Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Cálculo dos grupos $\nu(G)$ e $\nu(G)/\Delta(G)$ para grupos metacíclicos G e determinação de algumas de suas seções abelianas

por

Juliana Silva Canella

Brasília

2018

JULIANA SILVA CANELLA

Cálculo dos grupos $\nu(G)$ e $\nu(G)/\Delta(G)$ para grupos metacíclicos G e determinação de algumas de suas seções abelianas

Tese apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para a obtenção do grau de doutora em matemática

Tese de Doutorado

Orientador: Prof. Dr. Noraí Romeu Rocco

Brasilia

2018

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

CC221c

Canella, Juliana Silva
Cálculo dos grupos v(G) e v(G)/\Delta(G) para grupos metacíclicos G e determinação de algumas de suas seções abelianas / Juliana Silva Canella; orientador Noraí Romeu Rocco. -- Brasília, 2018.
116 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2018.

1. Grupos metacíclicos finitos. 2. Grupos metacíclicos infinitos. 3. Quadrado tensorial não abeliano. I. Rocco, Noraí Romeu , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Cálculo dos grupos $\gamma(G)$ e $\gamma(G)/\Delta(G)$,para grupos metacíclicos G e determinação de algumas de suas seções abelianas.

por

Juliana Silva Canella

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

DOUTORA EM MATEMÁTICA

Brasília, 16 de outubro de 2018.

Comissão Examinadora:

Prof. Dr. Noraí Romeu Rocco– Orientador (MAT-UnB)

Prof. Dr. Raimundo de Araújo Bastos Júnios (MAT-UnB)

Profa. Dra. Irene Naomi Nakaoka (UEM)

Prof. Dr. Ricardo Nunes de Oliveira (UFG)

DEDICATÓRIA

Dedico este trabalho aos meus três:
Ao meu pai, Lucio (in memoriam),
pelos seus ensinamentos, disciplina e dedicação.
Queria muito que estivesse presente neste momento!
A minha mãezinha, Cidinha, e à minha irmã, Daniela
Minha querida cooperativa...

Agradecimentos

É maravilhoso ter tantas pessoas incríveis a agradecer!

Ao meu orientador, Dr. Noraí Romeu Rocco, pelas horas absorvidas em conhecimento, pela paciência e confiança que depositou em mim, mesmo quando eu não achava ser possível.

À Professora Dra. Ticianne Proença Bueno Adorno, pela oportunidade de galgar meu mais lindo sonho, abrindo as portas para minha entrada no doutorado.

À Professora Dra. Shirlei Serconeck, por ter me despertado para o conhecimento e desenvolvimento da matemática e estimular meu amor pela Álgebra ainda na graduação quando monitora.

Aos amigos e parceiros de trabalho, Cleilton Aparecido Canal e Nathália Nogueira Gonçalves por todas as discussões, trocas de experiências, lamentos e risadas. Foi muito importante!

Aos amigos que o doutorado me deu: Alex Carrazedo, Camila Oliveira, Lais Moreira, Hiuri Reis, Hudson Piña, Daiane Soares Veras, Henrique Zanata, Edwin Salinas Reyes, Andréz Rosero, Jean Carlos Lelis, Yerko Contreas Rojas, Carol Lafetá, Danilo Sansão, Marcos Antônio Duarte, Welinton Gimarez, Michell L. Dias, Elson Leal, Bruno de Paula Miranda, Dióscoros Águiar Jr., Bruno Xavier, Valter Borges, Alireza Khatib, Elaine Cristine, Élis Gardel Mesquita, dentre tantos outros.

Aos Professores amigos Luciana Ávila, Jaqueline Godoy Mesquita, Daniele Nantes Sobrinho, João Paulo dos Santos, Marcelo Furtado, por todas as conversas, trabalhos, “ganbeis” e risadas.

Aos funcionários do Departamento de Matemática, com quem convivi tanto e tão longos dias. Em especial às secretárias Marta Adriana Souza, Bruna Vasconcelos, Cacau Queiroz e Solange da Matta.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico, pela bolsa de estudos e taxa de bancada concedidas durante o doutoramento.

À minha mãe, Cidinha Canella, por todo seu amor, carinho, confiança e confidências. Que em sua imensa sabedoria nunca exitou em me apoiar mesmo sem saber ao certo o que eu fazia. Te amo!

À minha irmã, Daniela Canella, pelas discussões sobre ciência e academia, pelo encorajamento e conselhos, pelos "sonhos compartilhados".

Aos amigos de longa data, que sempre se fizeram presentes, Franciely Jesus Guedes, Pablo Jacob Furlan, Valesca de Castro Almeida, Adriana Marcela Fonce Camacho, Esdra e Daiane Basílio, Flávio Silva, Marcos e Devs Oliveira, Lidiane Ayumi e Emerson de Melo, Juliana Fernandes, Gabriel Araújo, Paulo Henrique Rodrigues, por todo apoio e incentivo.

Aos amigos que Brasília me deu: Ana Paula Gabatteli Vieira, minha 'terapeuta', Graziela do Lago Maciel, Paula Machado Lacerda, Gabriel Franke Végas, Janaina Muniz Pedrosa, Lívia Pamplona de Miranda, Larissa Reis, Agda Sá por todos os 'caferem', conversas descontraídas, pelo não julgamento e leveza na amizade, pelo respeito.

Muito obrigada!

"Que eu continue confiando em mim
porque foi você que me criou assim
me acompanhe na jornada
e não me abandone nos desvios"

Hermínio Lucio Canella
(*in memoriam*)

Resumo

Nesta tese descrevemos o grupo $\nu(G)$, uma extensão do quadrado tensorial não abeliano de G pelo produto direto $G \times G$, para grupos metacíclicos finitos e infinitos G. Explicitamos várias das relevantes seções de $\nu(G)$, tais como o próprio quadrado tensorial, isomorfo ao subgrupo $[G, G^{\varphi}]$ de $\nu(G)$, o quadrado exterior, $G \wedge G$ e o multiplicador de Schur, $M(G)$, entre outras.

Palavras-chave: Grupos metacíclicos finitos, grupos metacíclicos infinitos, quadrado tensorial não abeliano.

Abstract

In this thesis we describe the group $\nu(G)$, an extension of the nonabelian tensor square of G by the direct product $G \times G$, for finite and infinite metacyclic groups G. We use such a description in order to express some of the relevant sections of $\nu(G)$ such as the nonabelian tensor square of G, here isomorphic to a subgroup $[G, G^{\varphi}]$ of $\nu(G)$, the nonabelian exterior square, $G \wedge G$, and the Schur multiplier, $M(G)$, among other sections.

Palavras-chave: Finite metacyclic groups, infinite metacyclic groups, nonabelian tensor square.

Lista de Símbolos

$\|G\|$	ordem do grupo ou do conjunto G
$H \leq G$	H é subgrupo de um grupo G
$H \trianglelefteq G$	H é subgrupo normal do grupo G
g^h	$(:= h^{-1}gh)$ conjugado de g por h
$[g, h]$	$(:= g^{-1}h^{-1}gh)$ comutador de g e h
$F(X)$	$(:= F)$ grupo livre sobre o conjunto X
$\langle X \rangle$	subgrupo gerado pelo conjunto X
X^G	fecho normal de X em G
$H \cong G$	isomorfismo entre os grupos H e G
$d(G)$	$(:= d)$ deficiência do grupo G
$o(x)$	ordem do elemento x
G'	$(:= [G, G])$ subgrupo derivado do grupo G
$o'(x)$	$(:= o(xG'))$ ordem de x relativo a G'
$G * H$	produto livre entre os grupos G e H
G_i	i-ésimo termo da série policíclica de G
$\mathcal{U}_m$	conjunto dos números inteiros relativamente primos com m
Φ	função Φ de Euler
G^{ab}	$(:= G/G')$ abelianizado do grupo G

$G \otimes H$	produto tensorial não abeliano dos grupos G e H
$G \otimes G$	quadrado tensorial não abeliano do grupo G
$\nu(G)$	grupo $\nu(G)$ de um grupo G qualquer
$G \ltimes H$	produto semidireto externo de G e H
GH	produto semidireto interno de G e H
$G \,]\, H$	produto semidireto parcial de G e H
$G \times H$	produto direto de G e H
$G \wedge G$	quadrado exterior do grupo G
$\Delta(G)$	grupo diagonal de G
$\Gamma(A)$	funtor quadrático de Whitehead do grupo abeliano A
$M(G)$	multiplicador de Schur do grupo G

Sumário

Introdução

O produto tensorial não abeliano de grupos G e H, denotado por $G \otimes H$, foi introduzido por Brown & Loday [9], e generaliza o produto tensorial usual de grupos abelianos. Esta é uma interessante construção em teoria de grupos que provém de aplicações do Teorema de Van Kampen generalizado [[9], §5] na Teoria de Homotopia.

O produto tensorial $G \otimes H$ é definido para qualquer par de grupos G e H, em que cada um deles age (à direita) sobre o outro e sobre si mesmo por conjugação, satisfazendo certas condições de compatibilidade. Especificamente, dados dois grupos G e H, munidos de uma ação (à direita), $(g, h) \mapsto g^h$ de H sobre G e uma ação $(h, g) \mapsto h^g$ de G sobre H, dizemos que G e H agem compativelmente um sobre o outro se as igualdades

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

ocorrem para todos $g, g_1 \in G,\ h, h_1 \in H$. Neste caso, o produto tensorial não abeliano de G e H, $G \otimes H$, é por definição o grupo gerado por todos os símbolos $g \otimes h$, $g \in G,\ h \in H$, satisfazendo as relações

$$\begin{aligned} gg_1 \otimes h &= (g^{g_1} \otimes h^{g_1})(g_1 \otimes h), \\ g \otimes hh_1 &= (g \otimes h_1)(g^{h_1} \otimes h^{h_1}), \end{aligned}$$

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

Em particular, como a ação por conjugação de um grupo G sobre si mesmo é compatível, então fica definido o *quadrado tensorial não abeliano* $G \otimes G$.

Dado o relacionamento do quadrado tensorial $G \otimes G$ com outros importantes invariantes de grupos, a computação desse objeto, para um dado grupo G, é de grande interesse, embora não seja uma tarefa fácil. Um método que segue decorrente a definição acima é o uso de transformações de Tietze para simplificar a apresentação e deduzir a sua estrutura [[10], §6]; esse método é pouco eficiente, uma vez que a apresentação dada envolve $|G|^2$ geradores e $2|G|^3$ relações. Outro método que tem sido mais frequentemente utilizado baseia-se na construção de uma *biderivação* [[3], páginas $658 - 659$], o que por sua vez demanda a "descoberta" de um candidato ao pretenso $G \otimes G$.

Um método que se mostrou mais eficiente, particularmente, para o cálculo do quadrado tensorial e de outros invariantes de grupos policíclicos, dados por uma apresentação policíclica, baseia-se numa construção introduzida por Rocco [34], em 1991 (veja também [[16], Theorem 1]), através de um operador ν na classe de grupos. Para um dado grupo G, considere uma cópia isomorfa G^{φ}, via o isomorfismo $\varphi : G \to G^{\varphi},\ g \mapsto g^{\varphi},\ \forall g \in G$. O grupo $\nu(G)$ é definido como sendo

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

Além do interesse grupo-teorético dessa construção, a motivação inicial para a sua introdução é que o subgrupo normal $[G, G^{\varphi}]$ de $\nu(G)$ é isomorfo ao quadrado tensorial $G \otimes G$, resultando em $\nu(G)$ ser uma extensão de $G \otimes G$ por $G \times G$. Uma vantagem de trabalhar-se dentro do grupo $\nu(G)$ é que o quadrado tensorial pode ser computado utilizando-se do cálculo de comutadores.

Neste trabalho exploramos essa abordagem para determinar tanto o grupo $\nu(G)$ quanto o quadrado tensorial $G \otimes G$ a partir da identificação estabelecida por [[34], Theorem 3.3]: $\nu(G) = ([G, G^{\varphi}]\ G)\ G^{\varphi}$, isomorfo ao produto $((G \otimes G) \rtimes G) \rtimes G$. Como consequência desta nossa abordagem, foi possível descrever também o quadrado exterior, $G \wedge G$, e o multiplicador de Schur, $M(G)$, entre outras seções de $\nu(G)$, para os grupos metacíclicos finitos e infinitos.

A partir de uma apresentação policíclica do grupo policíclico G, Blyth & Morse [8], estendendo resultados de Rocco [32] para grupos solúveis finitos, dão uma apresentação policíclica para $\nu(G)$. Isso proporciona a utilização de um algoritmo para o cálculo efetivo do quadrado tensorial não abeliano como subgrupo do grupo $\nu(G)$, o que permite o uso de ferramentas computacionais, como por exemplo o sistema GAP [18]. Ao longo da elaboração desta tese, fizemos o uso deste sistema; ao final, apresentamos um exemplo para ilustrar alguns dos comandos do sistema GAP para essa finalidade.

Um subgrupo que desempenha papel importante no estudo de $\nu(G)$ e suas seções é o chamado *subgrupo diagonal*, $\Delta(G)$, gerado por todos os elementos $[g, g^{\varphi}]$ com $g \in G$. Este subgrupo de $[G, G^{\varphi}]$ é central em $\nu(G)$ e o quociente $[G, G^{\varphi}]/\Delta(G)$ é isomorfo ao *quadrado exterior* de G, $G \wedge G$, que havia sido estudado por Miller [29].

A aplicação $\rho : \nu(G) \to G, g \mapsto g, g^{\varphi} \mapsto g$, para todo $g \in G$, induz um epimorfismo de $\nu(G)$ sobre G cujo núcleo, $\Theta(G)$, um subgrupo que centraliza $[G, G^{\varphi}]$ e é normal em $\nu(G)$. A restrição de ρ a $[G, G^{\varphi}]$ é a *aplicação derivada*, $\rho' : [G, G^{\varphi}] \to G', [g, h^{\varphi}] \mapsto [g, h]$, para todo $g, h \in G$, cujo núcleo, $\mu(G)$, possui aplicações em Teoria de Homologia [8]. De modo que $[G, G^{\varphi}]/\mu(G) \cong G'$. Além disso, $\mu(G)/\Delta(G)$ é isomorfo ao multiplicador de Schur, $M(G)$.

No **Capítulo 2**, coletamos algumas propriedades dos grupos metacíclicos finitos e infinitos. Dizemos que um *grupo finito* G, de ordem mn, é *metacíclico* gerado por a e b, se é definido pelas relações

$$a^m = 1, \quad b^n = a^s, \quad a^b = a^r$$

e satisfaz as seguintes condições numéricas:

$$\begin{array}{ll} (a) & 0 < m, n \\ (b) & r^n \equiv 1 \ (mod\ m) \\ (c) & s(r-1) \equiv 0 \ (mod\ m). \end{array}$$

Essas condições determinam, de fato, um grupo metacíclico de ordem mn, resultado esse devido a Hölder, que pode ser encontrado em [[45], Theorem 20]. Note que a quadra (m, n, r, s) determina completamente o grupo metacíclico finito $G := g(a, b; m, n, r, s)$. A partir da identificação do grupo G, enunciamos um resultado de Sims [[39], Lemma 2.7] a respeito do subgrupo derivado do grupo G, $G' = [G, G]$, e também sobre o centro do grupo G, $Z(G)$. Curtis & Reiner [[13], §(47.10)] já haviam verificado que a^{r-1} gera o subgrupo derivado de G e que este possui ordem exatamente igual a $m/(m, r-1)$. Com esta demonstração pudemos obter um dos principais resultados desta seção, a saber:

Proposição 0.0.1. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito, não abeliano. Então*

$$o'(a) = (m, r-1), \qquad o'(b) = \left(o(b),\ n\frac{s(r-1)}{(m,s)(s,r-1)}\right),$$

onde $o'(a)$ e $o'(b)$ são as ordens relativas às classes aG' e bG', respectivamente. Estes objetos, juntamente com a $o(b)$, são importantes para o cálculo das ordens de um conjunto gerador para o quadrado tensorial não abeliano do grupo G, visto como grupo isomorfo ao subgrupo $[G, G^{\varphi}]$ do grupo $\nu(G)$.

Na segunda seção deste mesmo Capítulo, tratamos dos grupos metacíclicos infinitos, classificados por Beuerle & Kappe [3]: se $G = g(a, b; m, n, r)$ é um grupo metacíclico infinito, então G é isomorfo ao grupo

$$\langle a, b \mid a^m = 1, b^n = 1, a^b = a^r \rangle,$$

onde $m, n, r \in \mathbb{Z}^+$, com $mn = 0$ e $r \in \mathcal{U}_m$, mostrando que grupos metacíclicos infinitos são sempre extensões cindidas e que ficam completamente identificados pela terna (m, n, r). Com um tratamento semelhante ao feito para os grupos metacíclicos finitos, obtemos o seguinte Lema como consequência da **Proposição 0.0.1**:

Lema 0.0.2. *Seja $g(a,b;m,n,r)$ um grupo metacíclico infinito. Então,*

$$o'(a) = (m, r-1), \qquad o'(b) = o(b) = n,$$

para m e n não simultaneamente nulos, finalizando assim nossas análises sobre os grupos metacíclicos finitos e infinitos.

O **Capítulo 3** tem como objetivo o cálculo do grupo $\nu(G)$ para grupos metacíclicos G. Na primeira parte tratamos dos grupos metacíclicos finitos e na segunda parte dos grupos metacíclicos infinitos.

A partir da análise das cotas para as ordens dos elementos geradores do grupo $[G, G^{\varphi}]$, $\{[a,b^{\varphi}], [a,a^{\varphi}], [b,b^{\varphi}], [a,b^{\varphi}][b,a^{\varphi}]\}$, obtemos apresentações para o grupo $\nu(G)$ quando $G = g(a,b;m,n,r,s)$, não abeliano ($r > 1$) e não cindido ($s > 0$) com m par (**Teorema A**) e com m ímpar (**Teorema B**). Como Corolários imediatos, obtemos as apresentações do grupo $\nu(G)$ quando $G = g(a,b;m,n,m-1,s)$, $s > 0$ e, por fim, quando $G = g(a,b;m,n,r,0)$, $r > 1$.

Ao estudarmos todas as potências e conjugações possíveis entre os elementos do conjunto gerador do quadrado tensorial, obtemos cotas para as suas ordens no grupo $[G, G^{\varphi}]$ e também relações importantes para a geração do grupo supracitado. É a partir destas relações que nos foi possível identificar e construir o grupo $\nu(G)$.

Como primeiro resultado envolvendo potências entre os elementos geradores do grupo $[G, G^{\varphi}]$, temos o Lema abaixo que nos sugere relações de potências envolvendo os números (n, r, s), independente da paridade de m:

Lema 0.0.3. *Seja $G = g(a,b;m,n,r,s)$ um grupo metacíclico finito. Então*

$$\begin{cases} [b,b^{\varphi}]^n = [a,b^{\varphi}]^s = [b,a^{\varphi}]^s, & se\ 2 \nmid s\ ou\ se\ 4 \mid s \\ [b,b^{\varphi}]^n = [a,b^{\varphi}]^s[a,a^{\varphi}]^{(r-1)} = [b,a^{\varphi}]^s[a,a^{\varphi}]^{(1-r)}, & se\ 2 \parallel s. \end{cases}$$

Antes de darmos prosseguimento aos resultados obtidos na primeira seção deste Capítulo, precisamos definir alguns números inteiros recorrentes e importantes para os cálculos das ordens dos elementos do conjunto gerador do grupo $[G, G^{\varphi}]$.

Para m um número inteiro não negativo, considere $\mathcal{U}_m = \{\bar{a} \in \mathbb{Z}_m \mid (a,m) = 1\}$ o grupo das unidades do anel $\mathbb{Z}_m$ e denote por s o menor inteiro positivo relativamente primo com m tal que $rs \equiv 1\ (mod\ m)$, sempre que $\bar{r} \in \mathcal{U}_m$.

Definição 0.0.4. [[3], Definition 2.1] *Defina a função $E_m : \mathcal{U}_m \times \mathbb{Z} \to \mathbb{Z}$ por*

$$E_m(r,x) = \begin{cases} x, & se\ r \equiv 1\ (mod\ m)\ ou\ x = 0 \\ 1 + r + \cdots + r^{x-1}, & se\ r \not\equiv 1\ (mod\ m)\ e\ x > 0 \\ -r^x E_m(r,-x), & se\ r \not\equiv 1\ (mod\ m)\ e\ x < 0 \end{cases}$$

O número inteiro $E_m(r,x)$ tem um papel importante na ordem dos elementos do grupo $[G, G^{\varphi}]$.

Com a mesma finalidade do número $E_m(r,x)$, considere o grupo metacíclico finito $G = g(a, b; m, n, r, s)$ determinado pela quadra (m, n, r, s):

Definição 0.0.5. *Para a quadra (m, n, r, s) definidora do grupo metacíclico finito $G = g(a, b; m, n, r, s)$, seja*

$$k := \left(\frac{m}{(m,s)}, 2\frac{[s, r-1]}{(m,s)}, n\frac{[s, r-1]^2}{(m,s)^2}, r-1, E_m(r, o(b)) \right).$$

Como resultados cruciais para a construção do grupo $\nu(G)$ para um grupo metacíclico finito $G = g(a, b; m, n, r, s)$, não abeliano, seguem as Proposições que estabelecem cotas para as ordens dos elementos do conjunto gerador do grupo $[G, G^{\varphi}]$ para m par e m ímpar, respetivamente, juntamente com as relações obtidas entre eles.

Proposição 0.0.6. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito, não abeliano com m par. Então, são cotas para as ordens dos elementos de um conjunto gerador do grupo $[G, G^{\varphi}]$:*

i) $[a, a^{\varphi}]$ tem ordem dividindo $(m, 2(r-1))$;

ii) $[b, b^{\varphi}]$ tem ordem dividindo nk;

iii) $[a, b^{\varphi}]$ tem ordem dividindo

$$\begin{cases} \begin{cases} (m, 2sk), & se\ 2 \nmid k \\ (m, sk), & se\ 2 \mid k \end{cases} & e\ \ 2 \parallel s, \\ (m, sk), \quad se\ 2 \nmid s\ ou\ se\ 4 \mid s; \end{cases}$$

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo

$$\begin{cases} (o'(a), o'(b), E_m(r, o'(b)), sk), & se\ 2 \nmid k, \\ (o'(a), o'(b), E_m(r, o'(b)), sk/2), & se\ 2 \mid k. \end{cases}$$

Ao longo da demonstração da **Proposição 0.0.6**, foram obtidas as seguintes relações entre os elementos do conjunto supracitado:

$$\begin{cases} [a, b^{\varphi}]^{E_m(r, o(b))} = [a, a^{\varphi}]^{-\frac{(r-1)^2}{2}\binom{o(b)}{2}}, \\ [b, a^{\varphi}]^{E_m(r, o(b))} = [a, a^{\varphi}]^{\frac{(r-1)^2}{2}\binom{o(b)}{2}}, \\ [a, b^{\varphi}]^{E_m(r, n)} = [a, a^{\varphi}]^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, \\ [b, a^{\varphi}]^{E_m(r, n)} = [a, a^{\varphi}]^{s+\frac{(r-1)^2}{2}\binom{n}{2}}. \end{cases}$$

Proposição 0.0.7. *Seja $G = g(a,b;m,n,r,s)$ um grupo metacíclico finito, não abeliano com m ímpar. Então, são cotas para as ordens dos elementos de um conjunto gerador do grupo $[G, G^{\varphi}]$:*

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, r-1)$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* nk;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* $(m, E_m(r, o(b)), sk)$;

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(o'(a), o'(b), E_m(r, o'(b)), sk)$.

As seguintes identidades satisfeitas no grupo $[G, G^{\varphi}]$ para $G = g(a,b;m,n,r,s)$ e m ímpar, foram obtidas a partir da demonstração **Proposição 0.0.7** e do **Lema 0.0.3**:

$$\begin{cases} [a, b^{\varphi}]^s = [b, a^{\varphi}]^s = [b, b^{\varphi}]^n, \\ [a, b^{\varphi}]^{E_m(r,n)} = [b, a^{\varphi}]^{E_m(r,n)} = [a, a^{\varphi}]^s. \end{cases}$$

Para a obtenção dos grupos $\nu(G)$ com $G = g(a,b;m,n,r,s)$, $r > 1$, $s > 0$ e m par do **Teorema A** (páginas $66-79$), definimos o grupo abeliano A, cujo geradores são u, v, w, z e as relações definidoras são as supracitadas obtidas na **Proposição 0.0.6**. A partir de uma adequada ação de G sobre A obtemos o grupo H como o produto semidireto $H = A \rtimes G$. Essa ação induz uma ação de G^{φ} sobre H cujo produto semidireto obtido por essa extensão é isomorfo ao proposto grupo $\nu(G)$. A obtenção do grupo $\nu(G)$ do **Teorema B** (páginas $81-89$) segue de maneira análoga, a partir do grupo abeliano A, cujo geradores são os mesmos e as relações definidoras são as obtidas da **Proposição 0.0.7**, alterando para adequadas ações.

Como Corolários dos **Teoremas A** e **B**, obtemos apresentações para os grupos $[G, G^{\varphi}]$, $G \wedge G$ e $M(G)$, para os casos em que m é par e m é ímpar, respectivamente.

Wamsley [[43], Lemma 1], em 1970, mostrou que grupos metacíclicos finitos, não cindidos possuem o multiplicador de Schur cíclico cuja ordem depende da quadra (m,n,r,s). Em 1994, Rocco [32] também calculou $M(G)$ de um grupo metacíclico finito G, não necessariamente cindido. Seus cálculos são baseados no isomorfismo $M(G) \cong \mu(G)/\Delta(G)$, tendo em conta que G' é um grupo cíclico isomorfo ao quociente $[G, G^{\varphi}]/\mu(G)$. Ou seja, as ordens relativas dos elementos geradores do multiplicador de Schur, certificadas via isomorfismo, são calculadas módulo $\Delta(G)$. Nossos resultados coincidem com a ordem do grupo $M(G)$ calculada por ambos, independente da paridade de m.

Beyl [[5], página 147, §5] classificou os chamados p-grupos metacíclicos de Schur, p-grupos metacíclicos que possuem multiplicador de Schur trivial, a menos de isomorfismo.

Ainda mostrou que grupos do tipo

$$\langle a, b \mid a^m = 1, b^n = a^{\frac{m}{(m,r-1)}}, a^b = a^r \rangle$$

possuem multiplicador de Schur trivial. Esse resultado pode ser obtido facilmente de nossos Corolários tomando $s = \dfrac{m}{(m, r-1)}$.

As seções abelianas do grupo $\nu(G)$ para grupos metacíclicos cindidos, $G = g(a, b; m, n, r, 0)$, descritas por Johnson, D .L., [[10], (16) Proposition] quando m é par, bem como as descritas por Brown, R., Johnson, D .L. & Robertson, E. F., [[10], Proposition 15], quando m é ímpar, ambas obtidas a partir de uma abordagem por biderivação, coincidem com as que ora obtivemos.

Independente da paridade de m, Brown, Johnson & Robertson [[10], Proposition 12] calcularam as ordens de um conjunto gerador para o grupo $[G, G^{\varphi}]$ quando $G = g(a, b; m, 2, m-1, 0)$. A estratégia usada por Brown, Johnson & Robertson [[10]] foi considerar o grupo diedral $\mathcal{D}_m$ como a extensão central do grupo dos quatérnios generalizados $\mathcal{Q}_m$.

Nesta tese, estudamos também uma outra seção do grupo $\nu(G)$ para grupos metacíclicos finitos, a saber, o grupo $\tau(G) = \nu(G)/\Delta(G)$, que ainda não havia sido explorado na literatura.

Na segunda parte do **Capítulo 3**, como mensionado anteriormente, calculamos uma apresentação do grupo $\nu(G)$ para grupos metacíclicos infinitos. Ao obtermos as ordens dos elementos do conjunto gerador do quadrado tensorial, foi possível perceber que não existem relações entre os mesmos, uma vez que o grupo $G = g(a, b; m, n, r)$ é sempre cindido.

Beuerle & Kappe [3] propuseram uma cota para as ordens dos elementos de um conjunto gerador do quadrado tensorial não abeliano de um grupo metacíclico infinito, não abeliano. Cota que foi verificada por eles como sendo a ordem efetiva dos geradores do grupo $[G, G^{\varphi}]$, via exibição de uma biderivação. No **Teorema C** (páginas $106 - 115$) pudemos verificar tais ordens cuja estratégia usada foi a mesma dos **Teoremas A** e **B**, mediante a construção do grupo $\nu(G)$.

Como Corolários, identificamos os grupos $G \wedge G$, $\mu(G)$ e $M(G)$, também calculados por Beuerle & Kappe [3], além do grupo $\tau(G)$.

Para finalizar, disponibilizamos no **Anexo A** alguns dos comandos utilizados no sistema GAP [18] para a verificação e checagem das apresentações propostas para m, n, r, s relativamente pequenos.

Capítulo 1

Preliminares

Neste Capítulo, apresentamos algumas definições e resultados em Teoria de Grupos, os quais fazem parte do aparato teórico necessário para o desenvolvimento deste trabalho. Para maiores referências, veja Curtis & Reiner [13], Gorenstein [19], Holt, Eick & O'Brien [21], Johnson [22], Robinson [31], Sims [41], dentre outros.

1.1 Cálculo com Comutadores

Sejam G um grupo e g, h elementos arbitrários de G. Chamamos de *conjugado* de g por h, g^h, o elemento dado por $g^h := h^{-1}gh$ e, o *comutador* de g e h, $[g,h]$, o elemento $[g,h] := g^{-1}h^{-1}gh = g^{-1}g^h$. Os comutadores são *normados à esquerda*, isto é, $[[x,y],z] = [x,y,z]$, e assim, indutivamente, $[[x_1,x_2,\ldots x_{n-1}],x_n] = [x_1,x_2,\ldots x_{n-1},x_n]$, para quaisquer $x_i \in G$. As Proposições abaixo são resultados obtidos a partir de computações simples entre comutadores:

Proposição 1.1.1. [[31], página 123] *Sejam x,y,z elementos de um grupo. Então:*
(i) $[x,y] = [y,x]^{-1}$;
(ii) $[xy,z] = [x,z]^y[y,z]$ *e* $[x,yz] = [x,z][x,y]^z$;
(iii) $[x,y^{-1}] = \left([x,y]^{y^{-1}}\right)^{-1}$ *e* $[x^{-1},y] = \left([x,y]^{x^{-1}}\right)^{-1}$;
(iv) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ *(Identidade de Hall-Witt).*

Dados dois subconjuntos H e K de um grupo G, denotamos por $[H,K]$ o subgrupo de G gerado pelo conjunto $\{[h,k] \mid h \in H, k \in K\}$, ou seja, $[H,K] = \langle [h,k] \mid h \in H, k \in K\rangle$. Em particular, $[G,G]$ é o *subgrupo derivado de* G, G'. Este subgrupo tem a propriedade de que G/G', chamado *grupo abelianizado* de G, ser o maior grupo quociente por G que é abeliano, ou seja, se H é normal em G com o quociente G/H abeliano, então $G' \leq H$.

1.2 Grupos Livres

Nesta seção introduzimos os conceitos de grupo livre e apresentação de um grupo, bem como algumas de suas propriedades, cujas demonstrações podem ser encontradas em Johnson [22].

Definição 1.2.1. *Um grupo F é dito ser livre sobre um subconjunto $X \subseteq F$ se, para qualquer grupo G dado e qualquer aplicação $\theta : X \longrightarrow G$, existe um único homomorfismo $\theta' : F \longrightarrow G$ tal que $x\theta = x\theta'$, para todo $x \in X$.*

Dizer que existe um único homomorfismo tal que $x\theta = x\theta'$, para todo $x \in X$ é equivalente a dizer que existe um único homomorfismo θ' que estende θ. Ou ainda, que o diagrama

$$\begin{tikzcd} X \arrow[r, "ic"] \arrow[d, "\theta"'] & F \arrow[dl, dashed, "\theta'"] \\ G & \end{tikzcd}$$

é comutativo, isto é, $\theta = ic \circ \theta'$; também conhecida como Propriedade Universal na Teoria de Categorias. X é então uma *base* de F e $|X|$ é o posto ('rank') de F, $r(F)$.

O resultado a seguir é uma junção de Proposições e Lemas que garantem a "boa-definição"do conceito de *posto*:

Proposição 1.2.2. [[22], páginas $3-4$] (i) *Se F é livre sobre X então X gera F;*
(ii) *Grupos livres de mesmo posto são isomorfos;*
(iii) *Grupos livres de postos diferentes não são isomorfos.*

Agora, dado um conjunto X não vazio de cardinalidade qualquer, é sempre possível construir um grupo livre sobre X, $F = F(X)$, e portanto obtemos grupos livres de qualquer posto (veja [[22], páginas $4-7$]). O resultado a seguir torna importante o estudo de grupos livres:

Proposição 1.2.3. [[22], página 7] *Todo grupo é uma imagem homomórfica de algum grupo livre.*

Sejam G um grupo e $\theta : F \longrightarrow G$ um epimorfismo de um grupo livre $F = F(X)$ sobre G. Então $G \cong F/N$, onde N é o núcleo de θ, $N := \ker(\theta)$. Considere R um subconjunto de F que gera N como subgrupo normal de F, ou seja, $\langle R \rangle^F = N$. Observe que X e R determinam G a menos de isomorfismo.

Definição 1.2.4. *Com a notação estabelecida anteriormente, escrevemos $G = \langle X \mid R \rangle$ e chamamos este par de apresentação livre ou apenas apresentação de G. Os elementos de X são chamados geradores e os elementos de R são relatores. Um grupo G é chamado finitamente gerado se X é finito e, finitamente apresentado se possui uma apresentação em que X e R sejam ambos finitos. Neste caso, o número $|R| - |X|$ é chamado deficiência do grupo G.*

Em alguns casos é conveniente trocar R em $\langle X \mid R \rangle$ por um conjunto de equações $R = 1$, isto é, para cada $r_i \in R$, fazer $r_i = 1$, chamadas *relações definidoras* para G.

Proposição 1.2.5. [[22], página 42] *Todo grupo possui uma apresentação e, todo grupo finito é finitamente apresentado.*

A seguir, damos exemplos de grupos e apresentações dos quais alguns destes serão mencionados ao longo de todo este trabalho:

Exemplo 1.2.6. 1. *$\langle X \mid \ \rangle$ é a apresentação de um grupo livre de posto $|X|$.*
2. *Todo grupo cíclico é uma imagem homomórfica de $\mathbb{Z} = \langle x \rangle$. E assim, se G é um grupo cíclico de ordem n, não é difícil verificar que uma apresentação para G é $\langle x \mid x^n = 1 \rangle$.*
3. *Em particular, grupos abelianos possuem comutadores triviais como relações definidoras.*
4. *Dado $n > 2$, o grupo diedral de ordem $2n$ possui uma apresentação da forma*

$$\mathcal{D}_n = \langle x, y \mid x^n = 1, y^2 = 1, x^y = x^{-1} \rangle.$$

No caso em que $n = 2$ o grupo $\mathcal{D}_2$ é abeliano.
5. *Para $n \geq 2$, o quatérnio generalizado de ordem 2^{n+1} tem uma apresentação*

$$\mathcal{Q}_{2^{n+1}} = \langle x, y \mid x^{2^n} = 1, y^2 = x^{2^{n-1}}, x^y = x^{-1} \rangle.$$

Lema 1.2.7. [[22], página 42] *Sejam G, H e K grupos, $\alpha : G \longrightarrow H$ um epimorfismo e $\beta : G \longrightarrow K$ um homomorfismo, tais que $ker(\alpha) \subseteq ker(\beta)$. Então existe um homomorfismo $\gamma : H \longrightarrow K$ tal que $\alpha\gamma = \beta$.*

$$\begin{tikzcd}
ker(\beta) \arrow[dr] & & H \arrow[dd, dashed, "\gamma"] \\
& G \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & \\
ker(\alpha) \arrow[uu, "ic"] \arrow[ur] & & K
\end{tikzcd}$$

Proposição 1.2.8 (von Dyck)**.** [[22], página 43] *Se $G = \langle X \mid R \rangle$ e $H = \langle X \mid S \rangle$ onde $R \subseteq S \subseteq F(X)$, então existe um epimorfismo $\phi : G \to H$ fixando todo $x \in X$ tal que* $\ker(\phi) = S \setminus R$. *Inversamente, todo quociente de $G = \langle X \mid R \rangle$ tem uma apresentação $\langle X \mid S \rangle$ com $S \supseteq R$.*

Proposição 1.2.9 (Teste da Substituição)**.** [[22], página 44] *Sejam G um grupo com apresentação $\langle X \mid R\rangle$, H um grupo arbitrário e $\theta : X \to H$ uma função. Então θ se estende a um homomorfismo $\theta' : G \to H$ se, e somente se, θ é consistente com os relatores de G, isto é, se para todo $x \in X$ e todo $r \in R$, o resultado da substituição de x pela sua imagem via θ em r dá a identidade de H.*

$$\begin{tikzcd}
 & R \arrow[d] & \\
X \arrow[r, "ic"] \arrow[dr, "\theta"'] & F \arrow[r, two heads] \arrow[d, "\theta''"] & G \arrow[dl, dashed, "\theta'"] \\
 & H &
\end{tikzcd}$$

O homomorfismo θ' é único pois G é gerado por X. Além disso, se H é gerado por θ', $x \in X$, então θ' é sobrejetivo.

Um grupo G pode ter várias apresentações, como por exemplo, o grupo diedral $\mathcal{D}_n$ pode ser apresentado como no **Exemplo 1.2.6**, item 4. ou por $\langle x, y \mid x^2 = y^2 = (xy)^n = 1\rangle$. Assim, surge a pergunta: a partir de uma apresentação de G dada, é possível obter qualquer outra apresentação para o mesmo grupo?

Em 1908, Tietze [42] mostrou que dada uma apresentação de um grupo G, $G = \langle a, b, c, \ldots \mid P, Q, R, \ldots\rangle$, existem manipulações simples que não mudam o grupo ou pelo menos a classe de isomorfismo definida pela apresentação. Essas são as conhecidas *Transformações de Tietze* de uma dada apresentação. São elas:

$T1$ **Adição de relações definidoras:** R^+
Se as palavras $S, T, \ldots$ são obtidas de $P, Q, R, \ldots$ então adicione $S, T, \ldots$ ao conjunto de relações definidoras;

$T2$ **Remoção de relações definidoras:** R^-
Se algum dos relatores, digamos $S, T, \ldots$ listados entre $P, Q, R, S, \ldots$ são obtidos dos outros então delete $S, T, \ldots$ do conjunto das relações definidoras;

$T3$ **Adição de um gerador:** X^+
Se $K, M, \ldots$ são palavras em $a, b, c, \ldots$ então adicione os símbolos $x, y, \ldots$ no conjunto de geradores e adicione as relações $x = K, y = M, \ldots$ no conjunto das relações definidoras;

$T4$ **Remoção de um gerador:** X^-
Se alguma das relações de G é da forma $p = V, q = W, \ldots$ onde $p, q, \ldots$ são geradores de G e $V, W, \ldots$ são palavras nos geradores diferentes de $p, q, \ldots$ então delete os geradores $p, q, \ldots$, troque estes elementos por $V, W, \ldots$ nas demais relações e delete $p = V, q = W, \ldots$ das relações definidoras.

Proposição 1.2.10. [[22], página 49] *Dadas duas apresentações finitas de um mesmo grupo, uma pode ser obtida da outra por uma sequência finita de Transformações de Tietze.*

Em contraste com a **Proposição 1.2.10**, não existe um algoritmo geral decidindo se duas apresentações finitas dadas produzem grupos isomórficos. Este é o conhecido **Problema do Isomorfismo**, proposto em uma série de artigos por Dehn, cuja discussão pode ser encontrada em [[27], Section 1.3]. O mesmo resolveu parcialmente alguns problemas sobre grupos finitamente apresentados, anunciando assim o nascimento de uma nova área de estudos, a Teoria Combinatória dos grupos. Tais problemas vão ao encontro da tentativa de obter informações sobre o grupo:

Problema da Palavra: Existe um algoritmo para determinar se uma palavra w em termos dos geradores de G define ou não a identidade de G, $w =_G 1$?

Problema da Conjugação: Existe um algoritmo para determinar se um par de palavras u, v em termos dos geradores definem ou não elementos conjugados, $u = v^g$, $g \in G$?

Problema do Isomorfismo: Dado um par de apresentações finitas, é possível decidir se os grupos dados por estas apresentações são ou não isomorfos?

O Problema da Palavra e o Problema da Conjugação são decidíveis em grupos livres finitamente gerados.

1.3 Grupos Nilpotentes e Solúveis

Nessa seção daremos algumas propriedades de grupos nilpotentes e solúveis, necessárias para o desenvolvimento do trabalho. Como referência básica, utilizamos Robinson [31]:

Definição 1.3.1. *Um grupo G é dito nilpotente se possui uma série normal de subgrupos*

$$1 = H_0 \leq \ldots \leq H_n = G$$

cujo quociente H_{i+1}/H_i está contido no centro de G/H_i, para todo i. Tal série é chamada série central de G. Equivalentemente, $[H_{i+1}, G] \leq H_i$, para todo i.

Na definição não é necessário dizer que a série é normal pois o fato de $[H_{i+1}, G] \leq H_i$ implica $H_i \trianglelefteq G$, para todo i.

Quando G é um grupo nilpotente, o comprimento c da menor série central de G é chamado *classe de nilpotência*, denotado por $c = cl(G)$. Se $cl(G) = c$, então H_c é abeliano.

Definição 1.3.2. *Um grupo G é dito ser solúvel se possui uma série abeliana, ou seja, se existe uma série*

$$1 = G^0 \rhd G^1 \rhd \ldots \rhd G^n = G$$

na qual o quociente G^{i+1}/G^i é abeliano, para todo i.

Definição 1.3.3. *Se G é um grupo solúvel então o comprimento da série abeliana 'mais curta' de G é chamado o comprimento derivado de G.*

Exemplo 1.3.4. 1$-$ *Um grupo G tem comprimento derivado 0 se, e somente se, possui ordem 1.*
2$-$ *Grupos com comprimento derivado no máximo 1 são apenas os abelianos.*
3$-$ *Um grupo solúvel com comprimento derivado no máximo 2 é dito metabeliano. Os grupos metacíclicos G também possuem comprimento derivado no máximo 2 pois G/H é cíclico logo abeliano com H cíclico.*

Na seção seguinte, trataremos de uma classe de grupos solúveis, os chamados *grupos policíclicos*:

1.4 Grupos Policíclicos

As definições, resultados e demonstrações desta seção podem ser encontrados em Holt, Eick & O'Brien [21].

Definição 1.4.1. *Um grupo G é dito policíclico se possui uma cadeia descendente de subgrupos*

$$G = G_1 \geqslant G_2 \geqslant \ldots \geqslant G_{n+1} = 1$$

em que cada G_{i+1} é um subgrupo normal em G_i (chamada série subnormal) e cada quociente G_i/G_{i+1} é cíclico. Tal cadeia de subgrupos é chamada série policíclica.

A propriedade 'policíclica' é fechada em relação a formação de subgrupos e de extensões. Como exemplos de grupos policíclicos temos os grupos abelianos, abeliano por metacíclico e nilpotentes finitamente gerados. Além disso, os grupos policíclicos são solúveis.

Os grupos policíclicos também podem ser definidos como grupos solúveis em que todo subgrupo é finitamente gerado. Em particular, todo grupo policíclico é finitamente gerado. Sims [39] mostra que se for possível verificar que um grupo é finitamente apresentado então este é policíclico via o algoritmo do quociente nilpotente. Porém, nem todo grupo solúvel finitamente apresentado é policíclico, a saber, o grupo $C_2 \wr C_\infty$, chamado produto entrelaçado de C_2 por C_∞ [[31], página 32].

Mais ainda, a classe dos grupos policíclicos é fechada para subgrupos, quocientes, extensões e produtos diretos finitos e, a classe de grupos solúveis finitos e policíclicos finitos são as mesmas. Desta forma, grupos policíclicos são Hopfianos, ou seja, são grupos em que todo epimorfismo é um automorfismo (veja Sims [[41], Corollary 3.11]).

Essa é uma classe de grupos computável, ou seja, que possuem o Problema da Palavra efetivamente solúvel (resolvível).

Da **Definição 1.4.1**, como cada G_i/G_{i+1} é cíclico, existe algum x_i em G_i tal que $\langle x_i G_{i+1}\rangle = G_i/G_{i+1}$, para qualquer índice i.

Definição 1.4.2. *Uma sequência de elementos* $X = [x_1, x_2, \ldots, x_n]$ *tal que* $\langle x_i G_{i+1}\rangle = G_i/G_{i+1}$*, para* $1 \leqslant i \leqslant n$*, é chamada sequência policíclica de* G*.*

É simples mostrar que toda cauda da sequência, isto é, $X_i = [x_i, x_{i+1}, \ldots x_n]$, para algum $i \in \{1, 2, \ldots, n\}$ é uma sequência policíclica para o grupo G_i. Este é um argumento recorrentemente usado para indução de alguns resultados e em métodos algorítmicos.

