Paula Macêdo Lins de Araujo

Produtos Entrelaçados Finitamente Apresentáveis

CAMPINAS
2014

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

PAULA MACÊDO LINS DE ARAUJO

PRODUTOS ENTRELAÇADOS FINITAMENTE APRESENTÁVEIS

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra em matemática.

Orientadora: Dessislava Hristova Kochloukova

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELA ALUNA PAULA MACÊDO LINS DE ARAUJO, E ORIENTADA PELA PROFA. DRA. DESSISLAVA HRISTOVA KOCHLOUKOVA.

Assinatura da Orientadora

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

Araujo, Paula Macêdo Lins de, 1989-
Ar15p Produtos entrelaçados finitamente apresentáveis / Paula Macêdo Lins de Araujo. – Campinas, SP : [s.n.], 2014.

Orientador: Dessislava Hristova Kochloukova.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos grupos. 2. Grupos livres. 3. Teoria dos grafos. I. Kochloukova, Dessislava Hristova,1970-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Finitely presented wreath products
Palavras-chave em inglês:
Group theory
Free groups
Graph theory
Área de concentração: Matemática
Titulação: Mestra em Matemática
Banca examinadora:
Dessislava Hristova Kochloukova [Orientador]
Said Najati Sidki
Vitor de Oliveira Ferreira
Data de defesa: 15-08-2014
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 15 de agosto de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof.(a). Dr(a). DESSISLAVA HRISTOVA KOCHLOUKOVA

Prof.(a). Dr(a). SAID NAJATI SIDKI

Prof.(a). Dr(a). VITOR DE OLIVEIRA FERREIRA

Abstract

We study a result in the paper *Finitely Presented Wreath Products And Double Coset Decompositions* by Y. de Cornulier, which asserts that a wreath product $W \wr_X G$ is finitely presented if and only if the following conditions hold:

i. W and G are finitely presented;

ii. G acts on X with finitely generated stabilizers;

iii. G acts diagonally on $X \times X$ with finitely many orbits.

Keywords: Group theory, finitely presented groups, wreath products, free product of groups.

Resumo

Estudamos um resultado que se encontra no artigo *Finitely Presented Wreath Products And Double Coset Decompositions* de Y. de Cornulier que afirma que o produto entrelaçado $W \wr_X G$ é finitamente apresentável se, e somente se, as seguintes condições são satisfeitas:

i. W e G são finitamente apresentáveis;

ii. G age sobre X com estabilizadores finitamente gerados;

iii. G age diagonalmente sobre $X \times X$ com finitas órbitas.

Palavras-chave: Teoria dos grupos, grupos finitamente apresentáveis, produtos entrelaçados, produto livre de grupos.

Conteúdo

À minha família
e ao Yuri.

Agradecimentos

Inicio os meus agradecimentos pelos meus pais, que sempre estiveram ao meu lado e me ensinaram a lutar para alcançar meus sonhos. Em particular, agradeço à minha mãe por ser sempre meu apoio, uma grande amiga e um exemplo de coragem e força. Ao meu pai, por todos os valores e conversas engrandecedoras. Agradeço a ambos por serem um exemplo a ser seguido e por me ensinarem as coisas mais importantes da vida. À Dani, por ser minha grande companheira e amiga para toda a vida e por toda a ajuda e principalmente pelas piadas bobas. À Lídia, por todo o apoio, bons conselhos e por toda a bondade contagiante que vem melhorando o meu mundo.

Agradeço à professora Dessislava pela paciência, por todos os conselhos, pelo enorme compromisso e por toda a ajuda a mim prestada. Agradeço também pelo exemplo de profissional a ser seguido.

Aos Professores Said Sidki, Vitor Ferreira, Adriano Moura e Lucio Centrone, membros da Banca Examinadora, por disporem de seu tempo e conhecimento para avaliar e contribuir com este trabalho. Agradeço em especial aos comentários e sugestões feitos pelos professores Said Sidki e Vitor Ferreira, pois estes contribuíram bastante com o conteúdo e a apresentação deste trabalho.

Gostaria de gradecer a todos os amigos que fiz durante esse período, pelos bons momentos de descontração, assim como por toda a ajuda nos estudos. Em particular, gostaria de agradecer aos meus queridos Matheus e Rafaela, por me fazerem me sentir em casa num lugar desconhecido e por todo o apoio nos momentos de maiores dificuldades.

Aos meus caros Jatobá e Yuri, por todos os bons e maus momentos que fizeram com que chegássemos até aqui. Pelas muitas horas de estudos, pelos ensinamentos de vida e, principalmente, pela paciência nas vésperas de prova.

A todos os professores e funcionários do IMECC, na Unicamp. Em particular, agradeço ao professor Lucio Centrone, pela matéria em Teoria de Grupos lecionada. Foi uma grande ajuda na minha decisão de área a ser seguida.

Agradeço também aos professores que ajudaram em minha formação como um todo. Em especial, ao Professor Mauro Rabelo, por todos os ensinamentos, matemáticos e de vida, também pela paciência, pelos conselhos e por toda a ajuda. Ao professor Celius Magalhães, por toda a experiência proporcionada nas monitorias, pelas risadas e lições de vida.

Aos professores Leandro Cioletti e Luís Henrique de Miranda, por todos os conselhos, muitos deles me trouxeram até aqui. Ao professor Nigel Pitt, pelos conselhos e “puxões de orelha” que pesaram bastante na hora de tomar decisões, garantindo sempre bons resultados.

À professora Aline Pinto, pelas matérias de álgebra lecionadas, dentre elas, aquela que despertou meu interesse na álgebra e me fez me encontrar na matemática. Agradeço também pela experiência nas monitorias e pelos conselhos.

Agradeço ao Emilio Brazil, por compartilhar a beleza da matemática comigo lá no início, influenciando bastante na minha escolha acadêmica.

Ao Yuri, por ter desempenhado um papel fundamental na minha vida desde sempre. Acima de tudo, agradeço por ser sempre meu melhor amigo e a melhor companhia que alguém poderia ter. Agradeço por toda a ajuda matemática, que também foi fundamental para o desenvolvimento desse trabalho e pelo espírito de aventura que nos trouxe para uma nova cidade para encontrar novos desafios.

Agradeço ao CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) por possibilitar a dedicação exclusiva a este trabalho através do apoio financeiro.

Introdução

Neste trabalho, estudamos um resultado que se encontra no artigo *Finitely Presented Wreath Products And Double Coset Decompositions* de Yves de Cornulier sobre produtos entrelaçados finitamente apresentáveis.

No primeiro capítulo, recordamos conceitos básicos de teoria de grupos. Tal capítulo segue o livro de J. J. Rotman – *An Introduction To The Theory Of Groups*.

O segundo capítulo contém conceitos de teoria combinatória de grupos como grupos livres e produtos livres. Nesse capítulo, seguimos o livro *Combinatorial Group Theory: A Topological Approach* de D. E. Cohen. Também introduzimos os conceitos e mostramos alguns resultados de grupos finitamente apresentáveis por meio de geradores e relações, bem como o Teorema de Schreier usando métodos topológicos, tais como recobrimentos de grafos.

O terceiro capítulo contém o resultado de Yves de Cornulier que classifica os produtos entrelaçados finitamente apresentáveis do tipo $W \wr_X G$, por meio de propriedades dos grupos W e G e da ação de G sobre X (Cf. 3.3.5, 3.3.25). O teorema principal estudado afirma que o produto entrelaçado $W \wr_X G$ é finitamente apresentável se, e somente se, G e W são finitamente apresentáveis, a ação de G em X tem estabilizadores finitamente gerados e a ação diagonal de G em $X \times X$ tem finitas órbitas. Não é difícil mostrar que essas três condições implicam que $W \wr_X G$ é finitamente apresentável. Entretanto, mostrar que tais condições são necessárias para que $W \wr_X G$ seja finitamente apresentável é bem mais complicado e envolve a utilização de uma ferramenta chamada produto grafo de grupos.

Na prática, é muito difícil encontrar grupos G e G-conjuntos X satisfazendo as condições do resultado principal. No último capítulo, estudamos o caso particular de quando G é o Grupo de Richard Thompson F e X é o conjunto $\{\frac{a}{2^b}\}_{a,b\in\mathbb{N}} \cap (0,1)$ e concluímos que $W \wr_X F$ é finitamente apresentável sempre que W for um grupo não trivial finitamente apresentável. Mais exemplos podem ser encontrados no artigo [3, Seção 3.1], tais como Grupos de Houghton e alguns grupos de 3-variedades.

Capítulo 1

Propriedades Básicas de Grupos

1.1 Grupos, Subgrupos e Classes Laterais

Neste capítulo vamos recordar propriedades básicas de grupos seguindo o livro [8]. Alguns resultados podem ser encontrados em [7] e [4].

Definição 1.1.1. Um *grupo* G é um conjunto não vazio munido com uma operação associativa $\cdot : G \times G \to G$ satisfazendo as seguintes condições:

- Existe um elemento e em G satisfazendo $g \cdot e = e \cdot g = g$, para todo $g \in G$
- Dado $g \in G$, existe um elemento h de G tal que $g \cdot h = h \cdot g = e$

O elemento e é dito o *elemento neutro de* G e também é denotado por 1 ou por 1_G, quando for necessário explicitar de que grupo esse é o elemento neutro. O elemento $h \in G$ tal que $g \cdot h = h \cdot g = e$ é o *elemento inverso de* g e será denotado por g^{-1}. Muitas vezes, escrevemos $(G, \cdot)$ para indicar que o conjunto G é grupo com a operação $\cdot$. Um grupo G é dito *abeliano* se vale $g \cdot h = h \cdot g$, $\forall g, h \in G$.

Por simplicidade, escreveremos apenas gh em vez de $g \cdot h$.

Exemplo 1.1.2. Dado um conjunto X arbitrário, o conjunto

$$\mathbb{Z}^X = \{f : X \to \mathbb{Z} : f \text{ é } \textit{função}\}$$

é um grupo com a operação $+$, definida por $(\alpha + \beta)(x) = \alpha(x) + \beta(x)$, para $\alpha, \beta \in \mathbb{Z}^X$ e $x \in X$.

Com efeito, a soma $\alpha(x) + \beta(x)$ é a soma usual em $\mathbb{Z}$ e por isso é associativa (e comutativa). Denote por $\mathbf{0}$ a função em $\mathbb{Z}^X$ constante e igual a zero. Tem-se que $(\alpha + \mathbf{0})(x) = \alpha(x) + 0 = \alpha(x)$, para todo $\alpha \in \mathbb{Z}^X$. Assim, $\mathbf{0}$ é elemento neutro de $\mathbb{Z}^X$. Dado $\alpha \in \mathbb{Z}^X$, defina $-\alpha(x) = -(\alpha(x))$. Tem-se que $(-\alpha + \alpha)(x) = -(\alpha(x)) + \alpha(x) = 0$, para cada $x \in X$. Logo, $(-\alpha + \alpha)(x) = \mathbf{0}(x)$. Assim, $-\alpha$ é o inverso de α.

Exemplo 1.1.3. Denotaremos por S_n o conjunto de todas as bijeções do tipo $\delta : \{1, \ldots, n\} \to \{1, \ldots, n\}$. A composição de funções é associativa e, além disso, a composição de bijeções é uma bijeção. Assim, é natural supor que $(S_n, \circ)$ seja um grupo.

De fato, a identidade $i(m) = m$, $\forall m \in \{1, \ldots, n\}$ é o elemento neutro de S_n e, para cada $\delta \in S_n$, como δ é bijeção, existe $\delta^{-1} : \{1, \cdots, n\} \to \{1, \ldots, n\}$ tal que $\delta \circ \delta^{-1} = i = \delta^{-1} \circ \delta$. Tal grupo é dito o *grupo de permutações de ordem n*.

De modo geral, dado um grupo X, podemos definir S_X como o grupo das permutações dos elementos de X, ou seja, das bijeções $\delta : X \to X$.

Chamamos de transposição um elemento de S_n que faz $p \mapsto q$, $q \mapsto p$ para dois números distintos p e q e mapeia os demais números em si mesmos. Todo $\sigma \in S_n$ pode ser escrito como composição de transposições. Essa composição não é única, mas tem uma propriedade interessante: os números de transposições das decomposições de σ sempre têm a mesma paridade. Esse é um fato bastante conhecido, mas que não será demonstrado aqui. Por causa de tal resultado, podemos separar os elementos de S_n em dois conjuntos: o das permutações pares e o das permutações ímpares, onde uma permutação é par se as suas decomposições em composições de transposições têm sempre número par de termos e ímpar caso contrário. O conjunto das permutações pares é, na verdade um grupo, que é chamado *grupo alternado* de ordem n e denotado por A_n.

Definição 1.1.4. Um subconjunto não vazio S de um grupo G é dito um *subgrupo* de G se S satisfaz:

- Para cada $s \in S$, tem-se que $s^{-1} \in S$;
- Se $s, t \in S$ então $st \in S$.

É importante observar que S é subgrupo de G se, e somente se, S é um grupo com a operação induzida por G. Escrevemos $S \leq G$ para denotar que S é subgrupo de G.

Uma *potência* de um elemento a de um grupo G é um elemento da forma a^n, onde $a^0 = 1$, $a^1 = a$, $a^n = a \cdot a^{n-1}$ e $a^{-n} = (a^{-1})^n$, onde n é um inteiro positivo. Dados um grupo G e um elemento g de G, denotamos por $\langle g \rangle$ o subgrupo de G formado por todas as potências de g. Esse subgrupo é chamado *subgrupo cíclico gerado por g*. Dizemos que o grupo G é *cíclico* se $G = \langle g \rangle$ para algum $g \in G$. Definimos a *ordem* de um elemento a de G como sendo o número de elementos de $\langle a \rangle$, ou seja, $|\langle a \rangle|$. Um grupo tal que todos os seus elementos, exceto pela unidade, têm ordem finita é dito *livre de torção.*

Dados G um grupo e X um subconjunto qualquer de G, o menor subgrupo de G que contém X será denotado por $\langle X \rangle$. Esse subgrupo é dito um *subgrupo de G gerado por X*. Nesse caso, dizemos que X gera $\langle X \rangle$. Dizemos que um grupo é *finitamente gerado* quando é gerado por um conjunto finito.

Exemplo 1.1.5. O grupo Diedral $2n$, denotado por D_{2n}, é o grupo das simetrias de um polígono regular de n lados, incluindo rotações e reflexões. Denotaremos por r a rotação por $\frac{2\pi}{n}$ e por f a reflexão do polígono. Cada simetria de um polígono regular pode ser descrita por rotações e reflexões do mesmo. Veja que duas reflexões ou n rotações fazem com que o polígono volte a sua posição original. Assim, $r^n = e$ e $f^2 = e$, onde e é o elemento neutro, ou seja, o polígono na posição original. Além disso, devemos ter que $(rf)^2 = e$, ou seja, $rf = (rf)^{-1}$, pois $(rf)^{-1} = f^{-1}r^{-1} = fr^{n-1}$ e, de fato, $(rf)(fr^{n-1}) = rffr^{n-1} = r^n = e$. Tem-se que $D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, f, rf, \ldots, r^{n-1}f\}$, ou seja, $D_{2n} = \langle r, f\rangle$.

O grupo Diedral infinito D_∞ é como o grupo dado acima, porém, consideramos um "polígono com infinitos lados". Ou seja, um número finito de rotações não fazem com que o polígono volte para a sua posição original. Devemos então ter que $f^2 = e$ e $(rf)^2 = e$, porém, não existe um número n tal que $r^n = e$. Tem-se que $D_\infty = \langle r, f\rangle$ é finitamente gerado, embora seja um grupo infinito.

Exemplo 1.1.6. O grupo de Heisenberg em $\mathbb{Z}$ de ordem 3, que será denotado por $\mathbb{H}_3(\mathbb{Z})$, é o grupo das matrizes da forma

$$\begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

onde a, b e c são inteiros. Aqui a operação considerada é a multiplicação de matrizes. Tome

$$X = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; Y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \; Z = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Veja que

$$X^a = \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; Y^b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \; Z^c = \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Desse modo, podemos escrever cada elemento de $\mathbb{H}_3(\mathbb{Z})$ como o produto de potências de X, Y e Z. Ou seja, $\{X, Y, Z\}$ é um gerador de $\mathbb{H}_3(\mathbb{Z})$. Isso nos diz que tal grupo é finitamente gerado.

Vale que $XYX^{-1}Y^{-1} = Z$. Podemos então simplificar o gerador desse grupo: $\mathbb{H}_3(\mathbb{Z}) = \langle X, Y\rangle$.

Exemplo 1.1.7. Dados dois grupos G_1 e G_2, o produto direto $G_1 \times G_2 = \{(g_1, g_2) : \; g_1 \in G_1, \; g_2 \in G_2\}$ é grupo com a operação $\cdot$ definida por $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$. De fato, se 1_{G_1} e 1_{G_2} denotam, respectivamente, a identidade de G_1 e de G_2, então $(1_{G_1}, 1_{G_2})$ é a identidade de $G_1 \times G_2$. Como as operações em G_1 e G_2 são associativas, $\cdot$ é associativa e, pela escolha dessa operação, tem-se que $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

Veja que G_1 e G_2 podem ser vistos como subgrupos de $G_1 \times G_2$, basta tomar as correspondências $g_2 \mapsto (1_{G_1}, g_2), \forall g_2 \in G_2$ e $g_1 \mapsto (g_1, 1_{G_2}), \forall g_1 \in G_1$. Vendo dessa forma, todo elemento de $G_1 \times G_2$ é um produto de um elemento de G_1 por um de G_2, pois $(g_1, g_2) = (g_1, 1_{G_1}) \cdot (1_{G_2}, g_2)$. Por esse motivo, se $G_1 = \langle X_1\rangle$ e $G_2 = \langle X_2\rangle$, então $G_1 \times G_2$ pode ser visto como o grupo $\langle X_1 \cup X_2\rangle$.

De modo geral, se $\{G_\lambda\}_{\lambda\in\Lambda}$ é uma família de grupos, então o produto direto $\times_{\lambda\in\Lambda} G_\lambda$ é grupo com a operação $\cdot$ dada por $(g_\lambda)_{\lambda\in\Lambda} \cdot (h_\lambda)_{\lambda\in\Lambda} = (g_\lambda h_\lambda)_{\lambda\in\Lambda}$. Aqui, também é possível considerar cada

G_λ como um subconjunto desse produto direto, basta fazer a identificação $g_{\bar{\lambda}} \mapsto (x_\lambda)_{\lambda\in\Lambda}$, onde $x_{\bar{\lambda}} = g_{\bar{\lambda}}$ e $x_\lambda = 1$, se $\lambda \neq \bar{\lambda}$.

Em especial, se Λ é finito e $G_\lambda = \langle X_\lambda \rangle$, então $\times_{\lambda\in\Lambda} G_\lambda = \langle \bigcup_{\lambda\in\Lambda} X_\lambda \rangle$, por um argumento análogo ao dado acima.

Definição 1.1.8. Sejam S um subgrupo de G e $t \in G$. Uma *classe lateral à direita* de S em G é um subconjunto de G da forma

$$St = \{st : s \in S\}$$

e uma *classe lateral à esquerda* de S em G é um subconjunto da forma

$$tS = \{ts : s \in S\}$$

Mais geralmente, dados dois subconjuntos K e T do grupo G, podemos definir o conjunto $KT = \{kt : k \in K,\ t \in T\}$. Nesse caso, as classes laterais St e tS podem ser vistas como os casos em que $K = S,\ T = \{t\}$ e $K = \{t\},\ T = S$, respectivamente.

Sejam G um grupo e $H \leq G$. Tem-se que G é a união de todas as classes laterais à direita (ou à esquerda) de H. De fato, se $g \in G$, então $g \in Hg$, pois $1 \in H$. Além disso, $Hg \subset G, \forall g \in G$.

Enunciaremos a seguir um importante resultados sobre classes laterais. A demonstração pode ser encontrada em [8].

Lema 1.1.9. Dados um grupo G e $H \leq G$, vale que duas classes laterais à direita (ou à esquerda) de H em G ou coincidem ou são disjuntas.

Definimos o *índice* de um subgrupo H no grupo G como sendo o número de classes laterais à direita de H em G. Pode-se mostrar que o número de classes laterais à direita e à esquerda de H em G coincide, assim, também podemos definir o índice de H em G como o número de classes laterais à esquerda sem que o conceito seja dúbio. O índice de H em G será denotado por $[G : H]$.

Definição 1.1.10. Sejam G um grupo e H, K subgrupos de G, não necessariamente distintos. Uma *classe lateral dupla* de H, K em G é um conjunto da forma

$$HgK = \{hgk \ : \ h \in H \ , \ k \in K\}$$

onde $g \in G$.

Veja que, como no caso de classes laterais simples, G é a união de todas as classes laterais duplas. O argumento é análogo ao do caso anterior: Dado $g \in G$, tem-se que $g \in HgK$, pois $1 \in H$ e $1 \in K$. Por definição, $HgK \subset G, \forall g \in G$.

Lema 1.1.11. Sejam G um grupo e H, K subgrupos de G. Então duas classes laterais duplas HxK, HyK ou coincidem ou são disjuntas.

Demonstração. Ver [7, pp. 12] □

1.2 Homomorfismos

Definição 1.2.1. Sejam $(G, \otimes)$ e $(H, \oplus)$ grupos. Dizemos que a função $\varphi : G \to H$ é um *homomorfismo* se vale

$$\varphi(m \otimes n) = \varphi(m) \oplus f(n), \forall m, n \in G$$

Um homomorfismo injetor é dito um *monomorfismo*, enquanto um homomorfismo sobrejetor é dito um *epimorfismo*. Um homomorfismo bijetor é dito um *isomorfismo*. Se $\varphi : G \to H$ é isomorfismo, dizemos que G é isomorfo a H e escrevemos $G \simeq H$.

Proposição 1.2.2. Seja $\varphi : G \to H$ um homomorfismo. Então,

i. $\varphi(1_G) = 1_H$, onde 1_G e 1_H denotam os elementos neutros de G e de H, respectivamente;

ii. $\varphi(g^{-1}) = (\varphi(g))^{-1}$, $\forall g \in G$;

iii. Para cada $g \in G$, tem-se $\varphi(g^n) = (\varphi(g))^n$, para todo $n \in \mathbb{Z}$.

Demonstração. Ver [8] □

O caso especial em que o homomorfismo é da forma $\varphi : G \to G$, ou seja, tem o mesmo grupo como domínio e imagem, é dito *endomorfismo*. Quando o endomorfismo é bijetivo, ou seja, um isomorfismo do tipo $\varphi : G \to G$, dizemos que é um *automorfismo*.

Denotamos por $AutG$ o conjunto de todos os automorfismo no grupo G. Com a composição de funções, $AutG$ é um grupo, pois a composição de funções é associativa, todo automorfismo é invertível e a identidade em G $id_G : G \to G$ é o elemento neutro.

1.3 Subgrupos Normais e Grupos Quociente

Definição 1.3.1. Dado um grupo G, dizemos que um subgrupo $N \leq G$ é um *subgrupo normal* se $gNg^{-1} = N, \forall g \in G$ e denotamos $N \lhd G$.

Em particular, se o subgrupo N de G é tal que $gNg^{-1} \subset N, \forall g \in G$, então $N \lhd G$. De fato, basta tomar $g^{-1} \in G$ no lugar de g obtendo-se $g^{-1}Ng \subset N$, ou seja, $N \subset gNg^{-1}$.

Exemplo 1.3.2. Seja $\varphi : G \to H$ um homomorfismo de grupos. O núcleo $\ker \varphi$ de φ, dado por $\ker \varphi = \{g \in G : \varphi(g) = 1\}$, é um exemplo de subgrupo normal de G.

Veja que, se $N \lhd G$, então $gN = Ng, \forall g \in G$. Assim, quando nos referimos a classes laterais de subgrupos normais, não precisamos especificar se é uma classe lateral à direita ou à esquerda.

Definição 1.3.3. Dados um grupo G e um subconjunto S de G, dizemos que o menor subgrupo normal de G contendo S é o *fecho normal* de S em G e o denotamos por $\langle S \rangle^G$

Teorema 1.3.4. Seja G um grupo. Se $N \lhd G$, então o conjunto de todas as classes laterais de N em G é um grupo de ordem $[G : N]$ com a operação $NaNb = Nab$.

Demonstração. Ver [8]. □

Definição 1.3.5. O grupo dado pelo teorema anterior é dito o *grupo quociente de G por N* e é denotado por G/N ou $\frac{G}{N}$.

Definição 1.3.6. Dados um grupo G e um subgrupo normal H, definimos a *projeção natural* (ou *canônica*) $\pi : G \to G/H$ por $\pi(g) = Hg$.

Corolário 1.3.7. Dados um grupo G e N um subgrupo normal do mesmo, tem-se que a aplicação natural $\pi : G \to G/N$ é um epimorfismo sobrejetivo cujo núcleo é N.

Demonstração. Para a primeira parte, veja que $\pi(ab) = Nab = NaNb = \pi(a)\pi(b)$. Agora, se $g \in \ker\pi$, então $\pi(g) = N$, ou seja, $g = g1^{-1} \in N$. Segue que $\ker\pi \subset N$. Por outro lado, se $n \in N$, então $\pi(n) = Nn = N$. Segue que $N = \ker\pi$. Finalmente, $Im\pi = \{gN : g \in G\} = G/N$. □

Como π é um epimorfismo, podemos nos referir a ele como *homomorfismo natural* (ou *canônico*) ou ainda por *epimorfismo natural* (ou *canônico*).

Proposição 1.3.8. Seja $f : G \to H$ um homomorfismo de grupos. Então, para todo epimorfismo $h : G \to K$ tal que $\ker(h) \subset \ker(f)$, existe um único homomorfismo $\phi : K \to H$ tal que $\phi \circ h = f$

Demonstração. Sejam $f : G \to H$ e $h : G \to K$ como na hipótese da proposição.

Dado $k \in K$, existe $g_k \in G$ tal que $h(g_k) = k$. Defina então $\phi : K \to H$ por $\phi(k) = f(g_k)$. Suponha que $h(g_1) = k$ e $h(g_2) = k$. Então, $h(g_1 g_2^{-1}) = 1_K$, ou seja, $g_1 g_2^{-1} \in \ker(h) \subset \ker(f)$. Consequentemente, $f(g_1) = f(g_2)$. Segue que ϕ está bem definida. Por construção, $\phi \circ h = g$ e é o único homomorfismo com tal propriedade.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "h"'] & H \\ K \arrow[ur, "\exists!\phi"'] & \end{tikzcd}$$

□

Corolário 1.3.9. Seja $f : G \to H$ um homomorfismo. Se subgrupo normal N de G está contido em $\ker(f)$, então existe um único homomorfismo $\phi : G/N \to H$ tal que $\phi(gN) = f(g), \forall g \in G$.

1.4 Série Derivada e Grupos Solúveis

Definição 1.4.1. Dados g, h elementos do grupo G, o *comutador* de g e h é definido por $[g, h] = ghg^{-1}h^{-1}$. O *Subgrupo Derivado* de G é o subgrupo de G gerado pelo conjunto de todos os comutadores. O subgrupo derivado é denotado por G', G^0 ou por $[G, G]$. De modo geral, dados subconjuntos X_1, X_2 de um grupo G, denotamos $[X_1, X_2] = \{[x_1, x_2] : \ x_1 \in X_1, \ x_2 \in X_2\}$.

Observe que, dados um homomorfismo de grupos $\varphi : G \to H$ e $g_1, g_2 \in G$, tem-se

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

Defina $G^0 = G$ e $G^n = [G^{n-1}, G^{n-1}], \forall n \in \mathbb{N}$. Os grupos G^n são ditos os n-ésimos grupos derivados de G. A *série derivada* de G é a série

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

Definição 1.4.2. Um grupo G é dito *solúvel* quando sua série derivada se estabiliza, ou seja, quando existe algum $n \in \mathbb{N}$ tal que $G^n = \{1\}$. O menor tal n é dito o *índice de solubilidade* de G.

Exemplo 1.4.3. Todo grupo G abeliano é solúvel com índice de solubilidade igual a 1, pois G é abeliano se, e somente se, o subgrupo comutador de G é trivial.

Proposição 1.4.4. Todo subgrupo de um grupo solúvel é também solúvel.

Demonstração. Sejam G um grupo solúvel e $H \leq G$. Então, como $H \subset G$, tem-se que $H^i \subset G^i, \forall i \in \mathbb{N}$. Existe $n \in \mathbb{N}$ tal que $G^n = \{1\}$, assim, $H^n \subset G^n = \{1\}$. Segue que $H^n = \{1\}$ e, portanto, H se estabiliza. $\square$

Proposição 1.4.5. Seja G um grupo solúvel. Se $\varphi : G \to H$ é um epimorfismo, então H é solúvel.

Demonstração. Defina φ^i como sendo a restrição de φ a G^i. Como φ é sobrejetiva, tem-se que $\varphi(G) = H$, desse modo, $\varphi(G^1) = \varphi([G, G]) = [\varphi(G), \varphi(G)] = [H, H] = H^1$. Assim, $\varphi^1 : G^1 \to H^1$ e é sobrejetiva. Indutivamente, vale que $\varphi^i : G^i \to H^i$ é sobrejetiva, para todo $i \in \mathbb{N}$. Por hipótese, existe $n \in \mathbb{N}$ tal que $G^n = \{1\}$. Assim, $H^n = \varphi(G^n) = \varphi(\{1\}) = \{1\}$. $\square$

Corolário 1.4.6. Todo quociente de um grupo solúvel é também solúvel.

Demonstração. Basta aplicar a proposição anterior à projeção canônica do grupo solúvel G no quociente desejado. $\square$

Proposição 1.4.7. Sejam G um grupo e $N \lhd G$. Se N e G/N são solúveis, então G é solúvel.

Demonstração. Existem $k, l \in \mathbb{N}$ tais que $N^k = \{1\}$ e $(G/N)^l = \{N\}$. Seja $\pi : G \to G/N$ a projeção canônica. Como π é epimorfismo, $\pi(G^1) = \pi([G, G]) = [G/N, G/N] = (G/N)^1$. Indutivamente, $\pi(G^i) = (G/N)^i$. Assim, a restrição de π a G^i é o epimorfismo $\pi_i : G^i \to (G/N)^i$. Em especial, $\pi_l(G^l) = (G/N)^l = \{N\}$. Assim, se $g \in G^l$, tem-se que $Ng = \pi_l(g) = N$, ou seja, $g \in N$. Segue que $G^l \subset N$. Consequentemente, $G^{l+1} = [G^l, G^l] \subset [N, N] = N^1$, $G^{l+2} \subset N^2$, etc. Em particular, $G^{l+k} \subset N^k = \{1\}$. Portanto, $G^{l+k} = \{1\}$. $\square$

1.5 Os Teoremas do Isomorfismo

Os Teoremas do Isomorfismo relacionam grupos normais, grupos quocientes e homomorfismos e são de grande importância no estudo da Teoria de Grupos. Nesta seção, veremos brevemente cada um deles.

Teorema 1.5.1. (O Primeiro Teorema do Isomorfismo) Dado um homomorfismo $\varphi : G \to H$, tem-se que $\ker\varphi \lhd G$ e que $G/\ker\varphi \simeq Im\varphi = \{\varphi(g) : \ g \in G\}$.

Demonstração. Escreva $K = Ker\varphi$ e defina $\delta : G/K \to Im\varphi$ por $\delta(Kg) = \varphi(g)$. Como δ é um isomorfismo entre G/K e $Im\varphi$, o resultado segue. $\square$

Teorema 1.5.2. (O Segundo Teorema do Isomorfismo) Seja G um grupo e sejam $N \lhd G$ e $H \leq G$. Então $N \cap H \lhd H$ e $H/(N \cap H) \simeq NH/N$.

Demonstração. Seja $\pi : G \to G/N$ o homomorfismo natural. Denote por $\tilde{\pi}$ a restrição $\pi|_H$. Veja que $\ker\tilde{\pi} = \{h \in H : \ \tilde{\pi}(h) = N\} = N \cap H$. Pelo Primeiro Teorema do Isomorfismo, segue que $N \cap H \lhd H$ e que $H/(N \cap H) \simeq Im\tilde{\pi}$. Agora, $Im\tilde{\pi} = \{\tilde{\pi}(h) : \ h \in H\} = \{Nh : \ h \in H\} = \{Nnh : \ h \in H, \ n \in N\} = NH/N$. $\square$

Teorema 1.5.3. (O Terceiro Teorema do Isomorfismo) Dados grupos $K \leq H \leq G$ tais que $H, K \lhd G$, tem-se que $H/K \lhd G/K$ e $(G/K)/(H/K) \simeq G/H$.

Demonstração. Defina $\phi : G/K \to G/H$ por $\phi(Kg) = Hg$. Tem-se que

$$\ker\phi = \{Kg \in G/K : \ \phi(Kg) = H\} = \{Kg \in G/K : \ g \in H\} = H/K$$

e $Im\phi = G/H$, pois ϕ é sobrejetiva. Pelo Teorema 1.5.1, $H/K \lhd G/K$ e $(G/K)/(H/K) \simeq G/H$. $\square$

Vejamos uma aplicação para tal teorema.

Definição 1.5.4. Um subgrupo H do grupo G é dito *maximal* quando $H \leq S \leq G$ implica que $S = H$ ou $S = G$. No caso em que H é normal, dizemos que ele é um *subgrupo normal maximal* quando $H \leq S \lhd G$ implica que $S = H$ ou $S = G$.

Corolário 1.5.5. Seja G um grupo. $H \lhd G$ é subgrupo normal maximal se, e somente se, G/H não tem subgrupos normais não triviais.

1.6 Ações de grupos

Definição 1.6.1. Dados um grupo G e um conjunto não vazio X, uma ação (à esquerda) de G em X é uma função que associa cada $g \in G$ a uma função $\phi_g : X \to X$ satisfazendo:

i. $\phi_1 = id_X$, ou seja, $\phi_1(x) = x, \forall x \in X$

ii. $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}, \forall g_1, g_2 \in G$

Nesse caso, dizemos que G age em X (à esquerda) e que X é um G-conjunto (à esquerda).

Por simplicidade, escreveremos apenas g no lugar de ϕ_g. Assim, $g \cdot x = \phi_g(x) \in X$. Sejam G e X como na definição acima. Os subgrupos de G

$$G_x = \{g \in G : g \cdot x = x\}, x \in X$$

são ditos *estabilizadores* de G, enquanto os conjuntos

$$G \cdot x = \{g \cdot x : g \in G\}, x \in X$$

são ditos *órbitas ou G-órbitas* de X.

Cada órbita em G é uma classe de equivalência da relação de equivalência $x \sim y$ quando $g \cdot x = y$ para algum $g \in G$. Consequentemente, duas órbitas ou são disjuntas ou coincidem. Além disso, $G = \bigcup_{x \in X} G \cdot x$, pois $1 \cdot x = x$, logo $x \in G \cdot x, \forall x \in X$. Denotamos o conjunto das G-órbitas de X por X/G.

Observação 1.6.2. Se G age em X, então G age diagonalmente em $X^2 = X \times X$, ou seja, G age sobre X^2 pela ação $g \cdot (x_1, x_2) = (g \cdot x_1, g \cdot x_2)$. Nesse caso, se $|X^2/G|$ é finito, então $|X/G|$ é finito. De fato, $|X/G| = |\{G \cdot x : \ x \in X\}| = |\{G \cdot (x, x) : \ x \in X\}| \leq |\{G \cdot (x_i, x_j) : \ x_i, x_j \in X\}| = |(X \times X)/G|$.

