarrow M \\ u &\longmapsto \sum_{x \in X} r_x f(x). \end{aligned}$$

Devido a unicidade da expressão de cada elemento de F, temos que $\tilde{f}$ é bem definida. Mais ainda, se $r \in R$ e $u' = \sum_{x \in X} r'_x x \in F$, então, por definição,

$$ru = \sum_{x \in X} r r_x x \ \text{ e } \ u + u' = \sum_{x \in X} (r_x + r'_x) x.$$

Segue pela definição que $\tilde{f}$ é uma R-função. Agora, dado que $F = \langle X \rangle$, então qualquer R-função $g : F \to M$ que estende f coincidirá com $\tilde{f}$ na base X, logo, em todo o F. Portanto, $\tilde{f}$ é única. ■

Definição 1.5.7 *Sejam R um anel, A um R-módulo à direita, B um R-módulo à esquerda, e G um grupo abeliano (com notação aditiva). Uma função $f : A \times B \to G$ é chamada R-**biaditiva** se, para todos $a, a' \in A$, $b, b' \in B$ e $r \in R$, satisfazer as seguintes condições:*

$$f(a + a', b) = f(a, b) + f(a', b),$$

$$f(a, b + b') = f(a, b) + f(a, b'),$$

$$f(ar, b) = f(a, rb).$$

Exemplo 1.2 Seja R um anel. Então, a multiplicação por escalar $\mu : R \times R \to R$ dada pela multiplicação de elementos de R é R-biaditiva. De fato, os dois primeiros axiomas são as leis distributivas em R e o terceiro axioma é a lei associativa da multiplicação em R.

Definição 1.5.8 *Sejam R um anel, A_R e $_RB$ módulos. O **produto tensorial de** A **por** B é um grupo abeliano $A \otimes_R B$ e uma função R-biaditiva*

$$h : A \times B \to A \otimes_R B,$$

tal que, para todo grupo abeliano G e toda função R-biaditiva $f : A \times B \to G$, existe um único $\mathbb{Z}$-homomorfismo $\tilde{f} : A \otimes_R B \to G$ fazendo o seguinte diagrama comutar:

$$\begin{tikzcd} A \otimes_R B \arrow[dr, dashed, "\tilde{f}"] & \\ A \times B \arrow[u, "h"] \arrow[r, "f"'] & G. \end{tikzcd}$$

Os próximos resultados nos dizem que o produto tensorial de R-módulos existe e é único, a menos de isomorfismos.

Proposição 1.5.3 [24, Proposição 2.44] *Se U e $A \otimes_R B$ são produtos tensoriais de A_R e ${}_RB$ sobre R, então $A \otimes_R B \simeq U$.*

Demonstração: Dado que U é um produto tensorial de R-módulos A_R e ${}_RB$, pela definição, se $\eta : A \times B \to U$ é a função R-biaditiva associada, então para todo grupo abeliano G e toda função R-biaditiva $f : A \times B \to G$, existe um único $\mathbb{Z}$-homomorfismo $f' : U \to G$ fazendo o diagrama

$$\begin{tikzcd}
U \arrow[dr, dashed, "f'"] & \\
A \times B \arrow[u, "\eta"] \arrow[r, "f"'] & G
\end{tikzcd}$$

comutar. Em particular, considerando $G = A \otimes_R B$ e $f = h$, existe um único $\mathbb{Z}$-homomorfismo $h' : U \to A \otimes_R B$ tal que $h'\eta = h$. Analogamente, dado que $A \otimes_R B$ é um produto tensorial de A_R e ${}_RB$, então temos uma função R-biaditiva associada $h : A \times B \to A \otimes_R B$, tal que para todo grupo abeliano G e para toda função $\eta' : A \times B \to G$, existe um único $\mathbb{Z}$-homomorfismo $\tilde{\eta} : A \otimes_R B \to G$ para o qual vale $\tilde{\eta}h = \eta'$. Neste caso, consideremos $G = U$, $\eta = \eta'$ e o seguinte diagrama

$$\begin{tikzcd}
 & A \otimes_R B \arrow[d, dashed, "\tilde{\eta}"] \\
A \times B \arrow[ur, "h"] \arrow[r, "\eta"'] \arrow[dr, "h"'] & U. \arrow[d, dashed, "h'"] \\
 & A \otimes_R B
\end{tikzcd}$$

Agora,

$$(h'\tilde{\eta})h = h'(\tilde{\eta}h) = h'\eta = h$$

nos diz que o diagrama

$$\begin{tikzcd}
 & A \otimes_R B \arrow[d, dashed, "\tilde{\eta}"] \arrow[dd, dashed, bend left, "id_{A \otimes_R B}"] \\
A \times B \arrow[ur, "h"] \arrow[dr, "h"'] & U \arrow[d, dashed, "h'"] \\
 & A \otimes_R B
\end{tikzcd}$$

comuta. Mas, a identidade $id_{A \otimes_R B}$ também faz o diagrama comutar. Logo, pela unicidade do $\mathbb{Z}$-homomorfismo da definição de produto tensorial temos que $h'\tilde{\eta} = id_{A \otimes_R B}$. Por um argumento similar, temos que $\tilde{\eta}h' = id_U$. Consequentemente, $\tilde{\eta} : A \otimes_R B \to U$ é um isomorfismo. ∎

Para a demonstração da próxima proposição, usaremos o seguinte fato:

Corolário 1.5.1 [24, pág. 66] *Seja $f : M \to N$ uma R-função e K um submódulo de um R-módulo à esquerda M com $K \subseteq \ker f$, então f induz uma R-função*

$$\begin{aligned} \hat{f} : \quad \tfrac{M}{K} &\longrightarrow N \\ m + K &\longmapsto f(m). \end{aligned}$$

Proposição 1.5.4 [24, Proposição 2.45] *Se R é um anel, A_R e ${}_RB$ são módulos, então o produto tensorial $A \otimes_R B$ existe.*

Demonstração: Seja F um grupo abeliano livre com base $A \times B$, isto é, F é livre em todos os pares ordenados (a, b) com $a \in A$ e $b \in B$. Definimos S como sendo o subgrupo de F gerado por todos os elementos do seguinte tipo:

$$(a, b + b') - (a, b) - (a, b'),$$

$$(a + a', b) - (a, b) - (a', b),$$

$$(ar, b) - (a, rb).$$

Pela Proposição 1.5.3 é suficiente mostrar que $\frac{F}{S}$ satisfaz as condições de produto tensorial. Denotando a classe $(a, b) + S$ por $a \otimes b$, podemos considerar a seguinte função:

$$\begin{aligned} h : \quad A \times B &\longrightarrow \frac{F}{S} \\ (a, b) &\longmapsto a \otimes b. \end{aligned}$$

Note que h é a restrição do homomorfismo canônico $\psi : F \to \frac{F}{S}$ à base $A \times B$ de F. Queremos mostrar que $\frac{F}{S}$ e h satisfazem a definição de produto tensorial. Como

$$(a, b + b') - (a, b) - (a, b') \in S,$$

segue que,

$$a \otimes (b + b') = a \otimes b + a \otimes b'.$$

Como

$$(a + a', b) - (a, b) - (a', b) \in S,$$

temos que

$$(a + a') \otimes b = a \otimes b + a' \otimes b.$$

Da mesma forma, como

$$(ar, b) - (a, rb) \in S$$

segue que

$$ar \otimes b = a \otimes rb.$$

Consequentemente, h é R-biaditiva. Agora, sejam G um grupo abeliano qualquer, $f : A \times B \to G$ uma função R-biaditiva, e seja $i : A \times B \to F$ a função inclusão. Dado que F

é abeliano livre com base $A \times B$, pela Proposição 1.5.2, existe um único homomorfismo $\varphi : F \to G$ tal que $\varphi(a,b) = f(a,b)$, para todo $(a,b) \in A \times B$. Segue que $S \subseteq \ker\varphi$, pois f é R-biaditiva. Então, pelo Corolário 1.5.1, φ induz uma R-função $\hat{f} : \frac{F}{S} \to G$ dada por

$$\hat{f}(a \otimes b) = \hat{f}((a,b) + S) = \varphi(a,b) = f(a,b).$$

Logo, $\hat{f}h = f$, isto é, o diagrama

$$\begin{tikzcd} & \frac{F}{S} \arrow[dd, dashed, bend left, "\hat{f}"] \\ A \times B \arrow[ur, "h"] \arrow[r, "i"'] \arrow[dr, "f"'] & F \arrow[u, "\psi"] \arrow[d, dashed, "\varphi"] \\ & G \end{tikzcd}$$

comuta. Mas, dado que $\frac{F}{S}$ é gerado pelo conjunto de todos $a \otimes b$'s, então $\hat{f}$ é o único que estende f. Daí, $(\frac{F}{S}, h)$ é um produto tensorial dos R-módulos A e B, e pela Proposição 1.5.3 segue que $\frac{F}{S} \simeq A \otimes_R B$. ∎

Teorema 1.5.1 [24, Teorema 2.65] *Sejam A um R-módulo à direita e $(B_i)_{i\in I}$ uma família de R-módulos à esquerda. Existe um $Z(R)$-isomorfismo*

$$\begin{aligned} \tau : \quad A \otimes_R (\textstyle\bigoplus_{i\in I} B_i) &\longrightarrow \bigoplus_{i\in I}(A \otimes_R B_i) \\ a \otimes (b_i)_{i\in I} &\longmapsto (a \otimes b_i)_{i\in I}. \end{aligned}$$

Mais ainda, se R é comutativo, então τ é um R-isomorfismo.

A seguir, denotaremos por $\mathbb{Z}_m$ ao grupo abeliano (aditivo) das classes de congruência módulo m em $\mathbb{Z}$.

Proposição 1.5.5 *Sejam m e n números inteiros positivos. Então,*

$$\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \simeq \mathbb{Z}_d,$$

onde $d = mdc(m,n)$.

Demonstração: Pela Proposição 1.5.3, é suficiente mostrar que $\mathbb{Z}_d$ satisfaz as condições para ser o produto tensorial de $\mathbb{Z}_m$ e $\mathbb{Z}_n$. Para isso, definiremos uma aplicação

$$\begin{aligned} \psi : \quad \mathbb{Z}_m \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_d \\ ([x]_m, [y]_n) &\longmapsto [xy]_d, \end{aligned}$$

onde $[z]_k$ é um elemento de $\mathbb{Z}_k$, com $k \in \{m,n,d\}$. Vejamos que ψ é bem definida. De fato, se

$$([x_1]_m, [y_1]_n) = ([x_2]_m, [y_2]_n),$$

então

$$m \mid (x_1 - x_2) \text{ e } n \mid (y_1 - y_2).$$

Como $d = mdc(m, n)$, temos

$$d \mid (x_1 - x_2) \text{ e } d \mid (y_1 - y_2).$$

Em particular,

$$d \mid (x_1 - x_2)y_1 \text{ e } d \mid (y_1 - y_2)x_2.$$

Logo, $d \mid (x_1y_1 - x_2y_2)$ e $[x_1y_1]_d = [x_2y_2]_d$, como queríamos. Além disso, segue da definição usual de soma em $\mathbb{Z}_k$ que ψ é $\mathbb{Z}$-biaditiva. Tomando um grupo abeliano G e uma função $g : \mathbb{Z}_m \times \mathbb{Z}_n \to G$, $\mathbb{Z}$-biaditiva, definiremos uma aplicação

$$\begin{aligned} \eta : \quad \mathbb{Z}_d &\longrightarrow G \\ [x]_d &\longmapsto g([1]_m, [x]_n). \end{aligned}$$

que é um $\mathbb{Z}$-homomorfismo, pois g é $\mathbb{Z}$-biaditiva. Além disso,

$$\eta\psi([x_1]_m, [y_1]_n) = \eta([x_1y_1]_d) = g([1]_m, [x_1y_1]_n) = g([1]_m, x_1[y_1]_n) = g([x_1]_m, [y_1]_n).$$

Agora, se $\tilde{\eta} : \mathbb{Z}_d \to G$ é outro $\mathbb{Z}$-homomorfismo para o qual $\tilde{\eta}\psi = g$, então segue que $\tilde{\eta} = \eta$, pois coincidem nos geradores de $\mathbb{Z}_d$. Portanto, $\mathbb{Z}_d$ satisfaz as condições para ser o produto tensorial de $\mathbb{Z}_m$ e $\mathbb{Z}_n$, e pela Proposição 1.5.3, segue que $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \simeq \mathbb{Z}_d$, para quaisquer inteiros m, n e $d = mdc(m, n)$. ∎

Vejamos alguns exemplos:

Exemplo 1.3 Denotando por C_p o grupo cíclico de ordem p, onde p é um número primo, vamos considerar os seguintes grupos abelianos:

$$G = C_p \times C_p \times C_p \text{ e } H = C_{p^2} \times C_{p^3},$$

Então, pelo Teorema 1.5.1 e pela Proposição 1.5.5, temos:

$$\begin{aligned} G \otimes_{\mathbb{Z}} G &= (C_p \times C_p \times C_p) \otimes_{\mathbb{Z}} (C_p \times C_p \times C_p) \\ &\overset{1.5.1}{\simeq} \underbrace{(C_p \otimes_{\mathbb{Z}} C_p) \times \cdots \times (C_p \otimes_{\mathbb{Z}} C_p)}_{9\, vezes} \\ &\overset{1.5.5}{\simeq} \underbrace{C_p \times C_p \times \cdots \times C_p}_{9\, vezes}. \end{aligned}$$

Em particular, $|G \otimes_{\mathbb{Z}} G| = p^9$. Analogamente,

$$\begin{aligned} H \otimes_{\mathbb{Z}} H &= (C_{p^2} \times C_{p^3}) \otimes_{\mathbb{Z}} (C_{p^2} \times C_{p^3}) \\ &\overset{1.5.1}{\simeq} (C_{p^2} \otimes_{\mathbb{Z}} C_{p^2}) \times (C_{p^2} \otimes_{\mathbb{Z}} C_{p^3}) \times (C_{p^3} \otimes_{\mathbb{Z}} C_{p^2}) \times (C_{p^3} \otimes_{\mathbb{Z}} C_{p^3}) \\ &\overset{1.5.5}{\simeq} C_{p^2} \times C_{p^2} \times C_{p^2} \times C_{p^3}. \end{aligned}$$

Logo, $|H \otimes_{\mathbb{Z}} H| = p^9$. Agora, considere

$$\begin{array}{rcl} G \otimes_{\mathbb{Z}} H & = & (C_p \times C_p \times C_p) \otimes_{\mathbb{Z}} (C_{p^2} \times C_{p^3}) \\ & \overset{1.5.1}{\simeq} & C_p \otimes_{\mathbb{Z}} (C_{p^2} \times C_{p^3}) \times C_p \otimes_{\mathbb{Z}} (C_{p^2} \times C_{p^3}) \times C_p \otimes_{\mathbb{Z}} (C_{p^2} \times C_{p^3}) \\ & \underset{1.5.1}{\overset{1.5.5}{\simeq}} & \underbrace{C_p \times \cdots \times C_p}_{6\, fatores}. \end{array}$$

Desse modo, $|G \otimes_{\mathbb{Z}} H| = p^6$.

Exemplo 1.4 Agora, considerando o grupo diedral D_8 de ordem 8, temos que

$$D_8 = \langle x, y \,|\, x^4 = 1 = y^2\,,\, y^{-1}xy = x^{-1} \rangle.$$

Além disso,

$$D_8' = \Phi(D_8) = Z(D_8) = \langle x^2 \rangle.$$

Logo, segue que

$$D_8' \simeq C_2, \;\; \frac{D_8}{D_8'} \simeq C_2 \times C_2, \;\; \frac{D_8}{\Phi(D_8)} \simeq C_2 \times C_2.$$

Portanto,

$$D_8' \otimes_{\mathbb{Z}} \frac{D_8}{D_8'} \;\; \simeq \;\; C_2 \otimes_{\mathbb{Z}} (C_2 \times C_2) \underset{1.5.1}{\overset{1.5.5}{\simeq}} C_2 \times C_2.$$

$$\frac{D_8}{\Phi(D_8)} \otimes_{\mathbb{Z}} \frac{D_8}{\Phi(D_8)} \;\; \simeq \;\; (C_2 \times C_2) \otimes_{\mathbb{Z}} (C_2 \times C_2) \underset{1.5.1}{\overset{1.5.5}{\simeq}} C_2 \times C_2 \times C_2 \times C_2.$$

$$\frac{D_8}{D_8'} \otimes_{\mathbb{Z}} \frac{D_8}{D_8'} \;\; \simeq \;\; (C_2 \times C_2) \otimes_{\mathbb{Z}} (C_2 \times C_2) \underset{1.5.1}{\overset{1.5.5}{\simeq}} C_2 \times C_2 \times C_2 \times C_2.$$

O próximo exemplo nos mostra que podemos obter o mesmo produto tensorial tomando diferentes grupos abelianos.

Exemplo 1.5 Consideraremos $G = C_p \times C_{p^2}$ e $H = C_p \times C_p$, onde p é um número primo. Então,

$$G \otimes_{\mathbb{Z}} H = (C_p \times C_{p^2}) \otimes_{\mathbb{Z}} (C_p \times C_p) \simeq C_p \times C_p \times C_p \times C_p \;\text{ e }\; H \otimes_{\mathbb{Z}} H \simeq C_p \times C_p \times C_p \times C_p.$$

1.6 Produto Tensorial Não Abeliano de Grupos

Nosso objetivo neste trabalho será desenvolver uma construção relacionada a um conceito mais geral que o produto tensorial de R-módulos, a saber o produto tensorial não abeliano de grupos. Tal construção foi introduzida por R. Brown e J. Loday, em [8], generalizando o produto tensorial usual $G_{ab} \otimes_{\mathbb{Z}} H_{ab}$ de grupos abelianizados, assumindo que um age sobre o outro compativelmente. Mais especificamente,

Definição 1.6.1 *Sejam G e H grupos e considere as ações (à direita)*

$$\begin{array}{rccc} \phi_1: & G\times H & \longrightarrow & G \\ & (g,h) & \longmapsto & \phi_1(g,h)=g^h \end{array} \quad , \quad \begin{array}{rccc} \phi_2: & H\times G & \longrightarrow & H \\ & (h,g) & \longmapsto & \phi_2(h,g)=h^g \end{array}$$

compatíveis, isto é, para todos $g, g_1 \in G$ e $h, h_1 \in H$, temos que

$$g^{(h^{g_1})} = \left((g^{g_1^{-1}})^h\right)^{g_1} \quad e \quad h^{(g^{h_1})} = \left((h^{h_1^{-1}})^g\right)^{h_1}, \tag{1.12}$$

*onde G e H agem sobre si mesmos por conjugação. Então, o **produto tensorial não abeliano** $G\otimes H$ é o grupo gerado pelos símbolos $g\otimes h$ (chamados de tensores), com $g\in G$, $h\in H$, satisfazendo as seguintes relações:*

$$gg_1\otimes h = (g^{g_1}\otimes h^{g_1})(g_1\otimes h), \quad g\otimes hh_1 = (g\otimes h_1)(g^{h_1}\otimes h^{h_1}), \tag{1.13}$$

para todos $g, g_1 \in G$, $h, h_1 \in H$, onde a ação de G sobre si mesmo é a conjugação $g^{g_1} = g_1^{-1}gg_1$, e analogamente para H.