Definição 1.4.3. *Seja* X *uma sequência policíclica para* G*. A sequência*

$$R(X) := (r_1, r_2, \ldots, r_n)$$

definida por $r_i := |G_i : G_{i+1}| \in \mathbb{N} \cup \{\infty\}$ *é chamado sequência de ordens relativas a* X*. O conjunto* $\{i \in \{1, 2, \ldots, n\} \mid r_i \ finito\}$ *é denotado por* $I(X)$*.*

A sequência $R(X)$ e o conjunto $I(X)$ dependem apenas da série policíclica de subgrupos $G_1, G_2, \ldots, G_n$ subjacente de X. Daí, se Y é uma sequência policíclica para o grupo G definindo a mesma série policíclica que X segue que $R(X) = R(Y)$ e $I(X) = I(Y)$.

As ordens relativas nos dão algumas informações básicas sobre o grupo G. Por exemplo, o grupo é finito se, e somente se, toda entrada em $R(X)$ é finita ou, equivalentemente, se $I(X) = \{1, 2, \ldots, n\}$. E, se o grupo é finito então o produto das entradas em $R(X)$ é exatamente a sua ordem.

Não é difícil a verificação de que os subgrupos de uma série policíclica são exibidos por sequências policíclicas X como $G_i = \langle x_i, \ldots, x_n\rangle$. Em particular, o grupo G é gerado pelos elementos da sequência X. Mais ainda, isto resulta que a série policíclica $G = G_1 \geqslant G_2 \geqslant \ldots \geqslant G_{n+1} = 1$ é unicamente determinada por X dado um conjunto $R(X)$ de ordens relativas.

Exemplo 1.4.4. *Seja $G = \langle (1234), (13) \rangle \cong D_4$. Vamos mostrar que o comprimento da sequência policíclica para G não é unicamente definida por G:*

(i) Seja $G_2 = \langle (1234) \rangle \cong C_4$. Então $G = G_1 \geqslant G_2 \geqslant G_3 = 1$ é uma série policíclica para G pois $X = [(13), (1234)]$ e $Y = [(24), (1432)]$ são sequências policíclicas definindo essa série. Daí, $I(X) = \{1, 2\} = I(Y)$ e $R(X) = R(Y) = (2, 4)$.

(ii) Sejam $G_2 = \langle (12)(34), (13)(24) \rangle \cong V_4$ e $G_3 = \langle (13)(24) \rangle \cong C_2$ com $G = G_1 \geqslant G_2 \geqslant G_3 \geqslant G_4 = 1$ uma série policíclica para G cuja sequências definidoras são $X = [(24), (12)(34), (13)(24)]$ e $Y = [(12)(34), (1234), (13)(24)]$, por exemplo. Assim, $I(X) = \{1, 2, 3\} = I(Y)$ e $R(X) = R(Y) = (2, 2, 2)$.

Um resultado elementar mas importante é:

Lema 1.4.5. [[21], Lemma 8.3] *Seja $X = [x_1, x_2, \ldots, x_n]$ uma sequência policíclica para o grupo G com sequência das ordens relativas $R(X) = (r_1, r_2, \ldots, r_n)$. Então, para todo $g \in G$, existe uma única sequência $(e_1, e_2, \ldots, e_n)$, com $e_1 \in \mathbb{Z}$, para $1 \leqslant i \leqslant n$ e $0 \leqslant e_i < r_i$, se $i \in I(X)$, tal que $g = x_1^{e_1} \ldots x_n^{e_n}$.*

Definição 1.4.6. *A expressão $g = x_1^{e_1} \ldots x_n^{e_n}$ do **Lema 1.4.5** é chamada forma normal do elemento g do grupo G com respeito a X. A sequência $(e_1, e_2, \ldots, e_n)$ é o vetor de expoentes de g com respeito a X, denotado por $exp_X(g) = (e_1, e_2, \ldots, e_n)$.*

É natural então pensarmos em uma aplicação injetora do grupo G em $\mathbb{Z}^n$, que associa $g \mapsto exp_X(g)$. Observe que esta aplicação não é um homomorfismo.

Exemplo 1.4.7. *(i) Considere a sequência policíclica $X = [(13), (12 \ldots n)]$ para o grupo diedral G de ordem $2n$.*

Caso n seja par, tome $g = (13 \ldots n-1)(24 \ldots n)$ um elemento de G. Pelas propriedades de G, $(12 \ldots n)(12 \ldots n) = (13 \ldots n-1)(24 \ldots n)$. Assim, $g = x_1^0 x_2^2 = x_2^2$ é uma forma normal para g cujo $exp_X(g) = (0, 2)$.

Analogamente, caso n seja ímpar, tome $g = (13 \ldots n)(24 \ldots n-1)$ um elemento de G. Pelas propriedades de G, $(12 \ldots n)(12 \ldots n) = (13 \ldots n)(24 \ldots n-1)$ resultando também em $g = x_1^0 x_2^2 = x_2^2$ ser uma forma normal para g cujo $exp_X(g) = (0, 2)$.
(ii) Considere agora o grupo G gerado pelas matrizes

$$x_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad e \quad x_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Não é difícil verificar que $x_2^2 = 1$ e $x_1^{x_2} = x_1^{-1}$. Assim, G é isomorfo ao grupo diedral infinito e $G \geq \langle x_1 \rangle \geq 1$ é uma série policíclica para G. A sequência $X = [x_1, x_2]$ é uma *sequência policíclica para G, com ordens relativas $(\infty, 2)$. Considere o elemento*

$$g = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \in G.$$

É fácil ver que $g = x_1^2 x_2^1$ e desta forma $exp_X(g) = (2, 1)$.

Os vetores de expoentes dos elementos de um grupo policíclico podem ser usados para descrever as relações do grupo G nos seus geradores X. Essas relações são a primeira e fundamental direção para a apresentação de G.

Lema 1.4.8. [[21], Lemma 8.6] *Seja $X = [x_1, \ldots, x_n]$ uma sequência policíclica para o grupo G com ordens relativas $R(X) = (r_1, \ldots, r_n)$.*
(i) Seja $i \in I(X)$. Então a forma normal de uma potência $x_i^{r_i}$ é dada por $x_i^{r_i} = x_{i+1}^{a_{i,i+1}} \ldots x_n^{a_{i,n}}$.
(ii) Sejam $1 \leq j < i \leq n$. Então a forma normal de um conjugado $x_j^{-1} x_i x_j$ é dada por $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} \ldots x_n^{b_{i,j,n}}$.
(iii) Sejam $1 \leq j < i \leq n$. Então a forma normal de um conjugado $x_j x_i x_j^{-1}$ é dada por $x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} \ldots x_n^{c_{i,j,n}}$.

Definição 1.4.9. *Uma apresentação $\langle x_1, \ldots, x_n \mid R \rangle$ é chamada uma apresentação policíclica se existem uma sequência $S = (s_1, \ldots, s_n)$ com $s_i \in \mathbb{N} \cup \{\infty\}$ e inteiros $a_{i,k}, b_{i,j,k}, c_{i,j,k}$ tais que R consiste das seguintes relações:*

$$\begin{aligned} x_i^{s_i} &= R_{i,i} \text{ com } R_{i,i} := x_{i+1}^{a_{i,i+1}} \ldots x_n^{a_{i,n}} \text{ para } 1 \leq i \leq n \text{ com } s_i < \infty, \\ x_j^{-1} x_i x_j &= R_{i,j} \text{ com } R_{i,j} := x_{j+1}^{b_{i,j,j+1}} \ldots x_n^{b_{i,j,n}} \text{ para } 1 \leq j < i \leq n, \\ x_j x_i x_j^{-1} &= R_{j,i} \text{ com } R_{j,i} := x_{j+1}^{c_{i,j,j+1}} \ldots x_n^{c_{i,j,n}} \text{ para } 1 \leq j < i \leq n. \end{aligned}$$

Essas relações são chamadas relações policíclicas. A primeira delas é de potências e as outras são relações de conjugação entre os elementos geradores. S é chamado de sequência das potências da apresentação.

As relações de conjugação da forma $x_j^{-1} x_i x_j = x_i$ e $x_j x_i x_j^{-1} = x_i$ são chamadas *triviais* e portanto são omitidas da apresentação para simplificação da notação. Isto significa que as apresentações policíclicas devem ser distinguidas das apresentações finitas arbitrárias. E portanto, serão denotadas por $Pc\langle x_1, \ldots, x_n \mid R \rangle$, ou por *pcp* somente. Um grupo assim definido e apresentado é conhecido como *Pc-grupo*.

Exemplo 1.4.10. *Seja $G = Pc\langle X|R \rangle$ um grupo definido por uma apresentação policíclica com um gerador, isto é, $X = [x_1]$. Temos duas possibilidades para R:*

1− Se $R = \varnothing$ então G é um grupo cíclico infinito.

2− *Se R contém apenas uma relação de potência, ou seja, $x_1^{s_1} = 1$, então G é um grupo cíclico finito de ordem s_1.*

Todo grupo policíclico G tem uma sequência policíclica X que induz um conjunto completo de relações esboçado no **Lema 1.4.9**. O conjunto S das potências de uma apresentação é igual as ordens relativas $R(X)$ neste caso. Isto é provado no resultado a seguir:

Teorema 1.4.11. [[21], Theorem 8.8] *Toda sequência policíclica determina uma (única) apresentação policíclica. Portanto, todo grupo policíclico pode ser definido por uma apresentação policíclica.*

Exemplo 1.4.12. *Seja $G = \langle (13), (1234) \rangle$ com sequência policíclica $X = [(13), (1234)]$. Uma série policíclica para G é $G = G_1 \geqslant G_2 \geqslant G_3 = 1$ com $G_2 = \langle (1234) \rangle$ e, $r_1 = |G_1 : G_2| = 2$ e $|G_2 : G_3| = 4$ determinando $R(X) = (2, 4)$. Portanto, uma apresentação policíclica para G é dada por*

$$\langle x_1, x_2 \mid x_1^2 = 1,\ x_2^4 = 1,\ x_1^{-1} x_2 x_1 = x_2^3,\ x_1 x_2 x_1^{-1} = x_2^3 \rangle.$$

A recíproca do **Teorema 1.4.11** nos diz que toda apresentação policíclica define um grupo policíclico:

Teorema 1.4.13. [[21], Theorem 8.9] *Sejam $Pc\langle x_1, \dots, x_n \mid R \rangle$ uma apresentação policíclica e G um grupo definido por esta apresentação. Então G é um grupo policíclico, $X = [x_1, \dots, x_n]$ é uma sequência policíclica para G e o conjunto das suas ordens relativas, $R(X) = (r_1, \dots, r_n)$, satisfaz $r_i \leq s_i$ para $1 \leq i \leq n$.*

A demonstração do **Teorema 1.4.13** acima consiste em tomar uma sequência policíclica para G de tal forma que $G_i = \langle x_i, \dots, x_n \rangle \leqslant G$ para $1 \leq i \leq n$.

Estas apresentações policíclicas para as quais o conjunto S das potências e o conjunto $R(X)$ das ordens relativas coincidem, desempenham um papel central na teoria algorítmica de grupos policíclicos. De fato, computações com grupos policíclicos são geralmente realizados em tais apresentações.

Definição 1.4.14. *Uma apresentação policíclica $Pc\langle X|R \rangle$ com expoentes de potências S é chamado consistente (ou confluente) se $R(X) = S$.*

É fácil observar que todo grupo policíclico tem uma apresentação policíclica consistente se usarmos o **Teorema 1.4.11**:

Teorema 1.4.15. [[21], Theorem 8.11] *Toda sequência policíclica determina uma apresentação policíclica consistente. Portanto, todo grupo policíclico pode ser definido por uma apresentação policíclica consistente.*

Um método efetivo para checar se uma apresentação policíclica dada é consistente ou modificar uma apresentação policíclica dada para uma apresentação consistente equivalente à dada, é baseado no processo de completação (ou completamento) de Knuth-Bendix no contexto de Sistema de Reescrita. Para maiores detalhes, veja Holt, Eick & O' Brien [21] e Sims [40].

1.5 Teoria dos Números

Vamos fixar algumas notações que serão usadas ao longo deste trabalho. Para quaisquer inteiros positivos α e β:
$(\alpha, \beta) :=$ *máximo divisor comum* entre α e β
$[\alpha, \beta] := \dfrac{\alpha\beta}{(\alpha, \beta)} :=$ *mínimo múltiplo comum* entre α e β.

Se $\alpha \mid \beta$, então dizemos que α é um *divisor* de β ou que α divide β. Se $\alpha \parallel \beta$, então $\alpha \mid \beta$ e $(\alpha, \beta/\alpha) = 1$; em outras palavras, α é a maior potência de α que divide β.

Seja m um número inteiro não negativo. O anel dos números inteiros módulo m é denotado por $\mathbb{Z}_m$. O conjunto dos números inteiros relativamente primos com m é denotado por $\mathcal{U}_m$, ou seja, $\mathcal{U}_m = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$. Se $m = 0$, então $\mathcal{U}_0 = \{-1, 1\}$. Caso $m > 0$, denote s o menor inteiro positivo em $\mathcal{U}_m$ tal que $rs \equiv 1\ (mod\ m)$, sempre que $r =: \bar{r} \in \mathcal{U}_m$.

Nesta seção, enunciaremos alguns resultados a respeito do conjunto dos inteiros relativamente primos com m, $\mathcal{U}_m$, e sua relação com a função de Euler. Os resultados apresentados podem ser encontrados em Beuerle & Kappe [3] e Shokranian, Soares & Godinho [37].

Definição 1.5.1. [[3], Definition 2.1] *Sejam m, r inteiros com $m \geq 0$ e $r \in \mathcal{U}_m$. Defina a função $E_m : \mathcal{U}_m \times \mathbb{Z} \to \mathbb{Z}$ por*

$$E_m(r, x) = \begin{cases} x, & se\ r \equiv 1\ (mod\ m)\ ou\ x = 0 \\ 1 + r + \cdots + r^{x-1}, & se\ r \not\equiv 1\ (mod\ m)\ e\ x > 0 \\ -r^x E_m(r, -x), & se\ r \not\equiv 1\ (mod\ m)\ e\ x < 0 \end{cases} \tag{1.1}$$

Lema 1.5.2. [[3], Lemma 2.3] *Sejam m, r, x inteiros com $m > 0$ par e $r \in \mathcal{U}_m$. Então*

$$E_m(r, x) \equiv x\ (mod\ 2).$$

Lema 1.5.3. [[3], Lemma 2.4] *Sejam x, r e m inteiros com $m \geq 0$ e par. Então:*

$$r^{2x} \equiv 1 \pmod{(m, 2(r-1))} \tag{1.2}$$

$$r^x + (r-1)x \equiv 1 \pmod{(m, 2(r-1))} \tag{1.3}$$

Definição 1.5.4. *Um conjunto de inteiros $\{a_1, a_2, \ldots, a_s\}$ é chamado um sistema completo de resíduos módulo m quando:*
(i) $a_i \not\equiv a_j (mod\ m)$ para todos $i, j \in \{1, 2, \ldots s\}$.
(ii) Para todo $n \in \mathbb{Z}$ existe $i \in \{1, 2, \ldots s\}$ tal que $n \equiv a_i (mod\ m)$.

Definição 1.5.5. *Um conjunto de inteiros $\{a_1, a_2, \ldots, a_s\}$ é chamado um sistema reduzido de resíduos módulo m se*
(i) $(a_i, m) = 1$ para todo $i \in \{1, 2, \ldots s\}$.
(ii) $a_i \not\equiv a_j (mod\ m)$ se $i, j \in \{1, 2, \ldots, s\}$ e $i \neq j$.
(iii) Para todo $n \in \mathbb{Z}$ satisfazendo $(m, n) = 1$, existe $i \in \{1, 2, \ldots s\}$ tal que $n \equiv a_i (mod\ m)$.

Definição 1.5.6 (A função Φ de Euler)**.** *Seja $m \in \mathbb{Z}_+^\star$. A função de Euler $\Phi(m)$ é definida como o número de inteiros positivos não excedendo m que são relativamente primos com m. Ou seja, $\Phi : \mathbb{Z}_+^\star \longrightarrow \mathbb{Z}_+^\star$ de tal forma que $\Phi(m) = |\mathcal{U}_m|$.*

Teorema 1.5.7. *Seja $m \in \mathbb{Z}_+^\star$, $m > 1$, e suponha que o conjunto $\{a_1, \ldots, a_s\}$ é um sistema reduzido de resíduos módulo m. Então $s = \Phi(m)$.*

Teorema 1.5.8. *Sejam $m, n \in \mathbb{Z}_+^\star$ tais que $(m, n) = 1$. Então $\Phi(mn) = \Phi(m)\Phi(n)$.*

Lema 1.5.9. *Para todo p primo e $\alpha \in \mathbb{Z}_+^\star$ temos*

$$\Phi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right).$$

Teorema 1.5.10. *Para cada $m \in \mathbb{Z}_+^\star$ temos*

$$\Phi(m) = m \prod_{p \in \mathbb{P}_m} \left(1 - \frac{1}{p}\right),$$

onde $\mathbb{P}_m = \{p\ primo;\ p \mid m\}$, ou seja, o conjunto dos primos divisores de m.

Teorema 1.5.11 (Euler)**.** *Sejam $a \in \mathbb{Z}$, $m \in \mathbb{Z}_+^\star$ tais que $(a, m) = 1$. Então*

$$a^{\Phi(m)} \equiv 1\ (mod\ m).$$

Corolário 1.5.12 (Pequeno Teorema de Fermat)**.** *Seja $p \in \mathbb{Z}_+^\star$ um número primo. Então $a^p \equiv a\ (mod\ p)$, para todo inteiro positivo a.*

1.6 Extensões de Grupos

As definições e resultados a seguir podem ser encontradas em Gorenstein [19], Johnson [22] e Rotman [35].

Definição 1.6.1. *Uma extensão de um grupo G por um grupo A é um grupo $\tilde{G}$ que possui um subgrupo normal N tal que $A \cong N$ e $\tilde{G}/N \cong G$.*

Observe que A não é necessariamente um subgrupo de $\tilde{\mathrm{G}}$. Uma das questões que envolvem o **Problema da Extensão** é identificar quais grupos $\tilde{\mathrm{G}}$, a menos de isomorfismo, que possuem uma extensão de G por A dados. Este Problema tem sido estudado desde o final do século XIX.

Nas condições mencionadas, considere a aplicação $i : A \longrightarrow \tilde{\mathrm{G}}$ que associa o grupo A e o grupo $\tilde{\mathrm{G}}$. Então i é uma injeção com $Im(i) \lhd \tilde{\mathrm{G}}$ e $\tilde{\mathrm{G}}$ é uma extensão de $\tilde{\mathrm{G}}/Im(i)$ por A. Da mesma forma, a aplicação que associa $\tilde{\mathrm{G}}$ e G, $\mu : \tilde{\mathrm{G}} \twoheadrightarrow G$, é um epimorfismo tal que $\tilde{\mathrm{G}}$ é uma extensão de G pelo $\ker(\mu)$. Identificando os isomorfismo $\alpha : A \longrightarrow N$ e $\beta : \tilde{\mathrm{G}}/N \longrightarrow G$, obtemos i e μ pelas respectivas composições $A \xrightarrow{\alpha} N \xrightarrow{inc} \tilde{\mathrm{G}}$, $\tilde{\mathrm{G}} \xrightarrow{\pi} \tilde{\mathrm{G}}/N \xrightarrow{\beta} G$; isto é, $i = inc \circ \alpha$ e $\mu = \beta \circ \pi$, resultando no diagrama $A \xrightarrow{i} \tilde{\mathrm{G}} \xrightarrow{\mu} G$ onde $\ker(i) = e_A$, $Im(i) = \ker(\mu)$ e $Im(\mu) = G$.

Essa discussão acena para a seguinte definição:

Definição 1.6.2. *A sequência*

$$A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} A_2 \longrightarrow \ldots \longrightarrow A_{n-1} \xrightarrow{\alpha_{n-1}} A_n$$

de grupos A_i e homomorfismos $\alpha_i : A_i \to A_{i+1}$ é chamada exata se

$$Im(\alpha_{i-1}) = \ker(\alpha_i),\ 1 \leq i \leq n-1.$$

Em particular, se $n = 4$, $A_0 = A_4$ são triviais, denotado por 1, a sequência é chamada sequência exata curta (de grupos).

Da **Definição 1.6.2**, segue que $1 \longrightarrow A \xrightarrow{i} \tilde{\mathrm{G}} \xrightarrow{\mu} G \longrightarrow 1$ é uma sequência exata curta de grupos. As ideias tratadas acima constituem o ponto de partida para a Teoria Homológica (algébrica) de grupos.

Definição 1.6.3. *Uma sequência exata curta $1 \longrightarrow A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} A_3 \longrightarrow 1$ cinde ('splits') se existe um homomorfismo $\sigma : A_3 \longrightarrow A_2$ tal que $\sigma \circ \alpha_2 = 1$.*

Exemplo 1.6.4. (*a*) *Sejam A e B grupos cíclicos de ordem 2. Vamos obter duas extensões distintas de A por B:*

(*a*.1) *Consideremos $K = \{1, a, b, ab\}$ o grupo de Klein. Temos que $|K| = 4$ e K não é um grupo cíclico. Tome $N = \langle a \rangle = \{1, a\}$ com $|N| = 2$. Logo, $N \cong B$, $N \trianglelefteq K$, $|K/N| = 2$ e K/N é um grupo cíclico com $K/N \cong A$. Assim, K é uma extensão de B por A. Observe que, em K, existe $H = \langle b \rangle = \{1, b\}$ tal que $|H| = 2$. Daí, $H \cong K/N \cong A$ com $H \cap N = 1$. Portanto $K = \langle a \rangle \langle b \rangle$.*

(*a*.2) *Seja C_4 o grupo cíclico de ordem 4 dado por $\{1, c, c^2, c^3\}$. Considere $N = \langle c^2 \rangle$ um subgrupo de C_4 de ordem 2 e cíclico. Então $N \cong B$. Mais ainda, $N \trianglelefteq C_4$, $|C_4/N|$ e daí, $C_4/N \cong A$. Logo, C_4 é extensão de B por A. Observe que em C_4 não existe outro subgrupo de ordem 2 além de N. E assim, não existe um subgrupo $H \neq N$ que seja isomorfo a A.*

(*b*) *K é uma extensão cindida de C_2 por C_2 e C_4 não é uma extensão cindida de C_2 por C_2.*

Um tipo de extensão cindida dos grupos A por G é o chamado *produto semidireto*:

Definição 1.6.5. *Seja A um subgrupo do grupo $\tilde{G}$ (não necessariamente normal). Então o subgrupo $G \leq \tilde{G}$ é um complemento de A em $\tilde{G}$ se $A \cap G = 1$ e $\tilde{G} = AG$.*

Um resultado clássico na teoria de grupos finitos relacionado ao produto semidireto é o seguinte:

Teorema 1.6.6 (Schur-Zassenhaus Theorem)**.** [[31], §9.12] *Sejam G um grupo finito e A um subgrupo normal em G. Se $(|A|, |G : A|) = 1$, então G contém um subgrupo de ordem $|G : A|$ e quaisquer dois destes subgrupos são conjugados em G.*

Um subgrupo A nem sempre precisa ter um complemento em $\tilde{G}$ e, caso exista, este não precisa ser único.

Definição 1.6.7. *Um grupo $\tilde{G}$ é o produto semidireto de A por G se $A \trianglelefteq \tilde{G}$ e A possui um complemento $B \cong G$.*

A noção de produto semidireto é uma generalização do *produto direto* de A por G:

Teorema 1.6.8. [[35], Theorem 229] *Seja $\tilde{G}$ um grupo com A e G dois subgrupos normais. Se $\tilde{G} = AG$ e $A \cap G = 1$, então $\tilde{G} \cong A \times G$.*

Corolário 1.6.9. [[19], Corollary 5.2] *O produto semidireto $\tilde{G}$ de A por G com respeito a ψ, homomorfismo de G em $Aut(A)$, é isomorfo ao produto direto de A por G se, e somente se, ψ leva G no subgrupo identidade de $Aut(A)$.*

Proposição 1.6.10. [[22], página 142] *Sejam* $G = \langle X \mid R \rangle$ *e* $A = \langle Y \mid S \rangle$ *grupos, e* $\psi : G \to Aut(A)$ *um homomorfismo tal que* $y(x\psi) = w_{x,y}$ *é uma palavra em* $Y \setminus \{0\}$ $(x \in X, y \in Y)$. *Então o produto semidireto* $\tilde{G}$ *de* A *por* G *tem a seguinte apresentação*

$$\langle X, Y \mid R, S, \{x^{-1}yxw_{x,y}^{-1} \mid x \in X, y \in Y\}\rangle.$$

Neste trabalho, faremos distinção entre produto semidireto interno, $\tilde{G}{=}AG$, e produto semidireto externo, $\tilde{G}{=}A \ltimes G$, onde A e G não são necessariamente subgrupos de $\tilde{G}$ mas isomorfos a algum subgrupo de $\tilde{G}$ e ψ o homomorfismo de G em $Aut(A)$.

Considere agora A um subgrupo normal de $\tilde{G}$. De maneira mais geral, definimos o *complemento parcial*:

Definição 1.6.11. *Dizemos que* G *é um complemento parcial de* A *em* $\tilde{G}$ *se* $\tilde{G}{=}AG$ *e* G *é um subgrupo de* $\tilde{G}$. *O subgrupo (apropriado)* M *de* $\tilde{G}$, $G \cap A = M$, *é normal em* G *mas não necessariamente a identidade.*

Como feito para o produto semidireto, temos agora o que seria a definição de *produto semidireto parcial*:

Definição 1.6.12. $\tilde{G}$ *é o produto semidireto parcial de* A *por* G, *denotado por* $A\ ]\ G$, *se* $\tilde{G}{=}AG$, A *é normal em* $\tilde{G}$ *e* $M = A \cap G$.

Exemplo 1.6.13. *Seja* $A = \langle a \rangle$ *um grupo cíclico de ordem* 2^n, $n > 1$. *Defina* $m = a^{2^{n-1}}$ *com* $M = \langle m \rangle$ *de ordem* 2. *Sejam* $G = \langle g \rangle$ *grupo cíclico de ordem* 4 *e* θ *o isomorfismo de* M *em* G *determinado por* $m\theta = g^2$. *Considere* $g\psi$ *o automorfismo de* A *que inverte todos os seus elementos e, então* ψ *determina um homomorfismo de* G *em* $Aut(G)$. *Logo, o produto semidireto parcial de* $\tilde{G}$ *existe e satisfaz as seguintes relações*

$$\langle g, a \mid a^{2^{n-1}} = g^2 = m, m^2 = 1, g^{-1}ag = a^{-1}\rangle.$$

Observe que esse grupo satisfaz as mesmas relações que os quatérnios generalizados. No caso especial em que $n = 2$, *a ordem do grupo é* 8, *o grupo dos quatérnios. Lembre-se que os quatérnios generalizados de ordem* 2^{n-1} *e o grupo diedral tem a mesma ordem mas não são isomorfos.*

1.7 O Grupo $\nu(G)$

Nesta seção apresentamos os resultados introdutórios dos principais grupos de estudo desta tese, a saber, os grupos $\nu(G)$, $[G, G^{\varphi}]$, $\Delta(G)$, $G \wedge G$, $\mu(G)$ e $M(G)$. Como principais referências e resultados, citamos: Blyth & Morse [8], Brown & Loday [9], Brown, Johnson & Robertson [10], Karpilovsky [25], Rocco [[32], [34]] e Whitehead [44].

Uma *ação* de um grupo G sobre um grupo H é um homomorfismo $\theta : G \to Aut(H)$. Escrevemos $(h)(g)\theta = h^g$, denotando a ação (à direita) de G sobre H. Se θ é o homomorfismo trivial, $h^g = h$, então dizemos que G *age trivialmente sobre* H ou que H *é* G*-trivial*.

Agora, consideramos que G age sobre H, que H age sobre G e que eles agem sobre si mesmos por conjugação. Dessa forma, temos uma ação do produto livre $G * H$ sobre G e H. Se, para todos $g, g_1 \in G$ e $h, h_1 \in H$, ocorrer

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

então dizemos que G *e* H *agem compativelmente* um sobre o outro.

Assumindo que G e H agem um no outro compativelmente, o produto tensorial não abeliano $G \otimes H$, introduzido por Brown & Loday [9], que generaliza o produto tensorial usual $G/G' \otimes_{\mathbb{Z}} H/H'$ de grupos abelianizados, é gerado por todos os símbolos $g \otimes h$, $g \in G$, $h \in H$, sujeito às seguintes relações:

$$gg_1 \otimes h = (g^{g_1} \otimes h^{g_1})(g_1 \otimes h) \tag{1.4}$$

$$g \otimes hh_1 = (g \otimes h_1)(g^{h_1} \otimes h^{h_1}), \tag{1.5}$$

para todos $g, g_1 \in G$, $h, h_1 \in H$. Observe que as relações (1.4) e (1.5) têm a forma das identidades de comutadores quando $g \otimes h$ é substituído por $[g, h]$ e as ações por conjugação.

Uma vez que a ação por conjugação do grupo G sobre si mesmo satisfaz (1.4) e (1.5), o *quadrado tensorial não abeliano* $G \otimes G$ de um grupo G fica naturalmente definido.

Definição 1.7.1. [[10], Remark 3] *Sejam* G, H *e* L *grupos. Uma aplicação* $\psi : G \times H \to L$ *é chamada de biderivação se, para todos* $g, g_1 \in G$ *e* $h, h_1 \in H$*, valem*

$$(gg_1, h)\psi = (g^{g_1}, h^{g_1})\psi \ (g_1, h)\psi$$

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

Aplicando o Teste da Substituição, **Teorema 1.2.9**, não é difícil verificar que uma biderivação $\psi : G \times H \to L$ determina um único homomorfismo $\psi^\star : G \otimes H \to L$ tal que $(g \otimes h)\psi^\star = (g, h)\psi$, para todos $g \in G$ e $h \in H$. Em outras palavras, o produto tensorial não abeliano satisfaz a Propriedade Universal na Teoria de Categorias a partir de uma biderivação.

Exemplo 1.7.2. *Considere G um grupo e a função $\psi : G \times G \to G'$ que associa $(g,h) \to [g,h]$, para todo $(g,h) \in G \times G$. Pela* ***Proposição 1.1.1****, vemos que ψ é uma biderivação. Portanto, ψ induz um único homomorfismo $\rho' : G \otimes G \to G'$ tal que $(g \otimes h)\rho = [g,h]$, para todos $g, h \in G$.*

A seguir, listamos alguns dos resultados obtidos por Brown, Johnson & Robertson [10] que também podem ser encontrados em Brown & Loday [9]:

Proposição 1.7.3. (a) [[10], Proposition 1 (i)] *Os grupos G e H atuam sobre $G \otimes H$ de modo que*

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

para todos $g, g_1 \in G$ e $h, h_1 \in H$. Daí, obtemos uma ação de $G * H$ em $G \otimes H$.
(b) [[10], Proposition 1 (iii)] *Existe um único isomorfismo $\tau : G \otimes H \longrightarrow H \otimes G$ tal que $(g \otimes h)\tau = (h \otimes g)^{-1}$, para todos $g \in G$ e $h \in H$.*

Buscando dar um tratamento grupo-teorético ao estudo do quadrado tensorial não abeliano de grupos e valendo-se do cálculo de comutadores, Rocco [34] introduziu um operador ν na classe dos grupos:

Definição 1.7.4. [[34], página 65] *Sejam G e G^{φ} grupos isomorfos via φ, que associa $g \mapsto g^{\varphi}$, $\forall g \in G$. Definimos o grupo*

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

Os grupos G e G^{φ} estão isomorficamente imersos em $\nu(G)$. Uma motivação para o estudo do grupo $\nu(G)$ é a conexão entre o grupo $\Upsilon(G) := [G, G^{\varphi}]$ e o quadrado tensorial não abeliano:

Proposição 1.7.5. (i) [[34], Proposition 2.6] *$\Upsilon(G) \cong G \otimes G$ via isomorfismo Ω que associa $[g, h^{\varphi}] \mapsto g \otimes h$, para todo $g, h \in G$.*
(ii) [[34], Theorem 3.3] $\nu(G) = (\Upsilon(G)\ G)\ G^{\varphi}$*, isomorfo ao produto $((G \otimes G) \rtimes G) \rtimes G$.*

A **Proposição 1.7.5** (ii) nos diz que o grupo $\nu(G)$ pode ser visto como o produto entre seu subgrupo normal $\Upsilon(G)$ e duas cópias do grupo G. De maneira análoga, podemos ver o grupo $\nu(G)$ como o isomorfismo entre o grupo resultante da ação de G sobre $G \otimes G$, garantida pela **Proposição 1.7.3**, pela ação do grupo G^{φ}.

O próximo Lema é um compêndio de propriedades e resultados que podem ser encontrados em Brown, Johnson & Robertson [10], Blyth & Morse [8] e Rocco [[32], [34]]:

Lema 1.7.6. *As seguintes relações valem em $\nu(G)$:*
(i) $[[g,h^\varphi],[x,y^\varphi]] = [[g,h],[x,y]^\varphi]$, *para todo* $g,h,x,y \in G$;
(ii) $[g_1,[g_2,g_3]^\varphi] = [g_1,g_2,g_3^\varphi]^{-1}$, *para todos* $g_1,g_2,g_3 \in G$;
(iii) $[g_1,g_2^\varphi]^{[g_3,g_4^\varphi]} = [g_1,g_2^\varphi]^{[g_3,g_4]}$, *para todos* $g_1,g_2,g_3,g_4 \in G$;
(iv) $[g_1,g_2^\varphi,g_3] = [g_1,g_2,g_3^\varphi] = [g_1,g_2^\varphi,g_3^\varphi] = [g_1^\varphi,g_2,g_3] = [g_1^\varphi,g_2,g_3^\varphi] = [g_1^\varphi,g_2^\varphi,g_3]$, *para todos* $g_1,g_2,g_3 \in G$;
(v) $[g,g^\varphi]$ *é central em* $\nu(G)$, *para todo* $g \in G$;
(vi) $[g_1,g_2^\varphi][g_2,g_1^\varphi]$ *é central em* $\nu(G)$, *para todos* $g_1,g_2 \in G$;
(vii) $[g,g^\varphi] = 1$, *para todo* $g \in G'$.

O subgrupo normal de $\Upsilon(G)$, $\Delta(G) := \langle [g,g^\varphi] \mid g \in G\rangle$, o qual chamaremos de *subgrupo diagonal*, é central em $\nu(G)$ pelo **Lema 1.7.6**. Identificaremos a seção $\nu(G)/\Delta(G)$ do grupo $\nu(G)$ por $\tau(G)$. Já o grupo quociente $\Upsilon(G)/\Delta(G)$ é isomorfo ao chamado *quadrado exterior*, $G \wedge G$, o qual foi estudado por Miller [29]. Para mais detalhes, veja Brown, Johnson & Robertson [[10], página 181].

Vejamos, a seguir, mais algumas propriedades do grupo $\nu(G)$:

Lema 1.7.7. [[34], Lemma 2.2] *Sejam* a,b,x *elementos de* G *tais que* $[x,a] = [x,b] = 1$. *Então, em* $\nu(G)$, *temos que* $[a,b,x^\varphi] = [[a,b]^\varphi,x] = 1$.

Lema 1.7.8. [[34], Lemma 2.3] *Sejam* x *e* y *elementos de* G *tais que* $[x,y] = 1$. *Então, em* $\nu(G)$, *temos que:*
(i) $[x^n,y^\varphi] = [x,y^\varphi]^n = [x,(y^\varphi)^n]$, *para todo* $n \in \mathbb{Z}$;
(ii) Se x *e* y *são elementos de torção com ordens* $o(x)$ *e* $o(y)$, *então* $o([x,y^\varphi])$ *divide* $(o(x),o(y))$.

Definição 1.7.9. *A partir do epimorfismo natural,* $\pi : G \longrightarrow G/G'$, *definimos* $o'(x) = o(xG')$, *a ordem relativa da classe* xG'. *Em outras palavras, dizemos que* $o'(x) = l$ *se* $x^l \in G'$ *e, se* $x^t \in G'$ *então* $l \mid t$.

Lema 1.7.10. [[32], Lemma 3.1] *Sejam* G *um grupo e* g, h *elementos genéricos de* G. *Então:*
(i) $[g,h^\varphi][h,g^\varphi] = [gh,(gh)^\varphi].[h,h^\varphi]^{-1}.[g,g^\varphi]^{-1}$ $(\in \Delta(G))$;
(ii) $[g,h^\varphi][h,g^\varphi] = [h,g^\varphi][g,h^\varphi]$;
(iii) Se $h \in G'$ *então* $[g,h^\varphi][h,g^\varphi] = 1$;
(iv) Se $gG' = hG'$ *então* $[g,g^\varphi] = [h,h^\varphi]$;
(v) Se $o'(g)$ *ou* $o'(h)$ *é finito então* $o([g,h^\varphi][h,g^\varphi])$ *divide* $(o'(g),o'(h))$;
(vi) Se $o'(h)$ *é finito então* $o([h,h^\varphi])$ *divide* $(o'(h)^2, 2o'(h))$.

Corolário 1.7.11. [[32], Corollary 3.2] *Sejam G um grupo finito de ordem impar e $g \in G$ um elemento com $o'(g) = s$. Então $o([g, g^{\varphi}])$ divide s.*

Proposição 1.7.12. [[32], Proposition 3.3] *Seja $X = \{x_i\}_{i \in I}$ um conjunto de geradores de um grupo G com I um conjunto totalmente ordenado. Então $\Delta(G)$ é gerado pelo conjunto*

$$\Delta := \{s_i := [x_i, x_i^{\varphi}], t_{jk} := [x_j, x_k^{\varphi}][x_k, x_j^{\varphi}] \mid i, j, k \in I, j < k\}.$$

Agora, apresentaremos a definição de um funtor quadrático que possui uma conexão com $G \otimes G$, ou seja, com $\Upsilon(G)$ em $\nu(G)$.

Dado um grupo abeliano (aditivo) A, $\Gamma(A)$ é definido como sendo o grupo gerado por todos os elementos γa, com $a \in A$, sujeito às relações:

$$\gamma(-a) = \gamma a,$$

$$\gamma(a + b + c) + \gamma a + \gamma b + \gamma c = \gamma(a + b) + \gamma(b + c) + \gamma(c + a).$$

Este funtor γ é conhecido como *funtor quadrático de Whitehead* [[44], página 61].

Proposição 1.7.13. [[10], página 181, §(14)] *Existe um homomorfismo bem definido $\psi : \Gamma(G^{ab}) \longrightarrow G \otimes G$ tal que $(\gamma \bar{g})\psi = g \otimes g$, onde $\bar{g}$ denota a classe lateral de g módulo G'.*

O subgrupo de $G \otimes G \cong [G, G^{\varphi}]$, $Im\psi$, é exatamente igual o subgrupo $\Delta(G)$, mencionado na **Proposição 1.7.13**.

Considere agora $\Theta(G)$ o subgrupo de $\nu(G)$ gerado por todos os elementos $g^{-1}g^{\varphi}$, para todo $g \in G$, usualmente escrito $[G, \varphi] := \langle [g, \varphi] \mid g \in G \rangle$, onde $[g, \varphi] = g^{-1}g^{\varphi}$.

Proposição 1.7.14. [[32], Proposition 2.4] *(i) O grupo $\Theta(G)$ centraliza $\Upsilon(G)$ e é normal em $\nu(G)$;*
(ii) $\nu(G) = \Theta(G) \rtimes G$;
(iii) Existe um epimorfismo $\rho : \nu(G) \longrightarrow G$ que associa $g \mapsto g$ e $g^{\varphi} \mapsto g$, para qualquer $g \in G$, tal que $\ker(\rho) = \Theta(G)$.

A restrição do epimorfismo ρ a $\Upsilon(G)$ nos dá a *aplicação derivada* $\rho' : \Upsilon(G) \longrightarrow G'$, definida por $\rho'([g, h^{\varphi}]) = [g, h]$, para todos $g, h \in G$. Vamos denotar $\ker(\rho') := \mu(G)$, com $\Delta(G) \lhd \mu(G)$ e $\mu(G) = \Upsilon(G) \cap \Theta(G)$.

O grupo $\mu(G)$ é identificado como sendo o grupo $J_2(G)$ na Teoria de Homologia, como pode ser visto em Brown & Loday [9]. O seguinte resultado proporciona um melhor entendimento de tal grupo:

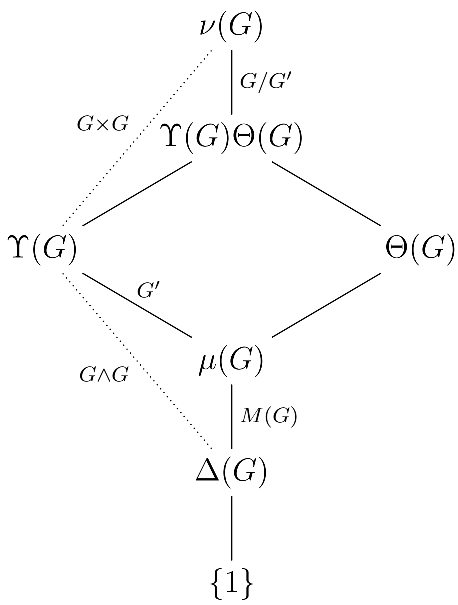
Proposição 1.7.15. [[32], Proposition 2.4] *(i)* $\mu(G)$ *consiste dos elementos de* $\Upsilon(G)$ *da forma* $[g_1, h_1^{\varphi}]^{\epsilon_1}[g_2, h_2^{\varphi}]^{\epsilon_2} \ldots [g_s, h_s^{\varphi}]^{\epsilon_s}$ *tal que* $[g_1, h_1]^{\epsilon_1}[g_2, h_2]^{\epsilon_2} \ldots [g_s, h_s]^{\epsilon_s} = 1$, *onde* s *é um número natural,* $g_i, h_i \in G$, $\epsilon_i \in \{-1, 1\}, 1 \leq i \leq s$;
(ii) $\mu(G)$ *é central em* $\nu(G)$.

Observe que o grupo $\mu(G)$ é abeliano. A próxima proposição é uma consequência dos resultados acima e da descrição do segundo grupo de homologia feita por Miller [29]:

Proposição 1.7.16. [[32], Proposition 2.8] *A seção* $\mu(G)/\Delta(G)$ *do grupo* $\nu(G)$ *é isomorfa ao segundo grupo de homologia* $\mathcal{H}_2(G)$.

O segundo grupo de homologia de um grupo dado G é identificado pelo *multiplicador de Schur*, $M(G)$, definido por Schur em 1904 com o propósito de estudar representações projetivas, [[31], página 347]. Um estudo mais detalhado pode ser encontrado em Karpilovsky [25].

O diagrama a seguir sumariza as informações acima descritas a respeito da estrutura do grupo $\nu(G)$:



1.7 Diagrama das seções do grupo $\nu(G)$

A partir de agora, usaremos a identificação do grupo $[G, G^{\varphi}]$ para o grupo $G \otimes G \cong \Upsilon(G)$ tal qual o tensor $g \otimes h$ será identificado por $[g, h^{\varphi}]$, para quaisquer $g, h \in G$.

Podemos sintetizar alguns dos principais resultados a respeito do grupo $\nu(G)$ envolvendo propriedades estruturais do grupo G, como o fato do grupo G ser p-grupo, finitude, solubilidade e nilpotência. Estes resultados podem ser encontrados em Rocco [[32], [34]]:

Teorema 1.7.17. [[32], [34]] *Seja G um grupo.*
(i) Se G é finito, então $\nu(G)$ é finito.
(ii) Se G é um π-grupo, então $\nu(G)$ é um π-grupo onde π é um conjunto de números primos.
(iii) Se G é nilpotente de classe c, então $\nu(G)$ é nilpotente de classe no máximo $c+1$.
(iv) Se G é solúvel de comprimento derivado d então $\nu(G)$ é solúvel de comprimento derivado no máximo $d+1$.

