Universidade de Brasília

Operações Entrelaçadas no Grupo de Automorfismos da Árvore Binária

Junio Rocha de Oliveira

Orientador: Prof. Dr. Alex Carrazedo Dantas

Departamento de Matemática
Universidade de Brasília

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

Fevereiro 2020

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Operações Entrelaçadas no Grupo de Automorfismos da Árvore Binária

por

Junio Rocha de Oliveira*

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

MESTRE EM MATEMÁTICA

Brasília, 14 de fevereiro de 2020.

Comissão Examinadora:

____

Prof. Dr. Alex Carrazedo Dantas - MAT/UnB (Orientador)

Emerson Ferreira de Melo
____

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

Ana Cristina
____

Profa. Dra. Ana Cristina Vieira – UFMG (Membro)

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

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

Ro

Rocha de Oliveira, Junio
Operações Entrelaçadas no Grupo de Automorfismos da Árvore Binária / Junio Rocha de Oliveira; orientador Alex Carrazedo Dantas. -- Brasília, 2020.
127 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2020.

1. Automorfismos de árvore. 2. Máquina de Mealy. 3. Tree wreathing. 4. Representação de estado-finito. 5. Produto entrelaçado. I. Carrazedo Dantas, Alex, orient. II. Título.

"Dentre nós, não há um ser que se mescle a outro;
Não há dois de nós que tenham formas idênticas;
E, por não possuirmos o terceiro olho,
Não enxergamos a esperança em nenhuma das quatro direções;
Mas o quinto caminho certamente existe, onde está o coração.
(Bleach, Volume 27: Goodbye, Halcyon Days)

Agradecimentos

Agradeço primeiramente a Deus por me conceder a determinação e resiliência necessárias para seguir nesta caminhada.

A minha família por todo o suporte financeiro e emocional. Ao meu pai Josias, à minha mãe Ivolene, aos meus irmãos Raihane e Thiago, aos meus sobrinhos Vitor e Rafaela. Agradeço por todas as mensagens e conversas reconfortantes, pelas recepções calorosas e por vibrarem por minhas conquistas.

Aos meus amigos da graduação, Lilian, Nádia, Nathan e Pâmella por todos os momentos juntos, pelas discussões, por me apoiarem nas dificuldades, pela cumplicidade, por torcerem por mim e pela amizade que levarei para toda vida.

A todos com quem tive oportunidade de conviver durante o período de pós-graduação, em especial, Adler, Bruna, Carla, Claudia, Deivid, Gabriel, Gabriela, Geovane, Jailson, João, Julia, Maria Edna, Mateus, Murilo, Paulo, Rosalina, Romulo, Tharles e Vítor. Agradeço a vocês por todos os momentos de descontração, de estudos em grupo e por todo o apoio oferecido durante este período. Meus mais sinceros agradecimentos ao meu amigo de mestrado e colega de quarto Kelvin John, por todos os motivos anteriores, pelo zelo dedicado a mim e pela companhia nos rolês aleatórios.

Ao meu orientador, Alex Carrazedo Dantas, pela confiança depositada em mim, por valorizar os acertos e pelo jeito nas palavras ao apontar os erros, pela dedicação, paciência e compromisso desempenhados para a conclusão deste trabalho.

Aos professores do departamento de matemática da UFMT/CUR, Adimar, Clayton, Erika, Eunice e Francislaine, por todo o suporte e incentivo.

Aos professores que contribuíram para minha formação durante o mestrado, Aline, Zhou, Tarcísio, Daniele Nantes, Sheila, Raimundo e Igor.

Aos funcionários do departamento de matemática da UnB, em especial, Claudia Messias, pelas orações, carinho e a preocupação com nosso bem-estar.

Aos membros da banca examinadora, Emerson Ferreira de Melo e Ana Cristina Vieira, pelas correções e sugestões.

Ao CNPq pelo apoio financeiro a este trabalho.

Resumo

Estudaremos uma operação estabelecida por Brunner e Sidki, denominada *tree-wreathing*, que é definida sobre os subgrupos $\widetilde{H}(r)$ e $K(r)$ do grupo de automorfismos da árvore binária, onde $\widetilde{H}(r)$ e $K(r)$ são cópias específicas construídas a partir do grupo H que age na árvore binária e do grupo abeliano livre K de posto r. O produto *tree-wreath* G dos grupos $\widetilde{H}(r)$ e $K(r)$ admite um subgrupo normal N tal que G/N é isomorfo a $H \wr K$, neste sentido, o produto *tree-wreath* generaliza o produto entrelaçado $H \wr K$. Para o caso onde H é abeliano, a operação produz uma representação fiel de $H \wr K$ no grupo de automorfismos da árvore binária. Além disso, a operação *tree-wreathing* preserva propriedades tais como solubilidade, finitude do número de estados e ser livre de torção. Por fim, obtemos uma representação fiel do grupo metabeliano livre de posto arbitrário no grupo de automorfismos da árvore binária como um subgrupo de automorfismos de estado-finito.

Palavras-chave: Automorfismos de árvore, máquina de Mealy, tree-wreathing, representação de estado-finito, produto entrelaçado.

Abstract

An operation called *tree-wreathing*, due to Brunner and Sidki, is defined over subgroups $\widetilde{H}(r)$ and $K(r)$ from the automorphism group of the binary tree, where $\widetilde{H}(r)$ and $K(r)$ are specific copies constructed from a group H which acts on the binary tree and a free abelian group K of rank r. The *tree-wreath* product G of the groups $\widetilde{H}(r)$ and $K(r)$ admits a normal subgroup N such that G/N are isomorphic to $H \wr K$, in this sense, the *tree-wreath* product generalizes the wreath product $H \wr K$. When H is abelian, the *tree-wreath* operation produces a faithful representation of $H \wr K$ in the automorphism group of the binary tree. Furthermore, the properties of solvability, having finite-state and torsion-freeness are preserved by the *tree-wreathing* construction. In the end, a faithful representation of a free metabelian group of any rank is obtained as a group having finite-state.

Keywords: Tree automorphisms, Mealy machine, tree-wreathing, finite-state representation, wreath product.

Notação

$H \leq G$	H é subgrupo de G
$H \lhd G$	H é subgrupo normal de G
$G \simeq H$	G é isomorfo a H
G/N	grupo quociente de G pelo subgrupo normal N
x^y	$y^{-1}xy$
X^Y	$\langle x^y \mid x \in X, y \in Y \rangle$
$[x,y]$	$x^{-1}y^{-1}xy$
$[A,B]$	$\langle [a,b] \mid a \in A, b \in B \rangle$
G'	$[G,G]$
$G^{(n)}$	n-ésima derivada de G
$\langle X \rangle$	grupo gerado pelo conjunto X
$\gamma_n(G)$	n-ésimo termo da série central inferior de G
$g \cdot x$	ação à esquerda de g em x
$G_1 \times \cdots \times G_n$	produto direto dos grupos $G_1, \ldots, G_n$
$G_1 \oplus \cdots \oplus G_n$	soma direta dos grupos abelianos $G_1, \ldots, G_n$
$Cr_{\lambda \in \Lambda} G_\lambda$	produto cartesiano dos grupos G_λ, $\lambda \in \Lambda$
$Dr_{\lambda \in \Lambda} G_\lambda$	produto direto dos grupos G_λ, $\lambda \in \Lambda$
$H \rtimes K$	produto semidireto dos grupos H e K
$H \wr K$	produto entrelaçado $Dr_{k \in K} H_k \rtimes K$
X^*	conjunto de todas as palavras finitas sobre o conjunto X
$\mathcal{T}_m$	árvore uni-raíz m-regular
$\mathcal{A}_m$	grupo de automorfismos de $\mathcal{T}_m$
$\mathcal{G}(A)$	subgrupo de $\mathcal{A}_m$ gerado pelo autômato A
$\mathbb{Z}_p$	anel dos interios p-ádicos
S_n	grupo de todas as permutações entre n elementos
S_X	conjunto de todas as bijeções de X em X
$R[G]$	anel de grupo proveniente de um anel comutativo com unidade R e um grupo G

$c(G)$	comprimento do maior circuito simples de um grafo ou dígrafo G
$Q(\beta)$	conjunto de estados de β, onde β é um automorfismo da árvore $\mathcal{T}_m$ ou um autômato
$Stab_G(n)$	estabilizador de um subgrupo G de $\mathcal{A}_m$ no nível n
$Trun_G(n)$	truncamento das ações de um grupo G no nível n de $\mathcal{T}_m$
$\theta(W;k,v)$	número de caminhos direcionados distintos de comprimento $k \geq 0$ iniciando em um vértice v e terminando em um vértice com a propriedade W
$\mathcal{F}(Y)$	subgrupo de todos os automorfismos de estado finito de $\mathcal{A}_m$, onde $\mid Y \mid = m$
$\mathcal{F}_n(Y)$	subgrupo de $\mathcal{F}(Y)$ cujas funções de crescimento de seus automorfismos são limitadas por $f(k) = ck^n$, onde $c > 0$
$\mathcal{F}_{0,m}(Y)$	subgrupo de $\mathcal{F}_0(Y)$ formado por elementos β tal que $c(\beta) = 0$ ou $c(\beta)$ divide m

Sumário

Lista de Figuras

Introdução

Árvores uni-raízes m-regulares $\mathcal{T}_m$ são grafos cujos vértices são palavras finitas em um alfabeto Y de tamanho m, a palavra vazia $\emptyset$ é designada como vértice raiz e as arestas conectam dois vértices u e v se, e somente se, $u = yv$ ou $v = yu$, onde $y \in Y$. Sua estrutura é de tal forma que cada vértice é raiz de uma sub-árvore isomorfa a própria árvore, consequentemente, os grupos de automorfismos das árvores em questão são isomorfos ao grupo de automorfismos $\mathcal{A}_m$ da própria árvore. Deste último fato, podemos inferir que um automorfismo de $\mathcal{T}_m$ é da forma $\alpha = (\alpha_0, \ldots, \alpha_{m-1})\sigma_\alpha$, onde $\sigma_\alpha \in S_m$ e α_i são automorfismos de $\mathcal{T}_m$ agindo a partir do vértice indexado por i, onde $i = 1, \ldots, m$.

Os automorfismos de $\mathcal{T}_m$ estão intimamente relacionados com uma máquina de Mealy, que consiste de uma 4-upla $A = (Q, Y, f, l)$, onde Y é um alfabeto finito, Q é um conjunto de estados, $f : Q \times Y \to Q$ é uma função de transição de estados e $l : Q \times Y \to Y$ é uma função de saída. Este conceito advém da teoria da computação, mais especificamente, é um caso particular de autômato.

O autômato supracitado sobre um alfabeto de tamanho m é dito invertível se para cada $q \in Q$ fixado, a restrição $f(q, -) : Y \to Y$ da função de saída é invertível, neste caso, podemos interpretá-lo como um automorfismo de $\mathcal{T}_m$. Dado um autômato invertível $A = (Q, Y, f, l)$ satisfazendo $f(q, i) = q_i$ e $l(q, i) = j$, podemos associá-lo com o automorfismo $\alpha_q = (\alpha_{q_0}, \ldots, \alpha_{q_{m-1}})\sigma_{\alpha_q}$, onde $i^{\sigma_{\alpha_q}} = j$. Por outro lado, um automorfismo $\alpha \in \mathcal{A}_m$ pode ser interpretado como uma máquina de Mealy, para isto, tomamos Y como alfabeto de entrada e de saída, definimos recursivamente o conjunto de estados como o conjunto $Q(\alpha) = \{\alpha, \alpha_0 \ldots \alpha_{m-1}\} \cup Q(\alpha_0) \cup \cdots \cup Q(\alpha_{m-1})$, $f(\beta, y) = \beta_y$ e $l(\beta, y) = y^\beta$, onde $\beta \in Q(\alpha)$. Deste modo, podemos construir um grupo gerado por autômatos dentro do grupo de automorfismos $\mathcal{A}_m$ do grafo $\mathcal{T}_m$. Além disso, se o conjunto $Q(\alpha)$ de um automorfismo α for finito, dizemos que o automorfismo α é de *estado-finito*.

O subconjunto de todos os automorfismos de estado-finito de $\mathcal{A}_m$, denotado por $\mathcal{F}(Y)$, possui estrutura de grupo e recebe um destaque especial. Em [1, página 120, 2010], verifica-se que grupos gerados por máquinas de Mealy com número finito de estados possuem o problema da palavra solúvel, consequentemente, obtemos através da correspondência entre automorfismos de $\mathcal{A}_m$ e máquinas de Mealy que o problema da palavra é solúvel em $\mathcal{F}(Y)$. Vale ressaltar que nem todo grupo finitamente gerado por automorfismos de estado-finito é um grupo gerado por uma máquina de Mealy de estado-finito.

Como objetivo principal, construiremos em $\mathcal{F}(\{0,1\})$ grupos abelianos livres K de posto r, posteriormente, buscamos subgrupos H de $\mathcal{F}(\{0,1\})$ para o qual $H \wr K$ possa ser imerso em $\mathcal{F}(\{0,1\})$. Este objetivo motivou Brunner e Sidki em [3, 2002] a construírem uma operação denominada *tree-wreathing* de H por K, denotada por $H \bar{\wr} K$, que consiste em tomar o grupo gerado por $\widetilde{H}(r)$ e K, onde $\widetilde{H}(r)$ é uma cópia isomorfa de H.

A operação *tree-wreathing* produz um grupo que preserva propriedades tais como solubilidade, ser livre de torção e ser gerado por automorfismos de estado-finito. Além destas propriedades, mostraremos que existe um subgrupo normal N em $H \bar{\wr} K$ de modo que $(H \bar{\wr} K)/N$ é isomorfo ao produto entrelaçado $H \wr K$, neste sentido, pensamos no produto *tree-wreath* $H \bar{\wr} K$ como uma generalização do produto entrelaçado $H \wr K$. Uma consequência imediata dos fatos acima é que se $\widetilde{H}(r), K(r) \in \mathcal{F}(\{0,1\})$, então $H \wr K$ possui uma representação como quociente de subgrupos de $\mathcal{F}(\{0,1\})$. Ademais, se H é abeliano, obtemos uma imersão de $H \wr K$ em $\mathcal{F}(\{0,1\})$ e como consequência deste resultado, podemos mostrar que todo grupo metabeliano livre de posto r possui uma representação fiel em $\mathcal{F}(\{0,1\})$.

No Capítulo 1, apresentaremos as preliminares referentes a teoria de grupos, à saber, produto direto finito, ações de grupos, produto semidireto, produto entrelaçado, grupos solúveis, grupos nilpotentes, grupos livres e grupos topológicos. A proposta do capítulo consiste em mencionar apenas o que será utilizado no tema principal, deste modo, um estudo aprofundado sobre os temas pode ser realizado através das referências citadas em cada seção.

O Capítulo 2 tem como objetivo explorar dois resultados fundamentais para a conclusão da questão principal. O primeiro destes resultados fundamentais se trata do Teorema de Gruenberg, demonstrado em [6, página 42, 1957], relaciona o produto entrelaçado a um tipo especial de propriedade, denominada propriedade raiz, satisfazendo:

(1) se um grupo G possui a propriedade $\mathcal{P}$ então seus subgrupos também a possuem;

(2) se G e H tem a propriedade $\mathcal{P}$ então $G \times H$ possui a propriedade;

(3) se $\{e\} \leq K \leq H \leq G$ é uma série de subgrupos, cada um normal no seu antecessor, G/H e H/K possuem a propriedade $\mathcal{P}$, então K contém um subgrupo L, normal em G, tal que G/L tem a propriedade $\mathcal{P}$.

O resultado em questão consiste de

Teorema 0.0.1. Sejam $\mathcal{P}$ uma propriedade raiz e suponha que os grupos G e H são residualmente $\mathcal{P}$. Se H é dado através de sua representação regular então $G \wr H$ é residualmente $\mathcal{P}$ se, e somente se H tem a propriedade $\mathcal{P}$ ou G é abeliano.

Desenvolveremos toda a teoria necessária para a compreensão e demonstração deste resultado. Em seguida, iremos explorar uma imersão em produtos entrelaçados, denominada imersão de Magnus, apresentada em [10, página 3, 1970], o qual enunciaremos a seguir.

Teorema 0.0.2. Seja F um grupo livre gerado por $\{x_1,\dots,x_n\}$ e $R \lhd F$. Seja A um grupo abeliano livre gerado por $\{a_1,\dots,a_n\}$. Então o grupo F/R' é imerso no grupo $A \wr (F/R)$ e essa imersão é dada pelo homomorfismo induzido por $x_iR' \mapsto (a_i, x_iR)$, $1 \leq i \leq n$.

Já no Capítulo 3, iremos definir e explorar a estrutura da árvore uni-raiz m-regular. Relacionaremos os automorfismo com autômatos e o grupo de automorfismos com o produto entrelaçado dele mesmo com um grupo de permutações. Também iremos explorar as funções de crescimento, tema este que emerge da interpretação dos automorfismos da árvore $\mathcal{T}_m$ como autômatos invertíveis, que por sua vez são representadas através de dígrafos. Além disso, veremos que a recursividade presente nesta árvore nos permite descrever o grupo $\mathcal{A}_m$ como o produto entrelaçado $\mathcal{A}_m \wr_m S_m$. Isto posto, é natural pensar em produtos entrelaçados ocorrendo como subgrupos de $\mathcal{A}_m$. Motivado por este fato, utilizamos o teorema de Gruenberg para explorar as propriedades de tais produtos entrelaçados.

Por fim, utilizaremos o Capítulo 4 para definir uma operação do grupo de automorfismos da árvore binária, denominado *tree-wreathing*. Iniciamos definindo o automorfismo de estado-finito $\alpha = (e,(\alpha,e))\sigma$, denominado operador translação, e criando uma cópia $\widetilde{H}$ de um grupo H que age na árvore binária. Em seguida, definimos $G = \langle \widetilde{H}, \alpha \rangle$ como sendo um produto *tree-wreath*, denotado por $H \,\bar{\wr}\, \mathbb{Z}$. O primeiro resultado fornece propriedades sobre esta nova operação e relaciona o produto *tree-wreath* ao produto entrelaçado. O resultado em questão nos afirma o seguinte:

Teorema 0.0.3. Seja $G = \langle \widetilde{H}, \alpha \rangle$, denominado o produto *tree-wreath* de H por α e denotado por $H \,\bar{\wr}\, \mathbb{Z}$. Então G satisfaz as seguintes propriedades:

(I) o subgrupo
$$N = \langle [\widetilde{H}^{\alpha^i}, \widetilde{H}^{\alpha^j}] | 0 \leq i < j \rangle$$
é normal em G e pode ser expresso através de suas ações sobre a árvore na forma $N = \nu(H') = (N \times H') \times (N \times H') = \langle u * H' \mid u \in (\{00,10\}^*)\{01,11\} \rangle$;

(II) o grupo quociente G/N é isomorfo ao produto entrelaçado restrito $H \wr \mathbb{Z}$;

(III) o subgrupo de G gerado por $(0^{2m-1}1) * H'$ e α possui um subgrupo em seu centro cujo quociente é isomorfo a $H' \wr \mathbb{Z}/2^m\mathbb{Z}$;

(IV) se J é um subgrupo de H, então $\langle \widetilde{J}, \alpha \rangle$, considerado como um subgrupo de $G = H \,\bar{\wr}\, \mathbb{Z}$, é isomorfo a $J \,\bar{\wr}\, \mathbb{Z}$, além disso, se J é abeliano, então $J \,\bar{\wr}\, \mathbb{Z} \simeq J \wr \mathbb{Z}$;

(V) o grupo G é de estado-finito (é solúvel, livre de torção) se, e somente se, H é de estado-finito (é solúvel, livre de torção).

Consequência do resultado acima é que, caso H seja abeliano, o produto *tree-wreath* G é isomorfo ao produto entrelaçado $H \wr \mathbb{Z}$. Além disso, se tomarmos $H = \langle \alpha \rangle$, obtemos uma representação fiel de $\mathbb{Z} \wr \mathbb{Z}$. Posteriormente, iremos definir os elementos, $\alpha(0) = \alpha$, $\alpha(i) = ((\alpha(i), \alpha(i-1)), (\alpha(i), \alpha(i-1)))$, $\tilde{h}(0) = h$, $\tilde{h}(i) = ((\tilde{h}(i), \tilde{h}(i-1)), e)$. Em seguida, definiremos os grupos $K(r) = \bigoplus_{i=0}^{r-1} \langle \alpha(i) \rangle$ e $\widetilde{H}(r) = \{\tilde{h}(r) \mid h \in H\}$, os quais nos permitem expandir a operação *tree-wreathing* e definir o produto *tree-wreath* $H \,\bar{\wr}\, \widehat{K(r)}$. O resultado

Teorema 0.0.4. O grupo $G = \langle \widetilde{H}(r), \widehat{K(r)} \rangle$ é um produto tree-wreath $H \,\bar{\wr}\, \widehat{K(r)}$.

utilizado em conjunto com a Imersão de Magnus, dão origem ao seguinte resultado, com o qual finalizamos nosso estudo:

Corolário 0.0.5. O grupo metabeliano livre $\mathbb{M}$ de posto r tem uma representação fiel como um grupo de automorfismos de estado-finito.

CAPÍTULO 1

Preliminares

Neste capítulo, desenvolveremos as noções de fatoração e extensão de grupos. Também estudaremos algumas classes de grupos com objetivo de compreender o Teorema de Gruenberg e a Imersão de Magnus, cujos resultados desempenham grande relevância para o desenvolvimento deste trabalho.

1.1 Produto de grupos

É sempre possível obter um polinômio através de produtos de polinômios, por outro lado, existem polinômios que podem ser expressos através de produtos de outros polinômios. Esta dualidade nos motiva a realizar um processo similar para os grupos, isto é, escrever grupos através de produtos de grupos e decompor um grupo dado em produto de grupos, quando possível. As definições e resultados expostos ao decorrer da seção podem ser encontrados em [12] e [13].

1.1.1 Produto direto finito

Definição 1.1.1. Se H e K são grupos, então seu *produto direto externo*, denotado por $H \times K$, é o grupo constituido de todos os pares ordenados (h,k), onde $h \in H$ e $k \in K$, cuja operação é definida por $(h,k)(h',k') = (hh',kk')$.

Note que H e K não são subgrupos de $H \times K$, porém, possuem cópias isomorfas como subgrupos, à saber, $H \times \{e_K\} = \{(h,e_K) \mid h \in H\}$ e $\{e_H\} \times K = \{(e_H,k) \mid k \in K\}$.

Definição 1.1.2. Um grupo G é um *produto direto interno* de H por K se, H e K são subgrupos normais de G, $H \cap K = \{e\}$ e $G = HK$.

Mostraremos que se G é um produto direto interno de H por K, então para quaisquer $h \in H$ e $k \in K$, temos $hk = kh$, ou equivalentemente, $h^{-1}k^{-1}hk = e$. Para isso, note que $h^{-1}k^{-1}h \in K$, pois $K \lhd G$, logo $(h^{-1}k^{-1}h)k \in K$. Analogamente, $k^{-1}hk \in H$, pois $H \lhd G$, logo $h^{-1}(k^{-1}hk) \in H$. Portanto, $h^{-1}k^{-1}hk \in H \cap K = \{e\}$, ou seja, $h^{-1}k^{-1}hk = e$.

Isto posto, se h_1k_1 e h_2k_2 são elementos de G, podemos expressar a operação destes elementos na forma $hk \in HK$. Com efeito, $h_1k_1h_2k_2 = h_1h_2k_1k_2 = hk$, onde $h = h_1h_2$ e $k = k_1k_2$.

A definição de produto direto interno reflete a noção de fatoração em um grupo. Nosso próximo objetivo e buscar uma relação entre o produto direto externo e o interno.

Lema 1.1.3. Sejam K e Q subgrupos de um grupo G tais que $K \lhd G$, $K \cap Q = \{e\}$ e $G = KQ$. Então todo elemento de $g \in G$ pode ser expresso unicamente por $g = kq$, onde $k \in K$ e $q \in Q$.

Demonstração. Se $g = k_1q_1$ e $g = k_2q_2$, com $k_1, k_2 \in K$ e $q_1, q_2 \in Q$, então $k_1q_1 = k_2q_2$ e $k_2^{-1}k_1 = q_2q_1^{-1} \in K \cap Q$, mas $K \cap Q = \{e\}$, do qual decorre que $k_2^{-1}k_1 = q_2q_1^{-1} = e$ implica $k_1 = k_2$ e $q_1 = q_2$. $\square$

Teorema 1.1.4. Seja G um grupo com subgrupos normais H e K. Se G é o produto direto interno de H e K, então $G \simeq H \times K$.

Demonstração. Se $g \in G$, então $g = hk$ para algum $h \in H$ e $k \in K$, pois $G = HK$.

Defina $\varphi : G \to H \times K$ por $(g)\varphi = (h,k)$, onde $g = hk$. Vimos no Lema 1.1.3 que se $g = hk$, então h e k são unicamente determinados, assim, $g_1 = h_1k_1 = h_2k_2 = g_2$ implica $h_1 = h_2$ e $k_1 = k_2$. Deste modo

$$g_1 = g_2 \iff h_1 = h_2 \text{ e } k_1 = k_2 \iff (g_1)\varphi = (h_1,k_1) = (h_2,k_2) = (g_2)\varphi$$

e a aplicação φ está bem definida e é injetiva.

Dado $(h,k) \in H \times K$, existe $g \in G$ tal que $g = hk$ e $(g)\varphi = (h,k)$, logo, a aplicação é sobrejetiva.

Finalmente,

$$(g_1g_2)\varphi = (h_1k_1h_2k_2)\varphi = (h_1h_2k_1k_2)\varphi = (h_1h_2,k_1k_2) = (h_1,k_1)(h_2,k_2) = (g_1)\varphi(g_2)\varphi,$$

donde concluímos que φ é um homomorfismo. Portanto, φ é um isomorfismo de $G = HK$ em $H \times K$. $\square$

1.1.2 Ações de grupos e produto semidireto

Neste momento, iremos estabelecer uma maneira de se obter interações de um grupo com um conjunto.

Definição 1.1.5. Se X é um conjunto e G é um grupo, então G age à esquerda em X se existe uma aplicação

$$\begin{array}{rcl} \alpha : G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x, \end{array}$$

denominada *ação*, tal que

(i) $e \cdot x = x$ para todo $x \in X$,

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ para todo $g,h \in G$ e $x \in X$.

Quando não há risco de confusão entre os elementos de um grupo G e do conjunto X, representaremos a ação $g \cdot x$ por $(x)g$ ou x^g, entretanto, para manter a compatibilidade entre a ação à esquerda e a notação de símbolo de aplicação à direita, convencionaremos que $gh \cdot x = (x)hg = x^{hg}$.

Dizemos que a ação de G em X é *transitiva* se para todo $x \in X$ temos $G \cdot x = X$.

Uma ação de um grupo G em um conjunto X pode ser interpretada como uma representação dos elementos de G no grupo $S(X)$ de todas as bijeções de X em X. Note que se X é um conjunto finito de n elementos, podemos identificar $S(X)$ com S_n.

Exemplo 1.1.6. Sejam G um grupo e $X = \{1,2,3\}$. Se $g \in G$ é tal que $g \cdot 1 = 2$, $g \cdot 2 = 1$ e $g \cdot 3 = 3$, então, g pode ser identificado como a permutação $(1\ 2) \in S_3$.

Grupos podem agir em si mesmos, dentre as ações, existem duas de grande interesse, as quais destacaremos à seguir.

Exemplo 1.1.7. Todo grupo age em si mesmo por multiplicação à esquerda, isto é,

$$g \cdot x = gx.$$

Esta ação é chamada de *ação regular*.

Exemplo 1.1.8. Todo grupo age em si mesmo por conjugação , isto é,

$$g \cdot x = gxg^{-1} = x^{g^{-1}}.$$

Observe que a lei definida acima é uma ação, pois

$$e \cdot c = exe^{-1} = x$$

e

$$g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x.$$

Note que se $g \cdot x = y$, então $g^{-1} \cdot y = x$. Com efeito,

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

Uma ação em classes laterais de um grupo dá origem a um teorema de grande relevância na Teoria de Grupos. O enunciaremos abaixo.

Teorema 1.1.9 (Cayley)**.** Seja H um subgrupo de um grupo G e M o conjunto de todas as classes laterais à esquerda de H em G. Defina a aplicação

$$\begin{aligned} \lambda : G &\longrightarrow S(M) \\ g &\longmapsto \lambda_g : M \longrightarrow M \\ &\qquad\qquad xH \longmapsto g^{-1}xH. \end{aligned}$$

Então λ é um homomorfismo com núcleo $Ker\lambda = \bigcap_{x \in G} H^x$.

Demonstração. Note que $(g_1g_2)^{-1}(xH) = g_2^{-1}(g_1^{-1}xH)$ para todo $x \in G$, deste modo,

$$(xH)\lambda_{g_1g_2} = (g_1g_2)^{-1}xH = g_2^{-1}(g_1^{-1}xH) = (g_1^{-1}xH)\lambda_{g_2} = ((xH)\lambda_{g_1})\lambda_{g_2} =,$$

ou seja, λ é um homomorfismo. Além disso,

$$g \in Ker\lambda \iff (g^{-1}xH = xH, \forall xH) \iff (g^{-1}H^{x^{-1}} = H^{x^{-1}}, \forall xH) \iff (g^{-1} \in H^{x^{-1}}, \forall x).$$

$\square$

No caso particular onde $H = \{e\}$, o homomorfismo λ do Teorema de Cayley é chamado de *representação regular à esquerda* do grupo G. Segue diretamente do Teorema de Cayley que a representação regular é uma imersão de G em $S(G)$.

Nosso objetivo agora é estender a noção de fatoração de um grupo em um produto de dois subgrupos.

Definição 1.1.10. Um grupo G é um *produto semidireto interno* de K por Q, se $K \lhd G$, $K \cap Q = \{e\}$ e $G = KQ$. Neste caso, utilizamos a notação $G = K \rtimes Q$.

Observe no produto direto interno que comutar um elemento $h \in H$ com um elemento $k \in K$ foi essencial para operar dois elementos da forma hk e obter um elemento em HK, isto é, $h_1k_1h_2k_2 = h_1h_2k_1k_2$. No caso do produto semidireto interno, um dos grupos pode não ser normal, deste modo, não temos a comutatividade. Entretanto, ainda é possível estabelecer uma ação que permita operar dois elementos da forma kq e obter um elemento em KQ.

Lema 1.1.11. Se G é o produto semidireto interno $G = K \rtimes Q$, então existe um homomorfismo

$$\begin{aligned} \theta : Q &\longrightarrow Aut(K) \\ x &\longmapsto \theta_x : K \longrightarrow K \\ &\qquad\qquad k \longmapsto k^{x^{-1}} = xkx^{-1}. \end{aligned}$$

Além disso, para todos $x, y \in Q$ e $k \in K$, $(k)\theta_e = k$ e $((k)\theta_x)\theta_y = (k)\theta_{xy}$.

Através do Lema 1.1.11, podemos estabelecer uma maneira de operar dois elementos da forma kq e obter um elemento em KQ. Dados $k_1q_1, k_2q_2 \in G$, temos

$$k_1q_1k_2q_2 = k_1q_1k_2q_1^{-1}q_1q_2 = k_1(k_2)\theta_{q_1}q_1q_2,$$

onde $k_1(k_2)\theta_{q_1}, \in K$ e $q_1q_2 \in Q$.

Sejam K, Q grupos e $\theta : Q \longrightarrow Aut(K)$ um homomorfismo. Diremos que um produto semidireto interno G de K por Q *realiza* θ se, para todo $x \in Q$ e $k \in K$, $\theta_x(k) = xkx^{-1}$.

Lema 1.1.12. Dados grupos K e Q, e um homomorfismo $\theta : Q \longrightarrow Aut(K)$, o *produto semidireto externo* $K \rtimes_\theta Q$ é o grupo de todos os pares ordenados $(k, x) \in K \times Q$ munido da operação $(k_1, x)(k_2, y) = (k_1\theta_x(k_2), xy)$.

Teorema 1.1.13. Dados dois grupos K e Q, e um homomorfismo $\theta : Q \longrightarrow Aut(K)$, então $G = K \rtimes_\theta Q$ é um produto semidireto interno de K por Q que realiza θ.

Demonstração. Vimos no Lema 1.1.11 que G é um grupo. Veremos agora que G é um produto semidireto interno de K por Q. Defina a aplicação

$$\begin{array}{cccc} \pi : & G & \longrightarrow & Q \\ & (k,x) & \longmapsto & x. \end{array}$$

A aplicação π é um homomorfismo, pois

$$((k_1, x)(k_2, y))\pi = (k_1(k_2)\theta_x, xy)\pi = xy = ((k_1, x))\pi((k_2, y))\pi.$$

A aplicação é sobrejetiva, visto que para todo $x \in Q$, existe $(k,x) \in G$ tal que $\pi(k,x) = x$, e $Ker\,\pi = \{(k,e) \mid k \in K\}$.

Identificamos K com o subgrupo normal $K^* = Ker\,\pi$ de G através do isomorfismo $k \mapsto (k,e)$, e o subgrupo $Q^* = \{(e,x) \mid Q\}$ com Q pelo isomorfismo $x \longmapsto (e,x)$. Note que $G = K^*Q^*$, $K^* \lhd G$ e que $K^* \cap Q^* = \{(e,e)\}$, assim, G é o produto semidireto interno de K^* com Q^*. Neste sentido, dizemos que G é o produto semidireto interno de K por Q. $\square$

O resultado a seguir estabelece a equivalência entre os produtos semidireto interno e externo.

Teorema 1.1.14. Se G é um produto semidireto interno de K por Q, então existe uma aplicação $\theta : Q \longrightarrow Aut(K)$ com $G \simeq K \rtimes_\theta Q$.

Demonstração. Seja $(k)\theta_x = xkx^{-1}$. Pelo Lema 1.1.3, cada $g \in G$ tem uma única expressão $g = kx$ onde $k \in K$ e $x \in Q$. Como a multiplicação em G satisfaz

$$k_1xk_2y = k_1xk_2x^{-1}xy = k_1(k_2)\theta_x xy,$$

a aplicação

$$\begin{array}{rcl} \varphi : K \rtimes_\theta Q & \longrightarrow & G \\ (k,x) & \longmapsto & kx \end{array}$$

é um isomorfismo. Com efeito, a aplicação é um homomorfismo, pois

$$((k_1,x)(k_2,y))\varphi = ((k_1(k_2)\theta_x, xy))\varphi = k_1(k_2)\theta_x xy = k_1xk_2y = ((k_1,x))\varphi((k_2,y))\varphi.$$

É injetiva e está bem definida, visto que $((k_1,x))\varphi = k_1x = k_2y = ((k_2,y))\varphi$ se, e somente se, $k_1 = k_2$ e $x = y$ (Lema 1.1.3), portanto $(k_1,x) = (k_2,y)$. Finalmente, a aplicação é sobrejetiva, uma vez que dado $g = kx \in G$, podemos tomar $(k,x) \in K \rtimes_\theta Q$ para obter $((k,x))\varphi = kx$. $\square$

1.1.3 Produto entrelaçado

Anteriormente, vimos a construção do produto direto externo através de dois grupos. Neste momento, iremos ampliar esta noção para uma quantidade arbitrária de grupos.

Definição 1.1.15. Sejam Λ um conjunto de índices e $\{G_\lambda \mid \lambda \in \Lambda\}$ uma família de grupos. Definimos o *produto cartesiano* dos G_λ's por

$$Cr_{\lambda \in \Lambda} G_\lambda = \{(g_\lambda)_{\lambda \in \Lambda} \mid g_\lambda \in G_\lambda\},$$

onde $(g_\lambda)_{\lambda\in\Lambda}$ representa um vetor cujas entradas são indexadas por $\lambda \in \Lambda$.

Com a operação

$$(g_\lambda)_{\lambda\in\Lambda}(h_\lambda)_{\lambda\in\Lambda} = (g_\lambda h_\lambda)_{\lambda\in\Lambda}$$

o conjunto $Cr_{\lambda\in\Lambda}G_\lambda$ é um grupo.

Desenvolveremos a seguir algumas noções que forneçam um subgrupo cujo número de entradas não-triviais seja finito.

Definição 1.1.16. Denominaremos por *suporte de um elemento* $(g_\lambda)_{\lambda\in\Lambda} \in Cr_{\lambda\in\Lambda}G_\lambda$ o conjunto $s((g_\lambda)_{\lambda\in\Lambda}) = \{g_\lambda \in G_\lambda \mid g_\lambda \neq e\}$, isto é, o conjunto contendo todas as entradas não triviais.

Definição 1.1.17. Definimos por *produto direto* dos G_λ's o conjunto

$$Dr_{\lambda\in\Lambda}G_\lambda = \{(g_\lambda)_{\lambda\in\Lambda} \mid g_\lambda \in G_\lambda \text{ e } (g_\lambda)_{\lambda\in\Lambda} \text{ tem suporte finito }\}.$$

Observe que $Dr_{\lambda\in\Lambda}G_\lambda$ é subgrupo de $Cr_{\lambda\in\Lambda}G_\lambda$ e que se Λ é finito, então $Cr_{\lambda\in\Lambda}G_\lambda = Dr_{\lambda\in\Lambda}G_\lambda$.

Considere K um grupo, Λ um conjunto e Q um grupo que age em Λ.

Definição 1.1.18. O *produto entrelaçado irrestrito* de K por Q é definido por

$$K wr_\Lambda Q = Cr_{\lambda\in\Lambda}K_\lambda \rtimes_\varphi Q$$

onde $K_\lambda = K$ para todo $\lambda \in \Lambda$ e a ação é definida por

$$\begin{aligned} \varphi : Q &\longrightarrow Aut(Cr_{\lambda\in\Lambda}K_\lambda) \\ q &\longmapsto \varphi_q : Cr_{\lambda\in\Lambda}K_\lambda \longrightarrow Cr_{\lambda\in\Lambda}K_\lambda \\ &\qquad\qquad (k_\lambda)_{\lambda\in\Lambda} \longmapsto (k_{q\cdot\lambda})_{\lambda\in\Lambda}. \end{aligned}$$

Definição 1.1.19. O *produto entrelaçado restrito* de K por Q é definido por

$$K \wr_\Lambda Q = Dr_{\lambda\in\Lambda}K_\lambda \rtimes_\varphi Q$$

com a mesma ação da definição anterior.

Um caso especial na construção do produto entrelaçado ocorre quando $\Lambda = Q$. Neste caso, Q é um conjunto que age em si mesmo por multiplicação à esquerda, então a ação φ da Definição 1.1.18 é dada por multiplicação à direita dos índices, isto é, $((k_\lambda)_{\lambda\in\Lambda})\varphi_q = (k_{q\lambda})_{\lambda\in\Lambda}$.

Esta ação produz uma representação por permutações dos elementos de Q, denominada representação regular. Nesse caso, escrevemos $K wr\, Q$ ($K \wr Q$) e denominamos produto entrelaçado irrestrito regular (produto entrelaçado restrito regular).

Dado um produto entrelaçado $G = K \wr_\Lambda Q$, diremos que $K^{(\Lambda)} = Dr_{\lambda\in\Lambda} K_\lambda$ é o *grupo base* de G e que $K^{(\Lambda)} \rtimes \{e\}$ é o *grupo diagonal* de G .

Exemplo 1.1.20. Seja C_2 o grupo cíclico de ordem 2, iremos explorar a estrutura de $C_2 \wr C_2$.

Sejam $\langle x\rangle$ e $\langle y\rangle$ dois grupos de ordem 2, defina $B = \langle x\rangle \times \langle x\rangle$ como sendo o grupo base de $C_2 \wr C_2$. A ação de y em B é definida por $((x_e,x_y))\varphi_y = (x_{ye},x_{yy}) = (x_y,x_e)$, onde $x_e,x_y \in \langle x\rangle$. Isto posto, note que $C_2 \wr C_2 = B \rtimes_\varphi \langle y\rangle$ é um grupo com oito elementos e que dados $r = ((x,e),y)$ e $s = ((e,e),y)$ em $C_2 \wr C_2$ segue que:

(i) $r^2 = ((x,e),y)((x,e),y) = ((x,e)((x,e))\varphi_y,y^2) = ((x,e)(e,x),e) = ((x,x),e)$, do que decorre que $r^4 = (e,(e,e))$;

(ii) $s^2 = ((e,e),y)((e,e),y) = ((e,e)((e,e))\varphi_y,e) = ((e,e),e)$;

(iii) $r^s = ((e,e),y)((x,e),y)((e,e),y) = ((e,x),e)((e,e),y) = ((e,x),y) = r^{-1}$.