Cabe ressaltar as semelhanças entre as relações (1.13) e as regras envolvendo comutadores, a saber:

$$[xy,z] = [x^y, z^y][y,z] \text{ e } [x,yz] = [x,z][x^z,y^z],$$

onde x, y e z são elementos genéricos de um grupo G. Além disso, como a ação por conjugação de um grupo G em si mesmo

$$\begin{array}{rccc} \phi: & G\times G & \longrightarrow & G \\ & (g,h) & \longmapsto & g^h = h^{-1}gh, \end{array}$$

satisfaz (1.12), o grupo $G\otimes G$ pode ser sempre definido. O grupo $G\otimes G$ é chamado de *quadrado tensorial não abeliano* de G.

Supondo que G e H agem compativelmente um sobre o outro, e além disso, considerando que G e H agem trivialmente um sobre o outro, isto é, $g_1^h = g_1$ e $h_1^g = h_1$ para todos $g, g_1 \in G, h, h_1 \in H$, então o produto tensorial não abeliano de G e H, $G\otimes H$ é isomorfo ao produto tensorial usual de $\mathbb{Z}$-módulos $G_{ab}\otimes_{\mathbb{Z}} H_{ab}$. Para mostrarmos isso, necessitamos de algumas propriedades encontradas em [7] e [8], e assumiremos que G e H agem compativelmente um sobre o outro e sobre si mesmos por conjugação.

Definição 1.6.2 *Sejam G, H e L grupos, onde G e H agem compativelmente um sobre o outro e sobre si mesmos por conjugação. Dizemos que uma aplicação $\theta: G\times H\to L$ é uma **biderivação** se satisfazer o seguinte:*

$$\theta(gg_1,h) = \theta(g^{g_1},h^{g_1})\theta(g_1,h) \quad e \quad \theta(g,hh_1) = \theta(g,h_1)\theta(g^{h_1},h^{h_1}), \tag{1.14}$$

para todos $g, g_1\in G$, $h, h_1\in H$.

Exemplo 1.6 Como a ação de G por conjugação sobre si mesmo é compatível, consideremos a seguinte aplicação:

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

Usando as relações de comutadores [Proposição 1.2.1], podemos verificar que a aplicação acima é uma biderivação.

Observação 1.2 Usando o Teste da Substituição 1.4.4, podemos verificar que a biderivação $\theta : G\times H \to L$ se estende para um único homomorfismo $\theta^* : G\otimes H \to L$ tal que $\theta^*(g\otimes h) = \theta(g,h)$, para todos $g\in G, h\in H$.

Proposição 1.6.1 [8, Proposição 2.3] *Os grupos G e H agem sobre $G\otimes H$ da seguinte maneira:*

$$(g\otimes h)^{g_1} = g^{g_1}\otimes h^{g_1}, \quad (g\otimes h)^{h_1} = g^{h_1}\otimes h^{h_1},$$

para todos $g, g_1 \in G, h, h_1 \in H$. Com isso, temos uma ação do produto livre $G * H$ sobre $G\otimes H$ dada por

$$(g\otimes h)^x = g^x \otimes h^x$$

para todos $g\in G, h\in H$ e $x\in G*H$.

Demonstração: Vamos construir um homomorfismo $\beta : G \to Aut(G\otimes H)$, onde $Aut(G\otimes H)$ denota o grupo de todos os automorfismos de $G\otimes H$. Para isso, consideramos a função

$$\begin{array}{rccc}\theta_{g_1}: & G\times H & \longrightarrow & G\otimes H\\ & (g,h) & \longmapsto & g^{g_1}\otimes h^{g_1},\end{array}$$

que é uma biderivação, pois, tomando quaisquer $g_1, g_2, g_3 \in G$ e $h\in H$, temos que

$$\begin{array}{rcl}\theta_{g_1}(g_2g_3,h) & = & (g_2g_3)^{g_1}\otimes h^{g_1}\\ & = & g_2^{g_1}g_3^{g_1}\otimes h^{g_1}\\ & \overset{(1.13)}{=} & ((g_2^{g_1})^{g_3^{g_1}}\otimes (h^{g_1})^{g_3^{g_1}})(g_3^{g_1}\otimes h^{g_1})\\ & = & (g_2^{g_3g_1}\otimes h^{g_3g_1})(g_3^{g_1}\otimes h^{g_1})\\ & = & \theta_{g_1}(g_2^{g_3}, h^{g_3})\theta_{g_1}(g_3,h).\end{array}$$

Analogamente, temos $\theta_{g_1}(g,hh_1) = \theta_{g_1}(g,h_1)\theta_{g_1}(g^{h_1},h^{h_1})$, para todos $g\in G, h, h_1\in H$. Portanto, pela Observação 1.2, θ_{g_1} se estende para um único homomorfismo $\theta^*_{g_1} : G\otimes H \to G\otimes H$, tal que $\theta^*_{g_1}(g\otimes h) = \theta_{g_1}(g,h)$. Em particular, $\theta^*_{g_1}$ é uma bijeção, pois $\theta^*_{g_1}\theta^*_{g_1^{-1}} = id_{G\otimes H} = \theta^*_{g_1^{-1}}\theta^*_{g_1}$. Segue que, $\theta^*_{g_1}$ é um automorfismo de $G\otimes H$. Agora, uma verificação direta nos mostra que a aplicação $\beta : G\to Aut(G\otimes H)$, dada por $\beta(g_1) = \theta^*_{g_1}$, é um homomorfismo, para todo $g_1\in G$. Analogamente se mostra a existência de um homomorfismo $\alpha : H \to Aut(G\otimes H)$. ∎

A seguir veremos algumas relações computacionais que são satisfeitas no produto tensorial não abeliano $G \otimes H$.

Proposição 1.6.2 [7, Proposição 3] *Para todos $g, g_1 \in G$ e $h, h_1 \in H$, temos as seguintes relações:*
(i) $(g^{-1} \otimes h)^g = (g \otimes h)^{-1} = (g \otimes h^{-1})^h$;
(ii) $(g \otimes h)^{-1}(g_1 \otimes h_1)(g \otimes h) = (g_1 \otimes h_1)^{[g,h]} = (g_1 \otimes h_1)^{g^{-1}g^h} = (g_1 \otimes h_1)^{h^{-g}h}$;
(iii) $g^{-1}g^h \otimes h_1 = (g \otimes h)^{-1}(g \otimes h)^{h_1}$ *e* $g_1 \otimes h^{-g}h = (g \otimes h)^{-g_1}(g \otimes h)$;
(iv) $[g \otimes h, g_1 \otimes h_1] = g^{-1}g^h \otimes h^{-g_1}h_1$.

Demonstração: (i) Antes de mostrarmos este item, verificaremos que o elemento neutro $1_{G\otimes H}$ de $G \otimes H$ pode ser dado por $1 \otimes h$ ou $g \otimes 1$. De fato,

$$(g \otimes h)1_{G\otimes H} = (g1 \otimes h) \overset{(1.13)}{=} (g^1 \otimes h^1)(1 \otimes h) = (g \otimes h)(1 \otimes h),$$

implica que $1_{G\otimes H} = 1 \otimes h$. Analogamente, mostra-se que $1_{G\otimes H} = g \otimes 1$. Continuando a demonstração, vejamos que para todos $g \in G, h \in H$,

$$1 \otimes h \;=\; g^{-1}g \otimes h \overset{(1.13)}{=} ((g^{-1})^g \otimes h^g)(g \otimes h) \overset{(1.6.1)}{=} (g^{-1} \otimes h)^g(g \otimes h).$$

Analogamente,

$$g \otimes 1 \;=\; g \otimes h^{-1}h = (g \otimes h)(g^h \otimes (h^{-1})^h) = (g \otimes h)(g \otimes h^{-1})^h.$$

De modo que, $(g^{-1} \otimes h)^g = (g \otimes h)^{-1} = (g \otimes h^{-1})^h$.
(ii) Tomando $m, n \in G$ e $a, b \in H$, segue da Proposição 1.6.1 que

$$\begin{aligned} mn \otimes ab &= (m \otimes ab)^n(n \otimes ab) = ((m \otimes b)(m \otimes a)^b)^n(n \otimes b)(n \otimes a)^b \\ &= (m \otimes b)^n(m \otimes a)^{bn}(n \otimes b)(n \otimes a)^b. \end{aligned}$$

Por outro lado,

$$mn \otimes ab \;=\; (mn \otimes b)(mn \otimes a)^b = (m \otimes b)^n(n \otimes b)(m \otimes a)^{nb}(n \otimes a)^b.$$

Comparando as duas últimas igualdades, temos

$$(m \otimes a)^{bn}(n \otimes b) = (n \otimes b)(m \otimes a)^{nb}. \tag{1.15}$$

Agora, para $g, g_1 \in G, h, h_1 \in H$, consideramos $m = g_1^{g^{-1}h^{-1}}, n = g, a = h_1^{g^{-1}h^{-1}}$ e $b = h$ na igualdade (1.15). Desse modo,

$$(g_1^{g^{-1}h^{-1}} \otimes h_1^{g^{-1}h^{-1}})^{hg}(g \otimes h) = (g \otimes h)(g_1^{g^{-1}h^{-1}} \otimes h_1^{g^{-1}h^{-1}})^{gh}.$$

Novamente pela Proposição 1.6.1,

$$(g_1 \otimes h_1)(g \otimes h) = (g \otimes h)(g_1 \otimes h_1)^{[g,h]}.$$

Consequentemente,

$$(g \otimes h)^{-1}(g_1 \otimes h_1)(g \otimes h) = (g_1 \otimes h_1)^{[g,h]}. \tag{1.16}$$

Agora, como G e H agem sobre si mesmos por conjugação, segue que

$$g_1^{[g,h]} \;=\; g_1^{g^{-1}h^{-1}gh} = \left(\left(g_1^{g^{-1}h^{-1}}\right)^g\right)^h = \left(g^{-1}(g_1^{g^{-1}h^{-1}})g\right)^h = g^{-h}(g_1^{g^{-1}h^{-1}h})g^h = g_1^{g^{-1}g^h}.$$

Como as ações são compatíveis,

$$h_1^{[g,h]} \;=\; h_1^{g^{-1}h^{-1}gh} = (h_1^{g^{-1}})^{h^{-1}gh} = (h_1^{g^{-1}})^{g^h} = h_1^{g^{-1}g^h}.$$

Portanto, usando também a Proposição 1.6.1, segue que

$$(g_1 \otimes h_1)^{[g,h]} = g_1^{[g,h]} \otimes h_1^{[g,h]} = g_1^{g^{-1}g^h} \otimes h_1^{g^{-1}g^h} = (g_1 \otimes h_1)^{g^{-1}g^h}.$$

Semelhantemente, $(g_1 \otimes h_1)^{[g,h]} = (g_1 \otimes h_1)^{h^{-g}h}$. Como queríamos demonstrar.
(iii) Para todos $g \in G, h, h_1 \in H$, vale que

$$\begin{aligned}
g^{-1}g^h \otimes h_1 &= (g^{-h^{-1}}g \otimes h_1^{h^{-1}})^h \\
&= [(g^{-h^{-1}} \otimes h_1^{h^{-1}})^g (g \otimes h_1^{h^{-1}})]^h \\
&= [(g^{-1} \otimes h_1)^{h^{-1}g}(g \otimes hh_1h^{-1})]^h \\
&= [(g^{-1} \otimes h_1)^{h^{-1}g}(g \otimes h^{-1})(g \otimes hh_1)^{h^{-1}}]^h \\
&= (g^{-1} \otimes h_1)^{h^{-1}gh}(g \otimes h^{-1})^h(g \otimes hh_1)^{h^{-1}h} \\
&\overset{(i)}{=} (g^{-1} \otimes h_1)^{gg^{-1}h^{-1}gh}(g \otimes h)^{-1}(g \otimes hh_1) \\
&\overset{(i)}{=} (g \otimes h_1)^{-[g,h]}(g \otimes h)^{-1}(g \otimes h_1)(g \otimes h)^{h_1} \\
&\overset{(ii)}{=} (g \otimes h)^{-1}(g \otimes h_1)^{-1}(g \otimes h)(g \otimes h)^{-1}(g \otimes h_1)(g \otimes h)^{h_1} \\
&= (g \otimes h)^{-1}(g \otimes h)^{h_1}.
\end{aligned}$$

O outro caso é análogo.
(iv) Para todos $g, g_1 \in G, h, h_1 \in H$, temos que

$$\begin{aligned}
[g \otimes h, g_1 \otimes h_1] &= (g \otimes h)^{-1}(g_1 \otimes h_1)^{-1}(g \otimes h)(g_1 \otimes h_1) \\
&\overset{(ii)}{=} (g \otimes h)^{-1}(g \otimes h)^{h_1^{-g_1}h_1} \\
&\overset{(iii)}{=} (g^{-1}g^h \otimes h_1^{-g_1}h_1).
\end{aligned}$$

A demonstração segue. ∎

Proposição 1.6.3 [8, Proposição 2.3] *(i) Existem homomorfismos* $\lambda : G \otimes H \to G$ *e* $\lambda' : G \otimes H \to H$*, dados por*

$$\lambda(g \otimes h) = g^{-1}g^h \quad e \quad \lambda'(g \otimes h) = h^{-g}h;$$

(ii) Se $g \in G$*,* $h \in H$ *e* $t \in G \otimes H$*, então* $\lambda(t) \otimes h = t^{-1}t^h$ *e* $g \otimes \lambda'(t) = t^{-g}t$*;*
(iii) As ações de G *sobre* $\ker \lambda'$ *e de* H *sobre* $\ker \lambda$ *são triviais.*

Demonstração: (i) Iremos mostrar a existência do homomorfismo λ. Para isso, consideremos a aplicação

$$\begin{array}{rccc} \theta: & G \times H & \longrightarrow & G \\ & (g,h) & \longmapsto & g^{-1}g^h, \end{array}$$

e vejamos que θ é uma biderivação. De fato, considerando $g, g_1 \in G$ e $h \in H$, temos

$$\begin{array}{rcl} \theta(gg_1, h) & = & (gg_1)^{-1}(gg_1)^h \\ & = & g_1^{-1}g^{-1}g^h g_1^h \\ & = & g_1^{-1}g^{-1}g_1g_1^{-1}g^h g_1 g_1^{-1} g_1^h \\ & = & (g^{g_1})^{-1}(g^h)^{g_1}g_1^{-1}g_1^h \\ & = & (g^{g_1})^{-1}((g^{g_1g_1^{-1}})^h)^{g_1}g_1^{-1}g_1^h \\ & \overset{(1.12)}{=} & (g^{g_1})^{-1}(g^{g_1})^{(h^{g_1})}g_1^{-1}g_1^h \\ & = & \theta(g^{g_1}, h^{g_1})\theta(g_1, h). \end{array}$$

Semelhantemente, mostra-se que

$$\theta(g, hh_1) = \theta(g, h_1)\theta(g^{h_1}, h^{h_1}),$$

para todos $g \in G$, $h, h_1 \in H$. Portanto, pela Observação 1.2, existe um único homomorfismo $\lambda : G \otimes H \to G$, tal que $\lambda(g \otimes h) = \theta(g, h) = g^{-1}g^h$. O caso para a existência de λ' é análogo.

(ii) Segue diretamente do item (iii) da Proposição 1.6.2.

(iii) Tomando $t \in \ker \lambda'$ e $g \in G$, pelo item (ii) segue que

$$1_{G\otimes H} = g \otimes \lambda'(t) = t^{-g}t.$$

Portanto, $t^g = t$, para todo $g \in G$. Logo, a ação de G em $\ker \lambda'$ é trivial. O outro caso é análogo. ■

Teorema 1.6.1 [8, Proposição 2.4] *Sejam G e H grupos, agindo trivialmente um sobre o outro. Então,*

$$G \otimes H \simeq G_{ab} \otimes_{\mathbb{Z}} H_{ab}.$$

Demonstração: Dados que G e H agem trivialmente um sobre o outro, segue do item (iv) da Proposição 1.6.2 que $G \otimes H$ é abeliano. Além disso, considerando os homomorfismos λ e λ' dados na proposição anterior segue que $G \otimes H = \ker \lambda = \ker \lambda'$. Logo, pelo item (iii) da proposição anterior, segue que G e H agem trivialmente em $G \otimes H$. Devido a unicidade do produto tensorial de $\mathbb{Z}$-módulos [Proposição 1.5.3], mostraremos que $G \otimes H$ satisfaz a Definição 1.5.8. Para isso, consideraremos a aplicação

$$\begin{array}{rccc} \theta: & G_{ab} \times H_{ab} & \longrightarrow & G \otimes H \\ & (\overline{g}, \overline{h}) & \longmapsto & g \otimes h, \end{array}$$

que é bem definida, pois se $\overline{g} = \overline{g_1}$, para algum $g_1 \in G$ e $\overline{h} = \overline{h_1}$, para algum $h_1 \in H$, então, existem $x \in G'$ e $y \in H'$, tais que $g = xg_1$ e $h = yh_1$. Portanto, como G e H agem trivialmente em $G \otimes H$ e $G \otimes H$ é abeliano, usando o item (i) da Proposição 1.6.2, temos que $[m, m_1] \otimes n = m \otimes [n, n_1] = 1$ para todos $m, m_1 \in G$, $n, n_1 \in H$. Consequentemente,

$$\begin{aligned} g \otimes h &= xg_1 \otimes yh_1 \\ &= (x \otimes yh_1)^{g_1}(g_1 \otimes yh_1) \\ &= (x \otimes h_1)^{g_1}(x \otimes y)^{h_1 g_1}(g_1 \otimes h_1)(g_1 \otimes y)^{h_1} \\ &= (x \otimes h_1)(x \otimes y)(g_1 \otimes h_1)(g_1 \otimes y) \\ &= (g_1 \otimes h_1). \end{aligned}$$

De modo que θ está bem definida. Novamente, pelo fato de G e H agirem trivialmente em $G \otimes H$ segue que θ é $\mathbb{Z}$-biaditiva. Agora, suponhamos que $f : G_{ab} \times H_{ab} \to M$ é uma aplicação $\mathbb{Z}$-biaditiva qualquer, onde M é um grupo abeliano. Queremos construir uma $\mathbb{Z}$-função $\tilde{f} : G \otimes H \to M$ tal que sua restrição na base $G_{ab} \times H_{ab}$ é igual ao valor f. Para isso, definimos uma aplicação

$$\begin{array}{rccc} f' : & G \times H & \longrightarrow & M \\ & (g, h) & \longmapsto & f(\overline{g}, \overline{h}), \end{array}$$

que, por sua vez, é uma biderivação, pois f é $\mathbb{Z}$-biaditiva, G_{ab} e H_{ab} são abelianos, e G e H agem trivialmente um sobre o outro. Portanto, pela Observação 1.2, existe um único homomorfismo $\tilde{f} : G \otimes H \to M$ tal que $\tilde{f}(g \otimes h) = f'(g, h) = f(\overline{g}, \overline{h})$. Portanto, $G \otimes H$ satisfaz a definição de produto tensorial de $\mathbb{Z}$-módulos. Em particular, $G_{ab} \otimes_{\mathbb{Z}} H_{ab} \simeq G \otimes H$, como queríamos demonstrar. ∎

Observação 1.3 O nosso estudo ficará restrito ao quadrado tensorial não abeliano de grupos $G \otimes G$. Para uma abordagem mais completa sobre produtos tensoriais não abelianos de grupos veja, por exemplo, [1], [2], [4], [11], [19].