Rocco [[34], Remark 2] dá uma demonstração para o item (i) do **Teorema 1.7.17** da finitude do grupo $\nu(G)$ caso o grupo G seja finito usando uma conexão com o grupo $\chi(G)$, introduzido por Sidki [[38], página 199, §4]:

Para um par de grupos isomorfos, G e G^{φ}, defina o grupo

$$\chi(G) = \langle G, G^{\varphi} \mid [g, g^{\varphi}] = 1, \ \forall g \in G \rangle.$$

Neste mesmo artigo, Sidki [38] demonstra algumas propriedades do grupo $\chi(G)$, das quais decorrem o **Teorema 1.7.17**:

Teorema 1.7.18. [[38], Theorem 4.2.4] *Seja G um π-grupo finito (π é um conjunto de primos), nilpotente finito ou solúvel de grau finito. Então $\chi(G)$ é também um π-grupo finito, nilpotente finito ou solúvel de grau finito.*

O subgrupo $R(G)$ do grupo $\chi(G)$, é tal que as relações $[g_1, g_2^{\varphi}]^{g_3^{\varphi}} = [g_1^{g_3}, (g_2^{g_3})^{\varphi}]$ seguem no quociente $\dfrac{\chi(G)}{R(G)}$, para todos $g_1, g_2, g_3 \in G$. Tal grupo é isomorfo a seção $\tau(G) = \dfrac{\nu(G)}{\Delta(G)}$ do grupo $\nu(G)$:

Teorema 1.7.19. [[32], página 69] *Para todo grupo G*

$$\frac{\chi(G)}{R(G)} \cong \frac{\nu(G)}{\Delta(G)}.$$

Ainda do **Teorema 1.7.17**, como consequência do item (iv), Rocco [32] dá uma apresentação finita e solúvel para o grupo $\nu(G)$, desde que G seja um grupo finito e solúvel:

Teorema 1.7.20. [[32], Theorem 2.1] *Sejam G e G^{φ} grupos finitos policíclicos com as respectivas sequências policíclicas, $\{a_1, a_2, \ldots, a_n\}$ e $\{b_1, b_2, \ldots, b_n\}$, onde $\varphi : G \to G^{\varphi}$ um isomorfismo tal que $a_i \mapsto b_i$, $1 \leq i \leq n$. Seja $\delta(G)$ o grupo dado pela apresentação abaixo*

$$\langle a_1, ..., a_n, b_1, ..., b_n \mid G\text{-relações},\ G^{\varphi}\text{-relações}, [a_i, b_j]^{a_k} = [a_i^{a_k}, b_j^{b_k}] = [a_i, b_j]^{b_k}, 1 \leq i, j, k \leq n \rangle.$$

Então $\delta(G) \cong \nu(G)$. Além disso, o subgrupo $[G, G^{\varphi}]$ é gerado por $\{[a_i, b_j] \mid 1 \leq i, j \leq n\}$.

Observe que a apresentação dada no **Teorema 1.7.20** depende apenas das sequências policíclicas e das relações policíclicas dos grupos G e G^{φ}, ou seja, são usados apenas os geradores policíclicos dos grupos em questão.

A fim de dar uma apresentação policíclica para $[G, G^{\varphi}]$ a partir de uma apresentação policíclica de $\nu(G)$, primeiramente Blyth & Morse [8] mostram que se a classe $\mathfrak{X}$ de grupos é fechada para extensões então, para qualquer grupo G tal que $\mu(G), G' \in \mathfrak{X}$, segue que $[G, G^{\varphi}] \in \mathfrak{X}$. A 'propriedade' policíclica é fechada para extensões e subgrupos. Assim, para mostrar que $[G, G^{\varphi}]$ é policíclico, é suficiente mostrar que $\mu(G)$ é finitamente gerado.

Proposição 1.7.21. [[8], Proposition 9] *Seja G um grupo policíclico. Então $[G, G^{\varphi}]$ e $\nu(G)$ são policíclicos.*

Antes de dar uma apresentação policíclica para o quadrado tensorial de um grupo policíclico, daremos algumas definições:

Definição 1.7.22. [[8], Definition 12] *Sejam G um grupo e $G = G_n \geqslant G_{n-1} \geqslant \ldots \geqslant G_0 = 1$ uma série subnormal para G. Se $\mathcal{T}_i$ denota um transversal para G_{i-1} em G_i e $\mathcal{G}_i$ denota o levantamento de um conjunto gerador de G_i/G_{i-1} para $\mathcal{T}_i$. Fazendo*

$$\mathcal{L}_i = \begin{cases} \mathcal{G}_i, & \text{se } G_i/G_{i-1} \text{ é abeliano} \\ \mathcal{T}_i, & \text{caso contrário} \end{cases}$$

então o conjunto $\mathcal{L}_G$ relativo a série subnormal acima é definido como

$$\mathcal{L}_G = \bigcup_{i=1}^{n} \mathcal{L}_i.$$

Se G é um grupo policíclico com alguma série policíclica $G = G_n \geq \ldots \geq G_1 \geq G_0 = 1$ e sequência policíclica $\wp$, então $\mathcal{L}_G$ relativa a esta série é $\wp$.

Para os resultados obtidos nessa tese, seria suficiente usar o **Teorema 1.7.20** quando trabalhamos com grupos policíclicos finitos. Em contrapartida, o seguinte resultado é uma generalização do mesmo para um grupo policíclico qualquer.

Teorema 1.7.23. [[8], Theorem 13] *Sejam $G = \langle X \mid R \rangle$ um grupo finitamente apresentado e S uma série subnormal de G. Então $\nu(G)$ tem a seguinte apresentação*

$$\nu(G) = \langle X, X^{\varphi} \mid R, R^{\varphi}, [g, h^{\varphi}]^k = [g^k, (h^k)^{\varphi}] = [g, h^{\varphi}]^{k^{\varphi}}, \forall g, h \in X, k \in \mathcal{L}_G \text{ relativo a } S \,\rangle.$$

O **Teorema 1.7.23** nos proporciona uma apresentação policíclica para o grupo $\nu(G)$ a partir da apresentação finitamente gerada do grupo G, generalizando assim o **Teorema 1.7.20**.

Observe que, para o caso em que G é um grupo infinito, o **Teorema 1.7.23** nos dá uma apresentação finita de $\nu(G)$, o que não seria possível obter a partir da definição do grupo $\nu(G)$ somente. Um dos principais resultados obtidos por Blyth & Morse [8] foi dar uma completa descrição dos geradores do quadrado tensorial $[G, G^{\varphi}]$ de um grupo policíclico G em termos de um conjunto gerador policíclico de G. O grupo $\tau(G)$ é definido como sendo o grupo quociente $\nu(G)/\Omega(\Delta(G))$, onde Ω é o isomorfismo da **Proposição 1.7.5**. Denotaremos o subgrupo $[G, G^{\varphi}]/\Omega(\Delta(G))$ de $\tau(G)$ por $[G, G^{\varphi}]_{\tau(G)}$, isomorfo a $G \wedge G$:

Teorema 1.7.24. [[8], Proposition 20] *Seja G um grupo policíclico com $X = [x_1, x_2, \ldots, x_k]$ uma sequência policíclica. Então $[G, G^{\varphi}]$, subgrupo de $\nu(G)$, é gerado por*

$$[G, G^{\varphi}] = \langle [x_i, x_i^{\varphi}], [x_i^{\delta}, (x_j^{\varphi})^{\epsilon}], [x_i, x_j^{\varphi}][x_j, x_i^{\varphi}] \rangle$$

e $[G, G^{\varphi}]_{\tau(G)}$, subgrupo de $\tau(G)$, é gerado por

$$[G, G^{\varphi}]_{\tau(G)} = \langle [x_i^{\delta}, (x_j^{\varphi})^{\epsilon}], [x_j^{\epsilon}, (x_i^{\varphi})^{\delta}] \rangle,$$

para $1 \leq i < j \leq k$, onde

$$\delta = \begin{cases} 1, & se\ |x_i| < \infty \\ \pm 1, & se\ |x_i| = \infty \end{cases} \qquad e \qquad \epsilon = \begin{cases} 1, & se\ |x_j^{\varphi}| < \infty \\ \pm 1, & se\ |x_j^{\varphi}| = \infty. \end{cases}$$

Com esses resultados revisitados, daremos prosseguimento ao nosso trabalho a fim de calcularmos uma apresentação para o grupo $\nu(G)$ onde G será um grupo metacíclico tanto finito quanto infinito. A partir de tal apresentação, graças aos resultados acima mencionados, será possível obter conjuntos geradores dos grupos $[G, G^{\varphi}]$, $G \wedge G$, $M(G)$ e $\tau(G)$, vistos como seções do grupo $\nu(G)$, dadas no diagrama 1.7. No caso em que o grupo G é metacíclico infinito, auferimos também uma apresentação para a seção abeliana $\mu(G)$, central em $\nu(G)$. Estes grupos vem despertando interesse há um tempo. O que pretendemos resgatando esse estudo é fechar todas as análises possíveis das seções supracitadas de um grupo metacíclico.

Capítulo 2

Grupos Metacíclicos

Neste Capítulo, dividido em duas partes, revisitaremos a teoria necessária para o estudo dos grupos metacíclicos finitos e infinitos. Na primeira seção, vamos analisar os grupos metacíclicos finitos gerados por a e b, denotados por $G = g(a, b; m, n, r, s)$. Uma apresentação para o grupo $g(a, b; m, n, r, s)$ é dada por:

$$\langle a, b \mid a^m = 1, b^n = a^s, a^b = a^r \rangle,$$

onde $m, n > 0$, $r^n \equiv 1 \ (mod\ m)$ e $s(r-1) \equiv 0 \ (mod\ m)$. Ou seja, os grupos metacíclicos finitos são totalmente identificados pela quadra (m, n, r, s). Ainda na seção dos grupos metacíclicos finitos, calcularemos as ordens relativas às classes aG' e bG', denotados por $o'(a)$ e $o'(b)$, respectivamente. Para o entendimento do número $o'(b)$ é necessário computar a ordem de b, $o(b)$, uma vez que o grupo é não necessariamente cindido. Estes três objetos influenciam diretamente na análise da ordem dos elementos de um conjunto gerador do quadrado tensorial não abeliano. Algumas definições e propriedades básicas podem ser encontradas em Curtis & Reiner [13], Johnson [22], Hall [28] e Zasenhauss [45]. Para este trabalho, é indiferente se o grupo $g(a, b; m, n, r, s)$ é um p-grupo ou não. Salvo menção em contrário, o grupo metacíclico finito é não cindido, ou seja, $s > 0$.

Na segunda parte deste Capítulo, baseado na classificação dada por Beuerle & Kappe [3], estudaremos os grupos metacíclicos infinitos, denotados por $G = g(a, b; m, n, r)$. Segundo eles, o grupo metacíclico infinito pode ser escrito de uma das seguintes maneiras:

$$g(a, b; m, 0, r) = \langle a, b \mid a^m = 1, a^b = a^r \rangle,$$
$$g(a, b; 0, n, -1) = \langle a, b \mid b^n = 1, a^b = a^{-1} \rangle \quad \text{ou}$$
$$g(a, b; 0, n, 1) = \langle a, b \mid b^n = 1, a^b = a \rangle,$$

se o grupo for abeliano. Como mencionado anteriormente, também estamos interessados no cálculo dos números $o'(a)$ e $o'(b)$ para o grupo metacíclico infinito G.

Definição 2.0.1. [[22], Definition 3, página 88] *Um grupo G é dito metacíclico se possui um subgrupo normal H cíclico tal que G/H é cíclico.*

Em particular, se G' é um subgrupo cíclico do grupo G tal que o quociente G/G' ainda é um grupo cíclico, então G é o chamado *grupo de Zassenhaus.*

Exemplo 2.0.2. (a) *Os grupos diedrais (finito ou infinito), quatérnios generalizado, definidos no* ***Exemplo*** 1.2.6*, itens* 4. *e* 5. *são metacíclicos. Na mesma classe de grupos contendo um elemento de ordem* 2 *não isomorfos, temos o quasidiedral, cuja apresentação é dada por* $\langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, a^b = a^{2^{n-2}-1}\rangle$, $n > 3$.

(b) *A garrafa de Klein é um grupo metacíclico infinito dado por* $\langle a, b \mid a^b = a^{-1}\rangle$, *definido em Firby & Gardiner* [[17], Definition 3.5.4].

2.1 Grupos Metacíclicos Finitos

A fim de darmos prosseguimento ao que nos propusemos a fazer nesta tese, focaremos em calcular as ordens relativas às classes aG' e bG', onde a, b são os geradores do grupo metacíclico G. No caso em que o grupo metacíclico G for finito, é possível calcular as ordens efetivas dos seus geradores dependendo dos parâmetros (m, n, r, s).

Teorema 2.1.1 (Hölder)**.** [[45], Theorem 20] *Um grupo finito G, de ordem mn, com um subgrupo cíclico normal $H = \langle a\rangle$ e com um grupo quociente $G/H = \langle bH\rangle$ cíclico de ordem n, gerado por a e b, é definido pelas relações*

$$a^m = 1, \quad b^n = a^s, \quad a^b = a^r \tag{2.1}$$

satisfazendo as seguintes condições numéricas:

$$\begin{array}{ll} (a) & 0 < m, n \\ (b) & r^n \equiv 1 \ (mod\ m) \\ (c) & s(r-1) \equiv 0 \ (mod\ m). \end{array}$$

Inversamente, se as condições numéricas são fielmente satisfeitas, então um grupo com as propriedades dadas previamente é definido pelas relações (2.1).

Um grupo metacíclico é uma extensão de um grupo cíclico por outro grupo cíclico. Para fixados m e n, onde $o(a) = m$, a renomeação de r e s por

$$r^\star = r^\nu, \quad (n, \nu) = 1,$$
$$s^\star = s\nu + (1 + r^\nu + \ldots + r^{\nu(n-1)}) = s\nu + E_m(r^\nu, n)$$

nos dá que as extensões cíclicas $g(a, b; m, n, r, s)$ e $g(a, b; m, n, r^{\star}, s^{\star})$ são isomorfas, como pode ser visto em [[45], página 100].

Para estudar os p-grupos metacíclicos finitos, é esperado que se restrinja a possíveis valores dos parâmetros, de modo que dois diferentes conjuntos de parâmetros correspondam a grupos não isomorfos. King [26] mostra que todo p-grupo metacíclico, não cíclico, finito possui uma apresentação única da forma:

$$\langle a, b \mid a^{p^M} = 1, b^{p^N} = a^{p^{M-S}}, a^b = a^{1+p^{M-C}} \rangle, \tag{2.2}$$

se p é ímpar e,

$$\langle a, b \mid a^{2^M} = 1, b^{2^N} = a^{2^{M-S}}, a^b = a^{-1+2^{M-C}} \rangle \tag{2.3}$$

se $p = 2$. Além disso, separa também as apresentações cindidas das não cindidas, envolvendo os parâmetros M, N, S e C, a menos de isomorfismo.

Recentemente, Hempel [20] classificou os 2-grupos metacíclicos. De maneira mais simplificada a apresentada anteriormente por King [26], Hempel deu uma apresentação para os p-grupos metacíclicos finitos, não abelianos, sem distinguir suas apresentações cindidas das não cindidas:

Teorema 2.1.2. [[20], Theorem 4.8] *Qualquer p-grupo metacíclico não abeliano tem uma apresentação da forma*

$$\langle a, b \mid a^{p^M} = 1, b^{p^N} = a^{p^S}, a^b = a^{1+p^K} \rangle$$

onde $M \geq K \geq 1$, $M \geq S \geq M - K$, $N \geq S \geq K$ e $K + p \geq 4$, ou da forma

$$\langle a, b \mid a^{2^M} = 1, b^{2^N} = a^{2^S}, a^b = a^{-1+2^K} \rangle$$

onde $M \geq K \geq 2$, $N + K \geq M$ e $M \geq S \geq M - 1$.

Para padronizar a notação, quando o grupo G for um p-grupo metacíclico finito, denotaremos por $p^M = m$, $p^N = n$, $p^S = s$, $p^K + t = r$, onde $t = \{-1, 1\}$, para p um primo qualquer. A partir de agora consideraremos $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito (p-grupo ou não), satisfazendo as propriedades do **Teorema 2.1.1**.

Neste trabalho, fixaremos $(m, r) = 1$ com $r > 1$ (não consideraremos o grupo abeliano) e $0 < s < m$ no caso em que o grupo não é uma extensão cindida e $s = 0$, caso contrário.

Observação 2.1.2.1. 1) *Não é difícil ver que $(m, s) \neq 1$ no grupo $G = g(a, b; m, n, r, s)$, para qualquer quadra (m, n, r, s) satisfazendo o **Teorema 2.1.1**.*

De fato, suponha que $(m, s) = 1$. Então, $\langle a^s \rangle = \langle a \rangle$ e, $\langle b \rangle \supseteq \langle a \rangle = \langle b^n \rangle$ implicando em G ser um grupo cíclico.

Portanto, se $G = g(a, b; m, n, r, s)$ *é um grupo metacíclico finito, então* $(m, s) \neq 1$.

2) *Quando* $G = g(a, b; m, n, m-1, s)$ *é um grupo metacíclico finito, temos que* n *é sempre par. Caso* m *seja ímpar, então* $G = g(a, b; m, n, m-1, 0)$ *é uma extensão cindida.*

O fato de n *ser par quando* $r = m - 1$ *ocorre porque:* $(m-1)^n \equiv 1 \ (mod \ m)$ *se, e somente se,* n *é par, para qualquer* m.

Já o fato da extensão ser cindida caso m *seja ímpar é devido o fato de* $m \mid (m-2)s$ *e* $s \in \{0, 1, \ldots, m-1\}$. *Mas isso já era sabido pelo* ***Teorema 1.6.6*** *(Schur-Zassenhaus Theorem), uma vez que* G *é um grupo finito e* H *é um subgrupo normal em* G *com* $(m, n) = 1$.

3) *Para qualquer* $x \in \mathbb{Z}$, *se* $n \mid x$, *então* $r^x \equiv 1 \ (mod \ m)$. *Isso ocorre porque existe algum* $\beta \in \mathbb{Z}$ *tal que*

$$r^x = r^{\beta n} = (r^n)^\beta \equiv 1 \ (mod \ m).$$

O Lema a seguir nos proporciona uma forma normal para os elementos do grupo metacíclico finito $G = g(a, b; m, n, r, s)$, para qualquer quadra (m, n, r, s):

Lema 2.1.3. *Seja* $G = g(a, b; m, n, r, s)$ *um grupo metacíclico finito, não abeliano, dado por*

$$g(a, b; m, n, r, s) = \langle a, b \mid a^m = 1, b^n = a^s, a^b = a^r \rangle, \tag{2.4}$$

onde $m, n > 0$, $r^n \equiv 1 \ (mod \ m)$ *e* $s(r-1) \equiv 0 \ (mod \ m)$. *Então, todo elemento* $g \in G$ *pode ser escrito da forma* $g = a^\alpha b^\beta$, *onde* α *e* β *são inteiros únicos módulo* m. *Ademais, se* $h \in G$ *com* $h = a^\gamma b^\delta$, *com* γ *e* δ *unicamente determinados, então as seguintes relações são satisfeitas em* G*:*

(*i*) $(a^\alpha)^{b^\beta} = a^{\alpha r^\beta}$ *e* $(b^\beta)^{a^\alpha} = b^\beta a^{\alpha(1-r^\beta)}$;
(*ii*) $gh = b^{\beta+\delta} a^{r^\delta(\gamma + \alpha r^\beta)}$;
(*iii*) $h^g = b^\delta a^{\alpha r^\beta(1-r^\delta) + \gamma r^{\beta+\delta}}$;
(*iv*) $g^\sigma = b^{\beta\sigma} a^{\alpha r^\beta E_m(r^\beta, \sigma)}$, *para qualquer* $\sigma \in \mathbb{Z}$.

Demonstração. (*i*) Demonstração por indução sobre α e β.

Da igualdade $a^b = a^r$ temos que $a^{b^{-1}} = a^t$ onde $rt \equiv 1 \ (mod \ m)$. Além disso,

$$(a^2)^b = b^{-1}aab = b^{-1}abb^{-1}ab = a^r a^r = a^{2r} \quad \text{e} \quad a^{b^2} = b^{-1}b^{-1}abb = a^{rb} = a^{r^2}.$$

Logo, $(a^2)^{b^2} = a^{2r^2}$. Indutivamente, segue que $(a^\alpha)^{b^\beta} = a^{\alpha r^\beta}$, ou seja, $a^\alpha b^\beta = b^\beta a^{\alpha r^\beta}$.

(*ii*) Pela relação $a^\alpha b^\beta = b^\beta a^{\alpha r^\beta}$ do item (*i*), temos que

$$gh = a^\alpha b^\beta a^\gamma b^\delta = a^\alpha b^\beta b^\delta a^{\gamma r^\delta} = b^{\beta+\delta} a^{\alpha r^{\beta+\delta}} a^{\gamma r^\delta}.$$

(iii) Observe que $g^{-1} = (a^\alpha b^\beta)^{-1} = b^{-\beta}a^{-\alpha}$. Logo,

$$\begin{aligned} g^{-1}hg &= b^{-\beta}a^{-\alpha}a^\gamma b^\delta a^\alpha b^\beta \\ &=_{(i)} b^{-\beta}b^\delta a^{(\gamma-\alpha)r^\delta+\alpha}b^\beta \\ &=_{(i)} b^\delta a^{[(\gamma-\alpha)r^\delta+\alpha]r^\beta} \end{aligned}$$

(iv) Vamos usar indução sobre $\sigma \in \mathbb{Z}_+$ na identidade. Fazendo $\alpha = \gamma$ e $\beta = \delta$ em (i):

$$g^2 = a^\alpha b^\beta a^\alpha b^\beta = b^{2\beta}a^{\alpha r^\beta E_m(r^\beta,2)}.$$

Suponha que a identidade seja satisfeita para σ. Queremos mostrar que vale para $\sigma + 1$:

$$\begin{aligned} g^{\sigma+1} &= a^\alpha b^\beta b^{\sigma\beta} a^{\alpha r^\beta E_m(r^\beta,\sigma)} \\ &=_{(i)} b^{\beta(1+\sigma)}a^{\alpha r^{\beta(\sigma+1)}+\alpha r^\beta E_m(r^\beta,\sigma)} \\ &= b^{\beta(1+\sigma)}a^{\alpha(r^\beta(1+r^\beta+\ldots+(r^\beta)^{\sigma-1}+r^{\beta\sigma}))} \\ &= b^{\beta(1+\sigma)}a^{\alpha r^\beta(1+r^\beta+\ldots+r^{\beta\sigma})}, \end{aligned}$$

pois $\alpha r^{\beta(\sigma+1)} + \alpha r^\beta E_m(r^\beta,\sigma) = \alpha r^\beta(1 + r^\beta + \ldots + r^{\beta(\sigma-1)} + r^{\beta\sigma})$. O mesmo ocorre para $\sigma \in \mathbb{Z}_-$, basta usar indução sobre g^{-1} de (iii). □

O próximo resultado, que pode ser encontrado em Sim [39], nos dá informações sobre os sugbrupos derivado, G', e centro, $Z(G)$, do grupo $G = g(a,b;m,n,r,s)$.

Teorema 2.1.4. [[39], Lemma 2.7] *Seja G um grupo metacíclico com uma fatoração $G = SK$. Sejam $S = \langle b\rangle$, $K = \langle a\rangle$ e r um inteiro tal que $a^b = a^r$. Defina $t := m/(m, r-1)$. Então*

$$G' = \langle a^{r-1}\rangle \cong C_t \quad e \quad Z(G) = \langle a^t, b^n\rangle.$$

Curtis & Reiner [[13], §(47.10)] haviam verificado que a^{r-1} gera o subgrupo derivado de $G = g(a,b;m,n,r,s)$ e que este possui ordem exatamente igual a $m/(m,r-1)$.

Para o prosseguimento deste trabalho, como mencionamos anteriormente, é bastante importante o controle das ordens dos elementos geradores do grupo $G = g(a,b;m,n,r,s)$ tanto quanto das ordens relativas às classes aG' e bG'. Os Lemas subsequentes vão em busca de tal controle:

Lema 2.1.5. *Seja $G = g(a,b;m,n,r,s)$ um grupo metacíclico finito, não abeliano. O subgrupo cíclico $\langle b\rangle$ tem ordem $nm/(m,s)$.*

Demonstração. Sendo $m = o(a)$, considere $u = (m, s)$ de modo que $u = \alpha m + \beta s$, para alguns $\alpha,\ \beta \in \mathbb{Z}$. Logo,

$$a^u = a^{\alpha m + \beta s} = a^{\beta s},$$

o que implica em $a^u \in \langle a^s \rangle$. Mas $u \mid s$, ou seja, existe $\gamma \in \mathbb{Z}$ tal que $s = \gamma u$. Desta forma,

$$a^s = a^{\gamma u} \in \langle a^u \rangle.$$

$$\begin{tikzcd}
\langle a \rangle \arrow[d, dash, "(m,s)"] \\
\langle a^s \rangle = \langle a^u \rangle \arrow[d, dash, "m/(m,s)"] \\
\{1\}
\end{tikzcd}
\qquad
\begin{tikzcd}
\langle b \rangle \arrow[d, dash, "n"] \arrow[dd, dotted, dash, bend left=60, "o(b)"] \\
\langle b^n \rangle = \langle a^s \rangle \arrow[d, dash, "m/(m,s)"] \\
\{1\}
\end{tikzcd}$$

Portanto, $\langle a^s \rangle = \langle a^u \rangle$ de índice u em $\langle a \rangle$. Em outras palavras,

$$o(a^s) = o(a^u) = m/u = \frac{m}{(m, s)}$$

e segue que $o(b) = n\dfrac{m}{(m, s)}$.

$\square$

A estratégia de análise do próximo resultado é o estudo da interseção entre os subgrupos $\langle a^{r-1} \rangle$ e $\langle a^s \rangle$ a saber, $\langle a^s \rangle \cap \langle a^{r-1} \rangle = \langle a^{[s,r-1]} \rangle$, onde $[s, r-1] = mmc(s, r-1)$:

Proposição 2.1.6. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito não abeliano. Então*

$$o'(a) = (m, r-1) \quad e \quad o'(b) = \left(o(b),\ n\frac{s(r-1)}{(m, s)(s, r-1)} \right).$$

Demonstração. Pelo **Teorema 2.1.4**, é fácil ver que $o'(a) = (m, r-1)$. Vamos analisar o índice $[\langle b \rangle : \langle a^t \rangle] = o'(b)$, onde $t = [s, r-1]$.

A interseção entre os subgrupos $\langle a^{r-1} \rangle$ e $\langle a^s \rangle$ é igual a $\langle a^t \rangle$, um subgrupo não trivial desde que $(s, r-1) \neq 1$. Além disso, o subgrupo $\langle a^t \rangle$ é o maior subgrupo de G contido em $\langle b \rangle$ e $\langle a^{r-1} \rangle$. Logo, pelo **Lema 2.1.5**, temos que

$$\begin{tikzcd}
 & & G \arrow[dll, dash] \arrow[drr, dash] & & \\
\langle\ a\ \rangle \arrow[d, dash, "o'(a)"'] \arrow[drr, dash] & & & & \langle\ b\ \rangle \arrow[dll, dash, "n"] \\
\langle a^{r-1} \rangle \arrow[drr, dash] & & \langle a^s \rangle = \langle b^n \rangle \arrow[d, dash] \arrow[dd, dotted, dash, bend left=60, "\frac{m}{(m,s)}"] & & \\
 & & \langle a^{[s,r-1]} \rangle \arrow[d, dash] & & \\
 & & \{1\} & &
\end{tikzcd}$$

$$\left| \frac{\langle b \rangle}{\langle b^n \rangle} \right| = n \quad \text{e} \quad o(a^s) = \frac{m}{(m, s)}$$

e, com uma análise análoga obtemos

$$|\langle a^{r-1} \rangle \cap \langle b^n \rangle| = \frac{m}{(m, t)}.$$

Portanto,

$$\left| \frac{\langle b \rangle}{\langle a^t \rangle} \right| = n \frac{\frac{m}{(m,s)}}{\frac{m}{(m,t)}} = n\frac{(m, t)}{(m, s)}.$$

$\square$

Ao longo deste trabalho, não restringiremos a quadra (m, n, r, s) às condições como $(r-1) \mid s$, $r - 1 = s$, $s \mid (r-1)$, $(r-1, s) = 1$ e $(r-1, s) = \alpha \neq r-1, \alpha \neq s$, pois estas restrinções geram vários casos (especificamente falando, 32 casos), combinados às condições em que $(m, s) = s$ ou $(m, s) = t \neq s$ e suas respectivas paridades.

Abaixo, segue alguns exemplos de grupos metacíclicos finitos que aparecem frequentemente na literatura:

Exemplo 2.1.7. *Para $k \geq 2$, o grupo*

$$g(x, y; 2^k, 2, -1, 2^{k-1}) = \langle x, y \mid x^{2^k} = 1, y^2 = x^{2^{k-1}}, x^y = x^{-1} \rangle,$$

é chamado quatérnio generalizado cuja ordem é 2^{k+1}. Não é difícil ver que seu subgrupo derivado é $\langle x^{-2} \rangle$ cujo ordem é 2^{k-1}. Observe que $\langle x^{-2} \rangle \cap \langle x^{2^{k-1}} \rangle = \langle x^{2^{k-1}} \rangle$, para qualquer $k > 1$ implicando em

$$o'(x) = (2^k, 2) = 2,$$

$$o(y) = \frac{2^k 2}{(2^k, 2^{k-1})} = 4$$

$$o'(y) = \left(o(y), \frac{2 2^{k-1} 2}{(2^k, 2^{k-1})(2^{k-1}, 2)} \right) = 2.$$

Carmichael, [[11], páginas 181-182]*, define o grupo dicíclico de ordem $4n$ por*

$$g(x, y; 2n, 2, -1, n) = \langle x, y \mid x^{2n} = 1, y^2 = x^n, x^y = x^{-1} \rangle,$$

para $n > 1$. Observe que seu subgrupo derivado é gerado por $\langle x^{-2} \rangle$ de ordem n, fazendo $n = 2^{k-1}$, $k > 1$, no grupo dos quatérnios generalizados. De forma análoga, a interseção $\langle x^{-2} \rangle \cap \langle x^n \rangle$ depende da paridade de n:

Se n é par, então $\langle x^{-2} \rangle \cap \langle x^n \rangle = \langle x^n \rangle$ implicando em $o'(x) = 2 = o'(y)$ e $o(y) = 4$, como feito acima para o grupo quatérnio generalizado.

*Se n é ímpar, então $\langle x^{-2} \rangle \cap \langle x^n \rangle = 1$, implicando em $o'(x) = 2$ e $o'(y) = 4 = o(y)$. Ambos podem ser verificados também pela **Proposição 2.1.6**. Em todos os casos, a ordem de y é igual a 4, coincidindo com o **Lema 2.1.5**.*

Exemplo 2.1.8. *O grupo diedral finito G de ordem $2m$ é dado por*

$$g(a, b; m, 2, -1, 0) = \langle a, b \mid a^m = 1, b^2 = 1, a^b = a^{-1} \rangle, \ m > 2.$$

Segue que $G' \cong \langle a^2 \rangle$ com ordem igual a $m/(m, 2)$. Como o grupo é uma extensão cindida, temos que $o'(b) = o(b) = 2$.

Agora, vamos calucular $o'(a)$:

Se m é um inteiro ímpar, $m > 2$, então $\mathcal{U}_m$ possui uma quantidade par de elementos. Além disso, temos que $o(a^2) = \dfrac{m}{(m, 2)} = m$. Logo, $\langle a^2 \rangle = \langle a \rangle$, implicando em $o'(a) = 1$.

Se m é um inteiro par maior do que 2, então $o'(a) = (m, 2) = 2$.

Exemplo 2.1.9. *O grupo semi-diedral (ou quasi diedral) G de ordem 2^n possui uma apresentação dada por*

$$g(x,y;2^{n-1},2,2^{n-2}-1,0) = \langle x,y \mid x^{2^{n-1}} = 1, y^2 = 1, x^y = x^{2^{n-2}-1}\rangle,\ n \geq 4.$$

O subgrupo derivado de G é gerado por $\langle x^{2^{n-2}-2}\rangle$ cujo ordem é igual a

$$\frac{2^{n-1}}{(2^{n-1},2^{n-2}-2)} = \frac{2^{n-1}}{2} = 2^{n-2},\ n > 3.$$

Como o grupo é uma extensão cindida, temos:

$$o'(x) = (2^{n-1},2^{n-2}-2) = \big(2(2^{n-2}),2(2^{n-3}-1)\big) = 2,\ n > 3,$$
$$o(y) = o'(y) = 2.$$

Exemplo 2.1.10. *Um exemplo puramente computacional, feito no software livre GAP* [18]*, para $G = g(a,b;16,2,15,8)$:*

```
gap > f := FreeGroup(2);;
gap > x := f.1;; y := f.2;;
gap > r := [x^16, y^2/x^8, x^y/x^15];;
gap > g := f/r;;
gap > Order(g.1);
16
gap > Order(g.2);
4
gap > dg := DerivedSubgroup(g);;
gap > gab := g/dg;;
gap > AbelianInvariants(gab);
[2, 2]
gap > Order(gab.1);
2
gap > Order(gab.2);
2
```

Aplicando os resultados anteriores neste Exemplo, obtemos:

$$o(b) = \frac{mn}{(m,s)} = \frac{16.2}{(16,8)} = 4,$$
$$o'(a) = (m,r-1) = (16,14) = 2,$$
$$o'(b) = \left(o(b), \frac{ns(r-1)}{(m,s)(r-1,s)}\right) = \left(4, \frac{2.8.14}{(16,8)(8,14)}\right) = (4,14) = 2.$$

Além disso, como $\langle a^{r-1}\rangle \cap \langle a^s\rangle = \langle a^{r-1}\rangle = \langle a^2\rangle \neq 1$, *os invariantes abelianos da abelianização* G/G' *não são exatamente as ordens relativas às classes* aG' *e* bG', *respectivamente.*

Desta forma, finalizamos a seção que caracteriza os grupos metacíclicos finitos $G = g(a, b; m, n, r, s)$ com os cálculos dos objetos dos quais precisaremos para o decorrer desta tese. Segue agora a seção dos grupos metacíclicos infinitos com o mesmo propósito.

2.2 Grupos Metacíclicos Infinitos

O respaldo teorético para essa seção pode ser encontrado em Beuerle & Kappe [3]. Em seu artigo, Beuerle & Kappe classificaram todos os grupos metacíclicos infinitos $G = g(a, b; m, n, r)$ a menos de isomorfismo e calcularam uma cota para a ordem dos elementos de um conjunto de geradores do grupo $[G, G^\varphi]$.

O Lema que segue, demonstrado por Beuerle & Kappe [3] para os grupos metacíclicos cindidos, é equivalente ao **Lema 2.1.3** para grupos metacíclicos finitos quaisquer, uma vez que usa propriedades gerais de grupos metacíclicos sem fazer distinção entre a apresentação ser cindida ou não. Desta forma, omitiremos sua demonstração.

Lema 2.2.1. [[3], Lemma 3.1] *Sejam* m, n *inteiros não negativos,* $r \in \mathcal{U}_m$ *e*

$$G = \langle a, b \mid a^m = 1, b^n = 1, a^b = a^r\rangle, \tag{2.5}$$

um grupo metacíclico cindido. Então, todo elemento $g \in G$ *pode ser escrito como* $g = a^\alpha b^\beta$, *onde* α *e* β *são inteiros únicos módulo* m *e* n, *respectivamente. Ademais, se* $h \in G$ *com* $h = a^\gamma b^\delta$, *com* γ *e* δ *são unicamente determinados, então as seguintes relações são satisfeitas em* G*:*

(i) $gh = b^{\beta+\delta} a^{r^\delta(\gamma+\alpha r^\beta)}$;

(ii) $h^g = b^\delta a^{\alpha r^\beta(r^\delta-1)+\gamma r^{\beta+\delta}}$;

(iii) $g^\sigma = b^{\beta\sigma} a^{\alpha r^\beta E_m(r^\beta,\sigma)}$, *para qualquer* $\sigma \in \mathbb{Z}$.

Mesmo que o **Lema 2.2.1** nos diga que a forma normal de um elemento em um grupo cindido seja da forma $a^\alpha b^\beta$ e apresente elementos da forma $b^\gamma a^\delta$ após simples cálculos no próprio grupo, é mais interessante que os elementos estejam desta última forma para os cálculos futuros. Além disso, é fácil ver que $(a^\alpha)^{b^\beta} = a^{\alpha r^\beta}$ e $(b^\beta)^{a^\alpha} = b^\beta a^{\alpha(1-r^\beta)}$, para α e β inteiros, como feito no **Lema 2.1.3** para grupos metacíclicos finitos.

O próximo resultado nos garante que todo grupo metacíclico infinito é uma extensão cindida:

Teorema 2.2.2. [[3], Theorem 3.2] *Seja G um grupo metacíclico infinito. Então, G é isomorfo ao grupo*

$$g(a, b; m, n, r) = \langle a, b \mid a^m = 1, b^n = 1, a^b = a^r \rangle, \tag{2.6}$$

onde $m, n, r \in \mathbb{Z}^+$, *com* $mn = 0$ *e* $r \in \mathcal{U}_m$. *Mais ainda, se* $r \equiv -1 \pmod{m}$ *então* n *é par e, se* $r \equiv 1 \pmod{m}$ *então* $m = 0$. *Em particular,* $g(a, b; m, n, r) \simeq g(a, b; m', n', r')$ *se, e somente se,* $m = m'$, $n = n'$ *e* $r \equiv s^l \pmod{m}$ *com* $l \in \{-1, 1\}$.

Observe que o grupo $g(a, b; m, n, r)$ apresentado no **Teorema 2.2.2** é metacíclico cindido. Usaremos $G = g(a, b; m, n, r)$ como notação para grupos metacíclicos (cindidos) infinitos gerados por a e b.

O resultado a seguir é uma adaptação do Teorema de Curtis [[13], página 336, §47.10] para grupos metacíclicos infinitos:

Proposição 2.2.3. *Seja G um grupo metacíclico infinito cindido tipo* $g(a, b; m, 0, r)$. *Então,* G' *é cíclico gerado por* a^{r-1} *cuja ordem é* $m/(m, r-1)$.

Demonstração. Seja $H = \langle a \rangle \trianglelefteq G$ e $N = \langle a^{r-1} \rangle \leq H$. Vamos mostrar que $N = G'$.

H é cíclico então qualquer automorfismo de H leva potências de a em potências de a. Segue que N *char* H e $N \trianglelefteq G$ pois $H \trianglelefteq G$ e N *char* H.

Tome $\pi : G \to G/N$ o epimorfismo que associa $a \mapsto aN$ e $b \mapsto bN$ onde

$$\pi(b^{-1})\pi(a)\pi(b) = \pi(b^{-1}ab) = \pi(a^r) = \pi(a^{r-1})\pi(a) = a^{r-1}NaN = aN = \pi(a)$$

implicando que G/N é abeliano. Logo, $G' \subseteq N$. Por outro lado, $N \subseteq [G, G]$ pois

$$a^{r-1} = [a, b] = [b, a]^{-1} = [b, a^{-1}]$$

$$(a^{r-1})^{-1} = [a, b]^{-1} = [b, a] = [b, a^{-1}]^{-1}.$$

Já que a tem ordem m em G e a^{r-1} gera G', temos que $|G'| = m/(m, r-1)$. $\square$

No caso em que G é um grupo do tipo $g(a, b; 0, 0, 1)$, então G' é trivial pois G é abeliano. Se G é um grupo do tipo $g(a, b; 0, 0, -1)$, então G' é infinito.

Análogo ao procedimento feito para os grupos metacíclicos finitos, o seguinte Lema vai de encontro as ordens relativas às classes aG' e bG' para o grupo metacíclico infinito:

Lema 2.2.4. *Seja* $G = g(a, b; m, n, r)$ *um grupo metacíclico infinito. Então*

$$o'(a) = (m, r-1) \qquad e \qquad o'(b) = o(b) = n.$$

Demonstração. A demonstração deste Lema é uma combinação entre a demonstração da **Proposição 2.1.6** e o fato do grupo $G = g(a, b; m, n, s)$ ser sempre uma extensão cindida, para m e n não simultaneamente nulos. □

Para finalizar, segue alguns exemplos de grupos metacíclicos infinitos:

Exemplo 2.2.5. *Na classe dos grupos metacíclicos infinitos $G = g(a, b; m, n, r)$, tomemos $n = 0$. Então, uma apresentação para o grupo G é dada por:*

$$g(a, b; m, 0, r) = \langle a, b \mid a^m = 1, a^b = a^r \rangle$$

com $r \in \mathcal{U}_m$ é um exemplo em que b tem ordem infinita, isomorfo a $C_\infty \times C_m$ ou $C_\infty \ltimes C_m$.

Além disso, no caso em que $G = g(a, b; m, 0, r) \cong C_\infty \ltimes C_m$, temos que $b^{\Phi(m)}$ centraliza a, onde $\Phi(m)$ é a função de Euler em m. Isso porque, pelo **Teorema 1.5.11** *e como $(m, r) = 1$, temos que $a^{b^{\Phi(m)}} = a^{r^{\Phi(m)}} = a$.*

*Agora, pela **Proposição 2.2.3** e pelo **Lema 2.2.4**, temos que $\langle a^{r-1} \rangle$ gera o subgrupo derivado de $g(a, b; m, 0, r)$ cuja ordem é $m/(m, r-1)$ e, $o'(a) = (m, r-1)$ e $o'(b)$ é infinito.*

Exemplo 2.2.6. *Ainda na classe $G = g(a, b; m, n, r)$ de grupos metacíclicos infinitos, consideremos $m = 0$. Por definição, teremos $r \in \{-1, 1\}$, uma vez que, os únicos automorfismos do grupo cíclico infinito são a identidade e a inversão.*

No caso em que o grupo é não abeliano, a apresentação é da forma

$$g(a, b; 0, n, -1) = \langle a, b \mid b^n = 1, a^b = a^{-1} \rangle.$$

Como consequência, b^2 centraliza a pois $(a^b)^b = (a^{-1})^b = a$, resultando em $g(a, b; 0, n, -1) \cong C_n \ltimes C_\infty$.

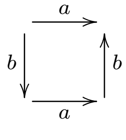
*Novamente, pela **Proposição 2.2.3** e pelo **Lema 2.2.4**, temos que $\langle a^{-2} \rangle$ gera o subgrupo derivado de $G(0, n, -1)$ de ordem infinita, $o'(a)$ tem ordem infinita e $o'(b) = n$.*

Em particular, quando $n = 2$, $g(a, b; 0, 2, -1)$ é o grupo diedral infinito. Neste caso, $o'(b) = 2$.

Exemplo 2.2.7. *Um outro exemplo de grupo metacíclico infinito K é a garrafa de Klein dada pela seguinte apresentação*

$$g(a, b; 0, 0, -1) = \langle a, b \mid a^b = a^{-1} \rangle$$

com $K' = \langle a^{-2} \rangle$ de ordem infinita e, $o'(a)$ e $o'(b)$ também de ordem infinita.



Na teoria de superfícies topológicas, a garrafa de Klein é chamada superfície compacta básica. Existe uma identificação entre K e o seu grupo fundamental.

Neste Capítulo, vimos que o subgrupo derivado de um grupo metacíclico G qualquer é sempre cíclico. Esta propriedade nos garante que o subgrupo normal do grupo $\nu(G)$, $\Upsilon(G) := [G, G^{\varphi}]$, é abeliano. Isto ocorre pois $[G, G^{\varphi}]/\mu(G) \cong G'$ e $\mu(G)$ é central em $\nu(G)$ (com um raciocínio análogo, temos que os grupos $G \wedge G$ e $M(G)$ também são abelianos). Esta informação é bastante necessária para os cálculos subsequentes.

Capítulo 3

Seções do Grupo $\nu(G)$ para Grupos Metacíclicos G

Neste Capítulo, com base no respaldo teorético do **Capítulo** 2, daremos apresentações para o grupo $\nu(G)$ quando G é um grupo metacíclico e, consequentemente, conseguiremos apresentações para os grupos $[G, G^{\varphi}]$, $G \wedge G$ e $M(G)$, vistos como seções abelianas do grupo $\nu(G)$, e para o grupo $\tau(G) = \nu(G)/\Delta(G)$. No caso em que o grupo G é metacíclico infinito, auferimos também o abeliano $\mu(G)$ como seção do grupo $\nu(G)$.

Na primeira seção, baseada nos resultados do **Capítulo** 2 para grupos metacíclicos finitos, $G = g(a, b; m, n, r, s)$, não abelianos $(r > 1)$, daremos uma apresentação para o grupo $\nu(G)$. Consideramos o grupo $G = g(a, b; m, n, r, s)$, não cindido, $r > 1$ com m par para o **Teorema A** e com m ímpar para o **Teorema B**. Como primeiro Corolário do **Teorema A**, foi possível a obtenção de uma apresentação para o grupo $\nu(G)$ quando $G = g(a, b; m, n, m-1, s)$ e $s > 0$. Por conseguinte, finalizamos as apresentações do grupo $\nu(G)$ quando G é metacíclico finito cindido. Dadas as apresentações do grupo $\nu(G)$ para um grupo metacíclico finito G qualquer, obtemos apresentações dos grupos abelianos $[G, G^{\varphi}]$, $G \wedge G$ e $M(G)$ e, por fim, do grupo $\tau(G)$ como Corolários.

Na segunda seção, uma mesma análise será feita para os grupos metacíclicos infinitos $G = g(a, b; m, n, r)$, classificados por Beuerle & Kappe [3]. Nesse artigo, os autores calcularam as ordens dos elementos de um conjunto gerador para o grupo $G \otimes G \cong [G, G^{\varphi}]$, com G não abeliano. Para isso, construíram uma biderivação e puderam obter os grupos $\mu(G)$, $M(G)$ e $G \wedge G$ como consequência da identificação do grupo $G \otimes G$. Neste trabalho, fazemos o uso da apresentação do grupo $\nu(G)$ para confirmarmos tal resultado, além de considerarmos a possibilidade do grupo G ser abeliano. Desta forma, a apresentação do grupo $\nu(G)$ obtida no **Teorema C** nos permite exibir as supracitadas seções abelianas do grupo $\nu(G)$. Ademais, daremos uma apresentação para a seção $\tau(G) = \nu(G)/\Delta(G)$.