Definição 1.6.3. Uma ação de G no conjunto X é dita:

i. *transitiva* se, dados $x, y \in X$, existe $g \in G$ tal que $g \cdot x = y$, ou seja, se X é uma órbita de G;

ii. *livre* quando, dados $g_1, g_2 \in G$, tem-se que $g_1 = g_2$ sempre que $g_1 \cdot x = g_2 \cdot x$, para algum $x \in X$;

iii. *simplesmente transitiva* se a ação de G em X é simultaneamente transitiva e livre.

Exemplo 1.6.4. Seja G um grupo com subgrupo H. Podemos definir uma ação de G em G/H por $g \cdot \bar{g}H = (g\bar{g})H$. Tal ação é transitiva, pois, dados $g_1H, g_2H \in G/H$, tem-se que $g_3 = g_2 g_1^{-1}$ é um elemento de G tal que $g_3 \cdot g_1 H = g_2 H$. Vendo de outra forma, como $g \cdot H = gH$, existe apenas uma órbita de G em G/H, o que também nos mostra que tal ação é transitiva.

Proposição 1.6.5. Se G age transitivamente em X, então existe um subgrupo H de G tal que $X = G/H$.

Demonstração. Fixe $x_0 \in X$ e tome $H = G_{x_0}$, o estabilizador de G em x_0. Queremos encontrar uma bijeção entre G/H e X que respeite ambas as ações de G, ou seja, $\varphi : G/H \to X$ tal que, se $\varphi(\tilde{g}H) = x$, então vale que $\varphi(g \cdot (\tilde{g}H)) = g \cdot x$.

Defina $\varphi : G/H \to X$ por $\varphi(\tilde{g}H) = \tilde{g} \cdot x_0$. Se $g_1 H = g_2 H$, então $g_1^{-1} g_2 \in H$, ou seja, $(g_1^{-1} g_2) \cdot x_0 = x_0$. Logo, $g_1 \cdot x_0 = g_2 \cdot x_0$. Segue que φ está bem definida. Como $X = G \cdot x_0$, φ é sobrejetiva. Além disso, se $g_1 \cdot x_0 = g_2 \cdot x_0$ então $g_1^{-1} g_2 \in H$, logo, $g_1 H = g_2 H$.

Por fim, mostremos que φ respeita as ações de G em G/H e de G em X. Dado $x \in X$, existe $\bar{g} \in G$ tal que $\bar{g} \cdot x_0 = x$. Assim, $x = \varphi(\bar{g}H)$. Para cada $g \in G$, vale que $\varphi(g \cdot (\bar{g}H)) = \varphi((g\bar{g})H) = (g\bar{g}) \cdot x_0 = g \cdot (\bar{g} \cdot x_0) = g \cdot x$. $\square$

Proposição 1.6.6. Se G age em X, então X é a união disjunta $\bigcup_{i\in I} G/H_i$, onde $H_i = G_{x_i}$ e I é um conjunto contendo exatamente um representante de cada G-órbita de X.

Demonstração. Na proposição anterior, mostramos que $G \cdot x$ é isomorfo a G/G_x. Como $X = \bigcup_{i\in I} G \cdot x_i$, tem-se que $X = \bigcup_{i\in I} G/H_i$. Além disso, a relação $x \sim y$ se $y \in G \cdot x$ é uma relação de equivalência que tem como classes de equivalência as G-órbitas de X. Assim, duas tais órbitas ou são disjuntas ou coincidem. Segue que a união dada é disjunta. $\square$

Proposição 1.6.7. Seja G um grupo que age no conjunto X. Então, vale que $|G \cdot x| = [G : G_x], \forall x \in X$.

Demonstração. Dado $x \in X$, denote por $\mathscr{G}(x) = \{gG_x : \ g \in G\}$ e defina $\varphi : G \cdot x \to \mathscr{G}(x)$ por $\varphi(g \cdot x) = gG_x$. Veja que, se $g_1 \cdot x = g_2 \cdot x$, então $g_2^{-1}g_1 \cdot x = x$, ou seja, $g_2^{-1}g_1 \in G_x$. Assim, $g_1G_x = g_2G_x$. Segue que φ está bem definida. Se $g_1G_x = g_2G_x$, então $g_2^{-1}g_1 \in G_x$. Isso nos diz que $g_2^{-1}g_1 \cdot x = x$, ou seja, $g_1 \cdot x = g_2 \cdot x$. Segue que φ é injetiva. Mais ainda, φ é sobrejetiva pois, para cada $g \in G$, tem-se que $gG_x = \varphi(g \cdot x)$. Segue do fato de φ ser bijeção que $|G \cdot x| = |\mathscr{G}(x)| = [G : G_x]$. $\square$

Proposição 1.6.8. Sejam G um grupo e X um G-conjunto. Então, para cada $x \in X$, vale que $|G \cdot x||G_x| = |G|$.

Demonstração. Seja $\mathscr{S} = \{G_xg : \ g \in G\}$. Defina $\varphi : G \cdot x \to \mathscr{S}$ por $\varphi(g \cdot x) = G_xg^{-1}$. Se $G_xg_1 = G_xg_2$, então $g_1^{-1}g_2 \in G_x$, ou seja, $g_1^{-1}g_2 \cdot x = x$, de modo que $g_1 \cdot x = g_2 \cdot x$. Segue que φ é injetiva. Agora, dado $G_xg \in \mathscr{S}$, tem-e que $\varphi(g^{-1}) = G_xg$.

Como φ é bijeção, tem-se que $|G \cdot x| = |\mathscr{S}| = [G : G_x] = |G|/|G_x|$

$\square$

Mostraremos uma aplicação do uso de ações em Teoria dos Grupos, demonstrando o seguinte famoso resultado.

Teorema 1.6.9. (Cauchy) Sejam G um grupo finito e p um número primo. Se p divide $|G|$, então G possui um elemento de ordem p.

Demonstração. Seja $n = |G|$. Defina $X = \{(x_1, x_2, \dots, x_p) : x_1x_2 \dots x_p = 1, \ x_i \in G, \forall i = 1, \dots, n\}$. Podemos reescrever X como sendo conjuntos das p-uplas $(x_1, x_2, \dots, x_{p-1}, (x_1x_2 \dots x_{p-1})^{-1})$ tais que $x_1, \dots, x_{p-1}$ são elementos de G. Assim, $|X| = n^{p-1}$. Em especial, p divide $|X|$. Seja $\sigma \in S_p$ a permutação que faz as seguintes associações: $\sigma(i) = i+1, \forall i = 1, 2, \dots, p-1$ e $\sigma(p) = 1$. Então, σ^p é a identidade. Defina $\frac{\mathbb{Z}}{p\mathbb{Z}} \times X \to X$ fazendo $(\bar{t}, (x_1, \cdots, x_p)) \mapsto (x_{\sigma^t(1)}, \dots, x_{\sigma^t(p)})$. Essa aplicação é uma ação. Desse modo, $p = |\frac{\mathbb{Z}}{p\mathbb{Z}}| = |\frac{\mathbb{Z}}{p\mathbb{Z}} \cdot x||(\frac{\mathbb{Z}}{p\mathbb{Z}})_x|$, para cada $x \in X$. Assim, as órbitas dessa ação possuem 1 elemento ou p elementos. Seja r o número de órbitas de tamanho p e seja s o número de órbitas de tamanho 1. Então, $|X| = pr + s$. Veja que a órbita de $(1, 1, \dots, 1)$ só possui um elemento. Assim, $s \geq 1$. Como p divide $|X|$, devemos ter que p divide s. Assim, $s \geq p \geq 2$. Consequentemente, existe um elemento $\tilde{x} = (x_1, \dots, x_p)$ em X tal que $\frac{\mathbb{Z}}{p\mathbb{Z}} \cdot \bar{x} = \{\bar{x}\}$. Isso significa que $\sigma^r(x_1, \dots, x_p) = (x_1, \dots, x_p)$, para cada $r = 1, 2, \dots, p$. Logo, $x_1 = x_2 = \dots x_p$. Como $\bar{x} \in X$, isso significa que $x_1 \in G$ é tal que $x_1^p = x_1x_2 \dots x_p = 1$. Portanto, x_1 é um elemento de ordem p em G. $\square$

1.7 Produto Semidireto de Grupos

Essa seção é destinada ao entendimento básico do produto semidireto entre dois grupos. Para um conhecimento mais aprofundado do assunto, ver [4].

Afirmação 1.7.1. Sejam G um grupo, $A \lhd G$ e $B \leq G$. Então, AB é um subgrupo de G.

Os elementos de AB são da forma ab com $a \in A$ e $b \in B$. Como A, B são grupos, tem-se que $1 \in A \cap B$, logo, $1 = 1 \cdot 1 \in AB$. Além disso, se $a_1b_1, a_2b_2 \in AB$, então $a_1b_1(a_2b_2)^{-1} \in AB$. De fato, $a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1(b_1b_2^{-1})a_2^{-1}(b_1b_2^{-1})^{-1}(b_1b_2^{-1})$. Como A é subgrupo normal de G, $a_2^{-1} \in A$ e $b_1b_2^{-1} \in B$, existe $a \in A$ tal que $(b_1b_2^{-1})a_2^{-1}(b_1b_2^{-1})^{-1} = a$. Segue que $a_1b_1(a_2b_2)^{-1} = a_1ab_1b_2^{-1} \in AB$.

Afirmação 1.7.2. Seja G um grupo. Dados dois subgrupos A e B de G tais que $A \cap B = \{1\}$, tem-se que AB está em bijeção com $A \times B$.

Defina $f : AB \to A \times B$ por $f(ab) = (a, b)$. Se $a_1b_1 = a_2b_2$, então $a_2^{-1}a_1 = b_2b_1^{-1}$. Como $a_2^{-1}a_1 \in A$ e $b_2b_1^{-1} \in B$, $a_2^{-1}a_1 = 1$ e $b_2b_1^{-1} = 1$, ou seja, $a_1 = a_2$ e $b_1 = b_2$, de modo que $(a_1, b_1) = (a_2, b_2)$. Segue que f está bem definida. Mostremos que f é bijetiva. Se $(a_1, b_1) = (a_2, b_2)$, então $a_1 = a_2$ e $b_1 = b_2$, logo, $a_1b_1 = a_2b_2$. Dado $(a, b) \in A \times B$, tem-se que $ab \in AB$ é tal que $f(ab) = (a, b)$.

Seja agora G um grupo com subgrupo B e subgrupo normal A tais que $A \cap B = \{1\}$. Como vimos, AB é um subgrupo de G que está em bijeção com $A \times B$. Queremos generalizar tal conceito para dois grupos A e B arbitrários. Para isso, dados A e B grupos, devemos encontrar um grupo G tal que $A \lhd G$ e $B \leq G$ e, como subgrupos de um mesmo grupo, devemos ter que $A \cap B = \{1\}$.

Seja $\varphi : B \to Aut(A)$ um homomorfismo de grupos. Considere a ação de B em A dada por $b \cdot a = \varphi(b)(a)$. Tome $G = \{(a, b) : a \in A \ e \ b \in B\}$ com a multiplicação

$$(a_1, b_1)(a_2, b_2) = (a_1(b_1 \cdot a_2), b_1b_2)$$

Afirmamos que G é grupo. Com efeito, $(1, 1) \in G$, onde 1 denota tanto o elemento neutro de A quanto o de B, é tal que $(1, 1)(a, b) = (1 \cdot a, b) = (a, b)$, pois φ é homomorfismo, logo $\varphi(1) = id_A$ e $(a, b)(1, 1) = (a(b \cdot 1), b) = (a, b)$, pois $\varphi(b)$ é homomorfismo, de modo que $\varphi(b)(1) = 1$. Logo, $(1, 1)$ é o elemento neutro de G. Além disso, para cada $(a, b) \in G$, tem-se que $(a, b)^{-1} = (b^{-1} \cdot a^{-1}, b^{-1}) \in G$ e tal operação é associativa:

$$\begin{aligned}
(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2(b_2 \cdot a_3), b_2b_3) \\
&= (a_1(b_1 \cdot (a_2b_2 \cdot a_3)), b_1b_2b_3) \\
&= (a_1(b_1 \cdot a_2)(b_1 \cdot (b_2 \cdot a_3)), b_1b_2b_3) \\
&= (a_1(b_1 \cdot a_2), b_1b_2)(a_3, b_3) \\
&= [(a_1, b_1)(a_2, b_2)](a_3, b_3)
\end{aligned}$$

Veja que A e B são isomorfos aos subgrupos de G: $A \times \{1\}$ e $\{1\} \times B$, respectivamente. Assim, podemos fazer as correspondências $(a, 1) \mapsto a$ e $(1, b) \mapsto b$. Vale que

$$\begin{aligned}(a,b)(\bar{a},1)(a,b)^{-1} &= (a,b)(\bar{a},1)(b^{-1} \cdot a^{-1}, b^{-1})\\ &= (ab \cdot \bar{a}, b1)(1, b^{-1}) = (a(b \cdot \bar{a})(b \cdot 1), bb^{-1})\\ &= (a\varphi(b)(\bar{a}), 1) \in A\end{aligned}$$

Segue que A é subgrupo normal de G. Veja também que $A \cap B = (1, 1)$. Além disso,

$$bab^{-1} = (1,b)(a,1)(1,b^{-1}) = (b \cdot a, b)(1, b^{-1}) = ((b \cdot a)(b \cdot 1), bb^{-1}) = (\varphi(b)(a), 1) = \varphi(b)(a) = b \cdot a$$

.

Definição 1.7.3. Dados dois grupos A e B e um homomorfismo de grupos $\varphi : B \to Aut(A)$, o produto semidireto entre A e B é o grupo AB com o produto $(a_1b_1)(a_2b_2) = a_1\varphi(b_1)(a_2)b_1b_2$. O produto semidireto será denotado por $A \rtimes_\varphi B$ ou simplesmente por $A \rtimes B$, quando não houver risco de confusão.

Capítulo 2

Grupo Livre e Apresentações de Grupos

Existem diversas maneiras de descrever um grupo. Para muitos grupos, a maneira mais compacta de defini-lo é usando a chamada apresentação de tal grupo. Nesse capítulo estudaremos grupos livres e suas apresentações, bem como apresentação de grupo de modo geral. Grupos Livres têm apresentação mais simples o possível, o que serve de motivação para tal estudo. As próximas seções têm como base [2].

2.1 Grupos Livres

Definição 2.1.1. Seja $i : X \to G$ uma função que leva o conjunto X no grupo G. Dizemos que o par (G, i) é *livre* sobre X se satisfaz a seguinte propriedade universal: dados um grupo H e uma função $f : X \to H$, existe um único homomorfismo de grupos $\varphi : G \to H$ satisfazendo $\varphi \circ i = f$.

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[d, "f"'] & G \arrow[dl, "\varphi"] \\ H & \end{tikzcd}$$

O grupo unitário $\{1\}$ é livre sobre o conjunto vazio. O grupo cíclico $\mathbb{Z}$ é livre sobre qualquer conjunto unitário $\{x\}$. Basta tomar $i(x) = 1$ ou $i(x) = -1$.

A seguir, mostraremos que dois grupos são livres sobre o mesmo conjunto X se, e somente se, tais grupos são isomorfos. Mostraremos inicialmente que, se o par (G, i) é livre sobre o conjunto X e existe um isomorfismo $\varphi : G \to H$, então o par $(H, \varphi \circ i)$ também é livre sobre X. Dados L um grupo e $f : X \to L$ uma função, existe um único homomorfismo $\chi : G \to L$ tal que $f = \chi \circ i$. Como φ é isomorfismo, em particular, é inversível. Seja $\varphi^{-1} : H \to G$ a sua inversa. Defina $\psi = \chi \circ \varphi^{-1} : H \to L$. A aplicação ψ é homomorfismo, pois é composição de homomorfismos. Além disso,

$$\psi \circ (\varphi \circ i) = (\chi \circ \varphi^{-1}) \circ (\varphi \circ i) = \chi \circ i = f.$$

Suponha que exista um homomorfismo de grupos $j : H \to L$ tal que $j \circ (\varphi \circ i) = f$. Então, $j \circ \varphi : G \to L$ é um homomorfismo tal que $(j \circ \varphi) \circ i = j \circ (\varphi \circ i) = f$. Por sua unicidade, χ é o único homomorfismo tal que $\chi \circ i = f$. Assim, $j \circ \varphi = \chi$, ou seja, $j = \chi \circ \varphi^{-1} = \psi$.

Para mostrar a recíproca de tal resultado, precisaremos observar o seguinte fato:

Observação 2.1.2. Dado um par (G, i) livre sobre o conjunto X, a única função $\phi : G \to G$ que satisfaz $\phi \circ i = i$ é a função identidade id_G de G.

$$\begin{tikzcd} X \arrow[r, "i_1"] \arrow[d, "i_1"'] & G_1 \arrow[dl, "\phi"] \\ G_1 & \end{tikzcd}$$

De fato, como (G, i) é livre sobre X, existe um único homomorfismo $\phi : G \to G$ tal que $i = \phi \circ i$. Como a função identidade $id_G : G \to G$ satisfaz tal condição, segue da unicidade de ϕ que $\phi = id_G$.

A recíproca mencionada é dada pela proposição seguinte.

Proposição 2.1.3. Sejam G_1 e G_2 grupos livres sobre o conjunto X com as funções $i_1 : X \to G_1, i_2 : X \to G_2$, respectivamente. Então, existe um isomorfismo $\varphi : G_1 \to G_2$ tal que $i_2 = \varphi \circ i_1$.

Demonstração. Como (G_1, i_1) é livre sobre X, existe um único homomorfismo $\varphi : G_1 \to G_2$ tal que $i_2 = \varphi \circ i_1$. Analogamente, como (G_2, i_2) é livre sobre X, existe um único homomorfismo $\psi : G_2 \to G_1$ satisfazendo $i_1 = \psi \circ i_2$.

Assim,

$$(\psi \circ \varphi) \circ i_1 = \psi \circ (\varphi \circ i_1) = \psi \circ i_2 = i_1 \text{ e}$$

$$(\varphi \circ \psi) \circ i_2 = \varphi \circ (\psi \circ i_2) = \varphi \circ i_1 = i_2.$$

$$\begin{tikzcd} G_1 \arrow[rr, shift left, "\varphi"] & & G_2 \arrow[ll, shift left, "\psi"] \\ & X \arrow[ul, "i_1"] \arrow[ur, "i_2"'] & \end{tikzcd}$$

Segue que $\psi \circ \varphi = id_{G_1}$ e $\varphi \circ \psi = id_{G_2}$, pela observação anterior a esta proposição. Ou seja, $\psi = \varphi^{-1}$. Logo, φ é isomorfismo. □

Lema 2.1.4. Dado um conjunto X, existem um grupo G e uma aplicação f que leva X injetivamente em G.

Demonstração. Como vimos em 1.1.2, $\mathbb{Z}^X = \{f : X \to \mathbb{Z} : \text{f é função}\}$ é um grupo com a soma de funções. Para cada $x \in X$, seja $\psi_x : X \to \mathbb{Z}$ a função que faz as seguintes associações: $\psi_x(x) = 1$ e $\psi_x(y) = 0$, para todo $y \neq x$ em X. Defina $\alpha : X \to \mathbb{Z}^X$ por $\alpha(x) = \psi_x$. Como $\psi_x \neq \psi_y$ se $x \neq y$, α é injetora. □

Proposição 2.1.5. Se (F, i) é livre sobre o conjunto X, então i é injetiva.

Demonstração. Com a notação do lema anterior, tem-se que $\alpha : X \to \mathbb{Z}^X$ é uma aplicação injetiva. Como (G, i) é livre sobre X, existe um único homomorfismo $\varphi : G \to \mathbb{Z}^X$ tal que $\alpha = \varphi \circ i$. Assim, i é injetiva. De fato, se não o fosse, existiriam $x_1, x_2 \in X$ tais que $x_1 \neq x_2$, porém $i(x_1) = i(x_2)$. Assim, $\varphi(i(x_1)) = \varphi(i(x_2))$, ou seja, $\alpha(x_1) = \alpha(x_2)$, contradizendo o fato de α ser injetiva. □

Mostramos que se um grupo G é livre sobre um conjunto X com a aplicação i, então i é injetora. O fato mais importante usado para tal demonstração foi a existência de um grupo no qual X é levado injetivamente, sem nos preocuparmos de fato com o grupo G ou com a aplicação i. Assim, seria natural se perguntar se, dado um conjunto X arbitrário, existe um par (G, i) que é livre sobre o conjunto X. A resposta é afirmativa. Para construir um grupo livre sobre um dado conjunto X, precisaremos de uma construção auxiliar, que será dada a seguir.

Seja X um conjunto arbitrário. Denotaremos por $\mathcal{S}(X)$ o conjunto de todas as sequências finitas $(x_{i_1}, ..., x_{i_m})$ de elementos de X. Quando $m = 0$, a sequência é dita *sequência vazia.* Veja que $\mathcal{S}(X)$ é um monoide com a multiplicação

$$(x_{i_1}, ..., x_{i_m})(x_{j_1}, ..., x_{j_s}) = (x_{i_1}, ..., x_{i_m}, x_{j_1}, ..., x_{j_s}),$$

pois essa multiplicação é associativa e tem como elemento neutro a sequência vazia. Denotaremos o elemento neutro, ou seja a *sequência vazia*, por $\varnothing$. Chamaremos $\mathcal{S}(X)$ de *monoide livre* sobre X.

A aplicação que leva cada elemento $x \in X$ na sequência $(x) \in \mathcal{S}(X)$ é injetora. Assim, cada elemento de $\mathcal{S}(X)$ é unicamente representado por um produto $(x_{i_1})...(x_{i_m})$. Por simplicidade, associaremos cada (x) a x, assim, tal elemento de $\mathcal{S}(X)$ será representado por $x_{i_1}...x_{i_m}$.

Um *segmento* de $x_{i_1}...x_{i_m} \in \mathcal{S}(X)$ é um elemento de $\mathcal{S}(X)$ da forma $x_{i_r}x_{i_{r+1}}...x_{i_s}$, com $1 \leq r \leq s \leq m$. Se $x_{i_r}x_{i_{r+1}}...x_{i_s} \neq x_{i_1}...x_{i_m}$, dizemos que esse é um segmento próprio de $x_{i_1}...x_{i_m}$.

Finalmente, tome um conjunto $\bar{X}$ disjunto de X que esteja em bijeção com X, digamos $\bar{x} \longmapsto x$. Chamaremos de *palavras* de X os elementos de $\mathcal{S}(X \cup \bar{X})$. Por simplicidade, denotaremos $\bar{x} \in \bar{X}$ por x^{-1}, onde x é a imagem de $\bar{x}$ pela bijeção dada. Poderemos também denotar $x \in X$ por x^1. Assim, uma palavra de X é da forma $w = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$, onde $\varepsilon_j = \pm 1$. O número m é dito o *comprimento* de w e é denotado por $|w|$. A palavra vazia pode ser vista como a palavra que não possui letras, assim, $|w| = 0 \Leftrightarrow w = \varnothing$.

Cada $x_{i_j}^{\varepsilon_j}$ é dito uma *letra* da palavra $w = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$. Nos referimos ao conjunto $X \cup \bar{X}$ como *alfabeto.*

Uma palavra w é dita *reduzida* quando é a palavra vazia ou quando é da forma $w = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$ e $i_{s+1} = i_s$ implica $\varepsilon_{s+1} \neq -\varepsilon_s$, ou seja, letras adjacentes não são imagem uma da outra na bijeção entre $\bar{X}$ e X.

Exemplo 2.1.6. As palavras xyx^{-1} e $xzxy$ são palavras reduzidas do alfabeto $\{x^{\pm 1}, y^{\pm 1}, z^{\pm 1}\}$ (ou seja, aqui $X = \{x, y, z\}$). Entretanto, $xx^{-1}yzx$ não é uma palavra reduzida, pois tem um segmento xx^{-1}.

Uma palavra reduzida $w = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$ é dita uma palavra *ciclicamente reduzida* se $i_1 \neq i_m$ ou se $i_1 = i_m$ mas $\varepsilon_1 \neq -\varepsilon_m$. Convencionamos que a palavra vazia é ciclicamente reduzida. Observe que

w é uma palavra ciclicamente reduzida se, e somente se, o produto ww é uma palavra reduzida. De modo geral, vale que $w^n = w \ldots w$ (n fatores) é reduzida. Logo, $|w^n| = n|w|$.

Seja $u = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$ uma palavra não reduzida com $i_{r+1} = i_r$ e $\varepsilon_{r+1} = -\varepsilon_r$. Denote por u' a palavra obtida de u ao retirar-se as letras adjacentes $x_{i_r}^{\varepsilon_r}$ e $x_{i_{r+1}}^{\varepsilon_{r+1}}$. Dizemos que *$u'$ é obtido de u por redução elementar*. Se u'' é obtido de u por uma sequência de reduções elementares, dizemos que *u'' é obtido de u por redução*.

Exemplo 2.1.7. Considere o alfabeto $X = \{x^{\pm 1}, y^{\pm 1}, z^{\pm 1}\}$. As palavras $xzyy^{-1}$ e $xzx^{-1}x$ são obtidas de $w = xzx^{-1}xyy^{-1}z$ por redução elementar, enquanto xzz é obtida de w por redução.

Escreveremos $w \sim w'$ se $w = w'$ ou se existir uma sequência de palavras $(w_1, ..., w_k)$, com $w_1 = w$ e $w_k = w'$, tal que w_j e w_{j+1} são obtidas uma do outra por redução elementar, para cada $j = 1, ..., k-1$.

Afirmação 2.1.8. $\sim$ é uma relação de equivalência.

Com efeito, $\sim$ é reflexiva por definição. Além disso, se $w \sim w'$, seja $(w_1, ..., w_n)$ uma sequência como na definição de $\sim$. Então, $(w_n, ..., w_1)$ é uma sequência com elementos adjacentes obtidos um do outro por reduções elementares. O primeiro fator é igual a w' e o último fator é igual a w. Por fim, se $w \sim w'$ e $w' \sim w''$, então existem sequências $(w_1, ..., w_r)$ e $(u_1, ..., u_s)$, com $w_1 = w$, $w_r = w' = u_1$ e $u_s = w''$ como na definição de $\sim$. A sequência $(w_1, ..., w_r, u_2, ..., u_s)$ garante então que $w \sim w''$.

Denotaremos por $F(X)$ o conjunto de todas as relações de equivalência. A classe de equivalência da palavra w com relação a $\sim$ será denotada por $[w]$.

Se $w \sim w'$, então $uwv \sim uw'v$, para quaisquer palavras u e v. De fato, se $(w_1, ..., w_n)$ é uma sequência que mostra que $w \sim w'$, então a sequência $(uw_1v, ..., uw_nv)$ é tal que $uw_1v = uwv$, $uw_nv = uw'v$ e dois elementos adjacentes são obtidos um do outro por redução elementar. Assim, se $w \sim w'$ e $u \sim u'$, então $uw \sim uw' \sim u'w'$. Podemos então definir uma multiplicação em $F(X)$, fazendo $[u][w] = [uw]$. $F(X)$ é grupo com essa multiplicação, pois ela é associativa e tem como identidade a classe de equivalência da sequência vazia. Além disso, para $w = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$, tem-se $ww^{-1} = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}x_{i_m}^{-\varepsilon_m}...x_{i_1}^{-\varepsilon_1}$. Assim, $ww^{-1} \sim \varnothing$, ou seja, $[w][w^{-1}] = [\varnothing]$. Logo, $[w]$ tem como inverso o elemento $[w^{-1}]$. Por fim, defina a função $i : X \to F(X)$, que associa cada $x \in X$ à sua classe de equivalência $[x] \in F(X)$. Tem-se que $F(X)$ é gerado por $i(X)$.

Mostraremos agora que existe um grupo livre sobre cada conjunto arbitrário X. Usaremos a notação dada acima.

Teorema 2.1.9. O par $(F(X), i)$ é livre sobre o conjunto X.

Demonstração. Dados um grupo G e uma função $f : X \to G$, defina a função $\bar{f} : \mathcal{S}(X \cup \bar{X}) \to G$ fazendo a seguinte correspondência:

$$\bar{f}(x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}) = f(x_{i_1})^{\varepsilon_1}...f(x_{i_m})^{\varepsilon_m},$$

para cada $x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m} \in \mathcal{S}(X \cup \bar{X})$. Dados $w = x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m}$, $u = x_{j_1}^{\delta_1}...x_{j_k}^{\delta_k}$, tem-se que

$$\bar{f}(wu) = f(x_{i_1})^{\varepsilon_1}...f(x_{i_m})^{\varepsilon_m} f(x_{j_1})^{\delta_1}...f(x_{j_k})^{\delta_k} = (f(x_{i_1})^{\varepsilon_1}...f(x_{i_m})^{\varepsilon_m})(f(x_{j_1})^{\delta_1}...f(x_{j_k})^{\delta_k}) = \bar{f}(w)\bar{f}(u).$$

Ou seja, $\bar{f}$ é homomorfismo de monoides.

Se w' é obtida de w por redução elementar, existem palavras $u, v \in \mathcal{S}(X \cup \bar{X})$ tais que $w' = ux_{i_j}^{\varepsilon_j} x_{i_j}^{-\varepsilon_j} v$. Assim,

$$\bar{f}(w') = f(v)f(x_{i_j})^{\varepsilon_j} f(x_{i_j})^{-\varepsilon_j} f(v) = f(u)f(v) = \bar{f}(w).$$

Dada uma sequência $(w_1, \ldots, w_m)$, na qual elementos adjacentes são obtidos um do outro por redução elementar, tem-se $\bar{f}(w_1) = \ldots = \bar{f}(w_m)$. Isso significa que duas palavras w, w' têm a mesma imagem se $w \sim w'$.

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[d, "f"'] & F(X) \arrow[dl, "\varphi"] \\ G & \end{tikzcd}$$

Devido a esse fato, a função $\varphi : F(X) \to G$ dada por $\varphi([w]) = \bar{f}(w)$ está bem definida. Além disso, φ é um homomorfismo de grupos, pois $\bar{f}$ é homomorfismo de monoides. Como $\varphi(i(x)) = \varphi([x]) = \bar{f}(x) = f(x)$, $\forall x \in X$, basta mostrar que esse é o único homomorfismo com tal propriedade. Suponha que exista um homomorfismo $\tilde{\varphi} : F(X) \to G$ tal que $\tilde{\varphi} \circ i = f$. Então, $\tilde{\varphi}|_{i(X)} = \varphi|_{i(X)}$. Como $i(X)$ gera $F(X)$, segue que $\tilde{\varphi} = \varphi$.

□

A cada redução elementar, o comprimento de uma palavra diminui. Podemos então aplicar numa mesma palavra uma sequência de reduções elementares de modo que o comprimento da palavra resultante seja mínimo, ou seja, de modo que não seja possível obter outra palavra por redução elementar da palavra resultante. Dessa forma, a palavra resultante é reduzida. Tal processo é aplicável a qualquer palavra e, portanto, toda classe de equivalência contém pelo menos uma palavra reduzida. O Teorema a seguir mostra a unicidade de cada palavra reduzida em sua respectiva classe de equivalência.

Teorema 2.1.10. (Forma Normal para Grupos Livres) Cada classe de equivalência de $F(X)$ contém exatamente uma palavra reduzida.

Demonstração. A existência de uma palavra reduzida em cada classe de equivalência decorre do comentário acima. Denote por R o conjunto de todas as palavras reduzidas de X e por S_R o grupo das permutações de R. Observe que $[\varnothing] = 1_{F(X)}$. Queremos encontrar um homomorfismo $\varphi : F(X) \to S_R$ tal que a ação $\varphi[w]$ quando aplicada na sequência vazia $\varnothing$ resulte na palavra w. A existência desse homomorfismo implica na unicidade da palavra reduzida numa determinada classe de equivalência. De fato, se w e w' são palavras reduzidas tais que $w \sim w'$, então $[w] = [w']$. Segue que $w = \varphi[w](\varnothing) = \varphi[w'](\varnothing) = w'$.

Seja $f : X \to S_R$ a aplicação que leva cada $x \in X$ na aplicação $f_x : R \to R$, dada por

$$f_x(w) = \begin{cases} xw, & \text{se } w \text{ não começa com o fator } x^{-1} \\ u, & \text{se } w = x^{-1}u \text{ para alguma palavra reduzida } u \end{cases}$$

Mostremos que, de fato, cada f_x é uma permutação de R. Para mostrar a injetividade de f_x, suponha que $f_x(w) = f_x(w')$, para certos $w, w' \in R$. Se w não começa em x^{-1}, então w' também não começa. De fato, se $w' = x^{-1}v$ para alguma palavra reduzida v, então $v = f_x(w') = f_x(w) = xw$, ou seja, $w = x^{-1}v$, contradizendo o fato de w não começar em x^{-1}. Analogamente, não podemos ter w' com primeiro fator diferente de x^{-1} e $w = x^{-1}u$, para alguma palavra reduzida u. O problema se resume então a dois casos: w, w' não começam em x^{-1} ou $w = x^{-1}u$ e $w' = x^{-1}v$, para certas palavras reduzidas u e v. No primeiro caso, tem-se que $xw = f_x(w) = f_x(w') = xw'$, logo, $w = w'$. No segundo caso, tem-se que $u = f_x(w) = f_x(v) = v$, de modo que $w = x^{-1}u = x^{-1}v = w'$.

Mostremos agora a sobrejetividade de f_x. Dada uma palavra reduzida w, se w não começa com o fator x, então $x^{-1}w \in R$ e $f_x(x^{-1}w) = w$. Caso $w = xv$, para alguma palavra reduzida v, então $f_x(v) = w$. Assim, $f_x : R \to R$ é permutação de R.

Veja que a inversa de f_x é dada por

$$f_x^{-1}(w) = \begin{cases} x^{-1}w, & \text{se } w \text{ não começa com o fator } x \\ v, & \text{se } xv = w, \text{ para alguma palavra reduzida } v \end{cases}$$

ou seja, $f_x^{-1} = f_{x^{-1}}$.

Pelo Teorema anterior, o par $(F(X), i)$ é livre sobre X. Assim, existe um único homomorfismo $\varphi : F(X) \to S_R$ tal que $\varphi \circ i = f$, ou seja, $\varphi[x] = \varphi(i(x)) = f_x$, $\forall x \in X$. Assim, se $w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ é uma palavra reduzida de $F(X)$, então $\varphi[w] = f_{x_1}^{\varepsilon_1} \dots f_{x_n}^{\varepsilon_n}$. Tem-se que $\varphi[x](\varnothing) = f_x(\varnothing) = x$. Segue que $\varphi[w](\varnothing) = f_{x_1}^{\varepsilon_1} \dots f_{x_{n-1}}^{\varepsilon_{n-1}}(f_{x_n}^{\varepsilon_n}(\varnothing)) = f_{x_1}^{\varepsilon_1} \dots f_{x_{n-1}}^{\varepsilon_{n-1}}(x_n^{\varepsilon_n}) = \dots = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} = w$, pois w é reduzida, logo, $x_k^{\varepsilon_k} \dots x_n^{\varepsilon_n}$ não começa em $x_{k-1}^{-\varepsilon_{k-1}}$, para nenhum $i = 1, \dots, k-1$. $\square$

Usualmente, identificamos os elementos de $F(X)$ com as respectivas palavras reduzidas. Consideramos também X um subconjunto de $F(X)$ e i a inclusão. Assim, poderemos omitir i.

Por simplicidade, escreveremos apenas $w = w'$ em vez de $w \sim w'$. Quando w e w' forem a mesma palavra, escreveremos $w \equiv w'$.

Definição 2.1.11. Um grupo G é *residualmente finito* se, para cada $w \in G$ com $w \neq 1$, existe um subgrupo normal N de G que não contém w e F/N é finito.