Capítulo 2

O Grupo $\nu(G)$

Neste capítulo apresentaremos os resultados encontrados em [21] sobre o grupo $\nu(G)$. Este grupo é um quociente do produto livre $G * G^{\varphi}$, onde φ é um isomorfismo de grupos. Além disso, ele é uma extensão de um subgrupo isomorfo ao quadrado tensorial não abeliano de grupos $G \otimes G$ e mostrou possuir vantagens computacionais para o estudo deste último grupo.

2.1 Definição e Propriedades

Nesta seção, temos por objetivo apresentar o grupo $\nu(G)$ e algumas propriedades. Além disso, definiremos o subgrupo $\Upsilon(G)$ que, além de ser normal em $\nu(G)$, é também isomorfo ao quadrado tensorial não abeliano $G \otimes G$ (como veremos a seguir).

Definição 2.1.1 *Sejam G e G^{φ} grupos isomorfos através de um isomorfismo $\varphi : G \to G^{\varphi}$ dado por $g \mapsto g^{\varphi}$. Definimos o grupo*

$$\nu(G) := \langle G \cup G^{\varphi} \mid [g_1, g_2^{\varphi}]^{g_3} = [g_1^{g_3}, (g_2^{g_3})^{\varphi}] = [g_1, g_2^{\varphi}]^{g_3^{\varphi}}, \forall\, g_1, g_2, g_3 \in G\rangle. \tag{2.1}$$

A seguir, listaremos algumas propriedades computacionais do grupo $\nu(G)$ que serão constantemente utilizadas nas demonstrações dos próximos resultados. Aqui, assumiremos que o leitor possui alguma familiaridade com propriedades usuais de comutadores, em especial, com as que foram descritas na Proposição 1.2.1.

Lema 2.1.1 *No grupo $\nu(G)$ valem as seguintes relações:*
(i) $[g_1, g_2^{\varphi}]^{[g_3^{\varphi}, g_4^{\varphi}]} = [g_1, g_2^{\varphi}]^{[g_3, g_4^{\varphi}]} = [g_1, g_2^{\varphi}]^{[g_3, g_4]} = [g_1, g_2^{\varphi}]^{[g_3^{\varphi}, g_4]}, \forall\, g_1, g_2, g_3, g_4 \in G$;
(ii) Para quaisquer elementos $g_1, g_2, g_3 \in G$, temos

$$[g_1, g_2^{\varphi}, g_3] = [g_1, g_2, g_3^{\varphi}] = [g_1^{\varphi}, g_2, g_3] = [g_1, g_2^{\varphi}, g_3^{\varphi}] = [g_1^{\varphi}, g_2, g_3^{\varphi}] = [g_1^{\varphi}, g_2^{\varphi}, g_3];$$

(iii) $[g, g^{\varphi}]$ *é central em* $\nu(G), \forall\, g \in G$;
(iv) $[g_1, g_2^{\varphi}][g_2, g_1^{\varphi}]$ *é central em* $\nu(G), \forall\, g_1, g_2 \in G$;
(v) $[c, c^{\varphi}] = 1, \forall\, c \in G'$;
(vi) $[c, g^{\varphi}][g, c^{\varphi}] = 1$, $\forall\, g \in G, c \in G'$.

Demonstração: *(i)* Para quaisquer elementos $g_1, g_2, g_3, g_4 \in G$, usando as relações (2.1) que definem o grupo $\nu(G)$, temos

$$\begin{array}{rcl} [g_1, g_2^{\varphi}]^{[g_3, g_4^{\varphi}]} & = & [g_1, g_2^{\varphi}]^{g_3^{-1} g_4^{-\varphi} g_3 g_4^{\varphi}} \\ & \overset{(2.1)}{=} & [g_1^{g_3^{-1}}, (g_2^{g_3^{-1}})^{\varphi}]^{g_4^{-\varphi} g_3 g_4^{\varphi}} \\ & = & [g_1^{g_3^{-1} g_4^{-1} g_3 g_4}, (g_2^{g_3^{-1} g_4^{-1} g_3 g_4})^{\varphi}] \\ & \overset{(2.1)}{=} & [g_1, g_2^{\varphi}]^{[g_3, g_4]}. \end{array}$$

Analogamente, as demais igualdades se mantêm.
(ii) Para todos $g_1, g_2, g_3 \in G$, usando as relações da Proposição 1.2.1, as relações (2.1) que definem o grupo $\nu(G)$ e o item anterior, temos

$$\begin{array}{rcl} [g_1, g_2, g_3^{\varphi}] & = & [g_1^{-1} g_1^{g_2}, g_3^{\varphi}] \\ & = & [g_1^{-1}, g_3^{\varphi}]^{g_1^{g_2}} [g_1^{g_2}, g_3^{\varphi}] \\ & \overset{(2.1)}{=} & [g_1, g_3^{\varphi}]^{-g_1^{-1} g_1^{g_2}} [g_1, (g_3^{g_2^{-1}})^{\varphi}]^{g_2^{\varphi}} \\ & \overset{2.1.1\,(i)}{=} & [g_1, g_3^{\varphi}]^{-[g_1, g_2^{\varphi}]} [g_1, (g_2 g_3 g_2^{-1})^{\varphi}]^{g_2^{\varphi}} \\ & = & [g_1, g_3^{\varphi}]^{-[g_1, g_2^{\varphi}]} [g_1, (g_2^{-1})^{\varphi}]^{g_2^{\varphi}} [g_1, (g_2 g_3)^{\varphi}]^{g_2^{-\varphi} g_2^{\varphi}} \\ & = & [g_1, g_3^{\varphi}]^{-[g_1, g_2^{\varphi}]} [g_1, g_2^{\varphi}]^{-g_2^{-\varphi} g_2^{\varphi}} [g_1, g_3^{\varphi}][g_1, g_2^{\varphi}]^{g_3^{\varphi}} \\ & = & [g_1, g_3^{\varphi}]^{-[g_1, g_2^{\varphi}]} [g_1, g_2^{\varphi}]^{-1} [g_1, g_3^{\varphi}][g_1, g_2^{\varphi}]^{g_3^{\varphi}} \\ & = & [g_1, g_2^{\varphi}]^{-1} [g_1, g_2^{\varphi}]^{g_3^{\varphi}} \\ & = & [g_1, g_2^{\varphi}, g_3^{\varphi}]. \end{array}$$

Mais ainda,

$$\begin{array}{rcl} [g_1, g_2^{\varphi}, g_3^{\varphi}] & = & [g_1, g_2^{\varphi}]^{-1} [g_1, g_2^{\varphi}]^{g_3^{\varphi}} \\ & \overset{(2.1)}{=} & [g_1, g_2^{\varphi}]^{-1} [g_1, g_2^{\varphi}]^{g_3} \\ & = & [g_1, g_2^{\varphi}, g_3]. \end{array}$$

Portanto, $[g_1, g_2, g_3^{\varphi}] = [g_1, g_2^{\varphi}, g_3^{\varphi}] = [g_1, g_2^{\varphi}, g_3]$, para todos $g_1, g_2, g_3 \in G$. Agora, como

$$[g_1^{\varphi}, g_2] = ([g_2, g_1^{\varphi}])^{-1} \in \nu(G),$$

então, para qualquer $g \in G$,

$$[g_1^{\varphi}, g_2]^g = ([g_2, g_1^{\varphi}]^g)^{-1} \overset{(2.1)}{=} ([g_2^g, (g_1^g)^{\varphi}])^{-1} = [(g_1^g)^{\varphi}, g_2^g].$$

Analogamente,

$$[g_1^{\varphi}, g_2]^{g^{\varphi}} = [(g_1^{g})^{\varphi}, g_2^{g}].$$

Portanto, segue que

$$\begin{aligned}
[g_1^{\varphi}, g_2^{\varphi}, g_3] &= [g_1^{-\varphi}(g_1^{g_2})^{\varphi}, g_3] \\
&= [g_1^{-\varphi}, g_3]^{(g_1^{g_2})^{\varphi}}[(g_1^{g_2})^{\varphi}, g_3] \\
&\overset{(2.1)}{=} [g_1^{\varphi}, g_3]^{-[g_1^{\varphi}, g_2^{\varphi}]}[g_1^{\varphi}, g_3^{g_2^{-1}}]^{g_2} \\
&= [g_1^{\varphi}, g_3]^{-([g_1, g_2])^{\varphi}}[g_1^{\varphi}, g_2g_3g_2^{-1}]^{g_2} \\
&\overset{2.1.1\,(i)}{=} [g_1^{\varphi}, g_3]^{-[g_1^{\varphi}, g_2]}[g_1^{\varphi}, g_2^{-1}]^{g_2}[g_1^{\varphi}, g_2g_3] \\
&= [g_1^{\varphi}, g_3]^{-[g_1^{\varphi}, g_2]}[g_1^{\varphi}, g_2]^{-g_2^{-1}g_2}[g_1^{\varphi}, g_3][g_1^{\varphi}, g_2]^{g_3} \\
&= [g_1^{\varphi}, g_3]^{-[g_1^{\varphi}, g_2]}[g_1^{\varphi}, g_2]^{-1}[g_1^{\varphi}, g_3][g_1^{\varphi}, g_2]^{g_3} \\
&= [g_1^{\varphi}, g_2]^{-1}[g_1^{\varphi}, g_2]^{g_3} \\
&= [g_1^{\varphi}, g_2, g_3].
\end{aligned}$$

Além disso,

$$\begin{aligned}
[g_1^{\varphi}, g_2, g_3] &= [g_1^{\varphi}, g_2]^{-1}[g_1^{\varphi}, g_2]^{g_3} \\
&\overset{(2.1)}{=} [g_1^{\varphi}, g_2]^{-1}[g_1^{\varphi}, g_2]^{g_3^{\varphi}} \\
&= [g_1^{\varphi}, g_2, g_3^{\varphi}].
\end{aligned}$$

Portanto, $[g_1^{\varphi}, g_2^{\varphi}, g_3] = [g_1^{\varphi}, g_2, g_3] = [g_1^{\varphi}, g_2, g_3^{\varphi}]$, para todos $g_1, g_2, g_3 \in G$. Agora, vejamos que

$$\begin{aligned}
[g_1^{\varphi}, g_2, g_3] &= [[g_2, g_1^{\varphi}]^{-1}, g_3] \\
&= [g_2, g_1^{\varphi}, g_3]^{-[g_2, g_1^{\varphi}]^{-1}} \\
&\overset{2.1.1\,(ii)}{=} [g_2, g_1, g_3^{\varphi}]^{-[g_2, g_1^{\varphi}]^{-1}} \\
&\overset{2.1.1\,(i)}{=} [g_2, g_1, g_3^{\varphi}]^{-[g_2, g_1]^{-1}} \\
&\overset{1.2.1\,(i)}{=} [g_1, g_2, g_3^{\varphi}].
\end{aligned}$$

Assim, concluímos a demonstração do item (ii).
(iii) Dado $g \in G$, segue do item anterior que

$$[g, g^{\varphi}, h^{\varphi}] = [g, g, h^{\varphi}] = 1 = [g, g^{\varphi}, h], \quad \forall\, h \in G.$$

De modo que $[g, g^{\varphi}]$ comuta com os geradores de $\nu(G)$. Portanto, $[g, g^{\varphi}] \in Z(\nu(G))$ para todo $g \in G$.
(iv) Pelo item anterior, $[g_1g_2, (g_1g_2)^{\varphi}]$, $[g_1, g_1^{\varphi}]$ e $[g_2, g_2^{\varphi}]$ são centrais em $\nu(G)$, para todos $g_1, g_2 \in G$. Entretanto,

$$\begin{aligned}
[g_1g_2, (g_1g_2)^{\varphi}] &= [g_1, (g_1g_2)^{\varphi}]^{g_2}[g_2, (g_1g_2)^{\varphi}] \\
&= [g_1, g_2^{\varphi}]^{g_2}[g_1, g_1^{\varphi}]^{g_2^{\varphi}g_2}[g_2, g_2^{\varphi}][g_2, g_1^{\varphi}]^{g_2^{\varphi}} \\
&\overset{(2.1)}{=} [g_1, g_2^{\varphi}]^{g_2^{\varphi}}[g_1, g_1^{\varphi}][g_2, g_2^{\varphi}][g_2, g_1^{\varphi}]^{g_2^{\varphi}} \\
&= ([g_1, g_2^{\varphi}][g_2, g_1^{\varphi}])^{g_2^{\varphi}}[g_1, g_1^{\varphi}][g_2, g_2^{\varphi}]
\end{aligned}$$

Portanto,

$$[g_1g_2, (g_1g_2)^{\varphi}][g_2, g_2^{\varphi}]^{-1}[g_1, g_1^{\varphi}]^{-1} = ([g_1, g_2^{\varphi}][g_2, g_1^{\varphi}])^{g_2^{\varphi}} \in Z(\nu(G)).$$

Daí, conjugando por $g_2^{-\varphi}$, concluiremos que

$$[g_1, g_2^{\varphi}][g_2, g_1^{\varphi}] \in Z(\nu(G)).$$

O resultado segue.
(v) Dado $c \in G'$, com $c = \prod_{i=1}^{n}[x_i, y_i]$, usaremos indução em n e os itens (i) e (ii) do Lema 2.1.1. Assim, para $n = 1$, segue que

$$[[x_1, y_1], [x_1, y_1]^{\varphi}] \overset{(ii)}{=} [[x_1, y_1^{\varphi}], [x_1, y_1]] = [x_1, y_1^{\varphi}]^{-1}[x_1, y_1^{\varphi}]^{[x_1,y_1]} \overset{(i)}{=} [x_1, y_1^{\varphi}]^{-1}[x_1, y_1^{\varphi}]^{[x_1,y_1^{\varphi}]} = 1.$$

Agora, suponhamos como hipótese de indução que, para algum $n \geq 1$,

$$\left[\prod_{i=1}^{n}[x_i, y_i], \prod_{i=1}^{n}[x_i, y_i]^{\varphi}\right] = 1.$$

Então,

$$\left[\prod_{i=1}^{n+1}[x_i, y_i], \prod_{i=1}^{n+1}[x_i, y_i]^{\varphi}\right] = \left[\prod_{i=1}^{n+1}[x_i, y_i], [x_{n+1}, y_{n+1}]^{\varphi}\right]\left[\prod_{i=1}^{n+1}[x_i, y_i], \prod_{i=1}^{n}[x_i, y_i]^{\varphi}\right]^{[x_{n+1},y_{n+1}]^{\varphi}}.$$

Usando o item (ii) da Proposição 1.2.1, o item (i) do Lema 2.1.1, e a hipótese de indução, esta última igualdade se torna

$$\left[\prod_{i=1}^{n}[x_i, y_i], [x_{n+1}, y_{n+1}]^{\varphi}\right]^{[x_{n+1},y_{n+1}^{\varphi}]}\left[[x_{n+1}, y_{n+1}], \prod_{i=1}^{n}[x_i, y_i]^{\varphi}\right]^{[x_{n+1},y_{n+1}^{\varphi}]}. \tag{2.2}$$

Portanto, pelo item (iv) do Lema 2.1.1, a equação (2.2) se reduz a

$$[x_{n+1}, y_{n+1}^{\varphi}]^{-1}[x_{n+1}, y_{n+1}^{\varphi}] = 1.$$

Assim, concluímos a demonstração de *(v)*.
(vi) Agora vamos considerar $g \in G$ e $c \in G'$ com $c = \prod_{i=1}^{r}[x_i, y_i]$. Mostraremos, por indução em r, que $[c, g^{\varphi}][g, c^{\varphi}] = 1$. Assim, pelo item (ii) do Lema 2.1.1, se $r = 1$, temos

$$[[x_1, y_1], g^{\varphi}][g, [x_1, y_1]^{\varphi}] \quad = \quad [[x_1, y_1]^{\varphi}, g][g, [x_1, y_1]^{\varphi}] = 1.$$

Assumindo que a afirmação é verdade para $i \leq r - 1$ e usando o item (i) do Lema 2.1.1, segue que

$$\left[\prod_{i=1}^{r}[x_i, y_i], g^{\varphi}\right]\left[g, \prod_{i=1}^{r}[x_i, y_i]^{\varphi}\right] = \left[\prod_{i=1}^{r-1}[x_i, y_i], g^{\varphi}\right]^{[x_r,y_r^{\varphi}]}[[x_r, y_r], g^{\varphi}][g, [x_r, y_r]^{\varphi}]\left[g, \prod_{i=1}^{r-1}[x_i, y_i]^{\varphi}\right]^{[x_r,y_r^{\varphi}]}.$$

Mas, por hipótese de indução, esta expressão se reduz a

$$\left[\prod_{i=1}^{r-1}[x_i, y_i], g^{\varphi}\right]^{[x_r,y_r^{\varphi}]}\left[g, \prod_{i=1}^{r-1}[x_i, y_i]^{\varphi}\right]^{[x_r,y_r^{\varphi}]} = 1, \ \forall\, r \geq 1.$$

Isto conclui a demonstração do item (vi). ■

Lema 2.1.2 *Sejam a, b, x elementos de G tais que*

$$[x, a] = [x, b] = 1. \tag{2.3}$$

Então,

$$[a, b, x^\varphi] = 1 = [[a, b]^\varphi, x].$$

Demonstração: Pelo item (ii) do Lema 2.1.1 e a definição de $\nu(G)$, vemos que

$$[a, b, x^\varphi] = [a, b^\varphi, x] = [a, b^\varphi]^{-1}[a, b^\varphi]^x \overset{(2.1)}{=} [a, b^\varphi]^{-1}[a^x, (b^x)^\varphi] \overset{(2.3)}{=} [a, b^\varphi]^{-1}[a, b^\varphi] = 1.$$

Analogamente,

$$[[a, b]^\varphi, x] = [a^\varphi, b^\varphi, x] = [a, b, x^\varphi] = 1,$$

como queríamos demonstrar. ∎

Lema 2.1.3 *Sejam $x, y \in G$ tais que $[x, y] = 1$. Então,*
(i) $[x^n, y^\varphi] = [x, y^\varphi]^n = [x, (y^\varphi)^n]$, para todo inteiro n.
(ii) Se x e y são elementos de torção de ordens $o(x)$ e $o(y)$, respectivamente, então $o([x, y^\varphi])$ divide o $mdc(o(x), o(y))$.