Em vista do isomorfismo $G \otimes G \cong [G, G^{\varphi}]$, garantido pela **Proposição 1.7.5** (i), identificaremos os elementos da forma $g \otimes h$ por $[g, h^{\varphi}]$, para quaisquer $g, h \in G$. A partir dessa identificação, o Lema a seguir estabelece as conjugações dos geradores de $G \otimes G$ pelos (potências dos) geradores de G, sem distinções nem especificações a respeito da quadra (m, n, r, s):

Lema 3.0.1. *As seguintes identidades são satisfeitas em $\nu(G)$, para quaisquer $\alpha, \beta \in \mathbb{N}$:*
(i) $[a, b^{\varphi}]^{a^{\alpha}} = [a, b^{\varphi}][a, a^{\varphi}]^{\alpha(r-1)}$,
(ii) $[a^{\alpha}, b^{\varphi}] = [a, b^{\varphi}]^{\alpha}[a, a^{\varphi}]^{\binom{\alpha}{2}(r-1)}$,
(iii) $[a, b^{\varphi}]^{b^{\beta}} = [a, b^{\varphi}]^{r^{\beta}}[a, a^{\varphi}]^{\binom{r^{\beta}}{2}(r-1)}$,
(iv) $[a, (b^{\beta})^{\varphi}] = [a, b^{\varphi}]^{E_m(r,\beta)}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{\beta-1}\binom{r^i}{2}}$,
(v) $[a^{\alpha}, b^{\varphi}]^{b^{\beta}} = [a, b^{\varphi}]^{\alpha r^{\beta}}[a, a^{\varphi}]^{(r-1)\binom{\alpha r^{\beta}}{2}}$,
(vi) $[a^{\alpha}, (b^{\beta})^{\varphi}] = [a, b^{\varphi}]^{\alpha E_m(r,\beta)}[a, a^{\varphi}]^{(r-1)\sum_{i=0}^{\beta-1}\binom{\alpha r^i}{2}}$,
(vii) $[b, a^{\varphi}]^{a^{\alpha}} = [b, a^{\varphi}][a, a^{\varphi}]^{\alpha(1-r)}$,
$(viii)$ $[b, (a^{\varphi})^{\alpha}] = [b, a^{\varphi}]^{\alpha}[a, a^{\varphi}]^{\binom{\alpha}{2}(1-r)}$,
(ix) $[b, a^{\varphi}]^{b^{\beta}} = [b, a^{\varphi}]^{r^{\beta}}[a, a^{\varphi}]^{\binom{r^{\beta}}{2}(1-r)}$,
(x) $[b^{\beta}, a^{\varphi}] = [b, a^{\varphi}]^{E_m(r,\beta)}[a, a^{\varphi}]^{(1-r)\sum_{i=1}^{\beta-1}\binom{r^i}{2}}$,
(xi) $[b, (a^{\alpha})^{\varphi}]^{b^{\beta}} = [b, a^{\varphi}]^{\alpha r^{\beta}}[a, a^{\varphi}]^{(1-r)\binom{\alpha r^{\beta}}{2}}$,
(xii) $[b^{\beta}, (a^{\alpha})^{\varphi}] = [b, a^{\varphi}]^{\alpha E_m(r,\beta)}[a, a^{\varphi}]^{(1-r)\sum_{i=0}^{\beta-1}\binom{\alpha r^i}{2}}$.

Demonstração. Esta demonstração será feita por indução sobre $\alpha, \beta \in \mathbb{N}$:

$(i) - (ii)$ A demonstração será simultânea de (i) e (ii).

Pela **Proposição 1.1.1** (ii), temos $[a^2, b^{\varphi}] = [a, b^{\varphi}]^a[a, b^{\varphi}]$. Agora, pelo **Lema 1.7.6** (iv) temos que

$$[a^2, b^{\varphi}] = [a, b^{\varphi}][a, b, a^{\varphi}][a, b^{\varphi}] = [a, b^{\varphi}]^2[a, a^{\varphi}]^{(r-1)}$$

e portanto, $[a, b^{\varphi}]^a = [a, b^{\varphi}][a, a^{\varphi}]^{(r-1)}$.

Queremos mostrar que as identidades ainda valem para $\alpha + 1$.

Pela **Proposição 1.1.1** (ii) e pelo **Lema 1.7.6** (iv), seguem as identidades abaixo:

$$\begin{aligned}
[a^{\alpha+1}, b^{\varphi}] &= [aa^{\alpha}, b^{\varphi}] \\
&= [a, b^{\varphi}]^{a^{\alpha}}[a^{\alpha}, b^{\varphi}] \\
&= [a, b^{\varphi}]^{a^{\alpha}}[a, b^{\varphi}]^{\alpha}[a, a^{\varphi}]^{\binom{\alpha}{2}(r-1)}.
\end{aligned}$$

$$\begin{aligned}
[a^{\alpha+1}, b^{\varphi}] &= [aa^{\alpha}, b^{\varphi}] \\
&= [a, b^{\varphi}][a, b, (a^{\varphi})^{\alpha}][a^{\alpha}, b^{\varphi}] \\
&= [a, b^{\varphi}]^{\alpha+1}[a, a^{\varphi}]^{\binom{\alpha}{2}(r-1)+\alpha(r-1)}.
\end{aligned}$$

Logo, $[a, b^{\varphi}]^{a^{\alpha}} = [a, b^{\varphi}][a, a^{\varphi}]^{\alpha(r-1)}$ e, como

$$\alpha(r-1) + \binom{\alpha}{2}(r-1) = (r-1)\frac{\alpha}{2}(\alpha+1) = (r-1)\binom{\alpha+1}{2}$$

temos que

$$[a^{\alpha+1}, b^{\varphi}] = [a, b^{\varphi}]^{\alpha+1}[a, a^{\varphi}]^{(r-1)\binom{\alpha+1}{2}}.$$

(iii) Observe que a identidade vale para $\beta = 1$ pois

$$[a, b^{\varphi}]^{b} = [a^{r}, b^{\varphi}] =_{(ii)} [a, b^{\varphi}]^{r}[a, a^{\varphi}]^{\binom{r}{2}(r-1)}.$$

Suponha que a identidade seja satisfeita pra todo $\beta < l$. Queremos mostrar que vale para l:

$$\begin{array}{rcl}
[a, b^{\varphi}]^{b^{l}} & = & ([a, b^{\varphi}]^{b^{l-1}})^{b} \\
 & =_{hip.} & ([a, b^{\varphi}]^{r^{l-1}}[a, a^{\varphi}]^{\binom{r^{l-1}}{2}(r-1)})^{b} \\
 & = & ([a, b^{\varphi}]^{b})^{r^{l-1}}([a, a^{\varphi}]^{b})^{\binom{r^{l-1}}{2}(r-1)} \\
 & = & [a^{r}, b^{\varphi}]^{r^{l-1}}[a^{r}, (a^{r})^{\varphi}]^{\binom{r^{l-1}}{2}(r-1)} \\
 & =_{(ii)} & [a, b^{\varphi}]^{r^{l}}[a, a^{\varphi}]^{\binom{r}{2}(r-1)r^{l-1} + r^{2}(r-1)\binom{r^{l-1}}{2}}.
\end{array}$$

Como

$$\begin{array}{rcl}
\binom{r}{2}r^{l-1} + r^{2}\binom{r^{l-1}}{2} & = & \dfrac{r^{l-1}r(r-1)}{2} + \dfrac{r^{2}r^{l-1}(r^{l-1}-1)}{2} \\
 & = & \dfrac{r^{l}(r-1) + r^{l}(r^{l}-r)}{2} \\
 & = & \dfrac{r^{l}(r^{l}-1)}{2},
\end{array}$$

segue o resultado.

(iv) Para $\beta = 1$, a identidade é satisfeita pois $E_m(r, 1) = 1$, pela **Definição 1.5.1**.

Suponha que a identidade seja satisfeita para $\beta < l$. Queremos mostrar que ainda vale para l.

Pela **Proposição 1.1.1** (ii), temos:

$$\begin{array}{rcl}
[a, (b^{l})^{\varphi}] & = & [a, (b^{l-1})^{\varphi}][a, b^{\varphi}]^{b^{l-1}} \\
 & =_{hip.} & [a, b^{\varphi}]^{E_m(r,l-1)}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{l-2}\binom{r^{i}}{2}}[a, b^{\varphi}]^{b^{l-1}} \\
 & =_{(iii)} & [a, b^{\varphi}]^{E_m(r,l-1)}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{l-2}\binom{r^{i}}{2}}[a, b^{\varphi}]^{r^{l-1}}[a, a^{\varphi}]^{\binom{r^{l-1}}{2}(r-1)} \\
 & = & [a, b^{\varphi}]^{E_m(r,l)}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{l-1}\binom{r^{i}}{2}},
\end{array}$$

como queríamos demonstrar.

(v) Observe que este item é uma variação do item (ii) pois

$$[a^\alpha, b^\varphi]^{b^\beta} = [a^{\alpha r^\beta}, b^\varphi] =_{(ii)} [a, b^\varphi]^{\alpha r^\beta}[a, a^\varphi]^{(r-1)\binom{\alpha r^\beta}{2}}.$$

(vi) Este item é uma combinação dos itens (iii) e (v) e da **Proposição 1.1.1** (ii), pois

$$\begin{aligned}
[a^\alpha, (b^\varphi)^\beta] &= ([a^\alpha, (b^{\beta-1})^\varphi][a^\alpha, b^\varphi]^{b^{\beta-1}} \\
&= ([a^\alpha, (b^{\beta-2})^\varphi][a^\alpha, b^\varphi]^{b^{\beta-2}}[a^\alpha, b^\varphi]^{b^{\beta-1}} \\
&\vdots \\
&= [a^\alpha, b^\varphi][a^\alpha, b^\varphi]^{b+b^2+\ldots+b^{\beta-1}} \\
&= [a, b^\varphi]^{\alpha(1+r+\ldots+r^{\beta-1})}[a, a^\varphi]^{(r-1)\binom{\alpha}{2}+(r-1)\binom{\alpha r}{2}+\ldots+(r-1)\binom{\alpha r^{\beta-1}}{2}}. \\
&= [a, b^\varphi]^{\alpha E_m(r,\beta)}[a, a^\varphi]^{(r-1)\sum_{i=0}^{\beta-1}\binom{\alpha r^i}{2}}.
\end{aligned}$$

(vii) Se $\alpha = 1$ então $[b, a^\varphi]^a = [b, a^\varphi][b, a, a^\varphi] = [b, a^\varphi][a^{1-r}, a^\varphi] = [b, a^\varphi][a, a^\varphi]^{(1-r)}$.

Suponha que a identidade seja satisfeita para $\alpha < l$. Queremos mostrar que vale para todo l:

$$\begin{aligned}
[b, a^\varphi]^{a^l} &= ([b, a^\varphi]^{a^{l-1}})^a \\
&=_{hip.} \left([b, a^\varphi][a, a^\varphi]^{(l-1)(1-r)}\right)^a \\
&= ([b, a^\varphi]^a)[a, a^\varphi]^{(l-1)(1-r)} \\
&= [b, a^\varphi][a, a^\varphi]^{(1-r)(l-1+1)}
\end{aligned}$$

$(viii)$ Para $\alpha = 1$, não há o que ser feito.

Suponha que a identidade seja satisfeita para $\alpha < l$. Queremos mostrar que vale para todo l:

$$\begin{aligned}
[b, (a^\varphi)^l] &= [b, (a^{l-1})^\varphi][b, a^\varphi]^{a^{l-1}} \\
&=_{hip.} [b, a^\varphi]^{(l-1)}[a, a^\varphi]^{\binom{l-1}{2}(1-r)}[b, a^\varphi]^{a^{l-1}} \\
&=_{(vii)} [b, a^\varphi]^{(l-1)}[a, a^\varphi]^{\binom{l-1}{2}(1-r)}[b, a^\varphi][a, a^\varphi]^{(1-r)(l-1)} \\
&= [b, a^\varphi]^l[a, a^\varphi]^{(1-r)\binom{l-1}{2}+(1-r)(l-1)}
\end{aligned}$$

Como

$$(l-1) + \binom{l-1}{2} = \frac{2(l-1) + (l-1)(l-2)}{2} = \frac{(l-1)(2+l-2)}{2},$$

segue o resultado.

(ix) Basta observar que

$$[b, a^\varphi]^{b^\beta} = [b, (a^\varphi)^{r^\beta}]$$

que o resultado segue do item $(viii)$.

A demonstração dos itens $(x) - (xii)$ é uma combinação dos itens anteriores. $\square$

Como dissemos anteriormente, nosso enfoque é dar uma apresentação para o grupo $\nu(G)$, para grupos metacíclicos G gerados por a e b quaisquer e, então, uma apresentação para os grupos $[G, G^{\varphi}]$, $G \wedge G$, $M(G)$ e $\tau(G)$. Para tanto, estabeleceremos uma cota para as ordens dos elementos do conjunto gerador $\{[a, b^{\varphi}], [a, a^{\varphi}], [b, b^{\varphi}], [a, b^{\varphi}][b, a^{\varphi}]\}$ do quadrado tensorial não abeliano do grupo G, juntamente com algumas relações entre os elementos supracitados.

3.1 Grupos Metacíclicos Finitos

O primeiro Lema desta seção relaciona uma potência do elemento $[b, b^{\varphi}]$ a uma potência dos elementos $[a, b^{\varphi}]$, $[b, a^{\varphi}]$ e $[a, a^{\varphi}]$, importante para o cálculo das ordens dos elementos do conjunto gerador do quadrado tensorial não abeliano do grupo $G = g(a, b; m, n, r, s)$, independente da quadra (m, n, r, s), salvo menção do contrário.

Lema 3.1.1. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito. Então*

$$\begin{cases} [b, b^{\varphi}]^n = [a, b^{\varphi}]^s = [b, a^{\varphi}]^s, & \text{se } 2 \nmid s \text{ ou se } 4 \mid s \\ [b, b^{\varphi}]^n = [a, b^{\varphi}]^s [a, a^{\varphi}]^{(r-1)} = [b, a^{\varphi}]^s [a, a^{\varphi}]^{(1-r)}, & \text{se } 2 \parallel s. \end{cases}$$

Demonstração. De fato, pelo **Lema 3.0.1**, itens (ii) e $(viii)$, temos

$$\begin{aligned} [b^n, b^{\varphi}] = [a^s, b^{\varphi}] = [a, b^{\varphi}]^s [a, a^{\varphi}]^{\binom{s}{2}(r-1)} \\ [b, (b^n)^{\varphi}] = [b, (a^s)^{\varphi}] = [b, a^{\varphi}]^s [a, a^{\varphi}]^{\binom{s}{2}(1-r)}. \end{aligned} \tag{3.1}$$

Se s é ímpar, então $[a, a^{\varphi}]^{\binom{s}{2}(r-1)} = [a, a^{\varphi}]^{\frac{(s-1)}{2}s(r-1)} = 1$, pois $m \mid s(r-1)$.

Se $4 \mid s$, então $[a, a^{\varphi}]^{\binom{s}{2}(r-1)} = [a, a^{\varphi}]^{\frac{s}{2}(s-1)(r-1)} = 1$, já que $\dfrac{s}{2}(s-1)$ é um número par e, pelo **Lema 1.7.10**, temos que $o([a, a^{\varphi}]) \mid (m, 2(r-1))$.

Para finalizar, se $2 \parallel s$, então existe um número ímpar s' tal que $s = 2s'$. Logo,

$$\binom{s}{2} = \frac{2s'(2s'-1)}{2} = s'(2s'-1)$$

é um número ímpar. Assim, da equação (3.1), temos que

$$[a, a^{\varphi}]^{\binom{s}{2}(r-1)} = [a, a^{\varphi}]^{s'(2s'-1)(r-1)} = [a, a^{\varphi}]^{[s'(2s'-1)-1](r-1)} [a, a^{\varphi}]^{(r-1)} = [a, a^{\varphi}]^{(r-1)},$$

pois $s'(2s'-1)-1$ é um número par e $o([a, a^{\varphi}]) \mid (m, 2(r-1))$. A outra identidade segue de maneira análoga. $\square$

Observe que não há distinção ou particularização para $r \in \mathcal{U}_m$ tampouco para m, no **Lema 3.1.1**. Desta forma, tendo o controle dos objetos $o'(a)$, $o'(b)$ e $o(b)$, asseverado pela

Proposição 2.1.6 e pelo **Corolário 2.1.5**, podemos começar a investigar cotas para as ordens dos elementos do conjunto gerador do quadrado tensorial não abeliano, $[G, G^{\varphi}]$, onde $G = g(a, b; m, n, r, s)$ é um grupo metacíclico finito, não abeliano. Com este tipo de análise, lograremos também relações entre potências dos mesmos, o que será fundamental para a identificação do grupo $\nu(G)$.

Antes de darmos prosseguimento, lembremo-nos do número $E_m(r, x)$ definido pela função $E_m : \mathcal{U}_m \times \mathbb{Z} \to \mathbb{Z}$, da **Definição 1.5.1**, que associa

$$E_m(r,x) = \begin{cases} x, & se\ r \equiv 1\ (mod\ m)\ ou\ x = 0 \\ 1 + r + \cdots + r^{x-1}, & se\ r \not\equiv 1\ (mod\ m)\ e\ x > 0 \\ -r^x E_m(r, -x), & se\ r \not\equiv 1\ (mod\ m)\ e\ x < 0 \end{cases}$$

Definiremos um número natural bastante importante para o cálculo de cotas para as ordens dos elementos do conjunto gerador do grupo $[G, G^{\varphi}]$.

Definição 3.1.2. *Para a quadra (m, n, r, s) definidora do grupo metacíclico finito $G = g(a, b; m, n, r, s)$, seja*

$$k := \left(\frac{m}{(m,s)}, 2\frac{[s, r-1]}{(m,s)}, n\frac{[s, r-1]^2}{(m,s)^2}, r-1, E_m(r, o(b)) \right).$$

Pela **Definição 3.1.2** temos que, a escolha de m ser ímpar implica em k também ímpar, independente da paridade de $r \in \mathcal{U}_m$. Mais ainda, quando $r = m - 1$, o número

$$k = \left(\frac{m}{(m,s)}, 2\frac{[s,2]}{(m,s)}, n\frac{[s,2]^2}{(m,s)^2}, 2, 0 \right)$$

pode admitir os valores $k = 1$ ou $k = 2$.

Para as Proposições subsequentes, separamos as análises de cotas para as ordens dos elementos do conjunto $\{[a, b^{\varphi}], [a, a^{\varphi}], [b, b^{\varphi}], [a, b^{\varphi}][b, a^{\varphi}]\}$ nos casos em que o grupo $G = g(a, b; m, n, r, s)$ é não cindido, com m par e com m ímpar, para $r > 1$. Como decorrência dessas Proposições, obtemos o caso em que o grupo $G = g(a, b; m, n, r, 0)$ é cindido.

Proposição 3.1.3. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito, não abeliano com m par. Então, são cotas para as ordens dos elementos de um conjunto gerador do grupo $[G, G^{\varphi}]$:*

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, 2(r-1))$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* nk;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo*

$$\begin{cases} \begin{cases} (m, 2sk), & se\ 2 \nmid k \\ (m, sk), & se\ 2 \mid k \end{cases} & e\quad 2 \parallel s, \\ (m, sk), & se\ 2 \nmid s\ ou\ se\ 4 \mid s; \end{cases}$$

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo*

$$\begin{cases} (o'(a), o'(b), E_m(r, o'(b)), sk), & se\ 2 \nmid k, \\ (o'(a), o'(b), E_m(r, o'(b)), sk/2), & se\ 2 \mid k. \end{cases}$$

Demonstração. Primeiro observamos que, sendo m par, r deve ser ímpar.

i) Pelo **Lema 1.7.10** (*vi*), temos que $o([a, a^{\varphi}]) \mid (o'(a)^2, 2o'(a))$, pois $o'(a)$ é finito. Mais ainda, $o'(a) = (m, r-1)$ é um número inteiro positivo par, uma vez que $(m, r) = 1$ e m é par. Logo, $[a, a^{\varphi}]$ tem ordem dividindo $(m, 2(r-1))$.

Consideraremos agora todas as possibilidades decorrentes do **Lema 1.7.6** e do **Lema 1.7.10** afim de tentarmos diminuir essa cota:

$$1 = [a^m, a^{\varphi}] = [a, a^{\varphi}]^m, \tag{3.2}$$

$$1 = [a^{r-1}, (a^{\varphi})^{r-1}] = [a, a^{\varphi}]^{(r-1)^2}, \tag{3.3}$$

$$1 = [a^{r-1}, a^{\varphi}][a, (a^{\varphi})^{(r-1)}] = [a, a^{\varphi}]^{2(r-1)}, \tag{3.4}$$

$$1 = [a^s, (a^{\varphi})^{r-1}] = [a, a^{\varphi}]^{s(r-1)}, \tag{3.5}$$

$$1 = [a^t, a^{\varphi}] = [a, a^{\varphi}]^t, \tag{3.6}$$

onde $t = [m, r-1]$.

Das identidades (3.2), (3.3), (3.4), (3.5) e (3.6), temos que $[a, a^{\varphi}]$ tem ordem dividindo $\big(m, (r-1)^2, 2(r-1), [m, r-1]\big) = (m, 2(r-1))$, pois $m \mid [m, r-1]$ e $(m, 2(r-1)) \mid (m, 2(r-1), (r-1)^2)$, uma vez que m é par.

Mais ainda, do **Lema 3.1.1**, temos que $[a, a^{\varphi}]^{(r-1)\binom{s}{2}} = 1$, se $2 \nmid s$ ou se $4 \mid s$, finalizando as possibilidades de cota para a ordem do elemento $[a, a^{\varphi}]$.

ii) Sabemos que $o([b, b^{\varphi}]) \mid (o'(b)^2, 2o'(b))$, pelo **Lema 1.7.10** (*vi*), já que $o'(b)$ é finito. Mais ainda

$$1 = [b^{o(b)}, b^{\varphi}] = [b, (b^{o(b)})^{\varphi}] = [b, b^{\varphi}]^{o(b)},$$

implicando em $o([b, b^{\varphi}]) \mid (o(b), o'(b)^2, 2o'(b))$.

Logo, $[b, b^{\varphi}]$ tem ordem dividindo

$$\left(\frac{mn}{(m,s)}, \frac{m^2n^2}{(m,s)^2}, 2\frac{mn}{(m,s)}, 2\frac{n[s, r-1]}{(m,s)}, \frac{n^2[s, r-1]^2}{(m,s)^2}\right),$$

ou seja,

$$n\left(\frac{m}{(m,s)}, 2\frac{[s, r-1]}{(m,s)}, n\frac{[s, r-1]^2}{(m,s)^2}\right). \tag{3.7}$$

Pelo **Lema 3.1.1**, devemos acrescentar $n(r-1)$ e $nE_m(r, o(b))$, pois

$$1 = [a, b^{\varphi}]^{s(r-1)} = [a, b^{\varphi}]^{sE_m(r, o(b))} = [b, b^{\varphi}]^{n(r-1)} = [b, b^{\varphi}]^{nE_m(r, o(b))},$$

independente da paridade de s.

Logo, $[b, b^{\varphi}]$ tem ordem dividindo

$$n\left(\frac{m}{(m,s)}, \frac{2[s,r-1]}{(m,s)}, \frac{n[s,r-1]^2}{(m,s)^2}, r-1, E_m(r,o(b))\right) = nk. \tag{3.8}$$

$iii) - iv)$ Faremos a demonstração dos itens $iii)$ e $iv)$ simultamenamente. Para a ordem de $[a, b^{\varphi}]$, segue do **Lema 3.0.1**:

$$\begin{aligned}
1 &= [a^m, b^{\varphi}] = [a, b^{\varphi}]^m [a, a^{\varphi}]^{\binom{m}{2}(r-1)}, && (3.9)\\
1 &= [a^{(r-1)}, (b^n)^{\varphi}] = [a^{(r-1)}, (a^s)^{\varphi}] = [a, a^{\varphi}]^{s(r-1)}, \\
1 &= [a, (b^{o(b)})^{\varphi}] = [a, b^{\varphi}]^{E_m(r,o(b))} [a, a^{\varphi}]^{(r-1)\sum_{i=1}^{o(b)-1}\binom{r^i}{2}}. && (3.10)
\end{aligned}$$

Uma vez que a identidade (3.9) nos garante que $o([a, b^{\varphi}]) \mid m$, iremos analisar a identidade (3.10):

Observe que, módulo $(m, 2(r-1))$,

$$\begin{aligned}
(r-1)\sum_{i=1}^{o(b)-1}\binom{r^i}{2} &= (r-1)\sum_{i=1}^{o(b)-1}\frac{r^i(r^i-1)}{2} \\
&= \frac{(r-1)}{2}\sum_{i=0}^{o(b)-1} r^{2i} - r^i \\
&= \frac{(r-1)}{2}\sum_{i=1}^{o(b)-1} r^{2i} - \frac{(r-1)}{2}\sum_{i=1}^{o(b)-1} r^i \\
&\equiv \frac{(r-1)}{2}\sum_{i=1}^{o(b)-1} 1 - \frac{(r-1)}{2}\sum_{i=1}^{o(b)-1}(1+(1-r)i), && \textbf{Lema 1.5.3} \\
&\equiv \frac{(r-1)}{2}\sum_{i=1}^{o(b)-1}(r-1)i \\
&\equiv \frac{(r-1)^2}{2}\left[\frac{(o(b)-1)o(b)}{2}\right] \\
&\equiv (r-1)\frac{(r-1)}{2}\binom{o(b)}{2}.
\end{aligned}$$

Voltando na identidade (3.10), temos então que:

$$[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{o(b)-1}\binom{r^i}{2}} = [a, a^{\varphi}]^{(r-1)\frac{(r-1)}{2}\binom{o(b)}{2}}$$

e, portanto,

$$[a, b^{\varphi}]^{E_m(r,o(b))} = [a, a^{\varphi}]^{-(r-1)\frac{(r-1)}{2}\binom{o(b)}{2}}.$$

Analogamente, obtemos

$$[b, a^{\varphi}]^{E_m(r,o(b))} = [a, a^{\varphi}]^{(r-1)\frac{(r-1)}{2}\binom{o(b)}{2}}.$$

Das identidades

$$[a, a^{\varphi}]^s = [a, b^{\varphi}]^{E_m(r,n)}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{n-1}\binom{r^i}{2}} \quad \text{e}$$
$$[a, a^{\varphi}]^s = [b, a^{\varphi}]^{E_m(r,n)}[a, a^{\varphi}]^{(1-r)\sum_{i=1}^{n-1}\binom{r^i}{2}},$$

e por uma análise semelhante a do expoente $(r-1)\displaystyle\sum_{i=1}^{o(b)-1}\binom{r^i}{2}$ de $[a, a^{\varphi}]$, obtemos as seguintes relações

$$[a, a^{\varphi}]^{s-\frac{(r-1)^2}{2}\binom{n}{2}} = [a, b^{\varphi}]^{E_m(r,n)},$$
$$[a, a^{\varphi}]^{s+\frac{(r-1)^2}{2}\binom{n}{2}} = [b, a^{\varphi}]^{E_m(r,n)}.$$

Em contrapartida, segundo o **Lema 1.7.10** (v), como $o'(a)$ e $o'(b)$ são finitos, temos a ordem de $[a, b^{\varphi}][b, a^{\varphi}]$ dividindo $(o'(a), o'(b))$.

Mais ainda, baseado no **Lema 1.7.10** (iii) e o respaldo do **Lema 3.0.1**, temos:

$$\begin{aligned} 1 &= [a, (b^{o'(b)})^{\varphi}][b^{o'(b)}, a^{\varphi}] \\ &= [a, b^{\varphi}]^{E_m(r,o'(b))}[a, a^{\varphi}]^{(r-1)\sum_{i=0}^{o'(b)-1}\binom{r^i}{2}} \\ &\quad [b, a^{\varphi}]^{E_m(r,o'(b))}[a, a^{\varphi}]^{(1-r)\sum_{i=0}^{o'(b)-1}\binom{r^i}{2}} \\ &= ([a, b^{\varphi}][b, a^{\varphi}])^{E_m(r,o'(b))} \end{aligned} \tag{3.11}$$

Não precisamos analisar quando $1 = [a, (b^{o(b)})^{\varphi}][b^{o(b)}, a^{\varphi}]$ pois como $o(b) \mid o'(b)$, temos que $E_m(r, o(b)) \mid E_m(r, o'(b))$. De fato, considere $r^{o'(b)} = y$ e $o(b) = \theta o'(b)$. Então

$$E_m(r^{o'(b)}, \theta) = \frac{y^{\theta}-1}{y-1} = \frac{r^{\theta o'(b)}-1}{r^{o'(b)}-1} = \frac{r^{o(b)}-1}{r^{o'(b)}-1} = \frac{\dfrac{r^{o(b)}-1}{r-1}}{\dfrac{r^{o'(b)}-1}{r-1}} = \frac{E_m(r, o(b))}{E_m(r, o'(b))}, \tag{3.12}$$

como queríamos demonstrar, já que $E_m(r^{o'(b)}, \theta) \in \mathbb{Z}_+^{\star}$. Ou ainda, porque $n \mid o'(b)$.

Para finalizar a demonstração destes itens, vamos analisar a paridade de k, uma vez que $o([a, b^{\varphi}][b, a^{\varphi}]) \mid (o'(a), o'(b), E_m(r, o'(b)))$, independente da paridade de m.

– Suponha que $2 \nmid s$ ou $4 \mid s$. Então, $[a, b^{\varphi}]^s = [b, a^{\varphi}]^s = [b, b^{\varphi}]^n$, pelo **Lema 3.1.1**.

Como $[b, b^{\varphi}]^{nk} = 1$, pelo item anterior, obtemos $[a, b^{\varphi}]^{sk} = [b, a^{\varphi}]^{sk} = 1$.

Para k um número ímpar, temos que

$$([a, b^{\varphi}][b, a^{\varphi}])^{sk} = [a, b^{\varphi}]^{sk}[b, a^{\varphi}]^{sk} = 1.$$

No caso em que k é par, obtemos

$$([a, b^{\varphi}][b, a^{\varphi}])^{sk/2} = [a, b^{\varphi}]^{sk/2}[b, a^{\varphi}]^{sk/2} = [a, b^{\varphi}]^{sk} = 1.$$

$-$ Suponha que $2 \parallel s$. Então, pelo **Lema 3.1.1**, as seguinte identidade é satisfeita

$$[a, b^{\varphi}]^{s}[a, a^{\varphi}]^{r-1} = [b, a^{\varphi}]^{s}[a, a^{\varphi}]^{-(r-1)} = [b, b^{\varphi}]^{n}.$$

Uma vez que $[b, b^{\varphi}]^{nk} = 1$, obtemos

$$[a, b^{\varphi}]^{sk}[a, a^{\varphi}]^{k(r-1)} = [b, a^{\varphi}]^{sk}[a, a^{\varphi}]^{-k(r-1)} = 1.$$

Se k é ímpar, temos que

$$\begin{aligned} 1 = [a, b^{\varphi}]^{sk}[a, a^{\varphi}]^{k(r-1)} &= [a, b^{\varphi}]^{sk}[a, a^{\varphi}]^{r-1} \quad \text{e} \\ 1 = [b, a^{\varphi}]^{sk}[a, a^{\varphi}]^{-k(r-1)} &= [b, a^{\varphi}]^{sk}[a, a^{\varphi}]^{-(r-1)}. \end{aligned}$$

Logo,

$$([a, b^{\varphi}][b, a^{\varphi}])^{sk} = [a, b^{\varphi}]^{sk}[b, a^{\varphi}]^{sk} = [a, a^{\varphi}]^{-(r-1)+(r-1)} = 1.$$

Para k par, segue que

$$([a, b^{\varphi}][b, a^{\varphi}])^{sk/2} = [a, b^{\varphi}]^{sk/2}[b, a^{\varphi}]^{sk/2} = [a, b^{\varphi}]^{sk} = 1,$$

já que $[a, a^{\varphi}]^{2(r-1)} = 1$.

Em resumo, $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo

$$\begin{cases} (o'(a), o'(b), E_m(r, o'(b)), sk)\,, & \text{se } 2 \nmid k, \\ (o'(a), o'(b), E_m(r, o'(b)), sk/2)\,, & \text{se } 2 \mid k, \end{cases}$$

e $[a, b^{\varphi}]$ tem ordem dividindo

$$\begin{cases} \begin{cases} (m, 2sk)\,, & \text{se } 2 \nmid k \\ (m, sk)\,, & \text{se } 2 \mid k \end{cases} & \text{e} \;\; 2 \parallel s, \\ \;(m, sk)\,, \;\; \text{se } 2 \nmid s \text{ ou se } 4 \mid s, & \end{cases}$$

finalizando esta demonstração. $\square$

Em decorrência da demonstração da **Proposição 3.1.3**, temos as seguintes relações entre elementos geradores do grupo $[G, G^{\varphi}]$:

$$\begin{cases} [a, b^{\varphi}]^{E_m(r, o(b))} = [a, a^{\varphi}]^{-\frac{(r-1)^2}{2}\binom{o(b)}{2}}, \\ [b, a^{\varphi}]^{E_m(r, o(b))} = [a, a^{\varphi}]^{\frac{(r-1)^2}{2}\binom{o(b)}{2}}, \\ [a, b^{\varphi}]^{E_m(r, n)} = [a, a^{\varphi}]^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, \\ [b, a^{\varphi}]^{E_m(r, n)} = [a, a^{\varphi}]^{s+\frac{(r-1)^2}{2}\binom{n}{2}}. \end{cases}$$

O resultado a seguir é bastante importante para o estudo do número k enunciado na **Definição 3.1.2**, para $r = m - 1$ em $G = g(a, b; m, n, r, s)$ e $s > 0$.

Lema 3.1.4. *Seja $G = g(a, b; m, n, m-1, s)$ um grupo metacíclico finito com $s > 0$. Então, $E_m(m-1, o(b)) = 0$.*

Demonstração. Pela **Definição 2.1.5**, temos que $o(b) = mn/(m, s)$. Como m e n são números pares, pela **Observação 2.1.2.1** *2*-, concluímos que $o(b)$ é par. Logo,

$$\begin{aligned} E_m(m-1, o(b)) &= 1 + (m-1)^1 + (m-1)^2 + (m-1)^3 + \ldots + (m-1)^{o(b)-1} \\ &= \sum_{i=1}^{o(b)} (m-1)^{i-1} \\ &\equiv \sum_{i=1}^{o(b)} (-1)^{i-1} \ (mod\ m) \\ &\equiv 0 \ (mod\ m), \end{aligned}$$

e fica assim demonstrado. □

Para dar prosseguimento a nossa análise de uma cota para as ordens dos elementos geradores do grupo $[G, G^{\varphi}]$, segue agora uma análise análoga a **Proposição 3.1.5** para grupos metacíclicos finitos com m ímpar, $r > 1$ e $s > 0$:

Proposição 3.1.5. *Seja $G = g(a, b; m, n, r, s)$ um grupo metacíclico finito, não abeliano com m ímpar. Então, são cotas para as ordens dos elementos de um conjunto gerador do grupo $[G, G^{\varphi}]$:*

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, r-1)$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* nk;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* $(m, E_m(r, o(b)), sk)$;

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(o'(a), o'(b), E_m(r, o'(b)), sk)$.

Demonstração. *i)* Pelo **Lema 1.7.10** (*vi*), temos que $o([a, a^{\varphi}]) \mid (o'(a)^2, 2o'(a))$, pois $o'(a)$ é finito. Mais ainda, como m é ímpar, temos que $o'(a) = (m, r-1)$ é um número ímpar, independente da paridade de r. Logo, $o([a, a^{\varphi}]) \mid (o'(a)^2, 2o'(a)) = o'(a) = (m, r-1)$.

Das identidades (3.2), (3.3), (3.4), (3.5) e (3.6) da **Proposição 3.1.3**, temos que $[a, a^{\varphi}]$ tem ordem dividindo $\big(m, (r-1)^2, 2(r-1), [m, r-1]\big) = (m, r-1)$, pois $m \mid [m, r-1]$ e $(m, r-1) \mid (m, 2(r-1), (r-1)^2)$, independente da paridade de r, uma vez que m é ímpar.

O fato de $[a, a^{\varphi}]^{(r-1)\binom{s}{2}} = 1$, se $2 \nmid s$ ou se $4 \mid s$, garantido pelo **Lema 3.1.1** não influencia na ordem de $[a, a^{\varphi}]$ pois $r-1$ ainda divide $\binom{s}{2}(r-1)$.

ii) Segue da **Proposição 3.1.3**.

iii) − *iv*) Por causa das relações estabelecidas no **Lema 3.1.1**, faremos a demonstração dos itens *iii*) e *iv*) simultaneamente.

Da identidade (3.9) da **Proposição 3.1.3**, temos que $[a, b^{\varphi}]^m = 1$, pois $[a, a^{\varphi}]^{r-1} = 1$, pelo item *i*).

Agora, quando aplicado o item *i*) na identidade

$$1 = [a, (b^{o(b)})^{\varphi}] = [a, b^{\varphi}]^{E_m(r,o(b))}[a, a^{\varphi}]^{(r-1)\sum_{i=1}^{o(b)-1}\binom{r^i}{2}},$$

é possível obter que $o([a, b^{\varphi}]) \mid E_m(r, o(b))$. Com um raciocínio análogo, obtemos as seguintes relações:

$$[a, b^{\varphi}]^{E_m(r,n)} = [b, a^{\varphi}]^{E_m(r,n)} = [a, a^{\varphi}]^s. \tag{3.13}$$

Portanto, $[a, b^{\varphi}]$ tem ordem dividindo $(m, E_m(r, o(b)))$.

Aplicando novamente o item *i*) às identidades do **Lema 3.1.1**, obtemos

$$[b, b^{\varphi}]^n = [a, b^{\varphi}]^s = [b, a^{\varphi}]^s,$$

independente da escolha de s.

Como $[b, b^{\varphi}]^{nk} = 1$, da equação (3.8) da **Proposição 3.1.3**, temos que

$$1 = [b, b^{\varphi}]^{nk} = [a, b^{\varphi}]^{sk} = [b, a^{\varphi}]^{sk}.$$

Uma vez que k é sempre ímpar, segue também que

$$([a, b^{\varphi}][b, a^{\varphi}])^{sk} = [a, b^{\varphi}]^{sk}[b, a^{\varphi}]^{sk} = 1.$$

Em resumo, $[a, b^{\varphi}]$ tem ordem dividindo

$$(m, E_m(r, o(b)), sk)$$

e, $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo

$$(o'(a), o'(b), E_m(r, o'(b)), sk),$$

pela **Proposição 3.1.3**. □

A partir da demonstração da **Proposição 3.1.5** acima e pelo **Lema 3.1.1**, obtemos as seguintes identidades satisfeitas no grupo $[G, G^{\varphi}]$ para $G = g(a, b; m, n, r, s)$ e m ímpar:

$$\begin{cases} [a, b^{\varphi}]^s = [b, a^{\varphi}]^s = [b, b^{\varphi}]^n, \\ [a, b^{\varphi}]^{E_m(r,n)} = [b, a^{\varphi}]^{E_m(r,n)} = [a, a^{\varphi}]^s. \end{cases}$$

Observação 3.1.5.1. *Segue da **Proposição 3.1.3** que, uma cota para as ordens dos elementos de um conjunto gerador do grupo* $[G, G^{\varphi}]$ *quando* $G = g(a, b; m, n, m-1, s)$ *é dado por:*

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, 2(m-2))$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* $\begin{cases} n, & se\ k = 1, \\ 2n, & se\ k = 2; \end{cases}$

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* $\begin{cases} (m, s), & se\ 2 \nmid s\ ou\ se\ 4 \mid s\ com\ k = 1, \\ (m, 2s), & caso\ contrário; \end{cases}$

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(m, m-2, s, o'(b))$.

Pelas **Proposições 3.1.3** e **3.1.5**, temos que

$$[a, b^{\varphi}]^{E_m(r,n)} \in \Delta(G),$$

para $G = g(a, b; m, n, r, s)$. Além de já termos que $[a, b^{\varphi}]^m \in \Delta(G)$, para qualquer m e $[a, b^{\varphi}]^s \in \Delta(G)$, pelo **Lema 3.1.1**. Análogo às análises feitas nas **Proposições 3.1.3** e **3.1.5**, segue agora uma cota para as ordens dos elementos de um conjunto gerador do quadrado tensorial não abeliano do $G = g(a, b; m, n, r, 0)$, $r > 1$:

Proposição 3.1.6. *Seja* $G = g(a, b; m, n, r, 0)$ *um grupo metacíclico finito com* $r > 1$.

(1) *Suponha que* m *seja par.*

(a) *Se* $r \neq m - 1$, *então são cotas para as ordens dos geradores de* $[G, G^{\varphi}]$:

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, 2(r-1))$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* n;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* m;

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(m, r-1, n, E_m(r, n))$.

(b) *Se* $r = m - 1$, *então são cotas para as ordens dos geradores de* $[G, G^{\varphi}]$:

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, 2(m-2))$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* n;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* m;

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(m, m-2, n)$.

(2) *Suponha que* m *seja ímpar. Então, são cotas para as ordens dos elementos geradores de* $[G, G^{\varphi}]$:

i) $[a, a^{\varphi}]$ *tem ordem dividindo* $(m, r-1)$;

ii) $[b, b^{\varphi}]$ *tem ordem dividindo* n;

iii) $[a, b^{\varphi}]$ *tem ordem dividindo* $(m, E_m(r, n))$;

iv) $[a, b^{\varphi}][b, a^{\varphi}]$ *tem ordem dividindo* $(m, r-1, n, E_m(r, n))$.

Demonstração. Se m for par, faça $s = 0$ na **Proposição 3.1.3**. Se m for ímpar, basta fazer $s = 0$ na **Proposição 3.1.5**. $\square$

Com base nas cotas estabelecidas pelas **Proposições 3.1.3** e **3.1.5** para os elementos do conjunto gerador do quadrado tensorial não abeliano $[G, G^{\varphi}]$ quando $G = g(a, b; m, n, r, s)$ é um grupo metacíclico finito, não abeliano e não cindido, estamos aptos a propor apresentações para o grupo $\nu(G)$ para os casos em que m é par e m é ímpar, respectivamente.

Teorema A Seja $G = g(x_1, y_1; m, n, r, s)$ um grupo metacíclico finito, não abeliano e não cindido com m par.

– Suponha que $2 \nmid k$:

(i) Se $2 \nmid s$ ou se $4 \mid s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, w^{nk} = 1,\\ & v^{(m,2(r-1))} = 1, z^{(o'(x_1), o'(y_1), sk, E_m(r, o'(y_1)))} = 1, u^{(m,sk)} = 1,\\ & u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}},\\ & u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)}, u^{x_1} = u^{x_2} = uv^{r-1}, u^{E_m(r,n)} = v^{s - \frac{(r-1)^2}{2}\binom{n}{2}},\\ & u^s = w^n = (u^{-1}z)^s, (u^{-1}z)^{E_m(r,n)} = v^{s + \frac{(r-1)^2}{2}\binom{n}{2}}, (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(ii) Se $2 \parallel s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^s v^{r-1} = w^n,\\ & w^n = (u^{-1}z)^s v^{1-r}, u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, u^{(m,2sk)} = 1, w^{nk} = 1,\\ & u^{E_m(r,n)} = v^{s - \frac{(r-1)^2}{2}\binom{n}{2}}, v^{(m,2(r-1))} = 1, z^{(o'(x_1), o'(y_1), sk, E_m(r, o'(y_1)))} = 1,\\ & (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, (u^{-1}z)^{E_m(r,n)} = v^{s + \frac{(r-1)^2}{2}\binom{n}{2}},\\ & u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)}, u^{x_1} = u^{x_2} = uv^{r-1},\ (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

– Suponha que $2 \mid k$:

(iii) Se $2 \nmid s$ ou se $4 \mid s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^{(m,sk)} = 1,\\ & v^{(m,2(r-1))} = 1, w^{nk} = 1, z^{(o'(x_1), o'(y_1), sk/2, E_m(r, o'(y_1)))} = 1,\\ & (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, (u^{-1}z)^{E_m(r,n)} = v^{s + \frac{(r-1)^2}{2}\binom{n}{2}},\\ & u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)}, u^{x_1} = u^{x_2} = uv^{r-1}, u^{E_m(r,n)} = v^{s - \frac{(r-1)^2}{2}\binom{n}{2}},\\ & u^s = w^n = (u^{-1}z)^s, u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}},\ (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(iv) Se $2 \parallel s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^s v^{r-1} = w^n,\\ & w^n = (u^{-1}z)^s v^{1-r}, u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, u^{(m,sk)} = 1, w^{nk} = 1,\\ & z^{(o'(x_1),o'(y_1),sk/2,E_m(r,o'(y_1)))} = 1, (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}},\\ & u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, v^{(m,2(r-1))} = 1,\\ & u^{x_1} = u^{x_2} = uv^{r-1}, u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)},\ (v, w, z\ centrais)\rangle.\end{aligned}$$

Demonstração. Primeiramente provaremos que o grupo $\nu(G)$ é uma imagem homomórfica do grupo M_1 dado pela apresentação do item (i). Para isso, usaremos a estrutura do grupo $\nu(G) = (\Upsilon(G)\ G)\ G^{\varphi}$, conforme **Proposição 1.7.5** (ii), onde $G \cong \langle a, b\rangle$ e $G^{\varphi} \cong \langle a^{\varphi}, b^{\varphi}\rangle$.