Equivalentemente, um grupo G é *residualmente finito* se $\bigcap_{N \in \mathscr{N}} N = \{1\}$, onde $\mathscr{N} = \{N \lhd G : [G : N] < \infty\}$. De fato, se G é residualmente finito no primeiro sentido, então não pode haver $g \neq 1$ tal que $g \in \bigcap_{N \in \mathscr{N}} N$, ou todos os subgrupos normais de índice finito em G teríam g como elemento, contradizendo a primeira definição dada. Por outro lado, se G é um grupo tal que $\bigcap_{N \in \mathscr{N}} N = \{1\}$, então, dado $g \in G \setminus \{1\}$, tem-se que $g \notin \bigcap_{N \in \mathscr{N}} N$, logo, existe $N \in \mathscr{N}$ tal que $g \in N$.

Proposição 2.1.12. Grupos livres são residualmente finitos.

Demonstração. Seja F um grupo livre com base X. Dada uma palavra reduzida $w = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$, com $w \not\equiv \varnothing$, sabemos que $[w] \neq [\varnothing]$, ou seja, $w \neq \varnothing$.

Queremos encontrar um subgrupo normal N de F tal que F/N seja finito e $w \notin N$.

Para cada $x \in X$, seja $f_x : \{1, \dots, n+1\} \to \{1, \dots, n+1\}$ uma aplicação que faz a seguinte associação:

$$\begin{cases} f_x(r) = r + 1, & \text{se } x_{i_r}^{\varepsilon_r} = x \\ f_x(r+1) = r, & \text{se } x_{i_r}^{-\varepsilon_r} = x. \end{cases}$$

Veja que, a rigor, f_x não é uma aplicação, pois não está definida para todo r. A condição anterior não faz com que f_x não esteja bem definida, pois tal f_x só poderia levar $r \in \{1, \dots, n+1\}$ em dois elementos distintos da seguinte maneira

$$f_x(r) = r + 1 \quad ou \quad f(r) = r - 1.$$

A primeira igualdade nos diz que $x_{i_r}^{\varepsilon_r} = x$ e a segunda equivale a $f_x((r-1)+1) = r-1$, assim, $x_{i_{r-1}}^{-\varepsilon_{r-1}} = x$. Logo, $x_{i_{r-1}}^{\varepsilon_{r-1}} x_{i_r}^{\varepsilon_r} = x^{-1}x$, contradizendo o fato de w ser uma palavra reduzida.

Além disso, f não leva dois elementos distintos em um mesmo $s \in \{1, \dots, n+1\}$, pois $f_x(r) = s$ quando $r = s-1$ e $x_{i_{s-1}}^{\varepsilon_{s-1}} = x$ ou quando $r = s+1$ e $x_{i_s}^{-\varepsilon_s} = x$. Consequentemente, a única maneira de dois elementos serem levados em s é $f_x(s-1) = s = f_x(s+1)$. Mas isso nos daria $x_{i_{s-1}}^{\varepsilon_{s-1}} = x$ e $x_{i_s}^{\varepsilon_s} = x^{-1}$, contrariando novamente o fato de w ser uma palavra reduzida.

Segue que f_x pode ser estendida a uma aplicação $\bar{f}_x \in S_{n+1}$, sendo S_{n+1} o grupo simétrico de $\{1, \dots, n\}$. Defina $f : X \to S_{n+1}$ por $f(x) = \bar{f}_x$. Denotando por i a inclusão de X em F, como F é livre, existe um único homomorfismo $\varphi : F \to S_{n+1}$ tal que $\varphi \circ i = f$. Pela definição de f, tem-se que $f(w) \neq id$, onde id é a identidade em S_{n+1}. Logo, $\varphi(w) \neq id$.

Pelo Primeiro Teorema do Isomorfismo, $Ker(\varphi)$ é um subgrupo normal de G tal que $G/Ker(\varphi)$ é isomorfo a $Im(\varphi)$. Como $Im(\varphi) \subset S_{n+1}$ e $|S_{n+1}| = (n+1)!$, tem-se que tal imagem é finita, assim como $G/Ker(\varphi)$. Além disso, como $\varphi(w) \neq id$, $w \notin Ker(\varphi)$. $\square$

Corolário 2.1.13. Se G é um grupo livre finitamente gerado, então todo endomorfismo sobrejetor de G é um automorfismo.

Demonstração. Seja $\alpha : G \to G$ um epimorfismo. Mostremos que α é isomorfismo. Seja N um subgrupo normal de índice finito em G. Como N é normal, $\alpha^{-n}(N)$ é normal, para cada $n \in \mathbb{N}$. Seja $\pi_N : G \to G/N$ a projeção canônica. Tem-se que $\alpha^{-1}(N) = \ker(\pi_N \circ \alpha)$, assim, pelo Primeiro Teorema do Isomorfismo, $\alpha^{-1}(N)$ é isomorfo a $Im(\pi_N \circ \alpha) = G/N$. Podemos repetir o processo, obtendo que $G/N \simeq G/\alpha^{-1}(N) \simeq G/\alpha^{-1}(\alpha^{-1}(N)) = G/\alpha^{-2}(N)$. Indutivamente, $G/N \simeq G/\alpha^{-n}(N)$, para todo natural n. Seja $V = \{\alpha^{-m}(N) : \ m \in \mathbb{N}\}$. Dado $K \in V$, existe $\varphi : G \to G/N$ tal que $\ker \varphi = K$. Como G é finitamente gerado e os valores de um homomorfismo $\varphi : G \to G/N$ são determinados pelos elementos do gerador finito de G, existem apenas finitos valores de G/N nos quais podemos mapear elementos do gerador de G. Assim, existem finitos tais homomorfismos, consequentemente V é finito. Existe então um $m \in \mathbb{N}$ tal que $m > n$ e $\alpha^{-m}(N) = \alpha^{-n}(N)$. Segue que $\alpha^{-(m-n)}(N) = N$ e, portanto, $N \supset \ker \alpha$. Como N é arbitrário, isso vale para qualquer $N \lhd G$ com índice finito em G. Denote por $\mathscr{N}$ o conjunto de todos os subgrupos normais de G com índice finito. Segue que $\ker \alpha \subset \bigcap_{N \in \mathscr{N}} N = \{1\}$, pois G é residualmente finito. $\square$

A demonstração acima foi feita usando-se apenas o fato de G ser residualmente finito e o fato de G ser finitamente gerado. Portanto, tal resultado vale para todo grupo finitamente gerado que é residualmente finito, não particularmente para grupos livres. Um grupo no qual todo endomorfismo sobrejetor é um automorfismo é chamado de *Hopfiano*.

Proposição 2.1.14. Sejam $F(X)$ e $F(Y)$ grupos livres sobre X e Y, respectivamente. Então, $F(X)$ e $F(Y)$ são isomorfos se, e somente se, $|X| = |Y|$.

Demonstração. Se $|X| = |Y|$, então existe uma bijeção $f : X \to Y$. Pela propriedade universal de grupo livre, podemos estender f a um homomorfismo $F(X) \to Y$ que, por sua vez, pode ser visto como um homomorfismo $\varphi : F(X) \to F(Y)$. Analogamente, $f^{-1} : Y \to X$ pode ser estendida a um homomorfismo $\phi : F(Y) \to F(X)$. Agora, como $f^{-1} \circ f = id_X$, tem-se que $\phi \circ \varphi$ e $id_{F(X)}$ estendem a identidade de X. Segue que $\phi \circ \varphi = id_{F(X)}$, pela unicidade de homomorfismos na definição de grupo livre. Analogamente, $\varphi \circ \phi = id_{F(Y)}$. Segue que φ é isomorfismo, com $\varphi^{-1} = \phi$.

Reciprocamente, suponha que $F(X)$ e $F(Y)$ sejam isomorfos. O número de homomorfismos que levam $F(X)$ no grupo cíclico de ordem dois $\mathbb{Z}_2$ é igual ao número de funções $X \to \mathbb{Z}_2$, ou seja, $2^{|X|}$. Análogo para $F(Y)$. Como $2^{|X|} = 2^{|Y|}$, se $|X|$ ou $|Y|$ é finito, então ambos são finitos e existe uma bijeção entre eles. Se $|X|$ e $|Y|$ são infinitos, vale que $|\mathcal{S}(X \cup \bar{X})| = |X \cup \bar{X}| = |X|$, pelo axioma da escolha. Como $F(X)$ é um conjunto de classes de equivalência de $\mathcal{S}(X \cup \bar{X})$, tem-se que $|F(X)| \leq |\mathcal{S}(X \cup \bar{X})| = |X|$. Por outro lado, $|X| \leq |F(X)|$, pois X pode ser visto como subconjunto de $F(X)$. Segue que $|F(X)| = |X| = |Y| = |F(Y)|$. $\square$

Definição 2.1.15. Um grupo G é dito um *grupo livre* se existem um conjunto X e um isomorfismo $i : F(X) \to G$. Nesse caso, dizemos que $i(X)$ é uma *base de* G. Também dizemos que G é livre em $i(X)$.

As bases de um grupo livre G são equipotentes entre si. De fato, se A e B são bases de G, existem isomorfismos $i_1 : F(X) \to G$ e $i_2 : F(Y) \to G$, para certos conjuntos X e Y, tais que $i_1(X) = A$ e $i_2(Y) = B$. Por ser composição de isomorfismos, $i_2^{-1} \circ i_1 : F(X) \to F(Y)$ é um isomorfismo. A proposição anterior tem como resultado que $|X| = |Y|$. Segue que $|A| = |B|$. Então, qualquer bijeção de A em B se estende a um automorfismo de G. Além disso, se G é um grupo livre com base A, existe um isomorfismo $i : F(X) \to G$ tal que $i(X) = A$. Dado um automorfismo $\alpha : G \to G$, tem -se que $\alpha \circ i : F(X) \to G$ é isomorfismo e portanto $\alpha(A) = \alpha(i(X))$ também é base de G.Podemos considerar cada base de G como um subconjunto de G, por simplicidade. Se β é um automorfismo de $F(X)$, então $i \circ \beta : F(X) \to G$ é um isomorfismo e $i(\beta(X))$ é base de G. Em particular, $F(X)$ é grupo livre com base $\beta(X)$.

Definição 2.1.16. Chamaremos de *posto* a cardinalidade das bases de um grupo livre.

Exemplo 2.1.17. Uma base para $F = F(x, y)$ é $\{x^{-1}, x^2y\}$. Defina $\varphi : F \to F$ fazendo $\varphi(x) = x^{-1}$ e $\varphi(y) = x^2y$. Veja que $\varphi(x^2y) = \varphi(x)^2\varphi(y) = (x^{-1})^2x^2y = y$ e $\varphi(x^{-1}) = \varphi(x)^{-1} = x$. Podemos então escrever cada elemento de F a partir de φ. Segue que φ é endomorfismo e, portanto, é isomorfismo.

Proposição 2.1.18. Sejam G um grupo e X um subconjunto de G. As seguintes afirmações são equivalentes:

i. G é livre com base X;

ii. Podemos escrever cada elemento de G de maneira única como $x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$, para algum $m \geq 0$, de modo que $x_{i_k} \in X$, $\varepsilon_k = \pm 1$ e $i_{k+1} = i_k$ implica $\varepsilon_{k+1} \neq \varepsilon_k$;

iii. O conjunto X gera G e 1 não pode ser escrito na forma $x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$, onde $m > 0$, $x_{i_k} \in X$, $\varepsilon_k = \pm 1$ e $i_{k+1} = i_k$ implica $\varepsilon_{k+1} \neq \varepsilon_k$.

Demonstração. Mostremos inicialmente que (ii) implica (iii). Se cada $g \in G$ é da forma $g = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$, com $x_k \in X$, então, por definição, X gera G. Se existisse $x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$ com $m > 0$ tal que $1 = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$, então $x_{i_1}^{-\varepsilon_1} = x_{i_2}^{\varepsilon_2} \dots x_{i_m}^{\varepsilon_m}$, ou seja, $x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m} = x_{i_1}^{\varepsilon_1} x_{i_1}^{-\varepsilon_1}$, contradizendo $\varepsilon_{k+1} \neq -\varepsilon_k$ se $i_{k+1} = i_k$.

Mostremos a recíproca da afirmação anterior. Se X gera G, todo elemento $g \in G$ é da forma $g = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$. Caso $\varepsilon_{k+1} = -\varepsilon_k$ com $i_{k+1} = i_k$ para algum k, basta excluir os fatores adjacentes $x_{i_k}^{\varepsilon_k} x_{i_k+1}^{\varepsilon_k+1}$. Agora, se $g = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$ e $g = x_{j_1}^{\delta_1} \dots x_{j_n}^{\delta_n}$, então $1 = x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m} x_{j_n}^{-\delta_n} \dots x_{i_1}^{-\delta_1}$. Realizando todos os cancelamentos possíveis, todos os fatores devem ser cancelados, caso reste algum $x_{p_r}^{\varepsilon_r} \dots x_{p_s}^{\varepsilon_s}$ que não possa ser cancelado, teremos $1 = x_{p_r}^{\varepsilon_r} \dots x_{p_s}^{\varepsilon_s}$, uma contradição.

Se G é livre sobre X, então existe um isomorfismo $i : F(X) \to G$. Como $F(X)$ satisfaz (ii) e (iii), G também satisfaz tais condições.

Suponha agora que G satisfaça a propriedade (ii) ou a propriedade (iii). Considere o homomorfismo $\phi : F(X) \to G$ induzido pela identidade em X. Como G é gerado por X, ϕ é sobrejetora. Por hipótese, nenhuma palavra trivial é levada em 1, logo, ϕ é injetiva. Portanto, $\phi : F(X) \to G$ é isomorfismo, ou seja, G é livre com base X. $\square$

Corolário 2.1.19. Seja G um grupo. Dados um conjunto X que gera G e $\varphi : G \to H$ um homomorfismo que é injetivo em X, se $\varphi(G)$ é livre com base $\varphi(X)$, então G é livre com base X.

Demonstração. Pelo Teorema anterior, $\varphi(X)$ gera $\varphi(G)$, logo, X gera G. Além disso, como 1 não pode ser escrito na forma $x_{i_1}^{\varepsilon_1} \dots x_{i_m}^{\varepsilon_m}$, onde $m > 0$, $x_{i_k} \in \varphi(X)$, $\varepsilon_k = \pm 1$ e de modo que $i_{k+1} = i_k$ implica $\varepsilon_{k+1} \neq \varepsilon_k$, como φ é injetiva em X, $1 \in G$ não pode ser escrito na forma $y_{j_1}^{\varepsilon_1} \dots y_{j_m}^{\varepsilon_m}$, onde $m > 0$, $y_{j_k} \in X$, $\varepsilon_k = \pm 1$ e de modo que $i_{k+1} = i_k$ implica $\varepsilon_{k+1} \neq \varepsilon_k$. Segue que G é livre com base X. $\square$

Corolário 2.1.20. Seja G um grupo livre com base X e seja $Y \subset X$. Então, $\langle Y \rangle$ é grupo livre com base Y.

Demonstração. Por definição, Y gera $\langle Y \rangle$. Além disso, Como $Y \subset X$, a restrição atribuída a 1 em (iii) também vale para Y. $\square$

Corolário 2.1.21. Seja F um grupo livre com base $\{x, y\}$. Então $\varphi : F \to \mathbb{Z}$ definida por $\varphi(x) = 1$ e $\varphi(y) = 0$ é tal que $Ker\varphi$ é grupo livre com base $\{x^{-i}yx^i : i \in \mathbb{Z}\}$.

Demonstração. Tome $K = \{x^{-i}yx^i : i \in \mathbb{Z}\}$ como $\varphi(x^{-i}yx^i) = -i\varphi(x) + \varphi(y) + i\varphi(x) = \varphi(y) = 0$, tem-se que $\langle K \rangle \subset Ker\varphi$.

Tem-se que $x^{-a}y^bx^a = (x^{-a}yx^a)(x^{-a}yx^a)\dots(x^{-a}yx^a) = (x^{-a}yx^a)^b$. Assim, cada x^ky^l pode ser escrito como $(x^{-k}yx^k)^lx^{-k}$. De forma geral,

$$x^{k_1}y^{l_1}\dots x^{k_n}y^{l_n} = (x^{k_1}yx^{-k_1})^{l_1}(x^{k_1+k_2}yx^{-(k_1+k_2)})\dots(x^{k_1+\dots k_n}yx^{-(k_1+\dots k_n)})^{l_n}x^{k_1+\dots k_n}$$

Por exemplo,

$$\begin{aligned} xyx^{-2}y^{-3}x^2yx^{-5} &= (xyx^{-1})(x^{-1}y^{-3}x^2yx^{-5}) \\ &= (xyx^{-1})(x^{-1}yx)^{-3}(xyx^{-5}) \\ &= (xyx^{-1})(x^{-1}yx)^{-3}(xyx^{-1})x^{-4} \end{aligned}$$

Segue que todo elemento de F pode ser escrito como kx^n, onde $k \in K$ e $n \in \mathbb{Z}$, ou seja, $F \subset K\langle x \rangle = \{kz : k \in K \text{ e } z \in \langle x \rangle\}$. A imagem de $kx^n \in K\langle x \rangle$ por φ é dada por $\varphi(kx^n) = \varphi(k)n\varphi(x) = n$. Como consequência, $kx^n \in Ker\varphi$ se, e somente se, $n = 0$. Segue que $K \subset Ker\varphi$. Logo, $Ker\varphi = K$.

Ponha $x_i = x^{-i}yx^i, i \in Z$. Consideremos agora as palavras reduzidas do alfabeto $\{x_i, x_i^{-1}\}_{i\in\mathbb{Z}}$. Qualquer palavra reduzida $w = x_{i_1}^{\varepsilon_1}\dots x_{i_n}^{\varepsilon_n}$ é, no alfabeto $\{x, y\} \cup \{x^{-1}, y^{-1}\}$, do tipo

$$x^{j_1}y^{l_1}x^{j_2}y^{l2}\dots x^{j_n}y^{l_n}x^{j_{n+1}},$$

onde $j_r = r_{r-1} - i_r$, com $i_0 = 0 = i_{n+1}$. Alegamos que uma tal palavra w de $\{x, y\} \cup \{x^{-1}, y^{-1}\}$ pode ter cancelamentos de x^k e x^{-k}, mas não de y^l com y^{-l}. De fato, se houver algum cancelamento de fatores y^{l_k} e $y^{l_{k+1}}$, então o segmento $x^{-i_k}y^{l_k}x^{i_k}x^{-i_{k+1}}y^{i_{k+1}}x^{i_{k+1}}$ deve cancelar $x^{i_k}x^{-i_{k+1}}$. Ou seja, $i_k = -i_{k+1}$, contradizendo o fato de w ser uma palavra reduzida. Assim, não existe $x_{i_1}^{\varepsilon_1}\dots x_{i_n}^{\varepsilon_n} = 1$.
$\square$

Lema 2.1.22. Sejam F um grupo livre com base X e $w \in F$. Então existem $u, v \in F$, com v uma palavra ciclicamente reduzida, tais que $w = uvu^{-1}$.

Demonstração. Se $w = \varnothing$, então basta tomar $u, v = \varnothing$. Consideremos então $w \neq \varnothing$. Se w é ciclicamente reduzida, basta tomar $u = 1$ e $v = w$. Caso contrário, seja $w = x_{i_1}^{\varepsilon_1}\dots x_{i_m}^{\varepsilon_m}$ uma palavra reduzida, mas não ciclicamente reduzida. Mostraremos o resultado por indução em m. O primeiro caso é para $m = 3$. Nesse caso, $w = x_{i_1}^{\varepsilon_1}x_{i_2}^{\varepsilon_2}x_{i_3}^{\varepsilon_3}$ é tal que $x_{i_1}^{\varepsilon_1} = x_{i_3}^{-\varepsilon_3}$. Assim, $u = x_{i_1}^{\varepsilon_1}$ e $v = x_{i_2}^{\varepsilon_2}$. Agora, para $w = x_{i_1}^{\varepsilon_1}\dots x_{i_m}^{\varepsilon_m}$, tome $\tilde{u} = x_{i_1}^{\varepsilon_1}$ e $\tilde{v} = x_{i_2}^{\varepsilon_2}\dots x_{i_{m-1}}^{\varepsilon_{m-1}}$. Tem-se que $w = \tilde{u}\tilde{v}\tilde{u}^{-1}$.

Se $\tilde{v}$ é ciclicamente reduzida, o problema está resolvido. Caso contrário, pela hipótese de indução, existem $u_1, v_1 \in F$, com v_1 ciclicamente reduzida, tais que $\tilde{v} = u_1 v_1 u_1^{-1}$. Tome $u = \tilde{u}u_1$ e $v = v_1$. Segue que $w = \tilde{u}\tilde{v}\tilde{u}^{-1} = \tilde{u}u_1 v_1 u_1^{-1}\tilde{u}^{-1} = uvu^{-1}$. Veja que, para $w \neq \varnothing$, deve-se ter que $v \neq \varnothing$, ou w não seria reduzida. □

Proposição 2.1.23. Todo grupo livre é livre de torção.

Demonstração. Seja F um grupo livre com base X. Dado $w \in F\backslash\{\varnothing\}$, queremos mostrar que $w^n \neq \varnothing, \forall n \in \mathbb{N}$. Equivalentemente, queremos mostrar que $|w^n| > 0$, para todo $n \in \mathbb{N}$. Pelo corolário anterior, existem palavras u, v de F, com $v \neq \varnothing$ ciclicamente reduzida, tais que $w = uvu^{-1}$. Assim,

$$|w| \geq |v^n| = n|v| > n > 0$$

□

Observe que, se F é um grupo livre de ordem 1, então $F \simeq \mathbb{Z}$ e, portanto, é abeliano.

Proposição 2.1.24. Todo grupo livre com posto pelo menos 2 não é solúvel. Em particular, grupos livres de posto 2 ou maior não são abelianos.

Demonstração. Seja F um grupo livre com base X, onde $|X| \geq 2$. Suponha que F seja solúvel. Dados x_1, x_2 dois elementos distintos de X, $F_2 = \langle x_1, x_2 \rangle$ é um subgrupo livre de F, pelo Corolário 2.1.20. O grupo alternado de ordem 5 tem dois geradores, a saber $a_1 = (12)(34), a_2 = (235)$. Podemos definir $f : \{x_1, x_2\} \to A_5$ que faz as correspondências $f(x_1) = a_1$ e $f(x_2) = a_2$. Pela propriedade universal de F_2, existe um único homomorfismo $\varphi : F_2 \to A_5$ tal que $\varphi(x_1) = a_1,\ \varphi(x_2) = a_2$. Como φ leva geradores de F_2 nos geradores de A_5, ela é sobrejetiva. Pela Proposição 1.4.4, F_2 é solúvel e, pela proposição 1.4.5, segue que A_5 é solúvel, uma contradição. □

2.2 Geradores e Apresentações de Grupos

Existem várias maneiras de definir um grupo, dentre elas, existe uma maneira bastante reduzida à qual chamamos a *apresentação do grupo*. Essa é construída a partir de dois conjuntos: um conjunto de elementos que geram o grupo e um conjunto que descreve igualdades entre elementos do grupo. Mais especificamente, um grupo tem apresentação como a descrita acima se for isomorfo ao quociente do grupo livre que tem como base o conjunto dos geradores do grupo pelo fecho normal do conjunto que descreve as igualdades entre elementos do conjunto.

Todo grupo possui apresentação, como mostra a seguinte proposição, mas, mais do que isso, todo grupo tem várias apresentações. Veremos como as várias apresentações de um mesmo grupo são relacionadas.

Proposição 2.2.1. Todo grupo é um quociente de algum grupo livre.

Demonstração. Dado um grupo G, pode-se estender a aplicação identidade $id_G : G \to G$ a um homomorfismo $\mathscr{I} : F(G) \to G$, que é sobrejetor, pois os elementos da base são levados em todo G. Assim, $F(G)/Ker\mathscr{I}$ é isomorfo a G, pelo primeiro Teorema do isomorfismo. □

2.2.1 Definições e Exemplos

Sejam G um grupo, X um conjunto e $\varphi : F(X) \to G$ um epimorfismo, onde $F(X)$ denota um grupo livre com base X, pela proposição anterior, $G \simeq F(X)/Ker(\varphi)$. Denote $N = Ker(\varphi)$.

Como X gera $F(X)$ e todo elemento de G pode ser visto como uma classe lateral Nf, com $f \in F(X)$, tem-se que $\{Nx : \ x \in X\}$ gera G de certa forma. Tem-se que $G = \langle \varphi(x) : \ x \in X \rangle$. Dizemos então que $\{\varphi(x) : \ x \in X\}$ é um *conjunto gerador de* G e nos referimos a seus elementos como *geradores* de G. Também podemos nos referir ao próprio X como um gerador de G, por conveniência.

Se $\tilde{f} \in N$, então $\varphi(\tilde{f})$ é a identidade em G. Dizemos que $N = Ker(\varphi)$ é o *conjunto de relatores* de G. Se x e y são palavras, não necessariamente reduzidas, tais que $\varphi(x) = \varphi(y)$, então $xy^{-1} \in N$. Dizemos nesse caso que xy^{-1} é um *relator* de G, ou ainda que $\varphi(xy^{-1})$ é um relator de G. Nesse caso, a igualdade $\varphi(x) = \varphi(y)$ é dita uma *relação* em G. Como a cada relator de G corresponde uma relação em G e a cada relação corresponde um relator em G, usaremos a notação mais adequada – de relator ou de relação – aos propósitos almejados.

Dados um grupo H e um subconjunto $S \subset H$, dizemos que o fecho normal $\langle S \rangle^H$ é o *conjunto das consequências* de S em H e que seus elementos são *consequências* do mesmo.

Se $Ker\varphi$ é o conjunto das consequências de algum subconjunto $R \subset F(X)$, dizemos que R é *conjunto de relatores de G com respeito a φ*. Nesse caso, existe o correspondente *conjunto de relações com respeito a φ*.

Uma *apresentação* do grupo G é constituída de um conjunto de geradores X, um epimorfismo φ do grupo livre $F(X)$ com base X em G e um conjunto R de relatores (ou relações, quando for conveniente) de G com respeito a φ. Tal apresentação é denotada por $\langle X|R \rangle^\varphi$. Para indicar que essa é uma apresentação de G, escreveremos $G = \langle X|R \rangle^\varphi$. Veja que isso é equivalente a afirmar que G é isomorfo a $F(X)/\langle R \rangle^{F(X)}$.

Por simplicidade, poderemos omitir φ da notação dada, especialmente quando φ for a projeção de $F(X)$ em $F(X)/\langle R \rangle^{F(X)}$ ou ainda quando φ for injetora em X, de modo que X pode ser visto como um subconjunto de G.

Diremos que um grupo G é *finitamente apresentável* se possui apresentação $\langle X|R \rangle^\varphi$ na qual X e R são finitos. Nesse caso, dizemos essa é uma *apresentação finita*.

Exemplo 2.2.2. Dado um grupo livre $F(X)$, seja $\varphi : F(X) \to F(X)/\langle \varnothing \rangle^{F(X)}$ o epimorfismo canônico.

Como o menor subgrupo normal de $F(X)$ contendo o vazio é $\{1\}$, tal epimorfismo coincide com a identidade. Tem-se então que $\langle X|\varnothing \rangle$ é uma apresentação para $F(X)$

Exemplo 2.2.3. Seja $G = \mathbb{Z} \times \mathbb{Z}$, grupo com a operação soma. Então $x = (1, 0)$ e $y = (0, 1)$ são geradores de G. Por se tratar de um grupo abeliano, devemos ter que todos os elementos em G comutam. Ou, equivalentemente, os elementos que o geram comutam. Logo, $xyx^{-1}y^{-1}$ é relator de G (com relação equivalente $xy = yx$). Tem-se $G = \langle x, y|xyx^{-1}y^{-1} \rangle$, ou seja, $G \simeq F/\langle \{xyx^{-1}y^{-1}\} \rangle^F$, onde F é o grupo livre com base $\{x, y\}$.

Exemplo 2.2.4. Seja $\langle a \rangle$ o grupo cíclico de ordem n gerado por a. Então $X = \{a\}$ é gerador de $\langle a \rangle$ e devemos ter $a^n = 1$. Logo, essa é uma relação em $\langle a \rangle$, com relator correspondente a^n. Assim, $\langle a \rangle = \langle a|a^n \rangle$ ou $\langle a|a^n = 1 \rangle$, ou seja, $\langle a \rangle \simeq F(a)/\langle a^n \rangle^{F(a)}$.

Exemplo 2.2.5. O grupo que possui apresentação $\langle x,y|xy^2=yx^3, yx^2=x^3y\rangle$ é o grupo trivial. De fato, da primeira relação dada, vem $xy^2x^{-1}=y^3$. Assim, $xy^4x^{-1}=(xy^2x^{-1})^2=(y^3)^2=y^6$. Segue que $x^2y^4x^{-2}=x(xy^4x^{-1})x^{-1}=xy^6x^{-1}=(xy^2x^{-1})^3=y^9$. Tem-se $y^9=yy^9y^{-1}=yx^2y^4x^{-2}y^{-1}=yx^2y^{-1}y^4yx^{-2}y^{-1}$. Da segunda relação dada, tem-se que $yx^2y^{-1}=x^3$, logo, $x^2y^4x^{-2}=yx^2y^{-1}y^4yx^{-2}y^{-1}=x^3y^4x^{-3}$. Como $x^2y^4x^{-2}=x^3y^4x^{-3}$, multiplicando os dois lados à direita por x^3 e à esquerda por x^{-2}, obtém-se $y^4x=xy^4$, ou seja, $y^4=xy^4x^{-1}=y^6$. Segue que $y^2=1$. Por isso, $x=xy^2=y^3x=yx$. Segue que $y=1$. Assim, $x^2=yx^2=x^3y=x^3$. Segue que $x=1$.

Exemplo 2.2.6. O grupo diedral D_{2n} tem como conjunto de geradores $X=\{r,f\}$, onde r é a rotação por $\frac{2\pi}{n}$ e f é a reflexão, como visto anteriormente. Devemos ter que $r^n=1$, que $f^2=1$ e que $(rf)^2=1$. Assim, $D_n=\langle r,f|r^n,f^2,(rf)^2\rangle$.
Já o grupo Diedral Infinito tem apresentação $D_\infty=\langle r,f|f^2,(rf)^2\rangle=\langle r,f|f^2,frf=r^{-1}\rangle$.

Exemplo 2.2.7. O Grupo $\mathbb{H}_3(\mathbb{Z})$ de Heisenberg em $\mathbb{Z}$ de ordem 3 tem como geradores

$$X=\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}\quad Y=\begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix}$$

Além disso, vimos que $Z=\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix}=XYX^{-1}Y^{-1}$. Devemos ter que $XYX^{-1}Y^{-1}=Z$ e que Z comuta com os demais elementos do grupo. Pode-se mostrar que essas são as únicas relações em $\mathbb{H}_3(\mathbb{Z})$. Assim,

$$H_3(\mathbb{Z})=\langle X,Y|XYX^{-1}Y^{-1}Z^{-1},XZX^{-1}Z^{-1},YZY^{-1}Z^{-1}\rangle$$

Exemplo 2.2.8. O produto cartesiano entre dois grupos $G=\langle X\rangle$ e $H=\langle Y\rangle$ pode ser considerado como um grupo gerado por $X\cup Y$, quando G e H são vistos como subgrupos de $G\times H$. Assim, se $G=\langle X|R\rangle$ e $H=\langle Y|S\rangle$, então $R\cup S$ é um conjunto de relatores em $G\times H$.

Tem-se também que os elementos de G comutam com os elementos de H. De fato, se $g\in G$ e $h\in H$, tem-se que $(g,1)(1,h)(g,1)^{-1}=(g,1)(1,h)(g^{-1},1)=(g,h)(g^{-1},1)=(1,h)$. Assim, $[G,H]$ (cf. Definição 1.4.1) é trivial em $G\times H$. Portanto, devemos ter $[X,Y]$ no conjunto de relatores de $G\times H$. A apresentação do produto direto entre $G\times H$ é dada por

$$G\times H=\langle X\cup Y|R\cup S\cup[X,Y]\rangle.$$

Mais geralmente, se $\{G_k\}_{k=1}^n$ é uma família de grupos, com $G_k=\langle X_k|R_k\rangle$, , então

$$\times_{k=1}^n G_k=\langle\bigcup_{k=1}^n X_n|\bigcup_{k=1}^n R_k,[X_i,X_j]:i\neq j\rangle$$

Exemplo 2.2.9. Sejam A e B grupos e $\varphi:B\to Aut(A)$ um homomorfismo de grupos. Dadas apresentações $A=\langle X|R\rangle$ e $B=\langle Y|S\rangle$, uma apresentação para produto semidireto $A\rtimes B$ com relação a φ é dada por

$$A\rtimes_\varphi B=\langle X,Y|R,S,\{yxy^{-1}(\varphi(y)(x))^{-1}:\ x\in X,\ y\in Y\}\rangle.$$

2.2.2 Teorema de Von Dick

Teorema 2.2.10. (Von Dick) Sejam G um grupo com apresentação $\langle X|R\rangle^{\varphi}$ e H um grupo. Seja ainda F um grupo livre com base X e $f : X \to H$ uma função que é estendida a um homomorfismo $\psi : F \to H$ dado pela propriedade universal de F. Se $\psi(R) = \{1\}$, então existe um homomorfismo $\zeta : G \to H$ tal que $f(x) = \zeta \circ \varphi(x), \forall x \in X$. Além disso, se $f(X)$ gera H, então ζ é sobrejetiva.

Demonstração. A afirmação $\psi(R) = \{1\}$ equivale a afirmar que $R \subset Ker(\psi)$. Por definição, $Ker(\varphi) = \langle R\rangle^{F}$, logo, $Ker(\varphi) \subset Ker(\psi)$.

Pela Proposição 1.3.8, como φ é epimorfismo, existe um homomorfismo $\zeta : G \to H$ tal que $\zeta \circ \varphi = \psi$.

Se $f(x)$ gera H, então φ é sobrejetiva. Assim, dado $h \in H$, existe $w \in F$ tal que $\varphi(w) = h$. Assim, $h = \psi(w) = \zeta(\varphi(w)) \in Im(\zeta)$.

$$\begin{tikzcd}
F \arrow[r, "\psi"] \arrow[d, "\varphi"'] & H \\
F/Ker(\varphi) \simeq G \arrow[ur, "\exists\zeta"'] &
\end{tikzcd}$$

□

Corolário 2.2.11. Sejam $G = \langle X|R\rangle$, Y um conjunto e $F(X), F(X \cup Y)$ grupos livres com bases X e $X \cup Y$. Dado $S \subset F(X \cup Y)$, existe um homomorfismo ζ que leva G em $\langle X \cup Y|R \cup S\rangle$.

Demonstração. Pelo Teorema 2.2.10, a inclusão $X \hookrightarrow \langle X \cup Y|R \cup S\rangle$ induz tal homomorfismo. □

Dado um grupo H, como saber se uma apresentação $\langle X|R\rangle$ é apresentação de H? O Teorema anterior pode ser utilizado com o intuito de resolver tal problema: Se X é um conjunto de geradores de H e R é algum conjunto constituído de relatores de G, então existe uma aplicação $f : X \to H$ com homomorfismo correspondente $\varphi : F(X) \to H$ tal que $R \subset Ker\varphi$. Como $F(X)$ gera H, pelo teorema anterior, existe um epimorfismo $\zeta : G \to H$, onde $G = \langle X|R\rangle$. Devemos então mostrar que ζ é injetor.

Se H é finito, basta mostrar que G também é finito e que $|G| \leq |H|$. Caso contrário, o processo dependerá do conjunto de relatores escolhido. Muitas vezes tal escolha permite que os elementos do grupo G sejam descritos de maneira mais simples, facilitando a verificação de que a aplicação é de fato injetiva.