Sob as considerações acima, segue que $C_2 \wr C_2$ é isomorfo ao grupo diedral D_8, gerado por r e s, tais que $r^4 = e$, $s^2 = e$ e $r^s = r^{-1}$.

1.2 Grupos solúveis

Nesta seção, iremos expor algumas definições e resultados sobre séries solúveis, grupos solúveis, série central inferior e grupos nilpotentes. Definições e resultados mais gerais podem ser consultados em [12] e [13]

Definição 1.2.1. Uma *série solúvel* de um grupo G é uma sequência de subgrupos

$$\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G,$$

onde $G_{i+1} \lhd G_i$ e G_i/G_{i+1} é abeliano, para todo i.

Os fatores da série solúvel são os grupos G_i/G_{i+1} onde $i = 0,1,\ldots,n-1$. Alguns destes fatores podem ser triviais, visto que na definição acima podemos ter $G_j = G_{j+1}$. Definiremos o comprimento da série solúvel como o número de inclusões estritas, ou equivalentemente, o número de grupos quocientes não triviais.

Definição 1.2.2. Dizemos que um grupo G é *solúvel* se admite uma série solúvel.

Exemplo 1.2.3. O grupo simétrico S_3 admite a série solúvel $\{e\} \lhd A_3 \lhd S_3$, onde $A_3/\{e\} \simeq A_3$ e $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$ são ambos abelianos. Portanto, S_3 é um grupo solúvel.

A solubilidade é uma propriedade hereditária no seguinte sentido:

Teorema 1.2.4. Todo subgrupo H de um grupo solúvel G é solúvel.

Os homomorfismos são aplicações utilizadas para se obter informações de um grupo a partir de um outro cujas propriedades sejam conhecidas. Neste contexto, solubilidade é uma informação que pode ser aferida a um grupo H caso haja um epimorfismo de um grupo G solúvel em H.

Teorema 1.2.5. Se G é um grupo solúvel e $f: G \longrightarrow H$ é um epimorfismo, então H é um grupo solúvel.

Corolário 1.2.6. Todo quociente de um grupo solúvel é solúvel.

Veremos a seguir que a solubilidade de um grupo G é uma propriedade que pode ser recuperada de um subgrupo normal H e do grupo quociente G/H, caso ambos sejam solúveis.

Teorema 1.2.7. Se $H \lhd G$ e ambos H e G/H são solúveis, então G é solúvel.

Corolário 1.2.8. Se K e Q são grupos solúveis, então $G = K \rtimes_\theta Q$ é um grupo solúvel.

O objetivo agora é construir um tipo especial de série, para isto, discorreremos sobre os *comutadores*.

Definição 1.2.9. Se $H, K \leq G$, então

$$[H,K] = \langle [h,k] \mid h \in H \text{ e } k \in K \rangle,$$

onde $[h,k] = h^{-1}k^{-1}hk$ é denominado comutador de h e k.

Note que $[H,K]$ é um subgrupo de G. No caso particular onde $H = K = G$, dizemos que $G' = [G,G]$ é o *subgrupo derivado* de G. Deste modo, podemos definir indutivamente

$$\begin{array}{rcl} G' & = & [G,G] \\ G'' & = & [G',G'] \\ G^{(3)} & = & [G'',G''] \\ & \vdots & \\ G^{(i)} & = & [G^{(i-1)},G^{(i-1)}] \end{array}$$

onde $G^{(i)}$ representa o *i-ésimo subgrupo derivado* de G.

Observação 1.2.10. Se G é um grupo e $N \lhd G$, então os elementos de $(G/N)^{(i)}$ são as classes laterais xN, onde $x \in G^{(i)}$. Entretanto, o comutador em questão nem sempre pode ser expresso por $G^{(i)}/N$, visto que se $G^{(i)} \subsetneq N$, então não podemos definir um grupo quociente $G^{(i)}/N$. Ainda assim, podemos corrigi-lo fazendo $(G/N)^{(i)} = G^{(i)}N/N$.

Encontrar os subgrupos derivados de um subgrupo H normal em G é uma técnica para se obter subgrupos normais em G, pois veremos abaixo que estes subgrupos preservam a normalidade em G.

Proposição 1.2.11. Se $H \lhd G$, então $H^{(i)} \lhd G$ para todo $i \geq 0$.

Demonstração. Utilizaremos indução em i. O caso $i = 0$ é válido por hipótese, suponha agora que o resultado seja válido para $i \geq 0$ fixado, mostraremos que vale para $i+1$. Tome $g \in G$, então

$$(H^{(n+1)})^g = [H^{(i)}, H^{(i)}]^g = [(H^{(i)})^g, (H^{(i)})^g] = [H^{(i)}, H^{(i)}] = H^{(i+1)}.$$

□

A seguir, tomaremos conhecimento de um método para construção de grupos quocientes abelianos de um grupo dado. Este método é de grande utilidade em algumas demonstrações onde se utiliza indução, e de extrema importância no contexto de grupos solúveis, uma vez que as séries almejadas possuem grupos quocientes abelianos.

Teorema 1.2.12. O subgrupo derivado G' é um subgrupo normal de G. Além disso, se $H \lhd G$, então G/H é abeliano se, e somente se, $G' \leq H$.

Decorre diretamente do teorema acima que G/G' é um grupo abeliano, basta tomar $H = G'$, além disso, G/G' é o maior grupo quociente abeliano de G. Dizemos que G/G' é a abelianização do grupo G e denotamos $G_{ab} = G/G'$.

Definição 1.2.13. A série

$$\cdots \leq G^{(3)} \leq G'' \leq G' \leq G^{(0)} = G$$

é denominada *série derivada* de G.

A série derivada é uma grande candidata a série solúvel de um grupo G, pois como observado anteriormente, seus quocientes são abelianos. Isto posto, dado um grupo solúvel, buscaremos uma relação entre a série derivada e uma série solúvel arbitrária.

Lema 1.2.14. Sejam G um grupo e $\{e\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$ uma série solúvel de G. Então $G^{(i)} \leq G_i$.

O resultado abaixo nos indica uma condição necessária e suficiente para que um grupo seja solúvel.

Teorema 1.2.15. Um grupo G é solúvel se, e somente se, $G^{(n)} = \{e\}$ para algum n.

Observe que os resultados do Lema 1.2.14 e do Teorema 1.2.15 nos afirmam que a série derivada é a menor série solúvel de um grupo G. Além disso, basta conhecer o comportamento da série derivada de um grupo para aferir se um grupo é solúvel ou não.

Produtos entrelaçados serão recorrentes ao decorrer deste trabalho, isto posto, iremos desenvolver a seguir dois resultados que relacionam produto entrelaçado e solubilidade.

Proposição 1.2.16. Se H é um grupo e Λ é um família de índices. Então

$$(Cr_{\lambda\in\Lambda}H)^{(n)} = Cr_{\lambda\in\Lambda}H^{(n)}.$$

Demonstração. Por indução em n.

Sejam $n = 1$ e $(g_\lambda)_{\lambda\in\Lambda}, (h_\lambda)_{\lambda\in\Lambda} \in Cr_{\lambda\in\Lambda}H$, então $[(g_\lambda)_{\lambda\in\Lambda}, (h_\lambda)_{\lambda\in\Lambda}] = ([g_\lambda, h_\lambda])_{\lambda\in\Lambda}$ e $(Cr_{\lambda\in\Lambda}H)' = Cr_{\lambda\in\Lambda}H'$.

Suponha que o resultado seja válido para $n-1$, com $n \geq 1$. Então

$$\begin{aligned}
(Cr_{\lambda\in\Lambda}H)^{(n)} =& [(Cr_{\lambda\in\Lambda}H)^{(n-1)}, (Cr_{\lambda\in\Lambda}H)^{(n-1)}] \\
=& [Cr_{\lambda\in\Lambda}H^{(n-1)}, Cr_{\lambda\in\Lambda}H^{(n-1)}] \\
=& Cr_{\lambda\in\Lambda}[H^{(n-1)}, H^{(n-1)}] \\
=& Cr_{\lambda\in\Lambda}H^{(n)}.
\end{aligned}$$

□

Proposição 1.2.17. Se H e K são grupos solúveis, então $H \wr K$ é solúvel.

Demonstração. Seja $G = H \wr K = Dr_{k\in K}H \rtimes K$, então $Dr_{k\in K}H \lhd G$ e $G/Dr_{k\in K}H \simeq K$ é solúvel. Além disso, como H é solúvel segue que existe $n \in \mathbb{N}$ tal que $H^{(n)} = \{e\}$, então $(Dr_{k\in K}H)^{(n)} = Dr_{k\in K}H^{(n)} = Dr_{k\in K}\{e\} = \{e\}$ implica a solubilidade de $Dr_{k\in K}H$. Portanto, G é solúvel. □

Anteriormente, utilizamos os comutadores para a construção da série derivada, faremos uso desta ferramenta novamente, desta vez, para definir indutivamente os subgrupos

$$\gamma_1(G) = G; \quad \gamma_{i+1}(G) = [\gamma_i(G), G].$$

Veremos que esta família de subgrupos possui propriedades que a caracterizam como um novo tipo de série.

Proposição 1.2.18. Sejam G um grupo e $H \lhd G$. Então $\gamma_i(H) \lhd G$ para todo $i \geq 1$. Além disso, $\gamma_{i+1}(H) \leq \gamma_i(H)$ e $\gamma_i(H)/\gamma_{i+1}(H) \leq Z(H/\gamma_{i+1}(H))$.

Demonstração. Faremos a demonstração através de indução em i.

Para $i = 1$ temos que $\gamma_1(H) = H$. Suponha por hipótese de indução que o resultado é válido para $i = n$, mostraremos que o resultado é verdadeiro para $i = n+1$. Tome $[x,y] \in [\gamma_n(H),H] = \gamma_{n+1}(H)$ e $g \in G$, então $[x,y]^g = [x^g,y^g]$. Por hipótese de indução, $\gamma_n(H) \lhd G$, então $x^g \in \gamma_n(H)$, como $y^g \in G$ temos que $[x,y]^g \in \gamma_{n+1}(H)$, do qual concluímos $\gamma_{n+1}(H) \lhd G$.

Para a segunda parte, tome $x \in \gamma_i(H)$ e $y \in H$, então $[x,y] = x^{-1}x^y \in \gamma_i(H)$. Daí, temos que $\gamma_{i+1}(H) = [\gamma_i(H),H] \leq \gamma_i(H)$. Finalmente, como $\gamma_{i+1}(H) \lhd G$, temos $\gamma_{i+1}(H) \lhd \gamma_i(H)$, assim, o grupo quociente $\gamma_i(H)/\gamma_{i+1}(H)$ está bem definido. Sejam $x \in \gamma_i(H)$ e $y \in H$ elementos arbitrários, então $[x,y] \in \gamma_{i+1}(H)$ por definição, deste modo, temos a igualdade $[x,y]\gamma_{i+1}(H) = \gamma_{i+1}(H)$. Portanto, $\gamma_i(H)/\gamma_{i+1}(H) \leq Z(H/\gamma_{i+1}(H))$. □

O resultado acima motiva a definição de uma nova série.

Definição 1.2.19. Seja G um grupo, a série

$$\cdots \leq \gamma_2(G) \leq \gamma_1(G) = G$$

é denominada *série central inferior* de G.

Definição 1.2.20. Um grupo G é *nilpotente* se existe um inteiro c tal que $\gamma_{c+1}(G) = \{e\}$, neste caso, c é chamado de *classe de nilpotência* do grupo G.

Grupos nilpotentes possuem uma propriedade interessante a qual não iremos demonstrar, a propriedade em questão é que em grupos nilpotentes finitos existem subgrupos para todo divisor de sua ordem, isto é, a recíproca do Teorema de Lagrange é válida para grupos nilpotentes finitos.

1.3 Grupos livres

A ideia intuitiva de um grupo F ser livre é a existência de um subconjunto X com a propriedade de que todo elemento em F é expresso unicamente como um produto dos elementos em $X \cup X^{-1}$, onde $X^{-1} = \{x^{-1} \mid x \in X\}$. Caso isto não ocorra, encontraremos uma relação entre os elementos de F. Por exemplo, no grupo ciclíco C_n, temos a relação

$g^n = e$, onde g é um gerador de C_n. Esta seção foi estruturada com base em [7] e [12], nela, definiremos o grupo livre segundo a ideia intuitiva, posteriormente, o definiremos segundo uma propriedade universal e concluiremos que estas definições são equivalentes. Além disso, estudaremos grupos relativamente livres, isto é, são grupos livres com exceção de alguma propriedade.

Definição 1.3.1. Seja X um conjunto de símbolos, uma *palavra* em X é um elemento da forma $w = x_1x_2 \dots x_n$, $n \geq 0$ um inteiro, com $x_i \in X$ para $i = 1, \dots n$. Dizemos que n é o *comprimento da palavra*, caso $n = 0$, teremos a palavra vazia, representada por e.

A definição acima deve ser encarada no sentido literal, isto é, X representa um *alfabeto* cujos símbolos são letras, e uma concatenação de letras é uma palavra. Construa o alfabeto $X^{-1} = \{x^{-1} \mid x \in X\}$ e defina $X^{\pm} := X \cup X^{-1}$. Perceba que xx^{-1} é uma palavra sobre o alfabeto $X^{\pm}$, utilizando-se desta analogia, se escrevessemos em um papel a palavra xx^{-1}, esta palavra não desaparece por si só, isto posto, xx^{-1} não representa a palavra vazia e.

O fato de que $xx^{-1} \neq e$ causa certo incomodo, entretanto, na vida real, é sempre possível apagar uma palavra. Nosso próximo passo e realizar um procedimento que permita apagar palavras da forma xx^{-1}. Seja w uma palavra em $X^{\pm}$. Descarte de w todos os pares dos tipos xx^{-1} e $x^{-1}x$, a palavra resultante desse processo de redução é chamada de *forma reduzida* de w. Perceba que caso haja redução de uma palavra w para a forma reduzida w_r, temos $w \neq w_r$, pois, assim como na vida real, palavras são diferentes se são escritas diferentes.

Exemplo 1.3.2. Seja $X = \{a, b, c\}$ o alfabeto, então $X^{\pm} = \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$. Seja $w = aa^{-1}bc^{-1}cb^{-1}a$ uma palavra em $X^{\pm}$, a forma reduzida de w é $w_r = a$.

Sob esta abordagem, podemos definir um grupo livre sobre a noção intuitiva.

Definição 1.3.3. Um grupo F é dito *livre* se existe um subconjunto gerador X tal que toda palavra reduzida não vazia em $X^{\pm}$ define um elemento não trivial de F.

A seguir, desenvolveremos um método para construir um grupo livre.

Teorema 1.3.4. Seja X um alfabeto, o conjunto $F(X)$ de palavras reduzidas em $X^{\pm}$ é um grupo livre.

Demonstração. Iniciaremos mostrando que $F(X)$ é um grupo. Para isto, defina a operação binária "concatenação com redução", isto é, dados $w_1, w_2 \in F(X)$, onde $w_1 = x_1 \dots x_l$ e $w_2 = y_1 \dots y_m$ com $l, m \geq 0$, faça $w_1w_2 = x_1 \dots x_{l-r}y_{r+1} \dots y_m$, onde r é tal que x_{l-r} não possa ser removido, em outras palavras, onde $x_{l-r}y_{r+1} \neq x_{l-r}x_{l-r}^{-1}$. O fechamento da operação é assegurado, pois a concatenação com redução de duas palavras reduzidas resulta uma palavra reduzida, assim $w_1w_2 \in F(X)$. A palavra vazia e é a identidade e o inverso é $(x_1 \dots x_n)^{-1} = x_n^{-1} \dots x_1^{-1}$, onde $(x^{-1})^{-1} = x$. Para a associatividade, tome w_1, w_2, w_1w_2 assim como definido acima e tome $w_3 = z_1 \dots z_n$, donde $w_2w_3 = y_1 \dots y_{m-s}z_{s+1} \dots z_n$ em $F(X)$. Se uma das palavras w_1, w_2 ou w_3 for a palavra vazia, a associatividade é imediata, então assumiremos $l, m, n \geq 1$. Temos três casos para considerar.

Caso 1: $r + s < m$

$$\begin{aligned}
(w_1w_2)w_3 &= (x_1 \dots x_{l-r}y_{r+1} \dots y_m)z_1 \dots z_n \\
&= x_1 \dots x_{l-r}y_{r+1} \dots y_{m-s}z_{s+1} \dots z_n \\
&= x_1 \dots x_l(y_1 \dots y_{m-s}z_{s+1} \dots z_n) \\
&= w_1(w_2w_3)
\end{aligned}$$

Caso 2: $r + s = m$

$$\begin{aligned}
(w_1w_2)w_3 &= (x_1 \dots x_{l-r}y_{r+1} \dots y_m)z_1 \dots z_n \\
&= x_1 \dots x_{l-r}z_{s+1} \dots z_n \\
&= x_1 \dots x_l(y_1 \dots y_{m-s}z_{s+1} \dots z_n) \\
&= w_1(w_2w_3)
\end{aligned}$$

Caso 3: $r + s > m$

Faça $\beta = y_1 \dots y_{m-s}$, $\gamma = y_{m-s+1} \dots y_r$ e $\delta = y_{r+1} \dots y_m$, por hipótese, $r + s > m$, portanto, γ tem comprimento positivo. Assim, podemos escrever $\beta\gamma = y_1 \dots y_r$ e $\gamma\delta = y_{m-s+1} \dots y_m$, donde concluímos que $(\beta\gamma)^{-1} = x_{l-r+1} \dots x_l$ e $(\gamma\delta)^{-1} = z_1 \dots z_s$. Isto posto, segue que

$$\begin{aligned}
w_2 &= \beta\gamma\delta, && \text{é definido sem ambiguidade, pois não há cancelamentos} \\
w_1 &= \alpha\gamma^{-1}\beta^{-1}, && \text{onde} \quad \alpha = x_1 \dots x_{l-r}, \text{ e} \\
w_3 &= \delta^{-1}\gamma^{-1}\varepsilon, && \text{onde} \quad \varepsilon = z_{s+1} \dots z_n.
\end{aligned}$$

Então

$$(w_1w_2)w_3 = (\alpha\gamma^{-1}\beta^{-1}\beta\gamma\delta)(\delta^{-1}\gamma^{-1}\varepsilon) = (\alpha\delta)(\delta^{-1}\gamma^{-1}\varepsilon) = \alpha(\gamma^{-1}\varepsilon)$$

e

$$w_1(w_2w_3) = (\alpha\gamma^{-1}\beta^{-1})(\beta\gamma\delta\delta^{-1}\gamma^{-1}\varepsilon) = (\alpha\gamma^{-1}\beta^{-1})(\beta\varepsilon) = (\alpha\gamma^{-1})\varepsilon$$

Como α e γ^{-1} são consecutivos na palavra reduzida $w_1 = \alpha\gamma^{-1}\beta^{-1}$, não há cancelamentos no produto $\alpha\gamma^{-1}$. Analogamente, não há cancelamentos no produto $\gamma^{-1}\varepsilon$, pois é um fator da palavra reduzida $w_3 = \delta^{-1}\gamma^{-1}\varepsilon$. Isto posto, segue que

$$\alpha(\gamma^{-1}\varepsilon) = (\alpha\gamma^{-1})\varepsilon = \alpha\gamma^{-1}\varepsilon,$$

portanto,

$$w_1(w_2w_3) = (w_1w_2)w_3.$$

Resta mostrar que $F(X)$ é livre em X. Por hipótese, X é um alfabeto gerador de $F(X)$, deste modo, toda palavra reduzida não-vazia em $X^{\pm}$ define um elemento não trivial. $\square$

Se por um lado, a definição intuitiva de um grupo livre permite a compreensão da estrutura de tal grupo, por outro lado, falha em exprimir a relevância do grupo em questão. A seguir, daremos uma nova definição para o grupo livre, fazendo uso de uma propriedade universal. Ao final, mostraremos a equivalência das duas definições.

Definição 1.3.5. Um grupo F é denominado *livre* em um subconjunto $X \subseteq F$ se, dado qualquer grupo G e qualquer aplicação $\theta : X \longrightarrow G$, existe um único homomorfismo $\theta' : F \longrightarrow G$ estendendo θ, isto é, tendo a propriedade que $(x)\theta' = (x)\theta$ para todo $x \in X$, ou equivalentemente que o diagrama

$$\begin{tikzcd} F \arrow[drr, dashed, "\exists!\theta'"] & & \\ X \arrow[u, hook, "i"] \arrow[rr, "\theta"'] & & G \end{tikzcd}$$

comute, onde $i : X \longrightarrow F$ é a aplicação inclusão definida por $x \longmapsto x$.

Observação 1.3.6. Seja F um grupo arbitrário, $X \subseteq F$ e G um grupo qualquer. Sejam $Hom(F,G)$ o conjunto de homomorfismos de F em G, $Apl(X,G)$ o conjunto de aplicações de X em G e

$$\begin{aligned} \rho : Hom(F,G) &\longrightarrow Apl(X,G) \\ \varphi &\longmapsto i \circ \varphi \end{aligned}$$

onde $i : X \longrightarrow F$ é a inclusão. Deste modo, $\varphi \circ inc = \varphi|_X$. Isto é, ρ pega um homomorfismo $\varphi : F \longrightarrow G$ e aplica na restrição à X. Então

(i) ρ é sobrejetivo se, e somente se, para todo θ, existe θ' como na Definição 1.3.5,

(ii) ρ é injetivo se, e somente se, θ' existe e é único.

Assim, F é livre em X se, e somente se, a aplicação ρ é uma bijeção para qualquer grupo G.

O lema a seguir fornece uma condição necessária para determinar se um grupo é livre sobre um subconjunto.

Lema 1.3.7. Se F é livre em X, então X gera F.

Demonstração. Seja $H = \langle X \rangle := \bigcap\{K \leq F \mid K \supseteq X\}$ e $\theta : X \longrightarrow H$ a inclusão de X em H, com $\theta' : F \longrightarrow H$ denotando a extensão correspondente. Defina $\iota : H \longrightarrow F$ a inclusão de H em F, através do diagrama

$$\begin{tikzcd}
F \arrow[dr, "\theta'"] \arrow[drr, "I_F"] & & \\
X \arrow[u, hook, "i"] \arrow[r, hook, "\theta"'] & H \arrow[r, hook, "\iota"'] & F
\end{tikzcd}$$

note que $\theta'\iota$ estende $\theta\iota = i$. Mas a aplicação identidade I_F também estende $\theta\iota = i$. Além disso, ι é a inclusão de H em F, então $Im\,\theta'\iota = Im\,\theta'$. Por unicidade, $\theta'\iota = I_F$, daí temos que $F = ImI_F = Im\,\theta'\iota = Im\,\theta' \subseteq H$. $\square$

Proposição 1.3.8. Se F_i é livre em X_i, com $i = 1,2$, e $F_1 \simeq F_2$, então existe uma bijeção de X_1 em X_2.

Demonstração. Aplicaremos a Observação 1.3.6 no grupo $G = \mathbb{Z}/2\mathbb{Z}$ de ordem 2. Note que $Hom(F_i, \mathbb{Z}/2\mathbb{Z})$ é um espaço vetorial com base X_i sobre o corpo $\mathbb{Z}/2\mathbb{Z}$. Por hipótese, $F_1 \simeq F_2$, denote este isomorfismo por φ. Então a aplicação de $Hom(F_1, \mathbb{Z}/2\mathbb{Z})$ em $Hom(F_2, \mathbb{Z}/2\mathbb{Z})$ definida por $\phi \mapsto \varphi\phi$ é um isomorfismo. Como os espaços vetoriais são isomorfos, então existe uma bijeção entre as bases X_1 e X_2. $\square$

Proposição 1.3.9. Se F_i é livre em X_i, com $i = 1,2$, e existe uma bijeção entre X_1 e X_2, então $F_1 \simeq F_2$.

Demonstração. Sejam $\kappa : X_1 \longrightarrow X_2$ uma bijeção, θ, φ as extensões

$$\begin{tikzcd}
F_1 \arrow[drr, "\theta"] & & \\
X_1 \arrow[u, hook] \arrow[r, "\kappa"'] & X_2 \arrow[r, hook, "j"'] & F_2
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
F_2 \arrow[drr, "\varphi"] & & \\
X_2 \arrow[u, hook] \arrow[r, "\kappa^{-1}"'] & X_1 \arrow[r, hook, "i"'] & F_1
\end{tikzcd}$$

Agora, para todo $x_1 \in X_1$, $(x_1)\theta\varphi = ((x_1)\kappa)\varphi = ((x_1)\kappa)\kappa^{-1} = x_1$, então a aplicação $\theta\varphi : F_1 \longrightarrow F_1$ estende $i : X_1 \longrightarrow F_1$. Mas a aplicação identidade I_{F_1} também estende $i : X_1 \longrightarrow F_1$, assim $\theta\varphi = I_{F_1}$ por unicidade. Similarmente, $\varphi\theta = I_{F_2}$, assim, θ é um isomorfismo. $\square$

Vimos que se F é livre em X então X gera F. Além disso, se fizermos $F = F_1 = F_2$, $X = X_1$ e $X_2 = Y$ na Proposição 1.3.8 temos uma bijeção entre X e Y. Isto posto, diremos que X é a *base* de F e $|X|$ é o *posto* de F.

O Teorema abaixo relaciona nossa definição de um grupo livre com a ideia intuitiva.

Teorema 1.3.10. Um grupo F é livre em um subconjunto X se, e somente se, X gera F e nenhuma palavra reduzida em $X^{\pm}$ de comprimento positivo é igual a e.

Demonstração. Seja $F(X)$ o grupo livre construído com base X, $\theta : X \longrightarrow F(X)$ a inclusão de X em F e $\theta' : F(X) \longrightarrow F$ o homomorfismo estendendo θ, deste modo,

$$(w)\theta' = (x_1 \dots x_n)\theta' = (x_1)\theta' \dots (x_n)\theta' = (x_1)\theta \dots (x_n)\theta = x_1 \dots x_n = w.$$

($\Rightarrow$) Se F é livre em X, então o Lema 1.3.7 afirma que X gera F. Note que θ' é injetiva, pois é a inclusão de $F(X)$ em F, deste modo, $(w)\theta' = e$ se, e somente se $w = e$, assim nenhuma palavra reduzida de comprimento positivo em $X^{\pm}$ é igual a e.

($\Leftarrow$) Se X gera F então θ' é sobrejetiva, pois $(w)\theta' = w$.

Se nenhuma palavra reduzida de comprimento positivo em $X^{\pm}$ é igual a e, então $(w)\theta' = e$ se, e somente se, $w = e$. Logo θ' é injetiva.

Portanto, θ' é um isomorfismo entre o grupo livre $F(X)$ e F, o que garante que F é livre em X. $\square$

Neste momento, iremos explorar as vantagens provenientes da definição de grupo livre através da propriedade universal.

Proposição 1.3.11. Todo grupo é isomorfo a um grupo quociente de algum grupo livre.

Demonstração. Dado um grupo G, tome X como um conjunto de geradores para G. Seja $\theta' : F(X) \longrightarrow G$ a extensão da inclusão $\theta : X \longrightarrow G$. Agora, $Im\,\theta' = G$, pois $G = \langle X \rangle$, com a notação $K = Ker\,\theta'$, o Primeiro Teorema do Isomorfismo afirma que

$$G = Im\,\theta' \simeq F(X)/K.$$

Dizemos que $F(X)/K$ é uma apresentação para G. $\square$

Iremos enunciar o conceito de apresentação de um grupo. Para tal, seja X um conjunto, $F = F(X)$ o grupo livre em X, $R \subset F$, $R^F = \langle w^{-1}Rw \mid w \in F \rangle$ o *fecho normal* de R em F e $G = F/R^F$. Seja $\bar{x}$ o representante da classe lateral $R^F x$. Note que $\overline{X} = \{\bar{x} \mid x \in X\}$ é um gerador de G e que as palavras em R^F representam a identidade em G, isto é, são relações de G.

Definição 1.3.12. Com a notação acima, $G = \langle X \mid R \rangle$ é chamado de *apresentação* de G. Os elementos de X são chamados de *geradores* e os de R de *relatores*.

A priori, somos induzidos a pensar que a apresentação de um grupo, tal como descrito acima, é da forma $G = \langle \overline{X} \mid R^F \rangle$, pois $\overline{X}$ gera G e R^F é o subgrupo normal de F. A apresentação descrita na Definição 1.3.12 é fruto de um aperfeiçoamento estético e matemático de $\langle \overline{X} \mid R^F \rangle$. Para tal, podemos cometer o abuso de notação de utilizar X ao invés de $\overline{X}$, desde que interpretemos R^F como o conjunto que descreve as identidades em G. Isto posto, note que se $u \in R^F$, então $\overline{uw} = \overline{w}$, para pode utilizar nossa convenção, uw e w devem representar o mesmo elemento em G, como u é uma identidade em G, temos $uw = ew = w$. Para a segunda parte, veja que os geradores de R^F são da forma r^w, onde $r \in R$ e $w \in F$ como r já é a identidade em G, pois $r \in R^F$, temos $r^w = w^{-1}rw = w^{-1}w = e$. Isto posto, concluímos que R é suficente para descrever as relações que ocorrem em G.

Exemplo 1.3.13. Um grupo livre F em X tem apresentação $F = \langle X \mid \quad \rangle$, isto é, não possui um conjunto R de relatores.

Tomando $r \in R$, dizemos que $r = e$ é uma *relação* em G. Convenientemente, podemos utilizar o conjunto de equações $R = e$ ao invés de R.

Exemplo 1.3.14. Seja $F = \langle x \rangle$ um grupo livre de posto 1. Seja $\{x^n\} \subset F$ e $N = \{x^n\}^F$ o fecho normal de $\{x^n\}$ em F. Tomando $G = F/N$, segue que G possui apresentação, $G = \langle x \mid x^n \rangle$, ou utilizando as relações ao invés dos relatores $G = \langle x \mid x^n = e \rangle$. Note que G assim definido é uma apresentação livre para $\mathbb{Z}/n\mathbb{Z}$.

O próximo resultado nos permitirá, sobre certas condições, obter homomorfismos entre grupos com mesmo conjunto gerador.

Lema 1.3.15. Sejam F, G, H grupos e $\alpha : F \longrightarrow G$, $\beta : F \longrightarrow H$ homomorfismos tais que $Im\,\alpha = G$ e $Ker\,\alpha \subseteq Ker\,\beta$. Então existe um homomorfismo $\gamma : G \longrightarrow H$ tais que $\alpha\gamma = \beta$.

Demonstração. Queremos encontrar um homomorfismo $\gamma : G \longrightarrow H$ que faça o diagrama

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

comute.

Dado $g \in G$, tome $f \in F$ tal que $(f)\alpha = g$ e defina $(g)\gamma = (f)\beta$. Um elemento f satisfazendo essas condições existe, pois $Im\,\alpha = G$ e γ está bem definida, uma vez que

$Ker\,\alpha \subseteq Ker\,\beta$ implica

$$(f_1)\alpha = (f_2)\alpha \Longleftrightarrow f_1 f2^{-1} \in Ker\,\alpha \Longrightarrow f_1 f2^{-1} \in Ker\,\beta \Longrightarrow (f_1)\beta = (f_2)\beta.$$

Agora, sejam $g_1, g_2 \in G$ e $f_1, f_2 \in F$ tais que $(f_1)\alpha = g_1$ e $(f_2)\alpha = g_2$. Como α é um homomorfismo, $(f_1 f_2)\alpha = g_1 g_2$, além disso,

$$\begin{aligned}(g_1g_2)\gamma &= (f_1f_2)\beta, \text{ por definição de } \gamma,\\ &= (f_1)\beta(f_2)\beta, \text{ pois } \alpha \text{ é um homomorfismo},\\ &= (g_1)\gamma(g_2)\gamma,\end{aligned}$$

donde concluímos que γ é um homomorfismo.

Finalmente, note que $f \in ((f)\alpha)\alpha^{-1}$, para todo $f \in F$, deste modo, temos a igualdade $((f)\alpha)\gamma = (g)\gamma = (f)\beta$, isto é, $\alpha\gamma = \beta$. □

Apresentaremos a seguir um resultado útil no contexto de grupos com apresentações similares e apresentações de grupos quocientes.

Proposição 1.3.16 (von Dyck)**.** Seja $F(X)$ um grupo livre sobre X. 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 $\phi : G \longrightarrow H$ fixando todo elemento $x \in X$ e tal que $Ker\,\phi = (S/R)^F$. Reciprocamente, todo grupo quociente de $G = \langle X \mid R\rangle$ tem apresentação $\langle X \mid S\rangle$ com $R \subseteq S$.

Demonstração. Sejam $\alpha : F(X) \longrightarrow G$ e $\beta : F(X) \longrightarrow H$ aplicações naturais. Como α é uma sobrejeção e $Ker\,\alpha = R^F \subseteq S^F = Ker\,\beta$, pelo Lema 1.3.15, existe um homomorfismo $\gamma : G \longrightarrow H$. Faça $\phi = \gamma$, como $(x)\alpha = x$ e $(x)\beta = x$ para todo $x \in X$, então $(x)\phi = (x)\alpha\phi = (x)\beta = x$, donde concluímos que θ fixa todos os elementos em X. O homomorfismo ϕ é sobrejetivo, pois $\beta = \alpha\phi$ e as aplicações α e β também o são. Além disso, $(f)\alpha\phi = (f)\beta = e$ implica $f \in (Ker\,\beta)\alpha$, portanto, $Ker\,\phi = (Ker\,\beta)\alpha = (S^F)\alpha = (S/R)^F$, pois $(R)\alpha = \{e\}$ em G.

Reciprocamente, seja H um grupo quociente e G. Defina ψ como a composição $\alpha\theta$, então $R \subseteq Ker\,\psi$ e $H = \langle X \mid Ker\,\psi\rangle$. □

Anteriormente, construimos uma família de grupos cujos elementos não possuem relações, o que exprimi a ideia de "liberdade" entre os elementos dos grupos livres. Estenderemos este conceito para os grupos satisfazendo uma propriedade $\mathcal{P}$.

Definição 1.3.17. Seja F_∞ um grupo livre sobre um conjunto infinito enumerável $\{x_1, x_2, \dots\}$ e seja W um subconjunto não-vazio de F_∞. Se $w = x_{i_1}^{l_1} \dots x_{i_r}^{l_r} \in W$ e $g_1, \dots, g_r$ elementos de um grupo G, definimos o valor da palavra w em $g_1, \dots, g_r$ como sendo $w(g_1, \dots, g_r) = g_1^{l_1} \dots g_r^{l_r}$.

O subgrupo de G gerado por todos os valores em G das palavras em W é denominada *subgrupo verbal* de G determinado por W e denotado por

$$W(G) = \langle w(g_1, g_2, \dots) \mid g_i \in G, w \in W \rangle.$$

Exemplo 1.3.18. Se $W = \{[x_1, x_2]\}$ e G é um grupo, então $W(G) = G'$.

Com a finalidade de estender a noção de grupos livres, precisamos de um método de coletar grupos que compartilham de uma propriedade. A definição abaixo irá suprir esta necessidade inicial.

Definição 1.3.19. Uma *classe de grupos* $\mathcal{C}$ é uma coleção de conjuntos, cujos membros são grupos, e detém as propriedades de que

(i) $\mathcal{C}$ contém um grupo de ordem 1,

(ii) Se $G \in \mathcal{C}$, então $H \in \mathcal{C}$ sempre que $H \simeq G$.

Se, por exemplo, definirmos $\mathcal{C}$ como a coleção de todos os grupos finitos, ou todos os grupos abelianos, segue que $\mathcal{C}$ é uma classe de grupos finitos, ou uma classe de grupos abelianos, respectivamente.

Definição 1.3.20. Uma *variedade* é uma classe de grupos definida equacionalmente. Mais precisamente, se W é um conjunto de palavras em $x_1, x_2, \dots$, a classe de todos os grupos G tais que $W(G) = \{e\}$ é denominada *variedade* $\mathcal{B}(W)$ determinada por W. Dizemos que W é um conjunto de leis para a variedade $\mathcal{B}(W)$.

Exemplo 1.3.21.

(i) Se $W = \{[x, y]\}$, então $\mathcal{B}(W)$ é a classe de grupos abelianos.

(ii) Se $W = \{[[x_1, x_2], [x_3, x_4]]\}$, então $\mathcal{B}(W)$ é a classe de grupos metabelianos.

(iii) Defina indutivamente $s_1 = [x_1, x_2]$, $s_2 = [[x_1, x_2], [x_3, x_4]]$ e $s_l = [s_{l-1}(x), s_{l-1}(y)]$ o comutador envolvendo 2^l variavéis. Se $W = \{s_1, \dots, s_l\}$, então $\mathcal{B}(W)$ é a classe de grupos cujo comprimento da série derivada é no máximo l.

(iv) Se $W = \{[x_1, x_2, \dots, x_c]\}$, então $\mathcal{B}(W)$ é a classe de todos os grupos cuja classe de nilpotência é menor ou igual a c.

Agora, estamos aptos a estender o conceito de grupos livres para classes de grupos.

Definição 1.3.22. Sejam $\mathcal{B}$ uma variedade, $F \in \mathcal{B}$ um grupo e X um conjunto não vazio de F. Dizemos que F é um grupo $\mathcal{B}$ livre se para qualquer aplicação $\theta : X \longrightarrow G$, onde $G \in \mathcal{B}$, existe um único homomorfismo $\theta' : F \longrightarrow G$ estendendo θ, isto é, tendo a propriedade que $\theta'(x) = \theta(x)$ para todo $x \in X$, ou equivalentemente que o diagrama

$$\begin{tikzcd} F \arrow[dr, dashed, "\exists!\theta'"] & \\ X \arrow[u, hook, "i"] \arrow[r, "\theta"'] & G \end{tikzcd}$$

comute, onde $i : X \longrightarrow F$ é a aplicação inclusão definida por $x \longmapsto x$.

Grupos que são livres em alguma variedade são também chamados de *relativamente livres*. Veremos que os grupos livres podem ser utilizados para descrever grupos livres sobre uma variedade $\mathcal{B}$.

Proposição 1.3.23. Seja X um conjunto não-vazio, F^* um grupo livre em X, e $\mathcal{B}$ uma variedade com conjunto de leis W. Então, $F = F^*/W(F^*)$ é um grupo $\mathcal{B}$ livre em X. Além disso, todo grupo $\mathcal{B}$ livre em X é isomorfo a F.

Demonstração. Seja $\sigma^* : X \longrightarrow F^*$ uma aplicação injetiva e $\nu : F^* \longrightarrow F$ o homomorfismo natural. Tome $\sigma = \sigma^*\nu$. Suponha que G é um grupo da variedade $\mathcal{B}$ e $\alpha : X \longrightarrow G$ uma aplicação. Como F^* é livre em X, existe um único homomorfismo $\beta : F^* \longrightarrow G$ tais que $\sigma^*\beta^* = \alpha$. Como $G \in \mathcal{B}$, temos $W(G) = \{e\}$, então $W(F^*)\beta = \{e\}$. Consequentemente, a aplicação $\beta : F \longrightarrow G$ definida por $W(F^*)x \mapsto (x)\beta^*$ é um homomorfismo. Agora, $(x)\nu\beta = (W(F^*)x)\beta = (x)\beta^*$, então $\nu\beta = \beta^*$ e $\sigma\beta = \sigma^*\nu\beta = \sigma^*\beta^* = \alpha$. Daí, temos a comutatividade da parte inferior do diagrama

$$\begin{tikzcd} & F^* \arrow[d, dashed, "\nu"] \arrow[ddr, "\beta^*"] & \\ & F \arrow[dr, dashed, "\beta"] & \\ X \arrow[uur, "\sigma^*"] \arrow[ur, dashed, "\sigma"] \arrow[rr, "\alpha"'] & & G \end{tikzcd}.$$

Se $\beta' : F \longrightarrow G$ é um outro homomorfismo satisfazendo as condições acima, $\sigma^*(\nu\beta') = \sigma\beta' = \alpha = \sigma^*\beta^*$, daí $\nu\beta' = \beta^* - \nu\beta$ pela unicidade de β^*. Decorre da sobrejetividade de ν que $\beta = \beta'$. Portanto, F é $\mathcal{B}$ livre em X.

Para a segunda parte, basta revisitar a Proposição 1.3.9 e trocar o substantivo grupo livre por grupo $\mathcal{B}$ livre. □

Note que a Proposição 1.3.8 pode ser adaptada para as variedades no Exemplo 1.3.21, visto que $\mathbb{Z}/2\mathbb{Z}$ pertence as variedades deste exemplo. Para a adaptação, basta trocar o substantivo livre por $\mathcal{B}$ livre, onde $\mathcal{B}$ é uma variedade do exemplo em questão.