O grupo $\Upsilon(G)$ é abeliano gerado pelos elementos $[a, b^{\varphi}]$, $[a, a^{\varphi}]$, $[b, b^{\varphi}]$ e $[a, b^{\varphi}][b, a^{\varphi}]$. Então, pela **Proposição 3.1.3** e relações duduzidas na sua demonstração (página 52), vemos que $\Upsilon(G)$ é uma imagem homomórfica do grupo abeliano A definido por

$$\begin{aligned}\langle u, v, w, z \mid\ & u^{(m,sk)} = 1, v^{(m,2(r-1))} = 1, w^{nk} = 1, z^{(o'(a),o'(b),sk,E_m(r,o'(b)))} = 1,\\ & u^s = w^n = (u^{-1}z)^s, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, u^{E_m(r,o(b))} = v^{-\frac{(r-1)^2}{2}\binom{o(b)}{2}},\\ & (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(r,o(b))} = v^{\frac{(r-1)^2}{2}\binom{o(b)}{2}},\\ & [u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle,\end{aligned}$$

onde os números $o(b)$, $o'(a)$, $o'(b)$ e $E_m(r, x)$, para qualquer $x \in \mathbb{Z}$, são identificados nas **Proposições 2.1.5 e 2.1.6** e na **Definição 1.5.1** para o grupo $G = g(a, b; m, n, r, s)$, respectivamente.

As relações de M_1 nos levam a considerar a aplicação $f : G \to Aut(A)$ definida nos geradores, pondo:

$$\begin{array}{ll} a \mapsto a^f : A \to A & b \mapsto b^f : A \to A \\ \quad u \mapsto (u)a^f := uv^{(r-1)} & \quad u \mapsto (u)b^f := u^r v^{\binom{r}{2}(r-1)} \\ \quad v \mapsto (v)a^f := v & \quad v \mapsto (v)b^f := v \\ \quad w \mapsto (w)a^f := w & \quad w \mapsto (w)b^f := w \\ \quad z \mapsto (z)a^f := z & \quad z \mapsto (z)b^f := z \end{array}$$

<u>Afirmação 1</u>: A aplicação f se estende a um homomorfismo de G em $Aut(A)$.

Serão necessários 3 passos para a demonstração da Afirmação 1:

<u>Passo 1</u>: a^f e b^f se estendem a homomorfismos de A.

Precisamos mostrar que a^f e b^f preservam as relações de A. Considere então a^f e b^f como definido anteriormente:

$$
\begin{aligned}
a^f : \{u, v, w, z\} &\to A \\
u &\mapsto (u)a^f = uv^{r-1} \\
v &\mapsto (v)a^f = v \\
w &\mapsto (w)a^f = w \\
z &\mapsto (z)a^f = z
\end{aligned}
\qquad
\begin{aligned}
b^f : \{u, v, w, z\} &\to A \\
u &\mapsto (u)a^f = u^r v^{(r-1)\binom{r}{2}} \\
v &\mapsto (v)a^f = v \\
w &\mapsto (w)a^f = w \\
z &\mapsto (z)a^f = z
\end{aligned}
$$

As aplicações a^f e b^f fixam os elementos v, w e z. Desta forma, é suficiente analisar as relações de A para a aplicação a^f nos elementos uv^{r-1} e $(u^{-1}v^{-(r-1)})z$ e, os elementos $u^r v^{(r-1)\binom{r}{2}}$ e $(u^{-r}v^{-(r-1)\binom{r}{2}})z$ para a aplicação b^f. Lembre-se que A é um grupo abeliano.

Para a^f:

$$(uv^{r-1})^m = u^m v^{m(r-1)} = 1.$$

$$(uv^{r-1})^s = u^s v^{s(r-1)} = u^s = w^n \quad \text{e}$$

$$(uv^{r-1})^{sk} = u^{sk} v^{s(r-1)k} = u^{sk} = 1,$$

pois $sr \equiv s \ (mod\ m)$. Mais ainda,

$$(uv^{r-1})^{E_m(r,o(b))} = u^{E_m(r,o(b))} v^{(r-1)E_m(r,o(b))} = u^{E_m(r,o(b))} \quad \text{e}$$

$$(uv^{r-1})^{E_m(r,n)} = u^{E_m(r,n)} v^{r^n-1} = u^{E_m(r,n)},$$

pois $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$.

$$\big((uv^{r-1})^{-1}z\big)^m = u^{-m} v^{-m(r-1)} z^m = 1,$$

$$\big((uv^{r-1})^{-1}z\big)^s = u^{-s} v^{-s(r-1)} z^s = (u^{-1}z)^s = w^n \quad \text{e}$$

$$\big((uv^{r-1})^{-1}z\big)^{sk} = u^{-sk} v^{-s(r-1)k} z^{sk} = (u^{-1}z)^{sk} = 1,$$

pois $sr \equiv s \ (mod\ m)$. Por fim,

$$\big((uv^{r-1})^{-1}z\big)^{E_m(r,o(b))} = u^{-E_m(r,o(b))} v^{-(r-1)E_m(r,o(b))} z^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))} \quad \text{e}$$

$$\big((uv^{r-1})^{-1}z\big)^{E_m(r,n)} = u^{-E_m(r,n)} v^{1-r^n} z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)},$$

pois $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$.

Para b^f:

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^m = u^{rm} v^{m(r-1)\binom{r}{2}} = 1.$$

Como $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$,

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^s = u^{sr} v^{s(r-1)\binom{r}{2}} = u^{sr} = u^s,$$

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{sk} = u^{rks} v^{s(r-1)k\binom{r}{2}} = u^{skr} = u^{sk} = 1 \quad \text{e}$$

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{E_m(r,o(b))} = u^{rE_m(r,o(b))} v^{(r-1)E_m(r,o(b))\binom{r}{2}} = u^{E_m(r,o(b))}.$$

Finalmente,

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{E_m(r,n)} = u^{rE_m(r,n)} v^{(r^n-1)\binom{r}{2}} = u^{E_m(r,n)},$$

pois $r^n \equiv 1 \ (mod\ m)$.

Vamos avaliar agora se as relações definidoras de A são também satisfeitas para o elemento $(u^{-r}v^{-(r-1)\binom{r}{2}})z$:

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^m = u^{-rm} v^{-m(r-1)\binom{r}{2}} z^m = 1.$$

As seguintes situações ocorrem:

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^s = u^{-rs} v^{-s(r-1)\binom{r}{2}} z^s = (u^{-1}z)^s = w^n \quad \text{e}$$

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^{sk} = u^{-rsk} v^{-sk(r-1)\binom{r}{2}} z^{sk} = (u^{-1}z)^{sk} = 1$$

pois $sr \equiv s \ (mod\ m)$. Para finalizar,

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^{E_m(r,o(b))} = u^{-rE_m(r,o(b))} v^{-(r-1)E_m(r,o(b))\binom{r}{2}} z^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))} \quad \text{e}$$

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^{E_m(r,n)} = u^{-rE_m(r,n)} v^{-(r-1)E_m(r,n)\binom{r}{2}} z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)}.$$

pois $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$.

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), a^f e b^f se estendem a homomorfismos de A.

Passo 2: a^f e b^f são automorfismos de A.

Garantido os homomorfismos a^f e b^f, é suficiente mostrar que estes são epimorfismos pois A é um grupo finito.

Para isto, basta verificar que

$$\langle (u)a^f, v, w, z\rangle = A = \langle (u)b^f, v, w, z\rangle,$$

uma vez que os homomorfismos a^f e b^f fixam v, w e z.

Como $\langle (u)a^f, v\rangle = \langle uv^{r-1}, v\rangle$, pela definição da aplicação a^f e, $\langle uv^{r-1}, v\rangle = \langle u, v\rangle$, visto que $u = uv^{(r-1)}v^{-(r-1)}$, é evidente que $A = \langle (u)a^f, v, w, z\rangle$.

Por outro lado, sendo $(u)b^f = u^r v^{(r-1)\binom{r}{2}}$ com m e r números relativamente primos, certamente r é relativamente primo com (m, sk). Isto é, existem inteiros λ e μ tais que

$$1 = \lambda(m, sk) + \mu r,$$

implicando em $u = u^{\mu r}$.

Logo,

$$(u^r v^{(r-1)\binom{r}{2}})^{\mu} = u^{\mu r} v^{\mu(r-1)\binom{r}{2}} = uv^{\mu(r-1)\binom{r}{2}}$$

e, por analogia ao caso anterior, vemos que $A = \langle (u)b^f, v, w, z\rangle$.

Portanto, a^f e b^f são automorfismos de A.

Passo 3: a^f e b^f satisfazem as relações de G.

É suficiente analisar a^f e b^f aplicado em $u \in A$, uma vez que ambas aplicações fixam v, w e z.

$$(u)[a^f]^2 = (uv^{r-1})a^f =_{a^f\ auto.} (u)a^f(v^{r-1})a^f = uv^{2(r-1)},$$

$$(u)[a^f]^3 = (uv^{2(r-1)})a^f =_{a^f\ auto.} (u)a^f(v^{2(r-1)})a^f = uv^{3(r-1)}.$$

Indutivamente,

$$(u)[a^f]^{\alpha} = uv^{\alpha(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$. Em particular, para $\alpha = m$, a identidade $(u)[a^f]^m = uv^{m(r-1)} = u$ implica em

$$[a^f]^m = Id_A.$$

$$\begin{aligned}
(u)[b^f]^2 &= (u^r v^{(r-1)\binom{r}{2}})b^f =_{b^f\ auto} (u^r)b^f(v^{(r-1)\binom{r}{2}})b^f = (u^r v^{(r-1)\binom{r}{2}})^r v^{(r-1)\binom{r}{2}} \\
&= u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} \\
(u)[b^f]^3 &= (u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}})b^f =_{b^f\ auto} (u^{r^2})b^f(v^{E_m(r,2)(r-1)\binom{r}{2}})b^f \\
&= (u^r v^{(r-1)\binom{r}{2}})^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} = u^{r^3} v^{E_m(r,3)(r-1)\binom{r}{2}}
\end{aligned}$$

Indutivamente, temos que

$$(u)[b^f]^{\beta} = u^{r^{\beta}} v^{E_m(r,\beta)(r-1)\binom{r}{2}},$$

para qualquer $\beta \in \mathbb{N}$. Em particular, se $\beta = n$ e $\alpha = s$, temos

$$(u)[a^f]^s = u = u^{r^n} v^{E_m(r,n)(r-1)\binom{r}{2}} = (u)[b^f]^n,$$

pois $r^n \equiv 1\ (mod\ m)$. Em outras palavras, $[a^f]^s = [b^f]^n$.

A igualdade $(u)[b^f]^{-1} = u^{r^{o(b)-1}}$ ocorre pois $b^{-1} = b^{o(b)-1}$. Daí,

$$\begin{aligned}
(u)[(b^f)^{-1} \circ a^f \circ b^f] &= \left[\left((u)b^f\right) a^f\right] (b^f)^{-1} \\
&= \left[[(u^r v^{(r-1)\binom{r}{2}})a^f\right] (b^f)^{-1} \\
&= (u^r v^{r(r-1)+(r-1)\binom{r}{2}})(b^f)^{-1} \\
&= (u^{r^{o(b)-1}} v^{E_m(r,o(b)-1)(r-1)\binom{r}{2}})^r v^{r(r-1)+(r-1)\binom{r}{2}} \\
&= u^{r^{o(b)}} v^{(r-1)\left(r\binom{r}{2}E_m(r,o(b)-1)+r+\binom{r}{2}\right)} \\
&= u^r v^{r(r-1)},
\end{aligned}$$

pois

$$\begin{aligned}
(r-1)\left(r\binom{r}{2}E_m(r,o(b)-1)+r+\binom{r}{2}\right) &= (r-1)\left[\binom{r}{2}(rE_m(r,o(b)-1)+1)+r\right] \\
&= (r-1)\left[\binom{r}{2}E_m(r,o(b))+r\right] \\
&= \binom{r}{2}(r^{o(b)}-1)+r(r-1).
\end{aligned}$$

Mas $n \mid o(b)$ e $r^n \equiv 1\ (mod\ m)$. Ou seja,

$$(u)[(b^f)^{-1} \circ a^f \circ b^f] = u^r v^{r(r-1)} = (uv^{r-1})^r = [(u)a^f]^r.$$

Logo, $(b^f)^{-1} \circ a^f \circ b^f = [a^f]^r$.

Desta forma, concluímos que a^f e b^f satisfazem as relações de G, ou seja,

$$[a^f]^m = Id_A, \qquad [b^f]^n = [a^f]^s, \qquad \left[(b^f)^{-1} \circ a^f \circ b^f\right] = [a^f]^r.$$

Os Passos 1, 2, 3 e o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação f se estende a um homomorfismo de G para $Aut(A)$, como queríamos constatar.

Podemos então formar o produto semidireto $H = A \rtimes_f G$ cuja apresentação é dada por:

$$\begin{aligned}
H = \langle a, b, u, v, w, z \mid\ & a^m = 1, b^n = a^s, [a,b] = a^{r-1}, u^{(m,sk)} = 1, v^{(m,2(r-1),\binom{s}{2}(r-1))} = 1, \\
& z^{(o'(a),o'(b),sk,E_m(r,o'(b)))} = 1, u^s = w^n = (u^{-1}z)^s, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, \\
& u^{E_m(r,o(b))} = v^{-\frac{(r-1)^2}{2}\binom{o(b)}{2}}, (u^{-1}z)^{E_m(r,o(b))} = v^{\frac{(r-1)^2}{2}\binom{o(b)}{2}}, u^a = uv^{r-1}, \\
& w^{nk} = 1, [u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1, \\
& (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, u^b = u^r v^{(r-1)\binom{r}{2}}, (v,w,z\ centrais)\rangle,
\end{aligned}$$

garantido pela **Proposição 1.6.10**, onde a dada ação f de G sobre A realizada é por conjugação em H.

A ação f de G sobre A induz uma aplicação $\epsilon : G^{\varphi} \to Aut(H)$ dada por:

$$\begin{array}{lcl} a^{\varphi} & \mapsto & a^{\varphi\epsilon} : H \to H \\ & & a \mapsto (a)a^{\varphi\epsilon} := av \\ & & b \mapsto (b)a^{\varphi\epsilon} := b(u^{-1}z) \\ & & u \mapsto (u)a^{\varphi\epsilon} := uv^{(r-1)} \\ & & v \mapsto (v)a^{\varphi\epsilon} := v \\ & & w \mapsto (w)a^{\varphi\epsilon} := w \\ & & z \mapsto (z)a^{\varphi\epsilon} := z \end{array} \qquad \begin{array}{lcl} b^{\varphi} & \mapsto & b^{\varphi\epsilon} : H \to H \\ & & a \mapsto (a)b^{\varphi\epsilon} := au \\ & & b \mapsto (b)b^{\varphi\epsilon} := bw \\ & & u \mapsto (u)b^{\varphi\epsilon} := u^r v^{(r-1)\binom{r}{2}} \\ & & v \mapsto (v)b^{\varphi\epsilon} := v \\ & & w \mapsto (w)b^{\varphi\epsilon} := w \\ & & z \mapsto (z)b^{\varphi\epsilon} := z \end{array}$$

<u>Afirmação 2</u>: A aplicação ϵ determina um homomorfismo de G^{φ} em $Aut(H)$.

Com o mesmo procedimento usado na demonstração da Afirmação 1, serão necessários 3 passos para a demonstração da Afirmação 2:

<u>Passo 1</u>: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Para isto, devemos mostrar que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ preservam as relações de H.

Como as aplicações $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ fixam v, w e z de H, devemos verificar que as relações de H são satisfeitas para os elementos av, $b(u^{-1}z)$, uv^{r-1} e $u^{-1}v^{-(r-1)}z$ de H, via aplicação $a^{\varphi\epsilon}$ e, para os elementos au, bw, $u^r v^{(r-1)\binom{r}{2}}$ e $u^{-r}v^{-(r-1)\binom{r}{2}}$ via aplicação $b^{\varphi\epsilon}$, sabendo que $[u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1$ em H:

Para $a^{\varphi\epsilon}$:

$$(av)^m = v^m a^m = 1.$$

Agora, observe que

$$(bu^{-1}z)^{ns} = w^{n^2} b^{ns}$$

e,

$$(av)^{s^2} = v^{s^2} a^{s^2} = v^{s^2} b^{ns}.$$

Mas

$$(v^s)^s = (u^{E_m(r,n)})^s = u^{s(1+r+\ldots+r^{n-1})} = u^{sn} = w^{nn},$$

pelas relações de H e também porque $sr \equiv s \ (mod\ m)$. Logo, $w^{n^2} = v^{s^2}$ e por conseguinte, $(av)^s = (bu^{-1}z)^n$.

Na equação

$$(av)^{bu^{-1}z} = (a^r v)^{u^{-1}} = (a^{u^{-1}})^r v^{r(r-1)+1},$$

temos $(a^u) = av^{(1-r)}$ de tal forma que $a = (a^u)^{u^{-1}} = a^{u^{-1}} v^{1-r}$, onde $r(r-1)+1 = (r-1)(r-1)+r$. Portanto, $(av)^{bu^{-1}z} = a^r v^{r(r-1)+1} = a^r v^r = (av)^r$.

Para finalizar,

$$(uv^{r-1})^{av} = u^a v^{r-1} = (uv^{r-1})v^{r-1}$$

e

$$(uv^{r-1})^{b(u^{-1}z)} = u^b v^{r-1} = u^r v^{r-1} v^{\binom{r}{2}(r-1)} = (uv^{r-1})^r v^{\binom{r}{2}(r-1)},$$

pois $r-1 = r(r-1)-(r-1)^2$ e $v^{(r-1)^2} = 1$.

Das relações envolvendo uv^{r-1} e $u^{-1}v^{-(r-1)}z$ em H:

$$(uv^{r-1})^m = v^{m(r-1)}u^m = 1.$$

$$\left((uv^{r-1})^{-1}z\right)^m = v^{-m(r-1)}u^{-m}z^m = 1.$$

Uma vez que $sr \equiv s \ (mod\ m)$, temos

$$(uv^{r-1})^s = u^s v^{s(r-1)} = u^s,$$

$$\left((uv^{r-1})^{-1}z\right)^s = v^{-s(r-1)}u^{-s}z^s = (u^{-1}z)^s = w^n,$$

$$(uv^{r-1})^{sk} = u^{ks}v^{s(r-1)k} = u^{sk} = 1 \quad \text{e}$$

$$\left((uv^{r-1})^{-1}z\right)^{sk} = v^{-s(r-1)k}u^{-sk}z^{sk} = (u^{-1}z)^{sk} = 1.$$

Além disso,

$$(uv^{r-1})^{E_m(r,o(b))} = u^{E_m(r,o(b))}v^{(r-1)E_m(r,o(b))} = u^{E_m(r,o(b))},$$

$$\left((uv^{r-1})^{-1}z\right)^{E_m(r,o(b))} = v^{-(r-1)E_m(r,o(b))}u^{-E_m(r,o(b))}z^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))},$$

$$(uv^{r-1})^{E_m(r,n)} = u^{E_m(r,n)}v^{r^n-1} = u^{E_m(r,n)} \quad \text{e}$$

$$\left((uv^{r-1})^{-1}z\right)^{E_m(r,n)} = v^{-(r-1)E_m(r,n)}u^{-E_m(r,n)}z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)},$$

pois $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$.

Para b^f:

$$(au)^m = u^m a^m = 1.$$

$$(bw)^n = w^n b^n = u^s a^s = (au)^s.$$

Da equação

$$[(au)^{bw}]^s = [(a^r u^b)]^s = [a^r u^r v^{(r-1)\binom{r}{2}}]^s = u^{rs}a^{rs} = [(au)^r]^s,$$

obtemos $(au)^{bw} = (au)^r$, uma vez que $s > 1$ e $s(r-1) \equiv 1 \ (mod\ m)$.

Para finalizar,

$$(u^r v^{(r-1)\binom{r}{2}})^{au} = (u^r)^a v^{(r-1)\binom{r}{2}} = (uv^{r-1})^r v^{\binom{r}{2}(r-1)} = (u^r v^{\binom{r}{2}(r-1)})v^{r-1},$$

pois $r-1 = r(r-1)-(r-1)^2$ e $v^{(r-1)^2} = 1$.

$$(u^r v^{(r-1)\binom{r}{2}})^{bw} = (u^b)^r v^{(r-1)\binom{r}{2}} = (u^r v^{(r-1)\binom{r}{2}})v^{(r-1)\binom{r}{2}},$$

como queríamos verificar.

Das relações envolvendo $u^r v^{(r-1)\binom{r}{2}}$ e $u^{-r}v^{-(r-1)\binom{r}{2}}z$ em H:

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^m = u^{rm}v^{m(r-1)\binom{r}{2}} = 1.$$

$$\left((u^r v^{(r-1)\binom{r}{2}})^{-1}z\right)^m = u^{-rm}v^{-m(r-1)\binom{r}{2}}z^m = 1.$$

Sabendo que $sr \equiv s\ (mod\ m)$, temos

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^s = u^{sr}v^{s(r-1)\binom{r}{2}} = u^s,$$

$$\left((u^r v^{(r-1)\binom{r}{2}})^{-1}z\right)^s = u^{-sr}v^{-s(r-1)\binom{r}{2}}z^{sr} = (u^{-1}z)^s = w^n,$$

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{sk} = u^{srk}v^{s(r-1)k\binom{r}{2}} = u^{sk} = 1 \quad \text{e}$$

$$\left(u^{-r}v^{-(r-1)\binom{r}{2}}z\right)^{sk} = u^{-srk}v^{-s(r-1)k\binom{r}{2}}z^{sk} = (u^{-1}z)^{sk} = 1.$$

Mais ainda,

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{E_m(r,o(b))} = u^{rE_m(r,o(b))}v^{(r-1)E_m(r,o(b))\binom{r}{2}} = u^{E_m(r,o(b))},$$

$$\left((u^r v^{(r-1)\binom{r}{2}})^{-1}z\right)^{E_m(r,o(b))} = v^{-(r-1)\binom{r}{2}E_m(r,o(b))}u^{-rE_m(r,o(b))}z^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))},$$

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^{E_m(r,n)} = u^{rE_m(r,n)}v^{(r-1)E_m(r,n)\binom{r}{2}} = u^{E_m(r,n)} \quad \text{e}$$

$$\left((u^r v^{(r-1)\binom{r}{2}})^{-1}z\right)^{E_m(r,n)} = v^{-(r-1)E_m(r,n)\binom{r}{2}}u^{-rE_m(r,n)}z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)},$$

pois $n \mid o(b)$ e $r^n \equiv 1\ (mod\ m)$.

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Passo 2: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são automorfismos de H.

Uma vez que H é um grupo finito, é suficiente verificarmos que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são sobrejetora. Ou seja, devemos verificar que

$$\langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle = H = \langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle,$$

já que os homomorfismos $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ fixam v, w e z.

Sabemos que $\langle (u)a^{\varphi\epsilon}, v\rangle = \langle uv^{r-1}, v\rangle$, pela definição da aplicação $a^{\varphi\epsilon}$ e, $\langle uv^{r-1}, v\rangle = \langle u, v\rangle$, uma vez que $u = uv^{(r-1)}v^{-(r-1)}$. Com um raciocínio semelhante, obtemos

$$\langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle = \langle a, b, u, v, w, z\rangle,$$

pois $(a)a^{\varphi\epsilon} = av$, $(b)a^{\varphi\epsilon} = b(u^{-1}z)$. Logo, $H = \langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle$.

Por outro lado, como $(u)b^{\varphi\epsilon} = u^r v^{(r-1)\binom{r}{2}}$ com $(m, r) = 1$, certamente r é relativamente primo com (m, sk). Ou seja, existem inteiros λ e μ tais que

$$1 = \lambda(m, sk) + \mu r,$$

implicando em $u = u^{\mu r}$.

Desta forma,

$$(u^r v^{(r-1)\binom{r}{2}})^{\mu} = u^{\mu r} v^{\mu(r-1)\binom{r}{2}} = uv^{\mu(r-1)\binom{r}{2}}$$

e, por analogia ao caso anterior, obtemos $\langle (u)b^{\varphi\epsilon}, v, w, z\rangle = \langle u, v, w, z\rangle$. Novamente, $\langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle = H$, visto que $a = auu^{-1}$, $b = bww^{-1}$.

Portanto, $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são automorfismos de H.

<u>Passo 3:</u> $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^{φ}.

Para isso, iremos analisar $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ aplicado em a, b e $u \in H$, uma vez que ambas aplicações fixam v, w e z.

$$(u)[a^{\varphi\epsilon}]^2 = (uv^{r-1})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (u)a^{\varphi\epsilon}(v^{r-1})a^{\varphi\epsilon} = uv^{2(r-1)},$$

$$(u)[a^{\varphi\epsilon}]^3 = (uv^{2(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (u)a^{\varphi\epsilon}(v^{2(r-1)})a^{\varphi\epsilon} = uv^{3(r-1)}.$$

Indutivamente, temos que

$$(u)[a^{\varphi\epsilon}]^{\alpha} = uv^{\alpha(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$.

$$(a)[a^{\varphi\epsilon}]^2 = (av)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v)a^{\varphi\epsilon} = av^2,$$

$$(a)[a^{\varphi\epsilon}]^3 = (av^2)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v^2)a^{\varphi\epsilon} = av^3.$$

Indutivamente,

$$(a)[a^{\varphi\epsilon}]^{\alpha} = av^{\alpha},$$

para qualquer $\alpha \in \mathbb{N}$.

$$\begin{aligned}(b)[a^{\varphi\epsilon}]^2 &= (bu^{-1}z)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-1})a^{\varphi\epsilon}(z)a^{\varphi\epsilon} = bu^{-1}zu^{-1}zv^{-(r-1)}\\ &= b(u^{-1}z)^2v^{-(r-1)},\end{aligned}$$

$$\begin{aligned}(b)[a^{\varphi\epsilon}]^3 &= (b(u^{-1}z)^2v^{-(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-2})a^{\varphi\epsilon}(z^2)a^{\varphi\epsilon}(v^{-(r-1)})a^{\varphi\epsilon}\\ &= bu^{-1}z(uv^{(r-1)})^{-2}z^2v^{-(r-1)}\\ &= b(u^{-1}z)^3v^{-3(r-1)},\end{aligned}$$

$$\begin{aligned}
(b)[a^{\varphi\epsilon}]^4 &= (b(u^{-1}z)^3v^{-3(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-3})a^{\varphi\epsilon}(z^3)a^{\varphi\epsilon}(v^{-3(r-1)})a^{\varphi\epsilon}\\
&= bu^{-1}z(uv^{(r-1)})^{-3}z^3v^{-3(r-1)}\\
&= b(u^{-1}z)^4v^{-6(r-1)}.
\end{aligned}$$

Indutivamente, temos que

$$(b)[a^{\varphi\epsilon}]^\alpha = b(u^{-1}z)^\alpha v^{-\binom{\alpha}{2}(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$.

$$\begin{aligned}
(u)[b^{\varphi\epsilon}]^2 &= (u^rv^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} (u^r)b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} = (u^rv^{(r-1)\binom{r}{2}})^rv^{(r-1)\binom{r}{2}}\\
&= u^{r^2}v^{E_m(r,2)(r-1)\binom{r}{2}}\\
(u)[b^{\varphi\epsilon}]^3 &= (u^{r^2}v^{E_m(r,2)(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} (u^{r^2})b^{\varphi\epsilon}(v^{E_m(r,2)(r-1)\binom{r}{2}})b^{\varphi\epsilon}\\
&= (u^rv^{(r-1)\binom{r}{2}})^{r^2}v^{E_m(r,2)(r-1)\binom{r}{2}} = u^{r^3}v^{E_m(r,3)(r-1)\binom{r}{2}}
\end{aligned}$$

Indutivamente, temos que

$$(u)[b^{\varphi\epsilon}]^\beta = u^{r^\beta}v^{E_m(r,\beta)(r-1)\binom{r}{2}},$$

para qualquer $\beta \in \mathbb{N}$.

$$(a)[b^{\varphi\epsilon}]^2 = (au)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u)b^{\varphi\epsilon} = auu^rv^{(r-1)\binom{r}{2}} = au^{(r+1)}v^{(r-1)\binom{r}{2}},$$

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^3 &= (au^{(r+1)}v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{(r+1)})b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon}\\
&= au(u^rv^{(r-1)\binom{r}{2}})^{E_m(r,2)}v^{(r-1)\binom{r}{2}}\\
&= au^{E_m(r,3)}v^{\binom{r}{2}(r-1)(1+1+r)} = au^{E_m(r,3)}v^{(r-1)\left[\binom{r}{2}+\binom{r^2}{2}\right]},
\end{aligned}$$

onde

$$\binom{r}{2}(r-1)(1+1+r) \equiv (r-1)\left[\binom{r}{2}+\binom{r^2}{2}\right]\ (mod\ (m,2(r-1)))$$

(vide **Proposição 3.1.3**).

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^4 &= (au^{E_m(r,3)}v^{\binom{r}{2}(r-1)})b^{\varphi\epsilon}\\
&=_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{E_m(r,3)})b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon}\\
&= au(u^rv^{(r-1)\binom{r}{2}})^{E_m(r,3)}v^{(r-1)\binom{r}{2}}\\
&= au^{E_m(r,4)}v^{\binom{r}{2}(r-1)(1+r+r^2+1)} = au^{E_m(r,4)}v^{(r-1)\left[\binom{r}{2}+\binom{r^2}{2}+\binom{r^3}{2}\right]},
\end{aligned}$$

onde

$$\binom{r}{2}(r-1)(1+1+r+r^2) \equiv (r-1)\left[\binom{r}{2}+\binom{r^2}{2}+\binom{r^3}{2}\right]\ (mod\ (m,2(r-1)))$$

(vide **Proposição 3.1.3**).

Indutivamente, temos que

$$(a)[b^{\varphi\epsilon}]^{\beta} = au^{E_m(r,\beta)}v^{(r-1)\sum_{i=1}^{\beta-1}\binom{r^i}{2}},$$

para qualquer $\beta \in \mathbb{N}$.

$$(b)[b^{\varphi\epsilon}]^2 = (bw)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w)b^{\varphi\epsilon} = bw^2$$

$$(b)[b^{\varphi\epsilon}]^3 = (bw^2)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w^2)b^{\varphi\epsilon} = bw^3.$$

Indutivamente, obtemos

$$(b)[b^{\varphi\epsilon}]^{\beta} = bw^{\beta},$$

para qualquer $\beta \in \mathbb{N}$.

Em particular, para $\alpha = m$, obtemos as seguintes igualdades:

$$\begin{cases} (u)[a^{\varphi\epsilon}]^m = uv^{m(r-1)} = u \\ (a)[a^{\varphi\epsilon}]^m = av^m = a \\ (b)[a^{\varphi\epsilon}]^m = b(u^{-1}z)^m v^{-m(r-1)} = b, \end{cases}$$

ou seja, $[a^{\varphi\epsilon}]^m = Id_H$.

Mais ainda, fazendo $\beta = n$ e $\alpha = s$, temos que

$$\begin{cases} (u)[a^{\varphi\epsilon}]^s = uv^s(r-1) = u = u^{r^n}v^{E_m(r,n)(r-1)\binom{r}{2}} = [(u)b^{\varphi\epsilon}]^n \\ (a)[a^{\varphi\epsilon}]^s = av^s = au^{E_m(r,n)}v^{\frac{(r-1)^2}{2}\binom{n}{2}} = au^{E_m(r,n)}v^{(r-1)\sum_{i=1}^{n-1}\binom{r^i}{2}} = [(a)b^{\varphi\epsilon}]^n \\ (b)[a^{\varphi\epsilon}]^s = b(u^{-1}z)^s v^{-s(r-1)} = bw^n = [(b)b^{\varphi\epsilon}]^n, \end{cases}$$

o que implica em $[a^{\varphi\epsilon}]^s = [b^{\varphi\epsilon}]^n$.

Para finalizar, como $b^{o(b)-1} = b^{-1}$, temos que $[b^{\varphi\epsilon}]^{-1} = [b^{\varphi\epsilon}]$. Logo, segue as seguintes identidades:

$$\begin{aligned} (u)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] &= [((u)b^{\varphi\epsilon})a^{\varphi\epsilon}]\, b^{\varphi\epsilon(o(b)-1)} \\ &= \left(((u)a^{\varphi\epsilon})^r((v)a^{\varphi\epsilon})^{\binom{r}{2}(r-1)}\right)[b^{\varphi\epsilon(o(b)-1)}] \\ &= \left((uv^{r-1})^r v^{\binom{r}{2}(r-1)}\right)[b^{\varphi\epsilon(o(b)-1)}] \\ &= (u)[b^{\varphi\epsilon(o(b)-1)}]^r(v)[b^{\varphi\epsilon(o(b)-1)}]^{(r-1)\left(\binom{r}{2}+r\right)} \\ &= uv^{r(r-1)} \\ &= (u)[a^{\varphi\epsilon}]^r \end{aligned}$$

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] &= [((a)b^{\varphi\epsilon})a^{\varphi\epsilon}]\, b^{\varphi\epsilon(o(b)-1)} \\
&= (((a)a^{\varphi\epsilon})((u)a^{\varphi\epsilon}))\,[b^{\varphi\epsilon(o(b)-1)}] \\
&= ((auv^r)[\, b^{\varphi\epsilon(o(b)-1)}] \\
&= (a)[b^{\varphi\epsilon(o(b)-1)}](u)[b^{\varphi\epsilon(o(b)-1)}](v)[b^{\varphi\epsilon(o(b)-1)}]^r \\
&= au^{(r-1)E_m(r,(o(b)-1))+1+E_m(r,(b)-1)}v^{r+(r^{o(b)-1}-1)\binom{r}{2}+\frac{(r-1)^2}{2}\binom{o(b)-1}{2}} \\
&= au^{E_m(r,(o(b)))}v^{r+\frac{(r-1)^2}{2}\left[\binom{o(b)-1}{2}-1\right]} \\
&= au^{E_m(r,(o(b)))}v^{r+\frac{(r-1)^2}{2}\binom{o(b)}{2}} \\
&= au^{E_m(r,(o(b)))}v^r u^{-E_m(r,(b))} \\
&= av^r \\
&= (a)[a^{\varphi\epsilon}]^r
\end{aligned}$$

O procedimento de análise da relação $(b)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = (b)[a^{\varphi\epsilon}]^r$ é análogo.

Desta forma, concluímos que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^{φ}, ou seja,

$$[a^{\varphi\epsilon}]^m = Id_H, \qquad [b^{\varphi\epsilon}]^n = [a^{\varphi\epsilon}]^s, \qquad \left[(b^{\varphi\epsilon})^{-1} \circ a^{\varphi\epsilon} \circ b^{\varphi\epsilon}\right] = [a^{\varphi\epsilon}]^r.$$

Os Passos 1, 2, 3 e o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação ϵ se estende a um homomorfismo de G^{φ} para $Aut(H)$, como queríamos constatar.

Logo, via o homomorfismo ϵ, obtemos o produto semidireto de H por G^{φ} dado por

$$K = H \rtimes_{\epsilon} G^{\varphi} = (A \rtimes_f G) \rtimes_{\epsilon} G^{\varphi}.$$

Analogamente à apresentação do grupo H, pela **Proposição 1.6.10**, obtemos a apresentação para K dada por:

$$\begin{aligned}
K = \langle a, b, u, v, w, z, a^{\varphi}, b^{\varphi} \mid\ & a^m = 1, b^n = a^s, [a,b] = a^{r-1}, (a^{\varphi})^m = 1, (b^{\varphi})^n = (a^{\varphi})^s, w^{nk} = 1, \\
& [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{r-1}, v^{(m,2(r-1))} = 1, u^s = w^n = (u^{-1}z)^s, \\
& z^{(o'(a),o'(b),sk,E_m(r,o'(b)))} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, u^{(m,sk)} = 1, \\
& u^{E_m(r,o(b))} = v^{-\frac{(r-1)^2}{2}\binom{o(b)}{2}}, (u^{-1}z)^{E_m(r,o(b))} = v^{\frac{(r-1)^2}{2}\binom{o(b)}{2}}, a^{a^{\varphi}} = au, \\
& (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, b^{a^{\varphi}} = b(u^{-1}z), u^{a^{\varphi}} = u, v^{a^{\varphi}} = v, \\
& w^{a^{\varphi}} = w, z^{a^{\varphi}} = z, a^{b^{\varphi}} = au, b^{b^{\varphi}} = bw, u^{b^{\varphi}} = u^r, v^{b^{\varphi}} = v, w^{b^{\varphi}} = w, \\
& z^{b^{\varphi}} = z,\ (v, w, z\ \mathit{centrais})\rangle.
\end{aligned}$$

Desta apresentação observamos que as ações de G sobre o subgrupo (normal) $\langle u, v, w, z\rangle$ é a mesma que aquela de G^{φ}.

Desta forma, trocando a por x_1, b por y_1, a^{φ} por x_2 e b^{φ} por y_2, concluímos que K possui precisamente a mesma apresentação do grupo M_1. Consequentemente, $M_1 \cong K$.

Agora, as ações de G sobre A e de G^{φ} sobre $H = A \rtimes_f G$ que definem o grupo K traduzem, respectivamente, as ações de G sobre $G \otimes G \cong [G, G^{\varphi}]$ (conforme **Proposição 1.7.3** (i)) e de G sobre $(G \otimes G) \rtimes G$, as quais definem o grupo $\nu(G) = (\ [G, G^{\varphi}]\ G)\ G^{\varphi} \cong ((G \otimes G) \rtimes G) \rtimes G$. Por conseguinte, o dado epimorfismo $A \twoheadrightarrow [G, G^{\varphi}] \cong G \otimes G$ induz um epimorfismo de K sobre $\nu(G)$.

Consequentemente, a aplicação $\phi : M_1 \to \nu(G)$ dada por $x_1 \mapsto a$, $y_1 \mapsto b$, $x_2 \mapsto a^{\varphi}$ e $y_2 \mapsto b^{\varphi}$ define um epimorfismo de M_1 sobre $\nu(G)$.

Reciprocamente, a aplicação $\psi : \nu(G) \to M_1$ que associa $a \mapsto x_1$, $b \mapsto y_1$, $a^{\varphi} \mapsto x_2$ e $b^{\varphi} \mapsto y_2$ preserva as relações de $\nu(G)$, na sua apresentação dada pelo **Teorema 1.7.20**, haja vista as relações de conjugação decorrentes do **Lema 3.0.1**

$$\begin{gathered}
[a, b^{\varphi}]^{a} = [a, b^{\varphi}]^{a^{\varphi}} = [a, b^{\varphi}][a, a^{\varphi}]^{(r-1)}, \\
[a, b^{\varphi}]^{b} = [a, b^{\varphi}]^{b^{\varphi}} = [a, b^{\varphi}]^{r}[a, a^{\varphi}]^{(r-1)\binom{r}{2}}, \\
[a, a^{\varphi}]^{a} = [a, a^{\varphi}]^{a^{\varphi}} = [a, a^{\varphi}]^{b} = [a, a^{\varphi}]^{b^{\varphi}} = [a, a^{\varphi}], \\
[b, b^{\varphi}]^{a} = [b, b^{\varphi}]^{a^{\varphi}} = [b, b^{\varphi}]^{b} = [b, b^{\varphi}]^{b^{\varphi}} = [b, b^{\varphi}], \\
[b, a^{\varphi}]^{a} = [b, a^{\varphi}]^{a^{\varphi}} = [b, a^{\varphi}][a, a^{\varphi}]^{-(r-1)}, \\
[b, a^{\varphi}]^{b} = [b, a^{\varphi}]^{b^{\varphi}} = [b, a^{\varphi}]^{r}[a, a^{\varphi}]^{-(r-1)\binom{r}{2}}.
\end{gathered}$$

das quais decorrem as relações definidoras de M_1, conforme **Proposição 3.1.3**.

Assim, os epimorfismos ϕ e ψ possuem inversas a direita, a saber, $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$. Portanto, obtemos o isomorfismo $\nu(G) \cong M_1$.

A verificação de que as apresentações dos itens (ii), (iii) e (iv) descrevem o grupo $\nu(G)$ para os respectivos grupos metacíclicos finitos G segue de maneira análoga e fica portanto demonstrado o **Teorema A**. $\square$

Como Corolário imediato do **Teorema A**, auferimos apresentações para o grupo $\nu(G)$ quando $G = g(a, b; m, n, m-1, s)$ é um grupo metacíclico finito, não abeliano e não cindido:

Corolário 3.1.7. *Seja $G = g(x_1, y_1; m, n, m-1, s)$ um grupo metacíclico finito, não abeliano e não cindido.*

– *Suponha que $k = 1$:*

(i) Se $2 \nmid s$ ou se $4 \mid s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{m-2}, [x_2, y_2] = x_2^{m-2},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^{(m,s)} = 1,\\ & v^{(m,2(m-2))} = 1, z^{(m,s,m-2,o'(y_1))} = 1, u^{x_1} = u^{x_2} = uv^{m-2}, w^n = 1,\\ & u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, u^{y_1} = u^{y_2} = u^{m-1}v^{\binom{m-1}{2}(m-2)},\\ & (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}},\ (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(ii) Se $2 \parallel s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{m-2}, [x_2, y_2] = x_2^{m-2},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^{(m,2s)} = 1,\\ & v^{(m,2(m-2))} = 1, w^n = 1, (u^{-1}z)^s = v^{m-2}, u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}},\\ & u^{y_1} = u^{y_2} = u^{m-1}v^{\binom{m-1}{2}(m-2)}, u^{x_1} = u^{x_2} = uv^{m-2}, u^s = v^{2-m},\\ & z^{(m,s,m-2,o'(y_1))} = 1, (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}},\\ & (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

– Suponha que $k = 2$:

(iii) Se $2 \nmid s$ ou se $4 \mid s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{m-2}, [x_2, y_2] = x_2^{m-2},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^{(m,2s)} = 1,\\ & v^{(m,2(m-2))} = 1, w^{2n} = 1, (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}}, w^n = u^s,\\ & u^{y_1} = u^{y_2} = u^{m-1}v^{\binom{m-1}{2}(m-2)}, u^{x_1} = u^{x_2} = uv^{m-2}, w^n = (u^{-1}z)^s\\ & u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, z^{(m,s,m-2,o'(y_1))} = 1, (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(iv) Se $2 \parallel s$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{m-2}, [x_2, y_2] = x_2^{m-2},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^{(m,2s)} = 1,\\ & u^{y_1} = u^{y_2} = u^{m-1}v^{\binom{m-1}{2}(m-2)}, u^{x_1} = u^{x_2} = uv^{m-2}, w^{2n} = 1,\\ & u^s v^{m-2} = w^n = (u^{-1}z)^s v^{2-m}, (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}},\\ & v^{(m,2(m-2))} = 1, z^{(m,s,m-2,o'(y_1))} = 1, u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}},\\ & (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

O seguinte resultado estabelece uma apresentação para o grupo $\nu(G)$ quando $G = g(a, b; m, n, r, s)$ é um grupo metacíclico finito com m ímpar, $r > 1$ e $s > 0$, a partir da cota das ordens dos elementos do conjunto gerador do quadrado tensorial não abeliano de G, estabelecida na **Proposição 3.1.5**, análoga à estratégia utilizada no **Teorema A**, cuja demonstração também segue.

Teorema B Seja $G = g(x_1, y_1; m, n, r, s)$ um grupo metacíclico finito, não abeliano e não cindido com m ímpar. Então, uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, w^{nk} = 1,\\ & u^s = w^n = (u^{-1}z)^s, v^s = (u^{-1}z)^{E_m(r,n)} = u^{E_m(r,n)}, v^{(m,r-1)} = 1,\\ & u^{(m,E_m(r,o(y_1)),sk)} = 1, z^{(o'(x_1),o'(y_1),sk,E_m(r,o'(y_1)))} = 1, u^{x_1} = u^{x_2} = u,\\ & u^{y_1} = u^{y_2} = u^r,\ (v, w, z\ centrais)\rangle.\end{aligned}$$

Demonstração. Provaremos primeiramente que o grupo $\nu(G)$ é uma imagem homomórfica do grupo M dado acima. Para isso, usaremos a estrutura de $\nu(G) = (\Upsilon(G)\ G)\ G^\varphi$ conforme **Proposição 1.7.5** (ii) onde $G \cong \langle a, b\rangle$ e $G^\varphi \cong \langle a^\varphi, b^\varphi\rangle$.

Já sabemos que $\Upsilon(G)$ é um grupo abeliano gerado pelos elementos $[a, b^\varphi]$, $[a, a^\varphi]$, $[b, b^\varphi]$ e $[a, b^\varphi][b, a^\varphi]$. Pela **Proposição 3.1.5** e relações duduzidas na sua demonstração (página 54), vemos que $\Upsilon(G)$ é uma imagem homomórfica do grupo abeliano A definido por

$$\begin{aligned}\langle u, v, w, z \mid\ & u^{(m,E_m(r,o(b)),sk)} = 1, v^{o'(a)} = 1, w^{nk} = 1, z^{(o'(a),o'(b),sk,E_m(r,o'(b)))} = 1,\\ & u^s = w^n = (u^{-1}z)^s, u^{E_m(r,n)} = v^s = (u^{-1}z)^{E_m(r,n)},\\ & [u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle,\end{aligned}$$

onde os números $o(b)$, $o'(a)$, $o'(b)$ e $E_m(r, x)$, para qualquer $x \in \mathbb{Z}$, são identificados nas **Proposições 2.1.5 e 2.1.6** e na **Definição 1.5.1** para o grupo $G = g(a, b; m, n, r, s)$, respectivamente.