Podemos encontrar uma apresentação para um grupo H usando o processo descrito acima, caso exista uma conjunto de relatores com geradores X que seja um candidato a conjunto de relatores de H. Um exemplo no caso finito é a apresentação do grupo cíclico $\langle a\rangle$ de ondem n, vista no Exemplo 2.2.4. Um conjunto de geradores é $X = \{a\}$ e um conjunto de relatores é $R = \{a^n\}$. Como $G = \langle a|a^n\rangle$ é finito e possui n elementos, tem-se que $|G| = |\langle a\rangle|$.

Exemplo 2.2.12. Para o caso infinito, mostraremos que o grupo $Iso(\mathbb{Z})$, das isometrias bijetivas em $\mathbb{Z}$, admite apresentação $\langle x, y|y^2, (xy)^2\rangle$.
Sejam $x, y \in Iso(\mathbb{Z})$ dadas por $x(z) = z + 1$ e $y(z) = -z$. Tem-se que $X = \{x, y\}$ é gerador de

$Iso(\mathbb{Z})$. Julgamos que $R = \{y^2, (xy)^2\}$ seja conjunto de relatores de $Iso(\mathbb{Z})$. Veja que $y^2(z) = y(y(z)) = y(-z) = z$ e que $(xy)^2(z) = x(y(x(y(z)))) = x(y(x(-z))) = x(y(-z+1)) = x(z-1) = z$. Logo, esses são relatores de $Iso(\mathbb{Z})$, de fato. Além disso, $y^j = y$, se j é ímpar e $y^j = 1$, se j é par. Assim, podemos considerar apenas os produtos em que y tem potência 1.

Como $xyxy = 1$, tem-se que $xyx = y^{-1} = y$. Assim, $x^k y x^l = x^{k-1}(xyx^{-1})x^{l-1} = x^{k-1}yx^{l-1} = \ldots = x^{k-l}y$. De modo geral, podemos repetir esse processo, encontrando sempre elementos da forma $x^\alpha y$. Ou seja, todo elemento de $G = \langle X|R\rangle$ é de uma das formas: $x^\alpha y$ ou x^α, $\alpha \in \mathbb{Z}$.

Tomando $i : X \hookrightarrow Iso(\mathbb{Z})$, a inclusão, e $\mathfrak{I} : F(X) \to Iso(\mathbb{Z})$ o homomorfismo correspondente, pelo Teorema 2.2.10, existe um homomorfismo $\zeta : \langle X|R\rangle \to Iso(\mathbb{Z})$ tal que $\zeta \circ \varphi = i$, onde $\varphi : F(X) \to F(X)/\langle R\rangle^{F(X)}$ é o homomorfismo canônico. Como $i(X)$ gera $Iso(\mathbb{Z})$, ζ é epimorfismo.

Tem-se que $x = i(x) = \zeta(\varphi(x))$ e $y = \zeta(\varphi(y))$, pois $x, y \in X$. Desse modo, como todo elemento de G é da forma $x^\alpha y$ ou da forma x^α, segue que $Ker\zeta = \{1\}$.

Teorema 2.2.13. (Von Dick II) Sejam G um grupo e R um subconjunto de G. Dado um homomorfismo de grupos $\psi : G \to H$ tal que $R \subset Ker(\psi)$ existe um homomorfismo $\zeta : G/\langle R\rangle^G \to H$ tal que $\zeta \circ \pi = \psi$, onde π é o homomorfismo canônico entre G e $G/\langle R\rangle^G$.

Demonstração. Como $R \subset Ker(\psi)$, tem-se que $Ker(\pi) = \langle R\rangle^G \subset Ker(\psi)$. Além disso, $\pi : G \to G/\langle R\rangle^G$ é um epimorfismo. Segue da Proposição 1.3.8 que existe um homomorfismo $\zeta : G/\langle R\rangle^G \to H$ tal que $\zeta \circ \pi = \psi$.

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[d, "\pi"'] & H \\
G/\langle R\rangle^G \arrow[ur, "\exists\zeta"'] &
\end{tikzcd}$$

$\square$

2.2.3 Transformações de Tietze

Um grupo G pode ter inúmeras apresentações $\langle X|R\rangle^\varphi$, mesmo para X e φ fixados. Por exemplo, o Grupo Diedral D_n tem apresentação $D_n = \langle r, f | r^n, f^2, (rf)^2\rangle$, como visto no Exemplo 2.2.6. Como $f^2 = 1$ e $r^n = 1$, tem-se que $f^{2m} = (f^2)^m = 1$ e $r^{nk} = (r^n)^k = 1, \forall\ m, k \in \mathbb{Z}$. Assim, $R_k = \{r^{jn} : j = 1, \ldots, k\} \cup \{f^{2j} : j = 1, \cdots, k\}$ é tal que $\langle r, f | R_k, (rf)^2\rangle$ é apresentação de $D_n, \forall k \in \mathbb{Z}^+$. Ou seja, existem infinitas apresentações de D_n.

Veremos agora como relacionar as diferentes apresentações de um grupo.

Se $\langle X|R\rangle^\varphi$ é uma apresentação de um grupo G, então, para cada $S \subset \langle R\rangle^{F(X)}$, tem-se que $\langle X|R \cup S\rangle^\varphi$ também é apresentação de G. Assim, podemos fazer a a seguinte definição:

Definição 2.2.14. Seja $\langle X|R\rangle^\varphi$ uma apresentação do grupo G. Dado $S \subset \langle R\rangle^{F(X)}$, dizemos que a apresentação $\langle X|R \cup S\rangle^\varphi$ de G é obtida de $\langle X|R\rangle^\varphi$ por uma *Transformação de Tietze do tipo I* e que $\langle X|R\cup S\rangle^{\varphi}$ é obtida de $\langle X|R\rangle^{\varphi}$ por uma *Transformação de Tietze do tipo* $\overline{I}$. Se $|S|=1$, dizemos que cada uma das apresentações dada é obtida da outra por uma *transformação simples de Tietze* do tipo correspondente.

Vejamos agora outra maneira de obter uma apresentação a partir de outra. Dado um grupo G com apresentação $\langle X|R\rangle^{\varphi}$, tome um conjunto Y disjunto de X e atribua cada $y\in Y$ a um elemento $m_y\in F(X)$. Afirmamos que $\langle X\cup Y|R\cup\{ym_y^{-1}:\ y\in Y\}\rangle^{\psi}$, onde $\psi(x)=\varphi(x),\forall x\in X$ e $\psi(y)=\varphi(m_y),\forall y\in Y$, é uma apresentação de G.

Denote por N o conjunto das consequências de $R\cup\{ym_y^{-1}\ :\ y\in Y\}$ em $F(X\cup Y)$. Como $R\subset Ker\varphi$, $\psi(r)=\varphi(r)=1,\forall r\in R$ e $\psi(ym_y^{-1})=\psi(y)\psi(m_y)^{-1}=\varphi(m_y)\varphi(m_y)^{-1}=1$, tem-se que $R\cup\{ym_y^{-1}\ :\ y\in Y\}\subset Ker\varphi$. Além disso, como φ é sobrejetora, ψ é sobrejetora. Assim, ψ induz um epimorfismo $\phi:F(X\cup Y)/N\to G$ tal que $\phi(uN)=\psi(u)$, para toda palavra $u\in F(X\cup Y)$.

Agora, $F(X)=\langle X|\varnothing\rangle$ é um grupo livre tal que $R\subset F(X)$. Sejam $i:F(X)\to F(X\cup Y)$ a inclusão e $\phi:F(X\cup Y)\to F(X\cup Y)/N$ o homomorfismo canônico. Considere o homomorfismo $\mu:\rho\circ i:F(X)\to F(X\cup Y)/N$. Pelo Teorema de Von Dick II (2.2.13), existe um homomorfismo ζ : $G=F(X)/\langle R\rangle^{F(X)}\to F(X\cup Y)/N$ tal que $\zeta\circ\varphi=\mu$, lembrando que $\varphi:F(X)\to F(X)/\langle R\rangle^{F(X)}$ é o homomorfismo canônico. Ou seja, $\zeta(\varphi(x))=xN$.

Dado $g\in G$, existe $w\in F(X)$ tal que $\varphi(w)=g$. Assim,

$$\phi\circ\zeta(g)=\phi(\zeta(\varphi(w)))=\phi(wN)=\psi(w)=\varphi(w)=g,$$

pois w é uma palavra do alfabeto X.

Além disso, dados $x\in X\subset F(X\cup Y)$ e $y\in Y\subset F(X\cup Y)$, tem-se que

$$\zeta\circ\phi(xN)=\zeta(\psi(x))=\zeta(\varphi(x))=\mu(x)=xN \text{ e}$$

$$\zeta\circ\phi(yN)=\zeta(\psi(y))=\zeta(\varphi(m_y))=\mu(m_y)=m_yN=yN,$$

pois $ym_y^{-1}\in N$.

Assim, se v é uma palavra em $F(X\cup Y)$, então $\zeta(\phi(vN))=vN$.

Segue que $\phi^{-1}=\zeta$ e, portanto, ϕ é um isomorfismo entre $F(X\cup Y)/N=\langle X\cup Y|R\cup\{ym_y^{-1}:\ y\in Y\}\rangle^{\psi}$ e G.

Definição 2.2.15. Com a notação anterior, dizemos que $\langle X\cup Y|R\cup\{ym_y^{-1}\ :\ y\in Y\}\rangle^{\psi}$ é obtido de $\langle X|R\rangle^{\varphi}$ por uma *Transformação de Tietze do tipo II* e que $\langle X|R\rangle^{\varphi}$ é obtido de $\langle X\cup Y|R\cup\{ym_y^{-1}\ :\ y\in Y\}\rangle^{\psi}$ por uma *Transformação de Tietze do tipo* $\overline{II}$. Se $|Y|=1$, iremos utilizar o termo *Transformação simples de Tietze* do tipo II ou $\overline{II}$.

Lema 2.2.16. Sejam G um grupo e $\langle X|R\rangle^{\varphi}$ uma apresentação de G.

i. Se $\langle X|R\cup S\rangle^{\varphi}$ é obtida de $\langle X|R\rangle^{\varphi}$ por uma Transformação de Tietze do tipo I e $|S|$ é finito, então $\langle X|R\cup S\rangle^{\varphi}$ pode ser obtido de $\langle X|R\rangle^{\varphi}$ por um número finito de transformações simples de Tietze do tipo I;

ii. Se $\langle X\cup Y|R\cup\{ym_y^{-1}\ :\ y\in Y\}\rangle^{\psi}$ é obtida de $\langle X|R\rangle^{\varphi}$ por uma Transformação de Tietze do tipo II e $|Y|$ é finito, então $\langle X\cup Y|R\cup\{ym_y^{-1}\ :\ y\in Y\}$ pode ser obtido de $\langle X|R\rangle^{\varphi}$ por um número finito de transformações simples de Tietze do tipo II.

Demonstração. Segue direto das respectivas definições. $\square$

Teorema 2.2.17. Seja G um grupo. Duas apresentações $\langle X|R\rangle^{\varphi}$ e $\langle Y|S\rangle^{\psi}$ de G são obtidas uma da outra por uma sequência de Transformações de Tietze.

Demonstração. Inicialmente, assuma que X e Y sejam disjuntos. Para cada $y \in Y$, escolha $m_y \in F(X)$ tal que $\psi(y) = \varphi(m_y)$ e, para cada $x \in X$, escolha $n_x \in F(Y)$ tal que $\varphi(x) = \psi(n_x)$. Defina

$$\chi(z) = \begin{cases} \varphi(z), \text{ se } z \in X \\ \psi(z), \text{ se } z \in Y \end{cases}$$

Então $\langle X \cup Y | R \cup \{ym_y^{-1} \ : \ y \in Y\}\rangle^{\chi}$ é uma apresentação de G obtida de $\langle X|R\rangle^{\varphi}$ por uma transformação de Tietze do tipo II.

Pela escolha de m_y, vale que $\chi(y) = \varphi(m_y) = \psi(y)$. Logo, $\chi(w) = \psi(w), \forall w \in F(Y)$. Em particular, $\chi(s) = \psi(s) = 1, \forall s \in S$, de modo que $S \subset Ker\chi$.

Por outro lado, $\chi(n_x) = \psi(n_x) = \varphi(x), \forall x \in X$. Como $\varphi(x) = \chi(x)$, tem-se que $\chi(n_x) = \chi(x)$, logo, $xn_x^{-1} \in Ker\chi, \forall x \in X$. Assim $\langle X \cup Y | R \cup S \cup \{xn_x^{-1} \ : \ x \in X\} \cup \{ym_y^{-1} \ : \ y \in Y\}\rangle$ é obtido de $\langle X \cup Y | R \cup S \cup \{ym_y^{-1} \ : \ y \in Y\}\rangle$.

Por simetria, essa apresentação também é obtida de $\langle Y|S\rangle^{\psi}$ por uma transformação de Tietze do tipo II seguida por uma transformação de Tietze do tipo I. Segue que $\langle Y|S\rangle^{\psi}$ é obtida de $\langle X \cup Y | R \cup S \cup \{xn_x^{-1} \ : \ x \in X\} \cup \{ym_y^{-1} \ : \ y \in Y\}\rangle$ por uma transformação de Tietze do tipo $\overline{I}$ seguida de uma do tipo $\overline{II}$. Como $\langle X \cup Y | R \cup S \cup \{xn_x^{-1} \ : \ x \in X\} \cup \{ym_y^{-1} \ : \ y \in Y\}\rangle$ é obtida de $\langle X|R\rangle^{\varphi}$ por uma transformação de Tietze, o resultado segue.

Agora, se $X \cap Y \neq \varnothing$, podemos achar um conjunto $\tilde{X}$ tal que exista uma bijeção $x \mapsto \tilde{x}$ entre X e $\tilde{X}$ mas tal que $\tilde{X}$ seja disjunto de X e de Y. Sejam $\tilde{R}$ o conjunto obtido de R fazendo a correspondência $x \mapsto \tilde{x}$ e $\tilde{\varphi}$, definida de forma similar: $\tilde{\varphi}(\tilde{x}) = \varphi(x)$. Então, $\langle \tilde{X}|\tilde{R}\rangle^{\tilde{R}}$ é apresentação de G. Pela parte anterior, $\langle \tilde{X}|\tilde{R}\rangle^{\tilde{R}}$ é obtida de $\langle X|R\rangle^{\varphi}$ e de $\langle Y|S\rangle^{\psi}$ por sequências de Transformações de Tietze. Portanto, $\langle X|R\rangle^{\varphi}$ é obtida de $\langle Y|S\rangle^{\psi}$ por sequências de Transformações de Tietze. $\square$

Corolário 2.2.18. Se $\langle X|R\rangle^{\varphi}$ e $\langle Y|S\rangle^{\psi}$ são apresentações finitas de um grupo G, então uma pode ser obtida da outra por uma sequência de Transformações simples de Tietze.

Esse corolário é consequência imediata do teorema anterior juntamente com o Lema 2.2.16. De fato, pelo teorema anterior, uma representação pode ser obtida da outra por uma sequência de transformações de Tietze (finita, pela demonstração) e, pelo lema, cada uma dessas Transformações é uma sequência finita de Transformações simples de Tietze.

Proposição 2.2.19. Seja G um grupo finitamente gerado. Se $\langle Y|S\rangle^{\psi}$ é apresentação de G, então existe subconjunto finito de Y que gera G.

Demonstração. G possui um gerador finito $X \subset G$. Cada elemento de X é produto de elementos de $\psi(Y)$ e de suas inversas, de modo que existe $Y_1 \subset Y$ tal que $X \subset \langle \psi(Y_1)\rangle$. Segue que Y_1 é o subconjunto de Y procurado. $\square$

Vale a pena ressaltar que muitas vezes o conjunto de relatores com respeito a Y_1 é maior que $S \cap F(Y_1)$.

Proposição 2.2.20. Seja G um grupo que possui apresentação finita $\langle X|R\rangle^{\varphi}$. Seja $\langle Y|S\rangle^{\psi}$ outra apresentação de G tal que Y é finito. Então existe um subconjunto finito $S_1 \subset S$ tal que $G = \langle Y|S_1\rangle^{\psi}$.

Demonstração. Para cada $y \in Y$, escolha $m_y \in F(X)$ tal que $\psi(y) = \varphi(m_y)$ e, para cada $x \in X$, escolha $n_x \in F(Y)$ tal que $\varphi(x) = \psi(n_x)$. Tome $\mathcal{R} = \{ym_y^{-1} \ : \ y \in Y\} \cup R$. Então, G tem apresentação $\langle X \cup Y|\mathcal{R} \cup \{xn_x^{-1}\}_{x\in X}\rangle^{\chi}$, onde $\chi(z) = \begin{cases} \varphi(z), \text{ se } z \in X \\ \psi(z), \text{ se } z \in Y \end{cases}$.

Dado $r \in \mathcal{R}$, denote por $\tilde{r}$ o elemento obtido de r ao substituir-se cada x por n_x, de modo que $\tilde{r} \in F(Y)$. Seja $\tilde{\mathcal{R}} = \{\tilde{r} : r \in \mathcal{R}\}$.

Mostremos que $\tilde{K} = \langle\tilde{\mathcal{R}}\rangle^{F(X\cup Y)} \subset K = \langle\mathcal{R} \cup \{xn_x^{-1}\}_{x\in X}\rangle^{F(X\cup Y)}$. Para isso, mostremos que $\tilde{K}$ está contido no núcleo da projeção canônica $\pi : F(X \cup Y) \to F(X \cup Y)/K$. Tem-se que

$$\pi(\tilde{K}) = \pi(\langle\tilde{\mathcal{R}}\rangle^{F(X\cup Y)}) = \langle\pi(\tilde{\mathcal{R}})\rangle^{\pi(F(X\cup Y))}$$

Assim, $\pi(\tilde{K}) = 1$ se, e somente se, $\pi(\tilde{\mathcal{R}}) = 1$.

Veja que, como $xn_x^{-1} \in K$, $\pi(x) = \pi(n_x^{-1})$. Assim, $\pi(r) = \pi(\tilde{r}), \forall r \in R$ e, como $r \in R$, vale que $\pi(\tilde{r}) = \pi(r) = 1$.
Por uma transformação de Tietze do tipo I, obtemos a apresentação $\langle X \cup Y|R, \tilde{\mathcal{R}}, \{xn_x^{-1}\}_{x\in X}\rangle^{\chi}$ e, por uma transformação de Tietze do tipo $\overline{I}$ desta, obtemos $\langle X \cup Y|\tilde{\mathcal{R}}, \{xn_x^{-1}\}_{x\in X}\rangle^{\chi}$. Além disso, $n_x \in F(Y)$ e $\tilde{\mathcal{R}} \subset F(Y)$. Por uma aplicação de Tietze do tipo $\overline{II}$, obtemos a apresentação $\langle Y|\tilde{\mathcal{R}}\rangle^{\psi}$. Por hipótese, X, Y e R são finitos, assim $\tilde{\mathcal{R}}$ é finito. Além disso, como $\tilde{\mathcal{R}} \subset \langle S\rangle^{F(Y)}$, cada um de seus elementos é o produto de finitos elementos conjugados em S e suas inversas. Escolha uma tal expressão para cada $\tilde{r}$ em $\tilde{\mathcal{R}}$ e seja S_1 constituído de tais escolhas de elementos. Por essa escolha, S_1 é finito. Tem-se ainda que $Ker\psi = \langle S\rangle^{F(Y)}$ e também que $Ker\psi = \langle\tilde{\mathcal{R}}\rangle^{F(Y)}$, logo, devemos ter que $Ker\psi = \langle S_1\rangle^{F(Y)}$. $\square$

2.3 Produtos Livres

Definição 2.3.1. Dados G_1, G_2, G grupos e $i_1 : G_1 \to G$, $i_2 : G_2 \to G$ homomorfismos, dizemos que o par $(G, \{i_1, i_2\})$ é um *produto livre* entre G_1 e G_2 se satisfaz a propriedade universal: para cada grupo H e homomorfismos $f_1 : G_1 \to H$, $f_2 : G_2 \to H$, existe um único homomorfismo $f : G \to H$ tal que $f_1 = f \circ i_1$ e $f_2 = f \circ i_2$.

$$\begin{tikzcd} G_1 \arrow[r, "i_1"] \arrow[d, "f_1"'] & G \arrow[dl, "f"'] \\ H & G_2 \arrow[l, "i_2"] \arrow[u, "f_2"'] \end{tikzcd}$$

Quando não houver necessidade de explicitar G e os homomorfismos i_j, denotaremos o produto livre entre G_1 e G_2 simplesmente por $G_1 * G_2$.

Podemos generalizar o conceito de produto livre para uma família de grupos $\{G_\alpha\}_{\alpha\in A}$, onde A é um conjunto de índices qualquer:

Definição 2.3.2. Dados $\{G_\alpha\}_{\alpha\in A}$ uma família de grupos, G um grupo e $i_\alpha : G_\alpha \to G$ homomorfismo, para cada $\alpha \in A$, dizemos que $(G, \{i_\alpha\}_{\alpha\in A})$ é um *produto livre* dos grupos G_α se satisfaz a seguinte propriedade universal: para cada grupo H e homomorfismos $f_\alpha : G_\alpha \to H$, existe um único homomorfismo $f : G \to H$ satisfazendo $f_\alpha = f \circ i_\alpha$.

Novamente, quando não houver necessidade de explicitar G e os homomorfismos i_α, denotaremos o produto livre dos G_α por $*_{\alpha\in A}G_\alpha$ ou simplesmente por $*G_\alpha$. No caso particular em que $A = \{1, 2, \ldots, n\}$, escreveremos $*_{\alpha\in A}G_\alpha$ na forma $G_1 * G_2 * \ldots * G_n$.

A seguir, mostraremos que o produto livre de uma família de grupos $\{G_\alpha\}_{\alpha\in A}$ é único, a menos de isomorfismo.

Proposição 2.3.3. Se $(G, \{i_\alpha\})$ e $(H, \{j_\alpha\})$ são produtos livres da mesma família de grupos $\{G_\alpha\}_{\alpha\in A}$, então existe um único isomorfismo $f : G \to H$ tal que $f \circ i_\alpha = j_\alpha, \forall \alpha \in A$.

Demonstração. Pela propriedade universal do produto livre $(G, \{i_\alpha\})$, existe um único homomorfismo $f : G \to H$ tal que $j_\alpha = f \circ i_\alpha$.

Já pela propriedade universal de $(H, \{j_\alpha\})$, existe um único homomorfismo $\tilde{f} : H \to G$ tal que $i_\alpha = \tilde{g} \circ j_\alpha$.

Assim,

$$(\tilde{f} \circ f) \circ i_\alpha = \tilde{f} \circ (f \circ i_\alpha) = \tilde{f} \circ j_\alpha = i_\alpha$$

$$(f \circ \tilde{f}) \circ j_\alpha = f \circ (\tilde{f} \circ j_\alpha) = f \circ i_\alpha = j_\alpha$$

Por um argumento análogo ao dado na Observação 2.1.2, segue que $f \circ \tilde{f} = id_H$ e $\tilde{f} \circ f = id_G$, onde id_H, id_G são as aplicações identidade em H e G, respectivamente. Portanto, f é o isomorfismo procurado. □

Como o produto livre é único a menos de isomorfismo, nos referiremos a ele como "o"produto livre dos grupos G_α e não como "um"produto livre dos mesmos.

No estudo de grupos livres, mostramos que, se o par (G, i) é livre sobre o conjunto X, então i é injetiva. Um resultado análogo vale para produtos livres, como veremos a seguir.

Proposição 2.3.4. Seja $(G, \{i_\alpha\})$ um produto livre da família de grupos $\{G_\alpha\}_{\alpha\in A}$. Então, cada i_α é injetivo.

Demonstração. Seja $id_\alpha : G_\alpha \to G_\alpha$ a identidade em G_α. Pela propriedade universal de $(G, \{i_\alpha\})$, para cada $\alpha \in A$, existe um único homomorfismo $\varphi_\alpha : G \to G_\alpha$ tal que $id_\beta = \varphi_\alpha \circ i_\beta, \forall \beta \in A$.

Se $g_1, g_2 \in G_\alpha$ são tais que $i_\alpha(g_1) = i_\alpha(g_2)$, então $g_1 = id_\alpha(g_1) = \varphi_\alpha(i_\alpha(g_1)) = \varphi_\alpha(i_\alpha(g_2)) = id_\alpha(g_2) = g_2$. Segue que i_α é injetiva. □

Mostramos a unicidade de produtos livres na Proposição 2.3.3. Agora, a pergunta natural que devemos fazer é se produtos livres de fato existem. A resposta é dada pelo teorema a seguir.

Teorema 2.3.5. Toda família de grupos possui produto livre.

Demonstração. Seja $\{G_\alpha\}_{\alpha\in A}$ uma família de grupos na qual cada G_α tem apresentação $G_\alpha = \langle X_\alpha | R_\alpha\rangle^{\varphi_\alpha}$. Podemos assumir que os X_α são dois a dois disjuntos, pois caso não sejam, podemos substituí-los por conjuntos que estejam em bijeção com eles e que sejam dois a dois disjuntos.

Seja $G = \langle\bigcup_{\alpha\in A} X_\alpha | \bigcup_{\alpha\in A} R_\alpha\rangle^{\varphi}$, onde φ é a aplicação canônica

$$\varphi : F(\bigcup_{\alpha\in A} X_\alpha) \to F(\bigcup_{\alpha\in A} X_\alpha)/\langle\bigcup_{\alpha\in A} R_\alpha\rangle^{F(\bigcup_{\alpha\in A} X_\alpha)} = G.$$

Considere a inclusão $\iota_\alpha : X_\alpha \to \bigcup_{\alpha\in A} X_\alpha$. Tal aplicação pode ser vista como $\iota_\alpha : X_\alpha \to F(\bigcup_{\alpha\in A} X_\alpha)$. Pela propriedade universal do grupo livre $F(X_\alpha)$, existe um homomorfismo $\bar{\iota}_\alpha : F(X_\alpha) \to F(\bigcup_{\alpha\in A} X_\alpha)$ que é a identidade em X_α. Tome

$$j_\alpha = \varphi \circ \bar{\iota}_\alpha : F(X_\alpha) \to F(\bigcup_{\alpha\in A} X_\alpha)/\langle\bigcup_{\alpha\in A} R_\alpha\rangle^{F(\bigcup_{\alpha\in A} X_\alpha)} = G,$$

para cada $\alpha \in A$. Como $R_\alpha \subset \langle\bigcup R_\alpha\rangle^{F(\bigcup_{\alpha\in A} X_\alpha)}$, $j_\alpha(R_\alpha) = \{1\}$. Pelo Teorema de Von Dick II, existe um homomorfismo $i_\alpha : G_\alpha = F(X_\alpha)/\langle R_\alpha\rangle^{F(X_\alpha)} \to G$ tal que $i_\alpha \circ \varphi_\alpha = j_\alpha$.

A ideia é mostrar que $(G, \{i_\alpha\})$ é o produto livre de $\{G_\alpha\}_{\alpha\in A}$. Para isso, sejam H um grupo e $h_\alpha : G_\alpha \to H$ homomorfismo, para cada $\alpha \in A$. Mostremos que existe um único homomorfismo $h : G \to H$ tal que $h_\alpha = h \circ i_\alpha, \forall\alpha \in A$.

Cada $h_\alpha : G_\alpha \to H$ induz um homomorfismo $\delta_\alpha : F(X_\alpha) \to H$ tal que $\delta_\alpha(R_\alpha) = \{1\}$. Existe então um homomorfismo $\delta : F(\bigcup_{\alpha\in A} X_\alpha) \to H$ tal que $\delta|_{X_\alpha} = \delta_\alpha$. Pela escolha de δ, $\delta(\bigcup_{\alpha\in A} R_\alpha) = \{1\}$. Assim, por Von Dyck II, δ induz um homomorfismo $f : G \to H$ tal que $f \circ \varphi = \delta$.

Assim, $f(i_\alpha(\varphi_\alpha(x_\alpha))) = f(\varphi(x_\alpha)) = \delta(x_\alpha), \forall x_\alpha \in X_\alpha$, pelas definições de i_α e de f. Além disso, $\delta(x_\alpha) = \delta_\alpha(x_\alpha) = f_\alpha(\varphi_\alpha(x_\alpha))$, pela escolha de δ e pela definição de δ_α. Como $\varphi_\alpha(X_\alpha)$ gera G_α, tem-se de $f \circ i_\alpha(\varphi_\alpha(x_\alpha)) = \delta(x_\alpha) = f_\alpha(\varphi_\alpha(x_\alpha))$ que $f_\alpha = f \circ i_\alpha$. A unicidade de f segue do fato de G ser gerado por $\bigcup_{\alpha\in A} i_\alpha \circ \varphi_\alpha(X_\alpha)$. $\square$

Considere $*G_\alpha$. Como cada i_α é monomorfismo, podemos ver G_α como um subgrupo de $*G_\alpha$, com i_α sendo a inclusão de G_α em G.

O Teorema 2.3.5 nos mostra que se $G_\alpha = \langle X_\alpha | R_\alpha\rangle$, então $*G_\alpha = \langle\bigcup_{\alpha\in A} X_\alpha | \bigcup_{\alpha\in A} R_\alpha\rangle^{\varphi}$, onde

$$\varphi : F(\bigcup_{\alpha\in A} X_\alpha) \to F(\bigcup_{\alpha\in A} X_\alpha)/\langle\bigcup_{\alpha\in A} R_\alpha\rangle^{F(\bigcup_{\alpha\in A} X_\alpha)} = G$$

é a aplicação natural. Vejamos alguns exemplos de produtos livres.

Exemplo 2.3.6. Dado um conjunto X, o produto livre de $C_x, \forall x \in X$, onde C_x é o grupo cíclico infinito com gerador x é $F(X)$.

Isso ocorre pois $C_x = \langle x|\varnothing\rangle$, assim, com a notação anterior, $\bigcup_{x\in X} R_x = \varnothing$ de modo que $\langle\bigcup_{x\in X} R_x\rangle^{F(X)} = \{1\}$. Pelo Teorema 2.3.5, $*_{x\in X} C_x = F(X)/\langle\bigcup_{x\in X} R_x\rangle^{F(X)} = F(X)$.

Exemplo 2.3.7. Sejam $C_2 = \{1, x\} = \langle x|x^2\rangle$ e $\overline{C}_2 = \{1, y\} = \langle y|y^2\rangle$. Tem-se que $C_2 * \overline{C}_2 = \langle x, y|x^2, y^2\rangle$. Seja $z \in C_2 * \overline{C}_2$ o elemento dado por xy. Tem-se que $z^{-1}xy = 1$ é uma relação em $C_2 * \overline{C}_2$. Assim, aplicando transformações de Tietze, podemos escrever

$$C_2 * \overline{C}_2 = \langle x, y, z|x^2, y^2, z^{-1}xy\rangle$$

Como $y = zx^{-1}$, vale que $1 = y^2 = (zx^{-1})^2$. Podemos escrever $C_2 * \overline{C}_2 = \langle x, z | x^2, (zx^{-1})^2 \rangle$. Como $x^2 = 1$, tem-se que $x = x^{-1}$. Assim,

$$C_2 * \overline{C}_2 = \langle x, z | x^2, (zx)^2 \rangle$$

é o grupo diedral infinito.

Definição 2.3.8. Sejam $\{G_\alpha\}_{\alpha \in A}$ e $\{H_\alpha\}_{\alpha \in A}$ famílias de grupos e $\varphi_\alpha : G_\alpha \to H_\alpha$ homomorfismos. Como observado anteriormente, H_α pode ser tratado como um subgrupo de $*_{\alpha \in A} H_\alpha$. Podemos então ver φ_α como um homomorfismo de G_α em $*_{\alpha \in A} H_\alpha$. Tais homomorfismos dão origem a um único homomorfismo de G em H, denotado por $*_{\alpha \in A} \varphi_\alpha$.

Teorema 2.3.9. (Forma Normal Para Produtos Livres) Seja $(G, \{i_\alpha\})$ o produto livre da família de grupos $\{G_\alpha\}_{\alpha \in A}$. Se considerarmos i_α como a inclusão, todo elemento de G pode ser escrito de maneira única como $g_1 g_2 \dots g_n$, onde $n \geq 0$, $g_i \in G_{\alpha_i}$, para algum $\alpha_i \in A$, $g_i \neq 1$, para todo i e $\alpha_r \neq \alpha_{r+1}, \forall r < n$.

Demonstração. Pela construção de G, $\bigcup_{\alpha \in A} i_\alpha(G_\alpha)$ gera G. Com isso, todo elemento $u \in G$ pode ser escrito como $u = i_{\alpha_1}(g_1) \dots i_{\alpha_n}(g_n)$, com $n \geq 0$, $g_i \in G_{\alpha_i}$, $g_i \neq 1$, porém, pode haver $\alpha_r = \alpha_{r+1}$ para $r < n$.

Se $h = i_\alpha(g_\alpha)$, então u cumpre as condições desejadas. Se $u = i_{\alpha_1}(g_1) \dots i_{\alpha_n}(g_n)$ e $\alpha_r = \alpha_{r+1}$, para algum $r < n$, então existem duas possibilidades:

- $g_r g_{r+1} \neq 1$. Nesse caso, podemos escrever $u = i_{\alpha_1}(g_1) \dots i_{\alpha_r}(g_r g_{r+1}) i_{r+2}(g_{r+2}) \dots i_{\alpha_n}(g_n)$.
- $g_r g_{r+1} = 1$. Nesse caso, podemos escrever $u = i_{\alpha_1}(g_1) \dots i_{\alpha_{r-1}}(g_{r-1}) i_{\alpha_{r+1}}(g_{r+1}) \dots i_{\alpha_n}(g_n)$.

Segue por indução em n que u pode ser escrito da maneira desejada.

Para mostrar a unicidade, utilizaremos o mesmo método adotado na demonstração do Teorema da Forma Normal para Grupos Livres. Denote por R o conjunto das sequências $(g_1, g_2, \dots, g_n)$, com $n > 0$, $g_i \in G_{\alpha_i}$, $g_i \neq 1$ e $\alpha_r \neq \alpha_{r+1}, \forall r < n$ e por S_R o grupo das permutações de R. Devemos encontrar um homomorfismo $\varphi : G \to S_R$ tal que, dado $u \in G$, com $u = g_1 \dots g_n$, tenha-se que $\varphi(u) \in S_R$ aplicada à sequência vazia, que será denotada por $\varnothing$, retorne a sequência $(g_1, \dots, g_n)$. Isso garante a unicidade, pois se u também pode ser escrito como $u = \tilde{g}_1 \dots \tilde{g}_m$, então

$$(g_1, \dots, g_n) = \varphi(g_1, \dots, g_n)(\varnothing) = \varphi(u)(\varnothing) = \varphi(\tilde{g}_1 \dots \tilde{g}_m)(\varnothing) = (\tilde{g}_1 \dots \tilde{g}_m)$$

Logo, $n = m$ e $g_i = \tilde{g}_i, \forall i = 1, \dots, n$.

Para cada $\alpha \in A$, defina $\varphi_\alpha : G_\alpha \to R^R = \{f : R \to R : \ f \text{ é função}\}$ por

$$\varphi_\alpha(g_\alpha)(g_1, \dots, g_n) = \begin{cases} (g_\alpha, g_1, \dots, g_n), \text{ se } \alpha_1 \neq \alpha \\ (g_\alpha g_1, \dots, g_n) \text{ , se } \alpha_1 = \alpha \text{ e } g_\alpha g_1 \neq 1 \\ (g_2, g_3, \dots, g_n) \text{ , se } \alpha_1 = \alpha \text{ e } g_\alpha g_1 = 1 \end{cases}$$

e $\varphi_\alpha(1) = id_S$, a identidade em S.