Demonstração: *(i)* Usaremos indução em $n \geq 0$. Como os casos $n = 0$ e $n = 1$ são triviais, dado que $[x, y] = 1$, para $n = 2$, segue que

$$[x^2, y^\varphi] = [xx, y^\varphi] = [x, y^\varphi]^x[x, y^\varphi] \overset{(2.1)}{=} [x^x, (y^x)^\varphi][x, y^\varphi] = [x, y^\varphi]^2.$$

Por outro lado, usando as relações (2.1) que definem $\nu(G)$,

$$[x, (y^\varphi)^2] = [x, y^\varphi y^\varphi] = [x, y^\varphi][x, y^\varphi]^{y^\varphi} \overset{(2.1)}{=} [x, y^\varphi][x^y, (y^y)^\varphi] = [x, y^\varphi]^2.$$

Suponhamos como hipótese de indução que, para algum $n \geq 2$,

$$[x^n, y^\varphi] = [x, y^\varphi]^n = [x, (y^\varphi)^n]. \tag{2.4}$$

Com isso,

$$\begin{aligned} [x^{n+1}, y^\varphi] &= [x^n x, y^\varphi] \\ &= [x^n, y^\varphi]^x[x, y^\varphi] \\ &\overset{(2.4)}{=} ([x, y^\varphi]^x)^n[x, y^\varphi] \\ &\overset{(2.1)}{=} [x^x, (y^x)^\varphi]^n[x, y^\varphi] \\ &= [x, y^\varphi]^{n+1}. \end{aligned}$$

Por outro lado,

$$\begin{aligned}[x,(y^{n+1})^{\varphi}] &= [x,(y^n)^{\varphi}y^{\varphi}]\\ &= [x,y^{\varphi}][x,(y^n)^{\varphi}]^{y^{\varphi}}\\ &\overset{(2.4)}{=} [x,y^{\varphi}]([x,y^{\varphi}]^{y^{\varphi}})^n\\ &\overset{(2.1)}{=} [x,y^{\varphi}][x^y,(y^y)^{\varphi}]^n\\ &= [x,y^{\varphi}]^{n+1}.\end{aligned}$$

Portanto, para todo $n \geq 0$,

$$[x^n, y^{\varphi}] = [x, y^{\varphi}]^n = [x, (y^{\varphi})^n]. \tag{2.5}$$

Agora, se $n = -1$, usando a definição de $\nu(G)$, nossa hipótese e o item (i) da Proposição 1.2.1, temos

$$[x^{-1}, y^{\varphi}] = [(x^{-1})^x, (y^x)^{\varphi}] \overset{(2.1)}{=} [x^{-1}, y^{\varphi}]^x = [x, y^{\varphi}]^{-1}. \tag{2.6}$$

Como $[x^{-1}, y] = [x, y]^{-x^{-1}} = 1$, segue que

$$[x^{-n}, y^{\varphi}] = [(x^{-1})^n, y^{\varphi}] \overset{(2.5)}{=} [x^{-1}, y^{\varphi}]^n \overset{(2.6)}{=} [x, y^{\varphi}]^{-n},$$

para todo $n \geq 0$. O caso $[x, (y^{-n})^{\varphi}]$ é análogo, pois

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

Logo, para todo $n \leq 0$, temos

$$[x^n, y^{\varphi}] = [x, y^{\varphi}]^n = [x, (y^{\varphi})^n]$$

Portanto, o resultado é válido para todo $n \in \mathbb{Z}$.
(ii) Suponhamos que $o(x) = n$, $o(y) = m$ e $o([x, y^{\varphi}]) = k$. Pelo item (i) anterior, temos

$$[x, y^{\varphi}]^n = [x^n, y^{\varphi}] = 1 = [x, (y^m)^{\varphi}] = [x, y^{\varphi}]^m.$$

Portanto, $k \mid m$ e $k \mid n$, ou seja, $k \mid mdc(m, n)$. ■

Considerando N como um subgrupo normal de G e o epimorfismo canônico

$$\begin{aligned}\pi : \ G &\twoheadrightarrow \frac{G}{N}\\ g &\mapsto Ng,\end{aligned}$$

conseguimos construir um epimorfismo de $\nu(G)$ em $\nu(\frac{G}{N})$, induzido por π. O núcleo de tal epimorfismo nos ajudará a obter uma descrição do grupo $\nu(G)$ quando G for um produto semidireto e, também, conseguir uma estimativa para a ordem de $\nu(G)$, quando G for finito.

Proposição 2.1.1 *Sejam N um subgrupo normal de G, $\overline{G}$ e $\overline{G^\varphi}$ os quocientes $\frac{G}{N}$ e $\frac{G^\varphi}{N^\varphi}$, respetivamente. Considere o epimorfismo*

$$\begin{aligned} \tilde{\pi}: \quad \nu(G) &\twoheadrightarrow \nu(\overline{G}) \\ g &\longmapsto \overline{g} \\ g^\varphi &\longmapsto \overline{g^\varphi}, \end{aligned}$$

induzido pelo epimorfismo canônico $\pi : G \twoheadrightarrow \overline{G}$ dado por $\pi(g) = \overline{g}$, onde $\overline{g} = Ng$ e $\overline{g^\varphi} = N^\varphi g^\varphi$. Então,
(i) $[N, G^\varphi] \trianglelefteq \nu(G)$, $[G, N^\varphi] \trianglelefteq \nu(G)$;
(ii) $\ker \tilde{\pi} = \langle N, N^\varphi \rangle [N, G^\varphi][G, N^\varphi]$.

Demonstração: *(i)* Para quaisquer que sejam $x \in N, g, h \in G$, pelo item (ii) do Lema 2.1.1, segue que

$$[x, g^\varphi]^h = [x, g^\varphi][x, g^\varphi, h] = [x, g^\varphi][x, g, h^\varphi] \in [N, G^\varphi].$$

Portanto, G normaliza $[N, G^\varphi]$ e segue analogamente que G^φ também normaliza $[N, G^\varphi]$. Para o caso $[G, N^\varphi]$, tomaremos quaisquer $n \in N$, $g, g_1 \in G$, de modo que

$$[g, n^\varphi]^{g_1} = [g, n^\varphi][g, n^\varphi, g_1] = [g, n^\varphi][g^\varphi, n^\varphi, g_1] \in [G, N^\varphi].$$

Daí, G normaliza $[G, N^\varphi]$ e, analogamente, G^φ normaliza $[G, N^\varphi]$. Com isso, os subgrupos $[N, G^\varphi]$ e $[G, N^\varphi]$ são normais em $\nu(G)$, como queríamos.
(ii) Definamos $M := \langle N, N^\varphi \rangle [N, G^\varphi][G, N^\varphi]$, mostraremos que $M = \ker \tilde{\pi}$. Pela própria definição de $\tilde{\pi}$ vemos que cada um dos fatores de M pertence ao $\ker \tilde{\pi}$, logo $M \leq \ker \tilde{\pi}$. Usando o item anterior, note que para qualquer $x \in \langle N, N^\varphi \rangle$, usando a normalidade de $[N, G^\varphi][G, N^\varphi]$ em $\nu(G)$, vemos que $x^h \in \langle N, N^\varphi \rangle [N, G^\varphi][G, N^\varphi]$ para todo $h \in \nu(G)$. Logo, M é normal em $\nu(G)$. Portanto, podemos definir a função

$$\begin{aligned} \theta: \quad \overline{G} \cup \overline{G^\varphi} &\longrightarrow \frac{\nu(G)}{M} \\ \overline{g} &\longmapsto Mg \\ \overline{g^\varphi} &\longmapsto Mg^\varphi. \end{aligned}$$

que é bem definida, pois $N, N^\varphi \subseteq M$. Além disso, a restrição de θ aos grupos $\overline{G}$ e $\overline{G^\varphi}$ são homomorfismos. Logo, pela Proposição 1.4.6, θ é estendido para um único homomorfismo θ^* no produto livre $\overline{G} * \overline{G^\varphi}$. Agora, vejamos que

$$[\overline{g_1 g_2}, \overline{g_3^\varphi}] = [\overline{(g_1^{g_2})}, \overline{(g_3^{g_2})^\varphi}][\overline{g_2}, \overline{g_3^\varphi}] \quad \text{e} \quad [\overline{g_1}, \overline{(g_2 g_3)^\varphi}] = [\overline{g_1}, \overline{g_3^\varphi}][\overline{(g_1^{g_3})}, \overline{(g_2^{g_3})^\varphi}]$$

são também relações definidoras do grupo

$$\nu(\overline{G}) = \langle \overline{G} \cup \overline{G^\varphi} \mid [\overline{g_1}, \overline{g_2^\varphi}]^{\overline{g_3}} = [\overline{(g_1^{g_3})}, \overline{(g_2^{g_3})^\varphi}] = [\overline{g_1}, \overline{g_2^\varphi}]^{\overline{g_3^\varphi}}, \overline{g_1}, \overline{g_2}, \overline{g_3} \in \overline{G} \rangle.$$

e que θ^* preserva tais relações, pois,

$$\begin{aligned}
([\overline{g_1g_2}, \overline{g_3^{\varphi}}])^{\theta^*} &= ([\overline{g_1g_2}, \overline{g_3^{\varphi}}])^{\theta}\\
&= [Mg_1Mg_2, Mg_3^{\varphi}]\\
&= M[g_1g_2, g_3^{\varphi}]\\
&= M[g_1^{g_2}, (g_3^{g_2})^{\varphi}][g_2, g_3^{\varphi}]\\
&= [Mg_1^{g_2}, M(g_3^{g_2})^{\varphi}][Mg_2, Mg_3^{\varphi}]\\
&= ([\overline{(g_1^{g_2})}, \overline{(g_3^{g_2})^{\varphi}}][\overline{g_2}, \overline{g_3^{\varphi}}])^{\theta}\\
&= ([\overline{(g_1^{g_2})}, \overline{(g_3^{g_2})^{\varphi}}][\overline{g_2}, \overline{g_3^{\varphi}}])^{\theta^*},
\end{aligned}$$

$$\begin{aligned}
([\overline{g_1}, \overline{(g_2g_3)^{\varphi}}])^{\theta^*} &= ([\overline{g_1}, \overline{(g_2g_3)^{\varphi}}])^{\theta}\\
&= [Mg_1, M(g_2g_3)^{\varphi}]\\
&= M[g_1, (g_2g_3)^{\varphi}]\\
&= M[g_1, g_3^{\varphi}][g_1^{g_3}, (g_2^{g_3})^{\varphi}]\\
&= [Mg_1, Mg_3^{\varphi}][Mg_1^{g_3}, M(g_2^{g_3})^{\varphi}]\\
&= ([\overline{g_1}, \overline{g_3^{\varphi}}][\overline{(g_1^{g_3})}, \overline{(g_2^{g_3})^{\varphi}}])^{\theta}\\
&= ([\overline{g_1}, \overline{g_3^{\varphi}}][\overline{(g_1^{g_3})}, \overline{(g_2^{g_3})^{\varphi}}])^{\theta^*}.
\end{aligned}$$

Logo, pelo Lema 1.4.1, θ induz um homomorfismo

$$\begin{aligned}
\tilde{\theta}: \ \nu(\overline{G}) &\to \frac{\nu(G)}{M}\\
\overline{g} &\longmapsto Mg\\
\overline{g^{\varphi}} &\longmapsto Mg^{\varphi}.
\end{aligned}$$

Dado que $M \leq \ker \tilde{\pi}$, temos um epimorfismo

$$\begin{aligned}
\overline{\pi}: \frac{\nu(G)}{M} &\twoheadrightarrow \nu(\overline{G})\\
Mg &\longmapsto \overline{g}\\
Mg^{\varphi} &\longmapsto \overline{g^{\varphi}}.
\end{aligned}$$

Mas, a composição de $\overline{\pi}$ com $\tilde{\theta}$ nos dá

$$\overline{\pi}\tilde{\theta}(\overline{g^{\varphi}}) = \overline{\pi}(Mg^{\varphi}) = \overline{g^{\varphi}} \ \text{ e } \ \overline{\pi}\tilde{\theta}(\overline{g}) = \overline{\pi}(Mg) = \overline{g},\ \forall\, \overline{g} \in \overline{G}.$$

Portanto, $\overline{\pi}\tilde{\theta} = id_{\nu(\overline{G})}$, pois $\overline{g}$ e $\overline{g^{\varphi}}$ são geradores de $\nu(\overline{G})$. Logo, $\tilde{\theta}$ é um isomorfismo e $M = \ker \tilde{\pi}$, como queríamos demonstrar. ∎

2.2 O Quadrado Tensorial Não Abeliano $\Upsilon(G)$

A partir de agora, consideraremos o subgrupo normal

$$\Upsilon(G) := [G, G^{\varphi}]$$

de $\nu(G)$. A sua normalidade segue imediatamente das relações que definem $\nu(G)$.

Proposição 2.2.1 *Seja G um grupo. Então, o quadrado tensorial $G \otimes G$ é isomorfo a $\Upsilon(G)$. Mais ainda, a função*

$$\begin{array}{rccc} \tau: & G \otimes G & \longrightarrow & \Upsilon(G) \\ & g_1 \otimes g_2 & \longmapsto & [g_1, g_2^{\varphi}] \end{array}$$

é um isomorfismo de grupos.

Demonstração: Sabemos que o quadrado tensorial não abeliano $G \otimes G$ é gerado pelos símbolos $g_1 \otimes g_2$, com $g_1, g_2 \in G$, possuindo as seguintes relações definidoras:

$$S_1 = \{(g_1g_3 \otimes g_2)^{-1}(g_1^{g_3} \otimes g_2^{g_3})(g_3 \otimes g_2), (g_1 \otimes g_2g_3)^{-1}(g_1 \otimes g_3)(g_1^{g_3} \otimes g_2^{g_3}) \mid g_1, g_2, g_3 \in G\}. \quad (2.7)$$

Denotemos por $A := \{g_1 \otimes g_2 \mid g_1, g_2 \in G\}$ ao conjunto de geradores de $G \otimes G$ e por $B := \{[g_1, g_2^{\varphi}] \mid g_1, g_2 \in G\}$ ao conjunto de geradores de $\Upsilon(G)$. Definamos uma aplicação

$$\begin{array}{rccc} \tau_1: & A & \longrightarrow & B \\ & g_1 \otimes g_2 & \longmapsto & [g_1, g_2^{\varphi}]. \end{array}$$

Note que $\Upsilon(G)$ é gerado pela imagem de τ_1 e que τ_1 é sobrejetiva. Considerando F como sendo o grupo livre em A, pela Proposição 1.4.3 existe um único epimorfismo $\theta' : F \twoheadrightarrow \Upsilon(G)$ que estende τ_1. Considerando a apresentação $\upsilon : F \twoheadrightarrow G \otimes G$ e notando que $\ker \upsilon \subseteq \ker \theta'$, pelo Teorema de Von Dyck, existe um epimorfismo bem definido

$$\begin{array}{rccc} \tau: & G \otimes G & \twoheadrightarrow & \Upsilon(G) \\ & g_1 \otimes g_2 & \longmapsto & [g_1, g_2^{\varphi}] \end{array}$$

induzido por θ'. Agora, consideremos o produto livre $G * G^{\varphi}$. Sabemos pela Proposição 1.4.7, que o subgrupo $K := [G, G^{\varphi}]$ é livre, normal em $G * G^{\varphi}$ e livremente gerado pelos símbolos $[g_1, g_2^{\varphi}]$ com $1 \neq g_1 \in G$ e $1 \neq g_2 \in G$. Logo, como subgrupo normal de $G * G^{\varphi}$, K admite a ação de G e G^{φ} por conjugação e as seguintes relações se mantêm em K:

$$\begin{array}{l} [g_1, g_2^{\varphi}]^g = [g_1g, g_2^{\varphi}][g, g_2^{\varphi}]^{-1}; \\ [g_1, g_2^{\varphi}]^{g^{\varphi}} = [g_1, g^{\varphi}]^{-1}[g_1, (g_2g)^{\varphi}] \quad , \forall\, g_1, g_2, g \in G. \end{array} \quad (2.8)$$

Novamente, pela Proposição 1.4.3, a aplicação

$$\begin{array}{rccc} \beta_1: & B & \longrightarrow & A \\ & [g_1, g_2^{\varphi}] & \longmapsto & g_1 \otimes g_2 \end{array}$$

pode ser estendida para um único epimorfismo

$$\begin{array}{rccc} \mu_1: & K & \twoheadrightarrow & G \otimes G \\ & [g_1, g_2^{\varphi}] & \longmapsto & g_1 \otimes g_2 \end{array}$$

do subgrupo livre K no grupo $G \otimes G$. Analogamente, obtemos um único epimorfismo

$$\begin{array}{rccc} \mu_2: & K & \twoheadrightarrow & \Upsilon(G) \\ & [g_1, g_2^{\varphi}] & \longmapsto & [g_1, g_2^{\varphi}] \end{array}$$

do subgrupo livre K no grupo $\Upsilon(G)$. Usando as relações (2.8), vemos que a relações definidoras de $\nu(G)$

$$[g_1^{g_3}, (g_2^{g_3})^{\varphi}] = [g_1, g_2^{\varphi}]^{g_3^{\varphi}} = [g_1, g_2^{\varphi}]^{g_3}$$

se tornam

$$[g_1^{g_3}, (g_2^{g_3})^{\varphi}] = [g_1, g_3^{\varphi}]^{-1}[g_1, (g_2g_3)^{\varphi}] = [g_1g_3, g_2^{\varphi}][g_3, g_2^{\varphi}]^{-1},$$

para todos $g_1, g_2, g_3 \in G$. Consequentemente, como $K \trianglelefteq G * G^{\varphi}$ podemos ver $\Upsilon(G)$ como quociente de K pelo fecho normal de

$$S = \{[g_1g_3, g_2^{\varphi}]^{-1}[g_1^{g_3}, (g_2^{g_3})^{\varphi}][g_3, g_2^{\varphi}], [g_1, (g_2g_3)^{\varphi}]^{-1}[g_1, g_3^{\varphi}][g_1^{g_3}, (g_2^{g_3})^{\varphi}] \mid g_1, g_2, g_3 \in G\}$$

em $G * G^{\varphi}$. Notemos que a imagem das relações em S por μ_1 são as relações que definem $G \otimes G$. Portanto, temos que μ_1 e μ_2 são duas apresentações com $\ker \mu_2 \leq \ker \mu_1$. Com isso, segue do Teorema de Von Dyck que existe um epimorfismo bem definido

$$\begin{array}{rccc} \mu: & \Upsilon(G) & \twoheadrightarrow & G \otimes G \\ & [g_1, g_2^{\varphi}] & \longmapsto & g_1 \otimes g_2. \end{array}$$

Além disso, vejamos que para todo $[g_1, g_2^{\varphi}] \in \Upsilon(G)$, temos

$$\tau\mu([g_1, g_2^{\varphi}]) = \tau(g_1 \otimes g_2) = [g_1, g_2^{\varphi}].$$

Mas, $\Upsilon(G)$ é gerado pelos comutadores do tipo $[g_1, g_2^{\varphi}]$, com $g_1, g_2 \in G$. Logo,

$$\tau\mu = id_{\Upsilon(G)}.$$

Analogamente,

$$\mu\tau = id_{G \otimes G}.$$

Daí, τ é um isomorfismo, como queríamos demonstrar. ■

Cabe ressaltar, que devido a este isomorfismo, os elementos $[g, h^{\varphi}] \in [G, G^{\varphi}]$ são também chamados de tensores.