As relações de M nos levam a considerar a aplicação $f : G \to Aut(A)$ definida nos geradores, pondo:

$$\begin{array}{lll} a & \mapsto & a^f : A \to A \\ & & u \mapsto (u)a^f := u \\ & & v \mapsto (v)a^f := v \\ & & w \mapsto (w)a^f := w \\ & & z \mapsto (z)a^f := z \end{array} \qquad \begin{array}{lll} b & \mapsto & b^f : A \to A \\ & & u \mapsto (u)b^f := u^r \\ & & v \mapsto (v)b^f := v \\ & & w \mapsto (w)b^f := w \\ & & z \mapsto (z)b^f := z \end{array}$$

Afirmação 1: A aplicação f se estende a um homomorfismo de G em $Aut(A)$.

Para verificarmos a Afirmação 1, precisaremos de 3 passos:

Passo 1: a^f e b^f se estendem a homomorfismos de A.

Precisamos mostrar que a^f e b^f preservam as relações de A. Para isto, considere a^f e b^f como definido anteriormente:

$$\begin{array}{rlrl} a^f : \{u,v,w,z\} \to A & & b^f : \{u,v,w,z\} \to A & \\ & u \mapsto (u)a^f = u & & u \mapsto (u)a^f = u^r \\ & v \mapsto (v)a^f = v & & v \mapsto (v)a^f = v \\ & w \mapsto (w)a^f = w & & w \mapsto (w)a^f = w \\ & z \mapsto (z)a^f = z & & z \mapsto (z)a^f = z \end{array}$$

A aplicação a^f fixa os elementos u, v, w e z de A. Então não há o que fazer. Já a aplicação b^f fixa os elementos v, w e z e portanto, é preciso analisar as relações de A para os elementos u^r e $u^{-r}z$:

$$(u^r)^m = u^{mr} = 1,$$

$$(u^{-r}z)^m = u^{-mr}z^m = 1.$$

Mais ainda,

$$(u^r)^s = u^s,$$

$$(u^{-r}z)^s = u^{-sr}z^s = (u^{-1}z)^s,$$

$$(u^r)^{sk} = u^{ks} = 1 \quad \text{e}$$

$$(u^{-r}z)^{sk} = u^{ks}z^s = (u^{-1}z)^s,$$

pois $sr \equiv s \ (mod\ m)$. Por fim,

$$(u^r)^{E_m(r,n)} = u^{r(1+r+\ldots+r^{n-1})} = u^{r+r^2+\ldots+r^{n-1}+1} = u^{E_m(r,n)},$$

$$(u^{-r}z)^{E_m(r,n)} = u^{-r(1+r+\ldots+r^{n-1})}z^{E_m(r,n)} = u^{-(r+r^2+\ldots+r^{n-1}+1)}z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)},$$

$$(u^r)^{E_m(r,o(b))} = u^{E_m(r,o(b))} = 1 \quad \text{e}$$

$$(u^{-r}z)^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))} = 1,$$

pois $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$.

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), a^f e b^f se estendem a homomorfismos de A.

<u>Passo 2</u>: a^f e b^f são automorfismos de A.

Para isto, devemos mostrar que a^f e b^f são epimorfismos uma vez que A é um grupo finito e, $\langle (u)a^f, v, w, z\rangle \leq A$ tanto quanto $\langle (u)b^f, v, w, z\rangle \leq A$, onde a^f e b^f são homomorfismos de A que fixam v, w e z.

Agora, $\langle (u)a^f, v\rangle = \langle u, v\rangle$, pela definição da aplicação a^f e, $\langle (u)b^f, v\rangle = \langle u^r, v\rangle = \langle u, v\rangle$, uma vez que $(m, r) = 1$.

Portanto, a^f e b^f são automorfismos de A.

Passo 3: a^f e b^f satisfazem as relações de G.

Como dizemos anteriormente, é suficiente analisar a^f e b^f aplicado em $u \in A$, uma vez que ambas aplicações fixam v, w e z.

A aplicação a^f também fixa u, o que implica em $(u)[a^f]^\alpha = u$, para qualquer $\alpha \in \mathbb{N}$. Em particular, para $\alpha = m$, a identidade $(u)[a^f]^m = u$ implica em

$$[a^f]^m = Id_A.$$

Vamos verificar que a^f e b^f satisfazem também as outras relações de G. Para isto, observe que:

$$\begin{aligned}(u)[b^f]^2 &= (u^r)b^f = u^{r^2},\\ (u)[b^f]^3 &= (u^{r^2})b^f = u^{r^3}.\end{aligned}$$

Indutivamente, temos que

$$(u)[b^f]^\beta = u^{r^\beta},$$

para qualquer $\beta \in \mathbb{N}$. Em particular, se $\beta = n$ e $\alpha = s$, temos

$$(u)[a^f]^s = u = u^{r^n} = (u)[b^f]^n,$$

pois $r^n \equiv 1$ $(mod\ m)$. Isto quer dizer que $[a^f]^s = [b^f]^n$.

Para finalizar, como $b^{-1} = b^{o(b)-1}$ temos a seguinte igualdade $(u)[b^f]^{-1} = u^{r^{o(b)-1}}$. Daí,

$$\begin{aligned}(u)[(b^f)^{-1} \circ a^f \circ b^f] &= \{[(u)b^f]a^f\}(b^f)^{-1}\\ &= ((u^r)[a^f])[b^f]^{-1} = (u^r)[b^f]^{-1}\\ &= u^{r^{o(b)-1}r} = u^{r^{o(b)}}.\end{aligned}$$

Mas $n \mid o(b)$ e $r^n \equiv 1$ $(mod\ m)$, ou seja, $(u)[(b^f)^{-1} \circ a^f \circ b^f] = u^r = (u)[a^f]^r$.

Logo, $[b^f]^{-1} \circ a^f \circ b^f = [a^f]^r$.

Desta forma, concluímos que a^f e b^f satisfazem as relações de G, ou seja,

$$[a^f]^m = Id_A, \qquad [b^f]^n = [a^f]^s, \qquad [b^f]^{-1} \circ [a^f] \circ [b^f] = [a^f]^r.$$

Os Passos 1, 2, 3 juntamente com o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação f se estende a um homomorfismo de G para $Aut(A)$, finalizando então a demonstração da nossa Afirmação 1.

Em outras palavras, f determina uma ação de G sobre A que nos dá uma extensão $H = A \rtimes_f G$ cuja apresentação é dada por:

$$\begin{aligned}\langle a, b, u, v, w, z \mid\ & a^m = 1, b^n = a^s, [a, b] = a^{r-1}, u^a = u, u^b = u^r, u^{(m, E_m(r, o(b)), sk)} = 1,\\ & v^{o'(a)} = 1, w^{nk} = 1, z^{(o'(a), o'(b), sk, E_m(r, o'(b)))} = 1, u^s = w^n = (u^{-1}z)^s,\\ & u^{E_m(r,n)} = v^s = (u^{-1}z)^{E_m(r,n)},\ (v, w, z \textit{ centrais}),\\ & [u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle,\end{aligned}$$

garantido pela **Proposição 1.6.10**.

A ação f de G sobre A induz uma aplicação $\epsilon : G^\varphi \to Aut(H)$ dada por:

$$\begin{aligned} a^\varphi \ \mapsto \ a^{\varphi\epsilon} &: H \to H \\ a &\mapsto (a)a^{\varphi\epsilon} := av \\ b &\mapsto (b)a^{\varphi\epsilon} := b(u^{-1}z) \\ u &\mapsto (u)a^{\varphi\epsilon} := u \\ v &\mapsto (v)a^{\varphi\epsilon} := v \\ w &\mapsto (w)a^{\varphi\epsilon} := w \\ z &\mapsto (z)a^{\varphi\epsilon} := z \end{aligned}$$

$$\begin{aligned} b^\varphi \ \mapsto \ b^{\varphi\epsilon} &: H \to H \\ a &\mapsto (a)b^{\varphi\epsilon} := au \\ b &\mapsto (b)b^{\varphi\epsilon} := bw \\ u &\mapsto (u)b^{\varphi\epsilon} := u^r \\ v &\mapsto (v)b^{\varphi\epsilon} := v \\ w &\mapsto (w)b^{\varphi\epsilon} := w \\ z &\mapsto (z)b^{\varphi\epsilon} := z \end{aligned}$$

Afirmação 2: A aplicação ϵ determina um homomorfismo de G^φ em $Aut(H)$.

Com o mesmo procedimento usado na demonstração da Afirmação 1, serão necessários 3 passos para a demonstração da Afirmação 2:

Passo 1: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Para isto, devemos mostrar que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ preservam as relações de H.

Como a aplicação $a^{\varphi\epsilon}$ fixa u, v, w e z de H, resta-nos avaliar se as relações de H são satisfeitas nos elementos av, $b(u^{-1}z)$. Já a aplicação $b^{\varphi\epsilon}$ fixa v, w e z de H e assim, devemos verificar se as relações de H são satisfeitas para os elementos au, bw, u^r e $u^{-r}z$ sabendo que $[u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1$ em H:

Para $a^{\varphi\epsilon}$:

$$(av)^m = v^m a^m = 1.$$

Como

$$(bu^{-1}z)^{ns} = w^{n^2} b^{ns}$$

e,

$$(av)^{s^2} = v^{s^2} a^{s^2} = v^{s^2} b^{ns},$$

onde

$$(v^s)^s = (u^{E_m(r,n)})^s = u^{s(1+r+\ldots+r^{n-1})} = u^{sn} = w^{nn},$$

pelas relações de H e também porque $sr \equiv s\ (mod\ m)$, segue que $w^{n^2} = v^{s^2}$. Portanto, $(av)^s = (bu^{-1}z)^n$.

Na equação
$$(av)^{bu^{-1}z} = (a^r v)^{u^{-1}} = (a^{u^{-1}})^r,$$
temos $(a^u) = a$ de tal forma que $a = (a^u)^{u^{-1}} = a^{u^{-1}}$ com $v^r = v \in H$. Portanto, $(av)^{bu^{-1}z} = a^r v = a^r v^r = (av)^r$.

$$(u)^{av} = u^a = u \quad \text{e} \quad (u)^{b(u^{-1}z)} = u^b = u^r,$$

finalizando esta análise.

Para b^f:
$$(au)^m = u^m a^m = 1.$$
$$(bw)^n = w^n b^n = u^s a^s = (au)^s.$$
$$(au)^{bw} = (a^r u^b) = a^r u^r = (au)^r.$$

Das relações envolvendo u^r e $u^{-r}z$ em H:
$$(u^r)^m = u^{rm} = 1.$$
$$((u^r)^{-1}z)^m = u^{-rm}z^m = 1.$$

Sabendo que $sr \equiv s\ (mod\ m)$, temos
$$(u^r)^s = u^{sr} = u^s,$$
$$((u^r)^{-1}z)^s = u^{-sr}z^{sr} = (u^{-1}z)^s = w^n,$$
$$(u^r)^{sk} = u^{srk} = u^{sk} = 1 \quad \text{e}$$
$$(u^{-r}z)^{sk} = u^{-srk}z^{sk} = (u^{-1}z)^{sk} = 1.$$

Mais ainda,
$$(u^r)^{E_m(r,o(b))} = u^{rE_m(r,o(b))} = u^{E_m(r,o(b))},$$
$$((u^r)^{-1}z)^{E_m(r,o(b))} = u^{-rE_m(r,o(b))}z^{E_m(r,o(b))} = (u^{-1}z)^{E_m(r,o(b))},$$
$$(u^r)^{E_m(r,n)} = u^{rE_m(r,n)} = u^{E_m(r,n)} \quad \text{e}$$
$$((u^r)^{-1}z)^{E_m(r,n)} = u^{-rE_m(r,n)}z^{E_m(r,n)} = (u^{-1}z)^{E_m(r,n)},$$
pois $n \mid o(b)$ e $r^n \equiv 1\ (mod\ m)$. Por fim,
$$(u^r)^{au} = (u^r)^a = u^r \quad \text{e} \quad (u^r)^{bw} = (u^b)^r = (u^r)^r,$$
$$(u^{-r}z)^{au} = (u^{-r}z)^a = u^{-r}z \quad \text{e} \quad (u^{-r}z)^{bw} = (u^b)^{-r}z = (u^{-r})^r z \quad .$$

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Passo 2: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são automorfismos de H.

Sendo a^f e b^f homomorfismos de H e H sendo um grupo finito, é suficiente verificar que

$$\langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle = H = \langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle,$$

uma vez que os homomorfismos $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ fixam v, w e z. Ou seja, a^f e b^f são epimorfismo.

A aplicação $a^{\varphi\epsilon}$ fixa u, v, w e z de H. Uma vez que $a = avv^{-1}$ e $b = b(u^{-1}z)(u^{-1}z)$, segue que $H = \langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle$.

Por outro lado, temos que $(u)b^{\varphi\epsilon} = u^r$ com $(m, r) = 1$. Então, existe um inteiro tal $u = u^{\mu r}$.

Logo, $(u^r)^\mu = u^{\mu r} = u$ e assim, obtemos $\langle (u)b^{\varphi\epsilon}, v, w, z\rangle = \langle u, v, w, z\rangle$. Por analogia ao caso anterior, $\langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle = H$, visto que $a = auu^{-1}$, $b = bww^{-1}$.

Portanto, $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são automorfismos de H.

Passo 3: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^φ.

Para isso, analisaremos $a^{\varphi\epsilon}$ aplicado em a e b, já que $a^{\varphi\epsilon}$ fixa u, v, w e z e $b^{\varphi\epsilon}$ aplicado em a, b e u, uma vez que esta fixa $v, w, z \in H$.

$$(a)[a^{\varphi\epsilon}]^2 = (av)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v)a^{\varphi\epsilon} = av^2,$$

$$(a)[a^{\varphi\epsilon}]^3 = (av^2)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v^2)a^{\varphi\epsilon} = av^3.$$

Indutivamente,

$$(a)[a^{\varphi\epsilon}]^\alpha = av^\alpha,$$

para qualquer $\alpha \in \mathbb{N}$.

$$(b)[a^{\varphi\epsilon}]^2 = (bu^{-1}z)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-1})a^{\varphi\epsilon}(z)a^{\varphi\epsilon} = bu^{-1}zu^{-1}z = b(u^{-1}z)^2,$$

$$(b)[a^{\varphi\epsilon}]^3 = (b(u^{-1}z)^2)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-2})a^{\varphi\epsilon}(z^2)a^{\varphi\epsilon} = bu^{-1}zu^{-2}z^2 = b(u^{-1}z)^3,$$

$$(b)[a^{\varphi\epsilon}]^4 = (b(u^{-1}z)^3)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-3})a^{\varphi\epsilon}(z^3)a^{\varphi\epsilon} = bu^{-1}zu^{-3}z^3 = b(u^{-1}z)^4.$$

Indutivamente,

$$(b)[a^{\varphi\epsilon}]^\alpha = b(u^{-1}z)^\alpha,$$

para qualquer $\alpha \in \mathbb{N}$.

$$(u)[b^{\varphi\epsilon}]^2 = (u^r)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} (u^r)^r = u^{r^2}$$

$$(u)[b^{\varphi\epsilon}]^3 = (u^{r^2})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} u^{r^3}$$

Indutivamente, temos que

$$(u)[b^{\varphi\epsilon}]^\beta = u^{r^\beta},$$

para qualquer $\beta \in \mathbb{N}$.

$$(a)[b^{\varphi\epsilon}]^2 = (au)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u)b^{\varphi\epsilon} = auu^r = au^{(r+1)},$$

$$(a)[b^{\varphi\epsilon}]^3 = (au^{(r+1)})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{(r+1)})b^{\varphi\epsilon} = au(u^r)^{E_m(r,2)} = au^{E_m(r,3)}.$$

$$(a)[b^{\varphi\epsilon}]^4 = (au^{E_m(r,3)})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{E_m(r,3)})b^{\varphi\epsilon} = au(u^r)^{E_m(r,3)} = au^{E_m(r,4)}$$

Indutivamente,

$$(a)[b^{\varphi\epsilon}]^\beta = au^{E_m(r,\beta)},$$

para qualquer $\beta \in \mathbb{N}$.

$$(b)[b^{\varphi\epsilon}]^2 = (bw)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w)b^{\varphi\epsilon} = bw^2$$

$$(b)[b^{\varphi\epsilon}]^3 = (bw^2)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w^2)b^{\varphi\epsilon} = bw^3.$$

Indutivamente,

$$(b)[b^{\varphi\epsilon}]^\beta = bw^\beta,$$

para qualquer $\beta \in \mathbb{N}$.

Em particular, para $\alpha = m$, obtemos as seguintes igualdades:

$$\begin{cases} (a)[a^{\varphi\epsilon}]^m = av^m = a \\ (b)[a^{\varphi\epsilon}]^m = b(u^{-1}z)^m = b, \end{cases}$$

ou seja, $[a^{\varphi\epsilon}]^m = Id_H$.

Mais ainda, fazendo $\beta = n$ e $\alpha = s$, temos que

$$\begin{cases} (u)[a^{\varphi\epsilon}]^s = u = u^{r^n} = (u)[b^{\varphi\epsilon}]^n \\ (a)[a^{\varphi\epsilon}]^s = av^s = au^{E_m(r,n)} = (a)[b^{\varphi\epsilon}]^n \\ (b)[a^{\varphi\epsilon}]^s = b(u^{-1}z)^s = bw^n = (b)[b^{\varphi\epsilon}]^n, \end{cases}$$

o que implica em $[a^{\varphi\epsilon}]^s = [b^{\varphi\epsilon}]^n$.

Para finalizar, como $b^{o(b)-1} = b^{-1}$, segue as seguintes identidades:

$$\begin{aligned} (u)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] &= [((u)b^{\varphi\epsilon})a^{\varphi\epsilon}]\, b^{\varphi\epsilon(o(b)-1)} \\ &= [((u)a^{\varphi\epsilon})^r]\, b^{\varphi\epsilon(o(b)-1)} = (u^{r^2})[b^{\varphi\epsilon(o(b)-1)}] \\ &= ((u)[b^{\varphi\epsilon(o(b)-1)}])^{r^2} = u^{r^{o(b)-1}rr} \\ &= u^r = (u)[a^{\varphi\epsilon}]^r \end{aligned}$$

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] &= (((a)b^{\varphi\epsilon})a^{\varphi\epsilon})\,[b^{\varphi\epsilon(o(b)-1)}] \\
&= (((a)a^{\varphi\epsilon})((u)a^{\varphi\epsilon}))\,[b^{\varphi\epsilon(o(b)-1)}] \\
&= (auv)[b^{\varphi\epsilon(o(b)-1)}] \\
&= (a)[b^{\varphi\epsilon(o(b)-1)}](u)[b^{\varphi\epsilon(o(b)-1)}](v)[b^{\varphi\epsilon(o(b)-1)}] \\
&= au^{(r-1)E_m(r,(o(b)-1))+1+E_m(r,(b)-1)}v \\
&= au^{E_m(r,(o(b)))}v = av^r \\
&= (a)[a^{\varphi\epsilon}]^r
\end{aligned}$$

A análise de que a relação $(b)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = (b)[a^{\varphi\epsilon}]^r$ ocorre é análogo.

Desta forma, concluímos que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^{φ}, ou seja,

$$[a^{\varphi\epsilon}]^m = Id_H, \qquad [b^{\varphi\epsilon}]^n = [a^{\varphi\epsilon}]^s, \qquad [b^{\varphi\epsilon}]^{-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = [a^{\varphi\epsilon}]^r.$$

Os Passos 1, 2, 3 e o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação ϵ se estende a um homomorfismo de G^{φ} para $Aut(H)$.

Obtemos então, via o homomorfismo $\epsilon : G^{\varphi} \to Aut(H)$, o produto semidireto de H por G^{φ} dado por

$$K = H \rtimes_{\epsilon} G^{\varphi} = (A \rtimes_f G) \rtimes_{\epsilon} G^{\varphi}.$$

Analogamente à apresentação do grupo H, pela **Proposição 1.6.10**, obtemos a apresentação para K dada por:

$$\begin{aligned}
\langle a, b, u, v, w, z, a^{\varphi}, b^{\varphi} \mid\ & a^m = 1, b^n = a^s, [a,b] = a^{r-1}, (a^{\varphi})^m = 1, (b^{\varphi})^n = (a^{\varphi})^s, \\
& [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{r-1}, u^a = u, u^b = u^r, u^{(m,E_m(r,o(b)),sk)} = 1, v^{o'(a)} = 1, \\
& w^{nk} = 1, z^{(o'(a),o'(b),sk,E_m(r,o'(b)))} = 1, u^s = w^n = (u^{-1}z)^s, a^{a^{\varphi}} = au, \\
& b^{a^{\varphi}} = b(u^{-1}z), u^{E_m(r,n)} = v^s = (u^{-1}z)^{E_m(r,n)}, u^{a^{\varphi}} = u, v^{a^{\varphi}} = v, \\
& w^{a^{\varphi}} = w, z^{a^{\varphi}} = z, a^{b^{\varphi}} = au, b^{b^{\varphi}} = bw, u^{b^{\varphi}} = u^r, v^{b^{\varphi}} = v, w^{b^{\varphi}} = w, \\
& z^{b^{\varphi}} = z, [u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1, \\
& (v, w, z \ \mathit{centrais})\rangle.
\end{aligned}$$

Desta apresentação observamos que as ações de G sobre o subgrupo (normal) $\langle u, v, w, z\rangle$ é a mesma que aquela de G^{φ}.

Consequentemente, trocando a por x_1, b por y_1, a^{φ} por x_2 e b^{φ} por y_2, concluímos que K possui precisamente a mesma apresentação do grupo M. Em outras palavras, $K \cong M$.

Agora, as ações de G sobre A e de G^{φ} sobre $H = A \rtimes_f G$ que definem o grupo K traduzem, respectivamente, as ações de G sobre $G \otimes G \cong [G, G^{\varphi}]$ (conforme **Proposição**

1.7.3 (i)) e de G sobre $(G \otimes G) \rtimes G$, as quais definem o grupo $\nu(G) = (\ [G, G^{\varphi}]\ G)\ G^{\varphi} \cong ((G \otimes G) \rtimes G) \rtimes G$. Por conseguinte, o dado epimorfismo $A \twoheadrightarrow [G, G^{\varphi}] \cong G \otimes G$ induz um epimorfismo de K sobre $\nu(G)$.

Consequentemente, a aplicação $\phi : M \to \nu(G)$ que associa $x_1 \mapsto a$, $y_1 \mapsto b$, $x_2 \mapsto a^{\varphi}$ e $y_2 \mapsto b^{\varphi}$ define um epimorfismo de M sobre $\nu(G)$.

Reciprocamente, a aplicação $\psi : \nu(G) \to M$ que associa $a \mapsto x_1$, $b \mapsto y_1$, $a^{\varphi} \mapsto x_2$ e $b^{\varphi} \mapsto y_2$ preserva as relações de $\nu(G)$, na sua apresentação dada pelo **Teorema 1.7.20**, haja vista as relações de conjugação decorrentes do **Lema 3.0.1**,

$$\begin{aligned}
[a, b^{\varphi}]^a &= [a, b^{\varphi}]^{a^{\varphi}} = [a, b^{\varphi}], \\
[a, b^{\varphi}]^b &= [a, b^{\varphi}]^{b^{\varphi}} = [a, b^{\varphi}]^r, \\
[a, a^{\varphi}]^a &= [a, a^{\varphi}]^{a^{\varphi}} = [a, a^{\varphi}]^b = [a, a^{\varphi}]^{b^{\varphi}} = [a, a^{\varphi}], \\
[b, b^{\varphi}]^a &= [b, b^{\varphi}]^{a^{\varphi}} = [b, b^{\varphi}]^b = [b, b^{\varphi}]^{b^{\varphi}} = [b, b^{\varphi}], \\
[b, a^{\varphi}]^a &= [b, a^{\varphi}]^{a^{\varphi}} = [b, a^{\varphi}], \\
[b, a^{\varphi}]^b &= [b, a^{\varphi}]^{b^{\varphi}} = [b, a^{\varphi}]^r.
\end{aligned}$$

das quais decorrem as relações definidoras de M, conforme **Proposição 3.1.5**.

Desta forma, os epimorfismos ϕ e ψ possuem inversas a direita, a saber, $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$. Obtemos, portanto, o então desejado isomorfismo $\nu(G) \cong M$ e fica assim demonstrado o **Teorema B**. □

A técnica usada para a demonstração dos **Teoremas A e B** é bastante conhecida na literatura como pode ser visto nos trabalhos de Rocco [[32],[34]]. Ainda sobre os **Teoremas A e B**, o seguinte Corolário nos dá uma apresentação para o grupo $\nu(G)$ quando $G = g(a, b; m, n, r, 0)$ é um grupo metacíclico finito, não abeliano e cindido:

Corolário 3.1.8. *Seja $G = g(x_1, y_1; m, n, r, 0)$ um grupo metacíclico finito, não abeliano.*

− Suponha m par:

(i) Se $r \neq m - 1$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}
\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = 1, y_2^n = 1, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, \\
& [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, \\
& v^{(m, 2(r-1))} = 1, w^n = 1, u^{(m, E_m(r,n))} = 1, u^{x_1} = u^{x_2} = uv^{r-1}, \\
& u^{y_1} = u^{y_2} = u^r v^{(r-1)\binom{r}{2}}, z^{(m, r-1, n, E_m(r,n))} = 1, \\
& (v, w, z \textit{ centrais})\rangle,
\end{aligned}$$

(ii) Se $r = m-1$, então uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = 1, y_2^n = 1, [x_1, y_1] = x_1^{m-2}, [x_2, y_2] = x_2^{m-2},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, w^n = 1,\\ & v^{(m,2(m-2))} = 1, z^{(m,m-2,n)} = 1, u^{x_1} = u^{x_2} = uv^{m-2},\\ & u^{(m,E_m(m-1,n))} = 1, u^{y_1} = u^{y_2} = u^{m-1}v^{(m-2)\binom{m-1}{2}}, (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

– Suponha m ímpar. Então, uma apresentação para o grupo $\nu(G)$ é dada por:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = 1, y_2^n = 1, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1},\\ & [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, w^n = 1,\\ & v^{(m,r-1)} = 1, z^{(m,r-1,n,E_m(r,n))} = 1, u^{x_1} = u^{x_1} = uv^{r-1},\\ & u^{y_1} = u^{y_2} = u^r v^{(r-1)\binom{r}{2}}, u^{(m,E_m(r,n))} = 1,\ (v, w, z \textit{ centrais})\rangle\end{aligned}$$

Como consequência das apresentações do grupo $\nu(G)$ dos **Teoremas A** e **B**, os seguintes Corolários, respectivamente, nos proporcionam um conjunto gerador para as seções abelianas do grupo $\nu(G)$, a saber, $[G, G^\varphi]$, $G \wedge G$ e $M(G)$ com suas relações definidoras. Por fim, respeitando as propriedades do grupo metacíclico finito, identificamos o grupo $\tau(G)$, seção não abeliana do grupo $\nu(G)$, a partir de sua apresentação.

Novamente, os grupos $\mu(G)$ e $\Delta(G)$ são centrais em $\nu(G)$ (vide **Proposição 1.7.15** *(ii)* e **Lema 1.7.6**). Além disso, $[G, G^\varphi]/\mu(G) \cong G'$ e G' é cíclico, implicando em $[G, G^\varphi]$ e $G \wedge G$ serem grupos abelianos. Com um argumento análogo, também temos que o grupo $M(G)$ é cíclico.

Corolário 3.1.9. *Seja $G = g(x_1, y_1; m, n, r, s)$ um grupo metacíclico finito, não abeliano e não cindido com m par.*

– Suponha que k seja ímpar.

(1) Se $2 \nmid s$ ou $4 \mid s$, então:

$$\begin{aligned}(i)\ [G, G^\varphi] = \langle u, v, w, z \mid\ & u^{(m,sk)} = 1, v^{(m,2(r-1))} = 1, w^{nk} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}},\\ & z^{(o'(x_1),o'(y_1),sk,E_m(r,o'(y_1)))} = 1, u^s = w^n = (u^{-1}z)^s, [u, z] = [w, z] = 1,\\ & (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, [v, w] = 1,\\ & (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, [u, v] = 1, [u, w] = 1, [v, z] = 1\rangle.\end{aligned}$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(r,n),s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m,E_m(r,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

(2) *Se* $2 \parallel s$, *então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid u^s v^{r-1} = w^n = (u^{-1}z)^s v^{1-r}, [u, w] = 1, u^{E_m(r, o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, u^{(m,2sk)} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, z^{(o'(x_1), o'(y_1), sk, E_m(r, o'(y_1)))} = 1, v^{(m, 2(r-1))} = 1, (u^{-1}z)^{E_m(r, o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, [u, v] = 1, w^{nk} = 1, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

– *Suponha que* k *seja par.*

(3) *Se* $2 \nmid s$ *ou* $4 \mid s$, *então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid u^{(m,sk)} = 1, (u^{-1}z)^{E_m(r, o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, v^{(m,2(r-1))} = 1, w^{nk} = 1, z^{(o'(x_1), o'(y_1), sk/2, E_m(r, o'(y_1)))} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, u^s = w^n = (u^{-1}z)^s, [u, v] = [u, w] = 1, u^{E_m(r, o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

(4) *Se* $2 \parallel s$, *então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid u^s v^{r-1} = w^n = (u^{-1}z)^s v^{1-r}, w^{nk} = 1, u^{E_m(r, o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}} u^{(m,sk)} = 1, z^{(o'(x_1), o'(y_1), sk/2, E_m(r, o'(y_1)))} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(r, o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, v^{(m,2(r-1))} = 1, [v, w] = [u, v] = [u, w] = [u, z] = 1, [v, z] = [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m, E_m(r,n), s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

Demonstração. Faremos a demonstração apenas do item (1).

Seja A um grupo abeliano dado por

$$\langle u, v, w, z \mid u^{(m,sk)} = 1, v^{(m,2(r-1))} = 1, w^{nk} = 1, z^{(o'(x_1), o'(y_1), sk, E_m(r, o'(y_1)))} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(r, o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, w^n = (u^{-1}z)^s, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, u^{E_m(r, o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, u^s = w^n, [u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle.$$

O **Teorema A** e as relações entre os elementos de $[G, G^{\varphi}]$ garantidas pelo **Lema 3.0.1** estabelecem o epimorfismo entre A e $[G, G^{\varphi}] \cong G \otimes G$. Por conseguinte, garantimos o epimorfismo de M_1 sobre $\nu(G)$.

Uma vez estabelecido o isomorfismo entre M_1 e $\nu(G)$, pela própria estrutura do grupo $\nu(G)$, segue o isomorfismo entre o grupo A, subgrupo de M_1, e $[G, G^{\varphi}]$.

A apresentação do grupo $G \wedge G$ é deduzida da apresentação do grupo $[G, G^{\varphi}]$ módulo $\Delta(G)$. Desta forma, relações como $u^s = (u^{-1}z)^s = w^n$ e $u^{E_m(r,n)} = v^{s-\binom{n}{2}\frac{(r-1)^2}{2}}$ ditam exatamente sobre a ordem do elemento gerador do grupo cíclico $G \wedge G$, já que este é isomorfo ao quociente $[G, G^{\varphi}]/\Delta(G)$.

Uma vez calculada a ordem do grupo $G \wedge G$ e sendo G' um grupo cíclico isomorfo ao quociente de $G \wedge G$ por $M(G)$ segue que

$$\begin{aligned} |M(G)| &= \frac{(m, E_m(r,n), s)}{\frac{m}{(m,r-1)}} \\ &= \frac{(m, r-1)}{m}(m, E_m(r,n), s), \end{aligned}$$

onde $|G'| = \dfrac{m}{(m, r-1)}$. □

Observação 3.1.9.1. *A apresentação do grupo $[G, G^{\varphi}]$ juntamente com as propriedades do grupo G' para um grupo metacíclico finito G qualquer seriam suficientes para obter uma apresentação para o grupo $\mu(G)$, o núcleo da aplicação ρ' (veja **Proposição 1.7.15**). Entretanto, o grupo $\mu(G)$ não será explorado no caso em que o grupo G é metacíclico finito por envolver exaustivas e extensas relações entre os geradores $\langle u^{|G'|}, v, w, z\rangle$ do grupo $\mu(G)$ e as relações definidoras do grupo $[G, G^{\varphi}]$.*

A demonstração dos Corolários subsequentes serão omitidas por decorrerem de um raciocínio análogo ao Corolário antecedente.

Corolário 3.1.10. *Seja $G = g(x_1, y_1; m, n, m-1, s)$ um grupo metacíclico finito não cindido.*

– Suponha que $k = 1$:

(1) Se $2 \nmid s$ ou se $4 \mid s$, então:

(i) $$\begin{aligned} [G, G^{\varphi}] = \langle u, v, w, z \mid\ & u^{(m,s)} = 1, v^{(m,2(m-2))} = 1, w^n = 1, z^{(m,s,m-2,o'(y_1))} = 1, [u,w] = 1, \\ & u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}}, \\ & [u,v] = [u,z] = [v,w] = [v,z] = [w,z] = 1\rangle. \end{aligned}$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,m-2)}{m}(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

(2) *Se* $2 \parallel s$, *então:*

$$(i)\ \ [G, G^{\varphi}] = \langle u, v, w, z \mid u^{(m,2s)} = 1, v^{(m,2(m-2))} = 1, w^n = 1, (u^{-1}z)^s = v^{m-2}, u^s = v^{2-m}, \\ z^{(m,s,m-2,o'(y_1))} = 1, u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, [u,v] = [u,w] = 1, \\ (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}}, [u,z] = [v,w] = [v,z] = [w,z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,m-2)}{m}(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

− *Suponha que* $k = 2$:

(3) *Se* $2 \nmid s$ *ou se* $4 \mid s$, *então:*

$$(i)\ \ [G, G^{\varphi}] = \langle u, v, w, z \mid u^{(m,2s)} = 1, v^{(m,2(m-2))} = 1, w^{2n} = 1, z^{(m,s,m-2,o'(y_1))} = 1, [w,z] = 1, \\ u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, w^n = (u^{-1}z)^s = u^s, [u,v] = [u,w] = 1, \\ (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}}, [u,z] = [v,w] = [v,z] = 1, \rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid u^{(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,m-2)}{m}(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

(4) *Se* $2 \parallel s$, *então:*

$$(i)\ \ [G, G^{\varphi}] = \langle u, v, w, z \mid u^{(m,2s)} = 1, w^{2n} = 1, [w,z] = [u,w] = [u,z] = [v,w] = [v,z] = 1, \\ u^s v^{m-2} = w^n = (u^{-1}z)^s v^{2-m}, (u^{-1}z)^{E_m(m-1,n)} = v^{s+\frac{(m-2)^2}{2}\binom{n}{2}}, \\ z^{(m,s,m-2,o'(y_1))} = 1, u^{E_m(m-1,n)} = v^{s-\frac{(m-2)^2}{2}\binom{n}{2}}, v^{(m,2(m-2))} = 1, \\ [u,v] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $u := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,m-2)}{m}(m,E_m(m-1,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

Na particularização de m ímpar, segue um Corolário decorrente do **Teorema B**, análogo aos supracitados cuja demonstração será omitida.

Corolário 3.1.11. *Seja* $G = g(x_1, y_1; m, n, r, s)$ *um grupo metacíclico finito, não abeliano e não cindido com* m *ímpar. Então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid u^{(m,E_m(r,o(y_1)),sk)} = 1, v^{(m,r-1)} = 1, z^{(o'(x_1),o'(y_1),sk,E_m(r,o'(y_1)))} = 1, \\ w^{nk} = 1, u^s = w^n = (u^{-1}z)^s, u^{E_m(r,n)} = v^s = (u^{-1}z)^{E_m(r,n)}, \\ [u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(r,n),s)} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m,E_m(r,n),s)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

Para finalizar, temos o Corolário que identifica as seções (abelianas) do grupo $\nu(G)$ para o grupo metacíclico finito, não abeliano e cindido $G = g(a, b; m, n, r, 0)$:

Corolário 3.1.12. *Seja* $G = g(x_1, y_1; m, n, r, 0)$ *um grupo metacíclico finito não abeliano.*

– *Suponha que* $r \neq m - 1$*:*

(1) *Se* m *é par, então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid v^{(m,2(r-1))} = 1, w^n = 1, u^{(m,E_m(r,n))} = 1, z^{(m,r-1,n,E_m(r,n))} = 1,$$
$$[u, v] = [u, w] = [u, z] = [v, w] = [v, z] = [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(r,n))} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m,E_m(r,n))} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

(2) *Se* m *é ímpar, então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid v^{(m,r-1)} = 1, z^{(m,r-1,n,E_m(r,n))} = 1, u^{(m,E_m(r,n))} = 1, [w, z] = [v, z] = 1,$$
$$w^n = 1, [u, v] = [u, w] = [u, z] = [v, w] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(r,n))} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(m,r-1)}{m}(m,E_m(r,n))} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

– *Suponha que* $r = m - 1$*:*

(3) *Se* m *é par, então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid w^n = 1, v^{(m,2(m-2))} = 1, z^{(m,m-2,n,E_m(m-1,n))} = 1, [v, w] = [v, z] = 1,$$
$$u^{(m,E_m(m-1,n))} = 1, [w, z] = [u, z] = [u, w] = [u, v] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(m-1,n))} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{(m,m-2)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

(4) *Se* m *é ímpar, então:*

$$(i)\ [G, G^{\varphi}] = \langle u, v, w, z \mid w^n = 1, u^{(m,E_m(m-1,n))} = 1, [u, v] = [v, w] = [v, z] = [w, z] = 1,$$
$$v = 1, z = 1, [u, w] = [u, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^{(m,E_m(m-1,n))} = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{(m,m-2)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}}\Delta(G)$.

O seguinte Corolário nos dá uma apresentação do grupo $\tau(G)$, seção do grupo $\nu(G)$ para um grupo G metacíclico finito, não abeliano, além de dar sua identificação:

Corolário 3.1.13. *Seja $G = g(x_1, y_1; m, n, r, s)$ um grupo metacíclico finito e não abeliano:*

(1) *Se $s > 0$, então:*

$$\begin{aligned}\tau(G) = \langle x_1, y_1, x_2, y_2, u \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, \\ & [x_1, y_2] = u, u^{(m,E_m(r,n),s)} = 1, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u^r\rangle. \\ \cong\ & (C_m \times C_m \times C_{(m,E_m(r,o(b)),s)})\ ]\ (C_{o(b)} \times C_{o(b)}),\end{aligned}$$

onde “] ” denota o produto semidireto parcial.

(2) *Se $s = 0$, então:*

$$\begin{aligned}\tau(G) = \langle x_1, y_1, x_2, y_2, u \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, \\ & [x_1, y_2] = u, u^{(m,E_m(r,n))} = 1, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u^r\rangle. \\ \cong\ & (C_m \times C_m \times C_{(m,E_m(r,n))})\ ]\ (C_{o(b)} \times C_{o(b)}).\end{aligned}$$

Demonstração. Faremos apenas a demonstração do item (1) para o caso satisfazendo o **Teorema A** (i).

Sejam $H = \langle x_1, x_2, u\rangle$ e $K = \langle y_1, y_2\rangle$ subgrupos do grupo $\tau(G) = \nu(G)/\Delta(G)$.

Para o grupo $G = g(x_1, y_1; m, n, r, s)$ no **Teorema A**, temos $\nu(G)$ dado por:

$$\begin{aligned}\nu(G) \cong \langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, y_1^n = x_1^s, y_2^n = x_2^s, [x_1, y_1] = x_1^{r-1}, \\ & [x_2, y_2] = x_2^{r-1}, [x_1, y_2] = u, [x_1, x_2] = v, [y_1, y_2] = w, \\ & [y_1, x_2] = u^{-1}z, w^{nk} = 1, (u^{-1}z)^{E_m(r,o(y_1))} = v^{\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, \\ & u^{E_m(r,o(y_1))} = v^{-\frac{(r-1)^2}{2}\binom{o(y_1)}{2}}, z^{(o'(x_1),o'(y_1),sk,E_m(r,o'(y_1)))} = 1, \\ & v^{(m,2(r-1),\binom{s}{2}(r-1))} = 1, u^{E_m(r,n)} = v^{s-\frac{(r-1)^2}{2}\binom{n}{2}}, u^{(m,sk)} = 1, \\ & u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)}, u^{x_1} = u^{x_2} = uv^{r-1}, u^s = w^n, \\ & w^{=}(u^{-1}z)^s, (u^{-1}z)^{E_m(r,n)} = v^{s+\frac{(r-1)^2}{2}\binom{n}{2}}, (v, w, z\ centrais)\rangle.\end{aligned}$$

Pelas relações definidoras do grupo $\nu(G)$, temos que $v = w = z = [u, x_1] = [u, x_2] = u^{(m,E_m(r,n),s)} = 1$, módulo $\Delta(G)$ e $x_1^m = x_2^m = 1$. Logo,

$$H \cong C_m \times C_m \times C_{(m,E_m(r,n),s)} \qquad \text{e} \qquad K \cong C_{o(b)} \times C_{o(b)}.$$

Ainda das relações definidoras do grupo $\nu(G)$, temos que:

$$(x_1^s)^{y_1} = x_1^{sr} = y_1^{nr},\ x_1^{y_1^n} = x_1^{r^n} = x_1,\ (x_2^s)^{y_2} = x_2^{sr} = y_2^{nr},$$

$$x_1^{y_2} = x_1 u, \; x_2^{y_1^n} = x_2, \; (x_1^s)^{y_2} = x_1^s u^s.$$

Ou seja, $H \cap K = M$, $M = \langle y_1^n \rangle = \langle x_1^s \rangle$, normal em H. Portanto, $\tau(G) \cong H \rbrack K$, onde " $\rbrack$ " é o produto semidireto parcial.

A demonstração da identificação do grupo $\tau(G)$ nos outros casos é análoga. $\square$

Em 1970, Wamsley [[43], Lemma 1] mostrou que grupos metacíclicos finitos da forma $G = g(a, b; m, n, r, s)$, com $s > 0$, possuem multiplicador de Schur cíclico cuja ordem depende da quadra (m, n, r, s). Rocco [[32],§3.4], em 1994, bem como Wamsley, calculou a ordem do $M(G)$ de um grupo metacíclico finito G, não cindido, a partir de um conjunto gerador para o quadrado tensorial não abeliano, módulo $\Delta(G)$. A ordem então calculada por ambos coincide com a apresentada nos **Corolários 3.1.11** e **3.1.9** pois, pelo **Lema 3.1.1**, temos que

$$[a, b^\varphi]^s, [a, b^\varphi]^{E_m(r,n)} \in \Delta(G).$$

Logo, $M(G) \cong C_{\frac{(m,r-1)}{m}(m, E_m(r,n), s)}$, independente da paridade dos inteiros m e n.

Beyl [[5], página 147, §5] classificou os p-grupos metacíclicos de Schur, a menos de isomorfismo. Ou seja, classificou os p-grupos metacíclicos que possuem multiplicador de Schur trivial. No mesmo artigo, Beyl mostrou que grupos do tipo

$$\langle a, b \mid a^m = 1, b^n = a^{\frac{m}{(m,r-1)}}, a^b = a^r \rangle$$

possuem multiplicador de Schur trivial. Novamente, com os argumentos dos **Corolários 3.1.11** e **3.1.9** juntamente com o **Lema 3.1.1**, obtemos

$$M(G) \cong C_{\frac{(m,r-1)}{m}(m, E_m(r,n), \frac{m}{(m,r-1)})} = 1.$$

As seções abelianas do grupo $\nu(G)$ para grupos metacíclicos finitos, não abelianos, $G = g(a, b; m, n, r, 0)$, descritas por Johnson, D .L., [[10], (16) Proposition] quando m é par, bem como as descritas por Brown, R., Johnson, D .L. & Robertson, E. F., [[10], Proposition 15], quando m é ímpar, ambas obtidas a partir de uma abordagem por biderivação, coincidem com as que obtivemos no **Corolário 3.1.12**.

O cálculo das ordens de um conjunto gerador para o grupo $[G, G^\varphi]$ quando $G = g(a, b; m, 2, m-1, 0)$ já havia sido feito por Brown, Johnson & Robertson [[10], Proposition 12], quando m é par e m é ímpar, cujas ordens coincidem com as calculadas no **Corolário 3.1.8** (i) de (3) e (4). A estratégia usada por eles foi considerar o grupo diedral $\mathcal{D}_m$ como a extensão central do grupo dos quatérnios generalizado $\mathcal{Q}_m$.