Utilizaremos a Proposição 1.3.23 para obter grupos livres sobre uma variedade de uma forma simples. Por exemplo, dado um grupo livre F em X, definiremos o *grupo abeliano livre* F_{ab} em X quocientando F por F', sua apresentação é dada por $F_{ab} = \langle X \mid F' \rangle$. O *grupo metabeliano livre* F_{meta} é definido quocientando F por F'', e tem apresentação $F_{meta} = \langle X \mid F'' \rangle$. Já o grupo solúvel livre é obtido ao tomar o quociente $F/F^{(l)}$. Quanto aos grupos nilpotentes livres, podemos defini-los por $F/\gamma_c(F)$.

1.4 Grupos topológicos

O objetivo desta seção é estudar grupos que admitem uma estrutura topológica. Isto posto, enunciaremos alguns resultados primordias da Topologia para o estudo dessa classe de grupos. Maiores detalhes sobre Topologia podem ser encontrados em [8], quanto a parte de grupos topológicos, consulte [11].

Definição 1.4.1. Uma *topologia* em um conjunto X é uma coleção τ de subconjuntos de X, chamados de *subconjuntos abertos* (segundo a topologia τ), satisfazendo as seguintes propriedades:

(1) $\emptyset$ e X são abertos;

(2) a união de uma família qualquer de subconjuntos abertos é um subconjunto aberto;

(3) a interseção de uma família finita de subconjuntos abertos é um subconjunto aberto.

Um *espaço topológico* é um par ordenado (X, τ) consistindo de um conjunto X e uma topologia τ em X que define os abertos em X. Neste sentido, interpretamos X como um conjunto cujos elementos são irrelevantes, já (X, τ) consiste dos mesmos objetos em X, com a diferença de que τ atribiu significância para subconjuntos de X.

Exemplo 1.4.2. Seja $X = \{1,2,3,4,5\}$ e $\tau = \{\emptyset, \{2,4,5\}, X\}$. Sob as notações acima, $\emptyset$, $\{2,4,5\}$ e X são abertos da coleção τ. Note que quaisquer interseções ou uniões entre os abertos resultam um aberto de τ, além disso, $\emptyset$ e X são abertos de τ. Portanto, τ é uma topologia. O espaço topológico proveniente de X e τ é o $(X, \tau) = \{1,2,3,4,5\}$ com a propriedade de que os abertos são $\emptyset$, $\{2,4,5\}$ e X.

É sempre possível definir uma topologia para um conjunto X. Para isto, defina a coleção τ_0 em X tomando todos os subconjuntos de X como abertos. Nesse caso, τ_0 chama-se *topologia discreta*.

Exemplo 1.4.3. Se $X = \{1,2,3\}$, então $\tau_0 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, X\}$ é a topologia discreta de X.

Dado um subconjunto Y de um espaço topológico (X, τ_X), podemos utilizar a topologia de X para induzir uma topologia em Y.

Proposição 1.4.4. Se (X, τ_X) é um espaço topológico e $Y \subseteq X$, então $\tau_Y = \{Y \cap A \mid A \in \tau_X\}$ é um topologia em Y, denominada *topologia induzida* em Y por τ_X.

Exemplo 1.4.5. Considere X o espaço topológico do Exemplo 1.4.2 e $Y = \{2,5\}$. Observe que de $\tau = \{\emptyset, \{2,4,5\}, X\}$, temos $\tau_Y = \{Y \cap \emptyset, Y \cap \{2,4,5\}, Y \cap X\} = \{\emptyset, \{2,5\}, Y\}$ é a topologia induzida de Y.

Observe que a união de todos os subconjuntos da topologia τ_X de um espaço topológico X resulta em todo o conjunto X, este fato é trivial visto que $X \subset \tau_X$. Não tão trivial e encontrar quais uniões de subconjuntos de τ_X resultam X. Formalizaremos esta noção de "cobrir" o conjunto X abaixo.

Definição 1.4.6. Sejam (X, τ_X) um espaço topológico e $A \subseteq X$. Dizemos que $\mathcal{U} \subseteq \tau_X$ é uma *cobertura aberta* para A se

$$A = \bigcup_{U \in \mathcal{U}} U.$$

Quando $\mathcal{V} \subseteq \mathcal{U}$ também for uma cobertura aberta de A, diremos que $\mathcal{V}$ é uma *subcobertura aberta* de A.

Na definição acima, se não exigirmos que $\mathcal{U} \subseteq \tau_X$, diremos que $\mathcal{U}$ é apenas uma cobertura de X.

Definição 1.4.7. Seja X um espaço topológico. Uma *cisão* em X é um par $A, B \subseteq X$ tais que $A \cap B = \emptyset$ e $X = A \cup B$.

Todo espaço topológico admite ao menos uma cisão, a saber, $X = \emptyset \cup X$, denominada cisão trivial. Se o espaço topológico X só admite a cisão trivial, diremos que X é um *espaço topológico conexo*, caso contrário, diremos que X é um *espaço topológico desconexo*. Além disso, se todo aberto conexo de X tiver apenas um elemento, diremos que X é um *espaço topológico totalmente desconexo*.

Convenientemente, distribuimos os espaços topológicos em classes com a finalidade de explorar as propriedades dos espaços em determinada classe. A seguir, definiremos uma classe a qual pertencem os objetos o qual estudaremos posteriormente.

Definição 1.4.8. Sejam (X,τ_X) um espaço topológico e $K \subseteq X$. Diremos que K é *compacto* se toda cobertura aberta $\mathcal{U}$ de K admite subcobertura aberta $\mathcal{V}$ finita. Se X for compacto, dizemos que X é um espaço topológico compacto..

Note que o espaço topológico no Exemplo 1.4.2 é compacto. Com efeito, suas coberturas de abertos são $\mathcal{U}_1 = \{\emptyset, X\}$, $\mathcal{U}_2 = \{\emptyset, \{2,3,5\}, X\}$ e $\mathcal{U}_3 = \{X\}$, note que $\mathcal{V} = \{X\}$ é subcobertura aberta de $\mathcal{U}_1$,$\mathcal{U}_2$ e $\mathcal{U}_3$, $\mathcal{W} = \{\emptyset, X\}$ é uma subcobertura aberta de $\mathcal{U}_1$ e que estas são todas as possíveis subcoberturas, além disso, $|\mathcal{V}| = 1$ e $|\mathcal{W}| = 2$, donde concluímos que estas subcoberturas abertas são finitas.

Em verdade, sempre que X for um espaço topológico finito, X é compacto com a topologia discreta, visto que a menor cobertura para X é

$$X = \bigcup_{x \in X} \{x\},$$

e X não possui uma subcobertura aberta diferente do próprio X.

Espaços topológicos finitos munidos da topologia discreta possuem mais duas propriedades interessantes, a qual enunciaremos a seguir.

Proposição 1.4.9. Seja X um espaço topológico finito. Se todo subconjunto conexo de X possui apenas um elemento, então X é totalmente desconexo.

Para a segunda propriedade, diremos que um espaço topológico (X,τ) é *espaço topológico de Hausdorff* se dados $x,y \in X$ distintos, existem abertos $A_x, A_y \subseteq \tau$ tais que $A_x \cap A_y = \emptyset$.

Proposição 1.4.10. Seja X um espaço topológico com a topologia discreta. Então X é Hausdorff.

Observação 1.4.11. Espaços topológicos finitos com a topologia discreta são compactos, totalmente desconexos e de Hausdorff.

Obter informações de um espaço topológico através de um outro pode ser possível ao se definir uma aplicação adequada. Definiremos abaixo um tipo de aplicação que viabiliza fazer inferências sobre espaços topológicos de Hausdorff, totalmente desconexos ou compactos.

Definição 1.4.12. Uma aplicação $f : X \longrightarrow Y$, de um espaço topológico X num espaço topológico Y, diz-se *contínua* quando a pré-imagem $(B)f^{-1}$ de todo aberto $B \subset Y$ for um aberto em X.

A definição de aplicações contínuas entre espaços topológicos resulta um bom comportamento quanto a composição.

Proposição 1.4.13. Sejam X,Y,Z espaços topológicos e $f:X\longrightarrow Y$ $g:Y\longrightarrow Z$ aplicações contínuas. Então $f\circ g:X\longrightarrow Z$ é uma aplicação contínua.

A seguir, veremos que aplicações contínuas preservam compacidade e conexidade de espaços topológicos.

Proposição 1.4.14. Sejam $f:X\longrightarrow Y$ uma aplicação contínua entre espaços topológicos e $K\subseteq X$. Se K é compacto (conexo), então $(K)f$ é compacto (conexo).

Para um conjunto X, estão associados diversas topologias. Veremos que estas topologias possuem um bom comportamento quanto a interseção.

Proposição 1.4.15. Seja X um conjunto e $\{\tau_\lambda \mid \lambda\in\Lambda\}$ uma família de topologias em X. Então $\tau_X=\bigcap\limits_{\lambda\in\Lambda}\tau_\lambda$ é uma topologia em X.

A Proposição 1.4.15 permite estabelecer um ínfimo sobre uma família de topologias em X. Isto é, dado uma família $\{\tau_\lambda \mid \lambda\in\Lambda\}$ de topologias em X, existe uma topologia τ_ι em X que é a maior topologia contida em todas as topologias τ_λ, e denotaremos $\tau_\iota=inf\{\tau_\lambda \mid \lambda\in\Lambda\}$ como sendo o ínfimo da família em questão.

Outro tema de interesse consiste em buscar uma topologia que contenha um subconjunto específico. Abaixo, descreveremos de que modo podemos criar uma topologia contendo o subconjunto desejado.

Definição 1.4.16. Sejam X um conjunto e $S\subseteq\tau_0$. Seja $\{\tau \mid S\subseteq\tau\}$ a família de todas as topologias contendo S. Definimos a *topologia gerada* por S como sendo o ínfimo das topologias em X contendo S, $\tau(S)=inf\{\tau \mid S\subseteq\tau\}$.

Vimos anteriormente que o produto cartesiano possibilita construções de grupos "maiores", utilizaremos desta mesma ferramenta para construir espaços topológicos a partir de uma família conhecida de espaços topológicos.

Considere uma família de espaços topológicos X_λ, com $\lambda\in\Lambda$. Denotaremos as projeções de $Cr_{\lambda\in\Lambda}X_\lambda$ por

$$\begin{array}{rcl}\pi_\gamma: Cr_{\lambda\in\Lambda}X_\lambda & \longrightarrow & X_\gamma\\ (x_\lambda)_{\lambda\in\Lambda} & \longmapsto & x_\gamma\end{array}$$

Definição 1.4.17. Seja $\mathcal{S}_\gamma$ a coleção

$$\mathcal{S}_\gamma=\{(A_\gamma)\pi_\gamma^{-1} \mid A_\gamma \text{ é aberto em } X_\gamma\},$$

e denote por $\mathcal{S}$ a união dessas coleções,

$$\mathcal{S} = \bigcup_{\gamma \in \Lambda} \mathcal{S}_\gamma.$$

A topologia gerada por $\mathcal{S}$, $\tau(\mathcal{S})$, é denominada *topologia produto*. Nesta topologia, $Cr_{\lambda \in \Lambda} X_\lambda$ é chamado de *espaço produto*.

Com as notações acima, suponha que $Cr_{\lambda \in \Lambda} X_\lambda = Cr_{\lambda_1 \in \Lambda_1} X_{\lambda_1} \times X_\gamma \times Cr_{\lambda_2 \in \Lambda_2} X_{\lambda_2}$. Então, se A_γ é um aberto de X_γ, segue que $(A_\lambda)\pi_\gamma^{-1} = Cr_{\lambda_1 \in \Lambda_1} X_{\lambda_1} \times A_\gamma \times Cr_{\lambda_2 \in \Lambda_2} X_{\lambda_2}$ é um aberto de $\tau(\mathcal{S})$. Como $\tau(\mathcal{S})$ é uma topologia, a interseção de abertos é um aberto, entretanto, as interseções de abertos são finitas. Logo, se Λ é um conjunto finito, então todos os abertos de $Cr_{\lambda \in \Lambda} X_\lambda$ são da forma $Cr_{\lambda \in \Lambda} A_\lambda$, onde A_λ é um aberto qualquer de X_λ. Caso Λ seja um conjunto infinito, observamos que podemos fazer finitas interseções, então todos os abertos de $Cr_{\lambda \in \Lambda} X_\lambda$ são da forma $Cr_{\lambda \in \Lambda} A_\lambda$, onde $A_\lambda \neq X_\lambda$ apenas para um número finito de indíces.

Observação 1.4.18. Note que, assim definida, a topologia produto torna automaticamente as projeções em aplicações contínuas.

Proposição 1.4.19. Seja $f : X \longrightarrow Cr_{\lambda \in \Lambda} X_\lambda$ uma aplicação entre espaços topológicos definida por $f(x) = Cr_{\lambda \in \Lambda} f_\lambda(x)$. Então f é contínua se, e somente se, cada aplicação coordenada $f_\lambda : X \longrightarrow X_\lambda$ é contínua.

Um questionamento natural é investigar se, dada uma família de espaços topológicos satisfazendo uma propriedade $\mathcal{P}$, o produto cartesiano destes espaços topológicos preserva a propriedade $\mathcal{P}$.

Proposição 1.4.20. O produto cartesiano de uma família arbritrária de espaços topológicos de Hausdorff é um espaço topológico de Hausdorff.

Proposição 1.4.21. O produto cartesiano de uma família arbritrária de espaços topológicos totalmente desconexos é um espaço topológico totalmente desconexo.

Não é difícil ver que o produto cartesiano de uma família finita de espaços topológicos compactos é compacto. Quando a família é arbitrária o resultado não é tão trivial, entretanto, a resposta é afirmativa. Este resultado decorre do famoso Teorema de Tychonoff, que enunciaremos. A demonstração pode ser encontrada em [8].

Teorema 1.4.22 (Teorema de Tychonoff)**.** O produto cartesiano de uma família arbritrária de espaços topológicos compactos é um espaço topológico compacto.

Em nosso contexto, aplicações contínuas serão utilizadas para a definir um espaço topológico com estrutura de grupo.

Definição 1.4.23. Um *grupo topológico* G é um espaço topológico, munido de uma estrutura de grupo tal que as aplicações

$$\begin{array}{rcl} \mu : G\times G & \longrightarrow & G \\ (x,y) & \longmapsto & xy \end{array} \qquad\qquad \begin{array}{rcl} \iota : G & \longrightarrow & G \\ x & \longmapsto & x^{-1}, \end{array}$$

são contínuas.

Exemplo 1.4.24. Seja $\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\ldots,\overline{n-1}\}$ o grupo das classes de resto módulo n. Seja U um subconjunto de $\mathbb{Z}/n\mathbb{Z}$, a topologia discreta τ_0 nada mais é que a coleção de todos os possíveis subconjuntos U de $\mathbb{Z}/n\mathbb{Z}$. Com isto, $\mathbb{Z}/n\mathbb{Z}$ é um espaço topológico com estrutura de grupo, resta avaliar se as aplicações da Definição 1.4.23 são contínuas. Para isto, defina $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ com a topologia produto, os abertos deste produto direto são da forma $A\times B$, onde A e B são abertos em $\mathbb{Z}/n\mathbb{Z}$ segundo a topologia discreta, isto é, qualquer subconjunto de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ é um aberto. A pré-imagem de qualquer subconjunto de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ é um aberto de $\mathbb{Z}/n\mathbb{Z}$, pois todo subconjunto de $\mathbb{Z}/n\mathbb{Z}$ também é um aberto sob a topologia discreta, portanto, μ e ι são aplicações contínuas.

Nosso objetivo agora e construir grupos topológicos a partir de grupos conhecidos. Para isto, definiremos uma relação de ordem que contribuirá com nosso objetivo.

Seja I um conjunto e $\preceq$ uma operação binária. Diremos que $I = (I,\preceq)$ é um *conjunto dirigido* se a relação $\preceq$ satisfazer as seguintes condições:

(i) $i\preceq i$, para $i\in I$,

(ii) $i\preceq j$ e $j\preceq k$ implica $i\preceq k$, com $i,j,k\in I$,

(iii) $i\preceq j$ e $j\preceq i$ implica $i=j$ para $i,j\in I$,

(iv) se $i,j\in I$, existe $k\in I$ tal que $i,j\preceq k$.

Um *sistema inverso* de grupos topológicos sobre I, consiste de uma coleção $\{G_i \mid i\in I\}$ de grupos topológicos indexada por I, e uma coleção de homomorfismos contínuos de grupos $\varphi_{ij} : G_i \longrightarrow G_j$, definidos sempre que $j\preceq i$, de modo que os diagramas da forma

$$\begin{tikzcd} G_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & G_k \\ & G_j \arrow[ur, "\varphi_{jk}"'] & \end{tikzcd}$$

comutem sempre que estiverem definidos, isto é, $i, j, k \in I$ tal que $k \preceq j \preceq i$. Denotaremos esse sistema por $\{G_i, \varphi_{ij}, I\}$, ou por $\{G_i, \varphi_{ij}\}$ quando não houver dúvidas quanto ao conjunto I utilizado.

Seja G um grupo topológico, $\{G_i, \varphi_{ij}, I\}$ um sistema inverso de grupos topológicos sobre um conjunto dirigido I, e $\varphi_i : G \longrightarrow G_i$ homomorfismos contínuos de grupos para todo $i \in I$. As aplicações φ_i são ditas compatíveis se $\varphi_i \varphi_{ij} = \varphi_j$ sempre que $j \preceq i$.

Definição 1.4.25. Diremos que um grupo topológico G munido de homomorfismos contínuos compatíveis

$$\varphi_i : G \longrightarrow G_i \quad (i \in I)$$

é um *limite inverso* do sistema inverso $\{G_i, \varphi_{ij}, I\}$ se a seguinte propriedade universal for satisfeita:

$$\begin{tikzcd}
H \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"'] & G \arrow[d, "\varphi_i"] \\
& G_i
\end{tikzcd}$$

sempre que H for um grupo topológico e $\psi_i : H \longrightarrow G_i$ $(i \in I)$ é um conjunto de homomorfismos contínuos compatíveis, então existe um único homomorfismo contínuo $\psi : H \longrightarrow G$ tal que $\psi\varphi_i = \psi_i$ para todo $i \in I$. Dizemos que ψ é induzido pelos homomorfismos compatíveis ψ_i e denotamos o limite inverso por (G, φ_i).

Antes de prosseguir com o estudo dos grupos topológicos, convém verificar que, dado um sistema inverso, existe limite inverso e é único a menos de isomorfismos.

Proposição 1.4.26. Seja $\{G_i, \varphi_{ij}, I\}$ um sistema inverso de grupos topológicos sobre um conjunto dirigido I. Então

(i) Existe um limite inverso do sistema inverso $\{X_i, \varphi_{ij}, I\}$;

(ii) O limite inverso é único no seguinte sentido: se (H, α_i) e (K, β_i) são dois limites inversos do sistema inverso $\{G_i, \varphi_{ij}, I\}$, então existe um único isomorfismo topológico $\alpha : H \longrightarrow K$ de forma que $\alpha\beta_i = \alpha_i$ para cada $i \in I$.

Demonstração. (i) Defina $G = \{(g_i)_{i\in I} \in Cr_{i\in I} G_i \mid \varphi_{ij}((g_i)_{i\in I}) = g_j,\ j \preceq i\}$ e

$$\begin{array}{rcl} \varphi_i : G & \longrightarrow & G_i \\ (g_i)_{i\in I} & \longmapsto & g_i. \end{array}$$

Seja $\psi_i : H \longrightarrow G_i$ uma família de homomorfismos contínuos definidos para todo $i \in I$. Vamos mostrar que G juntamente com as aplicações φ_i satisfazem a propriedade universal, ou seja, que existe um único homomorfismo contínuo ψ que faça o diagrama

$$\begin{tikzcd} H \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"'] & G \arrow[d, "\varphi_i"] \\ & G_i \end{tikzcd}$$

comutar. Para cada $h \in H$, defina $(h)\psi := ((h)\psi_i)_{i\in I}$. Note que $((h)\psi_i)_{i\in I} \in G$, pois $(h)\psi_j = (h)\psi_i\varphi_{ij}$ sempre que $j \preceq i$. Além disso, a aplicação ψ, avaliada coordenada a coordenada é um homomorfismo contínuo, isto é, $\psi\varphi_i = \psi_i$ é um homomorfismo contínuo para todo $i \in I$, deste modo, a aplicação

$$\begin{array}{rcl} \psi : H & \longrightarrow & G \\ h & \longmapsto & ((h)\psi_i)_{i\in I} \end{array}$$

é um homomorfismo contínuo. Para mostrar a unicidade, suponha que exista um homomorfismo $\phi : H \longrightarrow G$ satisfazendo $\phi\varphi_i = \psi_i$ para todo $i \in I$. Tome $h \in H$ e note que $(h)\phi = ((h)\phi\varphi_i)_{i\in I} = ((h)\psi_i)_{i\in I} = (h)\psi$.

(ii) Decorre imediatamete da propriedade universal de (H, α_i) aplicada a família β_i de aplicações compatíveis que existe um homomorfismo contínuo β de modo que o diagrama

$$\begin{tikzcd} K \arrow[r, dashed, "\beta"] \arrow[dr, "\alpha_i"'] & H \arrow[d, "\beta_i"] \\ & G_i \end{tikzcd}$$

comute. Analogamente, a propriedade universal de (K, β_i) aplicada a família α_i de aplicações compatíveis garante a existência de um homomorfismo contínuo β que torna o diagrama

$$\begin{tikzcd} H \arrow[r, dashed, "\alpha"] \arrow[dr, "\beta_i"'] & K \arrow[d, "\alpha_i"] \\ & G_i \end{tikzcd}$$

comutativo. Note que a aplicação $\alpha\beta$ faz o diagrama

$$\begin{tikzcd} H \arrow[r, dashed, "\alpha\beta"] \arrow[dr, "\alpha_i"'] & H \arrow[d, "\alpha_i"] \\ & G_i \end{tikzcd}$$

comutar para todo $i \in I$. Mas a aplicação identidade Id_H também faz o diagrama comutar, pela unicidade da aplicação segue que $\alpha\beta = Id_H$. Similarmente para K, obtemos $\beta\alpha = Id_K$. Deste modo, α é um isomorfismo topológico. $\square$

Se $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso, denotaremos o seu limite inverso por

$$G = \varprojlim_{i\in I} G_i,$$

onde $G = \{(g_i)_{i\in I} \in Cr_{i\in I}G_i \mid ((g_i)_{i\in I})\varphi_{ij} = g_j,\ j \preceq i\}$.

Proposição 1.4.27. O limite inverso $G = \varprojlim_{i\in I} G_i$, é um grupo topológico.

Demonstração. Para verificar que G é um espaço topológico, basta tomar a topologia produto. Definindo a operação $(g_i)_{i\in I}(h_i)_{i\in I} = (g_ih_i)_{i\in I}$, vemos que G é um grupo. Para finalizar, devemos verificar que as aplicações μ e ι de G da Definição 1.4.23 são contínuas. Denotando μ_i e ι_i como as aplicações da Definição 1.4.23 para G_i, segue que μ_i e ι_i são contínuas, pois por hipótese, G_i é um grupo topológico para todo $i \in I$. Note que $(g_i)_{i\in I}^{-1} = (g_i^{-1})_{i\in I}$, então podemos escrever $\iota = Cr_{i\in I}\iota_i$, pela Proposição 1.4.19 segue que ι é contínua. Finalmente, como $(g_i)_{i\in I}(h_i)_{i\in I} = (g_ih_i)_{i\in I}$, podemos definir $\mu = Cr_{i\in I}\mu_i$, como μ_i é contínua para todo $i \in I$, segue que μ é contínua. $\square$

Agora, construiremos um exemplo de grupo topológico dado através de um limite inverso. Exemplo este que aparecerá mais adiante neste trabalho.

Exemplo 1.4.28. Sejam p um primo e $\mathbb{Z}/p^n\mathbb{Z}$ grupos topológicos munidos da topologia discreta, onde $n \in \mathbb{N}$.

Observe que $\mathbb{N}$ é um conjunto dirigido com a ordenação usual $\leq$. De fato,

(i) $i \leq i$, para $i \in \mathbb{N}$,

(ii) $i \leq j$ e $j \leq k$ implica $i \leq k$, com $i, j, k \in \mathbb{N}$,

(iii) $i \leq j$ e $j \leq i$ implica $i = j$, para $i, j \in \mathbb{N}$,

(iv) se $i, j \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $i, j \leq K$, basta tomar $k \geq max\{i, j\}$.

Além disso,

$$\begin{array}{rcl} \varphi_{nm} : \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^m\mathbb{Z} \\ x + p^n\mathbb{Z} & \longmapsto & x + p^m\mathbb{Z} \end{array}$$

é um epimorfismo definido sempre que $m \leq n$. Portanto, $\{\mathbb{Z}/p^n\mathbb{Z}, \varphi_{nm}, \mathbb{N}\}$, é um sistema inverso, cujo limite inverso será denotado por

$$\mathbb{Z}_p = \lim_{\substack{\longleftarrow \\ n\in\mathbb{N}}} \mathbb{Z}/p^n\mathbb{Z}.$$

Vimos na Proposição 1.4.26 que

$$\mathbb{Z}_p = \{(x_n)_{n\in\mathbb{N}} \in Cr_{n\in\mathbb{N}} Z/p^n\mathbb{Z} \mid ((x_n)_{n\in\mathbb{N}})\varphi_{nm} = x_m,\, m \leq n\},$$

então

$$((x_n)_{n\in\mathbb{N}})\varphi_{nm} = x_m \Longleftrightarrow x_n + p^m\mathbb{Z} = x_m + p^m\mathbb{Z} \Longleftrightarrow x_n \equiv x_m \bmod p^m,$$

sempre que $m \leq n$. Deste modo, $(x_n)_{n\in\mathbb{N}} = (x_1, x_2, x_3, \dots) \in \mathbb{Z}_{\hat{p}}$ se, e somente se, $x_n \equiv x_m \bmod p^m$. Utilizaremos a forma de sequência acima para introduzir a forma polinomial. Tome $(x_1, x_2, x_3, \dots) \in \mathbb{Z}_{\hat{p}}$, representaremos sua forma polinomial por

$$x_1 + x_2 p + x_3 p^2 + \dots,$$

onde $0 \leq x_n \leq p-1$, para todo $n \in \mathbb{N}$.

O conjunto $\mathbb{Z}_p$ é conhecimo como *anel dos inteiros p-ádicos*. Mostraremos que neste conjunto, as unidades são da forma $x_1 + x_2 p + x_3 p^2 + \dots$, onde $x_1 \neq 0$.

Proposição 1.4.29. Um inteiro p-ádico x é uma unidade em $\mathbb{Z}_p$ se, e somente se, $x_1 \neq 0$.

Demonstração. Se $x = x_1 + x_2 p + x_3 p^2 + \dots$ é uma unidade, então existe $y \in \mathbb{Z}_p$ tal que $xy = 1$. Seja $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ o epimorfismo de projeção definido por $(x)\pi_n = x_n p^{n-1}$. Então $1 = (1)\pi = (xy)\pi_1 = (x)\pi_1 (y)\pi_1 = x_1 (y)\pi_1$, isto é, x_1 é uma unidade em $\mathbb{Z}/p\mathbb{Z}$, portanto, $x_1 \neq 0$.

Reciprocamente, suponha que $x_1 \neq 0$. Considere o caso onde $x_1 = 1$ e denote por $x_2 p + x_3 p^2 + \dots = (x_2 + x_3 p + \dots)p = -zp$, então $1 + x_2 p + x_3 p^2 + \dots = 1 - zp$. A série geométrica $\dfrac{1}{1-x} = 1 + x + x^2 + \dots$ nos fornece $\dfrac{1}{1-zp} = 1 + zp + z^2p^2 + \dots$ que é um elemento de $\mathbb{Z}_p$.

Finalmente,

$$\frac{1}{1-zp}(1-zp) = (1+zp+z^2p^2+\dots)(1-zp) = (1+zp+z^2p^2+\dots) - (zp+z^2p^2+\dots) = 1.$$

Caso $x_1 \geq 2$, como $x_1 \neq 0$, existe $c \in \mathbb{Z}/p\mathbb{Z}$ tal que $x_1 c = 1$. Então

$$(x_1 + x_2 p + x_3 p^2 + \dots)c = x_1 c + x_2 cp + x_3 cp^2 + \dots = 1 + y_2 p + y_3 p^2 + \dots,$$

onde $y_n = x_n c$ para todo $n \in \mathbb{N}$. Provamos acima que elementos da forma $1 + y_2 p + y_3 p^2 + \dots$ admitem inverso em $\mathbb{Z}_p$, logo, todo elemento da forma $x_1 + x_2 p + x_3 p^2 + \dots$ com $x_1 \neq 0$ é uma unidade. □

A seguir, desenvolveremos a noção de fecho topológico para grupos que possuem quocientes finitos. Denominamos este fecho por *fecho topológico profinito*

Sejam G um grupo arbitrário e $\mathcal{N}$ a coleção de subgrupos normais N de G tal que G/N é um grupo finito. Observe que $\mathcal{N}$ é um conjunto não vazio, pois $G \in \mathcal{N}$. Podemos tornar $\mathcal{N}$ em um conjunto dirigido definindo $M \preceq N$ sempre que $M \geq N$, com $M, N \in \mathcal{N}$. De fato,

(i) $N \preceq N$ para todo $N \in \mathcal{N}$, pois $N \geq N$;

(ii) $N \preceq M$ e $M \preceq L$ então $N \preceq L$ para quaisquer $M, N, L \in \mathcal{N}$, visto que $N \geq M$ e $M \geq L$ implica $N \geq L$;

(iii) $N \preceq M$ e $M \preceq N$ então $N = M$ para $M, NL \in \mathcal{N}$, uma vez que $N \geq M$ e $M \geq N$ implica $M = N$;

(iv) se $M, N \in \mathcal{N}$, existe $L \in \mathcal{N}$ tal que $M, N \preceq L$, basta tomar $L \leq M \cap N$, então $M \geq L$ e $N \geq L$ implicam $M, N \preceq L$.

Deste modo, G será um grupo topológico munido da *topologia profinita*, cuja base é definida por

$$\tau_{\mathcal{N}} = \{gN \mid N \in \mathcal{N}, g \in G\}.$$

Se $M, N \in \mathcal{N}$ e $M \preceq N$, defina o epimorfismo natural $\varphi_{NM} : G/N \longrightarrow G/M$. Então, segue que $\{G/N, \varphi_{NM}\}$ é um sistema inverso de grupos finitos G/N. Definiremos o *fecho topológico profinito* de G em relação a topologia profinita por

$$\widehat{G} = \varprojlim_{N \in \mathcal{N}} G/N.$$

Se na construção acima substituirmos grupo finito por p-grupos finitos, onde p é um primo fixado, teremos o *fecho topológico pro-p*. Por exemplo, $\mathbb{Z}_p$ é o fecho topológico pro-p de $\mathbb{Z}$.

CAPÍTULO 2

Propriedades residuais e imersões em produtos entrelaçados

Dados G, K grupos, um questionamento natural é estudar de que forma as propriedades do produto entrelaçado $G \wr K$ são influenciadas pelas propriedades de G e K. Para este fim, iremos explorar definições e resultados apresentados em [6]. Outro objetivo interessante é estudar quais grupos podem sem imersos em $G \wr K$, nos limitaremos a estudar uma imersão denominada Imersão de Magnus, apresentada em [10].

2.1 Propriedades residuais

A grosso modo, se $\mathcal{P}$ é uma propriedade de grupos, podemos pensar na propriedade residual $\mathcal{P}$ como uma propriedade recuperada de grupos que satisfazem $\mathcal{P}$. Esta seção é motivada por [6], nela, formalizaremos a noção de propriedade residual e estudaremos o Teorema de Gruenberg, que relaciona o produto entrelaçado a um tipo especial de propriedade residual.

Definição 2.1.1. Seja $\mathcal{P}$ uma propriedade. Dizemos que um grupo G é *residualmente* $\mathcal{P}$ se dado $g \in G$ não trivial, existe um subgrupo normal N_g de G tal que $g \notin N_g$ e G/N_g tem a propriedade $\mathcal{P}$.

Exemplo 2.1.2. Sejam $\mathbb{Z}$ o grupo ciclíco infinito e $\mathcal{P}$ a propriedade de ser um 2-grupo finito, isto é, um grupo cuja ordem é uma potência de 2. Como $\mathbb{Z}$ é um grupo abeliano, todos os seus subgrupos são normais. Note que $\mathbb{Z}$ não possui a propriedade $\mathcal{P}$, pois os elementos em $\mathbb{Z}$ tem ordem infinita. Ainda assim, dado $x \in \mathbb{Z}$, existe $n \in \mathbb{N}$ tal que x não é múltiplo de 2^n, deste modo, $x \notin 2^n\mathbb{Z} = \{2^n y \mid y \in \mathbb{Z}\}$ e $\mathbb{Z}/2^n\mathbb{Z}$ é um 2-grupo finito. Portanto, $\mathbb{Z}$ é residualmente um 2-grupo finito.

A Definição 2.1.1 pode ser reformulada em termos de um epimorfismo em um grupo com a propriedade $\mathcal{P}$, como veremos na proposição abaixo.

Proposição 2.1.3. Sejam G um grupo e $\mathcal{P}$ uma propriedade. Então G é residualmente $\mathcal{P}$ se, e somente se, para todo $g \in G$, existe um epimorfismo de G em um grupo H com a propriedade $\mathcal{P}$ satisfazendo $(g)\varphi \neq e$.

Demonstração. Seja G um grupo residualmente $\mathcal{P}$. Tome $g \in G$, então existe um subgrupo normal N_g tal que $g \notin N_g$. Defina a aplicação natural

$$\begin{aligned} \varphi : G &\longrightarrow G/N_g \\ x &\longmapsto xN_g. \end{aligned}$$

A aplicação φ é claramente um epimorfismo, além disso, $(g)\varphi = gN_g \neq N_g$, pois $g \notin N_g$.

Reciprocamente, suponha que para todo $g \in G$, existe um epimorfismo φ de G em um grupo H com a propriedade $\mathcal{P}$ satisfazendo $(g)\varphi \neq e$. Pelo Primeiro Teorema do Isomorfismo, $G/Ker\,\varphi \simeq H$, logo, $G/Ker\,\varphi$ tem a propriedade $\mathcal{P}$ e $g \notin Ker\,\varphi$. □

Para uma dada propriedade $\mathcal{P}$, veremos a seguir que a definição proveniente da Proposição 2.1.3 possibilita o uso de epimorfismos para determinar se um grupo é residualmente $\mathcal{P}$.

Proposição 2.1.4. Sejam G e H grupos. Se H é um grupo residualmente $\mathcal{P}$ e para todo elemento não trivial $g \in G$ existe um epimorfismo $\varphi_g : G \longrightarrow H$, onde $(g)\varphi_g \neq e$, então G é residualmente P.

Demonstração. Seja $h \in H$ tal que $h \neq e$, como H é residualmente $\mathcal{P}$, existe um epimorfismo ψ_h em um grupo K com a propriedade $\mathcal{P}$ satisfazendo $(h)\psi_h \neq e$. Tome $h = (g)\varphi_g$, então $\varphi_g\psi_h$ é um epimorfismo de G em K satisfazendo $(g)\varphi_g\psi_h = (h)\psi_h \neq e$, portanto, G é residualmente P. □

A seguir, definiremos um tipo de propriedade necessária nas hipóteses do Teorema de Gruenberg.

Definição 2.1.5. Dizemos que $\mathcal{P}$ é uma *propriedade raiz* se satifazer:

(1) se um grupo G possui a propriedade $\mathcal{P}$ então seus subgrupos também a possuem;

(2) se G e H tem a propriedade $\mathcal{P}$ então $G \times H$ possui a propriedade;

(3) se $\{e\} \leq K \leq H \leq G$ é uma série de subgrupos, cada um normal no seu antecessor, G/H e H/K possuem a propriedade $\mathcal{P}$, então K contém um subgrupo L, normal em G, tal que G/L tem a propriedade $\mathcal{P}$.

Exemplo 2.1.6. A propriedade $\mathcal{P}$:= "ordem potência de primo" é uma propriedade raiz. Com efeito, seja p um primo e $n, m \geq 1$,

(i) se $|G| = p^n$, então, pelo Teorema de Lagrange, a ordem dos subgrupos de G dividem $|G|$. Portanto, se $H \leq G$, então $|H| = p^m$, onde $m < n$;

(ii) se $|G| = p^n$ e $|H| = p^m$, então a ordem do produto direto $G \times H$ é uma potência de p, pois $|G \times H| = |G||H| = p^n p^m = p^{n+m}$;

(iii) se $\{e\} \leq K \leq H \leq G$ é uma série de subgrupos, cada um normal no seu antecessor, $|G/H| = p^n$ e $|H/K| = p^m$.

Note que para $K \leq H \leq G$, temos $[G : K] = [G : H][H : K]$ sempre que $[G : H]$ e $[H : K]$ são finitos. Se $K \lhd G$, então tomamos $L = K$ e $[G : K] = p^{n+m}$. Se K não é normal em G, defina $K_G = \bigcap_{g \in G} K^g$. Sob as notações do Teorema 1.1.9, como $[G : K]$ é finito, segue que $S(M)$ é finito, assim, $[G : K_G]$ é finito.

Como H/K é um p-grupo, então H/K é nilpotente, consequentemente, existe $c \in \mathbb{N}$ de forma que $\gamma_{c+1}(H/K) = K/K$, donde concluímos que $\gamma_{c+1}(H) \leq K$. De $H \lhd G$, segue pela Proposição 1.2.18 que $\gamma_{c+1}(H) \lhd G$. Como K_G é o maior subgrupo normal em G contido em K, segue que $\gamma_{c+1}(H) \leq K_G$, deste modo H/K_G é nilpotente e finito.

Observe que $[H : K_G] = [H : K][K : K_G]$, então H/K_G possui elementos de ordem potência de primo. Além disso, $K/K_G \leq H/K_G$ é nilpotente e finito, então $K/K_G \simeq P \times P_1 \times \cdots \times P_l$, onde $|P| = p^r$ e $P_1 \ldots P_l$ são grupos cujas ordens são potências de primos. Agora, tome $L/K_G \leq H/K_G$ de modo que $L/K_G \simeq P_1 \times \cdots \times P_l$, então $[K : L] = [K : K_G]/[L : K_G]$ é uma potência de primo. Como L/K_G é característico em H/K_G e $H/K_G \lhd G/K_G$ temos $L/K_G \lhd G/K_G$ e, pelo Teorema da Correspondência, $L \lhd G$. Note que $[G : L] = [G : H][H : L]$ e $[H : L] = [H : K][K : L]$, então $[G : L] = [G : H][H : K][K : L]$ é uma potência de p.

Exemplo 2.1.7. A propriedade $\mathcal{P}$:= "solúvel" é uma propriedade raiz. De fato,

(i) se G é um grupo solúvel, o Teorema 1.2.4 nos afirma que todo subgrupo de G é solúvel;

(ii) se H e K são grupos solúveis, segue do Corolário 1.2.8 que $H \times K$ é um grupo solúvel;

(iii) se $\{e\} \leq K \leq H \leq G$ é uma série de subgrupos, cada um normal no seu antecessor, onde G/H e H/K são solúveis, então existem $n,m \in \mathbb{N}$ satisfazendo $G^{(n)}H/H = H/H$ e $H^{(m)}K/K = K/K$. Sejam $\{G^{(i)}/H\}_{i=0}^{n}$ e $\{H^{(j)}/K\}_{j=0}^{m}$ séries solúveis para G/H e H/K, respectivamente.

Tome $L = H^{(m)}$, vimos na Proposição 1.2.11 que $L \lhd G$, logo, podemos formar a série

$$L/L \leq H^{(m-1)}L/L \leq \cdots \leq H/L \leq G^{(n-1)}/L \leq \cdots \leq G/L. \qquad (*)$$

Para $i \in \{0,\ldots,m-1\}$ e $j \in \{0,\ldots,n-1\}$, temos $G^{(i+1)} \lhd G^{(i)}$ e $H^{(j+1)} \lhd H^{(j)}$, pelo Teorema da Correspondência, $G^{(i+1)}/L \lhd G^{(i)}/L$ e $H^{(j+1)}/L \lhd H^{(j)}/L$. Além disso, o Terceiro Teorema do Isomorfismo nos assegura que os grupos quocientes da série em $(*)$ são abelianos, pois $(G^{(i)}/L)/(G^{(i+1)}/L) \simeq G^{(i)}/G^{(i+1)} \simeq G^{(i)}/G$ e $(H^{(j)}/L)/(H^{(j+1)}/L) \simeq H^{(j)}/H^{(j+1)}$ são abelianos, donde concluímos que a série em $(*)$ é solúvel. Portanto, existe $L \leq K$, onde $L \lhd G$ e G/L é solúvel.