Observação 2.1 Nas mesmas condições dadas na Proposição 2.1.1, isto é, considerando o epimorfismo $\tilde{\pi} : \nu(G) \twoheadrightarrow \nu(\overline{G})$ induzido pelo epimorfismo canônico $\pi : G \twoheadrightarrow \overline{G}$, onde $\overline{G} = \frac{G}{N}$, temos que

$$\ker \tilde{\pi} \cap \Upsilon(G) = [N, G^{\varphi}][G, N^{\varphi}].$$

De fato, seja $M = \langle N, N^{\varphi} \rangle [N, G^{\varphi}][G, N^{\varphi}]$. Sabemos que existe uma função bem definida

$$\begin{array}{rcl} \theta: \ \overline{G} \cup \overline{G^{\varphi}} & \longrightarrow & \dfrac{\nu(G)}{M} \\ \overline{g} & \longmapsto & Mg \\ \overline{g^{\varphi}} & \longmapsto & Mg^{\varphi}. \end{array}$$

que se estende para um único homomorfismo θ^* no produto livre $\overline{G} * \overline{G^\varphi}$. Considerando o subgrupo $[\overline{G}, \overline{G^\varphi}]$ de $\overline{G} * \overline{G^\varphi}$, vemos que

$$([\overline{G}, \overline{G^\varphi}])^{\theta^*} \subseteq \frac{\Upsilon(G)M}{M} \simeq \frac{\Upsilon(G)}{\Upsilon(G) \cap M}.$$

Entretanto, $\Upsilon(\overline{G})$ é um quociente do subgrupo $[\overline{G}, \overline{G^\varphi}]$ de $\overline{G} * \overline{G^\varphi}$ pelo fecho normal em $[\overline{G}, \overline{G^\varphi}]$ das relações definidoras de $\nu(\overline{G})$. O resultado segue analogamente à demonstração da Proposição 2.1.1.

Observação 2.2 A partir de agora, denotaremos $[G, G^\varphi]$ apenas para o subgrupo $\Upsilon(G)$.

2.3 Descrição de Alguns Subgrupos de $\nu(G)$

A seguir, vamos descrever alguns subgrupos do grupo $\nu(G)$ envolvendo os termos das séries derivada, central inferior e superior de G. Destacamos que não usaremos a notação usual $G^{(i)}$ para nos referir ao i-ésimo termo da série derivada de G, mas adotaremos a notação G_i, para todo i. Note também que G é o primeiro termo da série derivada de G, isto é, $G_1 = G$.

Proposição 2.3.1 *No grupo $\nu(G)$ temos:*
(i) $[Z_j(G), G^\varphi_{j+1}] = \{1\}$, para todo $j \geq 0$;
(ii) $[Z_{j+1}(G), \gamma_j(G^\varphi)] \cdot [\gamma_j(G), Z_{j+1}(G^\varphi)]$ é central em $\Upsilon(G)$, para todo $j \geq 1$;
(iii) $[Z_j(G), \gamma_j(G^\varphi)]$ é central em $\nu(G)$, para todo $j \geq 1$.

Demonstração: *(i)* O caso em que $j = 0$ segue trivialmente. Iremos mostrar que

$$[Z_j(G), ([G_j, G_j])^\varphi] = \{1\}, \forall\, j \geq 1.$$

Mas, pelo Lema 2.1.2, é suficiente mostrar que

$$[Z_j(G), G_j] = \{1\}, \forall\, j \geq 1.$$

Observe que o caso em que $j = 1$, segue trivialmente, pois $Z_1(G) = Z(G)$. Por indução em j, temos

$$G_j = [G_{j-1}, G_{j-1}] \leq [G_{j-1}, G] \leq [\gamma_{j-1}(G), G] = \gamma_j(G), \forall j > 1. \tag{2.9}$$

Agora, pelo item (ii) do Lema 1.2.2 e por (2.9),

$$[Z_j(G), G_j] \leq [Z_j(G), \gamma_j(G)] = \{1\}.$$

para todo $j \geq 1$, como desejávamos. Portanto, o resultado segue.
(ii) Como $\varphi : G \to G^\varphi$ é um isomorfismo de grupos, segue que

$$\varphi(\gamma_j(G)) = \gamma_j(G^\varphi), \forall\, j \geq 1.$$

Agora, tomemos $z \in Z_{j+1}(G)$, $g \in \gamma_j(G)$ e $g_1, g_2 \in G$ quaisquer, para todo $j \geq 1$. Então, pelo item (ii) do Lema 1.2.2 segue que $[z, g] \in Z(G)$, e pelo Lema 2.1.2

$$[[z, g], [g_1, g_2]^{\varphi}] = 1.$$

Portanto,

$$\begin{array}{rcl} [[z, g^{\varphi}], [g_1, g_2^{\varphi}]] & = & [z, g^{\varphi}]^{-1}[z, g^{\varphi}]^{[g_1, g_2^{\varphi}]} \\ & \overset{2.1.1\,(i)}{=} & [z, g^{\varphi}]^{-1}[z, g^{\varphi}]^{[g_1, g_2]} \\ & = & [z, g^{\varphi}, [g_1, g_2]] \\ & \overset{2.1.1\,(ii)}{=} & [[z, g], [g_1, g_2]^{\varphi}] \\ & = & 1. \end{array}$$

Consequentemente, $[Z_{j+1}(G), \gamma_j(G^{\varphi})]$ é central em $\Upsilon(G)$, para todo $j \geq 1$. Analogamente, se mostra que $[\gamma_j(G), Z_{j+1}(G^{\varphi})]$ é central em $\Upsilon(G)$, para todo $j \geq 1$. Portanto, o resultado segue.

(iii) Sejam $g_1 \in G$, $g_2^{\varphi} \in G^{\varphi}$, $z \in Z_j(G)$ e $h \in \gamma_j(G)$. Como $[Z_j(G), \gamma_j(G)] = 1$ para todo $j \geq 1$, temos, pelo item (ii) do Lema 2.1.1, que

$$[[z, h^{\varphi}], g_1] = [z, h, g_1^{\varphi}] = 1 = [z, h, g_2^{\varphi}] = [[z, h^{\varphi}], g_2^{\varphi}].$$

Daí, $[Z_j(G), \gamma_j(G^{\varphi})] \subseteq Z(\nu(G))$. ■

Consideremos a seguinte aplicação:

$$\begin{array}{rcl} \rho : [G, G^{\varphi}] & \rightarrow & G' \\ \prod_{i=1}^{n}[x_i, y_i^{\varphi}] & \longmapsto & \prod_{i=1}^{n}[x_i, y_i], \end{array}$$

que é bem definida, pois φ é um isomorfismo. Mais ainda, ρ é um epimorfismo. De fato, vejamos que ρ é um homomorfismo. Para isso, consideremos $\alpha = \prod_{i=1}^{r}[x_i, y_i^{\varphi}]$ e $\beta = \prod_{i=1}^{s}[a_i, b_i^{\varphi}] \in [G, G^{\varphi}]$. Denotando por $[g_i, h_i^{\varphi}] := [x_i, y_i^{\varphi}]$ para $i = 1, 2, \cdots, r$ e $[g_{r+i}, h_{r+i}^{\varphi}] := [a_i, b_i^{\varphi}]$ para $i = 1, 2, \cdots, s$, temos que

$$\rho(\alpha\beta) = \rho(\prod_{i=1}^{r+s}[g_i, h_i^{\varphi}]) = \prod_{i=1}^{r+s}[g_i, h_i] = \prod_{i=1}^{r}[g_i, h_i] \prod_{i=r+1}^{r+s}[g_i, h_i] = \rho(\alpha)\rho(\beta).$$

Em particular, pela definição de G', ρ é também epimorfismo.

Proposição 2.3.2 *O núcleo* $\ker \rho$ *é um subgrupo central do grupo* $\nu(G)$.

Demonstração: De fato, como

$$\ker \rho = \Big\{ \prod_{i=1}^{n}[x_i, y_i^{\varphi}] \in [G, G^{\varphi}] | \prod_{i=1}^{n}[x_i, y_i] = 1 \Big\},$$

é suficiente mostrar que

$$\Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g\Big] = \Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g^{\varphi}\Big] = \Big[\prod_{i=1}^{n}[x_i, y_i], g^{\varphi}\Big],$$

para todos $\prod_{i=1}^{n}[x_i, y_i^{\varphi}] \in [G, G^{\varphi}]$, $g \in G$. Para isso, faremos indução em n. Sendo assim, tomemos $[x_1, y_1^{\varphi}] \in [G, G^{\varphi}]$. Pelo item (ii) do Lema 2.1.1, temos que

$$[[x_1, y_1^{\varphi}], g^{\varphi}] = [[x_1, y_1^{\varphi}], g] = [[x_1, y_1], g^{\varphi}].$$

Suponhamos, como hipótese de indução, que para algum $n \geq 2$ tenhamos

$$\Big[\prod_{i=1}^{n-1}[x_i, y_i^{\varphi}], g\Big] = \Big[\prod_{i=1}^{n-1}[x_i, y_i^{\varphi}], g^{\varphi}\Big] = \Big[\prod_{i=1}^{n-1}[x_i, y_i], g^{\varphi}\Big].$$

Então, usando os itens (i) e (ii) do Lema 2.1.1, segue que

$$\begin{aligned}
\Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g\Big] &= \Big[\prod_{i=1}^{n-1}[x_i, y_i^{\varphi}], g\Big]^{[x_n, y_n^{\varphi}]}[[x_n, y_n^{\varphi}], g] \\
&= \Big[\prod_{i=1}^{n-1}[x_i, y_i], g^{\varphi}\Big]^{[x_n, y_n^{\varphi}]}[[x_n, y_n^{\varphi}], g] \\
&\overset{2.1.1\,(i),(ii)}{=} \Big[\prod_{i=1}^{n-1}[x_i, y_i], g^{\varphi}\Big]^{[x_n, y_n]}[[x_n, y_n], g^{\varphi}] \\
&= \Big[\prod_{i=1}^{n}[x_i, y_i], g^{\varphi}\Big].
\end{aligned}$$

Analogamente, mostra-se que

$$\Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g^{\varphi}\Big] = \Big[\prod_{i=1}^{n}[x_i, y_i], g^{\varphi}\Big].$$

Portanto, para todos $\prod_{i=1}^{n}[x_i, y_i^{\varphi}] \in \ker\rho$ e $g \in G$, segue que

$$\Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g\Big] = \Big[\prod_{i=1}^{n}[x_i, y_i^{\varphi}], g^{\varphi}\Big] = \Big[\prod_{i=1}^{n}[x_i, y_i], g^{\varphi}\Big] = 1.$$

Daí, temos que $\ker\rho \leq Z(\nu(G))$. ■

2.4 Série Central Inferior e Série Derivada de $\nu(G)$

Seja G um grupo, e suponhamos que $N \trianglelefteq G$ e exista um subgrupo H de G tal que $G = HN$ e $H \cap N = \{1\}$. Então, G é dito ser o *produto semidireto (interno)* de N e H. Em símbolos,

$$G = H \ltimes N \;\text{ ou }\; G = N \rtimes H.$$

Corolário 2.4.1 *Seja $\Upsilon(G) := [G, G^{\varphi}]$ subgrupo normal em $\nu(G)$. Então,*

$$(\Upsilon(G) \rtimes G) \trianglelefteq \nu(G) \quad e \quad (\Upsilon(G) \rtimes G^{\varphi}) \trianglelefteq \nu(G).$$

Demonstração: Como $\Upsilon(G)$ é normal em $\nu(G)$, para quaisquer elementos $h, k \in \Upsilon(G)$ e $g, g_1, g_2 \in G$ temos que

$$(hg_1)^{g^\varphi} = h^{g^\varphi} g_1^{g^\varphi} = h^{g^\varphi}[g^\varphi, g_1^{-1}]g_1 \in \Upsilon(G) \rtimes G.$$

Analogamente,

$$(kg_2^\varphi)^g = k^g(g_2^\varphi)^g = k^g[g, (g_2^{-1})^\varphi]g_2^\varphi \in \Upsilon(G) \rtimes G^\varphi$$

Além disso,

$$(hg_1)^g \in \Upsilon(G) \rtimes G \quad \text{e} \quad (kg_2^\varphi)^{g^\varphi} \in \Upsilon(G) \rtimes G^\varphi.$$

Desse modo,

$$(\Upsilon(G) \rtimes G) \trianglelefteq \nu(G) \quad \text{e} \quad (\Upsilon(G) \rtimes G^\varphi) \trianglelefteq \nu(G).$$

■

Uma consequência desse corolário é que existe uma ação bem definida do grupo G^φ em $\Upsilon(G) \rtimes G$. Em particular, conseguimos descrever o grupo $\nu(G)$ como o produto semidireto de $\Upsilon(G) \rtimes G$ por G^φ. Na verdade, um fato mais geral do que este pode ser encontrado em [9], demonstrado por T. Bueno para uma generalização do grupo $\nu(G)$.

Teorema 2.4.1 [9, Corolário 2.11] *Existe um isomorfismo*

$$\nu(G) \simeq (\Upsilon(G) \rtimes G) \rtimes G^\varphi.$$

A descrição de $\nu(G)$ como produto semidireto

$$\nu(G) \simeq (\Upsilon(G) \rtimes G) \rtimes G^\varphi$$

nos dá uma descrição das séries central inferior e derivada do grupo $\nu(G)$.

Teorema 2.4.2 *Para $i \geq 2$ o i-ésimo termo da série central inferior de $\nu(G)$ é dado por*

$$\gamma_i(\nu(G)) = \gamma_i(G)\gamma_i(G^\varphi)[\gamma_{i-1}(G^\varphi), G].$$

Demonstração: Usaremos indução em i. Logo, para $i = 2$, temos

$$\gamma_2(\nu(G)) = [\nu(G), \nu(G)] = [\Upsilon(G) \cdot G \cdot G^\varphi, \Upsilon(G) \cdot G \cdot G^\varphi].$$

Portanto, como $\Upsilon(G)$, $\Upsilon(G)G^\varphi$ e $\Upsilon(G)G$ são normais em $\nu(G)$, segue que

$$\begin{aligned}
\gamma_2(\nu(G)) &\leq [\Upsilon(G) \cdot G^\varphi, \Upsilon(G) \cdot G \cdot G^\varphi][\Upsilon(G) \cdot G, \Upsilon(G) \cdot G \cdot G^\varphi] \\
&\leq [\Upsilon(G) \cdot G^\varphi, \Upsilon(G) \cdot G][\Upsilon(G) \cdot G^\varphi, \Upsilon(G) \cdot G^\varphi][\Upsilon(G) \cdot G, \Upsilon(G) \cdot G] \\
&\leq \gamma_2(G)\gamma_2(G^\varphi)\Upsilon(G).
\end{aligned}$$

Como a inclusão contrária segue da decomposição de $\nu(G) = \Upsilon(G) \cdot G \cdot G^{\varphi}$, temos a igualdade. Em particular, para provar este teorema é suficiente mostrar apenas uma inclusão. Desse modo, suponhamos por hipótese de indução que para algum $i \geq 2$ tenhamos

$$\gamma_i(\nu(G)) \leq \gamma_i(G)\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G].$$

Então, dado que

$$\begin{aligned}
\gamma_{i+1}(\nu(G)) &= [\gamma_i(\nu(G)), \nu(G)] \\
&= [\gamma_i(\nu(G)), \Upsilon(G) \cdot G \cdot G^{\varphi}] \\
&\leq [\gamma_i(\nu(G)), \Upsilon(G) \cdot G^{\varphi}][\gamma_i(\nu(G)), \Upsilon(G) \cdot G],
\end{aligned}$$

é suficiente calcularmos os fatores

$$[\gamma_i(\nu(G)), \Upsilon(G) \cdot G^{\varphi}] \text{ e } [\gamma_i(\nu(G)), \Upsilon(G) \cdot G].$$

Antes disso, vejamos que pelo Lema 2.1.1, os subgrupos $[\gamma_{i-1}(G), G^{\varphi}]$ e $[\gamma_{i-1}(G^{\varphi}), G]$ são os mesmos. Mais ainda, eles são normais em $\nu(G)$, pela Proposição 2.1.1. Consequentemente, os subgrupos $\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G]$ e $\gamma_i(G)[\gamma_{i-1}(G^{\varphi}), G]$ são normais em $\nu(G)$, para todo $i \geq 2$. Daí, segue novamente pela Proposição 2.1.1, pelo Corolário 2.4.1, pelo Lema 2.1.1, e por nossa hipótese de indução, que

$$\begin{aligned}
[\gamma_i(\nu(G)), \Upsilon(G) \cdot G^{\varphi}] &\leq [\gamma_i(G)\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G^{\varphi}] \\
&\leq [\gamma_i(G)[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G^{\varphi}][\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G^{\varphi}] \\
&\leq \gamma_{i+1}(G^{\varphi})[\gamma_i(G^{\varphi}), G]. \qquad (2.10)
\end{aligned}$$

Semelhantemente, segue que

$$\begin{aligned}
[\gamma_i(\nu(G)), \Upsilon(G) \cdot G] &\leq [\gamma_i(G)\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G] \\
&\leq [\gamma_i(G)[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G][\gamma_i(G^{\varphi})[\gamma_{i-1}(G^{\varphi}), G], \Upsilon(G) \cdot G] \\
&\leq \gamma_{i+1}(G)[\gamma_i(G^{\varphi}), G]. \qquad (2.11)
\end{aligned}$$

Logo, de (2.10) e (2.11) que

$$\gamma_{i+1}(\nu(G)) \leq \gamma_{i+1}(G)\gamma_{i+1}(G^{\varphi})[\gamma_i(G^{\varphi}), G].$$

Como queríamos demonstrar. ∎

O próximo resultado nos diz uma consequência imediata do teorema anterior, para o caso em que G é um grupo nilpotente.