Cabe frisar que uma das técnicas utilizadas até então para o cálculo de objetos algébricos, como o quadrado tensorial não abeliano, consistia da construção de uma biderivação ou ainda, na verificação das ordens de cada um dos elementos geradores a partir das propriedades do grupo. Esta última técnica foi utilizada por Brown, Johnson & Robertson [[10], Proposition 13] e Johnson [[23], Proposition 16], por exemplo. A vantagem da técnica apresentada neste trabalho é que conseguimos a identificação de tantos outros objetos algébricos de interesse em outras áreas da Matemática. Ou seja, a partir da investigação de cotas para as ordens dos elementos de um conjunto gerador para o quadrado tensorial não abeliano, vendo $[G, G^{\varphi}] \cong G \otimes G$ como subgrupo normal de $\nu(G)$, foi possível obter relações cruciais para a geração do mesmo e de suas seções. O interesse algébrico e computacional na obtenção do nosso principal objeto de estudo, o grupo $\nu(G)$ de um grupo dado G é que, além de suas seções relevantes, este herda as propriedades do grupo, sendo também policíclico (logo computável), uma vez que o grupo dado inicialmente seja policíclico ou solúvel finito.

Para os exemplos a seguir, nos preocupamos em calcular os grupos $\nu(G)$, $[G, G^{\varphi}]$, $G \wedge G$, $M(G)$ e $\tau(G)$ de um grupo metacíclico finito G seguindo a própria literatura disponível. O único Exemplo aleatoriamente escolhido tem interesse teórico e computacional por ter sido feito no sistema GAP [18]:

Exemplo 3.1.14. *Para $\alpha \geq 2$, quatérnio generalizado $G = g(x, y; 2^{\alpha}, 2, 2^{\alpha} - 1, 2^{\alpha-1})$ possui $o'(x) = (2^{\alpha}, 2) = 2$, $o(y) = 4$ e $o'(y) = 2$, como calculamos no **Exemplo 2.1.7**.*

Considere $G = g(x, y; 2t, 2, 2t-1, t)$, $t > 1$, cuja apresentação foi dada por Carmichael [[11], páginas 181-182]. *Para $t = 2^{\alpha-1}$, o grupo G é o quatérnio generalizado supracitado.*

O valor de k é:

$$\begin{aligned} k &= \left(\frac{2t}{(2t,t)}, 2\frac{[t,2]}{(2t,t)}, 2\frac{[t,2]^2}{(2t,t)^2}, 2, 0\right) \\ &= \left(2, \frac{4}{(2,t)}, \frac{8}{(2,t)^2}\right) \\ &= 2, \end{aligned}$$

independente da paridade de t.

*Suponha que $2 \nmid t$ ou $4 \mid t$. Então, pelo **Corolário 3.1.7**, $\nu(G)$ é dado por:*

$$\begin{aligned} \langle x, y, x^{\varphi}, y^{\varphi}, u, v, w, z \mid\ & x^{2t} = 1, (x^{\varphi})^{2t} = 1, y^2 = x^t, (y^{\varphi})^2 = (x^{\varphi})^t, [x^{\varphi}, y^{\varphi}] = (x^{\varphi})^{2t-2}, \\ & [x, y^{\varphi}] = u, [x, x^{\varphi}] = v, [y, y^{\varphi}] = w, [y, x^{\varphi}] = u^{-1}z, u^{2t} = 1, \\ & v^{(2t, 2(2t-2), \binom{t}{2}(2t-2))} = 1, w^4 = 1, u^{E_{2t}(2t-1,2)} = v^{2-t}, [x, y] = x^{2t-2}, \\ & u^y = u^{y^{\varphi}} = u^{2t-1} v^{\binom{2t-1}{2}(2t-2)}, u^x = u^{x^{\varphi}} = uv^{2t-2}, z^{(2t,t,2t-2,2)} = 1, \\ & u^t = w^2 = (u^{-1}z)^t, (u^{-1}z)^{E_{2t}(2t-1,2)} = v^{3t-2}, u^{E_{2t}(2t-1,4)} = v^{12(1-t)}, \\ & (u^{-1}z)^{E_{2t}(2t-1,4)} = v^{12(t-1)},\ (v, w, z \textit{ centrais})\rangle, \end{aligned}$$

cujas seções abelianas são dadas pelo ***Corolário 3.1.10:***

$$\begin{aligned}[G,G^{\varphi}] = \langle u,v,w,z \mid\ & u^{2t}=1, v^{(2t,2(2t-2),\binom{t}{2}(2t-2))}=1, w^4=1, [u,w]=[u,z]=[v,z]=1,\\ & u^y = w^2 = (u^{-1}z)^t, u^{2t} = v^{t-\frac{(2t-2)^2}{2}}, [z,w]=[v,w]=[u,v]=1,\\ & z^{(2t,t,2t-2,2)}=1, (u^{-1}z)^{E_{2t}(2t-1,4)} = v^{6\frac{(2t-2)^2}{2}},\\ & (u^{-1}z)^{2t} = v^{t+\frac{(2t-2)^2}{2}}, u^{E_{2t}(2t-1,4)} = v^{6\frac{(2-2t)^2}{2}}\rangle.\end{aligned}$$

$G \wedge G = \langle \bar{u} \mid \bar{u}^t = 1\rangle.$

O grupo $M(G)$ é sempre trivial, segundo a tabela dada por Brown, Johnson & Robertson [[10], páginas 96 − 97], *que coincide com a nossa apresentação*

$$M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(2t,2t-2)}{2t}t} = 1\rangle = 1,$$

com $\bar{u} := u^{\frac{2t}{(2t,2t-2)}}\Delta(G).$

Já o grupo $\tau(G)$ é dado por:

$$\begin{aligned}\tau(G) &= \langle x,y,x^{\varphi},y^{\varphi},u \mid x^{2t}=1, (x^{\varphi})^{2t}=1, y^2=x^t, (y^{\varphi})^2=(x^{\varphi})^{2t}, [x,y]=x^{2t-2},\\ &\qquad [x^{\varphi},y^{\varphi}] = (x^{\varphi})^{2t-2}, [x,y^{\varphi}]=u, u^t=1, u^x = u^{x^{\varphi}} = u,\\ &\qquad u^y = u^{y^{\varphi}} = u^{-1}\rangle\\ &\cong (C_{2t}\times C_{2t}\times C_t) \rtimes (C_4\times C_4),\end{aligned}$$

pelo ***Corolário 3.1.13****.*

Para finalizar, suponha que $2 \parallel t$. Então, pelo ***Corolário 3.1.7***

$$\begin{aligned}\langle x_1,y_1,x_2,y_2,u,v,w,z \mid\ & x_1^{2t}=1, x_2^{2t}=1, y_1^2=x_1^t, y_2^2=x_2^t, [x_1,y_1]=x_1^{2t-2}, [x_2,y_2]=x_2^{2t-2},\\ & [x_1,y_2]=u, [x_1,x_2]=v, [y_1,y_2]=w, [y_1,x_2]=u^{-1}z, u^{2t}=1,\\ & v^{(2t,2(2t-2))}=1, w^4=1, u^{2t}=v^{t-\frac{(2t-2)^2}{2}}, z^{(2t,t,2t-2,2)}=1,\\ & u^{y_1}=u^{y_2}=u^{2t-1}v^{\binom{2t-1}{2}(2t-2)}, u^{x_1}=u^{x_2}=uv^{2t-2}, u^tv^{2t-2}=w^2,\\ & u^{E_{2t}(2t-1,4)} = v^{3(2-2t)^2}, w^2=(u^{-1}z)^tv^{2-2t}, (u^{-1}z)^{2t}=v^{t+\frac{(2t-2)^2}{2}},\\ & (u^{-1}z)^{E_{2t}(2t-1,4)} = v^{3(2t-2)^2},\ (v,w,z \textit{ centrais})\rangle.\end{aligned}$$

cujas seções abelianas são dadas pelo ***Corolário 3.1.10:***

$$\begin{aligned}[G,G^{\varphi}] = \langle u,v,w,z \mid\ & u^{2t}=1, v^{(2t,2(2t-2))}=1, w^4=1, u^tv^{2t-2}=w^2=(u^{-1}z)^tv^{2-2t},\\ & u^{2t}=v^{t-\frac{(2t-2)^2}{2}}, [u,z]=[v,w]=[v,z]=[w,z]=[u,v]=[u,w]=1,\\ & z^{(2t,t,2t-2,2)}=1, u^{E_{2t}(2t-1,4)}=v^{3(2-m)^2}, (u^{-1}z)^{E_{2t}(2t-1,4)}=v^{3(m-2)^2},\\ & (u^{-1}z)^{2t}=v^{t+\frac{(2t-2)^2}{2}}\rangle.\end{aligned}$$

$G \wedge G = \langle \bar{u} \mid \bar{u}^t = 1 \rangle$ *e*

$M(G) = \langle \bar{u} \mid \bar{u}^{\frac{(2t,2t-2)}{t}} = 1 \rangle = 1,$ *com* $\bar{u} := u^{\frac{2t}{(2t,2t-2)}} \Delta(G).$

Por fim, pelo ***Corolário 3.1.13****,*

$$\begin{aligned}\tau(G) &= \langle x, y, x^{\varphi}, y^{\varphi}, u \mid x^{2t} = 1, (x^{\varphi})^{2t} = 1, y^2 = x^t, (y^{\varphi})^2 = (x^{\varphi})^{2t}, [x, y] = x^{-2},\\ &\qquad [x^{\varphi}, y^{\varphi}] = (x^{\varphi})^{-2}, u = [x, y^{\varphi}], u^t = 1, u^x = u^{x^{\varphi}} = u,\\ &\qquad u^y = u^{y^{\varphi}} = u^{-1} \rangle\\ &\cong (C_{2t} \times C_{2t} \times C_t) \rtimes (C_4 \times C_4).\end{aligned}$$

Exemplo 3.1.15. *O grupo diedral finito* $G = g(a, b; m, 2, m-1, 0)$ *do* ***Exemplo 2.1.8*** *possui* $o'(b) = o(b) = 2$ *e,* $o'(a) = 1$*, se* m *é ímpar e* $o'(a) = 2$*, se* m *é par.*

Se m *é ímpar então, pelo* ***Corolário 3.1.8****,* $\nu(G)$ *é dado por*

$$\begin{aligned}\langle a, b, a^{\varphi}, b^{\varphi}, u, v, w, z \mid\ & a^m = 1, (a^{\varphi})^m = 1, b^2 = 1, (b^{\varphi})^2 = 1, [a, b] = a^{m-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{m-2},\\ & [a, b^{\varphi}] = u, [a, a^{\varphi}] = v, [b, b^{\varphi}] = w, [b, a^{\varphi}] = u^{-1}z, u^m = 1, w^2 = 1,\\ & v^{(m,m-2)} = 1, u^a = u^{a^{\varphi}} = uv^{m-2}, u^b = u^{b^{\varphi}} = u^{m-1}v^{(m-2)\binom{m-1}{2}},\\ & z = 1,\ (v, w, z \text{ centrais}) \rangle.\end{aligned}$$

As seções abelianas do grupo $\nu(G)$*, baseadas no* ***Corolário 3.1.12****, são:*

$$[G, G^{\varphi}] = \langle u, v, w, z \mid u^m = 1, v = 1, w^2 = 1, z = 1, [u, w] = 1 \rangle,$$

como Brown, Johnson & Robertson [[10], Proposition 14] *já haviam demonstrado. Ademais,*

$G \wedge G = \langle \bar{u} \mid \bar{u}^m = 1 \rangle.$

$M(G) = \langle \bar{u} \mid \bar{u}^{(m,m-2)} = 1 \rangle = 1,$ *onde* $\bar{u} := u^{\frac{m}{(m,m-2)}} \Delta(G).$

Como seção não abeliana, o grupo $\nu(G)$ *possui o grupo* $\tau(G)$ *cuja apresentação é:*

$$\tau(G) = \langle a, b, a^{\varphi}, b^{\varphi}, u \mid a^m = 1, (a^{\varphi})^m = 1, b^2 = 1, (b^{\varphi})^2 = 1, [a, b] = a^{-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{-2},$$

$$u = [a, b^{\varphi}], u^m = 1, u^a = u^{a^{\varphi}} = u, u^b = u^{b^{\varphi}} = u^{-1} \rangle$$

$$\cong C_m^3 \rtimes C_2^2.$$

Se m *é par então, pelo* ***Corolário 3.1.8****,*

$$\begin{aligned}\langle a, b, a^{\varphi}, b^{\varphi}u, v, w, z \mid\ & a^m = 1, (a^{\varphi})^m = 1, b^n = 1, (b^{\varphi})^n = 1, [a, b] = a^{m-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{m-2},\\ & [a, b^{\varphi}] = u, [a, a^{\varphi}] = v, [b, b^{\varphi}] = w, [b, a^{\varphi}] = u^{-1}z, v^{(m,2(m-2))} = 1,\\ & w^2 = 1, z^2 = 1, u^a = u^{a^{\varphi}} = uv^{m-2}, u^b = u^{b^{\varphi}} = u^{m-1}v^{(m-2)\binom{m-1}{2}},\\ & u^m = 1,\ (v, w, z \text{ centrais}) \rangle,\end{aligned}$$

*e daí, segue pelo **Corolário 3.1.12**,*

$$[G,G^\varphi] = \langle u,v,w,z \mid u^m=1, v^{(m,2(m-2))}=1, w^2=1, z^2=1, [u,w]=[u,z]=[v,w]=1,$$
$$[u,v]=[v,z]=[w,z]=1\rangle,$$

como havia sido verificado por Brown, Johnson & Robertson [[10], Proposition 14]. *Mais ainda,*

$G \wedge G = \langle \bar{u} \mid \bar{u}^m = 1\rangle.$

$M(G) = \langle \bar{u} \mid \bar{u}^2 = 1\rangle.$

E por fim,

$$\tau(G) = \langle a,b,a^\varphi,b^\varphi,u \mid a^m=1,(a^\varphi)^m=1,b^2=1,(b^\varphi)^2=1,[a,b]=a^{-2},[a^\varphi,b^\varphi]=(a^\varphi)^{-2},$$
$$u=[a,b^\varphi], u^m=1, u^a=u^{a^\varphi}=u, u^b=u^{b^\varphi}=u^{-1}\rangle$$
$$\cong C_m^3 \rtimes C_2^2.$$

Exemplo 3.1.16. *O grupo semi-diedral (ou quasi diedral) $G = g(x,y;2^{t-1},2,2^{t-2}-1,0)$ possui $o'(y)=o(y)=o'(x)=2$, para todo $t>3$.*

*Pelo **Corolário 3.1.8**, uma apresentação para o grupo $\nu(G)$ é dada por:*

$$\begin{aligned}\langle x,y,x^\varphi,y^\varphi,u,v,w,z \mid\ & x^{2^{t-1}}=1,(x^\varphi)^{2^{t-1}}=1,y^2=1,(y^\varphi)^2=1,[x,y]=x^{2^{t-2}-2},u^{2^{t-1}}=1,\\ & [x,y^\varphi]=u,[x^\varphi,y^\varphi]=(x^\varphi)^{2^{t-2}-2},[x,x^\varphi]=v,[y,x^\varphi]=u^{-1}z,\\ & [y^\varphi,y^\varphi]=w, v^{(2^{t-1},2(2^{t-2}-2))}=1,w^2=1,z^2=1,u^x=u^{x^\varphi}=uv^{2^{t-2}-2},\\ & u^y=u^{y^\varphi}=u^{2^{t-2}-1}v^{(2^{t-2}-2)\binom{2^{t-2}}{2}},u^{1+2^{t-1}}=v^{\frac{(2-2^{t-2})2}{2}},\\ & (u^{-1}z)^{1+2^{t-1}}=v^{\frac{(2^{t-2}-2)2}{2}},\ (v,w,z\ \textit{centrais})\rangle,\end{aligned}$$

*Novamente, pelo **Corolário 3.1.12**, temos:*

$$\begin{aligned}[G,G^\varphi] = \langle u,v,w,z \mid\ & u^{2^{t-1}}=1, v^{(2^{t-1},2(2^{t-2}-2))}=1, u^{2^{t-2}}=v^{\frac{(2-2^{t-2})2}{2}}, z^2=1, w^2=1,\\ & (u^{-1}z)^{2^{t-2}}=v^{\frac{(2^{t-2}-2)2}{2}},[u,w]=[u,z]=[v,w]=[v,z]=1,\\ & [u,v]=[w,z]=1\rangle.\end{aligned}$$

$G \wedge G = \langle \bar{u} \mid \bar{u}^{2^{t-1}} = 1\rangle.$

$M(G) = \langle \bar{u} \mid \bar{u}^{(2^{t-1},2^{t-2})} = 1\rangle.$

*E, para finalizar, pelo **Corolário 3.1.13**,*

$$\begin{aligned}\tau(G) &= \langle x,y,x^\varphi,y^\varphi,u \mid x^{2^{t-1}}=1,(x^\varphi)^{2^{t-1}}=1,y^2=1,(y^\varphi)^2=1,u^{2^{t-1}}=1\rangle\\ &\cong C_{2^{t-1}}^3 \rtimes C_2^2.\end{aligned}$$

Exemplo 3.1.17. *Considere $G = g(a, b; 16, 2, 15, 8)$ um grupo abstrato aleatório onde $o'(a) = 2$, $o(b) = 4$ e $o'(b) = 2$. Com a ajuda do GAP* [18]*, vamos verificar as ordens do conjunto gerador do quadrado tensorial não abeliano.*

Primeiramente, consideramos uma apresentação policíclica para G:

```
gap > f := FreeGroup(2);;
gap > x := f.1;; y := f.2;;
gap > R := [x^16, y^2/x^8, x^y/x^15];;
gap > h := f/R;; Definição do grupo
gap > j := Image(IsomorphismPcGroup(h));;
gap > g := Image(IsomorphismPcpGroup(j)); Aplicação que torna o grupo policíclico
gap > nag := NonAbelianTensorSquare(g); Cálculo do quadrado tensorial não abeliano
Pcp - group with orders [2, 2, 2, 2, 2, 4]
gap > neg := NonAbelianExteriorSquare(g); Cálculo do quadrado exterior
Pcp - group with orders [2, 2, 2]
gap > delta := Kernel(NonAbelianTensorSquareEpimorphism(g)); Grupo Δ(g)
Pcp - group with orders [2, 2, 2, 4]
gap > alpha := NonAbelianTensorSquareEpimorphism(g);;
gap > gamma := Range(alpha)!.epimorphism;;
gap > mu := Kernel(alpha * gamma); Grupo μ(g)
Pcp - group with orders [2,2,4]
gap > IsomorphismGroups(delta, mu);
[g14, g15, g16]- > [g14, g15, g16]
gap > AbelianInvariantsMultiplier(g); Grupo M(g)
[ ]
gap > nug := NonAbelianTensorSquarePlus(g); Grupo ν(g)
Pcp - group with orders [2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 4]
gap > AbelianInvariants(nug);
[2, 2, 2, 2]
```

Para evidenciar o fato de que a 'resposta' dada pelo GAP do grupo $\Delta(G)$ são os invariantes abelianos e não as ordens efetivas dos elementos geradores, confirmaremos nossas cotas a partir da definição (formal) do grupo $\nu(G)$:

```
gap > f := FreeGroup(4);;
gap > a := f.1;; b := f.2;; x := f.3;; y := f.4;;
gap > rel := [a^16, a^b/a^15, x^16, x^y/x^15, b^2/a^8, y^2/x^8, Comm(x, a)^a/Comm(x^x, a^a),
> Comm(x, a)^x/Comm(x^x, a^a), Comm(x, a)^b/Comm(x^y, a^b),
```

$> \mathtt{Comm(x,a)^y/Comm(x^y,a^b), Comm(x,b)^a/Comm(x^x,b^a)},$
$> \mathtt{Comm(x,b)^b/Comm(x^y,b^b), Comm(x,b)^x/Comm(x^x,b^a)},$
$> \mathtt{Comm(x,b)^y/Comm(x^y,b^b), Comm(y,a)^a/Comm(y^x,a^a)},$
$> \mathtt{Comm(y,a)^b/Comm(y^y,a^b), Comm(y,a)^x/Comm(y^x,a^a)},$
$> \mathtt{Comm(y,a)^y/Comm(y^y,a^b), Comm(y,b)^a/Comm(y^x,b^a)},$
$> \mathtt{Comm(y,b)^b/Comm(y^y,b^b), Comm(y,b)^x/Comm(y^x,b^a)},$
$> \mathtt{Comm(y,b)^y/Comm(y^y,b^b)}\ ];;$

```
gap > g := f/rel;;
gap > AbelianInvariants(g);
[2, 2, 2, 2]
gap > Order(Comm(g.1,g.3));
8
gap > Order(Comm(g.2,g.4));
8
gap > Order(Comm(g.1,g.4) * Comm(g.2,g.3));
4
gap > Order(Comm(g.1,g.4));
8
```

Observe que

$$k = \left(\frac{m}{(m,s)}, \frac{2[s,r-1]}{(m,s)}, \frac{n[s,r-1]^2}{(m,s)^2}, r-1, E_m(r,o(b))\right) = 2.$$

A partir da técnica usada no ***Teorema A****, daremos uma apresentação para o grupo $\nu(G)$, verificando também que o grupo abeliano A então definido é isomorfo ao grupo $[G,G^{\varphi}]$:*

Seja A o grupo com a seguinte apresentação

$$\begin{aligned}\langle u,v,w,z \mid\ & u^{16}=1, v^4=1, w^4=1, z^2=1, u^8=w^2, (u^{-1}z)^8=w^2, u^{16}=v^{-90},\\ & (u^{-1}z)^{16}=v^{106}, u^{3616}=v^{-588}, (u^{-1}z)^{3616}=v^{588},\\ & [u,v]=[u,w]=[u,z]=[v,w]=[v,z]=[w,z]=1\rangle.\end{aligned}$$

Defina $f: G \to Aut(A)$ como no ***Teorema A*** *e, não difícil ver que o grupo H, extensão de A por G, terá a seguinte apresentação:*

$$\begin{aligned}\langle a,b,u,v,w,z \mid\ & a^{16}=1, b^2=a^8, [a,b]=a^{14}, [a,b^{\varphi}]=u, [a,a^{\varphi}]=v, [b,a^{\varphi}]=u^{-1}z, u^{16}=1,\\ & b^{\varphi},b^{\varphi}]=w, v^4=1, w^4=1, z^2=1, u^a=uv^{14}, u^b=u^{15}v^{14\binom{15}{2}}, u^{16}=v^{-90},\\ & u^8=w^2, (u^{-1}z)^8=w^2, (u^{-1}z)^{16}=v^{106}, u^{3616}=v^{-588}, (u^{-1}z)^{3616}=v^{588},\\ & (v,w,z\ \textit{centrais})\rangle.\end{aligned}$$

Por fim, a partir da aplicalção $\epsilon : G^{\varphi} \to Aut(H)$, induzida de f, temos uma extensão K de H por G^{φ} dada por:

$$\begin{aligned}\langle a, b, a^{\varphi}, b^{\varphi}, u, v, w, z \mid\ & a^{16} = 1, (a^{\varphi})^{16} = 1, b^2 = a^8, (b^{\varphi})^2 = (a^{\varphi})^8, [a, b] = a^{14}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{14},\\ & [a, b^{\varphi}] = u, [a, a^{\varphi}] = v, [b, a^{\varphi}] = u^{-1}z, [b^{\varphi}, b^{\varphi}] = w, u^{16} = 1, u^{16} = v^{-90},\\ & v^4 = 1, w^4 = 1, z^2 = 1, u^a = u^{a^{\varphi}} = uv^{14}, u^b = u^{b^{\varphi}} = u^{15}v^{1470}, u^8 = w^2,\\ & (u^{-1}z)^8 = w^2, (u^{-1}z)^{16} = v^{106}, u^{3616} = v^{-588}, (u^{-1}z)^{3616} = v^{588},\\ & (v, w, z \ centrais)\rangle,\end{aligned}$$

que coincide com a proposta do grupo $\nu(G)$ do ***Corolário 3.1.7****, item (iii).*

Para finalizar, verificaremos o isomorfismo (computacional) entre o grupo A e o grupo $[G, G^{\varphi}]$:

```
gap > f := FreeGroup(4);
gap > u := f.1; ; v := f.2; ; w := f.3; ; z := f.4; ;
gap > r := [u^16, v^4, w^4, z^2, u^8/w^2, w^2/(u^-1 * z)^8, u^16/v^-90, (u^-1 * z)^16/v^106, u^3616/v^-588,
(u^-1 * z)^3616/v^588, Comm(u, v), Comm(u, w), Comm(u, z), Comm(v, w), Comm(v, z), Comm(w, z)]; ;
gap > nagg := f/r; ;
gap > IsomorphismGroups(nagg, nag);
[f.1^-4 * f.2^5 * f.3^-5 * f.4^5, f.1^-4 * f.2^4 * f.3^-3 * f.4^3, f.4, f.1^-1 * f.2 * f.3^-1 * f.4]- >
[g.13 * g.14 * g.15 * g.16 * g.18, g.13 * g.15 * g.16^3 * g.18, g.13 * g.16 * g.18,
g.11 * g.14 * g.15 * g.16^3 * g.19].
```

Este último Exemplo checa, computacionalmente, as apresentações dos grupos $\nu(G)$ e $[G, G^{\varphi}]$ para $G = g(a, b; 16, 2, 15, 8)$. Para verificar as outras seções do grupo $\nu(G)$, o trabalho é semelhante.

3.2 Grupos Metacíclicos Infinitos

Como fizemos na seção anterior, baseado nos resultados obtidos no **Capítulo** 2 a respeito dos grupos metacíclicos infinitos, $G = g(a, b; m, n, r)$, nos propomos a dar uma apresentação para o grupo $\nu(G)$ a partir do cálculo de uma cota para as ordens dos elementos $[a, b^{\varphi}]$, $[a, a^{\varphi}]$, $[b, b^{\varphi}]$ $[a, b^{\varphi}][b, a^{\varphi}]$ e as relações entre eles em $\nu(G)$. O fato do grupo G ser uma extensão cindida garante que a cota estabelecida para o conjunto gerador supracitado seja sufuciente para gerar o grupo $\nu(G)$, juntamente com as conjugações dos geradores de G sobre o tal conjunto. Como consequência, encontramos apresentações para suas seções abelianas $[G, G^{\varphi}]$, $G \wedge G$, $\mu(G)$ e $M(G)$, bem como a seção $\tau(G) = \nu(G)/\Delta(G)$, que podem ser vistas no diagrama (1.7).

Cotas para as ordens dos elementos de um conjunto gerador do quadrado tensorial não abeliano para um grupo metacíclico infinito, não abeliano, foram calculadas por Beuerle & Kappe [[3], Proposition 4.2] e verificadas nos Teoremas 4.3 e 4.4 do mesmo. Em seu trabalho, Beuerle & Kappe definem uma função no conjunto gerador supracitado envolvendo suas supostas ordens e mostram que ela é uma biderivação e que, portanto, as cotas são de fato ordens dos elementos em $G \otimes G$. Como aplicação, eles obtêm os grupos $G \wedge G$, $\mu(G)$ e $M(G)$. Nesta seção, além de obtermos os mesmos grupos a partir da apresentação do grupo $\nu(G)$, faremos o mesmo para o caso em que o grupo G é abeliano, caso não considerado por Beuerle & Kappe:

Proposição 3.2.1. *Seja $G = g(a, b; m, n, r)$ um grupo metacíclico infinito.*

(1) *Se $G = g(a, b; m, 0, r)$, então:*
(i) $[a, a^{\varphi}]$ tem ordem dividindo $(m, 2(r-1))$;
(ii) $[b, b^{\varphi}]$ tem ordem infinita;
(iii) $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo $(m, r-1)$;
(iv) $[a, b^{\varphi}]$ tem ordem dividindo m.

(2) *Se $G = g(a, b; 0, n, -1)$, então:*
(i) $[a, a^{\varphi}]$ tem ordem dividindo $(n, 4)$;
(ii) $[b, b^{\varphi}]$ tem ordem dividindo n;
(iii) $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo 2;
(iv) $[a, b^{\varphi}]$ tem ordem infinita.

(3) *Se $G = g(a, b; 0, n, 1)$ é abeliano, $n > 0$, então:*
(i) $[a, a^{\varphi}]$ tem ordem infinita;
(ii) $[b, b^{\varphi}]$ tem ordem dividindo n;
(iii) $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo n;
(iv) $[a, b^{\varphi}]$ tem ordem dividindo n.

Demonstração. (1) Considere $G = g(a, b; m, 0, r)$. Pelo **Lema 2.2.4**, sabemos que $o'(a) = (m, r-1)$ e $o'(b) = o(b)$ é infinito.
(i) O **Lema 1.7.10** (vi) nos garante que $o([a, a^{\varphi}]) \mid (o'(a)^2, 2o'(a))$. Como

$$1 = [a^m, a^{\varphi}] = [a, (a^m)^{\varphi}] = [a, a^{\varphi}]^m$$

segue que $[a, a^{\varphi}]$ tem ordem dividindo $(m, 2(r-1), (r-1)^2)$. Por outro lado,

$$[a, a^{\varphi}]^{r^2} = [a^r, (a^r)^{\varphi}] = [a^b, (a^b)^{\varphi}] = [a, a^{\varphi}]^b = [a, a^{\varphi}].$$

Ou seja, $[a, a^{\varphi}]^{1-r^2} = 1$. Como $(r-1)^2 + 1 - r^2 = -2r + 2 = 2(1-r)$, segue que $[a, a^{\varphi}]$ tem ordem dividindo $(m, 2(r-1))$.

(ii) Segue do fato de $o'(b)$ não ser finito, pelo **Lema 1.7.10** (vi).

(iii) O fato da ordem $o(a) = m$ implica em

$$\begin{aligned} 1 = [a^m, b^\varphi] &= [a, b^\varphi]^m [a, a^\varphi]^{\binom{m}{2}(r-1)} \\ &= [a, b^\varphi]^m [a^m, a^\varphi]^{\frac{(m-1)(r-1)}{2}} \\ &= [a, b^\varphi]^m, \end{aligned}$$

pois ou m é par, implicando em $r-1$ ser par, ou $m-1$ é par.

(iv) Pelo **Lema 1.7.10** (v), temos que $[a, b^\varphi][b, a^\varphi]$ tem ordem dividindo $(o'(a), o'(b)) = (m, r-1)$, já que $o'(b)$ é infinito.

(2) Suponha que $G = g(a, b; 0, n, -1)$.

Pelo **Teorema 2.2.2**, temos que n é par. Já pelo **Lema 2.2.4**, $o'(a) = (0, r-1) = 2$ e $o'(b) = o(b) = n$.
(i) Observe que $[a, a^\varphi]$ tem ordem divindo $(o'(a)^2, 2o'(a)) = 4$, pelo **Lema 1.7.10** (vi). Por outro lado,

$$\begin{aligned} 1 = [a, (b^n)^\varphi] &= [a, b^\varphi]^{E_0(-1,n)} [a, a^\varphi]^{(-2)\sum_{i=0}^{n-1} \binom{(-1)^i}{2}} \\ &= [a, a^\varphi]^n, \end{aligned} \tag{3.14}$$

pois $E_0(-1, n) = 1 + (-1) + \ldots + (-1)^{n-1} = 0$ e

$$\begin{aligned} \sum_{i=1}^{n-1} \binom{(-1)^i}{2} &= \sum_{i=1}^{n-1} \frac{(-1)^{2i} - (-1)^i}{2} \\ &= \frac{1}{2}[\underbrace{1 + 1 + \ldots + 1}_{n-1 \ vezes} - (-1)] \\ &= \frac{n}{2} \end{aligned}$$

(ii) Do **Lema 1.7.10** (vi), temos que $o([b, b^\varphi]) \mid (2n, n^2) = 2n$, pois $o'(b) = n$ e n é par. Por outro lado,

$$1 = [b^n, b^\varphi] = [b, b^\varphi]^n,$$

já que $o(b) = n$. Portanto, segue que $o([b, b^\varphi]) \mid (n, 2n) = n$, como queríamos demonstrar.

(iii) Suponha, por contradição, que existe $k \in \mathbb{Z}_+$ tal que $[a, b^\varphi]^k = 1$. Então, pela aplicação derivada, $\rho' : [G, G^\varphi] \longrightarrow G'$, temos que

$$1 = \rho'([a, b^\varphi]^k) = \rho'([a, b^\varphi])^k = [a, b]^k$$

O que é um absurdo pois G' é infinito. O fato de $1 = [a, (b^\varphi)^n]$ não influencia na ordem de $[a, b^\varphi]$, como pode ser visto na equação (3.14) do item (2)(i) acima.

(iv) Pelo **Lema 1.7.10** (v), temos que $o([a, b^{\varphi}][b, a^{\varphi}]) \mid (o'(a), o'(b)) = 2$, pois n é par.

(3) Se $G = g(a, b; 0, n, 1)$ é abeliano, temos $o'(a)$ infinito e $o'(b) = o(b) = n$, $n \geq 0$.

(ii) Do item (v) do **Lema 1.7.10**, temos que $[b, b^{\varphi}]$ tem ordem dividindo $(2n, n^2)$. Por outro lado,

$$1 = [b^n, b^{\varphi}] = [b, b^{\varphi}]^n$$

implicando em $o([b, b^{\varphi}]) \mid n$.

(iii) Pelo item (iv) do **Lema 3.0.1**, temos que

$$1 = [a, (b^n)^{\varphi}] = [a, b^{\varphi}]^{E_0(1,n)}[a, a^{\varphi}]^{(1-1)\sum_{i=0}^{n-1}\binom{1^i}{2}},$$

onde $E_0(1, n) = n$. Portanto, segue o resultado.

(iv) Para finalizar, pelo **Lema 1.7.10** (v), temos que $[a, b^{\varphi}][b, a^{\varphi}]$ tem ordem dividindo $(o'(a), o'(b)) = n$. □

A partir da investigação de cotas para as ordens dos elementos de um conjunto gerador para o grupo $[G, G^{\varphi}]$ quando G é um grupo metacíclico infinito, é possível identificar que não existem relações entre potências dos elementos do mesmo. Isto era de se esperar, uma vez que o grupo G é sempre cindido. Assim, baseado na **Proposição 3.2.1**, estamos aptos a propor uma apresentação para o grupo $\nu(G)$ quando G é um grupo metacíclico infinito:

Teorema C Seja $G = g(x_1, y_1; m, n, r)$ um grupo metacíclico infinito.

(1) Suponha que $m > 1$, $n = 0$ e $r \neq 1$, então uma apresentação para o grupo $\nu(G)$ é:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & x_1^m = 1, x_2^m = 1, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, [x_1, y_2] = u,\\ & [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^m = 1, v^{(m,2(r-1))} = 1,\\ & z^{(m,r-1)} = 1, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u^r v^{\binom{r}{2}(r-1)},\\ & (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(2) Suponha que $m = 0$, $n > 1$ e $r = -1$, então uma apresentação para o grupo $\nu(G)$ é:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & y_1^n = 1, y_2^n = 1, [x_1, y_1] = x_1^{-2}, [x_2, y_2] = x_2^{-2}, [x_1, y_2] = u,\\ & [x_1, x_2] = v, [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, v^{(n,4)} = 1, w^n = 1, z^2 = 1,\\ & u^{x_1} = u^{x_2} = uv^{-2}, u^{y_1} = u^{y_2} = u^{-1}v^{-2}\ (v, w, z \textit{ centrais})\rangle.\end{aligned}$$

(3) Suponha que $m = n = 0$ e $r = 1$, então uma apresentação para o grupo $\nu(G)$ é:

$$\begin{aligned}\langle x_1, y_1, x_2, y_2, u, v, w, z \mid\ & y_1^n = 1, y_2^n = 1, [x_1, y_1] = 1, [x_2, y_2] = 1, [x_1, y_2] = u, [x_1, x_2] = v,\\ & [y_1, y_2] = w, [y_1, x_2] = u^{-1}z, u^n = 1, z^n = 1, w^n = 1,\\ & (u, v, w, z \textit{ centrais})\rangle.\end{aligned}$$

Demonstração. Provaremos primeiramente que o grupo $\nu(G)$ é uma imagem homomórfica de M_1 dado pela apresentação do item (i). Para isso, usaremos a estrutura de $\nu(G) = (\Upsilon(G)\ G)\ G^\varphi$ conforme **Proposição 1.7.5** (ii) onde $G \cong \langle a, b\rangle$ e $G^\varphi \cong \langle a^\varphi, b^\varphi\rangle$.

O grupo $\Upsilon(G)$ é abeliano gerado pelos elementos $[a, b^\varphi]$, $[a, a^\varphi]$, $[b, b^\varphi]$ e $[a, b^\varphi][b, a^\varphi]$. Então, pela **Proposição 3.2.1** (página 96), vemos que $\Upsilon(G)$ é uma imagem homomórfica do grupo abeliano A definido por

$$\begin{aligned}\langle u, v, w, z \mid\ & u^m = 1, v^{(m,2(r-1))} = 1, z^{(m,r-1)} = 1, [u, v] = [u, w] = [u, z] = [v, w] = 1\\ & [v, z] = [w, z] = 1\rangle.\end{aligned}$$

As relações de M_1 nos levam a considerar a aplicação $f : G \to Aut(A)$ definida nos geradores, pondo:

$$\begin{array}{lllllll} a & \mapsto & a^f : A \to A & \qquad & b & \mapsto & b^f : A \to A \\ & & u \mapsto (u)a^f := uv^{(r-1)} & & & & u \mapsto (u)b^f := u^r v^{\binom{r}{2}(r-1)} \\ & & v \mapsto (v)a^f := v & & & & v \mapsto (v)b^f := v \\ & & w \mapsto (w)a^f := w & & & & w \mapsto (w)b^f := w \\ & & z \mapsto (z)a^f := z & & & & z \mapsto (z)f := z \end{array}$$

<u>Afirmação 1</u>: A aplicação f determina um homomorfismo de G em $Aut(A)$.

Serão necessários 3 passos para a demonstração da Afirmação 1:

<u>Passo 1</u>: a^f e b^f se estendem a homomorfismos de A.

Precisamos mostrar que as aplicações a^f e b^f preservam as relações de A.

As aplicações a^f e b^f fixam os elementos v, w e z. Desta forma, é suficiente analisar as relações de A para a aplicação a^f nos elementos uv^{r-1} e $(u^{-1}v^{-(r-1)})z$ e, os elementos $u^r v^{(r-1)\binom{r}{2}}$ e $(u^{-r}v^{-(r-1)\binom{r}{2}})z$ para a aplicação b^f. Lembre-se que $[u, v] = [u, w] = [u, z] = [v, z] = [v, w] = [w, z] = 1$ em A.

Para a^f:

$$(uv^{r-1})^m = u^m v^{m(r-1)} = 1.$$

$$\left((uv^{r-1})^{-1}z\right)^m = u^{-m}v^{-m(r-1)}z^m = 1,$$

Para b^f:

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^m = u^{rm}v^{m(r-1)\binom{r}{2}} = 1.$$

$$\left(\left(u^r v^{(r-1)\binom{r}{2}}\right)^{-1} z\right)^m = u^{-rm}v^{-m(r-1)\binom{r}{2}}z^m = 1.$$

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), a^f e b^f se estendem a homomorfismos de A.

Passo 2: a^f e b^f são automorfismos de A.

O fato do grupo A ser policíclico portanto Hopfiano nos diz que é suficiente garantir que a^f e b^f são epimorfismos (página 14).

Logo, basta verificar que

$$\langle (u)a^f, v, w, z\rangle = A = \langle (u)b^f, v, w, z\rangle,$$

uma vez que os homomorfismos a^f e b^f fixam v, w e z.

Como $\langle (u)a^f, v\rangle = \langle uv^{r-1}, v\rangle$, pela definição da aplicação a^f e, $\langle uv^{r-1}, v\rangle = \langle u, v\rangle$, visto que $u = uv^{(r-1)}v^{-(r-1)}$, é evidente que $A = \langle (u)a^f, v, w, z\rangle$.

Por outro lado, sendo $(u)b^f = u^r v^{(r-1)\binom{r}{2}}$ com m e r números relativamente primos, existem inteiros λ e μ tais que $1 = \lambda m + \mu r$, implicando em $u = u^{\mu r}$.

Logo,

$$(u^r v^{(r-1)\binom{r}{2}})^{\mu} = u^{\mu r} v^{\mu(r-1)\binom{r}{2}} = uv^{\mu(r-1)\binom{r}{2}}$$

e, por analogia ao caso anterior, vemos que $A = \langle (u)b^f, v, w, z\rangle$.

Portanto, a^f e b^f são automorfismos de A.

Passo 3: a^f e b^f satisfazem as relações de G.

É suficiente analisar a^f e b^f aplicado em $u \in A$, uma vez que ambas aplicações fixam v, w e z.

$$(u)[a^f]^2 = (uv^{r-1})a^f =_{a^f\ auto.} (u)a^f(v^{r-1})a^f = uv^{2(r-1)},$$
$$(u)[a^f]^3 = (uv^{2(r-1)})a^f =_{a^f\ auto.} (u)a^f(v^{2(r-1)})a^f = uv^{3(r-1)}.$$

Indutivamente,

$$(u)[a^f]^{\alpha} = uv^{\alpha(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$. Em particular, para $\alpha = m$, a identidade $(u)[a^f]^m = uv^{m(r-1)} = u$ implica em

$$[a^f]^m = Id_A.$$

$$\begin{aligned}
(u)[b^f]^2 &= (u^r v^{(r-1)\binom{r}{2}})b^f =_{b^f\ auto} (u^r)b^f(v^{(r-1)\binom{r}{2}})b^f = (u^r v^{(r-1)\binom{r}{2}})^r v^{(r-1)\binom{r}{2}} \\
&= u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} \\
(u)[b^f]^3 &= (u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}})b^f =_{b^f\ auto} (u^{r^2})b^f(v^{E_m(r,2)(r-1)\binom{r}{2}})b^f \\
&= (u^r v^{(r-1)\binom{r}{2}})^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} = u^{r^3} v^{E_m(r,3)(r-1)\binom{r}{2}}
\end{aligned}$$

Indutivamente, temos que

$$(u)[b^f]^{\beta} = u^{r^{\beta}} v^{E_m(r,\beta)(r-1)\binom{r}{2}},$$

para qualquer $\beta \in \mathbb{N}$.

A igualdade $(u)[b^f]^{-1} = u^{r^{o(b)-1}}$ ocorre pois $b^{-1} = b^{o(b)-1}$. Daí,

$$\begin{aligned}
(u)[[b^f]^{-1} \circ a^f \circ b^f] &= \left(\left((u)b^f\right) a^f\right) [b^{f^{-1}}] \\
&= \left((u^r v^{(r-1)\binom{r}{2}})a^f\right) [b^{f^{-1}}] \\
&= (u^r v^{r(r-1)+(r-1)\binom{r}{2}})[b^f]^{-1} \\
&= (u^{r^{o(b)-1}} v^{E_m(r,o(b)-1)(r-1)\binom{r}{2}})^r v^{r(r-1)+(r-1)\binom{r}{2}} \\
&= u^{r^{o(b)}} v^{(r-1)\left(r\binom{r}{2}E_m(r,o(b)-1)+r+\binom{r}{2}\right)} \\
&= u^r v^{r(r-1)},
\end{aligned}$$

pois

$$\begin{aligned}
(r-1)\left(r\binom{r}{2}E_m(r,o(b)-1)+r+\binom{r}{2}\right) &= (r-1)\left[\binom{r}{2}(rE_m(r,o(b)-1)+1)+r\right] \\
&= (r-1)\left[\binom{r}{2}E_m(r,o(b))+r\right] \\
&= \binom{r}{2}(r^{o(b)}-1)+r(r-1).
\end{aligned}$$

Mas $n \mid o(b)$ e $r^n \equiv 1 \ (mod\ m)$. Ou seja,

$$(u)[(b^f)^{-1} \circ a^f \circ b^f] = u^r v^{r(r-1)} = (uv^{r-1})^r = (u)[a^f]^r.$$

Logo, $[[b^{f^{-1}}] \circ a^f \circ b^f] = [a^f]^r$.

Desta forma, concluímos que a^f e b^f satisfazem as relações de G, ou seja,

$$[a^f]^m = Id_A, \qquad \left[[b^{f^{-1}}] \circ a^f \circ b^f\right] = [a^f]^r.$$

Os Passos 1, 2, 3 e o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação f se estende a um homomorfismo de G para $Aut(A)$, como queríamos constatar.

Podemos então formar o produto semidireto $H = A \rtimes_f G$ cuja apresentação é dada por:

$$\begin{aligned}
H = \langle a,b,u,v,w,z \mid\ & a^m = 1, [a,b] = a^{r-1}, u^m = 1, v^{(m,2(r-1))} = 1, z^{(m,r-1)} = 1, u^a = uv^{r-1}, \\
& [u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1, u^b = u^r v^{(r-1)\binom{r}{2}}, \\
& (v,w,z\ centrais)\rangle,
\end{aligned}$$

garantido pela **Proposição 1.6.10**.