Lema 2.1.8. Sejam $\mathcal{P}$ uma propriedade e G um grupo que satisfaz a propriedade (3) da Definição 2.1.5 com relação a $\mathcal{P}$. Se $H \lhd G$, H é residualmente $\mathcal{P}$ e G/H tem a propriedade $\mathcal{P}$, então G é residualmente $\mathcal{P}$.

Demonstração. Devemos mostrar que para cada $x \neq e$ em G, podemos encontrar um subgrupo normal N_x tal que $x \notin N_x$ e G/N_x possui a propriedade $\mathcal{P}$. Se $x \notin H$, podemos tomar $N_x = H$, pois por hipótese, G/H tem a propriedade $\mathcal{P}$. Se $x \in H$, como H é residualmente $\mathcal{P}$, podemos encontrar $K \lhd H$, tal que $x \notin K$ e H/K tem a propriedade $\mathcal{P}$. Por hipótese, K contém um subgrupo $L \lhd G$, tal que G/L possui a propriedade $\mathcal{P}$, assim, escolhendo $K_x = L$, segue que $x \notin L$ e G/L tem a propriedade $\mathcal{P}$. □

Definição 2.1.9. Uma família $(K_\lambda)_{\lambda\in\Lambda}$ de subgrupos normais de um grupo G será denominada filtro de unidade de G se $\bigcap\limits_{\lambda\in\Lambda} K_\lambda = \{e\}$ e para cada $\mu,\nu \in \Lambda$, existe $\lambda \in \Lambda$ tal que $K_\lambda \leq K_\mu \cap K_\nu$. Se, em adição, G/K_λ satisfaz a propriedade $\mathcal{P}$ para cada $\lambda \in \Lambda$, onde $\mathcal{P}$ é uma propriedade qualquer, então $(K_\lambda)_{\lambda\in\Lambda}$ é denominado $\mathcal{P}$-filtro de G.

Lema 2.1.10. Se $\mathcal{P}$ é uma propriedade arbitrária e G_λ é residualmente $\mathcal{P}$, para cada $\lambda \in \Lambda$, então $Cr_{\lambda\in\Lambda}G_\lambda$ e $Dr_{\lambda\in\Lambda}G_\lambda$ são ambos residualmente $\mathcal{P}$.

Demonstração. Se g não é o elemento neutro de $Cr_{\lambda\in\Lambda}G_\lambda$, então ao menos uma de suas coordenadas, digamos a α-coordenada é não trivial. Então o epimorfismo

$$\begin{array}{rcl} \pi_\delta : Cr_{\lambda\in\Lambda}G_\lambda & \longrightarrow & G_\alpha \\ (g_\lambda)_{\lambda\in\Lambda} & \longmapsto & g_\alpha \end{array}$$

satisfaz $(g)\pi_\alpha \neq e$. Agora, de G_α residualmente $\mathcal{P}$, dado $g_\alpha \in G_\alpha$ não trivial, existe um epimorfismo ψ_α de G_α em um grupo H com a propriedade $\mathcal{P}$, onde $(g_\alpha)\psi_\alpha \neq e$.

Como a composição de epimorfismos é um epimorfismo, segue que $\pi_\gamma\psi_\gamma$ é um epimorfismo de $Cr_{\lambda\in\Lambda}G_\lambda$ no grupo H que possui a propriedade $\mathcal{P}$, além disso, segue que $(g)\pi_\gamma\psi_\gamma = ((g)\pi_\gamma)\psi_\gamma = (g_\gamma)\psi_\gamma \neq e$. Logo, $Cr_{\lambda\in\Lambda}G_\lambda$ é residualmente $\mathcal{P}$. A demonstração para $Dr_{\lambda\in\Lambda}G_\lambda$ é análoga. □

Lema 2.1.11. Se $\mathcal{P}$ é uma propriedade satisfazendo (1) e (2) da Definição 2.1.5, então um grupo é residualmente $\mathcal{P}$ se, e somente se, possui um $\mathcal{P}$-filtro.

Demonstração. Um grupo que possui um $\mathcal{P}$-filtro é obviamente residualmente $\mathcal{P}$.

Reciprocamente, se G é residualmente $\mathcal{P}$, então para todo $g \in G$, existe um subgrupo K normal em G tal que G/K possui a propriedade $\mathcal{P}$. Considere $(K_\lambda)_{\lambda\in\Lambda}$ a família de todos os subgrupos normais cujo quociente tem a propriedade $\mathcal{P}$. Mostraremos a seguir que esta família é um $\mathcal{P}$-filtro.

(i) De G residualmente $\mathcal{P}$, segue que para todo elemento $g \in G$, existe um K_λ na família acima tal que $g \notin K_\lambda$, deste modo, $\cap_{\lambda\in\Lambda}K_\lambda = \{e\}$.

(ii) Sejam K_μ e K_ν dois membros da família $(K_\lambda)_{\lambda\in\Lambda}$, então G/K_μ e G/K_ν possuem a propriedade $\mathcal{P}$. Como $\mathcal{P}$ é uma propriedade satisfazendo (2), então $G/K_\mu \times G/K_\nu$ possui a propriedade $\mathcal{P}$. Agora note que $G/(K_\mu \cap K_\nu)$ pode ser mergulhado em $G/K_\mu \times G/K_\nu$. Com efeito, defina

$$\begin{aligned} \varphi : G/(K_\mu \cap K_\nu) &\longrightarrow G/K_\mu \times G/K_\nu \\ g(K_\mu \cap K_\nu) &\longmapsto (gK_\mu, gK_\nu). \end{aligned}$$

A aplicação φ está bem definida, pois dados $g_1(K_\mu \cap K_\nu), g_2(K_\mu \cap K_\nu) \in G/(K_\mu \cap K_\nu)$,

$$(g_1(K_\mu \cap K_\nu))\varphi = (g_1K_\mu, g_1K_\nu) = (g_2K_\mu, g_2K_\nu) = (g_2(K_\mu \cap K_\nu))\varphi.$$

Observe também que a aplicação φ é um monomorfismo, visto que para quaisquer que sejam $g_1(K_\mu \cap K_\nu), g_2(K_\mu \cap K_\nu) \in G/(K_\mu \cap K_\nu)$,

$$\begin{aligned} (g_1(K_\mu \cap K_\nu)g_2(K_\mu \cap K_\nu))\varphi = (g_1g_2(K_\mu \cap K_\nu))\varphi &= (g_1g_2K_\mu, g_1g_2K_\nu) \\ &= (g_1K_\mu, g_1K_\nu)(g_2K_\mu, g_2K_\nu) \\ &= (g_1(K_\mu \cap K_\nu))\varphi(g_2(K_\mu \cap K_\nu))\varphi, \end{aligned}$$

e $(g(K_\mu \cap K_\nu))\varphi = (gK_\mu, gK_\nu) = (K_\mu, K_\nu)$ se, e somente se, $g \in K_\mu$ e $g \in K_\nu$, ou seja, $g \in K_\mu \cap K_\nu$, logo, $Ker\,\varphi$ é trivial.

A propriedade $\mathcal{P}$ satisfaz (1), como $G/(K_\mu \cap K_\nu)$ pode ser identificado com um subgrupo de $G/K_\mu \times G/K_\nu$, então $G/(K_\mu \cap K_\nu)$ possui a propriedade $\mathcal{P}$. Isto posto, $K_\mu \cap K_\nu$ é uma coordenada da família $(K_\lambda)_{\lambda\in\Lambda}$. Mostramos que para quaisquer $K_\mu, K_\nu \in (K_\lambda)_{\lambda\in\Lambda}$, temos $K_\mu \cap K_\nu \in (K_\lambda)_{\lambda\in\Lambda}$. Tomando $K_\zeta \in (K_\lambda)_{\lambda\in\Lambda}$, segue que $K_\zeta \cap (K_\mu \cap K_\nu) \in (K_\lambda)_{\lambda\in\Lambda}$, então existe $\eta \in \Lambda$ tal que $K_\zeta \cap (K_\mu \cap K_\nu) = K_\eta$ e $K_\eta = K_\zeta \cap (K_\mu \cap K_\nu) \leq K_\mu \cap K_\nu$, como desejado.

(iii) G/K_λ satisfaz a propriedade $\mathcal{P}$ para cada $\lambda \in \Lambda$, pois os elementos da família $(K_\lambda)_{\lambda\in\Lambda}$ são justamente os subgrupos normais G/K_λ que tem a propriedade $\mathcal{P}$.

Logo, $(K_\lambda)_{\lambda\in\Lambda}$ é um filtro de unidade. □

Lema 2.1.12. Se $x_0 = e$, $x_1, \dots, x_n$ são elementos distintos de G e $(K_\lambda)_{\lambda\in\Lambda}$ é um filtro de unidade de G, então existe λ tal que $x_0, \dots, x_n$ pertencem a classes laterais distintas de K_λ.

Demonstração. Pela primeira propriedade de filtro de unidade, podemos encontrar λ_{ij}, onde $n \geq i > j \geq 0$, tal que $x_i x_j^{-1} \notin K_{\lambda_{ij}}$, e então, pela segunda propriedade, podemos escolher λ tal que $K_\lambda \leq \cap K_{\lambda_{ij}}$. □

Convencionaremos a notação de que $g_{(\lambda)}$ é o elemento $((\dots, e, g, e, \dots), e)$ onde g aparece na coordenada indexada por $\lambda \in \Lambda$.

Lema 2.1.13. Sejam $W = G \wr_\Lambda P$, onde P é um grupo de permutação transitiva em um conjunto Λ, $P^* = \{((e_q)_{q\in P}, p) \mid p \in P \text{ e } e_q \text{ é a identidade } \forall q \in P\}$ e N um subgrupo normal de W tal que $N \cap P^* > \{e\}$. Então o subgrupo derivado do grupo base está contido em N.

Demonstração. Observe que $(G^{(\Lambda)})' = Dr_{\lambda\in\Lambda} G'_\lambda$, onde $G_\lambda = G$ para todo $\lambda \in \Lambda$, e que geradores de $(G^{(\Lambda)})'$ são $[g,h]_{(\lambda)}$, onde $g, h \in G$. Então é suficente mostrar que $[g,h]_{(\lambda)} \in N$ para todo $\lambda \in \Lambda$. Além disso, como $P \simeq P^*$, podemos considerar P^* como um grupo de permutação transitiva em Λ.

Sejam $g, h \in G$ e $\lambda \in \Lambda$, vamos mostrar que existe $n \in N \cap P^*$ de modo que $n\lambda \neq \lambda$. Suponha por contradição que $n\lambda = \lambda$ para todo $n \in N \cap P^*$. Deste modo, dado $\beta \in P^*$, segue que $\beta^{-1} n \beta \in N \cap P^*$, pois $N \cap P^*$ é normal em P^*. Por hipótese de contardição, temos $(\beta^{-1} n \beta)\lambda = \lambda$, então

$$n\beta\lambda = \beta(\beta^{-1} n \beta)\lambda = \beta\lambda.$$

Como P^* é transitiva, $P^*\lambda = \Lambda$, e então $n\lambda' = \lambda'$ para todo $\lambda' \in \Lambda$ e todo $n \in N \cap P^*$. Isto contradiz $N \cap P^* > \{e\}$, assim podemos encontrar $n \in N \cap P^*$ tal que $n\lambda \neq \lambda$.

Mostraremos que

$$[g,h]_{(\lambda)} = [g_{(\lambda)}, h_{(\lambda)}] \equiv [n g_{(\lambda)} n^{-1}, h_{(\lambda)}] \pmod{N}.$$

Com efeito,

$$[g,h]_{(\lambda)}^{-1}[ng_{(\lambda)}n^{-1},h_{(\lambda)}] = h_{(\lambda)}^{-1}((g_{(\lambda)}^{-1}((h_{(\lambda)}((g_{(\lambda)}ng_{(\lambda)}^{-1})n^{-1})h_{(\lambda)}^{-1})n)g_{(\lambda)})n^{-1})h_{(\lambda)},$$

é um elemento de N, basta olhar os parenteses do mais interior até o mais exterior, utilizando hipóteses de normalidade e o fato de ser subgrupo. Como $[ng_{(\lambda)}n^{-1},h_{(\lambda)}] = [g_{(n\lambda)},h_{(\lambda)}] = e$, pois $n\lambda \neq \lambda$, obtemos $[g,h]_{(\lambda)} \equiv e \,(\text{mod}\, N)$. $\square$

Lema 2.1.14. Sejam $\mathcal{P}$ uma propriedade raiz, G e P grupos, onde P é um grupo de permutações de um conjunto X. Se G e P são ambos residualmente $\mathcal{P}$ e P tem a propriedade $\mathcal{P}$, então $W = G \wr P$ é residualmente $\mathcal{P}$.

Demonstração. Pelo Lema 2.1.10 o grupo base de $G \wr P$ é residualmente $\mathcal{P}$, consequentemente, se P tem a propriedade $\mathcal{P}$, então $G \wr P$ é residualmente $\mathcal{P}$, pelo item (ii) do Lema 2.1.8, pois $\mathcal{P}$ é uma propriedade raiz. $\square$

Lema 2.1.15. Sejam G e U grupos, com G abeliano. Então todo epimorfismo de U em um grupo V pode ser estendido de forma natural para um epimorfismo de $G \wr U$ em $G \wr V$.

Demonstração. Sejam $D_U = Dr_{u \in U} G_u$, onde $G_u = G$ e $D_V = Dr_{v \in V} G_v$, onde $G_v = G$. Se $u \mapsto v$ é um epimorfismo de U em V, mostraremos que a aplicação $g_{(u)} \mapsto g_{(v)}$ estende de forma natural o epimorfismo de D_U em D_V, pois G é abeliano.

Defina

$$\begin{aligned} \psi : Dr_{u\in U} G_u &\longrightarrow Dr_{v \in V} G_v \\ \bigoplus_{\substack{g\in G\\ u\in U}} g_{(u)} &\longmapsto \bigoplus_{\substack{g\in G\\ v\in V}} g_{(v)}. \end{aligned}$$

Primeiro, vamos verificar que a aplicação é, de fato, bem definida. Sejam $u_1, u_2 \in U$ com a mesma imagem $v \in V$ através do epimorfismo especificado, temos $g_{(u_1)}h_{(u_2)} = h_{(u_2)}g_{(u_1)}$. Então devemos ter $(g_{(u_1)}h_{(u_2)})\psi = (h_{(u_2)}g_{(u_1)})\psi$, o que realmente ocorre, uma vez que a abelianidade de G fornece $(g_{(u_1)}h_{(u_2)})\psi = g_{(v)}h_{(v)} = (gh)_{(v)} = (hg)_{(v)} = h_{(v)}g_{(v)} = (h_{(u_2)}g_{(u_1)})\psi$. Consequentemente, temos

$$\begin{aligned} (\bigoplus_{\substack{g\in G\\ u\in U}} g_{(u)} \bigoplus_{\substack{h\in G\\ u\in U}} h_{(u)})\psi = (\bigoplus_{\substack{g,h\in G\\ u\in U}} g_{(u)}h_{(u)})\psi = \bigoplus_{\substack{g,h\in G\\ v\in V}} g_{(v)}h_{(v)} &= \bigoplus_{\substack{g\in G\\ v\in V}} g_{(v)} \bigoplus_{\substack{h\in G\\ v\in V}} h_{(v)} \\ &= (\bigoplus_{\substack{g\in G\\ u\in U}} g_{(u)})\psi(\bigoplus_{\substack{h\in G\\ u\in U}} h_{(u)})\psi. \end{aligned}$$

Além disso, para todo $(g_v)_{v\in V} \in Dr_{v\in V} G_v$, existe um elemento $\bigoplus g_{(u)} \in Dr_{u\in U} G_u$ satisfazendo $(\bigoplus g_{(u)})\psi = \bigoplus g_{(v)} = (g_v)_{v\in V}$. Portanto, ψ é um epimorfismo.

Agora, obtemos uma aplicação sobrejetora φ de $G \wr U$ em $G \wr V$ definindo

$$\begin{aligned} \varphi : G \wr U &\longrightarrow G \wr V \\ ((g_x)_{x\in U}, u) &\longmapsto ((g_y)_{y\in V}, v), \end{aligned}$$

onde $x \mapsto y$ é um epimorfismo de U em V.

Para cada $u_1, u_2 \in U$ e cada $(g_x)_{x\in U}, (h_x)_{x\in U} \in D_U$,

$$\begin{aligned} \varphi(((g_x)_{x\in U}, u_1)((h_x)_{x\in U}, u_2)) &= \varphi(((g_x)_{x\in U}(h_{u_1x})_{x\in U}, u_1u_2)) \\ &= ((g_y)_{y\in V}(h_{v_1y})_{y\in V}, v_1v_2) \\ &= ((g_y)_{y\in V}, v_1)((h_y)_{y\in V}, v_2) \\ &= \varphi(((g_x)_{x\in U}, u_1))\varphi(((h_x)_{x\in U}, u_2)), \end{aligned}$$

consequentemente, φ é na verdade um epimorfismo. □

Lema 2.1.16. Se G e U são grupos residualmente $\mathcal{P}$, onde G é abeliano e $\mathcal{P}$ é uma propriedade raiz, então $W = G \wr U$ é residualmente $\mathcal{P}$.

Demonstração. Pela Proposição 2.1.4, o lema será estabelecido se dado $w \neq e$ em W, pudermos encontrar um subgrupo normal N tal que $w \notin N$ e W/N é residualmente $\mathcal{P}$.

Se w não está contido no grupo diagonal D de W, podemos tomar $N = D$, pois $W/D \simeq U$. Em contrapartida, se $w \in D$, então

$$w = g_{1(u_1)} \cdots g_{r(u_r)},$$

onde cada $g_i \neq e$ e $u_1, \ldots, u_r$ são elementos distintos de U. Como $\mathcal{P}$ é uma propriedade raiz, U tem um $\mathcal{P}$-filtro (Lema 2.1.11) e existe um subgrupo normal V de U tal que U/V tem a propriedade $\mathcal{P}$ e $u_1V, \ldots u_rV$ são elementos distintos de U/V (Lema 2.1.12). Além disso, como G é residualmente $\mathcal{P}$ e U/V tem a propriedade $\mathcal{P}$, pelo Lema 2.1.14 segue que $G \wr (U/V)$ é residualmente $\mathcal{P}$. O epimorfismo de W em $G \wr (U/V)$, definido pelo Lema 2.1.15, mapeia w em

$$g_{1(u_1V)} \cdots g_{r(u_rV)} \neq e,$$

tomando N como o núcleo desse epimorfismo, concluímos que $W/N \simeq G \wr (U/V)$ é residualmente $\mathcal{P}$, pois $G \wr (U/V)$ é residualmente $\mathcal{P}$. □

Teorema 2.1.17. Seja $\mathcal{P}$ uma propriedade satisfazendo a condição de que sempre que um grupo tem a propriedade $\mathcal{P}$ então todos os seus subgrupos também a tem. Se $G \wr_\Lambda P$ é residualmente $\mathcal{P}$, onde P é um grupo de permutação transitiva em Λ, então P tem a propriedade $\mathcal{P}$ ou G é abeliano.

Demonstração. Se G não é abeliano, podemos tomar $g \neq e$ no subgrupo derivado G' e então $g_x \neq e$ em D', o grupo derivado diagonal de $G \wr P$. Como $G \wr P$ é residualmente $\mathcal{P}$, existe um subgrupo normal N que não contém g_x e é tal que $(G \wr P)/N$ tem a propriedade $\mathcal{P}$. Se $N \cap P_\wr > \{e\}$, então pelo Lema 2.1.13, N contém D', mas isso é impossível, pois $g_x \in D'$ e $g_x \notin N$. Como $N \cap P_\wr = \{e\}$, então $P_\wr \simeq NP_\wr/N$. Agora $NP_\wr/N$, como um subgrupo de $(G \wr P)/N$, tem a propriedade $\mathcal{P}$ por hipótese, então $P \simeq P_\wr \simeq NP_\wr/N$ tem a propriedade $\mathcal{P}$. □

Teorema 2.1.18 (Gruenberg)**.** Sejam $\mathcal{P}$ uma propriedade raiz e suponha que os grupos G e H são residualmente $\mathcal{P}$. Se H é dado através de sua representação regular então $G \wr H$ é residualmente $\mathcal{P}$ se e somente se H tem a propriedade $\mathcal{P}$ ou G é abeliano.

Demonstração. A condição necessária é garantida pelos Lemas 2.1.14 e 2.1.16. A condição suficente é assegurada pelo Teorema 2.1.17. □

Corolário 2.1.19. O grupo $\mathbb{Z} \wr (\mathbb{Z} \wr \mathbb{Z})$ é residualmente um 2-grupo finito.

Demonstração. Vimos que a propriedade $\mathcal{P} :=$ 2-grupo finito é uma propriedade raiz. Além disso, $\mathbb{Z}$ é residualmente $\mathcal{P}$, é abeliano e é dado através de sua representação regular, isto é, age em si mesmo por multiplicação à esquerda, pelo Teorema de Gruenberg, $\mathbb{Z} \wr \mathbb{Z}$ é residualmente um 2-grupo finito.

Observe que $\mathbb{Z} \wr \mathbb{Z}$ também é dado através de sua representação regular, pois age em si mesmo por multiplicação à esquerda. Além disso, $\mathbb{Z}$ e $\mathbb{Z} \wr \mathbb{Z}$ são residualmente 2-grupo finito e $\mathbb{Z}$ é abeliano, portanto, segue do Teorema de Gruenberg que $\mathbb{Z} \wr (\mathbb{Z} \wr \mathbb{Z})$ é residualmente um 2-grupo finito. □

2.2 Imersão de Magnus

Sejam F um grupo livre de posto n, $R \lhd F$ e A um grupo abeliano livre com o mesmo posto de F. Sob as convenções anteriores, estudaremos o monomorfismo apresentado em [10] que consiste na imersão do quociente F/R' em $A \wr (F/R)$, denominada *Imersão de Magnus*. Para esta finalidade, desenvolveremos algumas noções básicas da teoria de anéis que podem ser encontradas em [5].

Definição 2.2.1. Um anel é um conjunto não vazio R, munido de duas operações binárias $+$ e $\cdot$, de modo que para todos $a,b,c \in R$, valem

(1) $(a+b)+c = a+(b+c)$

(2) $\exists 0 \in R$ tal que $a+0 = 0+a$

(3) $\exists a' \in R$ tal que $a+a' = 0$

(4) $a+b = b+a$

(5) $(ab)c = a(bc)$

(6) $a(b+c) = ab+ac$ e $(a+b)c = ac+ab$.

Se em um anel R existe $1 \in R$ de modo que $1a = a1 = a$ para todo $a \in R$, diremos que R é um *anel com unidade*. Se os elementos do anel R satisfazem $ab = ba$ para quaisquer $a,b \in R$, diremos que R é um *anel comutativo*. A seguir, iremos definir uma intereção de um grupo qualquer com um anel com unidade arbitrário.

Definição 2.2.2. Dados G um grupo e R um anel comutativo com unidade, definimos o *anel de grupo*, $R[G]$, de G com coeficientes em R como o conjunto de todas as somas formais

$$\sum_{x\in G} r_x x$$

onde $r_x \in R$ e $r_x \neq 0$ para um número finito de índices $x \in G$, munido com as regras de adição e multiplicação definidas respectivamente por

$$(\sum_{x\in G} r_x x) + (\sum_{x\in G} r'_x x) = \sum_{x\in G} (r_x + r'_x)x$$

e

$$(\sum_{x\in G} r_x x)(\sum_{x\in G} r'_x x) = \sum_{x\in G} (\sum_{yz=x} r_y r'_z)x$$

Exemplo 2.2.3. Seja G um grupo cíclico de ordem 3 e R o anel dos números reais. Tomando $G = \langle g \rangle$, o anel de grupo $R[G]$ é composto por todos os elementos da forma

$$a_2x^2 + a_1x + a_0e,$$

onde $a_0, a_1, a_2 \in R$ e e é a identidade de G, isto é, $R[G]$ é o conjunto de polinômios de grau até 2. Além disso, dados $a_2g^2 + a_1g + a_0e$ e $b_2g^2 + b_1g + b_0e$ segue que

$$(\sum_{i=0}^{2} a_i g^i) + (\sum_{i=0}^{2} b_i g^i) = (a_2+b_2)g^2 + (a_1+b_1)g + (a_0+b_0)e$$

e

$$(\sum_{i=0}^{2} a_i g^i)(\sum_{i=0}^{2} b_i g^i) = (a_2b_0+a_1b_1+a_0b_2)g^2+(a_2b_2+a_1b_0+a_0b_1)g+(a_2b_1+a_1b_2+a_0b_0)e$$

são a soma e produto, respectivamente, de dois elementos em $R[G]$.

A seguir, dado um grupo G, definiremos uma coleção de grupos abelianos a qual a ação de G é compatível com a estrutura abeliana. Esta família de grupos será fortemente utilizada em nosso resultado principal.

Definição 2.2.4. Seja G um grupo. Um G-*módulo* à esquerda é um grupo abeliano A munido de uma ação do grupo G à esquerda $\rho : G \times A \longrightarrow A$ tal que

$$g \cdot (a+b) = g \cdot a + g \cdot b,$$

onde $g \cdot a$ denota a ação à esquerda $\rho(g,a)$.

Dado um grupo G, A e B dois G-módulos. Um G-*módulo homomorfismo* se $\varphi : A \to B$ é um homomorfismo que preserva a estrutura de módulo, isto é, $(x+y)\varphi = (x)\varphi + (y)\varphi$ e $(gx)\varphi = g(x)\varphi$, onde $x, y \in A$ e $g \in G$.

Sejam H um grupo e A um $\mathbb{Z}[H]$-módulo à esquerda. Defina $G = A \rtimes H$, onde a ação é de conjugação. Observe que $A \lhd G$ e A é abeliano, isto posto, veremos que A pode ser visto como um $\mathbb{Z}[G]$-módulo com a mesma ação de H em A. Com efeito, para $a_1h \in G$, a ação é dada por $(a_1h)a(a_1h)^{-1} = a_1(hah^{-1})a_1^{-1} = hah^{-1}$, pois $hah^{-1} \in A$ e A é abeliano.

As definições representam toda a base teórica para a demonstração dos resultados a seguir, provenientes do artigo [15], que representm nosso objetivo nesta seção.

Teorema 2.2.5. Sejam R um subgrupo normal do grupo livre F, onde F é gerado por $\{x_1 \ldots, x_n\}$, A um $\mathbb{Z}[F/R]$-módulo e $a_1, \ldots, a_n \in A$.

(a) A aplicação

$$x_i \longmapsto (a_i, x_iR)$$

é estendida para um homomorfismo

$$\varphi : F \longrightarrow A \rtimes (F/R),$$

(b) $R' \leq ker\, \varphi \leq R$.

(c) Sejam $\bar{\varphi} : F \to F/R'$ o epimorfismo natural e $j : F/R' \to A \rtimes (F/R)$ a aplicação tal que $\bar{\varphi} j = \varphi$. Se A é o $\mathbb{Z}[F/R]$-módulo com base $\{a_1, \dots, a_n\}$, então j é injetiva.

Demonstração.

(a) Segue imediatamente do fato de que F é um grupo livre.

(b) Seja $\gamma : F \longrightarrow A$ a aplicação definida por $w(x_1, \dots, x_n) \mapsto w(a_1, \dots a_n)$, mostraremos que $ker\varphi \leq R$. Com efeito, seja $w(x_1, \dots x_n) \in Ker\,\varphi$, então

$$(w(x_1, \dots, x_n))\varphi = (w(a_1, \dots a_n), w(x_1, \dots, x_n)R) = (0, R)$$

implica $w \in R$.

Agora tome $u, v \in R$, note que

$$\begin{aligned}
(u)\varphi(v)\varphi &= ((u)\gamma, uR)((v)\gamma, vR)\\
&= ((u)\gamma, R)((v)\gamma, R)\\
&= ((u)\gamma + (v)\gamma, R)\\
&= ((v)\gamma + (u)\gamma, R)\\
&= ((v)\gamma, R)((u)\gamma, R)\\
&= (v)\varphi(u)\varphi.
\end{aligned}$$

De $(u)\varphi(v)\varphi = (v)\varphi(u)\varphi$ decorre que $\varphi([u, v]) = (0, R)$, logo $R' \leq ker\,\varphi$.

(c) Inicialmente, temos o diagrama a seguir

$$\begin{tikzcd}
F \arrow[r, "\overline{\varphi}"] \arrow[dr, "\varphi"'] & F/R' \arrow[d, "j"] \\
& A \rtimes (F/R)
\end{tikzcd}$$

Queremos mostrar que a aplicação j é injetiva, para isto, utilizaremos um $\mathbb{Z}[F/R]$-módulo N, o qual definiremos a seguir, em conjunto com uma imersão $\theta : F/R' \to N \rtimes (F/R)$. Na sequência, teremos o diagrama

$$\begin{tikzcd}
F \arrow[r] & F/R' \arrow[rr, "\theta"] \arrow[dr, "j"'] & & N \rtimes (F/R) \\
& & A \rtimes (F/R) \arrow[ur, dashed, "\overline{\theta}"'] &
\end{tikzcd}$$

e iremos mostrar que ele pode ser completado com uma aplicação $\overline{\theta}$ satisfazendo $\overline{\theta} j = \theta$. Uma vez que se $j(x) = j(y)$, temos $\overline{\theta}(j(x)) = \overline{\theta}(j(y))$, daí $x = y$, pois $\overline{\theta} j = \theta$ é injetiva. Logo j é injetiva e a demonstração estará finalizada.

Tome N como o grupo abeliano de todas as aplicações $f : F/R \longrightarrow R/R'$. Considere a aplicação

$$\begin{array}{rcl} F/R \times N & \longrightarrow & N \\ (yR, f) & \longmapsto & f^{y^{-1}R} \end{array}$$

satisfazendo a relação $f^{y^{-1}R}(xR) = f(y^{-1}xR)$ para todo $xR \in F/R$. Mostraremos que esta relação é uma ação a esquerda. De fato,

(i) $f^{R}(xR) = f(RxR) = f(xR)$ para todo $f \in N$ e $xR \in F/R$.

(ii) $f^{(y_1y_2R)^{-1}}(xR) = f(y_2^{-1}y_1^{-1}xR) = f^{y_2^{-1}R}(y_1^{-1}xR) = (f^{y_2^{-1}R})^{y_1^{-1}R}(x)$ para todos y_1R, y_2R e xR em F/R.

Além disso, N é um $\mathbb{Z}[F/R]$-módulo à esquerda, pois dados $yR \in \mathbb{Z}[F/R]$ e $f_1, f_2 \in N$, segue que

$$\begin{aligned} (f_1 + f_2)^{y^{-1}R}(xR) &= (f_1 + f_2)(y^{-1}xR) \\ &= f_1(y^{-1}xR) + f_2(y^{-1}xR) \\ &= f_1^{y^{-1}R}(x) + f_2^{y^{-1}R}(x) \quad \forall x \in H. \end{aligned}$$

Isto posto, podemos considerar o produto semidireto $N \rtimes (F/R)$. Além disso, a Proposição 1.3.16 nos assegura a existência do epimorfismo

$$\begin{array}{rcl} q : F/R' & \longrightarrow & F/R \\ wR' & \longmapsto & wR. \end{array}$$

Utilizando a ação de F/R em N, podemos induzir uma ação

$$\begin{array}{rcl} F/R' \times N & \longrightarrow & N \\ (wR', f) & \longmapsto & f^{w^{-1}R'} \end{array}$$

onde $f^{w^{-1}R'}(xR) = f(w^{-1}xR)$ para todo $xR \in F/R$.

Agora, construiremos a imersão $\theta : F/R' \longrightarrow N \rtimes (F/R)$.

Seja $T = \{t_{uR} \mid uR \in F/R'\}$ um transversal para R/R' em F/R', onde $(t_{uR})q = uR$. Observe que para todo $xR' \in F/R'$, temos $t_{uR}xt_{uxR}^{-1} \in Ker\, q = R/R'$, pois

$$(t_{uR}xt_{uxR}^{-1}R')q = (t_{uR}R')q(xR)q(t_{uxR}^{-1})q = uRxR(ux)^{-1}R = R.$$

Agora, para cada $xR \in F/R$, podemos definir uma aplicação $\sigma_{xR} : F/R \longrightarrow F/R'$ dada por $uR \mapsto t_{uR}xt_{uxR}^{-1}$. Observe que a composição de σ_{xR} com q é a função identidade em F/R, somente este fato é necessário para o desenvolvimento da demonstração, isto posto, iremos omitir o elemento xR fixado. Para cada $wR' \in F/R'$ defina $\delta_{wR'} \in N$ por

$$\delta_{wR'}(uR) = \sigma(uR)wR'(\sigma(w^{-1}uR))^{-1} \quad \text{para todo} \quad uR \in F/R.$$

Para δ tal como definido acima, temos

$$(\delta_{w_2R'})^{w_1^{-1}R'}(uR) = \delta_{w_2R'}(w_1^{-1}uR) = \sigma(w_1^{-1}uR)w_2R'(\sigma(w_2^{-1}w_1^{-1}uR))^{-1}$$

e

$$\delta_{w_1R'}(uR) = \sigma(uR)w_1R'(\sigma(w_1^{-1}uR))^{-1}.$$

Logo

$$\delta_{w_1R'}(uR).(\delta_{w_2R'})^{w_1R'}(uR) = \sigma(uR)w_1w_2R'(\sigma(w2^{-1}w_1^{-1}u))^{-1} = \delta_{w_1w_2R'}(uR)$$

para todo $uR \in F/R$.

Mostraremos que se $wR' \in R/R'$ é tal que $\delta_{wR'}$ é o elemento identidade de N, isto é, $\delta_{wR'}(uR) = R$ para todo $uR \in F/R$, então wR' é o elemento identidade de R/R'. Com efeito, se $\delta_{wR'}(uR)\delta_{vR'}(uR) = \delta_{vR'}(uR)$ para todo $uR \in F/R$ e $wR' \in R/R'$, então por definição de $\delta_{wR'}$ temos

$$\delta_{wR'}(uR) = \sigma(uR)wR'(\sigma(w^{-1}uR))^{-1} = \sigma(uR)wR'(\sigma(uR))^{-1},$$

mas $\delta_{wR'}$ é a aplicação identidade, então

$$\delta_{wR'}(uR) = R',$$

portanto, $wR' = R'$. Como $w \in R'$ concluímos que wR' é o elemento identidade de R/R'.

Defina

$$\begin{array}{rcl} \theta : F/R' & \longrightarrow & N \rtimes (F/R) \\ wR' & \longmapsto & (\delta_{wR'}, wR), \end{array}$$

então

$$\begin{aligned} (w_1R')\theta(w_2R')\theta =& (\delta_{w_1R'}, w_1R)(\delta_{w_2R'}, w_2R) \\ =& (\delta_{w_1R'}(\delta_{w_2R'})^{w_1^{-1}R}, w_1w_2R) \\ =& (\delta_{w_1w_2R'}, w_1w_2R) \\ =& (w_1w_2R')\theta \end{aligned}$$

para todo $w_1, w_2 \in F$, portanto, θ é homomorfismo. Além disso, se

$$\theta(wR') = (\delta_{wR'}, wR) = (0, R)$$

então $w \in R$ e $\delta_{wR'} = 0$, logo $w \in R'$. Portanto, θ é um homomorfismo injetivo.

Para concluir a demonstração, precisamos mostrar que o diagrama

$$\begin{tikzcd} F \arrow[r] & F/R' \arrow[rr, "\theta"] \arrow[dr, "j"] & & N \rtimes (F/R) \\ & & A \rtimes (F/R) \arrow[ur, dashed, "\overline{\theta}"] & \end{tikzcd}$$

pode ser completado com uma aplicação $\overline{\theta}$ satisfazendo $\overline{\theta} j = \theta$.

Defina $v_i \in N$ tal que

$$(x_iR')\theta = (v_i, x_iR)$$

e $\kappa : A \longrightarrow N$ o $\mathbb{Z}[F/R]$-módulo homomorfismo definido por $a_i \mapsto v_i$. Então, a aplicação

$$(a, yR) \mapsto ((a)\kappa, yR)$$

satisfaz a propriedade desejada para $\overline{\theta}$. De fato, dado $x_iR' \in F/R'$

$$(x_iR')j = (a_i, x_iR),$$

logo,

$$(x_iR')j\overline{\theta} = (a_i, x_iR)\overline{\theta} = (v_i, yR) = (x_iR')\theta.$$

□

Seja N o grupo abeliano de todas as aplicações definidas sobre um grupo H com valores em um grupo K. Um elemento $n \in N$ pode ser identificado com um elemento de $Dr_{h\in H}K$. De fato, seja $(k_h)_{h\in H} \in Dr_{h\in H}K$, defina a aplicação φ de modo que $((k_h)_{h\in H})\varphi = n$ onde n é a aplicação satisfazendo $(h)n = k_h$. Verificaremos que a aplicação φ é um isomorfismo. Sejam $(k_h)_{h\in H}, (l_h)_{h\in H} \in Dr_{h\in H}K$ tais que $((k_h)_{h\in H})\varphi = n$ e $((l_h)_{h\in H})\varphi = m$, então

$$\begin{aligned}((k_h)_{h\in H}(l_h)_{h\in H}))\varphi &= ((k_hl_h)_{h\in H}))\varphi \\ &= (h)nm \\ &= (h)n(h)m \\ &= ((k_h)_{h\in H})\varphi((l_h)_{h\in H}))\varphi.\end{aligned}$$

Além disso, n é a função nula se, e somente se, $(b)n = e_A$ para todo $b \in B$, isto é, $Ker\,\varphi = \{e\}$. A sobrejetividade é imediata da definição de φ. Observe que a ação de H em N definida por $(x)n^{h^{-1}} = (h^{-1}x)n$ é compatível com a ação de H em $Dr_{h\in H}K$. Deste modo podemos interpretar o grupo base de um produto entrelaçado restrito como um grupo de funções. Sob esta ótica podemos ver o grupo $N \rtimes (F/R)$ da proposição anterior como um produto entrelaçado, com esta reformulação, obtemos o seguinte corolário.

Corolário 2.2.6 (Imersão de Magnus)**.** *Seja F um grupo livre gerado por $\{x_1, \ldots, x_n\}$ e $R \lhd F$. Seja A um grupo abeliano livre gerado por $\{a_1, \ldots, a_n\}$. Então $F/R' \hookrightarrow A \wr (F/R)$, cuja imersão é dado pela aplicação $x_iR' \mapsto (a_i, x_iR)$, $1 \le i \le n$.*

Tomando $R = F'$ na proposição acima obtemos

$$F/F'' \hookrightarrow A \wr (F/F').$$

Note que F/F' é um grupo abeliano livre e F/F'' é um grupo metabeliano livre, ambos com o mesmo posto de F. Assim, obtemos uma imersão do grupo metabeliano livre de posto n no produto entrelaçado $A \wr (F/F')$.

CAPÍTULO 3

Automorfismos da árvore uni-raiz m-regular $\mathcal{T}_m$

Neste capítulo iremos definir a árvore uni-raiz m-regular bem como explorar determinados temas que emergem através do estudo deste objeto, tais como sua estrutura, as propriedades de seu grupo de automorfismos, a interpretação de automorfismos como autômato e funções de crescimento.

3.1 Grafos e dígrafos

O problema das sete pontes de Königsberg consiste em perguntar se, partindo de um determinado ponto, é possível atravessar todas as sete pontes uma única vez e chegar ao ponto de origem. Este problema foi resolvido por Leonhard Euler em 1736, cuja resposta negativa concebeu o estudo da Teoria de Grafos. Além da aplicação logística, grafos são estruturas capazes de organizar e expor informações de maneira simplificada. As definições presentes nesta seção são provenientes de [2] e [9], as quais podem ser consultadas para maiores informações.

Definição 3.1.1. Sejam $V(G)$, $R(G)$ e $E(G)$ conjuntos disjuntos dois a dois, onde $R(G)$ não necessariamente é não-vazio. Defina o conjunto $V_2(G) = \{\{u,v\} \mid u,v \in V(G)\}$ de pares não-ordenados de $V(G)$. Um grafo G é uma tripla ordenada $(V(G),R(G),E(G))$, onde $V(G)$ é o conjunto de vértices, $R(G)$ é o conjunto de rótulos, $E(G)$ o conjunto de arestas e $\psi_G : E(G) \to V_2(G) \times R(G)$ é uma aplicação de incidência. Para cada aresta $e \in E(G)$ está associado um elemento $(\{u,v\},x)$, com $u,v \in V(G)$ e $x \in R(G)$, isto é, $(e)\psi_G = (\{u,v\},x)$. Dizemos que aresta e conecta u e v e é rotulada por x e a representaremos por $(\{u,v\},x)$ ao invés de e.