Corolário 2.4.2 *Seja G um grupo nilpotente de classe c. Então, $\nu(G)$ é um grupo nilpotente de classe no máximo $c + 1$.*

Demonstração: A prova segue do teorema anterior, pois se G é nilpotente de classe c, então pela Proposição 1.2.4, temos $\gamma_{c+1}(G) = 1$. Logo, como

$$\gamma_i(\nu(G)) = \gamma_i(G)\gamma_i(G^\varphi)[\gamma_{i-1}(G^\varphi), G],$$

concluímos que,

$$\gamma_{c+2}(\nu(G)) = \gamma_{c+2}(G)\gamma_{c+2}(G^\varphi)[\gamma_{c+1}(G^\varphi), G] = 1.$$

■

Teorema 2.4.3 *Para $i \geq 2$ o i-ésimo termo da série derivada de $\nu(G)$ é dado por*

$$\nu(G)_i = G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi],$$

onde G_i denota o i-ésimo termo da série derivada de G.

Demonstração: Demonstraremos por indução em i. Logo, o caso $i = 2$ é válido pelo Teorema 2.4.2, uma vez que $\nu(G)_2 = \gamma_2(\nu(G))$. Suponhamos que para algum $i \geq 2$ se tenha

$$\nu(G)_i = G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi].$$

Agora, pelas relações que definem o grupo $\nu(G)$, o subgrupo $[G_{i-1}, G_{i-1}^\varphi]$ é normal em $\nu(G)$, para todo $i \geq 2$. Além disso, G_i normaliza $G_i^\varphi[G_{i-1}, G_{i-1}^\varphi]$ e G_i^φ normaliza $G_i[G_{i-1}, G_{i-1}^\varphi]$, pois $G_i \subseteq G_{i-1}$. Mais ainda, pelo Lema 2.1.1, temos as seguintes relações:

$$[[G_{i-1}, G_{i-1}^\varphi], G_i] = [[G_{i-1}, G_{i-1}], G_i^\varphi] = [[G_{i-1}, G_{i-1}^\varphi], G_i^\varphi] = [[G_{i-1}^\varphi, G_{i-1}^\varphi], G_i],$$

e

$$[[G_{i-1}, G_{i-1}^\varphi], [G_{i-1}, G_{i-1}^\varphi]] = [G_i, G_i^\varphi].$$

Portanto, usando a nossa hipótese de indução, segue que

$$\begin{aligned}
\nu(G)_{i+1} &= [\nu(G)_i, \nu(G)_i] \\
&= [G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi], G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi]] \\
&\leq [G_i [G_{i-1}, G_{i-1}^\varphi], G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi]][G_i^\varphi [G_{i-1}, G_{i-1}^\varphi], G_i G_i^\varphi [G_{i-1}, G_{i-1}^\varphi]],
\end{aligned}$$

Por sua vez, é subgrupo de

$$[G_i[G_{i-1}, G_{i-1}^\varphi], G_i[G_{i-1}, G_{i-1}^\varphi]][G_i[G_{i-1}, G_{i-1}^\varphi], G_i^\varphi[G_{i-1}, G_{i-1}^\varphi]][G_i^\varphi[G_{i-1}, G_{i-1}^\varphi], G_i^\varphi[G_{i-1}, G_{i-1}^\varphi]].$$

Por fim, usando novamente as informações dadas acima, temos que

$$\nu(G)_{i+1} \leq G_{i+1} G_{i+1}^\varphi [G_i, G_i^\varphi].$$

Como a inclusão contrária é válida, temos a igualdade, para todo $i \geq 2$. Concluindo a demonstração. ■

Uma consequência direta do Teorema anterior é dada a seguir.

Corolário 2.4.3 *Seja G um grupo solúvel de comprimento derivado l. Então, $\nu(G)$ é solúvel de comprimento derivado no máximo $l+1$.*

Demonstração: Se G tem comprimento derivado l, então pela Proposição 1.2.3, temos que $G_l = 1$. Consequentemente, dado que

$$\nu(G)_i = G_i G_i^{\varphi}[G_{i-1}, G_{i-1}^{\varphi}],$$

segue que

$$\nu(G)_{l+1} = G_{l+1} G_{l+1}^{\varphi}[G_l, G_l^{\varphi}] = 1.$$

Portanto, $\nu(G)$ é solúvel de comprimento derivado no máximo $l+1$. ∎

2.5 A Estrutura de $\nu(G)$ Quando $G = N \rtimes H$

Agora, vamos descrever a estrutura do grupo $\nu(G)$ quando G é um produto semidireto $N \rtimes H$, isto é, $N, H \leq G$, $N \trianglelefteq G$, $G = NH$ e $N \cap H = \{1\}$.

Proposição 2.5.1 *Sejam G um grupo, $N \trianglelefteq G$ e $H \leq G$. Suponhamos que $G = N \rtimes H$ é um produto semidireto. Então,*
(i) $\nu(G) = \langle N, N^{\varphi}\rangle[N, H^{\varphi}][H, N^{\varphi}] \rtimes \langle H, H^{\varphi}\rangle$;
(ii) $\langle H, H^{\varphi}\rangle \simeq \nu(H)$.

Demonstração: Observe que os subgrupos $[N, H^{\varphi}]$ e $[H, N^{\varphi}]$ são normais em $\nu(G)$. De fato, como $G = NH$, para qualquer elemento $g \in G$ existem $n \in N$ e $h \in H$ para os quais $g = nh$. Observe que pelas relações que definem $\nu(G)$ temos que H normaliza os subgrupos $[N, H^{\varphi}]$ e $[H, N^{\varphi}]$. Para verificar que N também normaliza os subgrupos $[N, H^{\varphi}]$ e $[H, N^{\varphi}]$ tomaremos $n_1, n_2 \in N$ e $h \in H$ quaisquer. Então,

$$[n_1, h^{\varphi}]^{n_2} = [n_1 n_2, h^{\varphi}][n_2, h^{\varphi}]^{-1} \in [N, H^{\varphi}].$$

De modo que N normaliza $[N, H^{\varphi}]$. Analogamente,

$$[h, n_1^{\varphi}]^{n_2} = [h, n_1^{\varphi}]^{n_2^{\varphi}} = [h, n_2^{\varphi}]^{-1}[h, n_1^{\varphi} n_2^{\varphi}] \in [H, N^{\varphi}].$$

Portanto, N normaliza $[H, N^{\varphi}]$ e, consequentemente, G normaliza os subgrupos $[N, H^{\varphi}]$ e $[H, N^{\varphi}]$. Pelas relações de $\nu(G)$ segue analogamente que G^{φ} normaliza os subgrupos $[N, H^{\varphi}]$ e $[H, N^{\varphi}]$. Agora, queremos mostrar que

$$\nu(G) = \langle N, N^{\varphi}\rangle[N, H^{\varphi}][H, N^{\varphi}] \rtimes \langle H, H^{\varphi}\rangle.$$

Notemos que

$$[N, N^{\varphi}H^{\varphi}] \leq [N, H^{\varphi}][N, N^{\varphi}] \quad \text{e} \quad [NH, N^{\varphi}] \leq [N, N^{\varphi}][H, N^{\varphi}],$$

pois, $[N, N^\varphi] \trianglelefteq \nu(G)$. Logo, podemos verificar pela Proposição 2.1.1 para $G = N \rtimes H$, que o núcleo do epimorfismo $\tilde{\pi} : \nu(G) \twoheadrightarrow \nu(\frac{G}{N})$, induzido pelo epimorfismo natural $\pi : G \twoheadrightarrow \frac{G}{N}$, é

$$\begin{aligned}\ker\tilde{\pi} &= \langle N, N^\varphi\rangle[N, N^\varphi H^\varphi][NH, N^\varphi]\\ &= \langle N, N^\varphi\rangle[N, N^\varphi][N, H^\varphi][H, N^\varphi]\\ &= \langle N, N^\varphi\rangle[N, H^\varphi][H, N^\varphi].\end{aligned}$$

Como $N \cap H = 1$, segue que

$$\ker\tilde{\pi} \cap \langle H, H^\varphi\rangle = \{1\}.$$

Agora, pelo Teorema 2.4.1, podemos escrever

$$\nu(G) = \nu(NH) = ([NH, N^\varphi H^\varphi] \rtimes NH) \rtimes N^\varphi H^\varphi.$$

Mas,

$$\begin{aligned}[NH, N^\varphi H^\varphi] &\leq [N, N^\varphi][N, H^\varphi][H, N^\varphi][H, H^\varphi]\\ &\leq \langle N, N^\varphi\rangle[N, H^\varphi][H, N^\varphi]\langle H, H^\varphi\rangle.\end{aligned}$$

Além disso,

$$NH \cdot N^\varphi H^\varphi \leq \langle N, N^\varphi\rangle[N, H^\varphi][H, N^\varphi]\langle H, H^\varphi\rangle.$$

Como a inclusão contrária acontece, a afirmação é verdadeira.
(ii) Para a prova deste item, tomaremos o epimorfismo $\tilde{\pi} : \nu(G) \twoheadrightarrow \nu(\frac{G}{N})$ como na Proposição 2.1.1 e restringiremos ao subgrupo $\langle H, H^\varphi\rangle$. Então,

$$(\langle H, H^\varphi\rangle)^{\tilde{\pi}} = \nu\left(\frac{G}{N}\right) \simeq \nu(H),$$

pois, $G = N \rtimes H$. Pelo item (i) vimos que $\ker\tilde{\pi} \cap \langle H, H^\varphi\rangle = \{1\}$. Logo,

$$\langle H, H^\varphi\rangle \simeq \frac{\langle H, H^\varphi\rangle}{\ker\tilde{\pi} \cap \langle H, H^\varphi\rangle} \simeq (\langle H, H^\varphi\rangle)^{\tilde{\pi}} = \nu\left(\frac{G}{N}\right) \simeq \nu(H).$$

Como queríamos. ■

Proposição 2.5.2 *Sejam G um grupo, H e N subgrupos normais de G. Suponha que $G = N \times H$ seja um produto direto. Então,*
(i) $\nu(G) = \langle N, N^\varphi\rangle[N, H^\varphi][H, N^\varphi]\langle H, H^\varphi\rangle$;
(ii) $\langle N, N^\varphi\rangle \simeq \nu(N)$ *e* $\langle H, H^\varphi\rangle \simeq \nu(H)$;
(iii) $\Upsilon(G) \simeq \Upsilon(N) \times \Upsilon(H) \times [N, H^\varphi][H, N^\varphi]$.

Demonstração: *(i)* Segue diretamente do item (i) da Proposição 2.5.1.
(ii) Considerando epimorfismos $\tilde{\pi}_1 : \nu(G) \twoheadrightarrow \nu(\frac{G}{N})$ e $\tilde{\pi}_2 : \nu(G) \twoheadrightarrow \nu(\frac{G}{H})$ como na Proposição

2.1.1. O resultado segue do item (ii) Proposição 2.5.1.
(iii) Dado que $G = N \times H$, temos

$$\Upsilon(G) = [NH, N^{\varphi}H^{\varphi}] = [N, N^{\varphi}][H, H^{\varphi}][H, N^{\varphi}][N, H^{\varphi}].$$

Mas, pelo item anterior,

$$[N, N^{\varphi}] \simeq \Upsilon(N) \quad \text{e} \quad [H, H^{\varphi}] \simeq \Upsilon(H),$$

$$\langle N, N^{\varphi}\rangle \cap ([N, H^{\varphi}][H, N^{\varphi}]\langle H, H^{\varphi}\rangle) = \{1\},$$

$$(\langle N, N^{\varphi}\rangle[N, H^{\varphi}][H, N^{\varphi}]) \cap \langle H, H^{\varphi}\rangle = \{1\}.$$

Em particular, as relações que definem $\nu(G)$ nos mostram que os subgrupos

$$[N, N^{\varphi}], [H, N^{\varphi}], [N, H^{\varphi}], [H, H^{\varphi}],$$

são todos normais em $\nu(G)$. Logo, podemos descrever $\Upsilon(G)$ como

$$\Upsilon(G) \simeq \Upsilon(N) \times \Upsilon(H) \times [N, H^{\varphi}][H, N^{\varphi}].$$

Como a interseção $[N, H^{\varphi}] \cap [H, N^{\varphi}]$ pode não ser trivial, pois, se $H' \neq \{1\}$ e $[n, [h_1, h_2]^{\varphi}] \in [N, H^{\varphi}]$, então

$$[n, [h_1, h_2]^{\varphi}] = [[h_1, h_2]^{\varphi}, n]^{-1} \overset{2.1.1(ii)}{=} [[h_1, h_2], n^{\varphi}]^{-1} \in [H, N^{\varphi}],$$

segue que

$$\Upsilon(G) \simeq \Upsilon(N) \times \Upsilon(H) \times [N, H^{\varphi}][H, N^{\varphi}].$$

■

Corolário 2.5.1 *Seja G um grupo nilpotente finito e $\pi(G) = \{p_1, p_2, \cdots, p_n\}$ o conjunto de primos que dividem a ordem de G. Então,*
(i) $\nu(G) \simeq \nu(P_1) \times \cdots \times \nu(P_n)$;
(ii) $\Upsilon(G) \simeq \Upsilon(P_1) \times \cdots \times \Upsilon(P_n)$,
onde cada P_i é um p_i-subgrupo de Sylow de G, para $i = 1, 2, \cdots, n$.

Demonstração: As demonstrações de (i) e (ii) seguem simultaneamente. Como G é um grupo finito, podemos dizer que

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

onde cada p_i é um número primo com $p_i \neq p_j$ sempre que $i \neq j$ e $\alpha_i \in \mathbb{N}$. Agora, usando indução em n, vemos que se $n = 1$, então $|G| = p_1^{\alpha_1}$, e o resultado segue trivialmente. Para o caso $n = 2$, temos $|G| = p_1^{\alpha_1} p_2^{\alpha_2}$. Denote por P_1 e P_2 os p_i-subgrupos de Sylow de G, $i = 1, 2$. Então, $G = P_1 \times P_2$, pois G é nilpotente, e pela Proposição 2.5.2

$$\nu(G) = \langle P_2, P_2^{\varphi}\rangle[P_1, P_2^{\varphi}][P_2, P_1^{\varphi}]\langle P_1, P_1^{\varphi}\rangle,$$

$$\Upsilon(G) \simeq \Upsilon(P_1) \times \Upsilon(P_2) \times [P_1, P_2^{\varphi}][P_2, P_1^{\varphi}].$$

Como elementos de ordens coprimas de um grupo nilpotente comutam [Corolário 1.2.1], segue do item (ii) do Lema 2.1.3 que

$$[P_1, P_2^{\varphi}] = [P_2, P_1^{\varphi}] = \{1\}.$$

Portanto,

$$\nu(G) = \langle P_2, P_2^{\varphi}\rangle\langle P_1, P_1^{\varphi}\rangle \simeq \nu(P_1)\nu(P_2),$$

$$\Upsilon(G) \simeq \Upsilon(P_1) \times \Upsilon(P_2).$$

Daí, como a ação por conjugação de $\langle P_1, P_1^{\varphi}\rangle$ em $\langle P_2, P_2^{\varphi}\rangle$ é trivial e a interseção de ambos também é trivial, segue que

$$\nu(G) = \langle P_1, P_1^{\varphi}\rangle \times \langle P_2, P_2^{\varphi}\rangle.$$

Agora, suponhamos que para algum $n \geq 2$, $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ e

$$\nu(G) \simeq \nu(P_1) \times \cdots \times \nu(P_n) \quad \text{e} \quad \Upsilon(G) \simeq \Upsilon(P_1) \times \cdots \times \Upsilon(P_n). \tag{2.12}$$

Então, para

$$|G| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}p_{n+1}^{\alpha_{n+1}}, \text{ com } p_{n+1} \neq p_i, i = 1, 2, \cdots, n,$$

temos $G = N \times P_{n+1}$, onde $N = P_1 \times \cdots \times P_n$ e $N \cap P_{n+1} = \{1\}$, pois G é nilpotente. Portanto, pela Proposição 2.5.2 e pelo item (ii) do Lema 2.1.3 que

$$\nu(G) \simeq \nu(N)[N, P_{n+1}^{\varphi}][P_{n+1}, N^{\varphi}]\nu(P_{n+1}) \overset{(2.12)}{\simeq} \nu(P_1) \times \cdots \times \nu(P_n) \times \nu(P_{n+1}).$$

Semelhantemente,

$$\Upsilon(G) \simeq \Upsilon(N) \times \Upsilon(P_{n+1}) \overset{(2.12)}{\simeq} \Upsilon(P_1) \times \cdots \times \Upsilon(P_n) \times \Upsilon(P_{n+1}).$$

∎

Capítulo 3

Critérios de Finitude (local) para $\Upsilon(G)$

O resultado a seguir é um corolário imediato de uma proposição de R. Brown, D. Johnson e E. Robertson [7, Proposição 5] que trata sobre a finitude do quadrado tensorial não abeliano de grupos finitos. Aqui, apresentaremos uma demonstração sem resultados de natureza homológica. Tal demonstração foi sugerida por N. Rocco.

Teorema 3.0.1 *Sejam π um conjunto de primos e G um grupo. Se G é finito (ou π-grupo finito), então o quadrado tensorial não abeliano $[G, G^{\varphi}]$ é finito (ou π-grupo finito), respectivamente. Em particular, $\nu(G)$ é finito (π-grupo finito), respectivamente.*

Demonstração: Dado G um grupo finito, como $\nu(G) \simeq ([G, G^{\varphi}] \rtimes G) \rtimes G^{\varphi}$ e $[G, G^{\varphi}] \trianglelefteq \nu(G)$, temos que

$$\left|\frac{\nu(G)}{[G, G^{\varphi}]}\right| = |G|^2 < +\infty.$$

Consideremos o epimorfismo

$$\begin{array}{rcl} \rho : [G, G^{\varphi}] & \rightarrow & G' \\ \prod_{i=1}^{n}[x_i, y_i^{\varphi}] & \longmapsto & \prod_{i=1}^{n}[x_i, y_i]. \end{array}$$

Pelo Teorema dos Isomorfismos $([G, G^{\varphi}] : \ker \rho) = |G'|$. Em particular,

$$\begin{array}{rcl} (\nu(G) : \ker \rho) & = & (\nu(G) : [G, G^{\varphi}])([G, G^{\varphi}] : \ker \rho) \\ & = & |G|^2 |G'| < +\infty. \end{array}$$

Pela Proposição 2.3.2, sabemos que $\ker \rho \leq Z(\nu(G))$. Logo, $(\nu(G) : Z(\nu(G)) < +\infty$. Portanto, pelo Teorema de Schur 1.3.1, $|\nu(G)'| < +\infty$. Mas, pelo Teorema 2.4.3, $[G, G^{\varphi}] \leq$

$\nu(G)'$. Logo, $|[G, G^{\varphi}]| < +\infty$, como queríamos e, em particular,

$$|\nu(G)| = |[G, G^{\varphi}]| \cdot |G| \cdot |G^{\varphi}| < +\infty.$$

Além disso, sendo G um π-grupo finito, então

$$\left|\frac{\nu(G)}{\ker \rho}\right| = |G|^2 |G'|$$

é um π-número. Mas, pela Proposição 2.3.2,

$$\left|\frac{\nu(G)}{Z(\nu(G))}\right| = n$$

é um π-número. Novamente, pelo Teorema de Schur 1.3.1, temos $\exp(\nu(G)')$ divide n, que por sua vez, é um π-número. Segue do Teorema 2.4.3 que $|[G, G^{\varphi}]|$ é um π-número. Portanto, $[G, G^{\varphi}]$ é um π-grupo finito e, consequentemente, $\nu(G)$ é um π-grupo finito. ■

Observação 3.1 Em [3, Proposição 3.2], R. Bastos, I. Nakaoka e N. Rocco obtiveram uma generalização desse resultado, levando em conta apenas o número de tensores, isto é, a cardinalidade do conjunto

$$T_{\otimes}(G) = \{[g, h^{\varphi}] \mid g, h \in G\}.$$

Definição 3.0.1 *Seja G um grupo. Dizemos que G é **localmente finito** se todo subgrupo finitamente gerado de G é finito.*

Exemplo 3.1 (1) Todo grupo finito é localmente finito.
(2) O grupo de Prüfer,

$$C_{p^{\infty}} := \bigcup_{n=1}^{\infty} C_{p^n}$$

é localmente finito.