Dados $g_\alpha, h_\alpha \in G_\alpha$, se $\alpha_1 \neq \alpha$, então

$$\begin{aligned}\varphi_\alpha(g_\alpha h_\alpha)(g_1,\ldots,g_n) &= (g_\alpha h_\alpha, g_1, \ldots, g_n)\\ &= \varphi_\alpha(g_\alpha)(h_\alpha, g_1,\ldots,g_n) \text{ (pois } g_\alpha \text{ e } h_\alpha \text{ estão em } G_\alpha)\\ &= \varphi_\alpha(g_\alpha)\varphi(h_\alpha)(g_1,\ldots,g_n)\end{aligned}$$

Se $\alpha_1 = \alpha$ e $g_\alpha h_\alpha = 1$, então $\varphi(g_\alpha h_\alpha) = id_S$. Além disso,

$$\begin{aligned}\varphi_\alpha(g_\alpha h_\alpha)(g_1,\ldots,g_n) &= (g_1,\ldots,g_n)\\ &= (g_\alpha h_\alpha, g_1,\ldots,g_n)\\ &= \varphi_\alpha(g_\alpha)\varphi_\alpha(h_\alpha)(g_1,\ldots,g_n)\end{aligned}$$

Se $\alpha_1 = \alpha$ e $g_\alpha h_\alpha \neq 1$, então

$$\begin{aligned}\varphi_\alpha(g_\alpha)\varphi(h_\alpha)(g_1,\ldots,g_n) &= \begin{cases}\varphi_\alpha(g_\alpha)(h_\alpha g_1,\ldots,g_n), \text{ se } h_\alpha g_1 \neq 1\\ \varphi(g_\alpha)(g_2,\ldots,g_n) \text{ , se } \alpha_1 = \alpha \text{ e } g_\alpha g_1 \neq 1\\ (g_2,g_3,\ldots,g_n) \text{ , se } h_\alpha g_1 = 1\end{cases}\\ &= \begin{cases}(g_\alpha h_\alpha g_1,\ldots,g_n), \text{ se } g_\alpha h_\alpha \neq g_1^{-1}\\ (g_2,\ldots,g_n) \text{ , se } h_\alpha g_1 \neq 1 \text{ e } g_2 h_\alpha = g_1^{-1}\\ (g_\alpha, g_2,\ldots,g_n) \text{ , se } h_\alpha g_1 = 1 \text{ (pois } \alpha_2 \neq \alpha_1)\end{cases}\\ &= \varphi_\alpha(g_\alpha h_\alpha)(g_1,\ldots,g_n)\end{aligned}$$

Logo, φ_α preserva multiplicações. Segue que φ_α leva G_α em S_R, pois $(\varphi_\alpha(g_\alpha))^{-1} = \varphi(g_\alpha^{-1})$.

Como S_R é grupo, pela propriedade universal de $(G, \{i_\alpha\})$, existe um único homomorfismo $\varphi : G \to S_R$ tal que $\varphi_\alpha = \varphi \circ i_\alpha, \forall \alpha \in A$. Dado $u = g_1 \ldots g_m \in G$, com $m \geq 1$, $g_i \in G_{\alpha_i}$, $g_i \neq 1$ e $\alpha_r \neq \alpha_{r+1}$, mostremos que $\varphi(u)(\varnothing) = (g_1,\ldots,g_m)$.

$$\varphi(u)(\varnothing) = \varphi(g_1\ldots g_m)(\varnothing) = \varphi(i_{\alpha_1}(g_1))\ldots\varphi(i_{\alpha_m}(g_m))(\varnothing) = \varphi_{\alpha_1}(g_1)\ldots\varphi_{\alpha_m}(g_m)(\varnothing)$$

$$= \varphi_{\alpha_1}(g_1)\ldots\varphi_{\alpha_{m-1}}(g_{m-1})(g_m) = \ldots = (g_1,\ldots,g_m)$$

□

Exemplo 2.3.10. Vimos que $C_2 * C_2 = \langle x\rangle * \langle y\rangle = \langle x, y | x^2, y^2\rangle$. Considere $N = \langle xy\rangle$, subgrupo de $C_2 * C_2$. Veja que

$$x^{-1}(xy)x = yx = (xy)^{-1} \in N \text{ , pois } x = x^{-1} \text{ e } y = y^{-1}$$

$$y^{-1}(xy)y = y^{-1}x = yx = (xy)^{-1} \in N$$

Logo, N é subgrupo normal de $C_2 * C_2$. Encontremos $(C_2 * C_2)/N$. Como $N = \langle xy\rangle$, devemos apenas adicionar xy aos relatores de $C_2 * C_2$. Assim,

$$(C_2 * C_2)/N = \langle x, y | x^2, y^2, xy\rangle$$

Como $xy = 1$, temos que $x = y^{-1} = y$. Consequentemente,

$$(C_2 * C_2)/N = \langle x | x^2, (x^{-1})^2\rangle = \langle x | x^2\rangle = C_2$$

Agora, daremos algumas propriedades específicas de produtos livres cujos termos são simultaneamente não triviais.

Proposição 2.3.11. Seja $\theta : C_2 * C_2 \to C_2 \times C_2$ a aplicação canônica. Então, $Ker\theta \simeq \mathbb{Z}$.

Demonstração. Tome $N = \langle xy \rangle$, como no exemplo anterior. Vimos que $(C_2 * C_2)/N = C_2$. Os únicos subgrupos normais de C_2 são os triviais. A Proposição 1.5.5 garante que N é subgrupo normal maximal de $C_2 * C_2$. Agora, $Ker\theta \lhd C_2 * C_2$, logo, $Ker\theta \lhd N$. Assim, $Ker\theta$ é cíclico, pois N é cíclico. Tem-se que $[x, y]^n \neq 1$ em $C_2 * C_2$ para todo $n \in \mathbb{N}$, mas $[x, y]^n \in Ker\theta$. Segue que $Ker\theta$ é infinto. Portanto, $Ker\theta \simeq \mathbb{Z}$. $\square$

Afirmação 2.3.12. Seja G um grupo com pelo menos três elementos. Então G tem um subgrupo isomorfo a $\mathbb{Z}$, C_p (para algum $p \geq 3$ primo), C_4 ou $C_2 \times C_2$.

Demonstração. Inicialmente, consideremos os casos em que $|G| < \infty$. Se $|G| = p$ é um primo ímpar, então $G \simeq C_p$. Se $|G| = k$, com $k \neq 2^n, \forall n \in \mathbb{N}$, então existe um primo $p \geq 3$ que divide k. Pelo Teorema de Cauchy, G tem um elemento de ordem p. Logo, tem um subgrupo isomorfo a C_p.

Se $|G| = 4$, então $G \simeq C_4$ ou $G \simeq C_2 \times C_2$. Suponha que grupos de ordem 2^{n-1} têm subgrupo isomorfo a C_4 ou a $C_2 \times C_2$. Tome G tal que $|G| = 2^n$. Todo subgrupo maximal de G tem índice 2 e é normal. Logo, se H é um subgrupo maximal de G, $|H| = 2^{n-1}$. Por hipótese de indução, H possui um subgrupo isomorfo a C_4 ou a $C_2 \times C_2$. Como $G \supset H$, tal subgrupo é também um subgrupo de G.

Agora, suponha que $|G|$ não seja finito. Se todos os elementos de G têm ordem finita, o subgrupo gerado por um de seus elementos é finito. Assim, voltamos ao caso anterior. Se G possui algum elemento de ordem infinita, o subgrupo gerado por tal elemento é isomorfo a $\mathbb{Z}$. $\square$

Lema 2.3.13. Sejam A e B grupos não triviais que não são simultaneamente isomorfos a C_2. Então, $A * B$ tem subgrupo livre de posto 2.

Demonstração. Um grupo gerado por elementos x, y distintos é livre de posto 2 quando toda palavra reduzida não trivial do alfabeto $\{x^{\pm 1}, y^{\pm 1}\}$ é diferente da unidade.

Suponha que A seja não isomorfo a C_2. Nesse caso, $|A| \geq 3$. Suponha inicialmente que $|A| \geq 4$. Então existem $a_1, a_2, a_3 \in A \backslash \{1\}$ distintos. Tome $b \in B \backslash \{1\}$. Sejam $c_1 = a_1 b$ e $c_2 = a_2 b a_3$. Queremos mostrar que o grupo gerado por $\{c_1, c_2\}$ é livre. Para isso, devemos garantir que $c_1^{i_1} c_2^{j_1} \ldots c_1^{i_m} c_2^{j_m} \neq 1$, para $m \geq 1$ e $i_k, j_k \in \mathbb{Z} \backslash \{0\}$, para todo k, mas i_1,j_m podendo ser zero. Observaremos então os produtos de dois elementos de $\{c_1^{\pm 1}, c_2^{\pm 1}\}$ juntamente com a sua escrita no alfabeto $\{a_1^{\pm 1}, a_2^{\pm 1}, a_3^{\pm 1}\}$. Lembramos que os a_i, a_i^{-1} não comutam com b.

$$\begin{array}{cccccc}
c_1 c_1 & a_1 b a_1 b & c_1 c_2 & a_1 b a_2 b a_3 & c_1 c_2^{-1} & a_1 b a_3^{-1} b^{-1} a_2^{-1} \\
c_2 c_1 & a_2 b \underline{a_3 a_1} b & c_2 c_2 & a_2 b \underline{a_3 a_2} b a_3 & c_2 c_1^{-1} & a_2 b a_3 b^{-1} a_1^{-1} \\
c_1^{-1} c_2 & b^{-1} \underline{a_1^{-1} a_2} b a_3 & c_1^{-1} c_1^{-1} & b^{-1} a_1^{-1} b^{-1} a_1^{-1} & c_1^{-1} c_2^{-1} & b^{-1} \underline{a_1^{-1} a_3^{-1}} b^{-1} a_2^{-1} \\
c_2^{-1} c_1 & a_3^{-1} b^{-1} \underline{a_2^{-1} a_1} b & c_2^{-1} c_1^{-1} & a_3^{-1} b^{-1} a_2^{-1} b^{-1} a_1^{-1} & c_2^{-1} c_2^{-1} & a_3^{-1} b^{-1} \underline{a_2^{-1} a_3^{-1}} b^{-1} a_2^{-1}
\end{array}$$

Os fatores sublinhados são os únicos possíveis cancelamentos. Queremos então que $a_3 \neq a_1^{-1}$, $a_3 \neq a_2^{-1}$ e $a_1 \neq a_2$, o que é possível para $|A| \geq 4$.

De fato, se $|A| > 3$, pela Afirmação 2.3.12, A tem um subgrupo isomorfo a $C_2 \times C_2$, C_4, $\mathbb{Z}$ ou C_p, com $p > 3$. Agora, $C_2 \times C_2 = \langle x, y | x^2,\ y^2\ (xy)^2 \rangle$. Se for esse o subgrupo, tome $a_1 = x$, $a_2 = y$ e $a_3 = xy$. Tem-se que $a_3 \neq a_1^{-1} = x$, $a_3 \neq a_2^{-1} = y$ e $a_1 = x \neq y = a_2$. Se o subgrupo for $C_4 = \langle x | x^4 \rangle$, tome $a_1 = x$, $a_2 = x^3$ e $a_3 = x^2$, pois $a_3 = x^2 \neq x = a_2^{-1}$, $a_3 = x^2 \neq x^3 = a_1^{-1}$ e $a_1 = x \neq x^3 = a_2$. Se o subgrupo for $C_p = \langle x | x^p \rangle$, tome $a_1 = x$, $a_2 = x^{p-1}$ e $a_3 = x^2$. Tem-se que $a_1^{-1} = x^{p-1} \neq x^2 = a_3$, pois $p > 3$, logo, $p - 1 > 2$. Além disso, $a_2^{-1} = x \neq x^2 = a_3$ e $a_1 = x \neq x^{p-1} = a_2$. No caso em que o subgrupo é $\mathbb{Z}$, tais elementos existem, pois o grupo possui um elemento de ordem infinita, basta tomar potências do mesmo.

Assim, $\langle c_1, c_2 \rangle$ é subgrupo livre de posto dois de $A * B$.

Para $|A| = 3$, isso não é possível. Tome então $b \in B \backslash \{1\}$ e $a \in A \backslash \{1\}$ e faça $c_1 = aba$ e $c_2 = babab^{-1}$. Para mostrar que $c_1^{i_1} c_2^{j_1} \dots c_1^{i_m} c_2^{j_m}$ como descrito acima é não trivial, iremos observar os fatores $c_1^{i_k}$ e $c_2^{j_k}$. Veja que, como $|A| = 3$, $aa \neq 1$. Para $m > 0$, tem-se

$$\begin{array}{lll}
c_1^m & = (aba)(aba)\dots(aba) & = abaaba\dots aba \\
c_1^{-m} & = (a^{-1}b^{-1}a^{-1})(a^{-1}b^{-1}a^{-1})\dots(a^{-1}b^{-1}a^{-1}) & = a^{-1}b^{-1}a^{-1}a^{-1}b^{-1}a^{-1}\dots a^{-1}b^{-1}a^{-1} \\
c_2^m & = (babab^{-1})(babab^{-1})\dots(babab^{-1}) & = (babab^{-1}) = b(aba)(aba)\dots(aba)b^{-1} \\
c_2^{-m} & = (ba^{-1}b^{-1}a^{-1}b^{-1})\dots(ba^{-1}b^{-1}a^{-1}b^{-1}) & = b(a^{-1}b^{-1}a^{-1})(a^{-1}b^{-1}a^{-1})\dots(a^{-1}b^{-1}a^{-1})b^{-1}
\end{array}$$

Como c_1^m começa e termina em a e c_2^1, c_2^{-1} começam com b e terminam com b^{-1}, não há cancelamentos em fatores do tipo $c_2^{j_k} c_1^m c_2^{j_{k+1}}$. Analogamente, como c_1^{-m} inicia e termina com a^{-1}, não existe cancelamento em fatores do tipo $c_2^{j_k} c_1^{-m} c_2^{j_{k+1}}$. Como anteriormente, $\langle c_1, c_2 \rangle$ é subgrupo livre de posto dois de $A * B$.

□

As propriedades anteriores são frutos de uma área mais geral da Teoria Geométrica de Grupos que é a Teoria de Bass-Serre (Cf. [9]). O lema anterior, por exemplo, pode ser visto como uma aplicação de [9, Prop. 18, pp. 36–37].

2.4 Limites Diretos de Grupos

Definição 2.4.1. Um conjunto Λ com uma relação $\leq$ é dito um *conjunto parcialmente ordenado* quando satisfaz:

i. $\mu \leq \mu$, para cada $\mu \in \Lambda$

ii. Dados $\mu, \lambda \in \Lambda$, se $\mu \leq \lambda$ e $\lambda \leq \mu$, então $\mu = \lambda$.

iii. Se $\mu \leq \lambda$ e $\lambda \leq \eta$, então $\mu \leq \eta$.

Se além disso I satisfizer:

iv. Dados $\mu, \lambda \in I$, existe $\eta \in \Lambda$ tal que $\mu \leq \eta$ e $\lambda \leq \eta$,

dizemos que $I = (I, \leq)$ é um *conjunto direcionado.*

Exemplo 2.4.2. Sejam S um conjunto e I o conjunto de todos os subconjuntos não vazios de S. I com a relação $A \leq B$ quando $A \supset B$ é um conjunto ordenado. De fato,

i. $A \supset A$, $\forall A \in I$

ii. Se $A \leq B$ e $B \leq A$, então $A \supset B$ e $B \supset A$. Segue que $A = B$.

iii. Se $A \leq B$ e $B \leq C$, então $A \supset B$ e $B \supset C$, logo, $A \supset C$. Portanto, $A \leq C$

Mais ainda, $(I, \leq)$ é um conjunto direcionado, pois se $A, B \in I$ então $A \cap B \in I$. Como $A \supset A \cap B$ e $B \supset A \cap B$, segue que $A \leq A \cap B$ e $B \leq A \cap B$.

O conjunto $(I, \tilde{\leq})$, onde $A \tilde{\leq} B$ quando $A \subset B$ também é um conjunto direcionado, o que pode ser mostrado por argumentos análogos.

Exemplo 2.4.3. $\mathbb{N}$ com a ordem $\leq$ usual é um conjunto direcionado.

Exemplo 2.4.4. $I = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}\}$ é um conjunto parcialmente ordenado com a inclusão, mas não direcionado. De fato, não existe nenhum elemento $\nu \in I$ tal que $\{1,2\} \subset \nu$ e $\{2,3\} \subset \nu$.

Definição 2.4.5. Seja $(\Lambda, \leq)$ um conjunto direcionado. Sejam G_λ grupos, para cada $\lambda \in \Lambda$ e $\varphi_\mu^\lambda : G_\lambda \to G_\mu$ homomorfismos de grupos, para todos $\lambda, \mu \in \Lambda$ tais que $\lambda \leq \mu$. Dizemos que $(G_\lambda, \varphi_\mu^\lambda)_{\lambda \leq \mu}^{\lambda,\mu \in \Lambda}$ é um *sistema direto indexado por* Λ quando $\varphi_\lambda^\lambda = id_{G_\lambda}$, a identidade de G_λ, e $\varphi_\eta^\mu = \varphi_\eta^\lambda \circ \varphi_\lambda^\mu$, sempre que $\mu \leq \lambda \leq \eta$.

Exemplo 2.4.6. Dados grupos $\{G_n\}_{n \in \mathbb{N}}$ tais que $G_1 \leq G_2 \leq \ldots \leq G_n \leq \ldots$, tem-se que $(G_n, \varphi_m^n)_{n \leq m}^{n,m \in \mathbb{N}}$, onde $\varphi_m^n : G_n \to G_m$ é a inclusão, é sistema direto.

Definição 2.4.7. Seja $(G_i, \varphi_j^i)_{i \leq j}^{i,j \in I}$ um sistema direto indexado pelo conjunto direcionado I. O *limite direto* desse sistema é o par $(G, \phi_i)_{i \in I}$, onde G é um grupo e $\phi_i : G_i \to G$ é um homomorfismo, de modo que tal par satisfaça a seguinte propriedade universal: para cada grupo H e homomorfismos $h_i : G_i \to H$ tais que $h_j \circ \varphi_j^i = h_i$, sempre que $i \leq j$, existe um único homomorfismo $\theta : G \to H$ tal que $h_i = \theta \circ \phi_i, \forall i \in I$. Ou seja, o diagrama abaixo comuta.

$$\begin{tikzcd}
G \arrow[rr, dashed, "\theta"] & & H \\
& G_i \arrow[ul, "\phi_i"'] \arrow[ur, "h_i"] \arrow[d, "\varphi_j^i"] & \\
& G_j \arrow[uul, "\phi_j"] \arrow[uur, "h_j"'] &
\end{tikzcd}$$

Por simplicidade, denotaremos $(G_i, \varphi_j^i)_{i \leq j}^{i,j \in I}$ apenas por (G_i, φ_j^i).

Proposição 2.4.8. O limite direto de um sistema direto (G_i, φ^i_j) é único, a menos de isomorfismo.

Demonstração. Suponha que ambos $(G, \phi_i)_{i\in I}$ e $(W, \psi_i)_{i\in I}$ sejam limites diretos para (G_i, φ^i_j).

$$\begin{tikzcd}
G \arrow[rr, shift left, "\theta_1"] & & W \arrow[ll, shift left, "\theta_2"] \\
& G_i \arrow[ul, "\phi_i"] \arrow[ur, "\psi_i"'] \arrow[d, "\varphi^i_j"] & \\
& G_j \arrow[uul, "\phi_j"] \arrow[uur, "\psi_j"'] &
\end{tikzcd}$$

Como $\psi_j \circ \varphi^i_j = \psi_i$, para todos $i, j \in I$ tais que $i \leq j$, a propriedade universal de (G, ϕ_i) garante a existência de um único $\theta_1 : G \to W$ tal que $\theta_1 \circ \phi_i = \psi_i, \forall i \in I$. Analogamente, a propriedade universal de (W, ψ_i) garante a existência de um único $\theta_2 : W \to G$ tal que $\theta_2 \circ \psi_i = \phi_i$, para todo $i \in I$. Assim,

$$\theta_1 \circ \theta_2 \circ \psi_i = \theta_1 \circ (\theta_2 \circ \psi_i) = \theta_1 \circ \phi_i = \psi_i$$

$$\theta_2 \circ \theta_1 \circ \phi_i = (\theta_2 \circ \theta_1) \circ \phi_i = \theta_2 \circ \psi_i = \phi_i$$

Ainda pela propriedade universal de (G, ϕ_i), existe um único homomorfismo $l : G \to G$ tal que $l \circ \phi_i = \phi_i, \forall i \in I$. Como a identidade $id_G : G \to G$ satisfaz $id_G \circ \phi_i = \phi_i, \forall i \in I$, tem-se que $l = id_G$. Ainda pela unicidade de tal homomorfismo, como $(\theta_2 \circ \theta_1) \circ \phi_i = \phi_i, \forall i \in I$, segue que $\theta_2 \circ \theta_1 = id_G$. Analogamente, a propriedade universal de (W, ψ_i) garante que $\theta_1 \circ \theta_2 = id_W$, pois $(\theta_1 \circ \theta_2) \circ \psi_i = \psi_i, \forall i \in I$.

□

Teorema 2.4.9. Todo sistema direto de grupos tem limite direto.

Demonstração. Seja (G_i, φ^i_j) um sistema direto indexado por I. Defina $K = \{g_i^{-1}\varphi^i_j(g_i) : g_i \in G,\ i \leq j,\ i, j \in I\} \subset *_{i\in I}G_i$. Seja N o fecho normal de K em $*_{i\in I}G_i$. Sejam ainda $\iota : G_i \to *_{i\in G}G_i$ a inclusão e $\pi : *_{i\in I}G_i \to *_{i\in I}G_i/N$ o homomorfismo canônico. Defina $\phi_i = \pi \circ \iota$. Mostremos que $(*_{i\in I}G_i/N, \phi_i)_{i\in I}$ é o limite direto procurado.

Dados um grupo H e homomorfismos $f_i : G_i \to H$ tais que $f_i = f_j \circ \varphi^i_j$, defina $\tilde{\theta} : *_{i\in I}G_i \to H$ fazendo $\tilde{\theta}|_{G_i} = f_i$. Para cada $g_i \in G_i$, $i \leq j$ com $i, i \in I$, tem-se que $\tilde{\theta}(g_i^{-1}\varphi^i_j(g_i)) = f_i(g_i)^{-1}f_j\varphi^i_j(g_i) = f_i(g_i)^{-1}f_i(g_i) = 1$. Logo, $N \subset Ker\tilde{\theta}$. Assim, $\tilde{\theta}$ induz um homomorfismo $\theta : *_{i\in I}G_i/N \to H$ tal que $\theta(gN) = \tilde{\theta}(g), \forall g \in *_{i\in I}G_i$. Agora, pela escolha de θ, vale que $\theta \circ \phi_i(g_i) = f_i(g_i), \forall g_i \in G_i$. □

2.5 O Teorema de Schreier

Esta seção é destinada à demonstração do Teorema de Schreier, que afirma que todo subgrupo de um grupo livre é livre. A demonstração conta com alguns resultados sobre grafos orientados e recobrimentos de grafos, os quais serão mostrados nas próximas subseções. A demonstração aqui dada é objetiva. Porém, tal teorema também pode ser obtido pela Teoria de Bass-Serre (Cf. [9, Teo. 5, p. 29]) com ações de grupos livres sobre árvores.

2.5.1 Grafos orientados

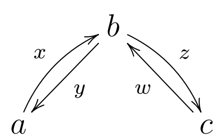
Definição 2.5.1. Um *grafo orientado* G é um par $(V(G), E(G))$, onde $V(G)$ e $E(G)$ são conjuntos disjuntos cujos elementos são ditos *vértices* e *arestas* de G, respectivamente, juntamente com duas funções $i : E(G) \to V(G)$ e $^{-}: E(G) \to E(G)$, na qual $\bar{a} \neq a$ e $\bar{\bar{a}} = a$, para todo $a \in E(G)$.

Dizemos que $i(a), i(\bar{a}) \in V(G)$ são o *vértice inicial* e o *vértice final* da aresta a, respectivamente. Ambos, $i(a)$ e $i(\bar{a})$, são ditos *vértices extremos* de a. Dizemos também que $\bar{a}$ é a aresta *inversa* de a.

Exemplo 2.5.2. Sejam $V(G) = \{a, b, c\}$ e $E(G) = \{x, y, z, w\}$. Defina $i : E(G) \to V(G)$ e $^{-}: E(G) \to E(G)$ fazendo as seguintes correspondências:

$$i(x) = a \qquad i(y) = b \qquad i(z) = b \qquad i(w) = c \qquad \bar{x} = y \qquad \bar{z} = w \qquad \bar{y} = x \qquad \bar{w} = z$$

Tem-se que $G = (V(G), E(G))$ com as operações acima é um grafo orientado. Em um exemplo simples como o aqui apresentado, é útil considerar a representação geométrica:



Com as notações dadas, se $e \in E(G)$, então $\bar{e}$ também deve estar em $E(G)$. Chamamos o par $e, \bar{e}$ de *par de arestas*.

Dizemos que $a \in E(G)$ é um *laço*, quando $i(a) = i(\bar{a})$, ou seja, quando seus vértices terminais coincidem. Nesse caso, o vértice que é o inicio e o fim de a é dito o ponto base do laço a.

Quando não houver risco de confusão, denotaremos $V(G)$ e $E(G)$ simplesmente por V e E, respectivamente.

Um *caminho* de comprimento $n > 0$ do grafo orientado G é uma sequência finita de arestas $a_1, \ldots, a_n$ tais que o vértice final de a_i é igual ao vértice inicial de a_{i+1}, para todo $i < n$. Dizemos que o caminho $a_1, \ldots, a_n$ tem *inicio* em $i(a_1)$ e fim em $i(\bar{a_n})$. Os *vértices* desse caminho são os vértices extremos das arestas a_i. Definimos o caminho de comprimento 0 como sendo apenas um vértice e esse é dito um *caminho trivial*. Um caminho é dito *simples* se todos os seus vértices são distintos.

Sejam f e g os caminho $e_1, \ldots, e_n$ e $e'_1, \ldots, e'_m$, com $i(\bar{e}_n) = i(e'_1)$, definimos o *produto* entre f e g por

$$fg = e_1, \ldots, e_n, e'_1, \ldots, e'_m.$$

Em especial, se f tem vértices extremos iguais, podemos definir o caminho f^k como sendo o produto de f por si mesmo k vezes, onde $k > 0$. O *caminho inverso* ou *inverso* de f, é $\bar{e}_n, \ldots, \bar{e}_1$, denotado por $\bar{f}$. No caso do caminho trivial constituído do vértice v, tem-se que o seu inverso é ainda v.

Um caso especial de caminho é o caminho que tem vértices inicial e final iguais. Esse tipo de caminho será denominado *ciclo*. O vértice inicial de um ciclo é dito o *ponto base* desse ciclo. Dizemos que um ciclo é um *ciclo simples* se todos os seus vértices são distintos, excetuando-se o inicio e o fim do ciclo. Em particular, exigimos que um ciclo simples não seja da forma $e, \bar{e}$. Dado um ciclo $e_1, \ldots, e_n$, tem-se que $e_j, e_{j+1}, \ldots, e_n, e_1, \ldots, e_{j-1}$ é também um ciclo. O mesmo é válido para ciclos simples. Denote por $\mathcal{C}_f$ o conjunto de todas essas permutações de f, ou seja, o conjunto de todas as permutações cíclicas de f. Muitas vezes, será conveniente denotaremos $\mathcal{C}_{\bar{f}}$ por $\bar{\mathcal{C}}_f$.

Um subgrafo G' do grafo orientado G é um grafo orientado $(V(G'), E(G'))$, onde $V(G') \subset V(G)$ e $E(G') \subset E(G)$, com as operações induzidas de G, de modo que $i(e) \in V(G')$ e $\bar{e} \in E(G')$, para todo $e \in E(G')$. Um subgrafo $G' = (V(G'), E(G'))$ de G é dito um *subgrafo completo* quando seu conjunto de arestas é dado por $E(G') = \{e \in E(G) : \ i(e), i(\bar{e}) \in V(G')\}$.

Dizemos que um grafo orientado G é *conexo* se, dados quaisquer dois vértices de G, existe um caminho com inicio em um e fim no outro. Defina a seguinte relação em G: $v \sim w$ quando existe um caminho que leva v em w. Tem-se que $\sim$ é uma relação de equivalência. Um subgrafo completo de G cujo conjunto de vértices é uma classe de equivalência dessa relação é dito uma *componente* ou *componente conexa* de G. Por definição, se G é conexo, então G só possui uma componente.

Um caminho $e_1, \ldots, e_n$ é dito *redutível*, se existe i tal que $e_i = \bar{e}_{i+1}$. Caso contrário, dizemos que esse é um caminho *irredutível*. Se o caminho dado é redutível, com $e_i = \bar{e}_{i+1}$, então $e_1, \ldots, e_{i-1}, e_{i+2}, \ldots, e_n$ também é um caminho, de modo que dois vértices que são ligados por um caminhos são ligados por um caminho irredutível. Por definição, um caminho redutível não é simples.

Um grafo cujos ciclos de comprimento positivos são redutíveis é dito uma *floresta*. Uma floresta conexa é dita uma *árvore*. Todo subgrafo de uma floresta é também uma floresta. Além disso, um grafo é uma floresta se, e somente se, suas componentes conexas são árvores. Veja que uma árvore não possui ciclos simples, lembrando que $e, \bar{e}$ não é considerado um ciclo simples.

Observamos que em uma floresta, existe no máximo um caminho irredutível que liga dois vértices. No caso de árvores, dados dois vértices, existe sempre um caminho que os une e, portanto, existe um caminho irredutível entre eles. Em especial, uma árvore é uma floresta, assim tem-se o seguinte resultado:

Lema 2.5.3. Em uma árvore, dois vértices podem ser ligados por exatamente um caminho irredutível.

Sejam G um grafo orientado e F um subgrafo de G que é uma floresta. Se F não está contida propriamente em nenhuma floresta de G, dizemos que F é uma *floresta maximal*. Em particular, se G é conexo, F é uma árvore, ao qual denominaremos *árvore maximal*.

Lema 2.5.4. Sejam G um grafo orientado conexo e T um subgrafo de G que é uma árvore. Então, T é árvore maximal se, e somente se, o conjunto de vértices de T é o mesmo de G.

Demonstração. Seja T uma árvore maximal em G que não contém todos os vértices de G. Seja e_n um vértice que não pertence a T. Como G é conexo, existe um caminho $e_1, \ldots, e_{n-1}, e_n$ entre um vértice $i(e_1)$ de T e $i(\bar{e}_n)$. Consequentemente, existe uma aresta e_i em tal caminho cujo inicio é um vértice de T mas o fim não é um vértice de T. A aresta $\bar{e}_i$ não está em T, porém, como ela é uma aresta cujo fim está em T, tem-se que o subgrafo T' obtido ao se adicionar $\bar{e}_i$ em T, é uma árvore que contém T, contradizendo o fato de T ser maximal.

Reciprocamente, seja T uma árvore em G que contém todos os seus vértices. Seja H um subgrafo de G que contém T propriamente. Seja e uma aresta de H que não está em T. Por hipótese, os vértices extremos de e estão em T. Assim, exite um único caminho irredutível f entre $i(e)$ e $i(\bar{e})$ em T. Como e e f são caminhos em H com inicio em $i(e)$ e fim em $i(\bar{e})$, segue que H não é uma árvore. Portanto, T é uma árvore maximal em G. □

Lema 2.5.5. Numa árvore com número finito de vértices $n \geq 2$, existem pelo menos dois vértices que são o inicio de exatamente uma aresta e o fim de exatamente uma aresta.

Demonstração. Seja T uma árvore como na hipótese do lema. Como T tem finitos vértices, existe um número máximo de caminhos com vértices disjuntos. Tome $e_1, \ldots, e_n$ o maior caminho irredutível com vértices distintos em T. Suponha que exista uma aresta e de T tal que $e \neq \bar{e}_n$ e que o vértice inicial de e seja igual ao vértice final de e_n. Se existir r tal que $i(\bar{e}) = i(e_r)$, então $e_r, \ldots, e_n, e$ é um ciclo irredutível, contradizendo o fato de T ser árvore.

Assim, $e_1, \ldots, e_n, e$ é uma caminho irredutível com vértices distintos. Isso contradiz a maximalidade de n. Consequentemente, não existe uma aresta de T distinta de e_n cujo vértice inicial seja igual a $i(\bar{e}_n)$. Desse modo, e_n é a única aresta de T quem tem $i(\bar{e}_n)$ como fim, bem como $\bar{e}_n$ é a única aresta que tem $i(\bar{e}_n)$ como inicio.

Analogamente, mostra-se que e_1 é a única aresta cujo inicio é $i(e_1)$ e $\bar{e}_1$ é a única aresta cujo fim é $i(e_1)$.

Portanto, os vértices procurados são e_1 e e_n. □

Proposição 2.5.6. Um grafo orientado com número finito n de vértices e m pares de arestas é uma árvore se, e somente se, $n = m + 1$

Demonstração. Seja G uma árvore. Mostraremos o resultado por indução em n. Se $n = 1$, devemos ter que $m = 0$, pois qualquer aresta seria uma laço. Pelo Lema 2.5.5, podemos tomar um vértice v que é inicio de exatamente uma aresta e. Pela escolha de v, podemos construir um subgrafo H de G ao retirarmos de G as arestas $e, \bar{e}$ e o vértice v. Em particular, G é uma floresta, assim H é uma floresta. Observe que H é uma árvore, assim, por hipótese de indução, $n - 1 = (m - 1) + 1$.

Reciprocamente, se G é um grafo orientado conexo com n vértices e $n - 1$ pares de arestas, tome uma árvore T maximal em G. Pela conexidade de G, tem-se que T tem n vértices. Pela primeira parte da proposição, T deve conter $n - 1$ pares de arestas. Assim, T é um subgrafo de G que contém os mesmos vértices e arestas que G. Portanto, $T = G$. □

2.5.2 Grupos Fundamentais de Grafos

Sejam Γ um grafo orientado e f o caminho $e_1, \ldots, e_n$ em K. Dizemos que o caminho g é *obtido por redução elementar* de f quando, para algum i, $e_{i+1} = \bar{e}_i$ e g é o caminho $e_1, \ldots, e_{i-1}, e_{i+2}, \ldots, e_n$.

Definição 2.5.7. Sejam Γ um grafo orientado e f, g caminhos de Γ. Dizemos que f é *homotópico* a g quando existe uma sequência de caminhos $(f_1, \ldots, f_r)$ de Γ tal que $f_1 = f$, $f_r = g$ e f_i, f_{i+1} são tais que um deles é obtido por redução elementar do outro. Escrevemos $f \simeq g$ para indicar que f é homotópico a g.

Tem-se que $\simeq$ é uma relação de equivalência e que as classes de homotopia de caminhos de Γ formam um grupoide (Cf. [2]), o qual chamaremos de *grupoide fundamental* de Γ e denotaremos por $\gamma(\Gamma)$. O inverso da classe do caminho f é a classe do caminho $\bar{f}$, em $\gamma(K)$.

Chamamos de *grupo fundamental* de Γ com *ponto base* v o conjunto das classes de homotopia dos laços com ponto base em v e o denotamos por $\pi_1(\Gamma, v)$.

Um caminho entre os vértices v e w de Γ induz isomorfismo entre $\pi_1(\Gamma, v)$ e $\pi_1(\Gamma, w)$ (Cf. [2]). Por esse motivo, quando Γ for conexo, podemos denotar seus grupos fundamentais apenas por $\pi_1(\Gamma)$, uma vez que são todos isomorfos, ou seja, em essência, o grupo fundamental de Γ é único e não depende do ponto base.