Para simplificar a notação, quando lidamos com um único grafo G, utilizaremos as notações V,R e E para o conjunto de vértices, rótulos e arestas de G, respectivamente. Além disso, iremos cometer um abuso de notação ao representar o elemento $(\{u,v\},x)$ por (u,v,x), levando em consideração que a ordem das duas primeiras entradas são irrelevantes.

Exemplo 3.1.2. Seja G o grafo constítuido por $V = \{A,B,C,D,E\}$, $R = \{1,2,3,4,5,6,7\}$ e $E = \{(A,B,1),(A,C,2),(A,D,3),(B,D,4),(B,E,5),(C,D,6),(C,E,7)\}$. Representamos G através do diagrama

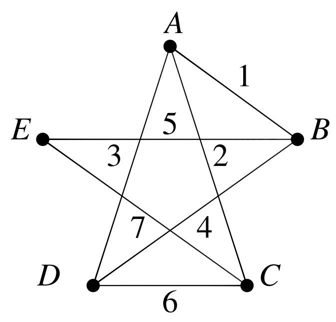


Figura 3.1 Grafo G

Se em um grafo G existir uma aresta $(v,v,l) \in E(G)$, dizemos que (v,v,l), ou simplesmente que l é um *loop* e o representamos por

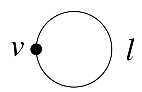


Figura 3.2 Loop

Além dos *loops*, nossa definição permite a existência de mais de uma aresta conectando um mesmo par de vértices. Se e_1 e e_2 são arestas de um grafo G tais que $(e_1)\psi_G = (u,v,x)$ e $(e_2)\psi_G = (u,v,y)$, com x não necessariamente distinto de y, dizemos que (u,v,x) e (u,v,y) são *paralelas* e as representamos por

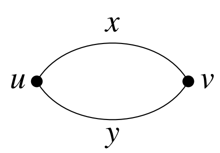


Figura 3.3 Arestas paralelas

Outra consequência da nossa definição é que os rótulos podem se repetir em arestas distintas, isto permite utilizar o conjunto de rótulos para descrever uma relação sobre dois vértices, como por exemplo, a distância entre eles.

Exemplo 3.1.3. Seja T o grafo constítuido pelo conjunto de vértices $V = \{A,B,C\}$, conjunto de rótulos $R = \{2cm, 3cm\}$ e conjunto de arestas $E = \{(A,B,3cm),(A,C,3cm),(B,C,2cm)\}$. Então T representa um triângulo isósceles com base medindo $2cm$, lados medindo $3cm$ e é expresso através do diagrama

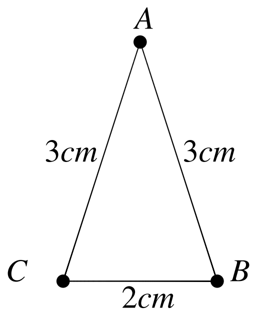


Figura 3.4 Grafo T

A definição utilizada para grafos, embora não seja usual, foi utilizada justamente por ter a vantagem de armazenar informações sobre a relação entre dois vértices, fato este que será explorado posteriormente. Ainda assim, quando não houver a necessidade do uso de rótulos, podemos considerar R como o conjunto vazio, neste caso, a notação para um grafo G é reduzida para $G = (V(G),E(G))$.

Diremos que duas arestas e_1 e e_2 são adjacentes se elas possuem um vértice em comum, isto é, se $e_1 = (\{u,v\},x)$ e $e_2 = (\{u,w\},y)$, então e_1 e e_2 são adjacentes.

Se G e H são grafos tais que $V(H) \subseteq V(G)$, $R(H) \subseteq R(G)$ e $E(H) \subseteq E(G)$, dizemos que H é um *subgrafo* de G.

Definição 3.1.4. Seja $G = (V(G),R(G),E(G))$ um grafo. Um caminho em G é um subgrafo $P = (V(P),R(P),E(P))$ onde o conjunto de arestas pode ser organizado na forma

$$E(P) = \{(v_{k_1},v_{k_2},x_1),(v_{k_2},v_{k_3},x_2)\ldots,(v_{k_{r-1}},v_{k_r},x_{r-1})\},$$

com $v_{k_i} \in V(P)$, v_{k_i} e v_{k_j} não necessariamente distintos, exceto quando $j = i+1$, nesse caso $v_{k_i} \neq v_{k_{i+1}}$. Em outras palavras, um caminho é uma sequência de arestas adjacentes.

Se v_{k_i} são todos distintos dizemos que P é um caminho simples. Representamos tal caminho por $P = v_{k_1}x_1v_{k_2}\ldots v_{k_{r-1}}x_{r-1}v_{k_r}$.

Exemplo 3.1.5. Seja G o grafo do Exemplo 3.1.2 e $P = (V(P),R(P),E(P))$ um subgrafo de G, onde $V(P) = \{A,B,C,E\}$ e $E(P) = \{(A,B,1),(B,E,5),(E,C,7),(C,A,2)\}$, então o subgrafo P é um caminho no grafo G representado por

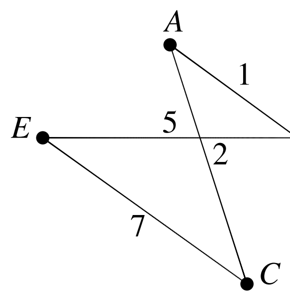


Figura 3.5 Caminho no grafo G

Denominamos por circuito de um grafo G o subgrafo $C = (V(C), R(C), E(C))$, onde C é um caminho tal como definido acima com a particularidade de que $v_{k_r} = v_{k_1}$. Um circuito simples é um circuito sem auto-interseções, ou seja, v_{k_i} são todos distintos exceto pelo primeiro e último.

O comprimento de um circuito simples é o número de vértices distintos que pertencem ao circuito. Diremos que o grafo G é do tipo m-circuito se o maior circuito simples em G tem comprimento m, neste caso, utilizaremos a notação $c(G) = m$. Caso $m = 0$ ou $m = 1$, isto é, G não tem circuito simples ou o único circuito simples é um *loop*, respectivamente, diremos que G é acíclico.

Exemplo 3.1.6. Seja G o grafo do Exemplo 3.1.2 e $C = (V(C), R(C), E(C))$ um subgrafo de G, onde $V(C) = \{A, C, D\}$, $R(C) = \{2, 3, 6\}$ e $E(C) = \{(A, C, 2), (A, D, 3), (C, D, 6)\}$, então C é um circuito no grafo G representado por

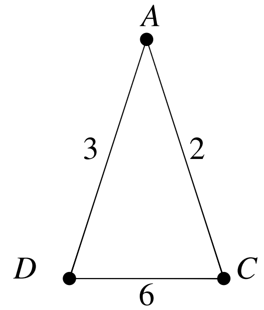


Figura 3.6 Circuito no grafo G

Note que C é um circuito simples e tem comprimento 3.

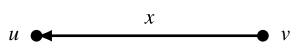
Um interesse que surge naturalmente nos estudos de qualquer estrutura é a comparação, utilizamos desta ferramenta para obter informações de um objeto e levar para outro. Em teoria de grupos, utilizamos os homomorfismos para tal. Isto posto, definiremos o que virá a ser o homomorfismo para um grafo.

Definição 3.1.7. Um homomorfismo de um grafo G em outro grafo H é uma aplicação $\varphi : V(G) \longrightarrow V(H)$ que preserva arestas. Em outras palavras, se $u, v \in V(G)$ são vértices conectados por uma aresta, então seus respectivos correspondentes $\varphi(u), \varphi(v) \in V(H)$ devem estar conectados por uma aresta. Um isomorfismo de grafos é um homomorfismo bijetor.

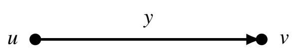
Em nossa definição de grafos, utilizamos o conjunto $V_2(G)$ constítuido de pares não-ordenados para definir o conjunto de arestas $E(G)$. Se na definição de grafo utilizarmos $V(G) \times V(G)$ ao invés de $V_2(G)$, a definição de grafo obtida deve preservar a ordem das entradas dos vetores em $(E(G))\psi_G$, esta definição dá origem ao que chamamos de *grafo direcionado* ou *dígrafo*. Embora a definição possa ser feita de modo análogo a definição de grafos, iremos optar por uma definição equivalente mais limpa.

Definição 3.1.8. Um grafo direcionado ou dígrafo D é uma tripla ordenada $(V(D), R(D), A(D))$, onde $V(D)$ é um conjunto de vértices, $R(D)$ é um conjunto de rótulos e $A(D) \subseteq V(D) \times V(D) \times R(D)$ é o conjunto de arcos. Para cada arco $a \in A(D)$ está associado uma tripla ordenada (u, v, x), com $u, v \in V(D)$ e $x \in R(D)$, neste caso, dizemos que u é o vértice inicial, v é o vértice final e x é o rótulo do arco (u, v, x).

Um arco (u, v, x) em um dígrafo é representado por



enquanto que (v, u, y) é representado por



.

Vale ressaltar que, para critério de simplificação, adotamos as mesmas notações para representar um arcos e arestas, portanto, sempre iremos explicitar se o objeto é um grafo ou um dígrafo.

Exemplo 3.1.9. Seja D o dígrafo constítuido por $V = \{a, b, c, d, e\}$, $R = \{1, 2, 3, 4, 5, 6\}$ e $E = \{(a, c, 1), (c, e, 2), (e, b, 3), (b, d, 4), (d, a, 5), (b, a, 6)\}$. Representamos D por

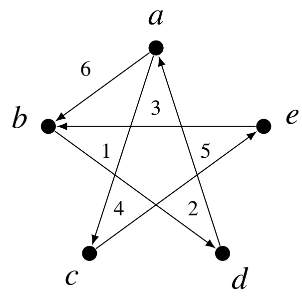


Figura 3.7 Dígrafo D

A seguir, iremos redefinir alguns conceitos de grafos de forma análoga para dígrafos.

Dizemos que e H é um *subdígrafo* de um dígrafo D se $V(H) \subseteq V(D)$, $R(H) \subseteq R(D)$ e $A(H) \subseteq A(D)$.

Definição 3.1.10. Seja $D = (V(D), R(D), E(D))$ um dígrafo. Um caminho em D é um subdígrafo $P = (V(P), R(P), E(P))$ onde o conjunto de arcos pode ser organizado na forma

$$E(P) = \{(v_{k_1}, v_{k_2}, x_1), (v_{k_2}, v_{k_3}, x_2) \ldots, (v_{k_{r-1}}, v_{k_r}, x_{r-1})\},$$

com $v_{k_i} \in V(P)$, v_{k_i} e v_{k_j} não necessariamente distintos, exceto quando $j = i+1$, nesse caso $v_{k_i} \neq v_{k_{i+1}}$. Isto é, um caminho é uma sequências de arcos onde o vértice final de um arco é o vértice inicial do arco seguinte. Se v_{k_i} são todos distintos dizemos que P é um caminho simples em um dígrafo.

Embora as definições sejam extremamente similares, é necessário observar que os caminhos em um dígrafo são mais restritivos, pois os arcos são triplas ordenadas. Isto posto, um caminho em um dígrafo deve sempre percorrer a direção da seta.

Exemplo 3.1.11. Seja D o dígrafo do Exemplo 3.1.9. O subdígrafo $P(D) = a1c2e$ é um caminho em D. Por outro lado, o subdígrafo H definido pelos arcos $A(H) = \{(a,b,6), (a,c,1)\}$ não é um caminho em um dígrafo, entretanto, seria um caminho em um grafo não-direcionado de D também fosse um grafo não-direcionado.

Denominamos por circuito de um dígrafo D o subgrafo $C = (V(C), R(C), E(C))$, onde C é um caminho em um dígrafo com a particularidade de que $v_{k_r} = v_{k_1}$. Um circuito simples em um dígrafo é um circuito sem auto-interseções, ou seja, v_{k_i} são todos distintos exceto pelo primeiro e último. As definições de comprimento de um circuito simples de um dígrafo e dígrafo do tipo m-circuito são análogas as suas versões para grafos.

Exemplo 3.1.12. O caminho $P = a6b4d5a6b$ no dígrafo do Exemplo 3.1.9 não é simples, pois o vértice a é revisitado uma segunda vez e não é o vértice final no caminho.

3.2 Árvore uni-raiz m-regular $\mathcal{T}_m$ e seu grupo de automorfismos

Sejam m um inteiro positivo e Y o alfabeto $\{0,\ldots,m-1\}$. Considere $\mathcal{M} = \mathcal{M}(Y)$ o conjunto de todas as palavras finitas formadas por elementos de Y. Com a operação de concatenação de palavras, $\mathcal{M}$ assume estrutura de *monoide*, isto é, um conjunto com uma operação associativa e um elemento neutro segundo a operação. Neste caso, o elemento neutro é a palavra vazia $\emptyset$.

Definição 3.2.1. A árvore uni-raiz m-regular $\mathcal{T}_m$ é o grafo $(V(\mathcal{T}_m), E(\mathcal{T}_m))$, onde $V(\mathcal{T}_m) = \mathcal{M}$ e um par não ordenado $\{u,v\}$ pertence a $E(\mathcal{T}_m)$ se e somente se $v = uy$ ou $u = vy$, para algum $y \in Y$, com $u,v \in \mathcal{M}$.

Em resumo, a árvore uni-raiz m-regular é um grafo sobre um alfabeto Y, cujos vértices são palavras finitas e as aretas conecatam duas palavras se, e somente se, uma delas é prefixo da outra.

Definição 3.2.2. Denominaremos por *nível n* da árvore $\mathcal{T}_m$ o conjunto de todas as palavras de comprimento n, isto é, $\{u \in \mathcal{M} \mid |u| = n\}$.

Para o caso em que $m = 2$, $\mathcal{T}_2$ será denominada árvore binária e pode ser representada graficamente por:

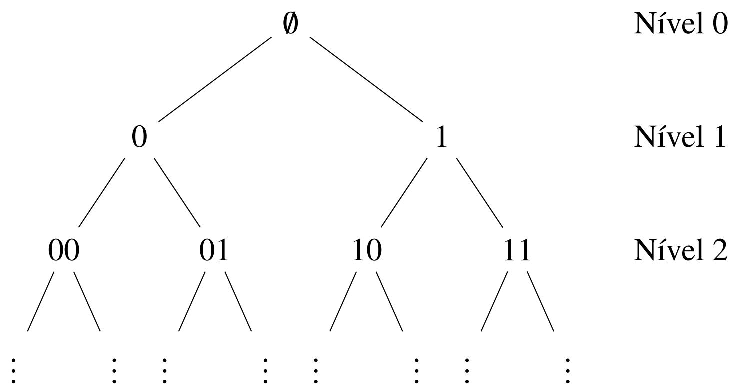


Figura 3.8 Árvore binária

Definição 3.2.3. Um automorfismo γ de $\mathcal{T}_m$ é um isomorfismo de grafos $\gamma : \mathcal{T}_m \longrightarrow \mathcal{T}_m$.

A Definição 3.1.7 nos diz que homomorfismos de grafos devem preservar as relações de arestas, com isto em mente, note que os automorfismos da árvore $\mathcal{T}_m$ devem necessariamente fixar a raiz e agem permutando os vértices em cada nível. Se munirmos o conjunto de todos os automorfismos com a operação de composição de funções, este conjunto se torna um grupo, denotado por $\mathcal{A}_m$. A seguir, iremos descrever uma expressão para os automorfismos em $\mathcal{A}_m$.

As permutações do conjunto Y podem ser estendidas "rigidamente"para automorfismos de $\mathcal{A}_m$ por

$$\sigma : yu \longrightarrow y^{\sigma}u, \quad \forall y \in Y, \quad \forall u \in \mathcal{M},$$

o que nos fornece uma imersão do grupo S_m em $\mathcal{A}_m$.

Em contrapartida, um automorfismo $\gamma \in \mathcal{A}_m$ induz uma permutação σ_γ no conjunto Y, basta tomar a restrição $\sigma_\gamma = \gamma : Y \longrightarrow Y$, isto é, restringir o automorfismo ao primeiro nível da árvore $\mathcal{T}_m$. Caso a restrição σ_γ seja não-trivial, diremos que γ é ativo. Em decorrência disso, vemos que γ e σ_γ possuem a mesma ação em Y, portanto, a composição $\gamma\sigma_\gamma^{-1}$ possui ação trivial em Y, o que nos fornece a representação $\gamma\sigma_\gamma^{-1} = (\gamma_0, \ldots, \gamma_{m-1})$, onde γ_y é um automorfismo da subárvore $y\mathcal{T}_m$.

Além disso, $(\gamma_0, \ldots, \gamma_{m-1})$ induz para cada $y \in Y$ um automorfismo γ_y da subárvore $y\mathcal{T}_m$ cujos vértices formam o conjunto $y\mathcal{M}$. Usando o isomorfismo canônico $yu \longrightarrow u$ entre a subárvore $y\mathcal{T}_m$ e a árvore $\mathcal{T}_m$, podemos identificar α_y como um automorfismo de $\mathcal{A}_m$, assim

$$\gamma = (\gamma_0, \ldots, \gamma_{m-1})\sigma_\gamma,$$

onde $\gamma_y \in \mathcal{A}_m$ para todo $y \in Y$. Com a observação anterior, podemos definir recursivamente para todo $u \in \mathcal{M}$ o automorfismo γ_u como a componente de γ que age na subárvore $u\mathcal{T}m$, também nos referimos a γ_u como o vértice u de γ. Com essas considerações, podemos identificar o grupo $\mathcal{A}_m$ com o produto entrelaçado dele mesmo com o grupo das permutações S_m de Y, ou seja,

$$\mathcal{A}_m = \mathcal{A}_m \wr_Y S_m = \mathcal{A}_m^{(Y)} \rtimes_\varphi S_m,$$

onde a ação de S_m é sobre os índices. Assim, dado $\sigma \in S_m$ e $(\gamma_0, \ldots, \gamma_{m-1})$ segue que

$$\sigma(\gamma_0, \ldots, \gamma_{m-1}) = (\gamma_{0^\sigma}, \ldots, \gamma_{(m-1)^\sigma})\sigma.$$

Em vista disso, podemos determinar o produto e o inverso de elementos de $\mathcal{A}_m$. Dados $\gamma = (\gamma_0, \ldots, \gamma_{m-1})\sigma_\gamma, \beta = (\beta_0, \ldots, \beta_{m-1})\sigma_\beta \in \mathcal{A}_m$,

$$\gamma\beta = (\gamma_0\beta_{0^{\sigma_\gamma}}, \ldots, \gamma_{m-1}\beta_{(m-1)^{\sigma_\gamma}})\sigma_\gamma\sigma_\beta$$

e

$$\gamma^{-1} = \sigma_\gamma^{-1}(\gamma_0^{-1}, \ldots, \gamma_{m-1}^{-1}) = (\gamma^{-1}_{0^{\sigma_\gamma^{-1}}}, \ldots, \gamma^{-1}_{(m-1)^{\sigma_\gamma^{-1}}}).$$

Para compreender a ação de um automorfismo de $\mathcal{T}_m$, devemos entender sua ação nas palavras que compõem os vértices da árvore em questão. Seja $yu \in \mathcal{M}$, onde $y \in Y$ e $u \in \mathcal{M}$, um automorfismo $\gamma = (\gamma_0, \ldots, \gamma_{m-1})\sigma_\gamma$ de $\mathcal{T}_m$ age em yu da forma

$$(yu)^\gamma = (yu)^{(\gamma_0,\ldots,\gamma_{m-1})\sigma_\gamma} = y^{\sigma_\gamma} u^{\gamma_y}.$$

Exemplo 3.2.4. Seja $\alpha = (\alpha_0, \alpha_1)\sigma$ um automorfismo da árvore binária $\mathcal{T}_2$, onde $\alpha_0 = (e,e)$ é o automorfismo identidade, $\alpha_1 = (\alpha, e)$ e σ é a transposição $(0\,1)$. Primeiro, observe que α pode ser reescrito na forma $\alpha = ((e,e),(\alpha,e))\sigma = (e,(\alpha,e))\sigma$. A ação de α na palavra 101 é descrita por

$$(101)^\alpha = (101)^{(e,(\alpha,e))\sigma} = 1^\sigma(01)^{\alpha_1} = 0(01)^{(\alpha,e)} = 0(0^e 1^{\alpha_0}) = 001^\alpha = 000.$$

Com isto, podemos aferir que o vértice 101 ocupará a posição do vértice 000 da árvore original.

Definição 3.2.5. Seja $\gamma = (\gamma_0, \ldots, \gamma_{m-1})\sigma_\alpha$ um automorfismo de $\mathcal{T}_m$, o conjunto de estados de γ é definido por

$$Q(\gamma) = \{\gamma_u \mid u \in \mathcal{M}\},$$

ou recursivamente por

$$Q(\gamma) = \{\gamma, \gamma_0, \ldots, \gamma_{m-1}\} \cup Q(\gamma_0) \cup \cdots \cup Q(\gamma_{m-1}).$$

Um elemento $\gamma_u \in Q(\gamma)$ é chamado de estado de γ.

A utilização do termo *estado* é motivada pelo conceito computacional denominado *autômato* que será desenvolvido adiante.

3.3 Autômato

A Teoria de Autômatos representa uma das áreas mais antigas na Ciência da Computação e dentre suas motivações iniciais estavam a construção de compiladores e design de circuitos eletrônicos. Para ampliar as aplicações dessa teoria, derivamos novos tipos de Autômatos da definição tradicional. Descreveremos abaixo uma das derivações de autômato, denominado Máquina de Mealy. Conceitos mais gerais sobre o tema podem ser consultados em [4].

A seguir definiremos a Máquina de Mealy, mas antes disso convencionaremos a nomenclatura de aplicação parcial como sendo uma aplicação que não necessariamente esta definida em todos os pontos do domínio.

Definição 3.3.1. Uma *máquina de Mealy* é uma sêxtupla $A_q = (Q, \Sigma, \Gamma, f, l, q_0)$ onde

- Q é um conjunto de estados;
- Σ é o alfabeto de entrada;
- Γ é o alfabeto de saída;
- $f : Q \times \Sigma \to Q$ é a aplicação parcial de transição de estados;
- $l : Q \times \Sigma \to \Gamma$ é a aplicação parcial de saída;
- q_0 é o estado denominado inicial.

Ao decorrer do texto, iremos nos referir a Máquina de Mealy apenas por autômato, pois utilizamos somente este tipo de autômato. Dizemos que o autômato é finito se o conjunto de estados Q é finito.

Para um q fixo, denotamos $l(q,a) = l_q(a)$ e chamamos $l_q : \Sigma \to \Gamma$ de *função de estados*.

Um autômato pode ser expresso por meio de um dígrafo, cujo o conjunto de vértices é o conjunto de estados Q, o conjunto de rótulos é $R = \{a|b \mid a,b \in Y\}$, onde Y é o alfabeto da árvore uni-raiz m-regular, e uma tripla ordenada $(q, p, a|b)$, com $q, p \in Q$ e $a, b \in Y$, pertence ao conjunto de arcos se, e somente se, $f(q,a) = p$ e $l(q,a) = b$. Um arco representa a transição do estado q para o estado p, graficamente, temos

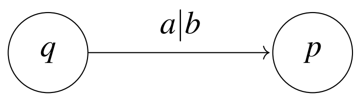


Figura 3.9 Transição de estados

A partir de agora, omitiremos o estado inicial e consideraremos um mesmo alfabeto para o alfabeto de entrada e de saída.

Definição 3.3.2. Dizemos que dois autômatos $A_1 = (Q_1, \Sigma_1, f_1, l_1)$ e $A_2 = (Q_2, \Sigma_2, f_2, l_2)$ são equivalentes se eles definem a mesma aplicação. Em outras palavras, se existem bijeções $\theta : Q_1 \longrightarrow Q_2$ e $\phi : \Sigma_1 \longrightarrow \Sigma_2$ tais que

$$\theta(f_1(q_1, a_1)) = f_2(\theta(q_1), \phi(a_1))$$

e

$$\phi(l_1(q_1, a_1)) = l_2(\theta(q_1), \phi(a_1)).$$

Definição 3.3.3. Dizemos que um autômato A é *invertível* se cada função de estado é uma bijeção.

Se A é um autômato invertível, então seu inverso é o autômato A^{-1}, onde a correspondência $A^{-1} \longrightarrow A$ é a bijeção $q^{-1} \longmapsto q$ e

$$f_A(q,a) = p \qquad l_A(q,a) = b$$

se, e somente se,

$$f_{A^{-1}}(q^{-1},b) = p^{-1} \qquad l_{A^{-1}}(q^{-1},b) = a$$

Se tivermos o dígrafo de A podemos obter o dígrafo de A^{-1} trocando um estado $q \in A$ por $q^{-1} \in A^{-1}$ e invertendo a entrada e saída em cada aresta. Assim, na Figura 3.9, obtemos

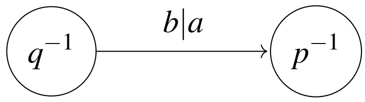


Figura 3.10 Transição de estados do autômato inverso

Um automorfismo $\beta \in \mathcal{A}_m$ possui uma interpretação como autômato, para tal, definimos $\Sigma = \Gamma = Y$, $Q = Q(\beta)$, $q_0 = \beta$, $f(\theta,y) = \theta_y$ e $l(\theta,y) = y^\theta$, onde Y é o alfabeto da árvore uni-raiz m-regular e $\theta \in Q(\beta)$.

Exemplo 3.3.4. Seja $\beta = (e,\beta)(0\,1)$ um automorfismo da árvore binária. Então $Y = \{0,1\}$, $Q(\beta) = \{\beta, e\}$

$$\begin{aligned} f(\beta,0) &= e & l(\beta,0) &= 1 \\ f(\beta,1) &= \beta & l(\beta,1) &= 0 \\ f(e,0) &= e & l(e,0) &= 0 \\ f(e,1) &= e & l(e,1) &= 1 \end{aligned}$$

e o dígrafo correspondente é

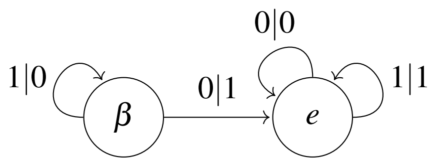


Figura 3.11 Autômato β

Por outro lado, cada estado de um autômato invertível $A = (Q,Y,f,l)$, onde $|Y| = m$, pode ser visto como um elemento de $\mathcal{A}_m$. Para tal, faremos a correspondência de um estado q com um automorfismo

$$\gamma_q = (\gamma_{q_0},\dots,\gamma_{q_{m-1}})\sigma_{\gamma_q}$$

onde $f(q,i) = q_i$ e $l(q,i) = j$ se, e somente se, $i^{\sigma_{\gamma_q}} = j$.

Deste modo, dado um autômato invertível A, podemos olhar seu conjunto de estados Q como um subconjunto de $\mathcal{A}_m$ e definir $\mathcal{G}(A) = \langle \gamma_q \mid q \in Q\rangle$ como o grupo gerado pelo autômato A.

3.4 Subgrupos de $\mathcal{A}_m$

A definição de produto entre automorfismos nos fornece propriedades importantes sobre Q, tais como

$$\begin{aligned} Q(\gamma^{-1}) &= Q(\gamma)^{-1} \\ Q(\gamma\beta) &\subseteq Q(\gamma)Q(\beta) \end{aligned}$$

para todo $\gamma,\beta \in \mathcal{A}_m$, onde $Q(\gamma)^{-1} = \{\gamma_u^{-1} \mid \gamma_u \in Q(\gamma)\}$.

Das observações acima, podemos concluir que o conjunto de automorfismos com número finito de estados $\mathcal{F}(Y)$ é um subgrupo de $\mathcal{A}_m$.

Definição 3.4.1. Dados G um subgrupo de $\mathcal{A}_m$ e n um inteiro não negativo, definimos o estabilizador em G no nível n como $Stab_G(n) = \{\gamma \in G \mid u^\gamma = u, \forall u \in \mathcal{M}(Y), |u| \leq n\}$.

Proposição 3.4.2. O conjunto $Stab_G(n)$ é um subgrupo normal de G, onde G é um grupo que age na árvore $\mathcal{T}_m$.

Demonstração. Sejam $\gamma,\beta \in Stab_G(n)$ e $g \in G$, então para todo $u \in \mathcal{M}$ onde $|u| = n$ segue que

$$u^{(\gamma\beta^{-1})} = (u^\gamma)^{\beta^{-1}} = u^{\beta^{-1}} = u,$$

donde concluímos que $Stab_G(n)$ é um subgrupo de G e

$$u^{(g\gamma g^{-1})} = ((u^g)^\gamma)^{g^{-1}} = (u^g)^{g^{-1}} = u^{(gg^{-1})} = u,$$

portanto, $g\alpha g^{-1} \in Stab_G(n)$. $\square$

A noção de estabilizador define um grupo de automorfismos cuja ação se inicia a partir de um nível n. Descreveremos agora grupos que a ação após o nível n é trivial.

Definição 3.4.3. Sejam G um grupo que age na árvore $\mathcal{T}_m$, $g \in G$ e n um nível dado. Definiremos o truncamento $g_{\leq n}$ de g no nível n como o elemento satisfazendo $(g_{\leq n})_u = g_u$ para todo $u \in \mathcal{M}$ com $|u| \leq k$, e $(g_{\leq n})_u = e$ caso $|u| > k$. Em outras palavras $g_{\leq n}$ é o elemento que possui a mesma ação de g até o nível n e depois deste nível age trivialmente.

Proposição 3.4.4. O conjunto $Trun_G(n) = \{g_{\leq n} \mid g \in G\}$ é um subgrupo de $\mathcal{A}_m$.

Demonstração. A quaisquer elementos $g_{\leq n}, h_{\leq n} \in Trun_G(n)$, estão associados $g,h \in G$, respectivamente. Como G é um grupo, então $gh^{-1} \in G$, portanto, $(gh^{-1})_{\leq n} \in Trun_G(n)$. Além disso, truncar a ação de dois elementos g e h^{-1} em um nível n e realizar a composição ou truncar a ação da composição gh^{-1} no nível n resulta o mesmo elemento, portanto,$(gh^{-1})_{\leq n} = g_{\leq n}(h^{-1})_{\leq n} \in Trun_G(n)$. Logo, $Trun_G(n) \leq \mathcal{A}_m$. □

A definição de truncamento de uma ação possibilita uma outra fatoração do grupo $\mathcal{A}_m$, a saber,

$$\mathcal{A}_m = Stab_{\mathcal{A}_m}(k+1)Trun_{\mathcal{A}_m}(k).$$

Definição 3.4.5. Dizemos que um elemento não trivial h de $\mathcal{A}_m$ tem profundidade k se $k+1$ é o menor inteiro tal que $h \in Trun_{\mathcal{A}_m}(k)$.

Em termos de ação, a profundidade de um elemento nos indica até que nível a ação de um elemento é não trivial. Então se $h \in Trun_{\mathcal{A}_m}(k)$, segue que $(uv)^h = u^h v$ para todos $u, v \in \mathcal{M}$ tal que $|u| = k$.

Outro tipo interessante de automorfismo são os que agem somente em uma subárvore. Descreveremos a seguir um procedimento para obter subgrupos de $\mathcal{A}_m$ que fixam todos os vértices fora de uma subárvore $u\mathcal{T}_m$, onde $u \in \mathcal{M}$. Seja H um grupo que age em $\mathcal{T}_m$, como $\mathcal{T}_m$ é isomorfa a sua subárvore $u\mathcal{T}_m$, podemos identificar uma ação de $h \in H$ em $\mathcal{T}_m$ com uma ação $u*h$ em $u\mathcal{T}_m$, e definir o grupo $u*H = \{u*h \mid h \in H\}$. Visualizando $u\mathcal{T}_m$ como subárvore de $\mathcal{T}_m$, segue que $u*H$ é um grupo que fixa todos os vértices fora de $u\mathcal{T}_m$. Em outras palavras, $u*H$ projeta as ações de H na subárvore $u\mathcal{T}_m$.

Exemplo 3.4.6. Seja $\langle\sigma\rangle$ o grupo cíclico de ordem 2. O grupo $10*\langle\sigma\rangle = \{10*e, 10*\sigma\}$ é o grupo que fixa todos os vértices fora da subárvore $10\mathcal{T}_2$. Representamos o elemento $10*e$ por $((e,e),(e,e))$ e $10*\sigma$ por $((e,e),(\sigma,e))$. Deste modo, projetamos a ação de $\langle\sigma\rangle$ para o vértice 10 dá árvore $\mathcal{T}_2$.

Definição 3.4.7. Definimos em $\mathcal{A}_2$ o grupo $\nu(H) = \langle u*H \mid u \in (\{00,10\}^*)\{01,11\}\rangle$, cujos elementos são produtos finitos de automorfismos, e que pode ser representado pela notação $\nu(H) = (\nu(H) \times H) \times (\nu(H) \times H)$.

O grupo em questão compõe uma das partes fundamentais para o desenvolvimento de um dos resultados principais do capítulo seguinte.

3.5 Funções de crescimento

A interpretação de um automorfismo com um autômato, que por sua vez é representado por meio de um dígrafo, permite explorar noções de funções associadas ao dígrafos. Motivado pelo artigo [14], iremos estudar funções de crescimento associado a um dígrafo e, através destes novos conceitos, definir novos subgrupos de $\mathcal{A}_m$.

Definição 3.5.1. Seja D um dígrafo, W uma propriedade de vértices e v um vértice fixado. Para um inteiro $k \geq 0$ fixado, o W-crescimento de D começando em v, denotado por $\theta(W;k,v)$, é o número de caminhos direcionados distintos de comprimento $k \geq 0$ que começam em v e terminam em um vértice com a propriedade W, relembrando que um caminho pode se auto-intersectar.

Dado um automorfismo $\gamma \in \mathcal{A}_m$, a questão em determinar todos os caminhos distintos de comprimento $k \geq 0$ se torna mais viável se interpretarmos o automorfismo através de uma árvore direcionada ao invés de seu dígrafo. Para o automorfismo $\gamma = (\gamma_0, \gamma_1)\sigma_\gamma$ da árvore binária, definimos a sua árvore de estados como a árvore direcionada

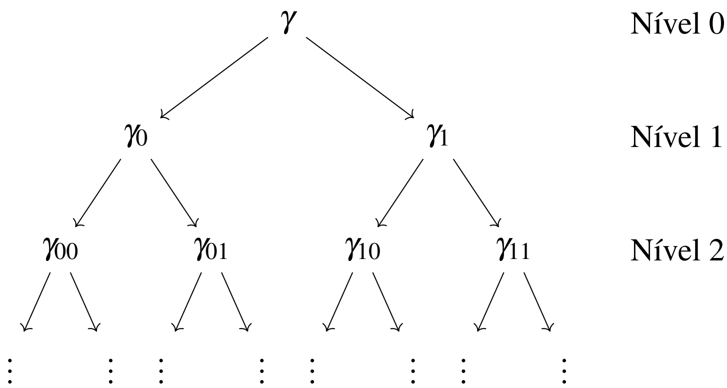


Figura 3.12 Árvore de estados

Esta representação é facilmente estendida para automorfismos em $\mathcal{A}_m$. Sob esta ótica, a questão de avaliar o número de caminhos distintos de comprimento k iniciando em γ e terminando em um vértice com a propriedade W é transladada em contar o número de vértices no nível k contendo a propriedade W.

Definição 3.5.2. Seja D o dígrafo do autômato que representa um automorfismo γ da árvore $\mathcal{T}_m$. Um vértice v deste dígrafo é denominado ativo caso o estado γ_v associado ao vértice v seja ativo, isto é, se a restrição $\sigma_{\gamma_v} = \gamma_v : Y \to Y$ age de forma não-trivial no primeiro nível da árvore.

Para a propriedade W: v possui W se v é ativo, simplificamos a notação da função de crescimento para

$$\theta(k,\gamma) = \#\{v \mid \sigma_{\gamma_v} \neq e, |v| = k\} \quad \text{para todo} \quad k \geq 0.$$

A condição $\sigma_{\gamma_v} \neq e$ é equivalente a $\gamma_v \notin Stab_{\mathcal{A}_m}(1)$. Mais geral, seja $\mathcal{H}$ um subgrupo de $\mathcal{A}_m$ e W a propriedade de que $\gamma_v \notin \mathcal{H}$. Em decorrência disto, podemos definir a função de crescimento

$$\theta_{\mathcal{H}}(k,\gamma) = \#\{v \mid \gamma_v \notin \mathcal{H}, |v| = k\} \quad \text{para todo} \quad k \geq 0$$

que mede a $\mathcal{H}$-inatividade de γ.

A função $\theta_{\mathcal{H}}(k,-) : \mathcal{A}_m \longrightarrow \mathbb{N}$ satisfaz as seguintes propriedades: para todo $\gamma, \beta \in \mathcal{A}_m$

(i) $\theta_{\mathcal{H}}(k,\gamma\beta) \leq \theta_{\mathcal{H}}(k,\gamma) + \theta_{\mathcal{H}}(k,\beta)$;

(ii) $\theta_{\mathcal{H}}(k,\gamma^{-1}) = \theta_{\mathcal{H}}(k,\gamma)$.

De fato, para (i), observe que $\{v \mid (\gamma\beta)_v \notin \mathcal{H}\} \subseteq \{v \mid (\gamma)_v \notin \mathcal{H}$ ou $(\beta)_v \notin \mathcal{H}\}$. Quanto a (ii), note que se $\gamma_v = \upsilon = (\upsilon_0, \ldots, \upsilon_m)\sigma_\upsilon$, então o seu inverso é o elemento descrito por $(\gamma_v)^{-1} = \upsilon^{-1} = ((\upsilon_{0^{\sigma_\upsilon^{-1}}})^{-1}, \ldots, (\upsilon_{(m-1)^{\sigma_\upsilon^{-1}}})^{-1})\sigma_\upsilon^{-1}$. Portanto, $\gamma_{vi} \notin \mathcal{H}$ sempre que $(\gamma_{(vi)^{\sigma_{\gamma_v}^{-1}}})^{-1} \notin \mathcal{H}$, isto fornece uma bijeção entre $\{v \mid \gamma_v \notin \mathcal{H}\}$ e $\{u \mid \gamma_u^{-1} \notin \mathcal{H}\}$, portanto, $\theta_{\mathcal{H}}(k,\gamma^{-1}) = \theta_{\mathcal{H}}(k,\gamma)$.

Seja **B** um subconjunto do conjunto de todas as funções de $\mathbb{N}$ em $\mathbb{N}$, onde **B** satisfaz as seguintes propriedades:

(i) a função nula $0 : \mathbb{N} \to \mathbb{N}$ definida por $n \mapsto 0$ pertence a **B**

(ii) para quaisquer $f, g \in \mathbf{B}$, existe $h \in \mathbf{B}$ tal que $f(n) + g(n) \leq h(n)$ para todo $n \in \mathbb{N}$.

Um exemplo dessa classe de funções,para um $n \geq 0$ fixado, é o conjunto de funções com crescimento k^n, definida por

$$\mathbf{P}_n = \{f \mid f(k) \leq ck^n \text{ para algum } c > 0\}.$$

De fato, observe que a função nula pertence a $\mathbf{P}_n$, pois $0(k) < c$ para todo $c > 0$. Além disso, se f e g são tais que $f(k) \leq c_1k^n$ e $g(k) \leq c_2k^n$, onde $c_1, c_2 > 0$, então para todo $c_3 \geq c_1 + c_2$, temos $f(k) + g(k) \leq c_3k^n = h(k) \in \mathbf{P}_n$.

Esta classe de funções de crescimento **B** permite limitar as funções de crescimento associadas a um automorfismo. Como consequência desta relação, temos a proposição a seguir.

Proposição 3.5.3. Sejam $\mathcal{H}$ um subgrupo de $\mathcal{A}_m$ e $\mathbf{B}$ um conjunto de funções com as propriedades acima. Então $\mathbf{B}(\mathcal{H}) = \{\gamma \in \mathcal{A}_m \mid \text{existe } b \in \mathbf{B} \text{ tal que } \theta_{\mathcal{H}}(k,\gamma) \leq b(k)\ \forall k > 0\}$ é um subgrupo de $\mathcal{A}_m$.