Lema 3.0.1 (O. Schmidt) [20, Proposição 14.3.1] *Seja G um π-grupo localmente finito. Se $H \leq G$ e $N \trianglelefteq G$, então H e $\frac{G}{N}$ são $\pi-$grupos localmente finitos.*

Demonstração: Dado que $H \leq G$ e notando que todo subgrupo finitamente gerado L de H é também um subgrupo finitamente gerado de G, segue que L é π-grupo finito, pela hipótese sobre G. Agora, dado qualquer subgrupo finitamente gerado $\frac{K}{N}$ de $\frac{G}{N}$, suponhamos que

$$\frac{K}{N} = \langle Nk_1, Nk_2, \cdots, Nk_m \rangle.$$

Então,

$$K = \langle k_1, k_2, \cdots, k_m, N \rangle.$$

Mas, pela hipótese sobre G, segue que $|\langle k_1, k_2, \cdots, k_m \rangle| < \infty$. Logo,

$$\frac{\langle k_1, k_2, \cdots, k_m \rangle}{\langle k_1, k_2, \cdots, k_m \rangle \cap N} \simeq \frac{\langle k_1, k_2, \cdots, k_m \rangle N}{N} = \frac{K}{N}$$

implica que $\frac{K}{N}$ é π-grupo finito, como queríamos demonstrar. ■

Lema 3.0.2 (O. Schmidt) [20, Proposição 14.3.1] *Seja G um π-grupo, tal que $N \trianglelefteq G$ e $\frac{G}{N}$ são ambos π-grupos localmente finitos. Então, G é um π-grupo localmente finito.*

Demonstração: Seja K um subgrupo finitamente gerado de G. Então, o quociente

$$\frac{K}{K \cap N} \simeq \frac{KN}{N} \leq \frac{G}{N}$$

é finitamente gerado e, pela hipótese sobre $\frac{G}{N}$, é π-grupo finito. Em particular, segue que $K \cap N$ é finitamente gerado, pois é subgrupo de índice finito de um grupo finitamente gerado [Lema 1.3.4]. Logo, pela hipótese sobre N, $K \cap N$ é π-grupo finito. Logo, pelo Teorema de Lagrange, K é π-grupo finito. ■

Consequentemente, a classe de π-grupos localmente finitos é fechada para extensões, quocientes, e formação de subgrupos. O próximo resultado é uma consequência do Teorema de Schur 1.3.1.

Lema 3.0.3 (I. Schur) *Seja G um grupo tal que $\frac{G}{Z(G)}$ é um π-grupo localmente finito. Então, o subgrupo derivado G' é um π-grupo localmente finito.*

Demonstração: Suponhamos que $\frac{G}{Z(G)}$ é um π-grupo localmente finito. Seja K um subgrupo finitamente gerado de G'. Então, existem $\alpha_1, \alpha_2, \cdots, \alpha_n$ e $\beta_1, \beta_2, \cdots, \beta_m \in G$, tais que

$$K \subseteq \langle [\alpha_1, \beta_1], \cdots, [\alpha_n, \beta_m] \rangle \subseteq H',$$

onde

$$H = \langle \alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_m \rangle.$$

Daí, é suficiente mostrarmos que H' é π-grupo finito. De fato, como $\frac{H}{Z(G) \cap H}$ é finitamente gerado e

$$\frac{H}{Z(G) \cap H} \simeq \frac{HZ(G)}{Z(G)} \leq \frac{G}{Z(G)},$$

pela hipótese sobre $\frac{G}{Z(G)}$, segue que $\frac{H}{Z(G) \cap H}$ é π-grupo finito. Além disso, note que a finitude de $\frac{H}{Z(G) \cap H}$ implica que $\frac{H}{Z(H)}$ é π-grupo finito. Portanto, segue do Teorema 1.3.1 que H' é π-grupo finito. Consequentemente, $K \leq H'$ é um π-grupo finito. Segue que G' é um π-grupo localmente finito. ■

Teorema 3.0.2 *Seja G um grupo localmente finito (π-grupo localmente finito). Então, $\nu(G)$ é localmente finito (π-grupo localmente finito), respectivamente.*

Demonstração: Consideremos o epimorfismo

$$\begin{array}{rcl} \rho : [G, G^{\varphi}] & \twoheadrightarrow & G' \\ \prod_{i=1}^{n} [x_i, y_i^{\varphi}] & \longmapsto & \prod_{i=1}^{n} [x_i, y_i], \end{array}$$

visto anteriormente [Proposição 2.3.2]. Usando a decomposição de $\nu(G)$ como $([G, G^{\varphi}] \rtimes G) \rtimes G^{\varphi}$, e o Lema 3.0.1, os quocientes

$$\frac{\nu(G)}{[G, G^{\varphi}]} \simeq G \times G \ \text{ e } \ \frac{[G, G^{\varphi}]}{\ker \rho} \simeq G',$$

são π-grupos localmente finitos. Em particular, pelo Teorema do Isomorfismo e pelo Lema 3.0.2, $\frac{\nu(G)}{\ker \rho}$ é um π-grupo localmente finito. Por outro lado, usando que $\ker \rho \leq Z(\nu(G))$, junto com o Lema 3.0.1 e o Teorema do Isomorfismo, temos $\frac{\nu(G)}{Z(\nu(G))}$ é um π-grupo localmente finito. Daí, segue do Lema 3.0.3 que $\nu(G)'$ é um π-grupo localmente finito. Novamente pelo Lema 3.0.1, $[G, G^{\varphi}] \leq \nu(G)'$ é um π-grupo localmente finito, e pelo Lema 3.0.2 segue que $\nu(G)$ é um π-grupo localmente finito, como queríamos. ∎

Observação 3.2 O resultado acima foi demonstrado originalmente por P. Moravec em [17, Teorema 1]. Entretanto, a demonstração apresentada aqui tem vantagens de ser elementar e não envolver técnicas "homológicas".

3.1 Uma Estimativa para a Ordem de $\Upsilon(G)$

Nesta seção, apresentaremos os demais resultados encontrados em [21]. Restringiremos nossa análise do grupo $\nu(G)$ quando G for um p-grupo finito, onde p é um número primo. Neste caso, pelo Teorema 3.0.1, $\Upsilon(G)$ é finito. Com isso, nosso objetivo é obter uma estimativa para a ordem do quadrado tensorial não abeliano $\Upsilon(G)$.

Lema 3.1.1 *Sejam G um p-grupo finito não abeliano e $c \in Z(G) \cap G'$ um elemento de ordem p. Se $\Phi(G)$ denota o subgrupo de Frattini de G, então*

$$|\nu(G)| \quad \textit{divide} \quad p^2 \cdot \left| \frac{G}{\Phi(G)} \right| \cdot \left| \nu\left(\frac{G}{\langle c \rangle} \right) \right|.$$

Demonstração: Dado que G é um p-grupo finito, pela Proposição 1.1.3, G é nilpotente com centro $Z(G)$ não trivial, logo, pela Proposição 1.2.5 e pelo Lema de Cauchy [23, Lema 4.1] para grupos abelianos finitos, existe um elemento $c \in Z(G) \cap G'$ de ordem p, em particular, $\langle c \rangle \trianglelefteq G$. Considerando o epimorfismo canônico

$$\begin{aligned} \pi : \ G &\twoheadrightarrow \frac{G}{\langle c \rangle} \\ g &\mapsto \langle c \rangle g, \end{aligned}$$

sabemos [Proposição 2.1.1] que π dá origem a um epimorfismo $\tilde{\pi} : \nu(G) \twoheadrightarrow \nu\left(\frac{G}{\langle c \rangle}\right)$, cujo núcleo é dado por

$$\begin{aligned} \ker \tilde{\pi} &= \langle c, c^{\varphi} \rangle [\langle c \rangle, G^{\varphi}][G, \langle c^{\varphi} \rangle] \\ &= \langle c \rangle \langle c^{\varphi} \rangle [c, G^{\varphi}][G, c^{\varphi}], \end{aligned}$$

pois, pelos Lemas 2.1.1 (v) e 2.1.3 (i)

$$[c, c^{\varphi}] = 1 \quad \text{e} \quad [c^m, g^{\varphi}] = [c, (g^m)^{\varphi}], \text{ para todos } g \in G, m \in \mathbb{Z}.$$

Em particular,

$$|\ker \tilde{\pi}| \text{ divide } p^2 \cdot |[c, G^{\varphi}][G, c^{\varphi}]|,$$

e pelo Teorema do Isomorfismo de grupos

$$|\nu(G)| \;=\; |\ker \tilde{\pi}| \cdot \left|\nu\left(\frac{G}{\langle c\rangle}\right)\right| \quad \text{divide} \quad p^2 \cdot |[c, G^{\varphi}][G, c^{\varphi}]| \cdot \left|\nu\left(\frac{G}{\langle c\rangle}\right)\right|.$$

Nos resta calcular a ordem de $[c, G^{\varphi}][G, c^{\varphi}]$. Entretanto, notemos que pelo Lema 2.1.1 (vi), em $[c, G^{\varphi}][G, c^{\varphi}]$, o produto $[c, g^{\varphi}][g, c^{\varphi}]$ é trivial para todos $g \in G$, $c \in G'$, e suponhamos que

$$\frac{G}{\Phi(G)} := \langle \overline{a_1}, \overline{a_2}, \cdots, \overline{a_d} \mid a_i \in G, i = 1, 2, \cdots, d\rangle.$$

Pelo Teorema 1.2.2 (Teorema da Base de Burnside),

$$G := \langle a_1, a_2, \cdots, a_d\rangle.$$

Logo, para $a_{j_s} \in \{a_1, a_2, \cdots, a_d\}$, temos

$$\begin{aligned}
[c, (a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_k}^{i_k})^{\varphi}] &= [c, (a_{j_k}^{i_k})^{\varphi}][c, (a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_{k-1}}^{i_{k-1}})^{\varphi}]^{(a_{j_k}^{i_k})^{\varphi}} \\
&\overset{2.3.1\,(iii)}{=} [c, (a_{j_k}^{i_k})^{\varphi}][c, (a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_{k-1}}^{i_{k-1}})^{\varphi}] \\
&= \cdots \\
&= [c, (a_{j_k}^{i_k})^{\varphi}][c, (a_{j_{k-1}}^{i_{k-1}})^{\varphi}] \cdots [c, (a_{j_2}^{i_2})^{\varphi}][c, (a_{j_1}^{i_1})^{\varphi}] \\
&\overset{2.1.3\,(i)}{=} [c, (a_{j_k})^{\varphi}]^{i_k}[c, (a_{j_{k-1}})^{\varphi}]^{i_{k-1}} \cdots [c, (a_{j_2})^{\varphi}]^{i_2}[c, (a_{j_1})^{\varphi}]^{i_1} \\
&\overset{2.3.1\,(iii)}{=} [c, a_d^{\varphi}]^{l_d}[c, a_{d-1}^{\varphi}]^{l_{d-1}} \cdots [c, a_1^{\varphi}]^{l_1}.
\end{aligned}$$

Agora, notemos que para todos $g, h \in G$ e $c \in Z(G)$, temos, em $\nu(G)$, que

$$[g, c^{\varphi}]^h = [g, c^{\varphi}]^{h^{\varphi}} = [g, c^{\varphi}][g, c^{\varphi}, h^{\varphi}] \overset{2.1.1\,(ii)}{=} [g, c^{\varphi}][g, c, h^{\varphi}] = [g, c^{\varphi}]. \tag{3.1}$$

Logo,

$$\begin{aligned}
[(a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_k}^{i_k}), c^{\varphi}] &= [(a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_{k-1}}^{i_{k-1}}), c^{\varphi}]^{a_{j_k}^{i_k}}[a_{j_k}^{i_k}, c^{\varphi}] \\
&\overset{(3.1)}{=} [(a_{j_1}^{i_1} a_{j_2}^{i_2} \cdots a_{j_{k-1}}^{i_{k-1}}), c^{\varphi}][a_{j_k}^{i_k}, c^{\varphi}] \\
&= \cdots \\
&= [a_{j_1}^{i_1}, c^{\varphi}][a_{j_2}^{i_2}, c^{\varphi}] \cdots [a_{j_k}^{i_k}, c^{\varphi}] \\
&\overset{2.1.3\,(i)}{=} [a_{j_1}, c^{\varphi}]^{i_1}[a_{j_2}, c^{\varphi}]^{i_2} \cdots [a_{j_k}, c^{\varphi}]^{i_k} \\
&= [a_d, c^{\varphi}]^{l_d}[a_{d-1}, c^{\varphi}]^{l_{d-1}} \cdots [a_1, c^{\varphi}]^{l_1}.
\end{aligned}$$

Logo,

$$[c, G^{\varphi}][G, c^{\varphi}] = \langle [c, a_1^{\varphi}], [c, a_2^{\varphi}], \cdots, [c, a_{d-1}^{\varphi}], [c, a_d^{\varphi}], [a_1, c^{\varphi}], [a_2, c^{\varphi}], \cdots, [a_{d-1}, c^{\varphi}], [a_d, c^{\varphi}] \rangle.$$

Mas, como o produto $[c, a_i^{\varphi}][a_i, c^{\varphi}]$ é trivial para todos $i = 1, 2, \cdots, d$, $c \in G'$, segue que

$$[c, G^{\varphi}][G, c^{\varphi}] = [c, G^{\varphi}] = [G, c^{\varphi}] = \langle [c, a_1^{\varphi}][c, a_2^{\varphi}], \cdots, [c, a_{d-1}^{\varphi}], [c, a_d^{\varphi}] \rangle.$$

Portanto, nosso problema se resumiu em calcular a ordem de $[c, G^{\varphi}]$. Sendo assim, consideremos a aplicação

$$\begin{aligned} \lambda : \ G &\to [c, G^{\varphi}] \\ g &\mapsto [c, g^{\varphi}]. \end{aligned}$$

Pela Proposição 2.3.1 (iii), λ é homomorfismo, já que

$$\lambda(g_1 g_2) = [c, g_1^{\varphi} g_2^{\varphi}] = [c, g_2^{\varphi}][c, g_1^{\varphi}]^{g_2^{\varphi}} = [c, g_1^{\varphi}][c, g_2^{\varphi}], \forall\, g_1, g_2 \in G.$$

Em particular, λ é um epimorfismo, pois

$$G := \langle a_1, a_2, \cdots, a_d \rangle \ \text{ e } \ [c, G^{\varphi}] := \langle [c, a_1^{\varphi}][c, a_2^{\varphi}], \cdots, [c, a_{d-1}^{\varphi}], [c, a_d^{\varphi}] \rangle.$$

Portanto, pelo Teorema do Isomorfismo de grupos

$$|G| = |\ker \lambda| \cdot |[c, G^{\varphi}]|.$$

Mas, $\Phi(G) \leq \ker \lambda$, pois como G é um p-grupo finito, pelo Teorema 1.2.2 (Teorema da Base de Burnside), $\Phi(G) = G'G^p$, onde $G^p := \langle x^p \,|\, x \in G \rangle$. Assim, se $y \in G'$, pela Proposição 2.3.1 (i) temos que $[c, y^{\varphi}] = 1$. Além disso, pelo Lema 2.1.3 (i) vemos que $[c, (x^p)^{\varphi}] = [c^p, x^{\varphi}] = 1$, para todo $x \in G$. Portanto, segue que

$$(G : \Phi(G)) = (G : \ker \lambda)(\ker \lambda : \Phi(G)) = |[c, G^{\varphi}]| \cdot (\ker : \Phi(G)).$$

Daí, $|[c, G^{\varphi}]|$ divide $(G : \Phi(G))$. Lembrando que

$$|\nu(G)| \quad \text{divide} \quad p^2 \cdot |[c, G^{\varphi}]| \cdot \left| \nu\left(\frac{G}{\langle c \rangle} \right) \right|.$$

Segue que,

$$|\nu(G)| \quad \text{divide} \quad p^2 \cdot \left| \frac{G}{\Phi(G)} \right| \cdot \left| \nu\left(\frac{G}{\langle c \rangle} \right) \right|.$$

como queríamos demonstrar. ■

Proposição 3.1.1 *Seja G um p-grupo finito de classe 2. Então,*

$$|\Upsilon(G)| \ \textit{divide} \ \left| G' \otimes_{\mathbb{Z}} \frac{G}{G'} \right| \cdot \left| \Upsilon\left(\frac{G}{G'} \right) \right|.$$

Demonstração: Dado que G é nilpotente de classe 2, segue que $G' \leq Z(G)$. Agora, consideremos o epimorfismo

$$\begin{array}{rcl} \tilde{\pi}: \ \nu(G) & \twoheadrightarrow & \nu\left(\dfrac{G}{G'}\right) \\ g & \longmapsto & G'g \\ g^{\varphi} & \longmapsto & (G')^{\varphi}g^{\varphi}. \end{array}$$

induzido pelo homomorfismo canônico

$$\begin{array}{rcl} \pi: \ G & \twoheadrightarrow & \dfrac{G}{G'} \\ g & \mapsto & G'g. \end{array}$$

Note que,

$$(\Upsilon(G))^{\tilde{\pi}} = \Upsilon\left(\frac{G}{G'}\right),$$

e pelo Teorema do Isomorfismo de grupos

$$\left|\frac{\Upsilon(G)}{\ker\tilde{\pi} \cap \Upsilon(G)}\right| = \left|\Upsilon\left(\frac{G}{G'}\right)\right|.$$

Dado que G' e $\frac{G}{G'}$ podem ser vistos como $\mathbb{Z}$-módulos, pela Proposição 1.5.4, o produto tensorial $G' \otimes_{\mathbb{Z}} \frac{G}{G'}$ existe e, pelo Teorema 1.5.1 e pela Proposição 1.5.5, $G' \otimes_{\mathbb{Z}} \frac{G}{G'}$ é finito. Portanto,

$$\left|G' \otimes_{\mathbb{Z}} \frac{G}{G'}\right| \cdot \left|\frac{\Upsilon(G)}{\ker\tilde{\pi} \cap \Upsilon(G)}\right| = \left|G' \otimes_{\mathbb{Z}} \frac{G}{G'}\right| \cdot \left|\Upsilon\left(\frac{G}{G'}\right)\right|.$$