A ação f de G sobre A induz uma aplicação $\epsilon : G^{\varphi} \to Aut(H)$ dada por:

$$\begin{array}{rcl} a^{\varphi} & \mapsto & a^{\varphi\epsilon} : H \to H \\ & & a \mapsto (a)a^{\varphi\epsilon} := av \\ & & b \mapsto (b)a^{\varphi\epsilon} := b(u^{-1}z) \\ & & u \mapsto (u)a^{\varphi\epsilon} := uv^{(r-1)} \\ & & v \mapsto (v)a^{\varphi\epsilon} := v \\ & & w \mapsto (w)a^{\varphi\epsilon} := w \\ & & z \mapsto (z)a^{\varphi\epsilon} := z \end{array} \qquad \begin{array}{rcl} b^{\varphi} & \mapsto & b^{\varphi\epsilon} : H \to H \\ & & a \mapsto (a)b^{\varphi\epsilon} := au \\ & & b \mapsto (b)b^{\varphi\epsilon} := bw \\ & & u \mapsto (u)b^{\varphi\epsilon} := u^r v^{(r-1)\binom{r}{2}} \\ & & v \mapsto (v)b^{\varphi\epsilon} := v \\ & & w \mapsto (w)b^{\varphi\epsilon} := w \\ & & z \mapsto (z)b^{\varphi\epsilon} := z \end{array}$$

Afirmação 2: A aplicação ϵ determina um homomorfismo de G^{φ} em $Aut(H)$.

Com o mesmo procedimento usado na demonstração da Afirmação 1, serão necessários 3 passos para a demonstração da Afirmação 2:

Passo 1: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Para isto, devemos mostrar que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ preservam as relações de H.

Como as aplicações $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ fixam v, w e z de H, devemos verificar que as relações de H são satisfeitas para os elementos av, $b(u^{-1}z)$, uv^{r-1} e $u^{-1}v^{-(r-1)}z$ de H, via aplicação $a^{\varphi\epsilon}$ e, para os elementos au, bw, $u^r v^{(r-1)}$ e $u^{-r}v^{-(r-1)\binom{r}{2}}$ via aplicação $b^{\varphi\epsilon}$, sabendo que $[u,v] = [u,w] = [u,z] = [v,w] = [v,z] = [w,z] = 1$ em H:

Para $a^{\varphi\epsilon}$:

$$(av)^m = v^m a^m = 1.$$

Na equação

$$(av)^{bu^{-1}z} = (a^r v)^{u^{-1}} = (a^{u^{-1}})^r v^{r(r-1)+1},$$

temos $(a^u) = av^{(1-r)}$ de tal forma que $a = (a^u)^{u^{-1}} = a^{u^{-1}}v^{1-r}$, onde $r(r-1)+1 = (r-1)(r-1)+r$. Portanto, $(av)^{bu^{-1}z} = a^r v^{r(r-1)+1} = a^r v^r = (av)^r$.

Por fim,

$$(uv^{r-1})^{av} = u^a v^{r-1} = (uv^{r-1})v^{r-1}$$

$$(uv^{r-1})^{b(u^{-1}z)} = u^b v^{r-1} = u^r v^{(r-1)\binom{r}{2}} v^{r-1} = (uv^{r-1})^r v^{(r-1)\binom{r}{2}},$$

já que $r-1 = r(r-1)-(r-1)^2$.

Das relações envolvendo uv^{r-1} e $u^{-1}v^{-(r-1)}z$ em H:

$$(uv^{r-1})^m = v^{m(r-1)}u^m = 1.$$

$$\left((uv^{r-1})^{-1}z\right)^m = v^{-m(r-1)}u^{-m}z^m = 1.$$

Para b^f:

$$(au)^m = u^m a^m = 1.$$

Da equação

$$[(au)^{bw}]^2 = [(a^r u^b)]^2 = [a^r u^r v^{(r-1)\binom{r}{2}}]^2 = u^{2r}a^{2r} = [(au)^r]^2,$$

obtemos $(au)^{bw} = (au)^r$.

Além disso,

$$(u^r v^{(r-1)\binom{r}{2}})^{au} = u^r v^{r(r-1)} v^{(r-1)\binom{r}{2}} = (u^r v^{(r-1)\binom{r}{2}})v^{r-1},$$

já que $r-1+(r-1)^2 = r(r-1)$ e

$$(u^r v^{(r-1)\binom{r}{2}})^{bw} = (u^r v^{(r-1)\binom{r}{2}})^r v^{(r-1)\binom{r}{2}}.$$

Das relações envolvendo $u^r v^{(r-1)\binom{r}{2}}$ e $u^{-r}v^{-(r-1)\binom{r}{2}}z$ em H:

$$\left(u^r v^{(r-1)\binom{r}{2}}\right)^m = u^{rm} v^{m(r-1)\binom{r}{2}} = 1.$$

$$\left((u^r v^{(r-1)\binom{r}{2}})^{-1} z\right)^m = u^{-rm} v^{-m(r-1)\binom{r}{2}} z^m = 1.$$

Logo, pelo Teste da Substituição (**Proposição 1.2.9**), $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ se estendem a homomorfismos de H.

Passo 2: $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são automorfismos de H.

Para verficar que ambos homomorfismos são sobrejetores, devemos verificar que

$$\langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle = H = \langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle,$$

já que os homomorfismos $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ fixam v, w e z.

Sabemos que $\langle (u)a^{\varphi\epsilon}, v\rangle = \langle uv^{r-1}, v\rangle$, pela definição da aplicação $a^{\varphi\epsilon}$ e, $\langle uv^{r-1}, v\rangle = \langle u, v\rangle$, uma vez que $u = uv^{(r-1)}v^{-(r-1)}$. Com um raciocínio semelhante, obtemos

$$\langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle = \langle a, b, u, v, w, z\rangle,$$

pois $(a)a^{\varphi\epsilon} = av$, $(b)a^{\varphi\epsilon} = b(u^{-1}z)$. Logo, $H = \langle (a)a^{\varphi\epsilon}, (b)a^{\varphi\epsilon}, (u)a^{\varphi\epsilon}, v, w, z\rangle$.

Por outro lado, como $(u)b^{\varphi\epsilon} = u^r v^{(r-1)\binom{r}{2}}$ com $(m, r) = 1$, existem inteiros λ e μ tais que $1 = \lambda m + \mu r$, implicando em $u = u^{\mu r}$.

Desta forma,

$$(u^r v^{(r-1)\binom{r}{2}})^{\mu} = u^{\mu r} v^{\mu(r-1)\binom{r}{2}} = uv^{\mu(r-1)\binom{r}{2}}$$

e, por analogia ao caso anterior, obtemos $\langle (u)b^{\varphi\epsilon}, v, w, z\rangle = \langle u, v, w, z\rangle$. Novamente, $\langle (a)b^{\varphi\epsilon}, (b)b^{\varphi\epsilon}, (u)b^{\varphi\epsilon}, v, w, z\rangle = H$, visto que $a = auu^{-1}$, $b = bww^{-1}$.

Logo, $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ são epimorfismos de H, uma vez que $b^{\varphi\epsilon}$ define um homomorfismo e sua imagem $\langle au, bw, u^r v^{(r-1)\binom{r}{2}}, v, w, z\rangle \leq H$ gera H.

O grupo $H = A \rtimes G$ é um grupo abeliano por metacíclico, finitamente apresentado e portanto policíclico. Assim sendo (página 14), temos que os epimorfismos $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ de H são automorfismos de H.

<u>Passo 3:</u> $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^{φ}.

Para isso, iremos analisar $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ aplicado em a, b e $u \in H$, uma vez que ambas aplicações fixam v, w e z.

$$(u)[a^{\varphi\epsilon}]^2 = (uv^{r-1})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (u)a^{\varphi\epsilon}(v^{r-1})a^{\varphi\epsilon} = uv^{2(r-1)},$$

$$(u)[a^{\varphi\epsilon}]^3 = (uv^{2(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (u)a^{\varphi\epsilon}(v^{2(r-1)})a^{\varphi\epsilon} = uv^{3(r-1)}.$$

Indutivamente,

$$(u)[a^{\varphi\epsilon}]^\alpha = uv^{\alpha(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$.

$$(a)[a^{\varphi\epsilon}]^2 = (av)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v)a^{\varphi\epsilon} = av^2,$$

$$(a)[a^{\varphi\epsilon}]^3 = (av^2)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (a)a^{\varphi\epsilon}(v^2)a^{\varphi\epsilon} = av^3.$$

Indutivamente,

$$(a)[a^{\varphi\epsilon}]^\alpha = av^\alpha,$$

para qualquer $\alpha \in \mathbb{N}$.

$$\begin{aligned}(b)[a^{\varphi\epsilon}]^2 &= (bu^{-1}z)a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-1})a^{\varphi\epsilon}(z)a^{\varphi\epsilon} = bu^{-1}zu^{-1}zv^{-(r-1)} \\ &= b(u^{-1}z)^2v^{-(r-1)},\end{aligned}$$

$$\begin{aligned}(b)[a^{\varphi\epsilon}]^3 &= (b(u^{-1}z)^2v^{-(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-2})a^{\varphi\epsilon}(z^2)a^{\varphi\epsilon}(v^{-(r-1)})a^{\varphi\epsilon} \\ &= bu^{-1}z(uv^{(r-1)})^{-2}z^2v^{-(r-1)} \\ &= b(u^{-1}z)^3v^{-3(r-1)},\end{aligned}$$

$$\begin{aligned}(b)[a^{\varphi\epsilon}]^4 &= (b(u^{-1}z)^3v^{-3(r-1)})a^{\varphi\epsilon} =_{a^{\varphi\epsilon}\ auto.} (b)a^{\varphi\epsilon}(u^{-3})a^{\varphi\epsilon}(z^3)a^{\varphi\epsilon}(v^{-3(r-1)})a^{\varphi\epsilon} \\ &= bu^{-1}z(uv^{(r-1)})^{-3}z^3v^{-3(r-1)} \\ &= b(u^{-1}z)^4v^{-6(r-1)}.\end{aligned}$$

Indutivamente,

$$(b)[a^{\varphi\epsilon}]^\alpha = b(u^{-1}z)^\alpha v^{-\binom{\alpha}{2}(r-1)},$$

para qualquer $\alpha \in \mathbb{N}$.

$$\begin{aligned}
(u)[b^{\varphi\epsilon}]^2 &= (u^r v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} (u^r)b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} = (u^r v^{(r-1)\binom{r}{2}})^r v^{(r-1)\binom{r}{2}} \\
&= u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} \\
(u)[b^{\varphi\epsilon}]^3 &= (u^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto} (u^{r^2})b^{\varphi\epsilon}(v^{E_m(r,2)(r-1)\binom{r}{2}})b^{\varphi\epsilon} \\
&= (u^r v^{(r-1)\binom{r}{2}})^{r^2} v^{E_m(r,2)(r-1)\binom{r}{2}} = u^{r^3} v^{E_m(r,3)(r-1)\binom{r}{2}}
\end{aligned}$$

Indutivamente, temos que

$$(u)[b^{\varphi\epsilon}]^\beta = u^{r^\beta} v^{E_m(r,\beta)(r-1)\binom{r}{2}},$$

para qualquer $\beta \in \mathbb{N}$.

$$(a)[b^{\varphi\epsilon}]^2 = (au)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u)b^{\varphi\epsilon} = auu^r v^{(r-1)\binom{r}{2}} = au^{(r+1)} v^{(r-1)\binom{r}{2}},$$

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^3 &= (au^{(r+1)} v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{(r+1)})b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} \\
&= au(u^r v^{(r-1)\binom{r}{2}})^{E_m(r,2)} v^{(r-1)\binom{r}{2}} \\
&= au^{E_m(r,3)} v^{\binom{r}{2}(r-1)(1+1+r)} = au^{E_m(r,3)} v^{(r-1)\left[\binom{r}{2}+\binom{r^2}{2}\right]},
\end{aligned}$$

onde

$$\binom{r}{2}(r-1)(1+1+r) \equiv (r-1)\left[\binom{r}{2}+\binom{r^2}{2}\right] \ (mod\ (m, 2(r-1)))$$

(vide **Proposição 3.1.3**).

$$\begin{aligned}
(a)[b^{\varphi\epsilon}]^4 &= (au^{E_m(r,3)} v^{\binom{r}{2}(r-1)})b^{\varphi\epsilon} \\
&=_{b^{\varphi\epsilon}\ auto.} (a)b^{\varphi\epsilon}(u^{E_m(r,3)})b^{\varphi\epsilon}(v^{(r-1)\binom{r}{2}})b^{\varphi\epsilon} \\
&= au(u^r v^{(r-1)\binom{r}{2}})^{E_m(r,3)} v^{(r-1)\binom{r}{2}} \\
&= au^{E_m(r,4)} v^{\binom{r}{2}(r-1)(1+r+r^2+1)} = au^{E_m(r,4)} v^{(r-1)\left[\binom{r}{2}+\binom{r^2}{2}+\binom{r^3}{2}\right]},
\end{aligned}$$

onde

$$\binom{r}{2}(r-1)(1+1+r+r^2) \equiv (r-1)\left[\binom{r}{2}+\binom{r^2}{2}+\binom{r^3}{2}\right] \ (mod\ (m, 2(r-1)))$$

(vide **Proposição 3.1.3**).

Indutivamente, teremos

$$(a)[b^{\varphi\epsilon}]^\beta = au^{E_m(r,\beta)} v^{(r-1)\sum_{i=1}^{\beta-1}\binom{r^i}{2}},$$

para qualquer $\beta \in \mathbb{N}$.

$$(b)[b^{\varphi\epsilon}]^2 = (bw)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w)b^{\varphi\epsilon} = bw^2$$

$$(b)[b^{\varphi\epsilon}]^3 = (bw^2)b^{\varphi\epsilon} =_{b^{\varphi\epsilon}\ auto.} (b)b^{\varphi\epsilon}(w^2)b^{\varphi\epsilon} = bw^3.$$

Indutivamente, temos que

$$(b)[b^{\varphi\epsilon}]^\beta = bw^\beta,$$

para qualquer $\beta \in \mathbb{N}$.

Em particular, para $\alpha = m$, obtemos as seguintes igualdades:

$$\begin{cases} (u)[a^{\varphi\epsilon}]^m = uv^{m(r-1)} = u \\ (a)[a^{\varphi\epsilon}]^m = av^m = a \\ (b)[a^{\varphi\epsilon}]^m = b(u^{-1}z)^m v^{-m(r-1)} = b, \end{cases}$$

ou seja, $[a^{\varphi\epsilon}]^m = Id_H$.

Para finalizar, como $b^{o(b)-1} = b^{-1}$, segue as seguintes identidades:

$$\begin{aligned} (u)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] &= (((u)b^{\varphi\epsilon})a^{\varphi\epsilon})\,[b^{\varphi\epsilon(o(b)-1)}] \\ &= \left(((u)a^{\varphi\epsilon})^r((v)a^{\varphi\epsilon})^{\binom{r}{2}(r-1)}\right)[b^{\varphi\epsilon(o(b)-1)}] \\ &= \left((uv^{r-1})^r v^{\binom{r}{2}(r-1)}\right)[b^{\varphi\epsilon(o(b)-1)}] \\ &= ((u)[b^{\varphi\epsilon(o(b)-1)}])^r((v)[b^{\varphi\epsilon(o(b)-1)}])^{(r-1)\left(\binom{r}{2}+r\right)} \\ &= uv^{r(r-1)} \\ &= (u)[a^{\varphi\epsilon}]^r \end{aligned}$$

O procedimento de análise das relações

$$(a)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = (a)[a^{\varphi\epsilon}]^r$$

$$(b)[b^{\varphi\epsilon}]^{o(b)-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = (b)[a^{\varphi\epsilon}]^r$$

é análogo.

Desta forma, concluímos que $a^{\varphi\epsilon}$ e $b^{\varphi\epsilon}$ satisfazem as relações de G^φ, ou seja,

$$[a^{\varphi\epsilon}]^m = Id_H, \qquad [b^{\varphi\epsilon}]^{-1} \circ [a^{\varphi\epsilon}] \circ [b^{\varphi\epsilon}] = [a^{\varphi\epsilon}]^r.$$

Os Passos 1, 2, 3 e o Teste da Substituição (**Proposição 1.2.9**) nos garantem que a aplicação ϵ se estende a um homomorfismo de G^φ para $Aut(H)$, como queríamos constatar.

Logo, via homomorfismo ϵ, obtemos o produto semidireto de H por G^φ dado por

$$K = H \rtimes_\epsilon G^\varphi = (A \rtimes_f G) \rtimes_\epsilon G^\varphi.$$

cuja apresentação, garantida pela **Proposição 1.6.10**, é dada por:

$$\begin{aligned} K = \langle a, b, u, v, w, z, a^\varphi, b^\varphi \mid\ & a^m = 1, [a,b] = a^{r-1}, (a^\varphi)^m = 1, [a^\varphi, b^\varphi] = (a^\varphi)^{r-1}, u^m = 1, \\ & v^{(m,2(r-1))} = 1, z^{(m,r-1)} = 1, a^{a^\varphi} = au, b^{a^\varphi} = b(u^{-1}z), u^{a^\varphi} = u, \\ & v^{a^\varphi} = v, w^{a^\varphi} = w, z^{a^\varphi} = z, a^{b^\varphi} = au, b^{b^\varphi} = bw, u^{b^\varphi} = u^r, \\ & v^{b^\varphi} = v, w^{b^\varphi} = w, z^{b^\varphi} = z,\ (v, w, z\ centrais)\rangle. \end{aligned}$$

Desta apresentação observamos que as ações de G sobre o subgrupo (normal) $\langle u, v, w, z\rangle$ é a mesma que aquela de G^{φ}.

Desta forma, trocando a por x_1, b por y_1, a^{φ} por x_2 e b^{φ} por y_2, concluímos que K possui precisamente a mesma apresentação do grupo M_1. Consequentemente obtemos o isomorfismo $K \cong M_1$.

Agora, as ações de G sobre A e de G^{φ} sobre $H = A \rtimes_f G$ que definem o grupo K traduzem, respectivamente, as ações de G sobre $G \otimes G \cong [G, G^{\varphi}]$ (conforme **Proposição 1.7.3** (i)) e de G sobre $(G \otimes G) \rtimes G$, as quais definem o grupo $\nu(G) = (\ [G, G^{\varphi}]\ G)\ G^{\varphi} \cong ((G \otimes G) \rtimes G) \rtimes G$. Por conseguinte, o dado epimorfismo $A \twoheadrightarrow [G, G^{\varphi}] \cong G \otimes G$ induz um epimorfismo de K sobre $\nu(G)$.

Consequentemente, a aplicação $\phi : M_1 \to \nu(G)$ dada por $x_1 \mapsto a$, $y_1 \mapsto b$, $x_2 \mapsto a^{\varphi}$ e $y_2 \mapsto b^{\varphi}$ define um epimorfismo de M_1 sobre $\nu(G)$.

Reciprocamente, a aplicação $\psi : \nu(G) \to M_1$ que associa $a \mapsto x_1$, $b \mapsto y_1$, $a^{\varphi} \mapsto x_2$ e $b^{\varphi} \mapsto y_2$ preserva as relações de $\nu(G)$, na sua apresentação dada pelo **Teorema 1.7.20**, haja vista as relações de conjugação decorrentes do **Lema 3.0.1**

$$\begin{gathered}
[a, b^{\varphi}]^{a} = [a, b^{\varphi}]^{a^{\varphi}} = [a, b^{\varphi}][a, a^{\varphi}]^{(r-1)},\\
[a, b^{\varphi}]^{b} = [a, b^{\varphi}]^{b^{\varphi}} = [a, b^{\varphi}]^{r}[a, a^{\varphi}]^{(r-1)\binom{r}{2}},\\
[a, a^{\varphi}]^{a} = [a, a^{\varphi}]^{a^{\varphi}} = [a, a^{\varphi}]^{b} = [a, a^{\varphi}]^{b^{\varphi}} = [a, a^{\varphi}],\\
[b, b^{\varphi}]^{a} = [b, b^{\varphi}]^{a^{\varphi}} = [b, b^{\varphi}]^{b} = [b, b^{\varphi}]^{b^{\varphi}} = [b, b^{\varphi}],\\
[b, a^{\varphi}]^{a} = [b, a^{\varphi}]^{a^{\varphi}} = [b, a^{\varphi}][a, a^{\varphi}]^{-(r-1)},\\
[b, a^{\varphi}]^{b} = [b, a^{\varphi}]^{b^{\varphi}} = [b, a^{\varphi}]^{r}[a, a^{\varphi}]^{-(r-1)\binom{r}{2}},
\end{gathered}$$

das quais decorrem as relações definidoras de M_1, conforme **Proposição 3.2.1**.

Assim, os epimorfismos ϕ e ψ possuem inversas a direita, a saber, $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$. Portanto, obtemos o isomorfismo $\nu(G) \cong M_1$.

A demonstração de que as apresentações dos itens (ii) e (iii) descrevem o grupo $\nu(G)$ para os respectivos grupos metacíclicos infinitos G segue de maneira análoga e fica assim demonstrado o **Teorema C**. $\square$

Como feito anteriormente, a estratégia usada agora neste trabalho é, a partir do grupo $\nu(G)$ construído no **Teorema C**, identificar não somente o quadrado tensorial como também as outras seções do grupo $\nu(G)$. Já sabemos que $\Delta(G)$ e $\mu(G)$ são centrais em $\nu(G)$, $[G, G^{\varphi}]$ é abeliano, $M(G)$ e $G \wedge G$ são cíclicos pois G' é cíclico, como pode ser verificado por Beuerle & Kappe [3]. Sobre o grupo $\tau(G) = \nu(G)/\Delta(G)$ nada sabemos a princípio.

No Corolário a seguir, damos uma apresentação para os grupos $[G, G^{\varphi}]$, $G \wedge G$, $\mu(G)$ e $M(G)$, vistos como seções abelianas do grupo $\nu(G)$, garantido pelos resultados obtidos em Blyth & Morse [8] e Rocco [[32], [34]]. Adiante, calculamos uma identificação para o grupo $\tau(G)$ via quociente $\nu(G)/\Delta(G)$.

Corolário 3.2.2. *Seja $G = g(a, b; m, n, r)$ um grupo metacíclico infinito.*

(1) Se $m \neq 0$, $n = 0$, $r \neq 1$, então:

(i) $$[G, G^{\varphi}] = \langle u, v, w, z \mid u^m = 1, v^{(m,2(r-1))} = 1, z^{(m,r-1)} = 1, [u, v] = [u, w] = [u, z] = 1, [v, w] = [v, z] = [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^m = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^{(m,r-1)} = 1\rangle$, *onde* $\bar{u} := u^{\frac{m}{(m,r-1)}}\Delta(G)$.

(2) Se $m = 0$, $n \geq 0$ e $r = -1$, então:

(i) $$[G, G^{\varphi}] = \langle u, v, w, z \mid v^{(n,4)} = 1, w^n = 1, z^2 = 1, [u, v] = [v, w] = [u, w] = [u, z] = [v, z] = 1, [w, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u}\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = 1$.

(3) Se $G = g(a, b; 0, n, 1)$, $n > 0$ é par, então:

(i) $$[G, G^{\varphi}] = \langle u, v, w, z \mid u^n = 1, w^n = 1, z^n = 1, [w, z] = [v, w] = [u, v] = [u, w] = [u, z] = 1, [v, z] = 1\rangle.$$

(ii) $G \wedge G = \langle \bar{u} \mid \bar{u}^n = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

(iii) $M(G) = \langle \bar{u} \mid \bar{u}^n = 1\rangle$, *onde* $\bar{u} := u\Delta(G)$.

Demonstração. A demonstração será feita apenas para o caso (1). Os outros seguem de maneira análoga.

Seja A um grupo abeliano dado por

$$\langle u, v, w, z \mid u^m = 1, v^{(m,2(r-1))} = 1, z^{(m,r-1)} = 1, [u, v] = 1, [u, w] = 1, [u, z] = 1, [v, w] = 1, [v, z] = 1, [w, z] = 1\rangle.$$

O **Teorema C** e as relações entre os elementos de $[G, G^{\varphi}]$ garantidas pelo **Lema 3.0.1** estabelecem o epimorfismo entre A e $[G, G^{\varphi}] \cong G \otimes G$. Por conseguinte, garantimos o epimorfismo de M_1 sobre $\nu(G)$.

Uma vez estabelecido o isomorfismo entre M_1 e $\nu(G)$, pela própria estrutura do grupo $\nu(G)$, segue o isomorfismo entre o grupo A, subgrupo de M_1, e $[G, G^\varphi]$.

A apresentação dos grupo $G \wedge G$ é deduzida da apresentação do grupo $[G, G^\varphi]$ módulo $\Delta(G)$, visto que $G \wedge G$ é isomorfo ao quociente $[G, G^\varphi]/\Delta(G)$.

Uma vez calculada a ordem do grupo $G \wedge G$ e sendo G' um grupo cíclico isomorfo ao quociente de $G \wedge G$ por $M(G)$ segue que

$$\begin{aligned} |M(G)| &= \frac{m}{\frac{m}{(m,r-1)}} \\ &= (m, r-1), \end{aligned}$$

onde $|G'| = \dfrac{m}{(m, r-1)}$. □

Como último Corolário do **Teorema C**, daremos apresentações para seção $\nu(G)/\Delta(G)$:

Corolário 3.2.3. *Seja $G = g(x_1, y_1; m, n, r)$ um grupo metacíclico infinito.*

(1) *Se $m \neq 0$, $n = 0$ e $r \neq 1$, então:*

$$\begin{aligned} \tau(G) &= \langle x_1, y_1, x_2, y_2, u \mid x_1^m = 1, (x_2)^m = 1, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, u^m = 1, \\ &\qquad [x_1, y_2] = u, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u^r \rangle \\ &\cong (C_m \times C_m \times C_m) \rtimes (C_\infty \times C_\infty). \end{aligned}$$

(2) *Se $m = 0$, $n \neq 0$ e $r = -1$, então:*

$$\begin{aligned} \tau(G) &= \langle x_1, y_1, x_2, y_2, u \mid y_1^n = 1, y_2^n = 1, [x_1, y_1] = x_1^{r-1}, [x_2, y_2] = x_2^{r-1}, \\ &\qquad [x_1, y_2] = u, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u^r \rangle \\ &\cong (C_\infty \times C_\infty \times C_\infty) \rtimes (C_n \times C_n). \end{aligned}$$

(3) *Se $m = 0$, $n > 0$ e $r = 1$, então:*

$$\begin{aligned} \tau(G) &= \langle x_1, y_1, x_2, y_2, u \mid y_1^n = 1, y_2^n = 1, [x_1, y_1] = 1, [x_2, y_2] = 1, u^n = 1, \\ &\qquad [x_1, y_2] = u, u^{x_1} = u^{x_2} = u, u^{y_1} = u^{y_2} = u \rangle \\ &\cong C_\infty \times C_\infty \times C_n \times C_n \times C_n. \end{aligned}$$

Demonstração. Sejam $H = \langle a, a^\varphi, u \rangle$ e $K = \langle b, b^\varphi \rangle$ subgrupos de $\tau(G) = \nu(G)/\Delta(G)$, onde $G = \langle a, b \rangle$ e $G^\varphi = \langle a^\varphi, b^\varphi \rangle$.

Considere $\nu(G)$ dado no **Teorema C**. Uma apresentação para o grupo $\tau(G)$, ou seja, $\nu(G)$ módulo $\Delta(G)$ é

$$\begin{aligned} &\langle a, b, a^\varphi, b^\varphi, u \mid a^m = (a^\varphi)^m = 1, [a, b] = a^{r-1}, [a^\varphi, b^\varphi] = (a^\varphi)^{r-1}, u = [a, b^\varphi], u^m = 1, \\ &\qquad u^a = u^{a^\varphi} = u, u^b = u^{b^\varphi} = u^r \rangle. \end{aligned}$$

Pelas relações definidoras de $\nu(G)$, temos que $[a, a^{\varphi}] = [b, b^{\varphi}] = [u, a] = [u, a^{\varphi}] = 1$, módulo $\Delta(G)$ e $u^m = a^m = (a^{\varphi})^m = 1$. Logo,

$$H \cong C_m^3 \ \ e \ \ K \cong C_{\infty}^2,$$

já que b e b^{φ} tem ordem infinita.

Ainda das relações definidoras de $\nu(G)$, temos que: $a^b = a^r$, $(a^{\varphi})^{b^{\varphi}} = (a^{\varphi})^r$, $a^{b^{\varphi}} = au$, $(a^{\varphi})^b = a^{\varphi}u$, $u^b = u^{b^{\varphi}} = u^{-1}$. Como $H \cap K = 1$, segue que $\tau(G) \cong H \rtimes K$.

No caso (3), temos que u também central em $\nu(G)$, implicando em $\tau(G)$ ser abeliano.

□

Buerle & Kappe [[3], Theorem 4.3 e 4.4] mostraram, via biderivação, que o grupo $[G, G^{\varphi}]$ de um grupo metacíclico infinito G é identificado por $C_{(m,2(r-1))} \times C_{(m,r-1)} \times C_m \times C_{\infty}$, quando $m > 0$ e $C_{(n,4)} \times C_2 \times C_{\infty} \times C_n$, quando $m = 0$, respecitvamente. Esta identificação coincide com as ordens do conjunto gerador do **Corolário 3.2.2**. Ademais, verificaram uma identificação para os grupos $G \wedge G$ e $M(G)$ [[3], Theorem 5.1] e, por fim, para o grupo $\mu(G)$ [[3], Theorem 5.2]. Novamente, nosso trabalho contempla e complementa tais cálculos por considerar o caso em que o grupo $G = g(a, b; m, n, r)$ é abeliano e calcular a seção $\nu(G)/\Delta(G)$ do grupo $\nu(G)$.

Para finalizar esse trabalho, exploramos a seguir alguns exemplos dos quais construímos o grupo $\nu(G)$. Focamos nos casos em que o grupo é não abeliano, que podem ser encontrados na literatura:

Exemplo 3.2.4. *Seja $G = g(a, b; 0, 2, -1)$ o grupo diedral infinito.*

*Pelo **Teorema C**, tomando $n = 2$, uma apresentação para o grupo $\nu(G)$ é dada por:*

$$\begin{aligned}\langle a, b, a^{\varphi}, b^{\varphi}, u, v, w, z \mid\ & b^2 = 1, (b^{\varphi})^2 = 1, [a, b] = a^{-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{-2}, u = [a, b^{\varphi}], v = [a, a^{\varphi}], \\ & w = [b, b^{\varphi}], u^{-1}z = [b, a^{\varphi}], z^2 = 1, v^2 = 1, w^2 = 1, u^a = u^{a^{\varphi}} = uv^{-2}, \\ & u^b = u^{b^{\varphi}} = u^{-1}v^{-2},\ (v, w, z \ centrais)\rangle.\end{aligned}$$

Blyth & Morse [[8], Theorem 22] *calcularam o quadrado tensorial de G, a saber, $[G, G^{\varphi}] \cong C_{\infty} \times C_2 \times C_2 \times C_2$, cujo conjunto gerador é dado por $\{u, v, w, z\}$ do grupo $\nu(G)$ acima. Este cálculo conincide com o **Corolário 3.2.2**, para $n = 2$,*

$$\begin{aligned}[G, G^{\varphi}] = \langle u, v, w, z \mid\ & v^2 = 1, w^2 = 1, z^2 = 1, [u, v] = [v, w] = [u, w] = [u, z] = [v, z] = 1, \\ & [w, z] = 1\rangle.\end{aligned}$$

*Ainda pelo **Corolário 3.2.2**,*

$G \wedge G = \langle u \rangle$.

$M(G) = 1$.

Ademais,

$$\begin{aligned}\tau(G) &= \langle a, b, a^{\varphi}, b^{\varphi}, u \mid b^2 = (b^{\varphi})^2 = 1, [a,b] = a^{-1}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{-2}, u = [a, b^{\varphi}], \\ &\qquad u^a = u^{a^{\varphi}} = u, u^b = u^{b^{\varphi}} = u^{-1} \rangle \\ &\cong (C_\infty \times C_\infty \times C_\infty) \rtimes (C_2 \times C_2).\end{aligned}$$

Exemplo 3.2.5. *Seja $G = g(a, b; 0, 0, -1)$ a garrafa de Klein com $G' = \langle a^2 \rangle$ de ordem infinita, $o'(a) = 2$ e $o'(b)$ é infinito.*

*Pelo **Teorema C**, uma apresentação para o grupo $\nu(G)$:*

$$\begin{aligned}\langle a, b, a^{\varphi}, b^{\varphi}, u, v, w, z \mid\ & [a,b] = a^{-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{-2}, u = [a, b^{\varphi}], v = [a, a^{\varphi}], w = [b, b^{\varphi}], \\ & u^{-1}z = [b, a^{\varphi}], v^4 = 1, z^2 = 1, u^a = u^{a^{\varphi}} = uv^{-2}, u^b = u^{b^{\varphi}} = u^{-1}v^{-2}, \\ & (v, w, z \text{ centrais})\rangle.\end{aligned}$$

cujas seções abelianas são identificadas:

$[G, G^{\varphi}] = \langle u, v, w, z \mid v^4 = 1, w^2 = 1 \rangle$.

$G \wedge G = \langle \bar{u} \rangle$.

$M(G) = 1$.

Por fim,

$$\begin{aligned}\tau(G) &= \langle a, b, a^{\varphi}, b^{\varphi}, u \mid [a,b] = a^{-2}, [a^{\varphi}, b^{\varphi}] = (a^{\varphi})^{-2}, u = [a, b^{\varphi}], u^a = u^{a^{\varphi}} = u, \\ &\qquad u^b = u^{b^{\varphi}} = u^{-1} \rangle \\ &\cong (C_\infty \times C_\infty \times C_\infty) \rtimes (C_\infty \times C_\infty).\end{aligned}$$

Observe que o grupo $\tau(G)$ contém duas cópias da garrafa de Klein, a saber, os subgrupos $\langle b, u \rangle$ e $\langle b^{\varphi}, u \rangle$.

Finalizamos então esse Capítulo com um estudo do grupo $\nu(G)$ de grupos metacíclicos finitos e infinitos como nos propusemos anteriormente. A seguir, no **Apêndice A** disponibilizamos alguns comandos utilizados no sistema GAP para o desenvolvimento desta tese.

Apêndice A

Funções e Comandos Usados no GAP

Reservamos este apêndice à apresentação das funções e comandos do GAP [18] usados ao longo deste trabalho com as devidas explicações:

A.1 $G = g(a,b;m,n,r,s)$, o Grupo $\nu(G)$ e Suas Seções

Função que exibe o par (r,s) de inteiros que definem o grupo $G = g(a,b;m,n,r,s)$ para dados (m,n)

```
G:=function(m,n)
   local l, r, s, u, v;
   l := [ ];
   for r in [2..m] do
   for s in [0..m - 1] do
if GcdInt(r, m) = 1 and EuclideanRemainder(r^n, m) = 1
and EuclideanRemainder(s * (r - 1), m) = 0 then
   Add(l, [r, s]); fi; od; od;
return l;
end; ;
```

Construção do grupo $G = g(a,b;m,n,r,s)$

```
gap > f := FreeGroup(2); ;
gap > a := f.1; ; b := f.2; ;
gap > r := [a^m, b^n/a^s, a^b/a^r]; ;
gap > G := f/r; ;
```

Apresentação policíclica para o grupo $G = g(a,b;m,n,r,s)$

gap > j := Image(IsomorphismPcGroup(G));;

gap > g := Image(IsomorphismPcpGroup(j));

Comandos para os grupos $[G, G^{\varphi}]$, $G \wedge G$, $\Delta(G)$, $\mu(g)$, $M(G)$, $\tau(G)$, $\nu(G)$

gap > nag := NonAbelianTensorSquare(g);

gap > neg := NonAbelianExteriorSquare(g);

gap > delta := Kernel(NonAbelianTensorSquareEpimorphism(g));

gap > alpha := NonAbelianTensorSquareEpimorphism(g);;

gap > gamma := Range(alpha)!.epimorphism;;

gap > mu := Kernel(alpha * gamma);

gap > ms := Kernel(NonAbelianExteriorSquareEpimorphism(g));

gap > tau := Range(NonAbelianExteriorSquarePlusEmbedding(g));

gap > nug := NonAbelianTensorSquarePlus(g);

gap > PrintPcpPresentation(nug); Uma apresentação policíclica para $\nu(G)$

A.2 $G = g(a, b; m, n, r)$, o Grupo $\nu(G)$ e Suas Seções

Para a definição de tal grupo no GAP [18], teríamos 3 possibilidades:

1− O comando InfiniteMetacyclicPcpGroup(n, m, r) que fornece uma *pcp*−apresentação do grupo $G = g(a, b; m, n, r)$, baseado no artigo de Beuerle & Kappe [3].

2− Construir o grupo $G = g(a, b; m, n, r)$ a partir de um grupo livre $F(2)$ e torná-lo um *pcp*−grupo.

3− Definir uma apresentação policíclica para o grupo $G = g(a, b; m, n, r)$ a partir dos 'collectors' do mesmo.

Faremos cada uma das situações para o grupo $G = g(a, b; 0, 8, -1)$:

1−

gap > g := InfiniteMetacyclicPcpGroup(8, 0, −1);

Pcp − group with orders[8, 0]

gap > IsAbelian(g);

true

Observe que esta construção não é de toda correta, pela própria teoria apresentada no **Teorema 2.2.2**. Portanto, desconsideraremos essa construção.

2−

```
gap > f := FreeGroup(2);;
gap > a := f.1;; b := f.2;;
gap > r := [b^8, a^b/a^-1];;
gap > h := f/r;;
gap > IsAbelian(h);
false
gap > j := Image(IsomorphismPcGroup(h));
Error, no method found! For debugging hints type ?Recovery from NoMethodFound
Error, no 3rd choice method found for 'IsomorphismPcGroup' on 1 arguments
called from < function "HANDLEMETHODNOTFOUND" >(< arguments >)
called from read - eval loop at line 198 of *stdin*
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue
brk >
```

Ou seja, o programa não consegue dar uma apresentação policíclica para o grupo infinito proposto. Portanto, não consideraremos esse método também.

3−

```
gap > col := FromTheLeftCollector(2);;
gap > SetRelativeOrder(col, 1, 8);
gap > SetConjugate(col, 2, 1, [2, -1]);
gap > SetConjugate(col, 2, -1, [2, 1]);
gap > UpdatePolycyclicCollector(col);
gap > IsConfluent(col);
true
gap > g := PcpGroupByCollector(col);
Pcp - group with orders [8, 0]
gap > IsAbelian(g);
false
```

E desta forma, concluímos que a maneira mais eficiente e coerente com a teoria até aqui apresentada a respeito do grupo $G = g(a, b; m, n, r)$ é a proposta pelo item 3− acima. Os comandos para o grupo $\nu(G)$ e suas seções foram definidos na seção anterior para qualquer grupo policíclico.

Referências Bibliográficas

[1] Arganbright, D., "The power-commutator structure of finite p-groups." *Pacific Journal of Mathematics* 29, no. 1 (1969): $11-17$.

[2] Bacon, M.R., Kappe, L.C. and Morse, R.F., "On the nonabelian tensor square of a 2-Engel group."*Archiv der Mathematik* 69, no. 5 (1997): $353-364$.

[3] Beuerle, J.R. and Kappe, L.C., "Infinite metacyclic groups and their non-abelian tensor squares." *Proceedings of the Edinburgh Mathematical Society* 43, no. 3 (2000): $651-662$.

[4] Beyl, F.R., *The classification of metacyclic p-groups, and other applications of homological algebra to group theory.* Cornell University, August, 1972.

[5] Beyl, F.R., "The Schur multiplicator of metacyclic groups." *Proceedings of the American Mathematical Society* 40, no. 2 (1973): $413-418$.

[6] Beyl, F.R. and Jones, M.R., "Addendum: “The Schur multiplicator of metacyclic groups” (Proc. Amer. Math. Soc. 40 (1973), 413?418) by FR Beyl." *Proceedings of the American Mathematical Society* 43, no. 1 (1974): $251-252$.

[7] Blyth, R.D., Fumagalli, F. and Morigi, M., "Some structural results on the non-abelian tensor square of groups." *Journal of Group Theory* 13, no. 1 (2010): $83-94$.

[8] Blyth, R.D. and Morse, R.F., "Computing the nonabelian tensor squares of polycyclic groups." *Journal of Algebra* 321, no. 8 (2009): $2139-2148$.

[9] Brown, R. and Loday, J.L., "Van Kampen theorems for diagrams of spaces." *Topology* 26, no. 3 (1987): $311-335$.

[10] Brown, R., Johnson, D.L. and Robertson, E.F., "Some computations of non-abelian tensor products of groups." *Journal of Algebra* 111, no. 1 (1987): $177-202$.

[11] Carmichael, R.D., *Introduction to the theory of groups of finite order.* Vol. 19. Boston: Ginn, 1937.

[12] Cohen, H., *Number theory: Volume I: Tools and diophantine equations.* Vol. 239. Springer Science & Business Media, 2008.

[13] Curtis, C.W. and Reiner, I., *Representation theory of finite groups and associative algebras.* Vol. 356. American Mathematical Soc., 1966.

[14] Dehn, M., "Über unendliche diskontinuierliche Gruppen." *Mathematische Annalen* 71, no. 1 (1911): $116-144$.

[15] Eick, B. and Nickel, W., "Computing the Schur multiplicator and the nonabelian tensor square of a polycyclic group." *Journal of Algebra* 320, no. 2 (2008): $927-944$.

[16] Ellis, G. and Leonard, F., "Computing Schur multipliers and tensor products of finite groups."In *Proceedings of the Royal Irish Academy.* Section A: Mathematical and Physical Sciences, pp. $137-147$. Royal Irish Academy, 1995.

[17] Firby, P.A. and Gardiner, C.F., *Surface topology.* Elsevier, 2001.

[18] GAP Group. "GAP-Groups, Algorithms, and Programming, Version 4.7.5; 2014."(2012): $242-291$. (http://www.gap- system.org).

[19] Gorenstein, D., *Finite groups.* Vol. 301. American Mathematical Soc., 2007.

[20] Hempel, C.E., "Metacyclic groups." *Communications in algebra* 28, no. 8 (2000): $3865-3897$.

[21] Holt, D.F., Eick, B. and O'Brien, E.A., *Handbook of computational group theory.* Chapman and Hall/CRC, 2005.

[22] Johnson, D.L., *Presentations of groups.* Vol. 15. Cambridge university press, 1997.

[23] Johnson, D.L., "The nonabelian tensor square of a finite split metacyclic group." *Proceedings of the Edinburgh Mathematical Society* 30, no. 1 (1987): $91-95$.

[24] Jones, M.R., "A property of finite p-groups with trivial multiplicator." *Transactions of the American Mathematical Society* 210 (1975): $179-183$.

[25] Karpilovsky, G., *The schur multiplier.* Oxford University Press, Inc., 1987.

[26] King, B.W., "Presentations of metacyclic groups." *Bulletin of the Australian Mathematical Society* 8, no. 1 (1973): 103-131.

[27] Magnus, W., Karrass, A. and Solitar, D., *Combinatorial group theory: Presentations of groups in terms of generators and relations.* Courier Corporation, 2004.

[28] Marshall Jr, H., *The theory of groups.* New York (1959).

[29] Miller, C., "The second homology group of a group; relations among commutators." *Proceedings of the American Mathematical Society* 3, no. 4 (1952): $588 - 595$.

[30] Neumann, B.H., "On some finite groups with trivial multiplicator." *Publ. Math. Debrecen* 4, no. 56 (1956): $190 - 194$.

[31] Robinson, D.J., *A Course in the Theory of Groups.* Vol. 80. Springer Science & Business Media, 2012.

[32] Rocco, N.R., "A presentation for a crossed embedding of finite solvable groups." *Communications in Algebra* 22, no. 6 (1994): $1975 - 1998$.

[33] Rocco, N.R., *Métodos de Lie Em Teoria dos Grupos.* In: Said Najati Sidki; Noraí Romeu Rocco. (Org.). (1987): $129 - 213$.

[34] Rocco, N.R., "On a construction related to the non-abelian tensor square of a group."*Boletim da Sociedade Brasileira de Matemática-Bulletin/Brazilian Mathematical Society* 22, no. 1 (1991): $63 - 79$.

[35] Rotman, J.J., *The theory of groups: an introduction.* (1973).

[36] Schur, J., "Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen."*Journal für die reine und angewandte Mathematik* 132 (1907): $85 - 137$.

[37] Shokranian, S., Soares, M. and Godinho, H., *Teoria dos números.* UnB, (1994).

[38] Sidki, S., "On weak permutability between groups."*Journal of Algebra* 63, no. 1 (1980): $186 - 225$.

[39] Sim, H.S., "Metacyclic groups of odd order." *Proceedings of the London Mathematical Society* 3, no. 1 (1994): $47 - 71$.

[40] Sims, C.C., "Verifying nilpotence." *Journal of Symbolic Computation* 3, no. 3 (1987): $231 - 247$.

[41] Sims, C.C., *Computation with finitely presented groups.* Encyclopedia of Mathematics and its Applications, 48. Cambridge University Press, Cambridge, (1994).

[42] Tietze, H., "Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten."*Monatshefte für Mathematik und Physik* 19, no. 1 (1908): 1 – 118.

[43] Wamsley, J.W., "The deficiency of metacyclic groups." *Proceedings of the American Mathematical Society* 24, no. 4 (1970): 724 – 726.

[44] Whitehead, J.H., "A certain exact sequence." *Annals of Mathematics* (1950): 51 – 110.

[45] Zassenhaus, H., *The theory of groups.* Courier Corporation, 1999.