Demonstração. Sejam $\gamma, \beta \in \mathbf{B}(\mathcal{H})$ tais que $\theta_{\mathcal{H}}(k,\gamma) \leq b_\gamma(k)$ e $\theta_{\mathcal{H}}(k,\beta) \leq b_\beta(k)$. Por definição, existe $b \in \mathbf{B}$ satisfazendo $b_\gamma(k) + b_\beta(k) < b(k)$ para todo $k \geq 0$. Então

$$\theta_{\mathcal{H}}(k,\gamma\beta^{-1}) \leq \theta_{\mathcal{H}}(k,\gamma) + \theta_{\mathcal{H}}(k,\beta^{-1}) = \theta_{\mathcal{H}}(k,\gamma) + \theta_{\mathcal{H}}(k,\beta) \leq b_\gamma(k) + b_\beta(k) \leq b(k),$$

portanto, $\gamma\beta^{-1} \in \mathbf{B}(\mathcal{H})$. $\square$

Definição 3.5.4. Seja Y um conjunto finito, definimos por $\mathcal{F}_n(Y)$ o conjunto de automorfismos de estado-finito α cuja função de atividade $\theta(k,\alpha)$ pertence a $\mathbf{P}_n$.

Corolário 3.5.5. O conjunto $\mathcal{F}_n(Y)$ é um subgrupo de $\mathcal{F}(Y)$ para todo $n \geq 0$.

As noções de função de crescimento associadas a um automorfismos nos permite definir o conceito de automorfismos limitados.

Definição 3.5.6. Um automorfismo γ da árvore é dito limitado se sua função de crescimento $\theta(k,\gamma)$ é limitada, isto é, se $\theta(k,\gamma) \in \mathbf{P}_0$.

Iremos verificar que todos os elementos de $Trun_{\mathcal{A}_m}(n)$ são automorfismos limitados. Primeiro, observe que um automorfismo $\tau \in Trun_{\mathcal{A}_m}(n)$, visto por sua representação através de um dígrafo, possui um número de vértices não triviais finito. Além disso, partindo de τ, temos $|Y|$ possibilidades para iniciar o caminho, isto é, sair de τ para τ_y. Para um caminho de comprimento k, temos $|y|^k$ possibilidades para tomar um caminho. Perceba ainda que $\theta(k,\tau) = 0$ sempre que $k \geq n$, pois os vértices abaixo do nível n são inativos. Finalmente, o número de caminhos saindo de um vértice v terminando em um vértice ativo é finito, então $\theta(k,\tau) \leq |Y|^n$ para todo $k \geq 0$, isto é, $\theta(k,\tau) \in \mathbf{P}_0$.

Definição 3.5.7. Seja γ um automorfismo não trivial de estado finito. Dizemos que γ é circuitado se for limitado e γ pertence a um circuito em seu próprio dígrafo.

O exemplo a seguir se refere a um automorfismo circuitado da árvore binária que, posteriormente, será revisitado no Capítulo 4 e desempenha papel importante na construção deste trabalho.

Exemplo 3.5.8. Seja $\alpha = (e,(\alpha,e))\sigma$ um automorfismo de $\mathcal{A}_2$, onde σ é a transposição $(0\ \ 1)$. O dígrafo de α é dado por

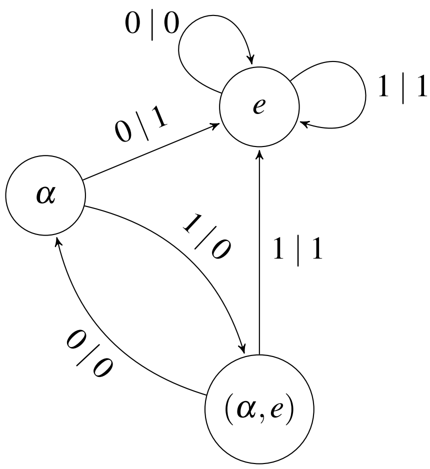


Figura 3.13 Dígrafo de α.

Note que α pertence a um circuito em seu próprio dígrafo. Além disso, os vértices de $\alpha = (e,(\alpha,e))\sigma$ com atividade são os vértices onde α aparece. Observando o dígrafo de α, vemos que para ir para um vértice ativo é necessário ir de α para (α,e) e depois retornar para α, ou seja, $\theta(2n,\alpha) = 1$ e $\theta(2n+1,\alpha) = 0$ para todo $n \geq 0$. Portanto, $\theta(k,\alpha) \in \mathbf{P}_0$, pois é limitada por 1.

Lema 3.5.9. Seja α o automorfismo do Exemplo 3.5.8. Então $\alpha_u = \alpha$ sempre que $u \in \{10\}^*$.

Demonstração. Observe que α pode ser desenvolvido da forma

$$\alpha = (e,(\alpha,e))\sigma = (e,((e,(\alpha,e))\sigma,e))\sigma,$$

e assim sucessivamente. Note que α aparece inicialmente na raiz $\emptyset$, depois aparece no vértice 10 em $(e,(\alpha,e))\sigma$, e no vértice 1010 em $(e,((e,(\alpha,e))\sigma,e))\sigma$. Através do dígrafo de α na Figura 3.13, é possível dizer em quais vértices o α aparece através dos circuitos iniciando e terminando em α. Por exemplo, através de um circuito de comprimento 2 é possível sair e retornar ao mesmo estado α, se coletarmos o alfabeto de entrada dos arcos, obtemos 1 do arco saindo de α e chegando em (α,e), e 0 do arco saindo de (α,e) e chegando em α, donde obtemos o vértice 10. Através deste procedimento, percebe-se que α irá aparecer nos vértices gerados pela palavra 10, isto é, nos vértices $u \in \{10\}^*$. Deste modo, $\alpha_u = \alpha$ sempre que $u \in \{10\}^*$ □

Para todo automorfismo circuitado γ está associado uma cadeia completa de índices $C(\gamma) = \{v \in \mathcal{M} \mid \gamma_v \text{ é circuitado}\}$. Mostraremos que existe um índice u de menor comprimento k tal que $\gamma_u = \gamma$, e este índice é único. De fato, suponha que existam dois índices u e v

de menor comprimento k tais que $\gamma_u = \gamma_v = \gamma$, então

$$\begin{aligned}
\theta(k,\gamma) &\geq \theta(0,\gamma_u) + \theta(0,\gamma_v) = 2\theta(0,\gamma) \\
\theta(2k,\gamma) &\geq \theta(k,\gamma) + \theta(k,\gamma) = 4\theta(0,\gamma) \\
&\vdots \\
\theta(xk,\gamma) &\geq \theta((x-1)k,\gamma) + \theta((x-1)k,\gamma) = 2^x\theta(0,\gamma)
\end{aligned}$$

Assim, α tem crescimento exponencial, o que é uma contradição, pois α é limitado.

Veremos abaixo que o m-circuito de um automorfismo circuitado α é preservado por multiplicação de elemento g de $Trun_{\mathcal{A}_m}(k)$. Antes disso, relembre que para um dígrafo D, o número $c(D)$ é o comprimento do maior circuito simples em D, de forma análoga, definiremos $c(\gamma)$ como o comprimento do maior circuito simples no dígrafo do automorfismo γ. Outra observação é se H é um subdígrafo de D, então todo circuito de H é também um circuito de D, consequentemente, $c(H) \leq c(D)$.

Iremos exemplificar o que acontece com um automorfismo circuitado quando multiplicado com um elemento de $Trun_{\mathcal{A}_m}(k)$. Em seguida, verificaremos a validade para o caso geral.

Exemplo 3.5.10. Sejam $\alpha = (e,(\alpha,e))\sigma$ e $g = (e,(\sigma,\sigma)) \in Trun_{\mathcal{A}_m}(2)$. Então temos que $\alpha g = (e,(\alpha\sigma,\sigma))\sigma = (e,((e,(\alpha,e)),\sigma))\sigma$ e seu dígrafo é dado por

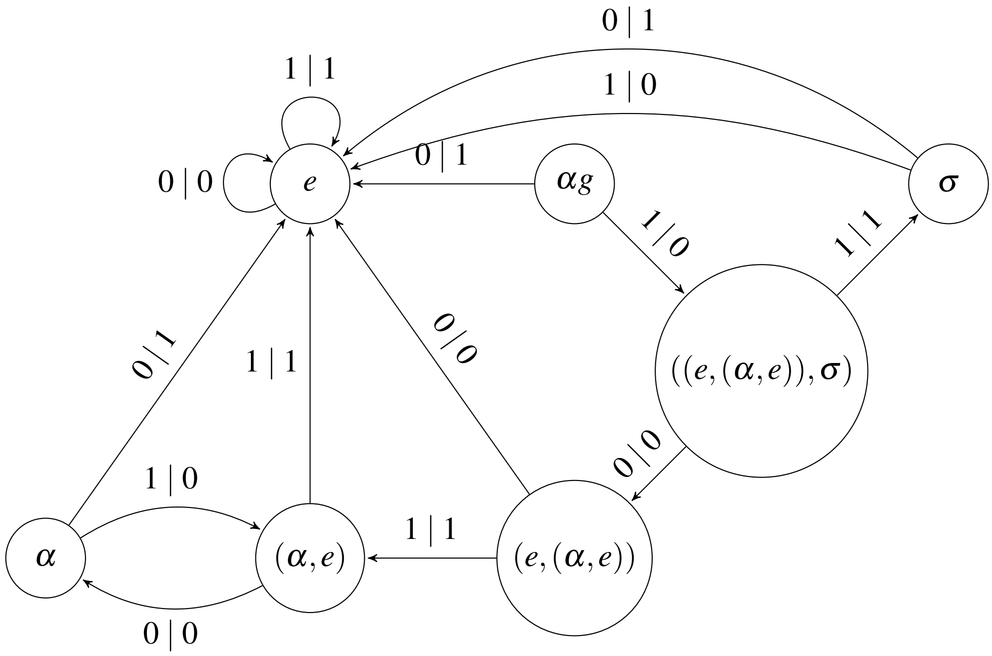


Figura 3.14 Dígrafo de αg.

O automorfismo α tem um 2-circuito, isto é, $c(\alpha) = 2$. Através do dígrafo de αg é fácil observar que $c(\alpha g) = 2$. Isto se dá pois, a partir de um indice $u \in C(\alpha)$ onde $u > 2$, é possivel chegar no estado α de αg, a saber, $u = 1010$, temos $(\alpha g)_{1010} = \alpha$.

Lema 3.5.11. Se γ é um automorfismo circuitado com $c(\gamma) > 0$ e $g \in Trun_{\mathcal{A}_m}(k)$, então $c(\gamma) = c(\gamma g)$

Demonstração. Sejam $\beta = \gamma g$ e $v \in C(\gamma)$ um índice de comprimento maior que k tal que $\gamma_v = \gamma$. Então $\beta_v = (\gamma g)_v = \gamma_v = \gamma$, assim, $c(\beta) \geq c(\gamma_v) = c(\gamma)$, pois γ é subdígrafo de β.

Mostraremos agora que $c(\beta) > c(\gamma)$ não pode ocorrer. Com efeito, suponha por contradição que $c(\beta) > c(\gamma)$, então existe um índice $u \in C(\beta)$ tal que $\beta_u = (\gamma g)_u = \gamma_u g_{u^\gamma}$ é circuitado e tem o maior comprimento dentre os circuitos simples de β, isto é, $c(\beta) = c(\beta_u)$. Observe que g_{u^γ} é trivial, caso contrário, g_{u^γ} é um vértice de g que aparece infinitas vezes no produto γg, consequentemente, aparece infinitas vezes como vértice de g, um absurdo pois $g \in Trun_{\mathcal{A}_m}(k)$. Então, $\beta_u = \gamma_u$ é o circuito simples de maior comprimento de β e está inteiramente contido em γ. Portanto, $c(\gamma) = c(\beta)$. $\square$

O resultado a seguir relaciona um conjunto especial de automorfismos circuitados ao grupo de automorfismos limitados de estado finito.

Teorema 3.5.12. O conjunto $\mathcal{F}_{0,m}(Y) = \{\alpha \in \mathcal{F}_0(Y) \mid c(\alpha) = 0 \text{ ou } c(\alpha) \text{ divide } m\}$ é um subgrupo de $\mathcal{F}_0(Y)$.

Demonstração. Inicialmente, perceba que os automorfismos de estado finito cujo dígrafo possui 0-circuito estão em $Trun_{\mathcal{A}_m}(k)$ para todo $k \geq 0$. De fato, se γ é um automorfismo do tipo 0-circuito, então não existe nenhum circuito em γ, ou equivalentemente, não existem $u, v \in \mathcal{T}_m$ tais que $\gamma_{uv} = \gamma_u$. Além disso, note que os conjuntos de estados $Q(\gamma_{uv})$ e $Q(\gamma_u)$ irão coincidir sempre que $\gamma_{uv} = \gamma_u$. Se não existe $k > 0$ tal que $\gamma \in Trun_{\mathcal{A}_m}(k)$, então γ tem infinitos vértices não triviais, além disso, todo vértice não trivial satisfaz $\gamma_{uv} \neq \gamma_u$ para todos $u, v \in \mathcal{T}_m$, consequentemente, temos infinitos estados.

Já os automorfismso com m-circuito para $m \geq 1$ são automorfismos circuitados ou o produto de um automorfismo circuitado com um elemento de $g \in Trun_{\mathcal{A}_m}(k)$ para algum $k > 0$.

Se $\gamma, \beta \in Trun_{\mathcal{A}_m}(k)$, então $\gamma\beta^{-1} \in Trun_{\mathcal{A}_m}(k)$, pois $Trun_{\mathcal{A}_m}(k)$ é subgrupo, além disso, $c(\gamma\beta^{-1}) = 0$, como observado acima.

Se γ é um automorfismo circuitado com $c(\gamma) = m \geq 1$ e $\beta \in Trun_{\mathcal{A}_m}(k)$, então o Lema 3.5.11 afirma que $c(\gamma) = c(\gamma\beta^{-1}) = m$

A seguir, iremos provar que para cada automorfismo circuitado γ e β temos que

$$c(\gamma\beta^{-1}) \mid \mathrm{m.m.c}(c(\gamma), c(\beta^{-1})).$$

Seja $\xi = \gamma\beta^{-1}$. Então, $\xi_v = \gamma_v(\beta^{-1})_{v'}$, onde $v^\gamma = v'$. Veremos que o tipo de circuito de ξ_v é $c(\xi_v) = 0$, $c(\gamma_v)$ ou $c(\beta_{v'})$, a menos possivelmente quando $v \in C(\gamma)$ e $v' \in C(\beta)$.

Se $v \in C(\gamma)$ e $v' \notin C(\beta^{-1})$ então $\xi_v = \gamma_v g$, onde $g \in Trun_{\mathcal{A}_m}(k)$. Neste caso, $c(\xi) = c(\gamma_v)$.

Se $v \notin C(\gamma)$ e $v' \in C(\beta^{-1})$ então $\xi_v = g(\beta^{-1})_{v'}$, onde $g \in Trun_{\mathcal{A}_m}(k)$. Neste caso, $c(\xi) = c((\beta^{-1})_{v'})$.

Assuma que $v' \in C(\beta^{-1})$ e $v \in C(\gamma)$. Sejam $c(\gamma) = a$, $c(\beta^{-1}) = b$, $l = \mathrm{m.m.c}(a,b)$, $a' = \dfrac{l}{a}$ e $b' = \dfrac{l}{b}$. Além disso, sejam $u \in C(\gamma)$ de comprimento a, $w \in C(\beta^{-1})$ de comprimento b e $v = u^{a'}$. Então, $\xi_v = \gamma_v\beta_{v'}$, onde $v' = w^{b'}$. Assim, $\xi_v = \gamma\beta = \xi$, do que decorre que $c(\xi)$ divide l.

Considere $m = ql + r$, onde $0 \leq r < l$. Como $a \mid m$ e $a \mid l$ segue que $a \mid r$, similarmente, $b \mid m$ e $b \mid l$, logo $b \mid r$. Assim r é múltiplo comum de a e b, mas $r < l$, então $r = 0$, donde concluímos que $l \mid m$.

Logo, $c(\gamma\beta^{-1}) \mid m$, portanto, $\gamma\beta^{-1} \in \mathcal{F}_{0,m}(Y)$.

$\square$

CAPÍTULO 4

O produto tree-wreath

O grupo de automorfismos da árvore binária é extremamente grande no sentido de abrigar representações de uma infinidade de grupos. Nosso objetivo principal consiste em obter uma representação fiel do grupo metabeliano livre de posto r como um grupo de automorfismos de estado-finito. Para este fim, iremos explorar os resultados em [3], que representam o núcleo deste trabalho. No artigo supracitado, Brunner e Sidki definem uma operação sobre os grupos de automorfismos que agem na árvore binária, denominada *tree-wreathing*. Iremos explorar as propriedades dessa operação e, posteriormente, utiliza-lá como ferramenta para atingir o objetivo citado.

4.1 O operador translação

Definiremos o automorfismo α da árvore binária por $\alpha = (e,(\alpha,e))\sigma$, onde σ é a transposição $(0\ 1)$. Este automorfismo foi utilizado anteriormente em alguns exemplos com a finalidade de promover uma melhor familiarização. O automorfismo α é um dos elementos que compõem a operação *tree-wreath* que definiremos posteriormente e o chamaremos de operador translação.

Neste momento, iremos explorar um pouco da estrutura de α. Inicialmente, observe que

$$\begin{aligned}
\alpha^2 =& \alpha\alpha \\
=& (e,(\alpha,e))\sigma(e,(\alpha,e))\sigma \\
=& (e,(\alpha,e))\sigma(e,(\alpha,e))\sigma^{-1}\sigma\sigma \\
=& (e,(\alpha,e))(e,(\alpha,e))^{\sigma^{-1}} \\
=& (e,(\alpha,e))((\alpha,e),e) \\
=& ((\alpha,e),(\alpha,e)),
\end{aligned}$$

e

$$\alpha^3 = \alpha^2\alpha = ((\alpha,e),(\alpha,e))(e,(\alpha,e))\sigma = ((\alpha,e),(\alpha^2,e))\sigma.$$

Isto sugere a proposição a seguir que caracteriza as potências de α.

Proposição 4.1.1. O operador translação definido anteriomente satisfaz as seguintes relações:

(i) $\alpha^{2i} = ((\alpha^i,e),(\alpha^i,e))$;

(ii) $\alpha^{2i+1} = ((\alpha^i,e),(\alpha^{i+1},e))\sigma$,

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

Demonstração. De fato, por indução em $i \geq 0$:

O resultado segue trivialmente para $i = 0$. Por hipótese de indução, suponha que a relação é válida para $i \geq 0$, mostraremos que é válida para $i+1$.

$$\alpha^{2(i+1)} = \alpha^{2i}\alpha^2 = ((\alpha^i,e),(\alpha^i,e))((\alpha,e),(\alpha,e)) = ((\alpha^{i+1},e),(\alpha^{i+1},e)).$$

Para $i \leq 0$ segue que

$$\alpha^{2i} = (\alpha^{-2i})^{-1} = ((\alpha^{-i},e),(\alpha^{-i},e))^{-1} = ((\alpha^i,e),(\alpha^i,e)).$$

Para o caso ímpar temos

$$\alpha^{2i+1} = \alpha^{2i}\alpha^1 = ((\alpha^i,e),(\alpha^i,e))(e,(\alpha,e))\sigma = ((\alpha^i,e),(\alpha^{i+1},e))\sigma.$$

□

Verificaremos que uma consequência imediata da proposição anterior é que α tem ordem infinita. Com efeito, note que α é não trivial pois σ age no primeiro nível da árvore binária. Assuma por hipótese de indução que α^n é não trivial. Se n é par então $\alpha^{n+1} = \alpha^n\alpha = ((\alpha^{\frac{n}{2}},e),(\alpha^{\frac{n}{2}+1},e))\sigma$ é não trivial, pois possui σ que é não trivial. Agora, se n é ímpar, então $\alpha^{n+1} = ((\alpha^{\frac{n+1}{2}},e),(\alpha^{\frac{n+1}{2}},e))$ é não trivial, pois a ação de $\alpha^{\frac{n+1}{2}}$ é não trivial por hipótese de indução. Portanto, segue que $\langle\alpha\rangle \simeq \mathbb{Z}$.

Observação 4.1.2. Pela caracterização de α^{2i}, segue que α^{2^s} produz entradas $\alpha^{2^{s-1}}$ no nível 2, $\alpha^{2^{s-1}}$ produz entradas $\alpha^{2^{s-2}}$ no nível 4 e assim sucessivamente. Isto posto, concluímos que α^{2^s} produz entradas α no nível $2s$ e, portanto, sua ação se inicia no nível $2s+1$.

4.2 Copiando subgrupos

Seja H um subgrupo que age na árvore binária. Queremos construir uma cópia $\widetilde{H}$ de H que seja compatível com a translação α, no sentido que $\widetilde{H}$ deva comutar com todos (ou o máximo possível) com seus conjugados por elementos de $\langle\alpha\rangle$.

Para cada $h \in H$ defina o automorfismo $\tilde{h}$ da árvore recursivamente como $\tilde{h} = ((\tilde{h}, h), e)$, então $\widetilde{H} = \{\tilde{h} \mid h \in H\}$ e $\widetilde{H} \simeq H$. Observe que o elemento $\tilde{h}$ projeta a ação de h em infinitos vértices da árvore binária, neste sentido, quando h é não trivial, $\tilde{h}$ age em infinitas sub-árvores. Este último fato motiva a definição a seguir.

Definição 4.2.1. Dizemos que um automorfismo γ de $\mathcal{T}_2$ tem suporte finito se age de forma não trivial em um número finito de sub-árvores de $\mathcal{T}_2$, caso contrário, diremos que γ tem suporte infinito.

O próximo passo é estudar a ação dos elementos de $\langle\alpha\rangle$ em $\widetilde{H}$. Uma potência par de α tem ação

$$\begin{aligned}\tilde{h}^{\alpha^{2i}} &= ((\alpha^{-i}, e), (\alpha^{-i}, e))((\tilde{h}, h), e)((\alpha^{i}, e), (\alpha^{i}, e))\\ &= ((\alpha^{-i}\tilde{h}\alpha^{i}, h), e)\\ &= ((\tilde{h}^{\alpha^{i}}, h), e),\end{aligned}$$

já uma potência ímpar age da forma

$$\begin{aligned}\tilde{h}^{\alpha^{2i+1}} &= (\tilde{h}^{\alpha^{2i}})^{\alpha}\\ &= ((\tilde{h}^{\alpha^{i}}, h), e)^{\alpha}\\ &= \sigma(e, (\alpha^{-1}, e))((\tilde{h}^{\alpha^{i}}, h), e)(e, (\alpha, e))\sigma\\ &= \sigma((\tilde{h}^{\alpha^{i}}, h), e)\sigma\\ &= (e, (\tilde{h}^{\alpha^{i}}, h)).\end{aligned}$$

Observe que α recebe o nome de operador translação justamente por sua ação transladar a ação de h nas árvores. Outra fato interessante é que

$$[\tilde{h}^{\alpha^{2i}}, \tilde{k}^{\alpha^{2j+1}}] = ((\tilde{h}^{-\alpha^{i}}, h^{-1}), e)(e, (\tilde{k}^{-\alpha^{j}}, k^{-1}))((\tilde{h}^{\alpha^{i}}, h), e)(e, (\tilde{k}^{\alpha^{j}}, k)) = ((e, e), (e, e)),$$

isto é, dois elementos de $\widetilde{H}$ conjugados por potências de α com paridades distintas comutam.

4.3 O produto tree-wreath $H \,\bar{\wr}\, \mathbb{Z}$

Nesta seção iremos enunciar a operação *tree-wreathing*, definida em [3], para os grupos H e $\langle\alpha\rangle$, onde H é um grupo que age na árvore binária e α é o operador translação.

Definição 4.3.1. Seja G o grupo gerado por $\widetilde{H}$ e α. Dizemos que G um produto *tree-wreath* de $\widetilde{H}$ pelo grupo cíclico infinto gerado por α e usamos a notação $G = H \,\bar{\wr}\, \mathbb{Z}$.

O termo *tree-wreath* pode ser traduzido por *entrelaçado na árvore*, a motivação para utilização desse termo provém de uma relação entre os produtos *tree-wreath* e o produto entrelaçado, assim sendo, deste modo, podemos nos remeter ao produto *tree-wreath* como uma operação entrelaçada na árvore binária. Entretanto, iremos manter o termo original. Como requisito para compreender a relação em questão, definiremos um grupo no lema a seguir.

Lema 4.3.2. Defina $N_0 = \{e\}$ e $N_s = \langle [\widetilde{H}^{\alpha^i}, \widetilde{H}^{\alpha^j}] \mid 0 \leq i < j < 2^{s+1}$ e $j - i \leq 2^s\rangle$ para todo inteiro $s \geq 1$. Então

(i) $N_s = \langle u * H' \mid u \in (\{00,10\}^*)\{01,11\}$ e $|u| \leq 2s\rangle = (N_{s-1} \times H') \times (N_{s-1} \times H')$, isto é, um elemento $n_s \in N_s$ é um automorfismo que age na árvore binária descrito por $((n_1,h'),(n_2,k'))$, onde $n_1, n_2 \in N_{s-1}$ e $h', k' \in H'$;

(ii) $[N_s, \alpha^{2^s}] = e$;

(iii) $N_s \lhd G$.

Demonstração. Para simplificar a notação, escreveremos $H_i = \widetilde{H}^{\alpha^i}$ e $H_{i,j} = [H_i, H_j]$. A demonstração será realizada via indução em $s \geq 1$.

Para $s = 1$, os índices i e j de $H_{i,j}$ satisfazem $0 \leq i < j < 4$ e $j - i \leq 2$, portanto, $N_1 = \langle H_{0,1}, H_{0,2}, H_{1,2}, H_{1,3}, H_{2,3}\rangle$. Como $[\tilde{h}^{\alpha^{2i}}, \tilde{k}^{\alpha^{2j+1}}] = e$, segue que $H_{i,j} = \{e\}$ sempre que i e j têm paridades distintas, assim $N_1 = \langle H_{0,2}, H_{1,3}\rangle$. Determinaremos agora $H_{0,2}$ e $H_{1,3}$. Sejam $h, k \in H$. Então

$$\begin{aligned}
[\tilde{h}, \tilde{k}^{\alpha^2}] &= \tilde{h}^{-1}\tilde{k}^{-\alpha^2}\tilde{h}\tilde{k}^{\alpha^2} \\
&= ((\tilde{h}^{-1}, h^{-1}), e)((\tilde{k}^{-\alpha}, \tilde{k}^{-1}), e)((\tilde{h}, h), e)((\tilde{k}^{\alpha}, \tilde{k}), e) \\
&= (([\tilde{h}, \tilde{k}^{\alpha}], [h,k]), e) \\
&= ((e, [h,k]), e) \\
&= 01 * [h,k]
\end{aligned}$$

e

$$
\begin{aligned}
[\tilde{h}^{\alpha}, \tilde{k}^{\alpha^3}] =& \tilde{h}^{-\alpha}\tilde{k}^{-\alpha^3}\tilde{h}^{\alpha}\tilde{k}^{\alpha^3}\\
=&(e,(\tilde{h}^{-1},h^{-1}))(e,(\tilde{k}^{-\alpha},\tilde{k}^{-1}))(e,(\tilde{h},h))(e,(\tilde{k}^{\alpha},\tilde{k}))\\
=&(e,([\tilde{h},\tilde{k}^{\alpha}],[h,k]))\\
=&(e,(e,[h,k]))\\
=&(11)*[h,k].
\end{aligned}
$$

Consequentemente, temos as expressões $H_{0,2} = (\{e\}\times H')\times(\{e\}\times\{e\}) = (01)*H'$ e $H_{1,3} = (\{e\}\times\{e\})\times(\{e\}\times\{H'\}) = (11)*H'$, da qual extraímos a caracterização $N_1 = (\{e\}\times H')\times(\{e\}\times\{e\}) = \langle (01)*H', (11)*H'\rangle$.

Na verdade, note que

$$
[\tilde{h}^{\alpha}, \tilde{k}^{\alpha^3}] = [\tilde{h}, \tilde{k}^{\alpha^2}]^{\alpha} = (01*[h,k])^{\alpha} = (01)^{(e,(\alpha,e))\sigma}*[h,k] = 0^{\sigma}1^{e}*[h,k] = 11*[h,k],
$$

isto nos sugere avaliar a ação das potências de α para evitar contas desnecessárias.

Agora, verificaremos que α^2 centraliza N_1. Sejam $h',k'\in H'$ e $n = ((e,h'),(e,k'))$. Então

$$
\begin{aligned}
[n,\alpha^2] =& [((e,h'),(e,k')),((\alpha,e),(\alpha,e))]\\
=&((e,(h')^{-1}),(e,(k')^{-1}))((\alpha^{-1},e),(\alpha^{-1},e))((e,h'),(e,k'))((\alpha,e),(\alpha,e))\\
=&((e,e),(e,e)),
\end{aligned}
$$

o que resulta em $[N_1,\alpha^2] = \{e\}$.

Mostraremos que $N_1 \lhd G$. Para tal, basta avaliar as conjugações dos elementos de N_1 pelos geradores de G, a saber, $\tilde{h}\in\widetilde{H}$ e α. Seja $n = ((e,[x,y]),(e,[z,w]))\in N_1$. Então

$$
\begin{aligned}
\tilde{h}^{-1}n\tilde{h} =& ((\tilde{h}^{-1},h^{-1}),e)((e,[x,y]),(e,[z,w]))((\tilde{h},h),e)\\
=&((e,h^{-1}[x,y]h),(e,[z,w]))\\
=&((e,[h^{-1}xh,h^{-1}yh]),(e,[z,w]))\in N_1
\end{aligned}
$$

e

$$
\begin{aligned}
\alpha^{-1}n\alpha =& \sigma(e,(\alpha^{-1},e))((e,[x,y]),(e,[z,w]))(e,(\alpha,e))\sigma\\
=&((\alpha^{-1},e),e)((e,[z,w]),(e,[x,y]))((\alpha,e),e)\\
=&((e,[z,w]),(e,[x,y]))\in N_1
\end{aligned}
$$

assim, $N_1 \lhd G$.

Uma vez demonstrada a base de indução, iremos assumir por hipótese de indução que $N_{s-1} = (N_{s-1} \times H') \times (N_{s-1} \times H') = \langle u * H' \mid u \in (\{00,10\}^*)\{01,11\} \text{ e } |u| \leq 2(s-1)\rangle$, $[N_{s-1}, \alpha^{2^{s-1}}] = e$ e $N_{s-1} \lhd G$ para todo $s \geq 2$ fixado.

Veremos que para determinar N_s é necessário apenas calcular $[H_0, H_{2^s}]$ e avaliar as ações das potências de α em $[H_0, H_{2^s}]$. Em primeiro lugar, observe que se $H_{i,j} \in N_s$, então $H_{i,j} = [H_i, H_j] = [H_0, H_{j-i}]^{\alpha^i}$. Além disso, se $j-i$ for ímpar, então $H_{i,j} = H_{0,j-i}^{\alpha^i} = e$, portanto, consideraremos apenas os valores tais que $j-i$ é par. Seja $j-i = 2^r m$, onde $r \geq 1$ e m é ímpar. Então para quaisquer $h,k \in H$ temos

$$\begin{aligned}
[\tilde{h}, \tilde{k}^{\alpha^{2^r m}}] &= [((\tilde{h},h),e),((\tilde{k}^{\alpha^{2^{r-1}m}},k),e)] \\
&= (([\tilde{h}, \tilde{k}^{\alpha^{2^{r-1}m}}],[h,k]),e) \\
&\ \ \vdots \\
&= (((((([\tilde{h},\tilde{k}^{\alpha^m}],[h,k]),e),\ldots),[h,k]),e) \\
&= (((((e,[h,k]),e),\ldots),[h,k]),e) \\
&= ((0^{2r-1}1)*[h,k])\ldots((0^3 1)*[h,k])((01)*[h,k]),
\end{aligned}$$

ou seja, $[H_0, H_{2^r m}] = [H_0, H_{2^r}]$, donde concluímos que é suficiente avaliar o caso $j-i = 2^r$, onde $1 \leq r \leq s$. O próximo passo será averiguar que $H_{i,2^r+i} \in N_r$ para todo i tal que $2^r + i < 2^{s+1}$. Com efeito, seja $i = \delta_1 + 2\delta_2 + \cdots + 2^t \delta_t$, onde $\delta_l \in \{0,1\}$ para todo $1 \leq l \leq t$ e $2^r + i < 2^{s+1}$, como α^{2^l} possui ação apenas no nível $2l+1$, obtemos a relação $[H_0, H_{2^r}]^{\alpha^i} = [H_0, H_{2^r}]^{\alpha^{\delta_1 + 2\delta_2 + \cdots + 2^{r-1}\delta_{r-1}}} \in N_r$. Com as observações anteriores, para determinar $N_s \backslash N_{s-1}$, basta considerar o caso $j-i = 2^s$, isto é, calcular $[H_0, H_{2^s}]$ e avaliar as ações de α^n em $H_{0,2^s}$. Seja $n = \delta_1 + 2\delta_2 + \cdots + 2^{s-1}\delta_s$, onde $\delta_l \in \{0,1\}$ para todo $1 \leq l \leq s-1$, temos 2^s possibilidades para tomar n e, para n_1 e n_2 distintos tomados entre as possibilidades, temos $[H_{n_1}, H_{n_1+2^s}] \neq [H_{n_2}, H_{n_2+2^s}]$, visto que α^{n_1} e α^{n_2} possuem ações distintas em $[H_0, H_{2^s}]$.

Dado $c \in [H_0, H_{2^s}]$ segue que $c = (01)*h'(0^3 1)*h'\ldots(0^{2s-3}1)*h'(0^{2s-1}1)*h'$, mas $d = (01)*h'(0^3 1)*h'\ldots(0^{2s-3}1)*h' \in N_{s-1} \subset N_s$, logo $cd^{-1} = (0^{2s-1}1)*h'$. Deste modo, produzimos $0^{2s-1}1 * H'$ em N_s. Como $c^{\alpha^{2^k}} \in [H_{2^k}, H_{2^s+2^k}]$, onde $k < s$, então $c^{\alpha^{2^k}}$ possui $(0^{2p}10^{2s-2p-2}1)*h'$ como um fator, deste modo, tomando $d^{\alpha^{2^k}}$ produzimos o elemento $c^{\alpha^{2^k}}(d^{\alpha^{2^k}})^{-1} = (0^{2k}10^{2s-2k-2}1)*h'$, donde concluímos que $(0^{2k}10^{2s-2k-2}1)*H' \subset N_s$. As potências de α agem transpondo os elementos de posição ímpar em $0^{2s-1}1$, dessa forma, conjugando c sucessivas vezes por α^{2^i}, com i distinto das conjugações anteriores, produzimos $u \in (\{00,10\}^*)\{01,11\}$ e $|u| = 2s$. Consequentemente, produzimos $u*H'$ onde

$u \in (\{00,10\}^*)\{01,11\}$ e $|u| = 2s$ em N_s, ou seja,

$$N_s = (N_{s-1} \times H') \times (N_{s-1} \times H') = \langle u * H' \mid u \in (\{00,10\}^*)\{01,11\} \text{ e } |u| \leq 2s\rangle.$$

Neste momento, nos atentaremos agora a questão de mostrar que $N_s \lhd G$. Seja $n_s \in N_s$. Então $n_s = ((n_{s-1},[x,y]),(m_{s-1},[z,w]))$, onde $n_{s-1}, m_{s-1} \in N_{s-1}$ e $x,y,z,w \in H$, assim

$$\begin{aligned}\tilde{h}^{-1} n_s \tilde{h} =& ((\tilde{h}^{-1},h^{-1}),e)((n_{s-1},[x,y]),(m_{s-1},[z,w]))((\tilde{h},h),e)\\ =& ((\tilde{h}^{-1} n_{s-1}\tilde{h}, h^{-1}[x,y]h),(m_{s-1},[z,w]))\\ =& ((n_{s-1}^{\tilde{h}},[x^h,y^h]),(m_{s-1},[z,w])) \in N_s\end{aligned}$$

e

$$\begin{aligned}\alpha^{-1} n_s \alpha =& \sigma(e,(\alpha^{-1},e))((n_{s-1},[x,y]),(m_{s-1},[z,w]))(e,(\alpha,e))\sigma\\ =& ((\alpha^{-1},e),e)((m_{s-1},[z,w]),(n_{s-1},[x,y]))((\alpha,e),e)\\ =& ((\alpha^{-1}m_{s-1}\alpha,[z,w]),(n_{s-1},[x,y])) \in N_s\end{aligned}$$

pois de $N_{s-1} \lhd G$ segue que $n_{s-1}^{\tilde{h}}, n_{s-1}^{-\alpha}, m_{s-1}^{\alpha} \in N_{s-1}$. Assim,$N_s \lhd G$.

Finalmente, $[N_s, \alpha^{2^s}] = \{e\}$, pois

$$\begin{aligned}[n_s,\alpha^{2^s}] =& [((n_{s-1},[x,y]),(m_{s-1},[z,w])),((\alpha^{2^{s-1}},e),(\alpha^{2^{s-1}},e))]\\ =& (([n_{s-1},\alpha^{2^{s-1}}],[[x,y],e]),([m_{s-1},\alpha^{2^{s-1}}],[[z,w],e]))\\ =& ((e,e),(e,e))\end{aligned}$$

uma vez que, por hipótese de indução, $[N_{s-1},\alpha^{2^{s-1}}] = \{e\}$. □

O teorema a seguir está entre os resultados de maior importância do capítulo. Iremos abordar algumas propriedades do produto *tree-wreath* $H \,\bar{\wr}\, \mathbb{Z}$ e descrever a relação entre o produto entrelaçado e o produto *tree-wreath*.

Teorema 4.3.3. Seja G o produto tree-wreath $H \,\bar{\wr}\, \mathbb{Z}$ definido acima. Então G satisfaz as seguintes propriedades:

(I) o subgrupo
$$N = \langle [\widetilde{H}^{\alpha^i}, \widetilde{H}^{\alpha^j}] | 0 \leq i < j\rangle$$
é normal em G e pode ser expresso através de suas ações sobre a árvore na forma $N = \nu(H') = (N \times H') \times (N \times H') = \langle u * H' \mid u \in (\{00,10\}^*)\{01,11\}\rangle$;

(II) o grupo quociente G/N é isomorfo ao produto entrelaçado restrito $H \wr \mathbb{Z}$;

(III) o subgrupo de G gerado por $(0^{2m-1}1) * H'$ e α possui um subgrupo em seu centro cujo quociente é isomorfo a $H' \wr \mathbb{Z}/2^m\mathbb{Z}$;

(IV) se J é um subgrupo de H, então $\langle \widetilde{J}, \alpha \rangle$, considerado como um subgrupo de $G = H \mathbin{\bar{\wr}} \mathbb{Z}$, é isomorfo a $J \mathbin{\bar{\wr}} \mathbb{Z}$, além disso, se J é abeliano, então $J \mathbin{\bar{\wr}} \mathbb{Z} \simeq J \wr \mathbb{Z}$;

(V) o grupo G é de estado-finito (é solúvel, livre de torção) se, e somente se, H é de estado-finito (é solúvel, livre de torção).

Demonstração. (I) Sejam $H_i = \widetilde{H}^{\alpha^i}$ e $H_{i,j} = [\widetilde{H}^{\alpha^i}, \widetilde{H}^{\alpha^j}] = [H_i, H_j]$ para todo $0 \leq i < j$. Além disso, defina $N = \langle H_{i,j} \mid 0 \leq i < j \rangle$. Observe que $N = \bigcup N_s$ é o grupo apresentado na Definição 3.4.7, onde N_s é o subgrupo definido no Lema 4.3.2, então $N = (N \times H') \times (N \times H')$. Além disso, N é normal em G, caso contrário, existiria um $s \in \mathbb{N}$ tal que N_s não é normal em G, o que não ocorre. $\square$

Demonstração. (II) Mostraremos agora que G/N é isomorfo a $H \wr \mathbb{Z}$.

Os elementos do conjunto de representantes de das classes laterais de N em G podem ser tomados como expressões da forma

$$w = (\tilde{h}_1^{\alpha^{2i_1}} \ldots \tilde{h}_s^{\alpha^{2i_s}})(\tilde{k}_1^{\alpha^{j_1+1}} \ldots \tilde{k}_t^{\alpha^{j_t+1}})\alpha^m$$

com inteiros $i_1, ..., i_s$ distintos e inteiros $j_1, ..., j_t$ distintos e $m = 2m' + \varepsilon$ onde $\varepsilon \in \{0, 1\}$. Com efeito, suponha que $i_p = i_q$ e se $p < r \neq s < q$ tem-se $i_r \neq i_s$, então

$$\begin{aligned}
\tilde{h}_p^{\alpha^{i_p}} \tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{i_{q-1}}} \tilde{h}_q^{\alpha^{i_q}} \alpha^m &= \tilde{h}_p^{\alpha^{i_p}} \tilde{h}_q^{\alpha^{i_q}} \tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{i_{q-1}}} [\tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{2i_{q-1}}}, \tilde{h}_q^{\alpha^{i_q}}] \alpha^m \\
&= \tilde{h}_p^{\alpha^{i_p}} \tilde{h}_q^{\alpha^{i_q}} \tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{i_{q-1}}} [\tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{2i_{q-1}}}, \tilde{h}_q^{\alpha^{i_q}}] \alpha^m \\
&= \tilde{h}_p^{\alpha^{i_p}} \tilde{h}_q^{\alpha^{i_q}} \tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{i_{q-1}}} \alpha^m [\tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{2i_{q-1}}}, \tilde{h}_q^{\alpha^{i_q}}]^{\alpha^m}
\end{aligned}$$

mas $[\tilde{h}_{p+1}^{\alpha^{i_{p+1}}} \ldots \tilde{h}_{q-1}^{\alpha^{2i_{q-1}}}, \tilde{h}_q^{\alpha^{i_q}}]^{\alpha^m} \in N$

Seja $l(m)$ a 2-valoração de m, ou seja, $l(m)$ é o maior inteiro não negativo tal que $2^{l(m)}$ divide m. Chamamos de forma semi-normal a forma de w tendo $(l(m), s+t)$ mínimo sobre a ordem lexicográfica.