Então, mostraremos que $|\ker\tilde{\pi} \cap \Upsilon(G)|$ divide $|G' \otimes_{\mathbb{Z}} \frac{G}{G'}|$. Mas, pela Observação 2.1, temos

$$\ker\tilde{\pi} \cap \Upsilon(G) = [G', G^{\varphi}][G, (G')^{\varphi}]. \tag{3.2}$$

Logo, nosso objetivo se resume a calcular a ordem de $[G', G^{\varphi}][G, (G')^{\varphi}]$. Para isso, afirmamos que $[G', G^{\varphi}][G, (G')^{\varphi}] = [G, (G')^{\varphi}]$. De fato, suponhamos que

$$G' := \langle c_1, c_2, \cdots, c_m\rangle \ \text{ e } \ \frac{G}{G'} := \langle \overline{d_1}, \overline{d_2}, \cdots, \overline{d_n}\rangle$$

Por um argumento análogo ao feito no lema anterior, vemos que $[G', G^{\varphi}][G, (G')^{\varphi}]$ é gerado pelo conjunto

$$\{[c_i, d_j^{\varphi}], [d_j, c_i^{\varphi}] \,|\, 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Mas, pelo Lema 2.1.1 (vi), em $[G', G^{\varphi}][G, (G')^{\varphi}]$ o produto $[c_i, d_j^{\varphi}][d_j, c_i^{\varphi}]$ é trivial para todo par (i, j). Portanto, $[G', G^{\varphi}][G, (G')^{\varphi}]$ é gerado pelo conjunto

$$\{[c_i, d_j^{\varphi}] \,|\, 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Consequentemente,

$$[G', G^{\varphi}][G, (G')^{\varphi}] = [G', G^{\varphi}].$$

Portanto, queremos calcular a ordem de $[G', G^{\varphi}]$. Sendo assim, dado que $G' \leq Z(G)$, pela Proposição 2.3.1 (*iii*), $[G', G^{\varphi}]$ é central em $\nu(G)$. Usando a Proposição 2.3.1 (*iii*) e o Lema 2.1.3 (*i*), vemos que

$$\begin{array}{rccc} \phi: & G' \times \frac{G}{G'} & \rightarrow & [G', G^{\varphi}] \\ & (c, \overline{d}) & \longmapsto & [c, d^{\varphi}] \end{array}$$

é $\mathbb{Z}$-biaditiva. Logo, pela Definição 1.5.8, existe um único $\mathbb{Z}$-homomorfismo

$$\begin{array}{rccc} \beta: & G' \otimes_{\mathbb{Z}} \frac{G}{G'} & \rightarrow & [G', G^{\varphi}] \\ & c \otimes \overline{d} & \longmapsto & [c, d^{\varphi}]. \end{array}$$

tal que $\beta(c \otimes \overline{d}) = \phi(c, \overline{d})$. Em particular, β é um epimorfismo, pois pela Proposição 2.3.1 (*i*), temos que $[G', (G')^{\varphi}] \overset{(*)}{=} 1$, além disso, para qualquer $g \in G$, existem $h \in G'$ e d_i com $i = 1, 2, \cdots, n$ tal que $g = d_i h$. Portanto, se $c \in G'$,

$$[c, (d_i h)^{\varphi}] = [c, h^{\varphi}][c, d_i^{\varphi}]^{h^{\varphi}} \overset{(*)}{=} [c, d_i^{\varphi}]^{h^{\varphi}} = [c, d_i^{\varphi}].$$

Sendo assim, pelo Teorema do Isomorfismo de grupos

$$|[G', G^{\varphi}]| \text{ divide } \left| G' \otimes_{\mathbb{Z}} \frac{G}{G'} \right|.$$

Portanto,

$$|\ker \tilde{\pi} \cap \Upsilon(G)| \text{ divide } \left| G' \otimes_{\mathbb{Z}} \frac{G}{G'} \right|.$$

E o resultado segue. ■

Corolário 3.1.1 *Seja G um p-grupo de classe menor ou igual a 2, com $|G| = p^n$ e $|G'| = p^m$. Então,*

$$|\Upsilon(G)| \textit{ divide } p^{n(n-m)}.$$

Demonstração: Suponhamos que G é nilpotente de classe 1. Então, G é abeliano e $G' = \{1\}$, em particular, $m = 0$ e

$$\Upsilon(G) \overset{2.2.1}{\simeq} G \otimes G \overset{1.6.1}{\simeq} G \otimes_{\mathbb{Z}} G.$$

Portanto, queremos mostrar que

$$|\Upsilon(G)| = |G \otimes_{\mathbb{Z}} G| \text{ divide } p^{n^2}.$$

Para isso, observemos que pelo Teorema sobre decomposição de grupos abelianos finitamente gerados [23, Teorema 6.5], temos

$$G \simeq C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_k}},$$

onde $\sum_{i=1}^{k} \alpha_i = n$. Logo,

$$G \otimes_{\mathbb{Z}} G = \left(\prod_{i=1}^{k} C_{p^{\alpha_i}}\right) \otimes_{\mathbb{Z}} \left(\prod_{i=1}^{k} C_{p^{\alpha_i}}\right) \overset{1.5.1}{\simeq} \prod_{i=1}^{k} \left(\prod_{j=1}^{k} C_{p^{\alpha_i}} \otimes_{\mathbb{Z}} C_{p^{\alpha_j}}\right). \tag{3.3}$$

Mas, pela Proposição 1.5.5, para cada $\alpha_{i_0} \in \{\alpha_1, \alpha_2, \cdots, \alpha_k\}$ temos que

$$|C_{p^{\alpha_{i_0}}} \otimes_{\mathbb{Z}} C_{p^{\alpha_j}}| \leq p^{\alpha_{i_0}}$$

para todo $j = 1, 2, \cdots, k$. Portanto, segue de (3.3) que

$$|G \otimes_{\mathbb{Z}} G| \leq p^{(\alpha_1+\alpha_2+\cdots+\alpha_k)k} \leq p^{n^2}.$$

Agora, se G é p-grupo de classe 2, então $G' \leq Z(G)$ e pela proposição anterior

$$|\Upsilon(G)| \text{ divide } \left|G' \otimes_{\mathbb{Z}} \frac{G}{G'}\right| \cdot \left|\Upsilon\left(\frac{G}{G'}\right)\right|. \tag{3.4}$$

Como $\frac{G}{G'}$ é abeliano, pelo mesmo argumento anterior segue que

$$\left|\Upsilon\left(\frac{G}{G'}\right)\right| = \left|\frac{G}{G'} \otimes_{\mathbb{Z}} \frac{G}{G'}\right| \text{ divide } p^{(n-m)^2}. \tag{3.5}$$

Para calcular a ordem de $\left|G' \otimes_{\mathbb{Z}} \frac{G}{G'}\right|$, suponhamos que

$$G' \simeq C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_k}} \text{ e } \frac{G}{G'} \simeq C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_s}},$$

onde $\sum_{i=1}^{k} \alpha_i = m$ e $\sum_{j=1}^{s} \beta_j = n - m$. Novamente, como

$$G' \otimes_{\mathbb{Z}} \frac{G}{G'} = \left(\prod_{i=1}^{k} C_{p^{\alpha_i}}\right) \otimes_{\mathbb{Z}} \left(\prod_{j=1}^{s} C_{p^{\beta_j}}\right) \overset{1.5.1}{\simeq} \prod_{i=1}^{k} \left(\prod_{j=1}^{s} C_{p^{\alpha_i}} \otimes_{\mathbb{Z}} C_{p^{\beta_j}}\right),$$

Segue pelo mesmo argumento para a estimativa de $|G \otimes_{\mathbb{Z}} G|$ que

$$\left|G' \otimes_{\mathbb{Z}} \frac{G}{G'}\right| \text{ divide } p^{m(n-m)}. \tag{3.6}$$

Portanto, segue de (3.4), (3.6) e (3.5) que

$$|\Upsilon(G)| \text{ divide } p^{n(n-m)}.$$

■

Teorema 3.1.1 *Seja G um p-grupo finito com $|G| = p^n$ e $|G'| = p^m$. Então,*

$$|\nu(G)| \textit{ divide } p^{n^2+2n-mn}.$$

Demonstração: Como

$$|\nu(G)| = |\Upsilon(G)| \cdot |G|^2, \tag{3.7}$$

é suficiente estimar a ordem de $\Upsilon(G)$. Façamos indução sobre a ordem $|G| = p^n$. Se G é nilpotente de classe ≤ 2, pelo resultado anterior

$$|\Upsilon(G)| \text{ divide } p^{n(n-m)} \text{ e, consequentemente, } |\nu(G)| \text{ divide } p^{n^2+2n-mn}.$$

Sem perda de generalidade, tomemos G de classe ≥ 3. Então, pela Proposição 1.2.5, $\gamma_3(G) \cap Z(G) \neq \{1\}$. Logo, existe um elemento $c \in \gamma_3(G) \cap Z(G)$ de ordem p. Em particular, $\langle c \rangle \trianglelefteq G$, $c \in G' \cap Z(G)$ e

$$\left|\frac{G}{\langle c \rangle}\right| = p^{n-1} \text{ e } \left|\frac{G'}{\langle c \rangle}\right| = p^{m-1}.$$

Suponhamos, por hipótese de indução, que

$$\left|\nu\left(\frac{G}{\langle c \rangle}\right)\right| \text{ divide } p^{(n-1)^2+2(n-1)-(n-1)(m-1)}.$$

Então, pelo Lema 3.1.1, temos

$$|\nu(G)| \text{ divide } p^2 \cdot \left|\frac{G}{\Phi(G)}\right| \cdot p^{(n-1)^2+2(n-1)-(n-1)(m-1)}. \tag{3.8}$$

Agora, pelo Teorema 1.2.2 (Teorema da Base de Burnside), temos que o subgrupo de Frattini é dado por $\Phi(G) = G'G^p$, logo

$$\left|\frac{G}{\Phi(G)}\right| \text{ divide } \left|\frac{G}{G'}\right| = p^{n-m}.$$

Sendo assim, usando (3.8), temos que

$$|\nu(G)| \text{ divide } p^{n^2+2n-mn},$$

como queríamos demonstrar. ■

Corolário 3.1.2 *Sejam G um p-grupo finito, com $|G| = p^n$, $|G'| = p^m$, e d o número minimal de geradores de G. Então,*

$$p^{d^2} \leq |\Upsilon(G)| \leq p^{n(n-m)}.$$

Demonstração: Como $|\nu(G)| = |\Upsilon(G)| \cdot |G|^2$, pelo teorema anterior, temos que

$$|\Upsilon(G)| \cdot |G|^2 \text{ divide } p^{n^2+2n-mn}.$$

Em particular,

$$|\Upsilon(G)| \text{ divide } p^{n(n-m)}.$$

Agora, dado que d é o número minimal de geradores de G, pelo Teorema da Base de Burnside, $\frac{G}{\Phi(G)}$ é um p-grupo abeliano elementar de ordem p^d. Considerando o epimorfismo,

$$\begin{aligned} \tilde{\pi}: \ \nu(G) & \twoheadrightarrow \nu\left(\frac{G}{\Phi(G)}\right) \\ g & \longmapsto \overline{g} \\ g^{\varphi} & \longmapsto \overline{g^{\varphi}}. \end{aligned}$$

induzido pelo epimorfismo canônico $\pi : G \twoheadrightarrow \frac{G}{\Phi(G)}$, temos pela Proposição 2.2.1 e pelo Teorema 1.6.1, que

$$(\Upsilon(G))^{\tilde{\pi}} = \Upsilon\left(\frac{G}{\Phi(G)}\right) = \left[\frac{G}{\Phi(G)}, \left(\frac{G}{\Phi(G)}\right)^{\varphi}\right] \simeq \frac{G}{\Phi(G)} \otimes_{\mathbb{Z}} \frac{G}{\Phi(G)}.$$

Portanto, como $\ker \tilde{\pi} \cap \Upsilon(G) = [\Phi(G), G^{\varphi}][G, (\Phi(G))^{\varphi}]$, segue do Teorema do Isomorfismo de grupos e pelo Corolário 3.1.1 que

$$|\Upsilon(G)| \geq \left|\frac{G}{\Phi(G)} \otimes_{\mathbb{Z}} \frac{G}{\Phi(G)}\right| = p^{d^2}.$$

Portanto,

$$p^{d^2} \leq |\Upsilon(G)| \leq p^{n(n-m)}.$$

Como queríamos demonstrar. ■

A cota superior do resultado acima foi melhorada por R. Blyth, F. Fumagalli e M. Morigi, em [4], a saber

Proposição 3.1.2 [4, Proposição 3.2] *Sejam G um p-grupo finito de ordem p^n e d o número minimal de geradores de G. Então*

$$p^{d^2} \leq |\Upsilon(G)| \leq p^{nd}.$$

Mais ainda, G. Ellis e A. McDermott, em [12, Proposição 1], a estenderam para o produto tensorial não abeliano de um p-grupo finito e um q-grupo finito, onde p e q são primos, não necessariamente iguais.

Algumas generalizações do produto tensorial não abeliano de grupos e do grupo $\nu(G)$ foram feitas. R. Brown e G. Ellis introduziram o produto q-tensorial de grupos em seus trabalhos [6] e [11], onde q é um inteiro maior ou igual a 1. Por sua vez, T. Bueno e N. Rocco introduziram uma generalização $\nu^q(G)$ do grupo $\nu(G)$ em [9]. Em [18], considerando dois grupos G e H agindo compativelmente um sobre o outro e H^{φ} um cópia isomórfica de H, I. Nakaoka definiu o grupo

$$\eta(G,H) := \langle G \cup H^{\varphi} \mid [g,h^{\varphi}]^{g_1} = [g^{g_1},(h^{g_1})^{\varphi}], [g,h^{\varphi}]^{h_1^{\varphi}} = [g^{h_1},(h^{h_1})^{\varphi}], \forall\, g, g_1 \in G, h, h_1 \in H\rangle.$$

de modo que, quando $H = G$ e todas as ações são por conjugação, $\eta(G,G)$ coincide com o grupo $\nu(G)$. Para maiores detalhes sobre tais construções consulte [19].

REFERÊNCIAS

[1] BACON, M. R.; KAPPE, L. C. *The nonabelian tensor square of a 2-generator p-group of class 2*. Archiv der Mathematik, v. 61, n. 6, p. 508-516, 1993.

[2] BACON, M. R.; KAPPE, L. C.; MORSE, R. F. *On the nonabelian tensor square of a 2-Engel group*. Archiv der Mathematik, v. 69, n. 5, p. 353-364, 1997.

[3] BASTOS, R.; NAKAOKA, I. N.; ROCCO, N. R. *Finiteness conditions for the non-abelian tensor product of groups*. Monatshefte für Mathematik, DOI: 10.1007/s00605-0117-1143-x, 2016.

[4] BLYTH, R. D.; FUMAGALLI, F.; MORIGI, M. *Some structural results on the non-abelian tensor square of groups*. Journal of Group Theory, v. 13, n. 1, p. 83-94, 2010.

[5] BLYTH, R. D.; MORSE, R. F.; REDDEN, J. L. *On computing the non-abelian tensor squares of the free 2-Engel groups*. Proceedings of the Edinburgh Mathematical Society, v. 47, n. 2, p. 305-323, 2004.

[6] BROWN, R. *Q-perfect groups and universal Q-central extensions*. Publicacions Matemàtiques, p. 291-297, 1990.

[7] BROWN, R.; JOHNSON, D. L.; ROBERTSON, E. F. *Some computations of non-abelian tensor products of groups*. Journal of Algebra, v. 111, n. 1, p. 177-202, 1987.

[8] BROWN, R.; LODAY, J.L. *Van Kampen theorems for diagrams of spaces*. Topology, v. 26, n. 3, p. 311-335, 1987.

[9] BUENO, T. P.; ROCCO, N. R. *On the q-tensor square of a group*. Journal of Group Theory, v. 14, n. 5, p. 785-805, 2011.

[10] DENNIS, R. K. *In search of new homology functors having a close relationship to K-theory*. Preprint. Cornell University, 1976.

[11] ELLIS, G. J. *Tensor products and q-crossed modules.* Journal of the London Mathematical Society, v. 51, n. 2, p. 243-258, 1995.

[12] ELLIS, G.; MCDERMOTT, A. *Tensor products of prime-power groups.* Journal of Pure and Applied Algebra, v. 132, n. 2, p. 119-128, 1998.

[13] GILBERT, N. D. *The non-abelian tensor square of a free product of groups.* Archiv der Mathematik, v. 48, n. 5, p. 369-375, 1987.

[14] JOHNSON, D. L. *Presentations of groups.* Vol. 15. Cambridge University Press, 1997.

[15] MAGNUS, W.; KARRASS, A.; SOLITAR, D. *Combinatorial group theory: Presentations of groups in terms of generators and relations.* Courier Corporation, 2004.

[16] MILLER, C. *The second homology of group; Relations Among Commutators.* Proceedings of the American Mathematical Society v.3, n.4, p.588-595, 1952.

[17] MORAVEC, P. *The exponents of nonabelian tensor products of groups.* Journal of Pure and Applied Algebra, v. 212, n. 7, p. 1840-1848, 2008.

[18] NAKAOKA, I. N.*Non-abelian tensor products of solvable groups.* Journal of Group Theory, v. 3, n. 2, p. 157-168, 2000.

[19] NAKAOKA, I. N.; ROCCO, N. R. *A survey of non-abelian tensor products of groups and related constructions.* Boletim da Sociedade Paranaense de Matemática, v. 30, n. 1, p. 77-89, 2012.

[20] ROBINSON, D. J. S. *A Course in the Theory of Groups.* New York: Springer Science & Business Media, 1995. 2ª ed.

[21] ROCCO, N. R. *On a construction related to the non-abelian tensor square of a group.* Bulletin of the Brazilian Mathematical Society 22.1 (1991): 63-79.

[22] ROCCO, N. R. *A presentation for a crossed embedding of finite solvable groups.* Communications in Algebra, v. 22, n. 6, p. 1975-1998, 1994.

[23] ROTMAN, J. J. *A Introduction To The Theory of Groups.* Springer Science & Business Media, 1995 4ª ed.

[24] ROTMAN, J. J. *An introduction to homological algebra.* Springer Science & Business Media, 2008.

[25] SIDKI, S. *On weak permutability between groups.* Journal of Algebra, v. 63, n. 1, p. 186-225, 1980.

[26] WHITEHEAD, J. H.C. *A certain exact sequence.* Annals of Mathematics, 2nd Ser., Vol. 52, No. 1. p. 51-110, 1950.

Índice