Seja $\varphi : K \to L$ um morfismo entre grafos. Observamos que se um caminho g é obtido por redução elementar de um caminho f, então $\varphi(g)$ é obtido por redução elementar de $\varphi(f)$. Consequentemente, se $f \simeq g$, então $\varphi(f) \simeq \varphi(g)$. Portanto, φ induz um homomorfismo $\varphi^* : \gamma(K) \to \gamma(L)$ e também a um homomorfismo $\varphi^* : \pi_1(K, v) \to \pi_1(L, \varphi(v))$. Para um morfismo $\psi : L \to M$ entre grafos, tem-se que $(\psi \circ \varphi)^* = \psi^* \circ \varphi^*$. Se $id_K : K \to K$ é a identidade em K, então $id_K^* = id_{\gamma(K)}$ é a identidade em $\gamma(L)$. Assim, se φ é um isomorfismo de grafos, φ^* é isomorfismo de grupoides .

Para dar continuidade ao estudo de apresentações de grupos, encontraremos uma apresentação para o grupo fundamental de um grafo conexo Γ.

Seja $F(E)$ o grupo livre cuja base é o conjunto de arestas E do grafo conexo Γ. Cada caminho $e_1, \ldots, e_n$ de Γ pode ser visto como o produto $e_1 \ldots e_n$ em $F(E)$. Assim, todo caminho de Γ pode ser visto como um elemento de $F(E)$ e, por simplicidade, será denotado como tal.

Fixe um vértice a de Γ e, para cada vértice v de Γ, escolha um caminho f_v entre a e v. Em especial, escolhemos f_a como sendo o caminho trivial. Defina então os subconjuntos de $F(E)$: $S = \{f_v : \ v \in V\}$ e $R = \{e\bar{e} : \ e \in E\}$. Queremos mostrar que $\langle E | S \cup R \rangle$ é uma apresentação de $\pi_1(\Gamma, a)$. Para isso, construiremos um isomorfismo entre o grupo $G = \langle E | S \cup R \rangle$ e $\pi_1(\Gamma, a)$.

Denote por $[f]$ a classe de homotopia do caminho f e defina $\tilde{\iota} : E \to \pi_1(\Gamma, a)$ fazendo a seguinte correspondência: Se e é uma aresta entre v e w, faça $\bar{\iota}(e) = [f_v e \bar{f}_w]$. Pela propriedade universal de $F(E)$, existe um homomorfismo $\iota : F(E) \to \pi_1(\Gamma, a)$ tal que $\iota(e) = [f_v e \bar{f}_w]$. Então, ι é um homomorfismo que leva $e\bar{e}$ na identidade, para cada $e \in E$: $\iota(e\bar{e}) = [f_v e \bar{f}_w][f_w \bar{e} \bar{f}_v] = [f_v e \bar{f}_w f_w \bar{e} \bar{f}_v]$ que é a classe de homotopia da identidade. Além disso, $\iota(f_v) = [f_a f_v \bar{f}_v] = [f_a]$, que é a identidade, pela escolha de f_a. Segue que $S \cup R \subset Ker \iota$. Consequentemente, ι induz um homomorfismo $\varphi : F(E)/N = G \to \pi_1(\Gamma, a)$, onde N denota o fecho normal $\langle S \cup R \rangle^{F(E)}$, pelo Teorema 2.2.13. Tem-se ainda que $\varphi(fN) = \iota(f) = [f_v f \bar{f}_w]$, em que f é um caminho entre v e w em $F(E)$.

Seja j a aplicação que leva cada caminho f de $F(E)$ em $fN \in G$. A aplicação j é multiplicativa no sentido de que, se o produto $f_1 f_2$ está definido, então j leva $f_1 f_2$ em $f_1 f_2 N = f_1 N f_2 N$. Além disso, se e é uma aresta entre v e w, então $j(e\bar{e})$ é a identidade, pois $e\bar{e} \in R \subset N$. Segue que j é constante nas classes de homotopia, de forma que j define um homomorfismo $\bar{\psi} : \gamma(\Gamma) \to G$. Seja ψ a restrição de $\bar{\psi}$ a $\pi_1(\Gamma, a)$. Mostremos que $\psi = \varphi^{-1}$.

Como $S = \{f_v : \ v \in V\}$, devemos ter que $\psi(f_v)$ é a identidade. Dada uma aresta e entre v e w,

$$\psi \circ \varphi(eN) = \psi([f_v e \bar{f}_w]) = \bar{\psi}([f_v])\bar{\psi}([e])\bar{\psi}([\bar{f}_w]) = \bar{\psi}([e]) = eN$$

Além disso, $\varphi \circ \bar{\psi}([e]) = \varphi(eN) = [f_v e \bar{f}_w]$. Indutivamente, para um caminho f entre v e w, $\varphi \circ \bar{\psi}([f]) = [f_v f \bar{f}_w]$. Em particular, dado um ciclo f com ponto base a, tem-se que

$$\varphi \circ \psi([f]) = [f_a f \bar{f}_a] = [f]$$

pois f_a é trivial. Segue que $\psi = \varphi^{-1}$. Logo, φ é isomorfismo.

Vejamos agora uma apresentação que faz uso de uma árvore maximal de Γ.

Teorema 2.5.8. Seja T uma árvore maximal do grafo conexo Γ. Então $\pi_1(\Gamma) = \langle E| \ \{e : \ e \in T\} \cup R\rangle$.

Demonstração. Mostraremos que $\langle E| \ S \cup R\rangle$ e $\langle E| \ \{e : \ e \in T\} \cup R\rangle$ são apresentações do mesmo grupo. Para isso, devemos mostrar que $S \cup R$ e $\{e : \ e \in T\} \cup R$ são consequências um do outro.

Como T é uma árvore maximal, o Lema 2.5.3 garante que existe um único caminho irredutível de a até v. Podemos tomar f_v na definição de S como sendo tal caminho. Como f_v é um caminho em T, f_v é consequência de $\{e : \ e \in T\}$, pois é um produto de arestas de T, quando visto como elemento de $F(E)$.

Por outro lado, dada uma aresta e de T que leva v em w, existem duas possibilidades: f_v termina ou não termina em $\bar{e}$. Se f_v tem $\bar{e}$ como última aresta, então o caminho obtido ao retirarmos $\bar{e}$ de f_v é um caminho irredutível entre a e w. Ou seja, $f_w \bar{e} = f_v$. Caso contrário, $f_v e$ é um caminho irredutível entre a e w, ou seja, $f_v e = f_w$. Em ambos os casos, e é consequência de $\{e\bar{e} : \ e \in E\} \cup \{f_v : \ v \in V\} \subset S \cup R$. □

Corolário 2.5.9. Sejam G um grafo orientado conexo e T uma árvore maximal em G. Então, $\pi_1(G)$ é livre, onde a cada par de arestas que não está em T, corresponde um elemento da base de $\pi_1(G)$. Além disso, o elemento de base que corresponde à aresta e que leva v em w é a classe de equivalência de $f_v e \bar{f}_w$, onde f_v denota o único caminho irredutível em T do ponto de base até v.

Para ver tal resultado, note que $\pi_1(G) = \langle E| \ \{e\bar{e} : \ e \in E\} \cup \{e : \ e \in T\}\rangle$. Pela escolha de $e, \bar{e}$, tem-se que $e\bar{e}$ é o elemento neutro, de modo que uma apresentação mais simplificada de $\pi_1(G)$ é $\langle E|\{e : \ e \in T\}\rangle$. Mas esse é o grupo livre com gerador $E \setminus \{e : \ e \in T\}$, ou seja, $\pi_1(G) = F(E \setminus T)$.

Corolário 2.5.10. Um grafo orientado conexo é uma árvore se, e somente se, seu grupo fundamental é trivial.

Corolário 2.5.11. Um grafo orientado conexo G com número finito n de vértices e m pares de arestas é livre de posto $m - n + 1$.

Demonstração. Pelo corolário 2.5.11, existe um elemento da base para cada par de arestas que não pertence a T. Como T é árvore maximal, seu conjunto de vértices coincide com o conjunto de vértices de G, ou seja, T tem n vértices. Pela Proposição 2.5.6, segue que T tem $n - 1$ pares de arestas. Como existem m pares de arestas ao todo, o número de elementos da base é $m - n + 1$.
□

2.5.3 Recobrimento

Neste capítulo, desenvolveremos a teoria de recobrimentos de grafos seguindo o livro [2]. Essa teoria é um caso particular da teoria geral de recobrimentos da Topologia Algébrica.

Sejam Γ um grafo e v um vértice de Γ. Denotaremos por $E_v(\Gamma)$ o conjunto das arestas de Γ que inciam em v.

Definição 2.5.12. Seja $p : \tilde{\Gamma} \to \Gamma$ uma aplicação entre grafos conexos. Se, para cada vértice $\tilde{v}$ de $\tilde{\Gamma}$, p induz uma bijeção entre $E_{\tilde{v}}(\tilde{\Gamma})$ e $E_{p(\tilde{v})}(\Gamma)$, dizemos que p é uma *aplicação de recobrimento* e que $\tilde{\Gamma}$ é um *recobrimento* de Γ.

Aplicações de recobrimento são sobrejetivas. A proposição a seguir nos dá uma importante caracterização desse tipo de aplicação.

Proposição 2.5.13. Seja $p : \tilde{\Gamma} \to \Gamma$ uma aplicação de recobrimento. Dado um caminho f de Γ com inicio em v, existe, para cada $\tilde{v}$ em $\tilde{\Gamma}$ tal que $p(\tilde{v}) = v$, um único caminho $\tilde{f}$ de $\tilde{\Gamma}$ com inicio em $\tilde{v}$ tal que $p(\tilde{f}) = f$

Demonstração. Veja [2]. $\square$

Definição 2.5.14. Na proposição acima, o caminho $\tilde{f}$ dado é dito um *levantamento* do caminho f com inicio em $\tilde{v}$.

Proposição 2.5.15. Sejam f, g dois caminhos com levantamentos $\tilde{f}, \tilde{g}$. Se $\tilde{f}$ e $\tilde{g}$ têm inicio no mesmo ponto $\tilde{v}$ e $f \simeq g$, então $\tilde{f} \simeq \tilde{g}$.

Demonstração. Veja [2]. $\square$

Seja $p : \tilde{\Gamma} \to \Gamma$ uma aplicação de recobrimento. Dizemos que o caminho f de Γ *representa um elemento* de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$ quando $[f] = p^*[g]$, para algum caminho g de $\tilde{\Gamma}$. Assim, $[f] = p^*[g] = [p(g)]$. Isso equivale a afirmar que $f \simeq p(g)$, para algum caminho g em $\tilde{\Gamma}$.

Se f é um ciclo em Γ com ponto base v que tem como levantamento $\tilde{f}$, um ciclo com ponto base $\tilde{v}$, onde $\tilde{v} \in p^{-1}(v)$, então $p(\tilde{f}) = f$, logo f representa um elemento de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$.

Por outro lado, se f representa um elemento de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$, então existe um ciclo $\tilde{g}$ com base $\tilde{v}$ em $p^{-1}(v)$ tal que $f \simeq p(\tilde{g})$. Como $p(\tilde{g})$ é um caminho em Γ com levantamento $\tilde{g}$, que inicia e termina em $\tilde{v}$, devemos ter que o levantamento de f tem inicio e fim em $\tilde{v}$.

A proposição anterior implica no seguinte resultado.

Proposição 2.5.16. Um ciclo f com ponto base v tem como levantamento um ciclo de $\tilde{\Gamma}$ com ponto base $\tilde{v} \in p^{-1}(v)$ se, e somente se, f representa um elemento de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$.

Corolário 2.5.17. Sejam $p : \tilde{\Gamma} \to \Gamma$ uma aplicação de recobrimento entre grafos e f, g caminhos entre os vértices v e w em Γ, com levantamentos $\tilde{f}$ e $\tilde{g}$ em $\tilde{\Gamma}$, com inicio em $\tilde{v}$. Então , $\tilde{f}, \tilde{g}$ têm o mesmo fim se, e somente se, $f\bar{g}$ representa um elemento de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$.

Demonstração. Veja [2]. $\square$

Observe que o inverso de $[g]$ é $[\bar{g}]$ no grupo $\pi_1(\Gamma, v)$. Assim, o corolário anterior afirma que $\tilde{f}$ e $\tilde{g}$ terminam no mesmo ponto se, e somente se, estão na mesma classe lateral de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$ em $\pi_1(\Gamma, v)$, pois $f\bar{g}$, ou seja, "fg^{-1}", representa um elemento de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$.

Corolário 2.5.18. Seja $p : \tilde{\Gamma} \to \Gamma$ um aplicação de recobrimento. Dado um vértice v de Γ, tem-se que $p^{-1}(v)$ está em bijeção com o conjunto $\mathscr{C}_{p^*}$, o conjunto das classes laterais de $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$ em $\pi_1(\Gamma, v)$.

Demonstração. Tal resultado pode ser visto em [2]. □

Teorema 2.5.19. Dada uma aplicação de recobrimento $p : \tilde{\Gamma} \to \Gamma$, tem-se que $p^* : \pi_1(\tilde{\Gamma}, \tilde{v}) \to \pi_1(\Gamma, v)$ é um monomorfismo.

Demonstração. Cf. [2]. □

Como consequência do teorema anterior, $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$ pode ser visto como um subgrupo de $\pi_1(\Gamma, v)$. Nesse caso, dizemos que o recobrimento $p : \tilde{\Gamma} \to \Gamma$ *pertence* ao subgrupo $p^*(\pi_1(\tilde{\Gamma}, \tilde{v}))$ de $\pi_1(\Gamma, v)$.

O subgrupo de $\pi_1(\Gamma, v)$ ao qual uma dada aplicação de recobrimento pertence é determinado a menos de conjugação (cf. [2, p. 153]). Tem-se também que, essencialmente, existe exatamente uma aplicação de recobrimento pertencente a um dado subgrupo de $\pi_1(\Gamma, v)$. O seguinte resultado fala da existência de tal recobrimento. Sua demonstração pode ser encontrada em [2, p. 155].

Teorema 2.5.20. Sejam Γ um grafo, v um vértice de Γ e H um subgrupo de $\pi_1(\Gamma, v)$. Então, existe um recobrimento $p : \tilde{\Gamma} \to \Gamma$ pertencente a H. Em outras palavras, existe uma aplicação de recobrimento $p : \tilde{\Gamma} \to \Gamma$ tal que $p(\pi_1(\tilde{\Gamma}, \tilde{v}))$ é isomorfo a H

2.5.4 O Teorema de Schreier

Finalmente, podemos provar o famoso resultado:

Teorema 2.5.21. (Schreier) Todo subgrupo de um grupo livre é também livre. Além disso, um subgrupo H de um grupo livre F de índice finito tem posto $d(H)$ dado por

$$d(H) = (d(F) - 1)[F : H] + 1$$

onde $d(F)$ é o posto de F ou, equivalentemente, é o número minimal de geradores de F.

Demonstração. Sejam F um grupo livre com base X e G um grafo com apenas um vértice v e um par de arestas $e_x, \bar{e}_x$ para cada elemento $x \in X$.

Pelo Corolário 2.5.9, cada elemento da base de $\pi_1(G)$ corresponde a um par de arestas $e_x, \bar{e}_x$, assim, $\pi_1(G)$ é isomorfo a F.

O Teorema 2.5.20 garante a existência de uma aplicação de recobrimento $p : \tilde{G} \to G$ que pertence a H, quando H é visto como um subgrupo de $\pi_1(G)$. Ou seja, $p^*(\pi_1(\tilde{G}))$ é isomorfo a H. Ainda pelo Corolário 2.5.9, $\pi_1(\tilde{G})$ é livre, pois $\tilde{G}$ é grafo. Portanto, H é livre.

Agora, como G tem apenas um vértice, o conjunto de vértices de $\tilde{G}$ é dado por $p^{-1}(v)$. Pelo Corolário 2.5.18, $p^{-1}(v)$ está em bijeção com o conjunto das classes laterais de $p^*(\pi_1(\tilde{G}))$ em $\pi_1(G)$, ou seja, está em bijeção com as classes laterais de H em F. Isso significa que $|p^{-1}(v)| = [F : H]$, ou seja, $\tilde{G}$ tem $[F : H]$ vértices.

Como G tem um par de arestas para cada elemento de X, G tem no total $2d(F)$ arestas e todas elas têm inicio em v. Como p induz uma bijeção entre $E_{\tilde{v}}(\tilde{\Gamma})$ e $E_v(\Gamma)$, para cada $\tilde{v} \in p^{-1}(v)$, $\tilde{G}$ tem $2d(F)$ arestas com inicio em cada um dos seus $[F : H]$ vértices, totalizando $2d(F)[F : H]$ arestas.

Pelo Corolário 2.5.11, como $\tilde{G}$ tem $[F : H]$ vértices e $d(F)[F : H]$ pares de arestas, o posto de $\pi_1(\tilde{G})$ e, portanto, o de H é dado por $d(H) = d(F)[F : H] - [F : H] + 1$, ou seja,

$$d(H) - 1 = (d(F) - 1)[F : H]$$

□

Vejamos uma pequena aplicação do Teorema 2.5.21.

Lema 2.5.22. Sejam A e B grupos não triviais tais que B e $A/[A, A]$ são finitos e A não é isomorfo a C_2. Seja ainda $\alpha : A * B \to A/[A, A] \times B$ a aplicação tal que $\alpha|_A$ é a projeção canônica e $\alpha|_B$ é a identidade em B. Então $\ker \alpha$ possui subgrupo livre não abeliano.

Demonstração. $A * B$ possui subgrupo livre F de posto 2, pelo Lema 2.3.13. Seja $\mu = \alpha|_F : F \to A/[A, A] \times B$. Como $F/\ker(\mu) \simeq Im(\mu)$, tem-se que $[F : \ker(\mu)] = |Im(\mu)| \leq |A/[A, A] \times B| < \infty$. Como $\ker(\mu)$ é livre, o Teorema 2.5.21 garante que, se $d(F), d(\ker \mu)$ denotam o número de geradores livres de F e de $\ker \mu$, respectivamente, então

$$d(\ker \mu) - 1 = (d(F) - 1)[F : \ker \mu]$$

Como F tem posto 2 e $[F : \ker(\mu)] \geq 1$, tem-se que $d(\ker(\mu)) - 1 \geq 1$, ou seja, $d(\ker(\mu)) \geq 2$. Como todo grupo livre de posto pelo menos dois é não abeliano (cf. 2.1.24), o resultado segue. □

Capítulo 3

Produtos Entrelaçados Finitamente Apresentáveis

Este capítulo tem como base o artigo *Finitely Presented Wreath Products And Double Coset Decompositions*, de Yves de Cournulier [3] e tem como objetivo a demonstração do seguinte resultado.

Teorema Principal. Sejam W um grupo não trivial e G um grupo que age sobre o conjunto não vazio X. Então, $W \wr_X G$ é finitamente apresentável se, e somente se, G e W são finitamente apresentáveis, os estabilizadores de G em X são finitamente gerados e G age diagonalmente em $X \times X$ com finitas órbitas.

Para obter tal resultado, mostraremos cada uma dessas implicações separadamente nos Teoremas 3.3.5 e 3.3.25.

3.1 Produto Entrelaçado de Grupos

Dados um grupo W e um conjunto X, escrevemos $W^{(X)}$ para denotar a soma direta $\bigoplus_{x \in X} W_x = \{(w_x)_{x\in X} : w_x \in W \ e \ (w_x)_{x\in X}$ tem suporte finito$\}$, onde $W_x \simeq W, \forall x \in X$. Lembramos que o suporte de $(w_x)_{x\in X}$ é conjunto $\{x \in X : w_x \neq 1\}$.

Dados dois grupos G e W e um G-conjunto X, existe uma ação à esquerda de G na soma direta $W^{(X)}$ que permuta os fatores de $W^{(X)}$ pela ação de G em X: $G \times W^{(X)} \to W^{(X)}$, definida por $g \cdot (w_x)_{x\in X} = (v_x)_{x\in X}$, com $v_x = w_{g\cdot x}$. Observe que $g \cdot (w_x)_{x\in X} = g(w_x)_{x\in X} g^{-1}$.

Definimos o *produto entrelaçado* (ou produto *wreath*) entre G e W como sendo o produto semidireto $W^{(X)} \rtimes_\varphi G$, em que $\varphi : G \to Aut(W^{(X)})$ é dado por $\varphi(g)(w) = g \cdot w$, onde $\cdot$ denota a ação de G em $W^{(X)}$ dada acima, assim em $W \rtimes G$ temos $\varphi(g)(w) = gwg^{-1}$. O produto entrelaçado será denotado por $W \wr_X G$.

Exemplo 3.1.1. Estudemos o produto entrelaçado $C_2 \wr_X C_2$. Vejamos o segundo C_2 como o grupo das permutações de ordem dois $S_2 = \{id, \delta\}$ e $X = \{1, 2\}$. Considere a ação natural de S_2 em X, dada por $\sigma \cdot x = \sigma(x)$, $\sigma \in S_2$ e $x \in X$. Tem-se que $C_2^{(X)} = \{(c_1, c_2) : \ c_1, c_2 \in C_2\}$. Assim,

$C_2 \wr_X S_2 = \{((c_1, c_2), \sigma) : \ (c_1, c_2) \in C_2^{(X)}, \ \sigma \in C_2\}$ com o produto $((c_1, c_2), \sigma_1)((\tilde{c}_1, \tilde{c}_2), \sigma_2) = ((c_1, c_2)(\sigma_1 \cdot (\tilde{c}_1, \tilde{c}_2)), \sigma_1 \circ \sigma_2)$, em que $id \cdot (\tilde{c}_1, \tilde{c}_2) = (\tilde{c}_1, \tilde{c}_2)$ e $\delta \cdot (\tilde{c}_1, \tilde{c}_2) = (\tilde{c}_2, \tilde{c}_1)$.

Seja $C_2 = \{1, x\}$. Então, $r = ((x, 1), \delta) \in C_2 \wr_X C_2$ é tal que

$$((x,1),\delta)^2 = ((x,x),id) \qquad ((x,1),\delta)^3 = ((1,x),\delta) \qquad ((x,1),\delta)^4 = ((1,1),id)$$

enquanto $f = ((x, x), \delta)$ e rf têm ordem 2. Além disso, $\langle((x, x), \delta)\rangle\langle((x, 1), \delta)\rangle = C_2 \wr_X S_2$. Assim, $C_2 \wr_X S_2$ é gerado por r e f. Portanto, $C_2 \wr_X C_2 \simeq D_8$.

3.2 Produtos Entrelaçados Finitamente Gerados e a Apresentação do Produto Entrelaçado

Nesta seção, veremos a apresentação de produtos entrelaçados. Iniciaremos tal processo mostrando condições necessárias e suficientes para que o produto $W \wr_X G$ seja finitamente gerado. Depois, mostraremos uma apresentação para um produto entrelaçado $W \wr_X G$ no qual G age transitivamente em X, seguida da apresentação no caso mais geral.

Proposição 3.2.1. Com as notações anteriores, se o G-conjunto X é não vazio e o grupo W for não trivial, a fim de que $W \wr_X G$ seja finitamente gerado, é necessário e suficiente que G e W sejam finitamente gerados e que G tenha finitas órbitas em X.

Demonstração. Daremos inicio à demonstração mostrando que tal condição é suficiente. Existem $A \subset W$ e $B \subset G$ subconjuntos finitos tais que $W = \langle A \rangle$ e $G = \langle B \rangle$. Seja I o conjunto dos representantes das G-órbitas sobre X. Tem-se que $X = G \cdot I$ e, por hipótese, I é finito.

Defina para cada $x \in X$, $\varphi_x : W \to W_x$, que leva W na sua cópia W_x, ou seja, $w \mapsto w_x$. Tem-se que $\varphi_x(A) = A_x \subset W_x$. Assim, $W_x = \varphi_x(W) = \varphi_x(\langle A \rangle) = \langle \varphi_x(A) \rangle = \langle A_x \rangle$. Como $W^{(X)} = \bigoplus_{x \in X} W_x = \bigoplus_{x \in X} \varphi_x(W)$, tem-se que $W^{(X)}$ é gerado por $\bigcup_{x \in X} A_x$, pois cada elemento em $W^{(X)}$ pode ser visto como um produto. Tem-se então que $W \wr_X G$ é gerado por $(\bigcup_{x \in X} A_x) \cup B$. Porém, pela definição da ação de G em $W^{(X)}$, basta tomarmos os geradores dos W_i com $i \in I$, pois $g \cdot W_i = W_{g \cdot i}$, assim, é possível chegar em todos os W_x com x na órbita $G \cdot i$ apenas com os geradores de G e os de W_i. Segue que o conjunto $(\bigcup_{i \in I} A_i) \cup B$ gera $W \wr_X G$. Como I, B e cada A_x são finitos, tal conjunto gerador é finito.

Por outro lado, seja S um conjunto finito tal que $W \wr_X G = \langle S \rangle$. Primeiramente, mostremos que G é finitamente gerado. Podemos tomar a projeção $\pi : W \wr_X G \to G$, na qual $\pi(W) = \{1\}$ e a restrição de π a G é a identidade. Assim, pela sobrejetividade de π, tem-se que

$$G = \pi(W \wr_X G) = \pi(\langle S \rangle) = \langle \pi(S) \rangle.$$

Como S é finito, $\pi(S)$ é finito. Logo, G é finitamente gerado.

Suponha que W não seja finitamente gerado. Então existe um subconjunto infinito D de W tal que $W = \langle D \rangle$ mas nenhum subconjunto de D gera W.

Como $W \wr_X G$ é finitamente gerado, é enumerável. Consequentemente, qualquer um de seus subconjuntos é finito ou infinito enumerável. Em particular, $D \subset W$ é enumerável. Considere então $D = \{d_i\}_{i \in \mathbb{N}}$ e denote $\langle d_1, d_2, \cdots d_i \rangle$ por W_i. Veja que $W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_n \subsetneq \cdots$. Tome

$H_i = W_i \wr_X G$, para cada inteiro positivo i. Como W_i é subgrupo próprio de W_{i+1}, devemos ter que H_i é subgrupo próprio de H_{i+1}, para todo inteiro positivo i. Além disso, $W = \bigcup_{i \in \mathbb{N}} W_i$, logo, $H = \bigcup_{i \in \mathbb{N}} H_i = W \wr_X G = \langle S \rangle$. Existe $n_0 \in \mathbb{N}$ tal que $S \subset H_{n_0}$, pois S é finito e está contido na união $\bigcup_{i \in \mathbb{N}} H_i$. Segue que $H = \langle S \rangle \subset H_{n_0} \subset H$, ou seja, $H = H_{n_0}$. Isso quer dizer que a sequência $H_1 \subsetneq H_2 \subsetneq \cdots \subsetneq H_i \subsetneq \cdots$ se estabiliza em H_{n_0}, isto é, $H_{n_0} = H_{n_0+l}, \forall l \in \mathbb{N}$, contradizendo a escolha dos H_i's. Segue que W é finitamente gerado.

Por fim, devemos mostrar que X possui um número finito de G-órbitas. Suponha que X possua infinitas G-órbitas. Então X pode ser escrito como união dos termos de uma sequência $X_1 \subsetneq X_2 \subsetneq \cdots$ de subconjuntos G-invariantes. Para isso, seja I um conjunto contendo exatamente um elemento de cada G-órbita de X. Tome $I_1 \subset I$ finito. Seja $X_1 = G \cdot I_1$. Em seguida, tome $I_2 \subset I \backslash \{I_1\}$ finito e seja $X_2 = G \cdot (I_1 \cup I_2)$. Pela escolha de X_2, tem-se que $X_1 \subsetneq X_2$. Indutivamente, podemos definir cada X_k tomando $I_k \in I \backslash \{I_1 \cup \ldots \cup I_{k-1}\}$ finito e fazendo $X_k = G \cdot (I_1 \cup \ldots I_k)$. Defina $J_n = W \wr_{X_n} G$. Tem-se que $J_n \subsetneq J_{n+1}, \forall n \in \mathbb{N}$, pois $X_n \subsetneq X_{n+1}$, e $W \wr_X G = \bigcup_{n \in \mathbb{N}} J_n$, mas não existe $n_0 \in \mathbb{N}$ tal que $W \wr_X G = J_{n_0}$, contradizendo o fato de $W \wr_X G$ ser finitamente gerado. □

Teorema 3.2.2. Sejam G e W grupos com apresentações $\langle X_1 | R_1 \rangle$ e $W = \langle X_2 | R_2 \rangle$, onde G age sobre X. Então, X é a união de G-órbitas $X = \bigcup_{i \in I} G \cdot i = \bigcup_{i \in I} G/H_i$, onde I é um conjunto de representantes das G-órbitas em X. Então, $W \wr_X G$ tem apresentação

$$W \wr_X G = \langle X_1 \cup X_2 |\ R_1,\ R_2,\ [H, W],\ \{[W, gWg^{-1}] :\ g \in G \backslash H\} \rangle \tag{3.2.1}$$

se G age transitivamente sobre X e

$$\begin{aligned} W \wr_X G =& \langle X_1 \cup (\bigcup_{i \in I} X_{2,i}) | R_1, \bigcup_{i \in I} R_{2,i}, \{[W_i, gW_ig^{-1}] : i \in I,\ g \in G \backslash H_i\}, \\ & \{[W_i, gW_jg^{-1}] :\ g \in G,\ i, j \in I \ \text{ e } i \neq j\} \\ & \{[H_i, W_i] :\ i \in I\} \rangle. \end{aligned} \tag{3.2.2}$$

caso contrário, em que as cópias W_i de W têm apresentação $W_i = \langle X_{2,i} | R_{2,i} \rangle$.

Demonstração. Considere inicialmente o caso em que G age transitivamente sobre X, caso em que podemos escrever $X = G/H$, para algum estabilizador $H = G_{x_0}$, $x_0 \in X$, pela proposição 1.6.5. Pela definição de ação transitiva, X é uma órbita de G, ou seja, $X = G \cdot x_0$. Ponha $W_{x_0} = W$.

Dado $x \in X$, existe $g \in G$ tal que $g \cdot x_0 = x$. Assim,

$$W_x = W_{g \cdot x_0} = g \cdot W_{x_0} = gW_{x_0}g^{-1}.$$

Consequentemente, $W^{(X)}$ é gerado por $X_1 \cup X_2$, de modo que $W \wr_X G$ também é gerado por tal conjunto.

Se $h \in H$, então $h \cdot x_0 = x_0$, pela escolha de H. Assim,

$$hW_{x_0}h^{-1} = h \cdot W_{x_0} = W_{h \cdot x_0} = W_{x_0}.$$

Ou seja, $hWh^{-1} = W,\ \forall h \in H$. Devemos ter que $[H, W] = \{1\}$ em $W \wr_X G$.

Além disso, como $W^{(X)} = \bigoplus_{x \in X} W_x$, devemos ter que $[W_{x_i}, W_{x_j}] = \{1\}$, sempre que $x_i \neq x_j$. Sejam $g_i, g_j \in G$ tais que $g_i \cdot x_0 = x_i$ e $g_j \cdot x_0 = x_j$. Tem-se que $g_i \cdot x_0 = x_i \neq x_j = g_j \cdot x_0$, logo, $g_i g_j^{-1} \cdot x_0 \neq x_0$, ou seja, $g_i g_j^{-1} \notin H$. Tem-se que

$$\begin{aligned} \{1\} = [W_{x_i}, W_{x_j}] &= [g_i W_{x_0} g_i^{-1}, g_j W_{x_0} g_j^{-1}] \\ &= g_i [W_{x_0}, g_i^{-1} g_j W_{x_0} g_j^{-1} g_i] g_i^{-1}. \end{aligned}$$

Mas isso ocorre se, e somente se, $[W_{x_0}, (g_i^{-1} g_j) \cdot W_{x_0}] = \{1\}$. Como x_i e x_j são arbitrários, segue que $[W_{x_0}, gW_{x_0}] = \{1\}, \forall g \in G \backslash H$.

Tome $R = R_1 \cup R_2 \cup [H, W] \cup \{[W, gWg^{-1}] : \ g \in G \backslash H\}$. Afirmamos que $W \wr_X G = \langle X_1 \cup X_2 |\ R \rangle$.

Seja F o grupo livre com base $X_1 \cup X_2$. Como $W \wr_X G$ é gerado por $X_1 \cup X_2$, podemos tomar a inclusão $X_1 \cup X_2 \hookrightarrow W \wr_X G$. A propriedade universal de F nos dá um homomorfismo $\varphi : F \to W \wr_X G$ tal que a sua restrição a $X_1 \cup X_2$ é a identidade.

Como R é o conjunto trivial em $W \wr_X G$, tem-se que $R \subset \ker \varphi$. Por 2.2.13, existe um homomorfismo $\bar{\varphi} : F/\langle R \rangle^F \to W \wr_X G$ tal que $\bar{\varphi}(f \langle R \rangle^F) = \varphi(f)$, para $f \in F$.

Defina $\psi : X_1 \cup X_2 \to F/\langle R \rangle^F$ por $\psi(x) = x \langle R \rangle^F$. Como $X_1 \cup X_2$ gera $W \wr_X G$, existe uma extensão $\bar{\psi} : W \wr_X G \to F/\langle R \rangle^F$. Tem-se que $\psi = \varphi^{-1}$. Portanto, φ é isomorfismo. Vale que

$$W \wr_X G = \langle X_1 \cup X_2 |\ R_1,\ R_2,\ [H, W],\ \{[W, gWg^{-1}] : \ g \in G \backslash H\} \rangle$$

Vejamos agora o caso em que G não age transitivamente sobre X. Nesse caso, X é uma união disjunta de G-órbitas em X: $X = \bigcup_{i \in I} G \cdot i = \bigcup_{i \in I} G/H_i$, onde I é um representantes das G-órbitas em X, que não necessariamente é finito, e H_i é o estabilizador G_i. Tem-se que $W^{(X)} = \bigoplus_{x \in X} W_x = \bigoplus_{i \in I} (\bigoplus_{g \in G \backslash H_i} W_{g \cdot i}) = \bigoplus_{i \in I} (\bigoplus_{g \in G \backslash H_i} g W_i g^{-1})$. Seja $W_i = \langle X_{2,i} | R_{2,i} \rangle$ a apresentação da cópia W_i de W. Veja que, se $g \in G \backslash H_i$, então $g \cdot i \neq i$, logo $[W_i, gW_i g^{-1}] = \{1\}$, pois esses são termos distintos da soma direta.

Agora, se $i \neq j$, então i e j são elementos de G-órbitas distintas, pela escolha de I. Assim, não pode haver $g \in G$ tal que $g \cdot i = j$. Como consequência, $[W_i, gW_j g^{-1}]$ é trivial para todos $i, j \in I$ distintos e $g \in G$.

Veja também que, como H_i estabiliza i, ou seja, dado $h_i \in H_i$, tem-se que $h_i \cdot i = i$, temos que $h_i W_i h_i^{-1} = W_i$. Consequentemente, $[H_i, W_i] = \{1\}$, para todo $i \in I$.

Juntamente com R_1 e R_2, essas são as únicas relações em $W \wr_X G$. Desse modo,

$$\begin{aligned} W \wr_X G = &\langle X_1 \cup (\bigcup_{i \in I} X_{2,i}) | R_1, \bigcup_{i \in I} R_{2,i}, \{[W_i, gW_i g^{-1}] : i \in I,\ g \in G \backslash H_i\}, \\ &\{[W_i, gW_j g^{-1}] : \ g \in G,\ i, j \in I \ \text{ e } i \neq j\} \\ &\{[H_i, W_i] : \ i \in I\} \rangle. \end{aligned}$$

$\square$

3.3 Produtos Entrelaçados Finitamente Apresentáveis

Nesta seção, estudaremos condições necessárias e suficientes para que um certo produto entrelaçado seja finitamente apresentável.

3.3.1 Condição Suficiente

Lema 3.3.1. Sejam G um grupo e A, B subgrupos finitamente gerados de G, digamos $A = \langle a_1, \cdots, a_n \rangle$ e $B = \langle b_1, \cdots, b_m \rangle$. Se $a_i b_j a_i^{-1} = b_j$, para todos $i = 1 \dots n$ e $j = 1 \dots m$, então $aba^{-1} = b$, para todos $a \in A$ e $b \in B$.