O elemento w pode ser desenvolvido através de suas ações na árvore como

$$\begin{aligned} w =&(\tilde{h}_1^{\alpha^{2i_1}} \dots \tilde{h}_s^{\alpha^{2i_s}})(\tilde{k}_1^{\alpha^{2j_1+1}} \dots \tilde{k}_t^{\alpha^{2j_t+1}})\alpha^{2m'}\alpha^{\varepsilon} \\ =&((\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}, h_1 \dots h_s), e)(e, (\tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}}, k_1 \dots k_t))((\alpha^{m'}, e), (\alpha^{m'}, e))\alpha^{\varepsilon} \\ =&((\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}\alpha^{m'}, h_1 \dots h_s), (\tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}}\alpha^{m'+\varepsilon}, k_1 \dots k_t))\sigma^{\varepsilon} \end{aligned}$$

e fazendo $u = (\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}\alpha^{m'}, h_1 \dots h_s)$ e $v = (\tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}}\alpha^{m'+\varepsilon}, k_1 \dots k_t))$ obtemos que $w = (u,v)\sigma^{\varepsilon}$.

Suponha que $w \in N$ assim como definido acima está na forma semi-normal e $w \neq e$. Tome w com essas propriedades e sendo minimal com respeito ao par ordenado de inteiros $(l(m), s+t)$. Como N estabiliza o primeiro nível da árvore segue que $\varepsilon = 0$. Portanto, $s+t$ ou m é diferente de zero. Denotemos $P = N \times H'$ e $N = P \times P$, segue que $u, v \in P$. Da mesma forma, como $P = N \times H'$, temos $\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}\alpha^{m'}, \tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}}\alpha^{m'} \in N$ e $h_1 \dots h_s, k_1 \dots k_t \in H'$.

Pela condição de minimalidade, $l(m') = 0$, assim m' é ímpar ou é igual a zero, como $\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}\alpha^{m'}, \tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}}\alpha^{m'} \in N$ e N estabiliza o primeiro nível da árvore segue que $m' = 0$. Portanto, $\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_s^{\alpha^{i_s}}, \tilde{k}_1^{\alpha^{j_1}} \dots \tilde{k}_t^{\alpha^{j_t}} \in N$. Novamente pela condição de minimalidade, encontraremos um novo elemento de comprimento menor que $s+t$, por repetição deste argumento teremos $s = 0$ e $t = 1$ ou $s = 1$ e $t = 0$. No primeiro caso teremos $w = \tilde{h}_p^{\alpha^{2i_p}}$ para algum $p \in \{1, \dots s\}$. Se conjugarmos w por α^{-2i_p} iremos obter a forma semi-normal $w = \tilde{h}_p = ((\tilde{h}_p, h_p), e)$, com $h_p \in H'$. No segundo caso teremos $w = \tilde{k}_q^{\alpha^{2q+1}}$ para algum $q \in \{1, \dots t\}$ e conjugando w por $\alpha^{-(2q+1)}$ temos a forma semi-normal $w = \tilde{k}_q = ((\tilde{k}_q, k_q), e)$. Em ambos os casos w tem suporte infinito, como os elementos de N tem suporte finito chegamos a uma contradição.

Uma vez que determinamos a forma dos representantes, podemos estabelecer o isomorfismo de G/N em $H \wr \mathbb{Z}$.

Seja $w = (\tilde{h}_1^{\alpha^{2i_1}} \dots \tilde{h}_s^{\alpha^{2i_s}})(\tilde{k}_1^{\alpha^{j_1+1}} \dots \tilde{k}_t^{\alpha^{j_t+1}})\alpha^p$ como definido acima e $s+t = r$. Para simplificação, tomaremos

$$w = \tilde{h}_1^{\alpha^{n_1}} \dots \tilde{h}_r^{\alpha^{n_r}}\alpha^n$$

com $n_1, \dots, n_r$ inteiros distintos entre si.

Considere agora a aplicação

$$\begin{aligned} \varphi : G/N &\longrightarrow H \wr \mathbb{Z} \\ \prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i}\alpha^n N &\longmapsto (\prod_{i=n_1}^{n_r} (\dots, e, h_i, e, \dots)^i, n). \end{aligned}$$

A aplicação φ é um homomorfismo pois

$$
\begin{aligned}
(\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n N \prod_{n=q_1}^{q_x} \tilde{k}_i^{\alpha^i} \alpha^q N)\varphi =& (\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n \prod_{i=q_1}^{q_x} \tilde{k}_i^{\alpha^i} \alpha^q N)\varphi \\
=& (\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \prod_{i=q_1}^{q_x} \tilde{k}_i^{\alpha^{i-n}} \alpha^{n+q} N)\varphi \\
=& (\prod_{i=n_1}^{n_r} (\ldots, e, h_i, e, \ldots)^i, e)(\prod_{i=q_1}^{q_x} (\ldots, e, k_i, e, \ldots)^{i-n}, n+q) \\
=& (\prod_{i=n_1}^{n_r} (\ldots, e, h_i, e, \ldots)^i, n)(\prod_{i=q_1}^{q_x} (\ldots, e, k_i, e, \ldots)^i, q) \\
=& (\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n N)\varphi(\prod_{i=q_1}^{q_x} \tilde{k}_i^{\alpha^i} \alpha^q N)\varphi.
\end{aligned}
$$

A aplicação é injetiva visto que $(\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n N)\varphi = ((\ldots, e, e, e, \ldots), 0)$ se, e somente se, $\tilde{h}_i^{\alpha^i} = e$ para todo $i \in \{1, \ldots, r\}$ e $\alpha^n = e$.

Finalmente, φ é sobrejetiva visto que dado $(\prod_{i=n_1}^{n_r} (\ldots, e, h_i, e, \ldots)^i, n) \in H \wr \mathbb{Z}$, existe $\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n N \in G/N$ tal que $(\prod_{i=n_1}^{n_r} \tilde{h}_i^{\alpha^i} \alpha^n N)\varphi = (\prod_{i=n_1}^{n_r} (\ldots, e, h_i, e, \ldots)^i, n)$.

□

Demonstração. (III) As potências de α agem transpondo os elementos de posição ímpar em $0^{2m-1}1$, dessa forma, $\langle 0^{2m-1}1 * H', \alpha \rangle$ produz $u * H'$, onde $u \in (\{00, 10\})^*\{01, 11\}$ e $|u| = 2m$. Deste modo, os elementos de $\langle 0^{2m-1}1 * H', \alpha \rangle$ podem ser expressos por

$$u_1 * h'_1 \ldots u_{2^m} * h'_{2^m} \alpha^p$$

onde $u_i \neq u_j$ para $i \neq j$.

Observe que α^n age permutando os índices u_i, pois $u_i^{\alpha^n} = u_j$. Como $\overline{n} \in \mathbb{Z}/2^m\mathbb{Z}$ também age nos índices em $H' \wr \mathbb{Z}/2^m\mathbb{Z}$, tomaremos convenientemente $u_i \in (\{00, 10\})^*\{01, 11\}$ de forma que $u_i^{\alpha^n} = u_j$ se, e somente se, $j^{\overline{n}} = i$.

Queremos mostrar que $\langle \alpha^{2^m} \rangle \leq Z(\langle 0^{2m-1} * H', \alpha \rangle)$ e $\langle 0^{2m-1} * H', \alpha \rangle / \langle \alpha^{2^m} \rangle \simeq H' \wr \mathbb{Z}/2^m\mathbb{Z}$. Com efeito, de $[N_m, \alpha^{2^m}] = e$ decorre que α^{2^m} comuta com os elemetos de $\langle 0^{2m-1}1 * H', \alpha \rangle$, consequentemente, $\langle \alpha^{2^m} \rangle \leq Z(\langle 0^{2m-1}1 * H', \alpha \rangle)$. Mostaremos agora que a aplicação

$$\begin{aligned} \varphi : \langle 0^{2m-1}1 * H', \alpha\rangle / \langle \alpha^{2^m}\rangle &\longrightarrow H' \wr \mathbb{Z}/2^m\mathbb{Z} \\ u_1 * h'_1 \ldots u_{2^m} * h'_{2^m}\alpha^n\langle\alpha^{2^m}\rangle &\longmapsto ((h'_1,\ldots,h'_{2^m}),\overline{n}) \end{aligned}$$

é um isomorfismo.

A aplicação φ é um homomorfismo, pois dados $x, y \in \langle 0^{2m-1}1 * H', \alpha\rangle$, cujas expressões são $x = u_1 * h'_1 \ldots u_{2^m} * h'_{2^m}\alpha^n$, $y = u_1 * k'_1 \ldots u_{2^m} * k'_{2^m}\alpha^q$, segue que

$$\begin{aligned} (x\langle\alpha^{2^m}\rangle y\langle\alpha^{2^m}\rangle)\varphi =& (xy\langle\alpha^{2^m}\rangle)\varphi \\ =& (u_1 * (h'_1 k'_{1^{\overline{n}}}) \ldots u_{2^m} * (h'_{2^m} k'_{(2^m)^{\overline{n}}})\alpha^{n+q}\langle\alpha^{2^m}\rangle)\varphi \\ =& ((h'_1 k'_{1^{\overline{n}}}, \ldots, h'_{2^m} k'_{(2^m)^{\overline{n}}}), \overline{n+q}) \\ =& ((h'_1,\ldots,h'_{2^m}),\overline{n})((k'_1,\ldots,k'_{2^m}),\overline{q}) \\ =& (x\langle\alpha^{2^m}\rangle)\varphi(y\langle\alpha^{2^m}\rangle)\varphi \end{aligned}$$

A aplicação φ é sobrejetora visto que para todo $((h'_1,\ldots,h'_{2^m}),\overline{n}) \in H' \wr \mathbb{Z}/2^m\mathbb{Z}$, podemos tomar $u_1 * h'_1 \ldots u_{2^m} * h'_{2^m}\alpha^n\langle\alpha^{2^m}\rangle \in \langle 0^{2m-1}1 * H', \alpha\rangle / \langle\alpha^{2^m}\rangle$ de forma que

$$(u_1 * h'_1 \ldots u_{2^m} * h'_{2^m}\alpha^n\langle\alpha^{2m}\rangle)\varphi = ((h'_1,\ldots,h'_{2^m}),\overline{n}).$$

A aplicação φ é injetiva, pois

$$(u_1 * h'_1 \ldots u_{2^m} * h'_{2^m}\alpha^n\langle\alpha^{2^m}\rangle)\varphi = e$$

se, e somente se, $h'_1 = \cdots = h'_{2^m} = e$ e $\alpha^n \in \langle\alpha^{2^m}\rangle$.

□

Demonstração. (IV) Por construção, se H é um grupo que age na árvore binária, então denotamos $\langle\widetilde{H},\alpha\rangle$ por $H \bar{\wr} \mathbb{Z}$. Se J é um subgrupo de H, então J age na árvore, dessa forma, se dado um subgrupo $\langle\widetilde{J},\alpha\rangle$ de $H \bar{\wr} \mathbb{Z}$ segue que $\langle\widetilde{J},\alpha\rangle$ é isomorfo a $J \bar{\wr} \mathbb{Z}$.

Considere agora $K = J \bar{\wr} \mathbb{Z}$ e $M = \langle[\widetilde{J}^{\alpha^i}, \widetilde{J}^{\alpha^j}] | 0 \leq i < j\rangle$, que pode ser expresso por $M = (M \times J') \times (M \times J')$. Se J é abeliano, então $M = (M \times \{e\}) \times (M \times \{e\}) = \{e\}$, pelo Item (II) do Teorema 4.3.3, segue que $K/M \simeq J \bar{\wr} \mathbb{Z} \simeq J \wr \mathbb{Z}$. □

Demonstração. (V) Dividiremos a demonstração em três partes.

(Estado-finito)

Se G é de estado-finito, então $\widetilde{H}$ é de estado-finito, pois $\widetilde{H} \leq \langle \widetilde{H}, \alpha \rangle$. Dado $\tilde{h} \in \widetilde{H}$ o conjunto $Q(\tilde{h}) = \{\tilde{h}, (\tilde{h}, h), e\} \cup Q(h)$ tem número finito de estados, consequentemente $Q(h)$ tem número finito de estados para todo $h \in H$, portanto, H é de estado-finito.

Reciprocamente, se H é de estado-finito, então $\widetilde{H}$ é de estado-finito. De fato, o conjunto $\{\tilde{h}, (\tilde{h}, h), e\}$ é finito e $Q(h)$ tem número finito de estados, assim, $Q(\tilde{h}) = \{\tilde{h}, (\tilde{h}, h), e\} \cup Q(h)$ tem número finito de estados.

Note que $Q(\alpha^i)$ tem número finito de estados. De fato, por indução em i:

Base de Indução: $i = 0$

$Q(\alpha^0) = Q(e) = \{e\}$ tem número finito de estados.

Hipótese de Indução: Suponha o resultado válido para $i = n-1$, $\forall n \geq 1$

$Q(\alpha^n) = Q(\alpha^{n-1}\alpha) \subseteq Q(\alpha^{n-1})Q(\alpha)$, como $Q(\alpha^{n-1})$ e $Q(\alpha)$ tem número finito de estados segue que $Q(\alpha^{n-1})Q(\alpha)$ tem número finito de estados. Portanto, $Q(\alpha^n)$ tem número finito de estados.

De $Q(\alpha^{-1})$=$Q(\alpha)^{-1}$ segue que $Q(\alpha^{-n})$ tem número finito de estados, então $Q(\alpha^i)$ tem número finito de estados $\forall i \in \mathbb{Z}$.

Todo elemento $g \in G$ pode ser expresso por:

$$g = \tilde{h}_1^{\alpha^{i_1}} \ldots \tilde{h}_m^{\alpha^{i_m}} \alpha^p$$

onde $m \in \mathbb{N}$, $i_1, \ldots, i_m \in \mathbb{Z}$, $\tilde{h}_1, \ldots \tilde{h}_m \in \widetilde{H}$ e $\alpha^p \in \langle \alpha \rangle$, segue que

$$\begin{aligned} Q(g) =& Q(\tilde{h}_1^{\alpha^{i_1}} \ldots \tilde{h}_m^{\alpha^{i_m}} \alpha^p) \\ =& Q(\alpha^{-i_1}\tilde{h}_1\alpha^{i_1} \ldots \alpha^{-i_m}\tilde{h}_m\alpha^{i_m}\alpha^p) \\ \subseteq& Q(\alpha^{-i_1})Q(\tilde{h}_1)Q(\alpha^{i_1}) \ldots Q(\alpha^{-i_m})Q(\tilde{h}_m)Q(\alpha^{i_m})Q(\alpha^p) \end{aligned}$$

Observe que cada fator em $Q(\alpha^{-i_1})Q(\tilde{h}_1)Q(\alpha^{i_1}) \ldots Q(\alpha^{-i_m})Q(\tilde{h}_m)Q(\alpha^{i_m})Q(\alpha^p)$ possui número finito de estados, portanto, $Q(g)$ tem número finito de estados $\forall g \in G$. Logo, G é de estado-finito.

(Solúvel)

Se G é solúvel, então $\widetilde{H}$ é solúvel, pois $\widetilde{H} \leq G$. Como $\widetilde{H} \simeq H$ segue que H é solúvel.

Reciprocamente, suponha que H seja solúvel. Seja $N = (N \times H') \times (N \times H')$, então $[N,N] = ([N,N] \times H^{(2)}) \times ([N,N] \times H^{(2)})$, indutivamente, temos a seguinte fórmula para o $(n-1)$-ésimo comutador de N:

$$N^{(n-1)} = (N^{(n-1)} \times H^{(n)}) \times (N^{(n-1)} \times H^{(n)}).$$

Pela Proposição 1.2.17, temos que $H \wr \mathbb{Z}$ é solúvel. Além disso, $\exists n \in \mathbb{N}$ tal que $H^{(n)} = \{e\}$, então

$$N^{(n-1)} = (N^{(n-1)} \times H^{(n)}) \times (N^{(n-1)} \times H^{(n)}) = (N^{(n-1)} \times \{e\}) \times (N^{(n-1)} \times \{e\}) = \{e\}$$

logo, N é sóluvel.

Temos que $N \triangleleft G$ e $G/N \simeq H \wr \mathbb{Z}$ são solúveis, portanto, G é solúvel.

(Livre de torção)

Se G é livre de torção, então $\widetilde{H}$ é livre de torção, pois $\widetilde{H} \leq G$. Assim, dado $\tilde{h} \in \widetilde{H}$, onde $\tilde{h} \neq e$, segue que

$$\tilde{h}^n = ((\tilde{h}^n, h^n), e) \neq e$$

logo, $h^n \neq e \; \forall n \in \mathbb{Z} \backslash \{0\}$, portanto, H é livre de torção.

Se H é livre de torção, então $h^n \neq e \; \forall n \in \mathbb{Z} \backslash \{0\}$, assim $\tilde{h}^n \neq e$ pois $\tilde{h}^n = ((\tilde{h}^n, h^n), e)$ e $h^n \neq e$. Concluímos que $\widetilde{H}$ é livre de torção.

Consideraremos dois casos:

(1º Caso) Seja $g \in G$ onde $g = \tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_m^{\alpha^{i_m}}$ e $n \neq 0$. Como $\tilde{h}^{\alpha^{2i}}$ e $\tilde{k}^{\alpha^{2j+1}}$ comutam $\forall h, k \in H$, podemos reorganizar os fatores em g do seguinte modo:

$$\begin{aligned} g =& (\tilde{h}_{\lambda_1}^{\alpha^{2n_1}} \dots \tilde{h}_{\lambda_t}^{\alpha^{2n_t}})(\tilde{h}_{\theta_1}^{\alpha^{2q_1+1}} \dots \tilde{h}_{\theta_k}^{\alpha^{2q_k+1}}) \\ =& ((\tilde{h}_{\lambda_1}^{\alpha^{n_1}} \dots \tilde{h}_{\lambda_t}^{\alpha^{n_t}}, h_{\lambda_1} \dots h_{\lambda_t}), (\tilde{h}_{\theta_1}^{\alpha^{q_1}} \dots \tilde{h}_{\theta_k}^{\alpha^{q_k}}, h_{\theta_1} \dots h_{\theta_k})) \end{aligned}$$

Podemos repetir o procedimento de separar os elementos em blocos de forma a separar os elemetos conjugados por potências pares de α que estejam em um bloco e os de potências ímpares que estejam em outro. As potências são finitas, então o último procedimento resulta em $g=(u,v)$, onde

$$u=((((\tilde{h}_{\omega_1}\ldots\tilde{h}_{\omega_x},h_{\omega_1}\ldots h_{\omega_x}),(\tilde{h}_{\delta_1}\ldots\tilde{h}_{\delta_d},h_{\delta_1}\ldots h_{\delta_d})),\ldots),h_{\lambda_1}\ldots h_{\lambda_t})$$

e

$$v=((((\tilde{h}_{\sigma_1}\ldots\tilde{h}_{\sigma_y},h_{\sigma_1}\ldots h_{\sigma_y}),(\tilde{h}_{\varepsilon_1}\ldots\tilde{h}_{\varepsilon_e},h_{\varepsilon_1}\ldots h_{\varepsilon_e})),\ldots),h_{\theta_1}\ldots h_{\theta_k}).$$

Assim,

$$\begin{aligned}
g^n =&(\tilde{h}_{\lambda_1}^{\alpha^{2n_1}}\ldots\tilde{h}_{\lambda_t}^{\alpha^{2n_t}})^n(\tilde{h}_{\theta_1}^{\alpha^{2q_1+1}}\ldots\tilde{h}_{\theta_k}^{\alpha^{2q_k+1}})^n\\
=&(((\tilde{h}_{\lambda_1}^{\alpha^{n_1}}\ldots\tilde{h}_{\lambda_t}^{\alpha^{n_t}})^n),(h_{\lambda_1}\ldots h_{\lambda_t})^n,((\tilde{h}_{\theta_1}^{\alpha^{q_1}}\ldots\tilde{h}_{\theta_k}^{\alpha^{q_k}})^n,(h_{\theta_1}\ldots h_{\theta_k})^n))\\
&\vdots\\
=&(u^n,v^n)
\end{aligned}$$

Suponha que $g^n=e$, como H é livre de torção, então todo fator da forma $h_{\gamma_1}\ldots h_{\gamma_i}$ coincide com a identidade, o que nos retorna a seguinte informação de g:

$$\begin{aligned}
g =&(\tilde{h}_{\lambda_1}^{\alpha^{2n_1}}\ldots\tilde{h}_{\lambda_t}^{\alpha^{2n_t}})(\tilde{h}_{\theta_1}^{\alpha^{2q_1+1}}\ldots\tilde{h}_{\theta_k}^{\alpha^{2q_k+1}})\\
=&((\tilde{h}_{\lambda_1}^{\alpha^{n_1}}\ldots\tilde{h}_{\lambda_t}^{\alpha^{n_t}},h_{\lambda_1}\ldots h_{\lambda_t}),(\tilde{h}_{\theta_1}^{\alpha^{q_1}}\ldots\tilde{h}_{\theta_k}^{\alpha^{q_k}},h_{\theta_1}\ldots h_{\theta_k}))\\
=&((\tilde{h}_{\lambda_1}^{\alpha^{p_1}}\ldots\tilde{h}_{\lambda_t}^{\alpha^{p_t}},e),(\tilde{h}_{\theta_1}^{\alpha^{q_1}}\ldots\tilde{h}_{\theta_k}^{\alpha^{q_k}},e))\\
&\vdots\\
=&(e,e)
\end{aligned}$$

Concluímos que $g^n=e$, para $n\neq 0$, se, e somente se, $g=\tilde{h}_1^{\alpha^{i_1}}\ldots\tilde{h}_m^{\alpha^{i_m}}=e$.

(2º Caso) Seja $g\in G$ onde $g=\tilde{h}_1^{\alpha^{i_1}}\ldots\tilde{h}_m^{\alpha^{i_m}}\alpha^q$ e $n\neq 0$. Então

$$g^n=\tilde{h}_1^{\alpha^{i_1}}\ldots\tilde{h}_m^{\alpha^{i_m}}\ldots\tilde{h}_1^{\alpha^{i_1-(n-1)q}}\ldots\tilde{h}_m^{\alpha^{i_m-(n-1)q}}\alpha^{nq}$$

Se $\tilde{h}_1^{\alpha^{i_1}}\ldots\tilde{h}_m^{\alpha^{i_m}}\ldots\tilde{h}_1^{\alpha^{i_1-(n-1)q}}\ldots\tilde{h}_m^{\alpha^{i_m-(n-1)q}}\neq e$, então $g^n\neq e$, caso contrário teremos que $g^n=\alpha^{nq}$. Se $\alpha^{nq}=e$, então $q=0$, assim retornamos ao (1º Caso), pois deste modo $g=\tilde{h}_1^{\alpha^{i_1}}\ldots\tilde{h}_m^{\alpha^{i_m}}$.

Consequentemente, se $g\in G$ é um elemento não trivial de G, verificamos que $g^n\neq e$ para todo $n>0$, deste modo, concluímos que G é livre de torção. □

No sentido do Item (II) do Teorema acima, dizemos que um grupo G é um produto *tree-wreath* $H\,\bar{\wr}\,\mathbb{Z}$ se existe um subgrupo normal N de G tal que $G/N\simeq H\wr\mathbb{Z}$.

Observação 4.3.4. (i) O grupo quociente $\widehat{G}/\widehat{N}$ é metabeliano.

Seja $\mathcal{N} = \{Stab_G(i) \mid i \geq 0\}$. Note que $\mathcal{N}$ é um conjunto direcionado parcialmente ordenado, onde $Stab_G(i+1) \leq Stab_G(i)$.

Como $Stab_G(i) \lhd G$, os grupos quocientes $G/Stab_G(i)$ ficam definidos. Além disso, um elemento $gStab_G(i)$ de $G/Stab_G(i)$ age na árvore com a mesma ação de g até o nível i e depois age trivialmente, isto posto, concluímos que $G/Stab_G(i) \simeq Trun_G(i)$.

Tomaremos o completamento profinito de G com relação a $\mathcal{N}$, então

$$\widehat{G} = \varprojlim_{i\geq 1} G/Stab_G(i) \simeq \varprojlim_{i\geq 1} Trun_G(i),$$

onde

$$\varprojlim_{i\geq 1} Trun_G(i) = \{(\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_n, \ldots) \mid \hat{g}_i \in Trun_G(i) \text{ e } (\hat{g}_{i+1})_u = (\hat{g}_i)_u \forall u \in \mathcal{M}, |u| \leq i\},$$

por exemplo, se $\hat{g}_2 = ((e,\sigma)\sigma, e)$, então $\hat{g}_1 = (\sigma, e)$.

Os elementos $\hat{g}$ em $\widehat{G}$ podem ser interpretados como produtos infinitos de elementos de G que ficam bem definidos. Com esta identificação para $\hat{g}$, podemos expressá-lo por

$$\hat{g} = (\tilde{g}_{\lambda_1}^{\alpha^{2n_1}} \ldots \tilde{g}_{\lambda_t}^{\alpha^{2n_t}} \ldots)(\tilde{g}_{\theta_1}^{\alpha^{2q_1+1}} \ldots \tilde{g}_{\theta_k}^{\alpha^{2q_k+1}} \ldots)\alpha^{\eta},$$

onde $\tilde{g}_{\lambda_i}, \tilde{g}_{\theta_j} \in G$ e η é um inteiro diádico. Além disso, se $h \in H'$, então $\tilde{h} \in \widehat{N}$.

Sejam $\hat{g}, \hat{h} \in \widehat{G}$ dados por $\hat{g} = (\tilde{g}_{\lambda_1}^{\alpha^{2n_1}} \ldots \tilde{g}_{\lambda_t}^{\alpha^{2n_t}} \ldots)(\tilde{g}_{\theta_1}^{\alpha^{2q_1+1}} \ldots \tilde{g}_{\theta_k}^{\alpha^{2q_k+1}} \ldots)$ e $\hat{h} = (\tilde{h}_{\lambda_1}^{\alpha^{2r_1}} \ldots \tilde{h}_{\lambda_t}^{\alpha^{2r_t}} \ldots)(\tilde{h}_{\theta_1}^{\alpha^{2s_1+1}} \ldots \tilde{h}_{\theta_k}^{\alpha^{2s_k+1}} \ldots)$.

Então $\hat{g} = (a,b)$ e $\hat{h} = (c,d)$ com

$$\begin{aligned}
a &= (((\ldots),(g_{\delta_1}\cdots g_{\delta_d}\cdots, g_{\delta_1'}\cdots g_{\delta_d'}\cdots), g_{\lambda_1}\cdots g_{\lambda_t}\cdots)\\
b &= (((\ldots),(g_{\varepsilon_1}\cdots g_{\varepsilon_e}\cdots, g_{\varepsilon_1'}\cdots g_{\varepsilon_e'}\cdots), g_{\theta_1}\cdots g_{\theta_t}\cdots)\\
c &= (((\ldots),(h_{\delta_1}\ldots h_{\delta_d}\ldots, h_{\delta_1'}\ldots h_{\delta_d'}\ldots), h_{\lambda_1}\ldots h_{\lambda_t}\ldots)\\
d &= (((\ldots),(h_{\varepsilon_1}\ldots h_{\varepsilon_e}\ldots, h_{\varepsilon_1'}\ldots h_{\varepsilon_e'}\ldots), h_{\theta_1}\ldots h_{\theta_t}\ldots).
\end{aligned}$$

Para simplificação, tomaremos $k_\eta = k_{\eta_1} \ldots k_{\eta_t} \ldots$

Assim,

$$\begin{aligned}
[\hat{g},\hat{h}] =&([a,c],[b,d])\\
=&((((\ldots),([g_\delta,h_\delta],[g_{\delta'},h_{\delta'}])),[g_\lambda,h_\lambda]),(((\ldots),([g_\varepsilon,h_\varepsilon],[g_{\varepsilon'},h_{\varepsilon'}]),[g_\theta,h_\theta]))
\end{aligned}$$

e concluímos que $[\hat{g},\hat{h}] \in \widehat{N}$.

Agora considere $g = \hat{g}\alpha^{\zeta_1}$ e $h = \hat{h}\alpha^{\zeta_2}$, então

$$\begin{aligned}[g,h] =& \alpha^{-\zeta_1}\hat{g}^{-1}\alpha^{-\zeta_2}\hat{h}^{-1}\hat{g}\alpha^{\zeta_1}\hat{h}\alpha^{\zeta_2}\\ =&(\hat{g}^{-1})^{\alpha^{\zeta_1}}(\hat{h}^{-1})^{\alpha^{\zeta_1+\zeta_2}}(\hat{g})^{\alpha^{\zeta_1+\zeta_2}}(\hat{h})^{\alpha^{\zeta_2}}\\ =&(\tilde{k}_{\lambda_1}^{\alpha^{2a_1}}\ldots\tilde{k}_{\lambda_t}^{\alpha^{2a_t}}\ldots)(\tilde{k}_{\theta_1}^{\alpha^{2b_1+1}}\ldots\tilde{k}_{\theta_r}^{\alpha^{2b_r+1}}\ldots).\end{aligned}$$

Logo, $\forall \hat{x}_1,\hat{x}_2,\hat{x}_3,\hat{x}_4 \in \widehat{G}$, segue que $[[\hat{x}_1,\hat{x}_2],[\hat{x}_3,\hat{x}_4]] \in \widehat{N}$.

Consequentemente,

$$\begin{aligned}[\hat{x}_1,\hat{x}_2][\hat{x}_3,\hat{x}_4]\widehat{N} =& [\hat{x}_3,\hat{x}_4][\hat{x}_1,\hat{x}_2][[\hat{x}_1,\hat{x}_2],[\hat{x}_3,\hat{x}_4]]\widehat{N}\\ =&[\hat{x}_3,\hat{x}_4][\hat{x}_1,\hat{x}_2]\widehat{N}\end{aligned}$$

ou seja, $[\widehat{G}/\widehat{N},\widehat{G}/\widehat{N}]$ é abeliano.

(ii) Como $\mathbb{Z}\wr(\mathbb{Z}\wr\mathbb{Z})$ é residualmente um 2-grupo finito, podemos nos perguntar se existe uma cópia de tal grupo em $H\,\bar{\wr}\,\mathbb{Z}$ para algum grupo H, ou seja, se existem $h_1,h_2 \in H$ de forma que $\mathbb{Z}\wr(\mathbb{Z}\wr\mathbb{Z}) \simeq \langle\tilde{h}_2\rangle\wr(\langle\tilde{h}_1\rangle\wr\langle\alpha\rangle) \simeq \langle\tilde{h}_1,\tilde{h}_2,\alpha\rangle \leq \langle\widetilde{H},\alpha\rangle$.

Assuma que $\mathbb{Z}\wr(\mathbb{Z}\wr\mathbb{Z}) = \langle x\rangle\wr(\langle y\rangle\wr\langle z\rangle)$, pelo Item (IV) do Teorema 4.3.3, segue que $\langle y,z\rangle \simeq \langle y\rangle\wr\langle z\rangle$, pois $\langle y\rangle$ é abeliano.

Tome $(x_i)_{i\in\langle y\rangle\wr\langle z\rangle}$. Note que

$$(x_i)^w_{i\in\langle y\rangle\wr\langle z\rangle} \neq (x_i)_{i\in\langle y\rangle\wr\langle z\rangle},$$

para todo $w \in \langle y,z\rangle$ não trivial.

Sejam $h_1,h_2 \in H$. Se h_1 é tal que $\langle\tilde{h}_1\rangle$ é livre de torção, por argumento análogo ao de cima, segue que $\langle\tilde{h}_1,\alpha\rangle \simeq \langle\tilde{h}_1\rangle\wr\langle\alpha\rangle$, pois $\langle\tilde{h}_1\rangle$ é abeliano. Deste modo, temos a relação $\langle\tilde{h}_2\rangle\wr(\langle\tilde{h}_1\rangle\wr\langle\alpha\rangle) \simeq \langle\tilde{h}_2\rangle\wr\langle\tilde{h}_1,\alpha\rangle$. Agora, note que

$$\tilde{h}_1^{\alpha} = (e,(\tilde{h}_1^{\alpha},h_1)), \quad (\tilde{h}_2)^{\tilde{h}_1^{\alpha}} = \tilde{h}_2$$

gera uma contradição com $(x_i)^w_{i\in\langle y\rangle\wr\langle z\rangle} \neq (x_i)_{i\in\langle y\rangle\wr\langle z\rangle}$. Portanto, não existem $h_1,h_2 \in H$ não-triviais tais que $\langle\tilde{h}_1,\tilde{h}_2,\alpha\rangle \simeq \langle\tilde{h}_1\rangle\wr\langle\tilde{h}_2,\alpha\rangle$.

(iii) A translação $\alpha = (e,(\alpha,e))\sigma$ tem crescimento limitado e possui um 2-circuito. Se H for de crescimento limitado, então o produto tree-wreath $H\,\bar{\wr}\,\langle\alpha\rangle$ também tem crescimento limitado. Com efeito, seja $\tilde{h} = \tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_n^{\alpha^{i_n}} \alpha^n$. Então para todo $k \geq 0$, existe $c > 0$

$$\theta(k+1,h) \leq \theta(k+1,\alpha^{-i_1}) + \theta(k+1,\tilde{h}_1) + \theta(k+1,\alpha^{i_1}) + \dots + \theta(k+1,\alpha^n) \leq c$$

Além disso, se H é gerado por automorfismos com estrutura de circuito limitado, então $H \bar{\wr} \langle\alpha\rangle$ também possui estrutura de circuito limitado. Portanto, a construção *tree-wreath* preserva subgrupos de $\mathcal{F}_{0,2}(Y)$.

Finalizaremos a seção com o resultado a seguir que, para um grupo solúvel (nilpotente) H, relaciona o grau de solubilidade (classe de nilpotência) de $\tilde{H}$ e seu fecho normal em $H \bar{\wr} \mathbb{Z}$.

Proposição 4.3.5. Seja $L = \widetilde{H}^{\langle\alpha\rangle}$ o fecho normal de $\widetilde{H}$ em G. Se H é solúvel (nilpotente), então L e H tem o mesmo grau de solubilidade (classe de nilpotência).

Demonstração. Sejam R um subgrupo de $\mathcal{A}$, $\nu(R) = (\nu(R) \times R) \times (\nu(R) \times R)$ e $\tilde{h} \in \widetilde{H}$. Então

$$\begin{aligned}
[\nu(R),\tilde{h}] =&[(\nu(R) \times R) \times (\nu(R) \times R), ((\tilde{h},h),e)]\\
=&([(\nu(R) \times R), (\tilde{h},h)]), [(\nu(R) \times R), e])\\
=&([\nu(R),\tilde{h}] \times [R,h], e)
\end{aligned}$$

$$\begin{aligned}
[\nu(R),\tilde{h}^{\alpha}] =&[(\nu(R) \times R) \times (\nu(R) \times R), (e,(\tilde{h},h))]\\
=&(e, [\nu(R),\tilde{h}] \times [R,h])
\end{aligned}$$

Mais geral, $\langle [\nu(R), H_i] \mid i \geq 0 \rangle = [\nu(R), \langle H_i \mid i \geq 0 \rangle] = \nu([R,H])$. Tome $0^{2s-1}1 * r \in \nu(R)$ e $\tilde{h}^{\alpha^{2s}} \in H_{2s}$, então

$$[0^{2s-1}1 * r, \tilde{h}^{\alpha^{2s}}] = 0^{2s-1}1 * [r,h] \in \nu([R,H])$$

Como $[\nu(R), H_i]^{\alpha^p} = [\nu(R)^{\alpha^p}, H_i^{\alpha^p}] = [\nu(R), H_{i+p}] \subseteq [\nu(R), \langle H_i \mid i \geq 0 \rangle]$ e as potências de α agem em $0^{2s-1}1$ transpondo as entradas de posição ímpar, produzimos $u * [r,h]$ para todo $u \in (\{00,10\}^*)\{01,11\}$, ou seja, $[\nu(R), \langle H_i \mid i \geq 0 \rangle] = \nu([R,H])$. Como L é o fecho normal de $\widetilde{H}$ em G segue que $L = \langle \widetilde{H}^g \mid g \in G \rangle$. Assim, $\langle H_i \mid i \geq 0 \rangle \subseteq L$. Além disso, um elemento de G pode ser expresso por, $g = \tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_m^{\alpha^{i_m}} \alpha^p$, logo

$$\begin{aligned}
g^{-1}\tilde{h}g =&\alpha^{-p}\tilde{h}_m^{\alpha^{-i_m}} h_1^{\alpha^{i_1}} \tilde{h}\tilde{h}_1^{\alpha^{i_1}} \dots \tilde{h}_m^{\alpha^{i_m}} \alpha^p\\
=&\tilde{h}_m^{\alpha^{-i_m+p}} h_1^{\alpha^{i_1+p}} \alpha^{-p}\tilde{h}\alpha^p \tilde{h}_1^{\alpha^{i_1-p}} \dots \tilde{h}_m^{\alpha^{i_m-p}}\\
=&\tilde{h}_m^{\alpha^{-i_m+p}} h_1^{\alpha^{i_1+p}} \tilde{h}^{\alpha^p} \tilde{h}_1^{\alpha^{i_1-p}} \dots \tilde{h}_m^{\alpha^{i_m-p}} \in \langle H_i \mid i \geq 0 \rangle
\end{aligned}$$

ou seja, $L \subseteq \langle H_i \mid i \geq 0 \rangle$. Portanto,

$$L = \langle H_i \mid i \geq 0 \rangle.$$

Daqui em diante, o objetivo é determinar fórmulas para a série derivada $L^{(j)}$ e para a série central inferior $\gamma_j(L)$.

$$\begin{aligned} L' =& [L, L] \\ =& [\langle H_i \mid i \geq 0 \rangle, \langle H_i \mid i \geq 0 \rangle] \\ =& \langle [H_i, H_i], [H_i, H_j] \mid 0 \leq i < j \rangle \\ =& \langle H_i', \nu(H') \mid i \geq 0 \rangle. \end{aligned}$$

Suponha por indução em $j \geq 2$ que $L^{(j-1)} = \langle H_i^{(j-1)}, \nu(H^{(j-1)}) \mid i \geq 0 \rangle$, então

$$\begin{aligned} L^{(j)} =& [L^{(j-1)}, L^{(j-1)}] \\ =& [\langle H_i^{(j-1)}, \nu(H^{(j-1)}) \mid i \geq 0 \rangle, \langle H_i^{(j-1)}, \nu(H^{(j-1)}) \mid i \geq 0 \rangle] \\ =& \langle [H_i^{(j-1)}, H_i^{(j-1)}], [\nu(H^{(j-1)}), H_i^{(j-1)}], [\nu(H^{(j-1)}), \nu(H^{(j-1)})] \mid i \geq 0 \rangle \\ =& \langle H_i^{(j)}, \nu(H^{(j)}), \nu(H^{(j)}) \mid i \geq 0 \rangle \\ =& \langle H_i^{(j)}, \nu(H^{(j)}) \mid i \geq 0 \rangle. \end{aligned}$$

Quanto a série central inferior de L, para $j = 2$ temos

$$\begin{aligned} \gamma_2(L) =& [L, L] \\ =& \langle H_i', \nu(H') \mid i \geq 0 \rangle, \end{aligned}$$

por indução em $j \geq 3$, supondo que $\gamma_{j-1}(L) = \langle \nu(\gamma_{j-1}(H)), \gamma_{j-1}(H_i) \mid i \geq 0 \rangle$, segue que

$$\begin{aligned} \gamma_j(L) =& [\gamma_{j-1}(L), L] \\ =& [\langle \nu(\gamma_{j-1}(H)), \gamma_{j-1}(H_i) \mid i \geq 0 \rangle, \langle H_i \mid i \geq 0 \rangle] \\ =& \langle [\nu(\gamma_{j-1}(H)), \langle H_i \mid i \geq 0 \rangle], [\langle \gamma_{j-1}(H_i) \mid i \geq 0 \rangle, \langle H_i \mid i \geq 0 \rangle] \rangle \\ =& \langle \nu([\gamma_{j-1}(H), H]), [\gamma_{j-1}(H_i), H_i \mid i \geq 0], [\gamma_{j-1}(H_i), H_k \mid 0 \leq i < k] \rangle \\ =& \langle \nu(\gamma_j(H)), \gamma_j(H_i), \nu(\gamma_j(H)) \mid i \geq 0] \rangle \\ =& \langle \nu(\gamma_j(H)), \gamma_j(H_i) \mid i \geq 0] \rangle. \end{aligned}$$

Mas $\langle [\gamma_{j-1}(H_i), H_k \mid 0 \leq i < k] \rangle = \nu(\gamma_j(H))$, a demonstração deste fato é feito de forma análoga ao item (I) do Teorema 4.3.3, basta substituir H_i por $\gamma_{j-1}(H_i)$ em $\nu(H') = \langle [H_i, H_k \mid 0 \leq i < k] \rangle = \nu(\gamma_j(H))$. Então

$$\begin{aligned}\gamma_j(L) =& \langle \nu([\gamma_{j-1}(H), H]), [\gamma_{j-1}(H_i), H_i \mid i \geq 0], [\gamma_{j-1}(H_i), H_k \mid 0 \leq i < k] \rangle \\ =& \langle \nu(\gamma_j(H)), \gamma_j(H_i), \nu(\gamma_j(H)) \mid i \geq 0] \rangle \\ =& \langle \nu(\gamma_j(H)), \gamma_j(H_i) \mid i \geq 0] \rangle.\end{aligned}$$

□

4.4 O centralizador de α

Seja $\gamma = (\gamma_0, \gamma_1)\sigma_\gamma$ um elemento do centralizador de α em $\mathcal{A}_2$, denotado por $C_{\mathcal{A}_2}(\alpha)$. Como γ também comuta com $\gamma\alpha$ podemos considerar γ inativo, ou seja $\sigma_\gamma = 0$. Com efeito, caso γ seja inativo teremos $\gamma = (\gamma_0, \gamma_1)$, deste modo

$$\gamma\alpha = (\gamma_0, \gamma_1)(e, (\alpha, e))\sigma = (\gamma_0, \gamma_1(\alpha, e))\sigma$$

e

$$\alpha\gamma = (e, (\alpha, e))\sigma(\gamma_0, \gamma_1) = (\gamma_1, (\alpha, e)\gamma_0)\sigma$$

assim, $\gamma_0 = \gamma_1$, γ_0 comuta com (α, e) e fazendo $\gamma_0 = (\gamma_{00}, \gamma_{01})$ segue que γ_{00} comuta com α e γ_{01} é um elemento arbitrário de $\mathcal{A}_2$.

Suponha agora que $\gamma' = (\gamma_0, \gamma_1)\sigma(\gamma')$ seja ativo, ou seja, $\sigma(\gamma') = \sigma$, então

$$\gamma'\alpha = (\gamma_0, \gamma_1)\sigma(e, (\alpha, e))\sigma = (\gamma_0(\alpha, e), \gamma_1)$$

e

$$\alpha\gamma' = (e, (\alpha, e))\sigma(\gamma_0, \gamma_1)\sigma = (\gamma_1, (\alpha, e)\gamma_0)$$

deste modo, $\gamma_1 = \gamma_0(\alpha, e)$ e γ_0 comuta com (α, e), retornando em γ' obtemos a expressão

$$\gamma' = (\gamma_0, \gamma_0(\alpha, e))\sigma) = (\gamma_0, \gamma_0)(e, (\alpha, e))\sigma = (\gamma_0, \gamma_0)\alpha$$

e neste sentido, um elemento γ' ativo do centralizador de α pode ser escrito como $\gamma' = \gamma\alpha$ onde γ é um elemento inativo do centralizador de α tal como descrito acima.

Para $\beta \in \mathcal{A}_2$, definimos a notação $\beta^x = (\beta, \beta)$ que também é um elemento de $\mathcal{A}_2$. Concluímos que $C_{\mathcal{A}_2}(\alpha)$ tem a seguinte decomposição por meio de suas ações sobre a árvore binária

$$C_{\mathcal{A}_2}(\alpha) = C_{\mathcal{A}_2}((\alpha,e))^x\langle\alpha\rangle, \qquad C_{\mathcal{A}_2}((\alpha,e)) = C_{\mathcal{A}_2}(\alpha)\times\mathcal{A}_2.$$

Dado $\delta\in\mathcal{A}_2$, definimos $\delta' = (\delta',\delta)^x = ((\delta',\delta),(\delta',\delta))$ em $\mathcal{A}_2$. O seguinte cálculo mostra que $\delta'\in C_{\mathcal{A}_2}(\alpha)$:

$$\begin{aligned}
\alpha^{\delta'} =& (\delta')^{-1}\alpha\delta' \\
=& (((\delta')^{-1},\delta^{-1}),((\delta')^{-1},\delta^{-1}))(e,(\alpha,e))\sigma((\delta',\delta),(\delta',\delta)) \\
=& (((\delta')^{-1},\delta^{-1}),((\delta')^{-1},\delta^{-1}))(e,(\alpha,e))((\delta',\delta),(\delta',\delta))\sigma \\
=& (e,(\alpha^{\delta'},e))\sigma \\
=& \alpha.
\end{aligned}$$

Utilizando esta última definição, produzimos indutivamente a seguinte sequência de elementos em $C_{\mathcal{A}_2}(\alpha)$:

$$\alpha(0) = \alpha, \qquad \alpha(i) = (\alpha(i),\alpha(i-1))^x = ((\alpha(i),\alpha(i-1)),(\alpha(i),\alpha(i-1)))$$

para todo $i\geq 1$.

Observação 4.4.1. Em $\alpha(i)$, a primeira incidência de α ocorre no nível $2i$.

Com efeito, $\alpha(0)=\alpha$ ocorre na raiz, ou seja, no nível 0. Suponha por hipótese de indução que o resultado é válido para $j=i-1$ com $i\geq 1$. Como $\alpha(i) = (\alpha(i),\alpha(i-1))^x$, considerando $\alpha(i-1)$ agindo a partir da raiz, temos por hipótese de indução que α ocorre no nível $2(i-1)$, como $\alpha(i-1)$ aparece agindo no nível 2 em $\alpha(i)$, segue que α aparece pela primeira vez agindo no nível $2s$ em $\alpha(i)$.

Defina $K(r)$ como o grupo gerado por $\{\alpha(i)\mid 0\leq i\leq r-1\}$.

Lema 4.4.2. O grupo $K(r)$ como definido acima é abeliano livre de posto r.

Demonstração. Inicialmente, verificaremos que $K(r)$ é de fato um grupo abeliano.

Por construção, $\alpha(i)^{\alpha} = \alpha(i)$ para todo $i\in\{0,\dots r-1\}$. Suponha por hipótese de indução que $\alpha(i)^{\alpha(j-1)} = \alpha(i)$ para todo $i\in\{0,\dots,r-1\}$ e $j\geq 1$, então

$$\begin{aligned}
\alpha(i)^{\alpha(j)} =& (\alpha(j)^{-1},\alpha(j-1)^{-1})^x(\alpha(i),\alpha(i-1))^x(\alpha(j),\alpha(j-1))^x \\
=& (\alpha(i)^{\alpha(j)},\alpha(i-1)^{\alpha(j-1)})^x \\
=& (\alpha(i)^{\alpha(j)},\alpha(i-1))^x \\
=& \alpha(i).
\end{aligned}$$

A seguir, iremos mostrar que os geradores de $K(r)$ não admitem relações. Note que $\alpha(0) = \alpha$ gera um grupo cíclico infinito, portanto $\alpha^n \neq e$ para todo $n \neq 0$. Suponha por indução que $\alpha(i-1)^n \neq e$ para todo $n \neq 0$, então $\alpha(i)^n = (\alpha(i)^n, \alpha(i-1)^n)^x \neq e$ visto que $\alpha(i-1)^n \neq e$.

Além disso, um elemento arbitrário de $K(r)$ tem a forma $w = \alpha(0)^{n_0} \dots \alpha(r-1)^{n_r}$ onde $n_0, \dots n_r \in \mathbb{Z}$, visto que $K(r)$ é abeliano. Observe em w que se n_0 for ímpar, então w sempre será não trivial, pois os únicos elementos que agem no nível 1 são as potências ímpares de $\alpha(0) = \alpha$, isto posto, nos resta somente analisar as palavras onde n_0 é par. Sejam $i, n_1 \in \mathbb{Z}$. Então

$$\begin{aligned}
\alpha^{2i}\alpha(1)^{n_1} &= ((\alpha^i, e), (\alpha^i, e))((\alpha(1)^{n_1}, \alpha^{n_i}), (\alpha(1)^{n_1}, \alpha^{n_i})) \\
&= (\alpha^i, e)^x (\alpha(1)^{n_1}, \alpha^{n_1})^x \\
&= (\alpha^i \alpha(1)^{n_1}, \alpha^{n_1})^x \\
&= (e, e)^x
\end{aligned}$$

se, e somente se, $i = n_1 = 0$. Assuma por hipótese de indução que, dados $i, n_1, \dots n_{r-2} \in \mathbb{Z}$, $w = \alpha(0)^{2i} \dots \alpha(r-2)^{n_{r-2}} = e$ se, e somente se, $i = n_1 = \dots = n_{r-2} = 0$. Suponha que

$$\begin{aligned}
w =& \alpha^{2i} \dots \alpha(r-1)^{n_{r-1}} \\
=& (\alpha^i \dots \alpha(r-1)^{n_{r-1}}, \alpha^{n_1} \dots \alpha(r-2)^{n_{r-1}})^x \\
=& (e, e)^x
\end{aligned}$$

seja trivial. Então, por hipótese de indução, segue que $n_1 = \dots = n_{r-2} = 0$, consequentemente,

$$w = (\alpha^i, e)^x = (e, e)^x$$

se, e somente se, $i = 0$. Portanto, concluímos que não existem relações entre os geradores de $K(r)$. Logo, $K(r)$ é um grupo abeliano livre. $\square$

4.5 O fecho topológico de $K(r)$ e seu normalizador

O fecho topológico de $\langle \alpha(i) \rangle$, com respeito ao 2-completamento, é isormofo ao conjunto dos inteiros diádicos $\mathbb{Z}_2$, visto que $\langle \alpha(i) \rangle \simeq \mathbb{Z}$. Neste sentido, decorre o seguinte lema.

Lema 4.5.1. O fecho de $K(r)$ é a soma direta $\widehat{K(r)} = \bigoplus_{i=0}^{r-1} \widehat{\langle \alpha(i) \rangle}$.

Demonstração. O resultado segue direto do fato de $K(r)$ ser um grupo abeliano gerado por $\{\alpha(i) \mid 0 \leq i \leq r-1\}$. $\square$

A seguir, produziremos elementos de $\mathcal{A}_2$ que normalizam $\widehat{K(r)}$. Para cada unidade diádica $\xi = 1 + \sum_{i=1}^{+\infty} a_i 2^i$, onde $a_i = 0$ ou 1, defina em $\mathcal{A}_2$ o elemento $\lambda_\xi = ((\lambda_\xi, e), (\lambda_\xi \alpha^{(\xi-1)/2}, e))$, e defina o conjunto $\Lambda = \{\lambda_\xi \mid \xi$ é uma unidade diádica.$\}$. Então λ_ξ conjuga α para α^ξ. Com efeito,

$$\begin{aligned}
\beta =& \alpha^{\lambda_\xi} \\
=& \lambda_\xi^{-1} \alpha \lambda_\xi \\
=& ((\lambda_\xi^{-1}, e), (\alpha^{-(\xi-1)/2} \lambda_\xi^{-1}, e))(e, (\alpha, e))\sigma((\lambda_\xi, e), (\lambda_\xi \alpha^{(\xi-1)/2}, e)) \\
=& ((\lambda_\xi^{-1}, e), (\alpha^{-(\xi-1)/2} \lambda_\xi^{-1}, e))(e, (\alpha, e))((\lambda_\xi \alpha^{(\xi-1)/2}, e), (\lambda_\xi, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{-(\xi-1)/2} \alpha^{\lambda_\xi}, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{-(\xi-1)/2} \beta, e))\sigma
\end{aligned}$$

Por outro lado, note que se $\xi = 1 + \sum_{i=1}^{+\infty} a_i 2^i$, então temos as relações $(\xi - 1)/2 = \sum_{i=1}^{+\infty} a_i 2^{i-1}$ e $(\xi + 1)/2 = 1 + (\xi - 1)/2 = 1 + \sum_{i=1}^{+\infty} a_i 2^{i-1}$, além disso, $(\xi - 1)/2 + (\xi + 1)/2 = \xi$. Então

$$\begin{aligned}
\gamma =& \alpha^\xi \\
=& \alpha^{1+\sum_{i=1}^{+\infty} a_i 2^i} \\
=& \alpha^{1+2\sum_{i=1}^{+\infty} a_i 2^{i-1}} \\
=& ((\alpha^{\sum_{i=1}^{+\infty} a_i 2^{i-1}}, e), (\alpha^{1+\sum_{i=1}^{+\infty} a_i 2^{i-1}}, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{(\xi+1)/2}, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{-(\xi-1)/2} \alpha^{(\xi-1)/2} \alpha^{(\xi+1)/2}, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{-(\xi-1)/2} \alpha^\xi, e))\sigma \\
=& ((\alpha^{(\xi-1)/2}, e), (\alpha^{-(\xi-1)/2} \gamma, e))\sigma,
\end{aligned}$$

portanto, como β e γ possuem a mesma ação, concluímos que eles coincidem, isto é, $\alpha^{\lambda_\xi} = \alpha^\xi$.

Observe que α é gerador de $\widehat{\langle \alpha \rangle}$ e que qualquer outro gerador de $\widehat{\langle \alpha \rangle}$ deve gerar α. As potências dos elementos em $\widehat{\langle \alpha \rangle}$ são inteiros diádicos, além disso, um elemento α^ζ é um gerador de $\widehat{\langle\alpha\rangle}$ se, e somente se, existe $\eta \in \mathbb{Z}_2$ tal que $\zeta\eta = 1$ e, consequentemente, $(\alpha^{\zeta})^{\eta} = \alpha$. Através da Proposição 1.4.29 podemos afirmar que α^{ζ} gera α se, e somente se, ζ é uma unidade diádica. Como todo automorfismo de um grupo G fica completamento determinado pela imagem dos geradores, todos os automorfismos de $\widehat{\langle\alpha\rangle}$ são definidos por $\alpha \mapsto \alpha^{\xi}$, onde ξ é uma unidade diádica. Como $\alpha^{\lambda_\xi} = \alpha^{\xi}$, existe uma bijeção entre os automorfismo $\alpha \mapsto \alpha^{\xi}$ e os elementos λ_ξ, portanto, $Aut(\widehat{\langle\alpha\rangle}) \simeq \Lambda$. Agora, defina

$$\lambda_\xi(0) = \lambda_\xi = ((\lambda_\xi, e), (\lambda_\xi \alpha^{(\xi-1)/2}, e))$$

e indutivamente

$$\lambda_\xi(i) = (\lambda_\xi(i), \lambda_\xi(i-1))^x$$

para todo $i \geq 1$.

Sejam $\Lambda_i = \{\lambda_\xi(i) \mid \xi \text{ é uma unidade diádica}\}$ e $\Lambda(r) = \langle \Lambda_i \mid 0 \leq i \leq r-1 \rangle$. Então $Aut(\widehat{\langle\alpha(i)\rangle}) \simeq \Lambda_i$, pois

$$\alpha(i)^{\lambda_\xi(i)} = (\alpha(i)^{\lambda_\xi(i)}, \alpha(i-1)^{\lambda_\xi(i-1)})^x = \alpha(i)^{\xi}.$$

Proposição 4.5.2. O grupo $\Lambda(r) = \langle \Lambda_i \mid 0 \leq i \leq r-1 \rangle$ normaliza $\widehat{K(r)}$ e o grupo $\langle \widehat{K(r)}, \Lambda(r) \rangle$ é a soma direta

$$\bigoplus_{i=0}^{r-1} \widehat{\langle\alpha(i)\rangle} \Lambda_i.$$

Demonstração. Vimos anterirmente que $\alpha(i)^{\lambda_\xi(i)} = \alpha(i)^{\xi} \in \widehat{\langle\alpha(i)\rangle}$. Observe agora que, para $i \geq 1$, $\lambda_\xi(i)$ possui a caracterização do elemento δ' exposto na Seção 4.4, portanto, segue que $\lambda_\xi(i) \in C_{\mathcal{A}_2}(\alpha)$ para todo $i \geq 1$, logo $\alpha^{\lambda_\xi(i)} = \alpha$. Por fim, verificaremos os conjugados de $\alpha(i)$ para $i \geq 1$. Inicialmente, temos

$$\begin{aligned}
\alpha(i)^{\lambda_\xi(0)} =& ((\alpha(i)^{\lambda_\xi}, \alpha(i-1)), (\alpha(i)^{\lambda_\xi \alpha^{\xi-1/2}}, \alpha(i-1))) \\
=& ((\alpha(i)^{\lambda_\xi}, \alpha(i-1)), (\alpha(i)^{\lambda_\xi}, \alpha(i-1))) \\
=& \alpha(i),
\end{aligned}$$

e por indução em j, para $j \neq i$,

$$\begin{aligned}
\alpha(i)^{\lambda_\xi(j)} =& (\alpha(i)^{\lambda_\xi(j)}, \alpha(i-1)^{\lambda_\xi(j-1)})^x \\
=& (\alpha(i)^{\lambda_\xi(j)}, \alpha(i-1))^x \\
=& \alpha(i).
\end{aligned}$$

Concluímos que $\Lambda(r) = \langle \Lambda_i \mid 0 \leq i \leq r \rangle$ normaliza $\widehat{K(r)}$.

A seguir, iremos verificar que $\Lambda(r) = \bigoplus_{i=0}^{r-1} \Lambda_i$, para isto, note que

$$\begin{aligned}
[\lambda_\xi(0), \lambda_\xi(i)] =& [((\lambda_\xi, e), (\lambda_\xi \alpha^{(\xi-1)/2}, e)), ((\lambda_\xi(i), \lambda_\xi(i-1)), (\lambda_\xi(i), \lambda_\xi(i-1)))] \\
=& (([\lambda_\xi, \lambda_\xi(i)], e), ([\lambda_\xi \alpha^{(\xi-1)/2}, \lambda_\xi(i)], e)) \\
=& (([\lambda_\xi, \lambda_\xi(i)], e), ([\lambda_\xi \alpha^{(\xi-1)/2}, \lambda_\xi(i)]^{\alpha^{(\xi-1)/2}} [\alpha^{(\xi-1)/2}, \lambda_\xi(i)], e)) \\
=& (([\lambda_\xi, \lambda_\xi(i)], e), ([\lambda_\xi, \lambda_\xi(i)]^{\alpha^{(\xi-1)/2}}, e)) \\
=& e,
\end{aligned}$$

para todo $i \geq 1$, e supondo por hipótese de indução que $[\lambda_\xi(j-1), \lambda_\xi(i)] = e$ temos

$$\begin{aligned}
[\lambda_\xi(j), \lambda_\xi(i)] =& ([\lambda_\xi(j), \lambda_\xi(i)], [\lambda_\xi(j-1), \lambda_\xi(i-1)])^x \\
=& ([\lambda_\xi(j), \lambda_\xi(i)], e)^x \\
=& e,
\end{aligned}$$

para todo $i, j \geq 1$. Assim, $\Lambda(r) = \bigoplus_{i=0}^{r-1} \Lambda_i$.

Vimos que $\alpha(i)$ comuta com $\lambda_\xi(j)$ sempre que $i \neq j$, além disso, $\widehat{K(r)} = \bigoplus_{i=0}^{r-1} \widehat{\langle \alpha(i) \rangle}$ e $\Lambda(r) = \bigoplus_{i=0}^{r-1} \Lambda_i$, consequentemente, segue que

$$\langle \widehat{K(r)}, \Lambda(r) \rangle = \bigoplus_{i=0}^{r-1} \widehat{\langle \alpha(i) \rangle} \Lambda_i.$$

□

4.6 O grupo $H \,\bar{\wr}\, \widehat{K(r)}$

O processo de copiar H utilizado na Seção 4.2 pode ser iterado para permanecer compatível com o entrelaçamento por $K(r)$, para tal, defina para cada $h \in H$,

$$\tilde{h}(0) = h, \quad \tilde{h}(1) = \tilde{h} = ((\tilde{h}(1), h), e),$$

e indutivamente para todo $i \geq 1$

$$\tilde{h}(i) = ((\tilde{h}(i), \tilde{h}(i-1)), e).$$

Note que $\widetilde{H}(i) = \{\tilde{h}(i) \mid h \in H\}$ é um grupo isomorfo a H.

Além disso, podemos estender a definição do produto *tree-wreath* apresentada anteriormente.

Definição 4.6.1. Seja H um grupo que age na árvore binária. Diremos que G é um produto *tree-wreath* $H \bar{\wr} \widehat{K(r)}$ se existir um subgrupo normal N de G tal que $G/N \simeq \widetilde{H}(r) \wr \widehat{K(r)}$.

O teorema a seguir é uma versão do Item (II) do Teorema 4.3.3 para nosso novo produto *tree-wreath*. Este resultado é peça fundamental para resolver a problemática proposta neste texto.

Teorema 4.6.2. O grupo $G = \langle \widetilde{H}(r), \widehat{K(r)} \rangle$ é um produto tree-wreath $H \bar{\wr} \widehat{K(r)}$.

Demonstração. Seja $N(r)$ o subgrupo de G gerado pelos grupos comutadores $[\widetilde{H}(r), \widetilde{H}(r)^{\gamma}]$ para todo $\gamma \in \widehat{K(r)}$. Precisamos mostrar que o quociente comutador $G/N(r)$ é isomorfo a $\widetilde{H}(r) \wr \widehat{K(r)}$ e que $N(r)$ é a soma direta de um número infinito de cópias do grupo derivado H'.

Seja ξ um inteiro diádico e denote por $l(\xi)$ sua 2-valoração. Considere $\xi = \varepsilon + 2\xi'$, onde $\varepsilon = 0$ ou 1. Então,

$$\alpha^{\xi} = \begin{cases} (\alpha^{\xi'}, e)^{x}, \text{ se } \varepsilon = 0 \\ ((\alpha^{\xi'}, e), (\alpha^{1+\xi'}, e))\sigma, \text{ se } \varepsilon = 1. \end{cases}$$

Defina

$$\begin{aligned} &\xi_i = \varepsilon_i + 2\xi_i', \quad \varepsilon_i = 0, 1, \\ &\gamma = \alpha(0)^{\xi_0} \alpha(1)^{\xi_1} \ldots \alpha(r)^{\xi_r}, \\ &\beta = \alpha(1)^{\xi_1} \ldots \alpha(r)^{\xi_r}. \end{aligned}$$

Então,

$$\beta = (\beta, \beta')^{x} \quad \beta' = \alpha(0)^{\xi_1} \alpha(1)^{\xi_2} \ldots \alpha(r-1)^{\xi_r},$$

e γ é ativo se, e somente se, ε_0 ou 1.

Sejam $\tilde{h}(r) = ((\tilde{h}(r), \tilde{h}(r-1)), e), \tilde{b}(r) = ((\tilde{b}(r), \tilde{b}(r-1)), e) \in \widetilde{H}(r)$. Então,

$$\tilde{h}(r)^{\gamma} = \tilde{h}(r)^{\alpha(0)^{\xi_0}\beta} = \begin{cases} ((\tilde{h}(r)^{\alpha(0)^{\xi_0'}\beta}, \tilde{h}(r-1)^{\beta'}), e), \text{ se } \varepsilon_0 = 0 \\ (e, (\tilde{h}(r)^{\alpha(0)^{\xi_0'}\beta}, \tilde{h}(r-1)^{\beta'}) \text{ se } \varepsilon_0 = 1 \end{cases}$$

Note que

$$[\tilde{h}(r), \tilde{b}(r)^{\gamma}] = \begin{cases} (([\tilde{h}(r), \tilde{b}(r)^{\alpha(0)^{\xi_0'}\beta}], [\tilde{h}(r-1), \tilde{b}(r-1)^{\beta'}]), e), \text{ se } \varepsilon_0 = 0 \\ e, \text{ se } \varepsilon_0 = 1 \end{cases}$$

Argumentaremos por indução em r que $[\tilde{h}(r), \tilde{b}(r)^{\gamma}]$, visto como um mapa parcial do monóide $\mathcal{M}$ em H', tem um número finito de entradas em lugares cujos índices estão em $U^r = (\{00,10\}^*)\{u\}$ onde $u \in (\{01,11\}^*)$, $|u| = 2r$ e $U = (\{00,10\}^*)\{01,11\}$, além disso, essas entradas são iguais a $[h,b]$.

O caso $r = 1$ foi demonstrado no Teorema 4.3.3

Suponha por hipótese de indução que a afirmação seja válida para $r-1$, com $r \geq 1$. Então o termo $[\tilde{h}(r-1), \tilde{b}(r-1)^{\beta'}]$ de $[\tilde{h}(r), \tilde{b}(r)^{\gamma}]$ está em conformidade com a afirmação. Agora, se o conjugado $\alpha(0)^{\xi_0'\beta}$ é ativo, isto é, ξ_0' é uma unidade diádica, então o primeiro termo é $[\tilde{h}(r), \tilde{b}(r)^{\alpha(0)^{\xi_0'\beta}}] = e$ e

$$[\tilde{h}(r), \tilde{b}(r)^{\gamma}] = ((e, [\tilde{h}(r-1), \tilde{b}(r-1)^{\beta'}]), e).$$

Por outro lado, $[\tilde{h}(r), \tilde{b}(r)^{\alpha(0)^{\xi_0'\beta}}]$ é não-trivial se e somente se $l(\xi_0') \geq 1$, neste caso, repetimos o procedimento acima realizado para $[\tilde{h}(r), \tilde{b}(r)^{\gamma}]$. Se $\xi_0 \neq 0$ então $l(\xi_0) = s$ para algum s finito e então este procedimento termina após no máximo s passos.

Seja $N(r) = \langle [\widetilde{H}(r), \widetilde{H}(r)^{\gamma}]^{\lambda} \mid \gamma, \lambda \in \widehat{K(r)} \rangle$. Queremos mostrar que $N(r) = P(r) \times P(r)$, onde $P(r) = N(r) \times N(r-1)$, $N(0) = H'$ e $N(r) \lhd G$.

O caso $r = 1$ foi demonstrado no Teorema 4.3.3.

Assuma que a afirmação seja verdadeira para $r-1$, com $r \geq 1$ e que $[\tilde{h}(r), \tilde{b}(r)^{\gamma}]^{\lambda} \in N(r)$ é um elemento não trivial. Além disso, defina

$$\begin{aligned} \eta_i &= \delta_i + 2\eta_i', \quad \delta_i = 0, 1, \\ \lambda &= \alpha(0)^{\eta_0}\alpha(1)^{\eta_1} \dots \alpha(r)^{\eta_r}, \\ \zeta &= \alpha(1)^{\eta_1} \dots \alpha(r)^{\eta_r}. \end{aligned}$$

Então,

$$\zeta = (\zeta, \zeta')^x \quad \zeta' = \alpha(0)^{\eta_1}\alpha(1)^{\eta_2}\ldots\alpha(r-1)^{\eta_r},$$

e λ é ativo se e somente se $\delta_0 = 1$. Reutilizando a notação acima, temos

$$\begin{aligned}[\tilde{h}(r),\tilde{b}(r)^{\gamma}]^{\lambda} =& ((([\tilde{h}(r),\tilde{b}(r)^{\alpha(0)^{\xi_0'}\beta}],[\tilde{h}(r-1),\tilde{b}(r-1)^{\beta'}]),e)^{\lambda}\\ =& \begin{cases} ((([\tilde{h}(r),\tilde{b}(r)^{\alpha(0)^{\xi_0'}\beta}]^{\eta_0'\zeta},[\tilde{h}(r-1),\tilde{b}(r-1)^{\beta'}]^{\eta'}),e), & \text{se } \delta_0 = 0\\ (e,([\tilde{h}(r),\tilde{b}(r)^{\alpha(0)^{\xi_0'}\beta}]^{\eta_0'\zeta},[\tilde{h}(r-1),\tilde{b}(r-1)^{\beta'}]^{\eta'})), & \text{se } \delta_0 = 1.\end{cases}\end{aligned}$$

Assim, de $([\tilde{h}(r),\tilde{b}(r)^{\alpha(0)^{\xi_0'}\beta}]^{\eta_0'\zeta},[\tilde{h}(r-1),\tilde{b}(r-1)^{\beta'}]^{\eta'}) \in P(r) = N(r)\times N(r-1)$ segue que $[\tilde{h}(r),\tilde{b}(r)^{\gamma}]^{\lambda} \in P(r)\times P(r)$.

O argumento para mostrar que $G/N(r)$ é isomorfo a $H \wr \widehat{K(r)}$ é análogo ao utilizado no Teorema 4.3.3. Os representantes das classes laterais de $N(r)$ em G podem ser tomados como expressões da forma

$$w = (\tilde{h}_1(r)^{\gamma_1}\ldots\tilde{h}_s(r)^{\gamma_s})(\tilde{b}_1(r)^{\mu_1}\ldots\tilde{b}_t(r)^{\mu_s})(\alpha(0)^{\xi_0}\ldots\alpha(r-1)^{\xi_{r-1}}),$$

onde $\gamma_1\ldots\gamma_s$ são elementos inativos de $\widehat{K(r)}$ e $\mu_1,\ldots,\mu_t$ são elementos ativos de $\widehat{K(r)}$.

Diremos que w está na forma semi-normal quando w estiver em uma forma tendo $(\sum\{l(\xi_i) \mid i \geq 0\}, s+t)$ minimal.

Suponha $w \in N(r)$ como acima, na forma semi-normal e $w \neq e$. Como $N(r)$ estabiliza o primeiro nível da árvore então $l(\xi) > 0$. Assim, de $N(r) = P(r)\times P(r)$, segue que $w = (u,v)$ onde $u,v \in P(r)$. Da mesma forma, como $P(r) = N(r)\times N(r-1)$, considerando a minimalidade de w, obtemos a forma $w = \tilde{h}(r) = ((\tilde{h}(r),\tilde{h}(r-1)),e)$, que é uma contradição, pois os elementos de $N(r)$ tem suporte finito enquanto os elementos de $\widetilde{H}(r)$ tem suporte infinito. Agora, estabeleceremos o isomorfismo entre $G/N(r)$ e $H \wr \widehat{K(r)}$. Tome

$$w = (\tilde{h}_1(r)^{\gamma_1}\ldots\tilde{h}_s(r)^{\gamma_s})(\tilde{b}_1(r)^{\mu_1}\ldots\tilde{b}_t(r)^{\mu_s})(\alpha(0)^{\xi_0}\ldots\alpha(r-1)^{\xi_{r-1}})$$

assim como acima, e por simplificação, faça

$$w = (\tilde{h}_1(r)^{\lambda_1}\ldots\tilde{h}_s(r)^{\lambda_n})\widehat{\alpha},$$

onde $\lambda_1,\ldots,\lambda_n \in \widehat{K(r)}$ e $s+t = n$.

Considere agora a aplicação

$$\begin{aligned} \varphi : G/N(r) &\longrightarrow H \wr \widehat{K(r)} \\ \prod_{i=1}^{n} \tilde{h}_i(r)^{\lambda_i} \widehat{\alpha} N(r) &\longmapsto (\prod_{i=1}^{n} (\ldots, e, h_i, e, \ldots)^{\lambda_i}, \widehat{\alpha}). \end{aligned}$$

A aplicação φ é um homomorfismo, pois

$$\begin{aligned} (\prod_{i=1}^{n} \tilde{h}_i(r)^{\lambda_i} \widehat{\alpha} \prod_{i=1}^{n} \tilde{k}_i(r)^{\eta_i} \widehat{\beta} N(r))\varphi =& (\prod_{i=1}^{n} \tilde{h}_i(r)^{\lambda_i} \prod_{i=1}^{n} \tilde{k}_i(r)^{\eta_i + (\widehat{\alpha})^{-1}} \widehat{\alpha}\widehat{\beta} N(r))\varphi \\ =& (\prod_{i=1}^{n} (\ldots, e, h_i, e, \ldots)^{\lambda_i} \prod_{i=1}^{n} (\ldots, e, k_i, e, \ldots)^{\eta_i (\widehat{\alpha})^{-1}}, \widehat{\alpha}\widehat{\beta}) \\ =& (\prod_{i=1}^{n} (\ldots, e, h_i, e, \ldots)^{\lambda_i}, e)(\prod_{i=1}^{n} (\ldots, e, k_i, e, \ldots)^{\eta_i (\widehat{\alpha})^{-1}}, \widehat{\alpha}\widehat{\beta}) \\ =& (\prod_{i=1}^{n} (\ldots, e, h_i, e, \ldots)^{\lambda_i}, \widehat{\alpha})(\prod_{i=1}^{n} (\ldots, e, k_i, e, \ldots)^{\eta_i}, \widehat{\beta}) \\ =& (\prod_{i=1}^{n} \tilde{h}_i(r)^{\lambda_i} \widehat{\alpha} N(r))\varphi (\prod_{i=1}^{n} \tilde{k}_i(r)^{\eta_i} \widehat{\beta} N(r))\varphi. \end{aligned}$$

A aplicação é injetiva visto que $(\prod_{i=1}^{n} \tilde{h}_i(r)^{\lambda_i} \widehat{\alpha} N(r))\varphi = ((\ldots, e, e, e, \ldots), e)$ se, e somente se, $\tilde{h}_i(r)^{\lambda_i} = e$ para todo $i \in \{1, \ldots, n\}$ e $\widehat{\alpha} = e$.

Finalmente, φ é sobrejetiva visto que dado $(\prod_{i=1}^{n} (\ldots, e, h_n, e, \ldots)^{\lambda_n}, \widehat{\alpha}) \in H \wr \widehat{K(r)}$, existe $\prod_{i=1}^{n} \tilde{h}_i^{\lambda_i} \widehat{\alpha} N(r) \in G/N(r)$ tal que $(\prod_{i=1}^{n} \tilde{h}_i^{\lambda_i} \widehat{\alpha} N(r))\varphi = (\prod_{i=1}^{n} (\ldots, e, h_i, e, \ldots)^{\lambda_i}, \widehat{\alpha})$.

□

Corolário 4.6.3. O grupo $\Lambda(r)$ normaliza o produto tree-wreath $H \,\bar{\wr}\, \widehat{K(r)}$.

Demonstração. Primeiro, observe que para $\tilde{h} = ((\tilde{h}, h), e)$ e $\lambda_\xi = ((\lambda_\xi, e), (\lambda_\xi \alpha^{(\varepsilon-1)/2}, e))$, temos $\tilde{h}^{\lambda_\varepsilon} = ((\tilde{h}^{\lambda_\varepsilon}, h), e) = \tilde{h}$, assim, λ_ε centraliza $\widetilde{H}$. Suponha por hipótese de indução que $\Lambda(r-1)$ centraliza $\widetilde{H}$, então

$$\begin{aligned} \tilde{h}^{\lambda_\varepsilon(r)} &= ((\tilde{h}^{\lambda_\varepsilon(r)}, h^{\lambda_\varepsilon(r-1)}), e) \\ &= ((\tilde{h}^{\lambda_\varepsilon(r)}, h), e) \\ &= ((\tilde{h}, h), e) \\ &= \tilde{h}, \end{aligned}$$

logo, $\Lambda(r)$ centraliza $\widetilde{H}$.

Suponha agora que $\Lambda(r)$ centraliza $\widetilde{H}(r-1)$, então

$$\begin{aligned}\tilde{h}(r)^{\lambda_\varepsilon(r)} &= ((\tilde{h}(r)^{\lambda_\varepsilon(r)}, \tilde{h}(r-1)^{\lambda_\varepsilon(r-1)}), e)\\ &= ((\tilde{h}^{\lambda_\varepsilon(r)}, \tilde{h}(r-1)), e)\\ &= ((\tilde{h}(r), \tilde{h}(r-1)), e)\\ &= \tilde{h}(r),\end{aligned}$$

portanto, $\Lambda(r)$ centraliza $\widetilde{H}(r)$. Vimos na Proposição 4.5.2 que $\Lambda(r)$ normaliza $\widehat{K(r)}$, então $\Lambda(r)$ normaliza o grupo $\langle \widetilde{H}(r), \widehat{K(r)} \rangle$. □

Finalizaremos com resultado a seguir que, através da Imersão de Magnus e do Teorema 4.6.2, exibe uma representação fiel do grupo metabeliano livre de posto r como um grupo de automorfismos de estado-finito.

Corolário 4.6.4. O grupo metabeliano livre $\mathbb{M}$ de posto r tem uma representação fiel como um grupo de automorfismos de estado-finito.

Demonstração. Sejam $F = \langle x_1, \ldots, x_r \rangle$ um grupo livre de posto r, $H = \langle h_1, \ldots, h_r \rangle$, $K = \langle \alpha(0), \ldots, \alpha(r-1) \rangle$ dois grupos abelianos livres de posto r com estado-finito, onde $F/F' \simeq K$ e $F/F'' \simeq \mathbb{M}$. Utilizando a *Imersão de Magnus* (Teorema 2.2.6), vimos que a imersão do grupo metabeliano $\mathbb{M}$ é dada por $x_iF'' \mapsto (h_i, (x_i)F')$. Utilizando a correspondência.

$$(h_i, x_iF') \mapsto (f(h_i), k_i)$$

onde $f(x_i) \in H^{(K)}$, concluímos que $\mathbb{M}$ é isomorfo ao subgrupo $\langle (f(h_1), k_1), \ldots, (f(h_r), k_r) \rangle$ de $H \wr K$.

Além disso, sob as notações do teorema anterior, de $\widetilde{H}(r)$ abeliano segue que $N(r)$ é trivial, assim,

$$\langle \widetilde{H}(r), K(r) \rangle \simeq H \wr K(r),$$

Como $\langle \widetilde{H}(r), K(r) \rangle$ tem estado-finito, segue que $H \wr K(r)$ possui uma representação fiel no grupo de automorfismos de estado-finito $\mathcal{F}(0,1)$, assim, concluímos a prova visto que $\langle (f(x_1), y_1), \ldots, (f(h_r), y_r) \rangle \leq H \wr K$. □

Bibliografia

[1] L. Bartholdi and P. Silva. Groups defined by automata. 12 2010.

[2] A. Bondy and U. Murty. *Graph theory*. Graduate texts in mathematics 244. Springer, 3rd corrected printing. edition, 2008.

[3] A. Brunner and S. Sidki. Wreath operations in the group of automorphisms of the binary tree. *Journal of Algebra*, 257:51–64, 11 2002.

[4] S. Eilenberg. *Automata, languages, and machines*, volume Volume A of *Pure and applied mathematics a series of monographs and text books, 58 [i.e. 59]*. Academic Press, 1974.

[5] A. Gonçalves. *Introdução à álgebra*. Projeto Euclides. Instituto de Matemática Pura e Aplicada, 1979.

[6] K. W. Gruenberg. Residual properties of infinite soluble groups. *Proceedings of the London Mathematical Society*, s3-7(1):29–62, 1957.

[7] D. L. Johnson. *Presentations of Groups*. London Mathematical Society Student Texts. Cambridge University Press, 2nd edition, 1997.

[8] J. Munkres. *Topology*. Prentice Hall, Inc, 2nd edition, 2000.

[9] O. Ore. *Theory of graphs*. Colloquium Publications. American Mathematical Society, 3rd edition, 1962.

[10] V. N. Remeslennikov and V. G. Sokolov. Some properties of a magnus embedding. *Algebra and Logic*, 9(5):342–349, Sep 1970.

[11] L. Ribes and P. Zalesskii. *Profinite groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge A Series of Modern Surveys in Mathematics. Springer-Verlag Berlin Heidelberg, 2nd edition, 2010.

[12] D. J. S. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics 80. Springer-Verlag New York, 2nd edition, 1996.

[13] J. J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics 148. Springer-Verlag New York, 4th edition, 1995.

[14] S. Sidki. Automorphisms of one-rooted trees: Growth, circuit structure, and acyclicity. *Journal of Mathematical Sciences*, 100(1):1925–1943, Jun 2000.

[15] J. Wilson. Free subgroups in groups with few relators. *L'Enseignement Mathématique. IIe Série*, 56, 01 2010.

Índice