Demonstração. Cada elemento de A pode ser visto como uma palavra do alfabeto $\{a_1^{\pm 1}, \cdots, a_n^{\pm 1}\}$ e cada elemento de B como uma palavra do alfabeto $\{b_1^{\pm 1}, \cdots, b_m^{\pm 1}\}$. A demonstração será feita por dupla indução no comprimento de $a = a_{i_1}^{\varepsilon_1} \cdots a_{i_p}^{\varepsilon_p}$ e de $b = b_{j_1}^{\delta_1} \cdots b_{j_q}^{\delta_q}$.

Se $a = a_i$ e $b = b_j$, então $a_i b_j a_i^{-1} = b_j$, por hipótese. Suponha que, para $|\bar{a}| = p - 1$ e $b = b_j$ tenha-se $\bar{a} b_j \bar{a}^{-1} = b_j$. Então, para $a = a_{i_1}^{\varepsilon_1} \cdots a_{i_p}^{\varepsilon_p}$, tem-se

$$aba^{-1} = a_{i_1}^{\varepsilon_1} \cdots a_{i_p}^{\varepsilon_p} b_j a_{i_p}^{-\varepsilon_p} \cdots a_{i_1}^{-\varepsilon_1} = a_{i_1}^{\varepsilon_1} (a_{i_2}^{\varepsilon_2} \cdots a_{i_p}^{\varepsilon_p} b_j a_{i_p}^{-\varepsilon_p} \cdots a_{i_2}^{-\varepsilon_2}) a_{i_1}^{-\varepsilon_1} = a_{i_1}^{\varepsilon_1} b_j a_{i_1}^{-\varepsilon_1} = b_j = b$$

Logo, $ab_ja^{-1} = b_j, \forall a \in A$ e $1 \leq j \leq m$. Suponha que $|\tilde{b}| = q - 1$ implica $a\tilde{b}a^{-1} = \tilde{b}, \forall a \in A$. Então se $b = b_{j_1}^{\delta_1} \cdots b_{j_q}^{\delta_q}$, tem-se

$$aba^{-1} = ab_{j_1}^{\delta_1} \cdots b_{j_q}^{\delta_q} a^{-1} = (ab_{j_1}^{\delta_1} \cdots b_{j_{q-1}}^{\delta_{q-1}} a^{-1})(ab_{j_q}^{\delta_q} a^{-1}) = (b_{j_1}^{\delta_1} \cdots b_{j_{q-1}}^{\delta_{q-1}})(b_{j_q}^{\delta_q}) = b_{j_1}^{\delta_1} \cdots b_{j_q}^{\delta_q} = b$$

□

Observação 3.3.2. Num grupo K, com $\alpha_1, \alpha_2, \beta \in K$, se $[\alpha_1, \beta] = 1 = [\alpha_2, \beta]$, então $[\alpha_1 \alpha_2^{-1}, \beta] = 1$. De fato, veja que $[\alpha_2, \beta] = 1 \Rightarrow [\alpha_2^{-1}, \beta] = 1$, assim,

$$[\alpha_1 \alpha_2^{-1}, \beta] = \alpha_1 \alpha_2^{-1} \beta \alpha_2 \alpha_1^{-1} \beta^{-1} = \alpha_1 (\alpha_2^{-1} \beta \alpha_2 \beta^{-1}) \beta \alpha_1^{-1} \beta^{-1} =$$

$$= \alpha_1 [\alpha_2^{-1}, \beta] \beta \alpha_1^{-1} \beta^{-1} = \alpha_1 \beta \alpha_1^{-1} \beta^{-1} = [\alpha_1, \beta] = 1$$

Analogamente, tem-se que $[\beta, \alpha_1] = 1$ e $[\beta, \alpha_2] = 1$ implica em $[\beta, \alpha_1 \alpha_2^{-1}] = 1$.

Lema 3.3.3. Sejam W um grupo finitamente gerado e G um grupo que age transitivamente no conjunto X. Sejam H um estabilizador de G em X e $\mathscr{T}$ um conjunto contendo exatamente um elemento de cada classe lateral dupla de $H \backslash G / H$. Como W é finitamente gerado, existe um subconjunto S finito de W tal que $W = \langle S \rangle$. Se $\{[s_i, ts_jt^{-1}], s_i, s_j \in S, \ t \in \mathscr{T}\}$ é trivial, então $\{[w_1, gw_2g^{-1}] : w_1, w_2 \in W, \ g \in G \backslash H\}$ é trivial.

Demonstração. Como a ação de G em X é transitiva, tem-se que $X = G/H$, onde $H = G_{x_0}$, para algum $x_0 \in X$. Fixamos, como anteriormente, $W_{x_0} = W$. Vimos que cada cópia W_x de W pode ser obtida de W_{x_0} pois $W_x = gW_{x_0}g^{-1}$, onde $g \in G$ é tal que $g \cdot x_0 = x$. Vimos também que H fixa os elementos de $W = W_{x_0}$. Como consequência, para cada $h \in H$ e cada $g \in G \setminus H$, vale que $[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, (hg)s_j(hg)^{-1}] = 1$, $\forall s_i, s_j \in S$ e $\forall g \in G$. De fato, se $[s_i, gs_jg^{-1}] = 1$, então, dado $h \in H$, tem-se $1 = h[s_i, gs_jg^{-1}]h^{-1} = [hs_ih^{-1}, hgs_jg^{-1}h^{-1}] = [h \cdot s_i, (hg)s_j(hg)^{-1}] = [s_i, (hg)s_j(hg)^{-1}]$. Por outro lado, se $[s_i, (hg)s_j(hg)^{-1}] = 1$, então $1 = [s_i, (hg)s_j(hg)^{-1}] = [h \cdot s_i, (hg)s_j(hg)^{-1}] = [hs_ih^{-1}, hgs_jh^{-1}g^{-1}] = h[s_i, gs_jg^{-1}]h^{-1}$. Segue que $[s_i, gs_jg^{-1}] = 1$.

Analogamente, $[g^{-1}s_ig, s_j] = 1 \Leftrightarrow [hg^{-1}s_igh^{-1}, s_j] = 1$. Como $[g^{-1}s_ig, s_j] = 1$ e $[hg^{-1}s_igh^{-1}, s_j] = 1$ são equivalentes a $[s_i, gs_jg^{-1}] = 1$ e $[s_i, gh^{-1}s_jhg^{-1}] = 1$, respectivamente, vale que $[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, gh^{-1}s_jhg^{-1}] = 1 \Leftrightarrow 1 = [hs_ih^{-1}, hgh^{-1}s_jhg^{-1}h^{-1}] = [s_i, hgh^{-1}s_jhg^{-1}h^{-1}]$.

Logo, para cada $t \in HgH$, $[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, ts_jt^{-1}] = 1$.

Além disso, se $\{[s_i, gs_jg^{-1}] : s_i, s_j \in S,\ g \in G\backslash H\}$ é trivial, então $\{[w_1, gw_2g^{-1}] : w_1, w_2 \in W,\ g \in G\backslash H\}$ é trivial, pela Observação 3.3.2. Segue então que, se $\{[s_i, ts_jt^{-1}], s_i, s_j \in S,\ t \in \mathscr{T}\}$ é trivial, então $\{[w_1, gw_2g^{-1}] : w_1, w_2 \in W,\ g \in G\backslash H\}$ também é trivial. $\square$

Vejamos uma generalização do lema anterior, no caso em que a ação de G em X não necessariamente é transitiva. Nesse caso, podemos escrever X como uma união disjunta de órbitas de G: $X = \bigcup_{i\in I} G\cdot i = \bigcup_{i\in I} G/H_i$, onde I é um conjunto de representantes das G-órbitas em X e H_i é o estabilizador G_i. Para cada $i \in I$, tome uma cópia W_i de W. Como, por hipótese, W é finitamente gerado, cada cópia W_i é finitamente gerada. Assim, existe um conjunto finito S_i tal que $W_i = \langle S_i\rangle$, $\forall i \in I$. Podemos então enunciar:

Lema 3.3.4. Nas condições dadas, vale que, se $\{[s_i, ts_jt^{-1}] :\ s_i \in S_i,\ s_j \in S_j,\ t \in \mathscr{T}\}$ é trivial, então $\{[W_i, gW_jg^{-1}] :\ g \in G,\ i, j \in I\}$ é trivial, onde $\mathscr{T}$ é um conjunto contendo exatamente um elemento de cada classe lateral dupla de $H_i\backslash G/H_j$, para cada $i, j \in I$.

Demonstração. Como $W_i = \langle S_i\rangle$ e $W_j = \langle S_j\rangle$, $i, j \in I$, se $\{[s_i, gs_jg^{-1}] :\ g \in G,\ s_i \in S_i,\ s_j \in S_j,\ i, j \in I\}$ é trivial, então $\{[W_i, gW_jg^{-1}] :\ g \in G,\ i, j \in I\}$ também é, pela observação 3.3.2. Mostremos então que, se o conjunto dado no enunciado é trivial, então $\{[s_i, gs_jg^{-1}] :\ g \in G,\ s_i \in S_i,\ s_j \in S_j,\ i, j \in I\}$ é trivial.

Tomando $w \in W_i$, tem-se que $h_i \in H_i$ é tal que $h_i \cdot w = h_iwh_i^{-1} = w$. Em particular, $h_i \cdot s_i = s_i, \forall s_i \in S_i$. Assim, para cada $h_i \in H_i$,

$$[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, h_igs_jg^{-1}h_i^{-1}] = 1$$

com $s_i \in S_i$, $s_j \in S_j$, $i, j \in I$ e $g \in G$. Além disso, analogamente ao resultado mostrado no lema anterior, tem-se que

$$[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, gh_j^{-1}s_jh_jg^{-1}] = 1$$

para cada $h_j \in H_j$, $s_i \in I$, $s_j \in S_j$, $i, j \in I$ e $g \in G$.

Tome então um único elemento g_{ij} de H_igH_j de cada classe lateral de $H_i\backslash G/H_j$ e para cada par (i, j) de elementos de $I \times I$. Seja $\mathscr{T} = \{g_{ij}\}_{i,j\in I}$. Tem-se que

$$[s_i, gs_jg^{-1}] = 1 \Leftrightarrow [s_i, g_{ij}s_jg_{ij}^{-1}] = 1$$

Desse modo, se o conjunto $\{[s_i, ts_jt^{-1}] :\ s_i \in S_i,\ s_j \in S_j,\ t \in \mathscr{T}\}$ for trivial, teremos que o conjunto $\{[W_i, gW_jg^{-1}] :\ g \in G,\ i, j \in I\}$ também é trivial. $\square$

Teorema 3.3.5. Sejam W e G grupos finitamente apresentáveis, onde G age num conjunto X, de modo que seus estabilizadores são finitamente gerados. Se a ação de G em X^2 tem finitas órbitas, então $W \wr_X G$ é finitamente apresentável.

Demonstração. Mostraremos primeiro o caso em que G age transitivamente sobre X, ou seja, $X = G/H$, com $H = G_{x_0}$, para algum $x_0 \in X$.

Como G e W são finitamente apresentáveis, existem apresentações $G = \langle X_1 | R_1 \rangle$ e $W = \langle X_2 | R_2 \rangle$ tais que X_1, X_2, R_1, R_2 são finitos. Defina $T_1 = \{[h, w] : \ h \in H \ , \ w \in W\}$, $T_2 = \{[w_1, gw_2g^{-1}] : w_1, w_2 \in W \ , \ g \in G \backslash H\}$ e tome $T = T_1 \cup T_2$. Como vimos na apresentação 3.2.1, $\langle X_1, X_2 | R_1, R_2, T \rangle$ é uma apresentação para $W \wr_X G$. Queremos simplificar tal apresentação para que seja finita. Para isso, basta que T seja consequência de um número finito de relatores, ou seja, devemos encontrar um subconjunto finito $\tilde{T}$ de T tal que as relações de $\tilde{T}$ impliquem nas relações de T. Podemos escrever $H = \langle h_1, \ldots, h_m \rangle$ e $X_2 = \{\tilde{w}_1, \ldots \tilde{w}_k\}$, pois, por hipótese, H e W são finitamente gerados.

Em particular, como T_1 é trivial, $\tilde{T}_1 = \{h_i \tilde{w}_j h_i^{-1} \tilde{w}_j^{-1} : 1 \leq i \leq m \ , \ 1 \leq j \leq k\}$ é trivial. Pelo Lema 3.3.1, $\tilde{T}_1 = \{1\}$ implica $T_1 = \{1\}$, logo, as relações contidas em T_1 são consequência das relações de $\tilde{T}_1$. Isso nos permite tomar apenas o conjunto finito $\tilde{T}_1$ em vez de T_1 na apresentação de $W \wr_X G$, ou seja, $W \wr_X G = \langle X_1, X_2 | R_1, R_2, \tilde{T}_1, T_2 \rangle$.

Como a ação de G em X é transitiva, estamos no caso do Lema 3.3.3, T_2 é trivial quando o conjunto $\tilde{T}_2 = \{[\tilde{w}_i, t\tilde{w}_j t^{-1}], i, j \in \{1, \ldots, k\}, \ t \in \mathscr{T}\}$ for trivial, onde $\mathscr{T}$ é um conjunto contendo exatamente um elemento de cada uma das distintas classes laterais duplas de $H \backslash G / H$. Assim, $W \wr_X G = \langle X_1, X_2 | R_1, R_2, \tilde{T}_1, \tilde{T}_2 \rangle$. Por hipótese, a ação de G sobre $X \times X$ tem um número finito de órbitas $|(X \times X)/G|$. Agora, tem-se que $|\{HgH : g \in G\}| = |(G/H \times G/H)/G| = |(X \times X)/G| < \infty$. Segue que $\tilde{T}_2$ é finito.

Vejamos o caso geral. Como W é finitamente apresentável, cada uma de suas cópias também é. Para cada $i \in I$, sejam $X_{2,i}$ e $R_{2,i}$ finitos tais que $W_i = \langle X_{2,i} | R_{2,i} \rangle$. Seja ainda Δ_i um cojunto finito que gera H_i. Vimos em 3.2.2 que $W \wr_X G = \langle X_1, (\bigcup_{i \in I} X_{2,i}) | R_1, \bigcup_{i \in I} R_{2,i}, \{[W_i, gW_ig^{-1}] : i \in I, \ g \in G \backslash H_i\}, \ \{[W_i, gW_jg^{-1}] : \ g \in G, \ i, j \in I \ \text{ e } i \neq j\}, \{[H_i, W_i] : \ i \in I\} \rangle$. Denote por $\mathscr{T}_{ij}$ um conjunto contendo exatamente um elemento de cada classe lateral de $H_i \backslash G / H_j$. Pelo Lema 3.3.1, podemos tomar $\{[h_i, x_i] : \ h_i \in \Delta_i, \ x_i \in X_{2,i}, \ i \in I\}$ no lugar de $\{[H_i, W_i] : \ i \in I\}$ e, pelo Lema 3.3.4, podemos tomar $\{[x_i, tx_it^{-1}] : x_i \in X_{2,i}, \ t \in \mathscr{T}_{ii}\}_{i \in I}$ no lugar de $\{[W_i, gW_ig^{-1}] : i \in I, \ g \in G \backslash H_i\}$ e $\{[x_i, tx_jt^{-1}] : \ x_i, \in X_{2,i}, \ x_j \in X_{2,j}, \ t \in \mathscr{T}_{ij}, i, j \in I \text{ distintos}\}$ no lugar de $\{[W_i, gW_jg^{-1}] : \ g \in G, \ i, j \in I \ \text{ e } i \neq j\}$, na apresentação dada.

Como cada Δ_i, cada $X_{2,i}$ e I são finitos, o primeiro conjunto obtido é finito. Os demais conjuntos obtidos são finitos porque a ação de G em $X \times X$ tem finitas órbitas e $|(X \times X)/G| = |\{H_igH_j : \ i, j \in I, \ g \in G\}|$. □

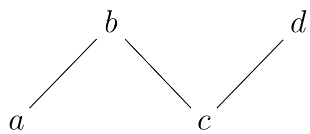
A recíproca do teorema anterior é válida. Para mostrá-la, contaremos com uma ferramenta conhecida como *produto grafo*, que será vista na subseção seguinte.

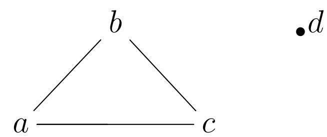
3.3.2 O Produto Grafo e a Condição Necessária

Nesta subseção, estudaremos o produto grafo entre grupos. Para isso precisaremos de algumas definições relativas a grafos. Aqui, um grafo não pode ter laços e não é direcionado. Proibimos também o caso em que existe mais de uma aresta ligando dois vértices. Para um estudo mais aprofundado no assunto, veja [5].

Definição 3.3.6. Um grafo Γ é um par (Γ^0, Γ^1), onde Γ^0 é um conjunto não vazio, cujos elementos são chamados de *vértices* e Γ^1 é um conjunto de subconjuntos de cardinalidade dois de Γ^0, chamados de *arestas*.

Exemplo 3.3.7. O grafo $\Gamma = (\Gamma^0, \Gamma^1)$, onde $\Gamma^0 = \{a, b, c, d\}$ e $\Gamma^1 = \{\{a, b\}, \{b, c\}, \{c, d\}\}$ pode ser representado com na figura abaixo à esquerda, enquanto o grafo $\tilde{\Gamma} = (\Gamma^0, \tilde{\Gamma}^1)$, onde $\tilde{\Gamma}^1 = \{\{a, b\}, \{b, c\}, \{a, c\}\}$, pode ser representado pela figura abaixo à direita.





Dizemos que dois vértices $u, v \in \Gamma^0$ do grafo $\Gamma = (\Gamma^0, \Gamma^1)$ são *adjacentes* se $\{u, v\} \in \Gamma^1$. Duas arestas de Γ são adjacentes se têm um vértice em comum. Um grafo no qual todos os vértices são adjacentes é dito um *grafo completo*.

O *grau* de um vértice é o número de arestas incidentes a ele. Dizemos que um vértice de grau zero é um *vértice isolado*. Um grafo cujos vértices têm o mesmo grau r é dito um *grafo regular de grau r*.

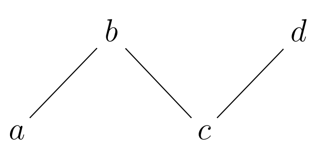
O *grafo complementar* de $\Gamma = (\Gamma^0, \Gamma^1)$ é o grafo $(\Gamma^0, (\Gamma^1)^C)$, onde $(\Gamma^1)^C = \{\{v_i, v_j\} : \{v_i, v_j\} \notin \Gamma^1\}$. Denotaremos o grafo complementar de Γ por Γ^C.

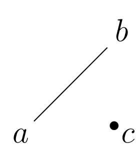
Dois grafos $\Gamma = (\Gamma^0, \Gamma^1), \tilde{\Gamma} = (\tilde{\Gamma}^0, \tilde{\Gamma}^1)$ são *isomorfos* se existe uma bijeção $\varphi : \Gamma^0 \to \tilde{\Gamma}^0$ tal que, para $u, v \in \Gamma^0$, o número de arestas ligando u e v é igual ao número de arestas ligando $\varphi(u)$ e $\varphi(v)$.

Um *subgrafo* $G = (G^0, G^1)$ de $\Gamma = (\Gamma^0, \Gamma^1)$ é um grafo tal que $G^0 \subset \Gamma^0$ e $G^1 \subset \Gamma^1$. Um subgrafo $G = (G^0, G^1)$ de $\Gamma = (\Gamma^0, \Gamma^1)$ é dito um *subgrafo induzido* de Γ se $\forall u, v \in G^0,\ \{u, v\} \in G^1 \Leftrightarrow \{u, v\} \in \Gamma^1$.

Dados dois grafos $\Gamma_1 = (\Gamma_1^0, \Gamma_1^1)$ e $\Gamma_2 = (\Gamma_2^0, \Gamma_2^1)$, onde $\Gamma_1^0 \cap \Gamma_2^0 = \varnothing$, definimos a *união* entre Γ_1 e Γ_2 como sendo o grafo $\Gamma_1 \cup \Gamma_2 = (\Gamma_1^0 \cup \Gamma_2^0, \Gamma_1^1 \cup \Gamma_2^1)$. Dizemos que um grafo é *conexo* se não pode ser escrito como a união de dois subgrafos distintos. Caso contrário, dizemos que o grafo é *desconexo*. O grafo que não contém nenhuma aresta é dito *totalmente desconexo*.

Exemplo 3.3.8. O grafo $(\{a, b, c, d\}, \{\{a, b\}, \{b, c\}, \{c, d\}\})$, dado no exemplo anterior é conexo, pois se o conjunto de vértices for dividido em dois, alguma aresta não poderá existir. O grafo $(\{a, b, c\}, \{\{a, b\}\})$ é desconexo, pois é a união dos grafos $(\{a, b\}, \{\{a, b\}\})$ e $(c, \varnothing)$.





Todo grafo desconexo pode ser escrito de forma única como a união de subgrafos conexos. Tais subgrafos conexos são denominados *componentes conexas* do grafo.

Definição 3.3.9. Chamamos um grupo G de *grupo grafo* se G tem apresentação $G = \langle X | R \rangle$ com $R \subset [X, X]$.

Essa definição é equivalente a

Definição 3.3.10. Dado um grafo $\Gamma = (\Gamma^0, \Gamma^1)$, o *grupo grafo* relativo a Γ é o grupo $G\Gamma = \langle \Gamma^0 | \{[v_i, v_j] : \{v_i, v_j\} \in \Gamma^1\}\rangle$

Exemplo 3.3.11. Quando Γ é o grafo é totalmente desconexo, ou seja, quando $R = \varnothing$, tem-se que $G\Gamma = \langle X|\varnothing\rangle$ é o grupo livre gerado por X.

Definição 3.3.12. Sejam $\Gamma = (\Gamma^0 = \{v_1, \dots, v_n\}, \Gamma^1)$ um grafo, $\{G_k\}_{k=1}^n$ uma família de grupos, onde cada G_k tem apresentação $G_k = \langle X_k | R_k\rangle$ e $\sigma \in S_n$. Tome $\mathbb{N}_0 = \{1, \dots, n\}$. Definimos o *produto grafo* dos G_k com relação a Γ e a σ como sendo o grupo

$$(G_k)_{k\in\mathbb{N}_0}^{\langle\Gamma\rangle}(\sigma) = \langle \bigcup_{k=1}^{n} X_k | \bigcup_{k=1}^{n} R_k, [G_{\sigma(i)}, G_{\sigma(j)}],\ \forall\{v_i, v_j\} \in \Gamma^1\rangle$$

Vimos que $*_{k=1}^n G_k = \langle \bigcup_{k=1}^n X_k | \bigcup_{k=1}^n R_k\rangle$. Assim, $(G_k)_{k\in\mathbb{N}_0}^{\langle\Gamma\rangle}(\sigma)$ é o quociente do produto livre dos G_k pelo fecho normal dos subgrupos comutadores apropriados.

Daqui para frente, omitiremos σ da notação acima sempre que não for importante explicitá-lo. Nesse caso, escreveremos simplesmente G_i em vez de $G_{\sigma(i)}$. Se todos os G_k forem iguais a um mesmo grupo G, denotaremos o produto grafo entre eles apenas por $G^{\langle\Gamma\rangle}$.

Exemplo 3.3.13. Com a notação acima, se Γ é o grafo completo, então $\{[G_i, G_j] : \{v_i, v_j\} \in \Gamma^1\} = \{[G_i, G_j] : i \neq j \text{ e } 1 \leq i, j \leq n\}$. Consequentemente, produto grafo da família $\{G_k\}_{k=1}^n$ com relação a Γ é

$$(G_k)_{k\in\mathbb{N}_0}^{\langle\Gamma\rangle} = \langle \bigcup_{k=1}^{n} X_k | \bigcup_{k=1}^{n} R_k, [G_i, G_j], \forall i, j \text{ distintos}\rangle = \times_{k=1}^n G_k$$

Exemplo 3.3.14. Ainda com a notação acima, se Γ é o grafo totalmente desconexo, então, como $\Gamma^1 = \varnothing$, o conjunto $\{[G_i, G_j] : \{v_i, v_j\} \in \Gamma^1\}$ é vazio. Segue que

$$(G_k)_{k\in\mathbb{N}_0} = \langle \bigcup_{k=1}^{n} X_k | \bigcup_{k=1}^{n} R_k\rangle = *G_k$$

é o produto livre entre os G_k.

Lema 3.3.15. Seja $\Gamma = (\Gamma^0, \Gamma^1)$ um grafo. Para cada $i \in \Gamma^0$, tome um grupo W_i. Seja $P = (W_i)_{i\in\Gamma^0}^{\langle\Gamma\rangle}$. Denote por σ_i os homomorfismos naturais (inclusão) que levam W_i em P. Então,

i. $\sigma_i : W_i \to P$ é injetiva, para todo $i \in \Gamma^0$;

ii. O homomorfismo natural $\sigma_i * \sigma_j : W_i * W_j \to P$ é injetivo, sempre que $\{i, j\} \notin \Gamma^1$;

iii. O homomorfismo natural $\sigma_i \times \sigma_j : W_i \times W_j \to P$ é injetivo, para todo $\{i, j\} \in \Gamma^1$;

iv. Se $\{i, k\}, \{j, k\}, \{i, j\} \notin \Gamma^1$, o homomorfismo natural $\sigma_i * \sigma_j * \sigma_k : W_i * W_j * W_k \to P$ é injetor.

v. Se $\{i, k\}, \{j, k\} \notin \Gamma^1$ mas $\{i, j\} \in \Gamma^1$, o homomorfismo natural $(\sigma_i \times \sigma_j) * \sigma_k : (W_i \times W_j) * W_k \to P$ é injetor.

Demonstração. Para cada $i \in \Gamma^0$, seja $W_i = \langle X_i | R_i \rangle$ uma apresentação para W_i.

i. Mostremos que σ_i tem inversa à esquerda. Seja π_i o homomorfismo canônico $\pi_i : P \to P/N$, onde N é o subgrupo normal de P gerado por todos os W_l, com $l \neq i$. Como $P = \langle \bigcup_{\lambda \in \Gamma^0} X_\lambda | \bigcup_{\lambda \in \Gamma^0} R_\lambda, \{[W_{\lambda_1}, W_{\lambda_2}] : \{\lambda_1, \lambda_2\} \in \Gamma^1\} \rangle$, tem-se que $P/N \simeq \langle X_i | R_i \rangle = W_i$. Como $P/N \simeq W_i$, segue que $\pi_i \circ \sigma_i = id_{W_i}$, quando consideramos $\pi_i : P \to W_i$.

ii. Esse caso é análogo ao anterior. Encontraremos um subgrupo normal N de P tal que P/N seja isomorfo a $W_i * W_j$ e assim, pelo argumento dado em **i.**, obteremos que o homomorfismo canônico $P \to P/N$ é a inversa à esquerda da aplicação dada.

Seja N é o subgrupo normal de P gerado por todos os W_l com $l \neq i, j$, então

$$P/N = \langle \bigcup_{\lambda \in \Gamma^0} X_\lambda | \bigcup_{\lambda \in \Gamma^0} R_\lambda, \{[W_{\lambda_1}, W_{\lambda_2}] : \{\lambda_1, \lambda_2\} \in \Gamma^1\} \rangle / N \simeq \langle X_i \cup X_j | R_i \cup R_j \rangle = W_i * W_j$$

pois $\{i, j\} \notin \Gamma^1$, por hipótese.

As demonstrações seguintes serão feitas usando o mesmo argumento, sem mais comentários.

iii. Com as notações do item **ii.**, tem-se que

$$P/N \simeq \langle X_i \cup X_j | R_i \cup R_j, [W_i, W_j] \rangle = W_i \times W_j$$

pois $\{i, j\} \in \Gamma^1$.

iv. Se $\{i, j\}, \{j, k\}, \{i, j\} \notin \Gamma^1$ e N é o subgrupo normal de P gerado por todos os W_l com $l \neq i, j, k$, então

$$P/N \simeq \langle X_i \cup X_j \cup X_k | R_i \cup R_j \cup X_k \rangle = W_i * W_j * W_k$$

v. Se $\{i, k\}, \{j, k\} \notin \Gamma^1$ e $\{i, j\} \in \Gamma^1$, então para N como em **iv.**, tem-se que

$$P/N \simeq \langle X_i \cup X_j \cup X_k | R_i \cup R_j \cup X_k, [W_i, W_j] \rangle$$

$$\simeq \langle X_i \cup X_j | R_i \cup R_j, [W_i, W_j] \rangle * \langle X_k | R_k \rangle = (W_i \times W_j) * W_k$$

□

Veremos agora propriedades do produto grafo que serão necessárias para a demonstração da outra implicação do Teorema Principal.

Dados dois grafos Γ e $\tilde{\Gamma}$, com o mesmo conjunto de vértices Γ^0 e conjuntos de arestas Γ^1 e $\tilde{\Gamma}^1$, respectivamente, com $\tilde{\Gamma}^1 \supseteq \Gamma^1$, podemos definir um homomorfismo ω entre $P = (W_i)_{i \in \Gamma^0}^{\langle \Gamma \rangle}$ e $\tilde{P} = (W_i)_{i \in \Gamma^0}^{\langle \tilde{\Gamma} \rangle}$, basta tomar ω como sendo o homomorfismo canônico, ao coniderar $\tilde{P}$ um quociente de P.

Afirmação 3.3.16. ω é bijetivo se, e somente se, $\tilde{\Gamma}^1 = \Gamma^1$

A definição de ω garante a sua sobrejetividade. Além disso, se $\Gamma^1 = \tilde{\Gamma}^1$, então ω é a identidade, logo, é bijetiva. Mostremos que também vale a recíproca, ou seja, se ω é bijetiva, então $\Gamma^1 = \tilde{\Gamma}^1$. De fato, se $\{i,j\} \in \tilde{\Gamma}^1$, então $\omega([W_i, W_j]) = \{1\}$. Como ω é injetiva, $\ker \omega = \{1\}$, logo, $[W_i, W_j] = \{1\}$

Se $\{i,j\} \notin \Gamma^1$, então, pelo Lema 3.3.15, $\sigma_i * \sigma_j$ é uma aplicação injetora que leva $W_i * W_j$ em P. Porém, $W_i * W_j = \langle X_i \cup X_j | R_i \cup R_j \rangle$, assim, dados $w_i \in W_i$ e $w_j \in W_j$, devemos ter que $w_i w_j w_i^{-1} w_j^{-1} \neq 1$, pois não há relação com elementos de W_j em R_i, nem com elementos de W_i em R_j. Porém, $\sigma_i * \sigma_j(w_i w_j w_i^{-1} w_j^{-1}) \in [W_i, W_j]$ que é trivial em P. Isso contradiz a injetividade de $\sigma_i * \sigma_j$.

Ainda com a notação acima, considere o homomorfismo canônico $\varphi : (W_i)_{i\in\Gamma^0}^{\langle\Gamma\rangle} = P \to \bigoplus_{i\in\Gamma^0} W_i$. Queremos mostrar que $\ker \varphi = Q$ normalmente contém um grupo livre não abeliano.

Seja $\tilde{\Gamma} = (\Gamma^0, \tilde{\Gamma}^1)$ o grafo completo. Pela Afirmação 3.3.16, ω é injetiva se, e somente se, $\Gamma^1 = \tilde{\Gamma}^1$. Assim, se Γ não é o grafo completo, então $Q \neq \{1\}$.

Seja Γ^C o grafo complementar de Γ. Veja que a decomposição de Γ em componentes conexas corresponde à decomposição de P em produtos livres, enquanto a decomposição de Γ^C corresponde à decomposição de P em somas diretas, pelo Lema 3.3.15.

Lema 3.3.17. Com a notação dada, suponha que cada W_i seja não trivial. Então as afirmações a seguir são equivalentes.

i. O núcleo de φ não contém subgrupos livres não abelianos.

ii. Cada componente conexa do grafo Γ^C tem no máximo dois elementos e W_i e W_j são isomorfos ao grupo cíclico de ordem dois C_2, sempre que $(\{i,j\}, \{\{i,j\}\})$ é uma componente conexa de Γ^C.

Demonstração. Suponha que valha **ii.**. Denote por J o conjunto de todos os vértices isolados de Γ^C. Seja também K um conjunto contendo exatamente um elemento de cada componente conexa com dois elementos de Γ^C. Então, o produto $P = (W_i)_{i\in\Gamma^0}^{\langle\Gamma\rangle}$ pode ser escrito da seguinte forma, considerando $W_i = \langle X_i | R_i \rangle, \forall i \in \Gamma^0$.

$$
\begin{aligned}
P &= \langle \bigcup_{i\in\Gamma^0} X_i | \bigcup_{i\in\Gamma^0} R_i, [W_i, W_j] : \{i,j\} \notin (\Gamma^1)^C \rangle \\
&= \langle \bigcup_{i\in\Gamma^0} X_i | \bigcup_{i\in\Gamma^0} R_i, \{[W_i, W_j] :\ i \in J,\ j \neq i\},\ \{[W_i, W_j], i,j \in K \text{ tais que } \{i,j\} \notin (\Gamma^1)^C\} \rangle \\
&= (\times_{j\in J} W_j) \times (\times_{\{i,j\}\in(\Gamma^1)^C} (W_i * W_j))
\end{aligned}
$$

onde a última igualdade é justificada pelo fato de $\Gamma^0 \backslash J$ só possuir componentes conexas com exatamente dois elementos: segue do Lema 3.3.15 pois, como $\{i,j\} \in (\Gamma^1)^C$, por definição, $\{i,j\} \notin \Gamma^1$ e o produto grafo entre eles é o produto livre. Ainda tem-se que i e j são adjacentes a todos os demais vértices, justificando o produto direto. Denote a segunda soma direta por P_0 e a primeira por C.

Veja que φ é a aplicação (id_C, φ_0), onde $\varphi_0 : P_0 \to \times_{i\in\Gamma^0\backslash J} W_i$ é restrição sobrejetiva a P_0. Podemos supor que $J = \varnothing$, pois $K = \ker \varphi \subset P_0$. Por hipótese, cada W_i é isomorfo a C_2, pois agora só estamos considerando as componentes conexas com exatamente dois elementos. Assim, $P = P_0 = (C_2 * C_2) \times \ldots \times (C_2 * C_2)$, um produto com $|\Gamma^0|/2 = n$ termos. Considere a aplicação natural $\theta : C_2 * C_2 \to C_2 \times C_2$, definida de modo que $\theta|_{C_2} = id_{C_2}$. Veja que $Q = \ker\theta \times \ker\theta \times \ldots \times \ker\theta$ (n fatores). Pelo Lema 2.3.11, $\ker\theta \simeq \mathbb{Z}$. Assim, $Q \simeq \mathbb{Z}^n$ é abeliano e não pode ter subgrupos livres não abelianos.

Para mostrar a outra aplicação, negaremos a parte **ii.**. Tal procedimento será dividido em dois casos: primeiramente, negaremos o fato de componentes que não são vértices isolados terem subgrupos isomorfos a C_2 em Γ^C. Em seguida, negaremos o fato de cada componente conexa de Γ^C ter no máximo dois elementos.

Caso 1. Suponha que Γ^C tenha uma componente conexa, com pelo menos dois elementos, com vértice i tal que W_i não é isomorfo a C_2. Seja j um vértice tal que $\{i, j\} \in (\Gamma^1)^C$

Tome um subgrupo Z_j cíclico não trivial de W_j e um subgrupo Z_i do tipo $\mathbb{Z}$, C_p com $p \geq 3$ primo, C_4 ou $C_2 \times C_2$ de W_i, pois $|W_i| \geq 3$.

Como $\{i, j\} \notin \Gamma^1$, pelo Lema 3.3.15, $W_i * W_j$ mergulha em P. Assim, $Z_i * Z_j \hookrightarrow W_i * W_j \hookrightarrow P$. Além disso, P é levado em $\bigoplus_{i\in\Gamma^0} W_i$ por φ. Logo, $Z_i * Z_j$ é mapeado no grupo abeliano $Z_i \times Z_j$ em $\bigoplus_{i\in\Gamma^0} W_i$ por φ. Queremos mostrar que $Q = \ker\varphi$ possui subgrupo livre não abeliano. Se $Z_i * Z_j$ tem um subgrupo livre não abeliano, o grupo derivado $[Z_i * Z_j, Z_i * Z_j]$ também tem. Veja que $[Z_i * Z_j, Z_i * Z_j] \subset Q$. Assim, se $Z_i * Z_j$ possui subgrupo livre não abeliano, Q também possui.

Inicialmente, suponha que $Z_i, Z_j \neq \mathbb{Z}$. Então, $Z_i \times Z_j$ é finito. Como Z_i não é isomorfo a C_2, podemos aplicar o Lema 2.5.22 com $A = Z_i$ e $B = Z_j$. Seja α a aplicação dada no lema. Tem-se que $\ker(\alpha)$ tem subgrupo livre não abeliano. Como $\ker(\alpha) \lhd Z_i * Z_j$, segue que $Z_i * Z_j$ contém tal subgrupo.

Se Z_i e $\mathbb{Z}_j$ são isomorfos a $\mathbb{Z}$, defina $g : \mathbb{Z}*\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$. Como $\ker(g) \leq \mathbb{Z}*\mathbb{Z}$, $\ker(g)$ é livre. Como g é sobrejetiva, $Im(g) = \mathbb{Z} \times \mathbb{Z}$. Pelo Teorema do Isomorfismo, tem-se que $\mathbb{Z} * \mathbb{Z}/\ker(g) \simeq \mathbb{Z} \times \mathbb{Z}$. Mas $\mathbb{Z} \times \mathbb{Z}$ é solúvel. Se $\ker(g)$ fosse abeliano, então seria solúvel. Isso implicaria na solubilidade de $\mathbb{Z} * \mathbb{Z}$. Contradizendo o resultado 2.1.24.

Por fim, suponha que apenas um dos dois, Z_i ou Z_j é isomorfo a $\mathbb{Z}$. Então, existe um grupo cíclico $A \neq \mathbb{Z}$ tal que $Z_i * Z_j = \mathbb{Z} * A$. Defina $h : \mathbb{Z} * A \to \mathbb{Z} \times A$ a aplicação tal que $h|_{\mathbb{Z}} = id_{\mathbb{Z}}$ e $h|_A = id_A$. Queremos encontrar um subgrupo livre não abeliano de $\ker(h)$. O produto livre $\mathbb{Z} * A$ possui subgrupo livre H de posto 2, pelo Lema 2.3.13. Seja ν a restrição $h|_H : H \to \mathbb{Z} \times A$. Como H é livre e $\ker\nu \lhd H$, $\ker\nu$ é livre. Pelo Teorema de Schreier, tem-se que $d(\ker\nu) \geq 2$.

Caso 2. Suponha que Γ^C possua uma componente conexa com pelo menos três elementos. Tome $i, j, k \in \Gamma^0$ tais que $\{i, k\}, \{j, k\} \in (\Gamma^1)^C$. Se algum dos grupos não for isomorfo a C_2, voltamos ao caso anterior. Podemos então assumir que Z_i,Z_j e Z_k são todos C_2.

Se $\{i, j\} \in (\Gamma^1)^C$, pelo Lema 3.3.15, existe um mergulho de $C_2 * C_2 * C_2$ em P, que é levado em $C_2 \times C_2 \times C_2$ em $\bigoplus_{i\in\Gamma^0} W_i$, por φ. Agora, podemos aplicar o Lema 2.5.22 com $A = C_2 * C_2$ e $B = C_2$. Tem-se que $\ker(\alpha)$, onde α é como no lema, possui subgrupo livre não abeliano. Como $\ker(\alpha) \lhd A * B = C_2 * C_2 * C_2$, segue que $C_2 * C_2 * C_2$ tem subgrupo livre não abeliano.

O caso $\{i, j\} \notin (\Gamma^1)^C$ é análogo: pelo Lema 3.3.15, existe um mergulho de $(C_2 \times C_2) * C_2$ em P que é levado $C_2 \times C_2 \times C_2$. Novamente, aplicamos o Lema 2.5.22 para $A = C_2 \times C_2$ e $B = C_2$, obtendo que $(C_2 \times C_2) * C_2$ tem subgrupo livre não abeliano.

Agora, como $C_2 * C_2 * C_2$ e $(C_2 \times C_2) * C_2$ têm subgrupos livres não abelianos, como no caso 1., obtemos que os respectivos grupos derivados também têm e, portanto, Q tem um subgrupo livre não abeliano.

$\square$

Quando Γ é um grafo totalmente desconexo, Γ^C é um grafo completo. Com isso, as únicas maneiras desse grafo satisfazer a condição **ii.** do lema anterior são: Γ^0 ter no máximo dois elementos e, no caso de Γ^0 ter exatamente dois elementos i e j, deve-se ter que W_i e W_j são isomorfos a C_2. Consequentemente, para um grafo Γ totalmente desconexo, o Lema 3.3.17 se resume a

Lema 3.3.18. Sejam Γ um grafo totalmente desconexo e $(W_i)_{i\in\Gamma^0}$ uma família de grupos não triviais. Denote por Q o núcleo do homomorfismo natural do produto livre entre todos os W_i na soma direta dos mesmos. Se Γ^0 tem pelo menos 2 elementos ou, no caso particular em que todos os W_i são isomorfos a C_2, Γ^0 tem pelo menos 3 elementos, então Q tem um subgrupo livre não abeliano.

Uma família ascendente de grafos em X é uma família de grafos $\{\Gamma_k\}$ na qual cada Γ_k tem X como conjunto de vértices e tal que

$$\Gamma_1 \subset \Gamma_2 \subset \ldots \subset \Gamma_k \subset \ldots,$$

ou seja, tal que $\Gamma_k = (X, \Gamma_k^1)$, com $\Gamma_k^1 \subset \Gamma_{k+1}^1, \forall k \in \mathbb{N}$.

Lema 3.3.19. Sejam X um conjunto e $\{\Gamma_n\}$ uma família ascendente de grafos em X. Suponha que X possa ser escrito como uma união disjunta $X = \bigcup_{i=1}^k X_i$ tal que, para cada $n \in \mathbb{N}$, o grafo complementar Γ_n^C pode ser escrito como uma união disjunta de subgrafos de grau constante e finito $\Lambda_{n,i} = (X_i, \Lambda_{n,i}^1)$. Então, a sequência (Γ_n) se torna constante, eventualmente.

Demonstração. Denote por $d_{n,i}$ o grau de $\Lambda_{n,i}$. A sequência $(\sum_{i=1}^k d_{n,i})_{n\in\mathbb{N}}$ decresce, pois a sequência (Γ_n^C) decresce. Assim, $(\sum_{i=1}^k d_{n,i})_{n\in\mathbb{N}}$ eventualmente se torna constante. Consequentemente, todas as sequências $(d_{n,i})_{n\in\mathbb{N}}$ se tornam constantes eventualmente.

Se $d_{n,i} = d_{n+1,i}$, então $\Lambda_{n,i}$ e $\Lambda_{n+1,i}$ são grafos com mesmos vértices e que têm graus constantes e iguais a $d_{n,i}$, logo, tais grafos coincidem. Assim, se $(d_{n,i})$ se torna constante no m_i-ésimo termo, tome $M = max\{m_1, \ldots, m_k\}$. Tem-se que $\Lambda_{m,i} = \Lambda_{m+1,i}, \forall m \geq M$ e $\forall i = 1, \ldots, k$. Logo, $\Gamma_m^C = \bigcup_{i=1}^k \Lambda_{m,i} = \bigcup_{i=1}^k \Lambda_{m+1,i} = \Gamma_{m+1}^C, \forall i$ e $\forall m \geq M$. Segue que (Γ_n^C) se torna constante eventualmente e, portanto, (Γ_n) também se torna constante eventualmente. $\square$

Suponha agora que todos os W_i são iguais ao grupo não trivial W. Seja ainda G um grupo que age no grafo $\Gamma = (\Gamma^0, \Gamma^1)$, ou seja, G age em Γ^0, preservando Γ^1. Nesse caso, o produto semidireto $W^{\langle\Gamma\rangle} \rtimes G$ está bem definido. Devemos então descrever o que é uma estrutura preservada por G. Seja X um conjunto. Definiremos o *conjunto de arestas* em X como sendo um subconjunto simétrico de $X \times X$ que não intersecta a sua diagonal $\{(x, x) : x \in X\}$. Veja que um conjunto de arestas A define uma estrutura de grafo a X, a saber (X, A).

Se X é um G-conjunto, então X pode ser decomposto em uma união disjunta de G-órbitas $X = \bigcup_{i\in I} X_i$, onde $X_i = G/H_i$, onde I é um representante de G-órbitas em X e H_i o estabilizador G_i.

Lema 3.3.20. Com a notação acima, seja E é um conjunto de arestas em X G-invariante (ou seja, $G \cdot E \subset E$). Defina $B_{ij} = B_{ij}(E) = \{g \in G : (i, g \cdot j) \in E\}$, para cada $(i, j) \in I^2$. Então, vale que

i. $B_{ij}^{-1} = B_{ji},\ \forall i, j \in I$

ii. $H_i B_{ij} = B_{ij}$

iii. $H_i \cap B_{ii} = \varnothing$

Reciprocamente, se $(V_{ij})_{i,j\in I}$ é uma família de subconjuntos de G satisfazendo **i.**, **ii.** e **iii.**, então existe um único conjunto de arestas G-invariante E satisfazendo $V_{ij} = B_{ij}(E)$, para todos $i, j \in I$.

Demonstração. Suponha primeiramente que E é um conjunto de arestas G-invariante.

i.

$$\begin{aligned}
B_{ij}^{-1} &= \{g \in G :\ g^{-1} \in B_{ij}\} \\
&= \{g \in G :\ (i, g^{-1} \cdot j) \in E\} \\
&= \{g \in G :\ g \cdot (i, g^{-1} \cdot j) \in E\} && \text{(pois } E \text{ é } G\text{-invariante)} \\
&= \{g \in G :\ (g \cdot i, j) \in E\} \\
&= \{g \in G :\ (j, g \cdot i) \in E\} && \text{(pois } E \text{ é simétrico)} \\
&= B_{ji}
\end{aligned}$$

ii. Seja $hg \in H_i B_{ij}$. Mostremos que $hg \in B_{ij}$. Tem-se que $(i, hg \cdot j) = h \cdot (h^{-1} \cdot i, g \cdot j)$. Como $H_i = G_i$ e $h^{-1} \in H_i$, tem-se que $h^{-1} \cdot i = i$. Assim, $(i, hg \cdot j) = h \cdot (i, g \cdot j)$. Como $g \in B_{ij}$, vale que $(i, g \cdot j) \in E$. Além disso, como $h \in H_i \subset G$ e E é G-invariante, vale que $h \cdot (i, g \cdot j) \in E$. Ou seja, $(i, hg \cdot j) \in E$. Segue que $hg \in B_{ij}$. A inclusão $B_{ij} \subset H_i B_{ij}$ segue do fato de $1 \in H_i$, pois $1 \cdot i = i$. Com isso, tem-se que, se $g \in B_{ij}$, então $g = 1g \in H_i B_{ij}$.

iii. Suponha que $h \in H_i \cap B_{ii}$. Pela definição de H_i, tem-se que $h \cdot i = i$ e, pela definição de $H_i B_{ii}$, tem-se que $(i, h \cdot i) \in E$. Segue que $(i, i) \in E$, contradizendo o fato de E ser conjunto de arestas.

Agora, para a recíproca, defina E da seguinte maneira: para $i, j \in I$, $(g \cdot i, \bar{g} \cdot j) \in E$ se, e somente se, $g^{-1}\bar{g} \in V_{ij}$. Mostremos que E é G-invariante. Seja $(x_m, x_n) \in E$. Como $X = \bigcup_{i\in I} X_i$, onde X_i é G-órbita em X, exitem $g_1, g_2 \in G$ e $i, j \in I$ tais que $g_1 \cdot i = x_m$ e $g_2 \cdot j = x_n$. Ou seja, $(g_1 \cdot i, g_2 \cdot j) = (x_m, x_n) \in E$. Pela escolha de E, $g_1^{-1} g_2 \in V_{ij}$.

Dado $g \in G$, devemos mostrar que $g \cdot (x_m, x_n) \in E$. De fato, $g \cdot (x_m, x_n) = g \cdot (g_1 \cdot i, g_2 \cdot j) = (gg_1 \cdot i, gg_2 \cdot j)$. Como $(gg_1)^{-1}(gg_2) = g_1^{-1} g^{-1} g g_2 = g_1^{-1} g_2 \in V_{ij}$, o resultado segue.

Além disso,

$$\begin{aligned}
B_{ij}(E) &= \{g \in G :\ (i, g \cdot j) \in E\} \\
&= \{g \in G :\ (1 \cdot i, g \cdot j) \in E\} \\
&= \{g \in G :\ g = 1^{-1} g \in V_{ij}\} && \text{(Pela definição de } E\text{)} \\
&= V_{ij}
\end{aligned}$$

Para a unicidade, seja A um conjunto de arestas em X que seja G-invariante e tal que $B_{ij}(A) = V_{ij},\ \forall i, j \in I$. Seja $(x_a, x_b) \in A$. Podemos escrever tal elemento na forma $(x_a, x_b) = (g_1 \cdot i, g_2 \cdot j)$. Como A é G-invariante, tem-se que $(i, g_1^{-1}g_2 \cdot j) = g_1^{-1} \cdot (g_1 \cdot i, g_2 \cdot j) \in A$. Pela definição de $B_{ij}(A)$, segue que $g_1^{-1}g_2 \in B_{ij}(A) = V_{ij} = B_{ij}(E)$. Consequentemente, $(i, g_1^{-1}g_2 \cdot j) \in E$. Como E também é G-invariante, $(x_a, x_b) = g_1 \cdot (i, g_1^{-1}g_2 \cdot j) \in E$. Segue que $A \subset E$.

Por outro lado, seja $(g_1 \cdot i, g_2 \cdot j)$ um elemento arbitrário de E. Pela escolha de E, tem-se que $g_1^{-1}g_2 \in B_{ij}(E)$, logo, $g_1^{-1}g_2 \in B_{ij}(A)$. Segue que $(i, g_1^{-1}g_2 \cdot j) \in A$ e, portanto, $(g_1 \cdot i, g_2 \cdot j) = g_1 \cdot (i, g_1^{-1}g_2 \cdot j) \in A$. □

Com as ferramentas acima obtidas, daremos inicio à demonstração da outra implicação do Teorema Principal.

Proposição 3.3.21. Sejam G e W grupos, com W não trivial, e X um G-conjunto não vazio tal que a ação diagonal de G em X^2 tem infinitas órbitas. Então, dado um epimorfismo $\rho : H \to W \wr_X G$, de um grupo finitamente apresentável H em $W \wr_X G$, tem-se que $\ker(\rho)$ possui subgrupo livre não abeliano.

Demonstração. Escreva X como a união disjunta $\bigcup_{i\in I} G/H_i$, onde cada H_i é um estabilizador de G em X. Por hipótese, existem infinitas órbitas de G em $X^2 = X \times X$. Existe então uma classe lateral dupla $H_k\backslash G/H_l$ infinita.

Se $k \neq l$, tome uma sequência estritamente crescente $(A_n)_{n\in\mathbb{N}}$ de subconjuntos de $H_k\backslash G/H_l$ tal que $\bigcup_{n\in\mathbb{N}} A_n = H_k\backslash G/H_l$. Defina então $V_{kl}^n = A_n$ e $V_{lk}^n = A_n^{-1}$, para cada $n \in \mathbb{N}$.

Se $k = l$, tome uma sequência estritamente crescente $(B_n)_{n\in\mathbb{N}}$ de subconjuntos de $(H_k\backslash G/H_k) \setminus \{H_k\}$ que são simétricos pela inversão, de modo que $\bigcup_{n\in\mathbb{N}} B_n = (H_k\backslash G/H_k) \setminus \{H_k\}$. Defina $V_{kk}^n = B_n$.

Em ambos os casos, dados $n \in \mathbb{N}$ e $i, j \in I$ tais que $\{i, j\} \neq \{k, l\}$, ponha

$$V_{ij}^n = \begin{cases} H_i\backslash G/H_j & , \text{se } i \neq j \\ (H_i\backslash G/H_i) \setminus \{H_i\} & , \text{se } i = j \end{cases}$$

Pelas escolhas de V_{ab}^n, $a, b \in I$, tem-se que $(V_{ab}^n)^{-1} = V_{ba}^n$, para todos $a, b \in I$ e $n \in \mathbb{N}$. Além disso, se $k \neq l$, V_{kl}^n é um subconjunto de $H_k\backslash G/H_l$, logo, é da forma $H_k\backslash S/H_l$, onde S é um subconjunto de G. Consequentemente, $H_kV_{kl}^n = H_k(H_k\backslash S/H_l) = H_k\backslash S/H_l = V_{kl}^n$. Analogamente, se $k = l$, então V_{kk}^n é da forma $(H_k\backslash S/H_k) \setminus \{H_k\}$, onde $S \subset G$. Assim, $H_kV_{kk}^n = V_{kk}^n$. Vale ainda que, para $n \in \mathbb{N}$ e $i, j \in I$ tais que $\{i, j\} \neq \{k, l\}$,

$$H_iV_{ij}^n = H_i(H_i\backslash G/H_j) = H_i\backslash G/H_j, \text{ se } i \neq j \qquad H_iV_{ii}^n = H_i((H_i\backslash G/H_i) \setminus \{h_i\}) = V_{ii}^n, \text{ se } i \neq k, l$$

Tem-se também que $H_i \cap V_{ii}^n = H_i \cap ((H_i\backslash G/H_i) \setminus \{H_i\}) = \varnothing,\ \forall i \neq k, l$ e, se $k = l$, então $H_k \cap V_{kk}^n = H_k \cap ((H_k\backslash S/H_k) \setminus \{H_k\}) = \varnothing$. Pelo Lema 3.3.20, para cada $n \in \mathbb{N}$, existe um conjunto G-invariante de arestas E_n tal que $V_{ab}^n = B_{ab}(E_n), \forall a, b \in I$, com a notação do lema. Denote por X_n o grafo $X_n = (X, E_n)$.

Como $V_{kl} = B_{kl}(E_n) = \{g \in G :\ (k, g \cdot l) \in E_n\}$ e $V_{kl}^n \subsetneq V_{kl}^{n+1}$, existe $g \in V_{kl}^{n+1}\backslash V_{kl}^n$, ou seja, $(k, g \cdot l) \in E_{n+1}\backslash E_n$. Logo, $E_n \subsetneq E_{n+1}$. Isso nos diz que (E_n) é uma sequência estritamente crescente. Além disso, a união de todos os V_{ij}^n, $i, j \in I$ e $n \in \mathbb{N}$ é $G - \bigcup_{i\in I} H_i$, de modo que $E = \bigcup_{n\in\mathbb{N}} E_n$ é o conjunto completo de arestas $X^2 - \{(x, x) :\ x \in X\}$

Escrevendo $W^{(X)} \rtimes G$ na forma $F_0/\langle S\rangle^{F_0}$, para cada $n \in \mathbb{N}$, existe $S_n \subset F_0$ finito tal que $W^{\langle X_n\rangle} \rtimes G = F_0/\langle S_n\rangle^{F_0}$. Como $X_n \subsetneq X_{n+1}, \forall n \in \mathbb{N}$, pela definição do produto grafo, $W^{\langle X_n\rangle} \supsetneq W^{\langle X_{n+1}\rangle}$. Assim, as projeções canônicas $W^{\langle X_n\rangle} \rtimes G \to W^{\langle X_{n+1}\rangle} \rtimes G$ são epimorfismos que não são isomorfismos. Segue que $\langle S_n\rangle^{F_0} \subsetneq \langle S_{n+1}\rangle^{F_0}, \forall n \in \mathbb{N}$, consequentemente, $\bigcup_{n\in\mathbb{N}} S_n = S$. [1]

Suponha que o núcleo de $\psi_n : W^{\langle X_n\rangle} \to W^{(X)}$ não possua subgrupo livre não abeliano. Pelo Lema 3.3.17, cada componente conexa do grafo complementar $X_n^C = (X, (\Gamma_n^1)^C)$ de X_n tem no máximo dois vértices, ou seja, os vértices de X_n^C têm grau no máximo 1. Denote por $X_{n,0}$ e $X_{n,1}$ os conjuntos dos vértices de X_n^C de grau 0 e 1, respectivamente. Tem-se que $X = X_{n,0} \cup X_{n,1}$ e $\Lambda_0 = (X_{n,0}, \varnothing)$, $\Lambda_1 = (X_{n,1}, (\Gamma_n^1)^C)$ são grafos disjuntos de grau constante. Segue do Lema 3.3.19 que (X_n) se torna constante a partir de algum índice $m \in \mathbb{N}$, uma contradição.

Seja $\rho : H \to W \wr_X G$ um epimorfismo, onde H é um grupo finitamente apresentável. Seja ainda $H = F/\langle R\rangle^F$ uma apresentação finita de H. Denote por π a projeção de F em H. Então, $\rho \circ \pi : F \to W^{(X)} \rtimes G$ é um epimorfismo. Queremos encontrar $\delta : F \to F_0$ tal que $\gamma \circ \delta = \rho \circ \pi$, onde γ é a projeção canônica entre F_0 e $F_0/\langle S\rangle^{F_0}$. Sejam X base do grupo livre F e $i : X \to F$ a inclusão. Podemos atribuir a cada $x_i \in X$ um $g_i\langle S\rangle^{F_0} \in W^{(X)} \rtimes G$ (faça $g_i = \rho \circ \pi \circ i(x_i)$).

$$\begin{tikzcd} W^{(X)} \rtimes G = F_0/\langle S\rangle^{F_0} & F \arrow[l, "\rho\circ\pi"'] \arrow[dl, "\delta"] \\ F_0 \arrow[u, "\gamma"] & \end{tikzcd}$$

Defina $f : X \to F_0$ atribuindo a cada elemento $x_i \in X$ um único elemento $f(x_i)$ de $\gamma^{-1}(g_i\langle S\rangle^{F_0})$. Pela propriedade universal do grupo livre, existe um único homomorfismo $\delta : F \to F_0$ tal que $\delta \circ i = f$. Agora, $\gamma \circ \delta(x_i) = g_i\langle S\rangle^{F_0} = \rho \circ \pi(x_i)$. Logo, δ é o mapa procurado.

Como R é conjunto de relações de H, $\pi(R)$ é trivial, de modo que $\rho \circ \pi(R)$ é também trivial. Isso implica em $\gamma \circ \delta(R) = \rho \circ \pi(R) = \{1\}$, ou seja, $\delta(R) \subset \gamma^{-1}(\{1\}) = \langle S\rangle^{F_0} = \bigcup_{n\in\mathbb{N}} \langle S_n\rangle^{F_0}$. Existe então $k \in \mathbb{N}$ tal que $\delta(R) \subset \langle S_k\rangle^{F_0}$ e δ induz o mapa $\rho_k : F/\langle R\rangle^F \to F_0/\langle S_k\rangle^{F_0}$ (ou seja, $\rho_k : H \to W^{\langle X_k\rangle} \rtimes G$), no qual $\psi_k \circ \rho_k = \rho$, onde $\psi_k : W^{\langle X_k\rangle} \rtimes G \to W^{(X)} \rtimes G$, definido acima. Como ρ fatora em ψ_k e vimos que $\ker(\psi_k)$ possui subgrupo livre não abeliano, segue que $\ker(\rho)$ também possui. $\square$

Corolário 3.3.22. Sejam G e W grupos, com W não trivial, e X um G-conjunto não vazio tal que a ação de G em X^2 tem infinitas órbitas. Então, $W \wr_X G$ não é finitamente apresentável.

Demonstração. Na demonstração da proposição anterior, vimos que, dado um epimorfismo $\rho : H \to W^{(X)} \rtimes G$ onde H é finitamente apresentável, existe um epimorfismo $\rho_k : H \to W^{\langle X_k\rangle}$ tal que $\rho = \psi_k \circ \rho_k$, onde ψ_k é a projeção canônica. Mostremos que ρ não pode ser isomorfismo, pois nesse caso $W^{(X)} \rtimes G$ não é isomorfo a nenhum grupo finitamente apresentável e, portanto, não pode ser finitamente apresentável.

[1] Vendo de outra forma, $W^{(X)} \rtimes G$ é o limite direto de $\{W^{\langle X_n\rangle} \rtimes G\}_{n\in\mathbb{N}}$ com mapas $W^{\langle X_n\rangle} \rtimes G \to W^{\langle X_{n+1}\rangle} \rtimes G$.

$$\begin{tikzcd}
H \arrow[r, "\rho"] \arrow[d, "\rho_k"'] & W^{(X)} \rtimes G \\
W^{\langle X_k \rangle} \rtimes G \arrow[ur, "\psi_k"'] &
\end{tikzcd}$$

Sabemos que ψ_k não é isomorfismo, pois $W^{\langle X_k \rangle} = F_0/\langle S_n \rangle^{F_0}$, onde $\langle S_n \rangle^{F_0} \subsetneq \langle S_{n+1} \rangle^{F_0}, \forall n \in \mathbb{N}$ e $W^{(X)} = F_0/\langle S \rangle^{F_0}$ é tal que $\langle S \rangle^{F_0} = \bigcup \langle S_n \rangle^{F_0}$, mas $\langle S \rangle^{F_0} \supsetneq \langle S_n \rangle^{F_0}, \forall n \in \mathbb{N}$. Assim, existem $a, b \in W^{\langle X_k \rangle} \rtimes G$ distintos tais que $\psi_k(a) = \psi_k(b)$. Como ρ_k é epimorfismo, existem $\tilde{a}, \tilde{b} \in H$ tais que $\rho_k(\tilde{a}) = a$ e $\rho_k(\tilde{b}) = b$. Como $a \neq b$, devemos ter que $\tilde{a} \neq \tilde{b}$. Segue que

$$\rho(\tilde{a}) = \psi_k(\rho_k(\tilde{a})) = \psi_k(a) = \psi_k(b) = \psi_k(\rho(\tilde{b})) = \rho(\tilde{b})$$

Assim, ρ é epimorfismo, mas não isomorfismo.

□

Proposição 3.3.23. Dados dois grupos G e $W \neq \{1\}$, onde G age sobre um conjunto não trivial X, se existe $x \in X$ tal que G_x não é finitamente gerado, então todo epimorfismo ρ de um grupo finitamente apresentável em $W \wr_X G$ é tal que $\ker(\rho)$ tem subgrupo livre não abeliano.

Demonstração. Seja $x_i \in X$ tal que $H_i = G_{x_i}$ não é finitamente gerado. Podemos tomar uma sequência estritamente crescente $(H_{i,n})_{n \in \mathbb{N}}$ de subgrupos de H_i tal que $\bigcup_{n \in \mathbb{N}} H_{i,n} = H_i$.

Defina o grafo X_n com conjunto de vértices $(\bigcup_{j \neq i} G/H_j) \cup G/H_{i,n}, \forall n \in \mathbb{N}$ com conjunto de arestas $\Gamma_n = \{\{x, y\} \in X_n^2 : \ x \neq y \text{ e } xH_i \neq yH_i, \text{ se } x, y \in G/H_{i,n}\}$. Por simplicidade, denotaremos o conjunto de vértices de X_n também por X_n e os subgrafos induzidos de X_n serão denotados pelos conjuntos de vértices dos mesmos. Seja $\psi_n : W^{\langle X_n \rangle} \to W^{(X)}$ a projeção canônica. Veja que ψ_n pode ser vista como a identidade em $W^{\langle X_n \setminus (G/H_{i,n}) \rangle}$ e a projeção $\beta_n : W^{\langle G/H_{i,n} \rangle} \to W^{(G/H_i)}$ em $W^{\langle G/H_{i,n} \rangle}$. Logo, $\ker(\varphi_n) = \ker(\beta_n)$.

Em $G/H_{i,n}$, X_n não possui arestas nos elementos de $H_i/H_{i,n}$, pois, dados $xH_{i,n}, yH_{i,n} \in H_i/H_{i,n}$, tem-se que $xH_i = yH_i$. Logo, $W^{\langle G/H_{i,n} \rangle} = W^{*H_i/H_{i,n}} \times W^{\langle (G/H_{i,n}) \setminus (H_i/H_{i,n}) \rangle}$. Assim, $\ker(\beta_n)$ contém o núcleo da aplicação natural $\zeta_n : W^{*H_i/H_{i,n}} \to W$.

Como $(H_{i,n})_{n \in \mathbb{N}}$ é estritamente crescente, $H_{i,n}$ tem índice infinito em H_i. Em particular, $|H_i/H_{i,n}| > 3$. Assim, $\ker(\zeta_n)$ possui subgrupo livre não abeliano, pelo Lema 3.3.18. Consequentemente, $\ker(\psi_n)$ possui um subgrupo livre não abeliano.

Tem-se que $\bigcup_{n \in \mathbb{N}} X_n = X$. [2]

Por um argumento análogo ao dado na demonstração da Proposição 3.3.21, dado um epimorfismo $\rho : H \to W \wr_X G$, no qual H é um grupo finitamente apresentável, tem-se que ρ fatora em $\rho_n : H \to W^{\langle X_n \rangle} \rtimes G$, para algum $n \in \mathbb{N}$. Logo, como $\ker \rho_n$ contém um subgrupo livre não abeliano, ρ também contém. □

Corolário 3.3.24. Dados dois grupos G e $W \neq \{1\}$, onde G age sobre um conjunto não trivial X, se existe $x \in X$ tal que G_x não é finitamente gerado, então $W \wr_X G$ não é finitamente apresentável.

Demonstração. Segue de um argumento inteiramente análogo ao do Corolário 3.3.22. □

[2] Nesse caso, podemos ver $W^{(X)} \rtimes G$ como o limite direto de $\{W^{\langle X_n \rangle} \rtimes G\}_{n \in \mathbb{N}}$ com mapas $W^{\langle X_n \rangle} \rtimes G \to W^{\langle X_{n+1} \rangle} \rtimes G$, as projeções canônicas.

Teorema 3.3.25. Sejam G e W grupos e X um G-conjunto não vazio. Se $W \wr_X G$ é finitamente apresentável, então G e W também o são. Além disso, se W é não trivial, a ação de G em X^2 tem finitas órbitas e a ação de G em X tem estabilizadores finitamente gerados.

Demonstração. Tem-se que G e W são finitamente gerados, pela Proposição 3.2.1. Pela mesma proposição, G tem finitas órbitas em X. Seja I um conjunto finito contendo exatamente um elemento de cada G-órbita em X. Então, $X = \bigcup_{i \in I} G \cdot i$. Uma vez que W é finitamente gerado, podemos tomar um subconjunto finito $L \subset W^I$ que gera $W^{(X)}$ como subgrupo normal de $W \wr_X G$.

Obtemos então que $G = (W \wr_X G)/W^{(X)} = (W^{(X)} \rtimes G)/W^{(X)} = (W \wr_X G)/\langle L \rangle^{W \wr_X G}$, ou seja, G é finitamente apresentável, pois $W \wr_X G$ é finitamente apresentável.

Agora, mostraremos que W é finitamente apresentável. Escreva $W \wr_X G = F_0/\langle R \rangle^{F_0}$, com F_0 finitamente gerado e R finito. Observe que $W^{(I)} = (W \wr_X G)/\langle G \rangle^{W \wr_X G}$. Como G é finitamente gerado, segue que $W^{(I)}$ é finitamente apresentável. Além disso, como I é finito, dado $i_0 \in I$, tem-se que $W_{i_0} = W^{(i_0)} \simeq W^{(I)}/W^{(I \setminus \{i_0\})}$, logo, $W^{(i_0)}$ é finitamente apresentável. Pela escolha de $W^{(i_0)}$, tem-se $W^{(i_0)} \simeq W$.

Além disso, para W não trivial, como X é não vazio, se a ação de G em $X \times X$ tivesse infinitas órbitas, o corolário 3.3.22 implicaria no fato de $W \wr_X G$ ser não finitamente apresentável, uma contradição.

Ainda para W não trivial, como X é não vazio, se existisse um estabilizador de G em X que não é finitamente gerado, o corolário 3.3.24 garantiria que $W \wr_x G$ não fosse finitamente apresentável.

$\square$

Capítulo 4

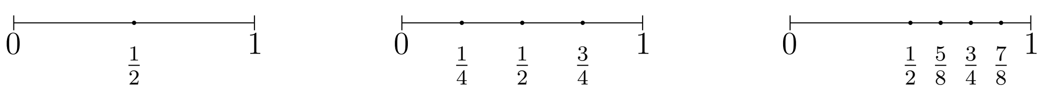
Aplicação

Mostraremos nesse capítulo uma aplicação do Teorema 3.3.5. Usaremos tal teorema para mostrar que, se W é um grupo não trivial finitamente apresentável, então $W \wr_I F$ é finitamente apresentável, onde F é o grupo de Thompson e I é um F-conjunto que será definido posteriormente.

4.1 O Grupo de Thompson F

Nesta seção, veremos definições e propriedades básicas do Grupo de Thompson F. Para uma leitura mais aprofundada do tema, veja [6] e [1], onde se situam muitos dos resultados aqui apresentados.

Uma subdivisão do intervalo real $[0,1]$ é dita uma *subdivisão diádica* se é obtida ao dividir intervalos sempre pela metade. Veja abaixo alguns exemplos de tal subdivisão.



Os intervalos de uma subdivisão diádica são da forma $[\frac{p}{2^q}, \frac{p+1}{2^q}]$, $p, q \in \mathbb{N}$. Denominamos um intervalo desse tipo por *intervalo diádico canônico*. Um número racional da forma $\frac{p}{2^q}$ com $p \in \mathbb{Z}$ e $q \in \mathbb{N}$ é dito um *racional diádico*.

Denote por F o conjunto de todos os homeomorfismos lineares por partes $f : [0,1] \to [0,1]$ que fixam 0 e 1 e que são diferenciáveis, exceto por um número finito de racionais diádicos de $[0,1]$, e tais que a derivada em cada intervalo diferenciável é uma potência de 2.

Como as derivadas dos elementos de F são positivas, os elementos de F são funções crescentes.

Vejamos uma forma alternativa de caracterizar os elementos do conjunto F: Sejam $f \in F \backslash \{id\}$. e $0 = a_0 < a_1 < \ldots < a_r = 1$ os pontos onde f não é diferenciável. Como $f(0) = 0$ e f é linear no intervalo (a_0, a_1), tem-se que $f(x) = m_0 x$, para $a_0 \leq x \leq a_1$. Além disso, $m_0 = f'(x)$ é uma potência de 2, logo, $f(a_1) = m_0 a_1$ é um racional diádico. De fato, sejam $m_0 = 2^k$ e $a_1 = \frac{m}{2^l}$. Se $l \leq k$, $m_0 a_1 = m2^{k-l} \geq 1$, uma contradição. Logo, $l > k$ e $m_0 a_1 = \frac{m}{2^{l-k}}$. Em $[a_1, a_2]$, f é da forma $f(x) = m_1 x + n_1$, onde m_1 é alguma potência de 2. Como $m_0 a_1 = f(a_1)$ é um racional diádico e, como f é contínua, $m_0 a_1 = m_1 a_1 + n_1$. Assim, $n_1 = (m_0 - m_1) a_1$ é um racional diádico.

Indutivamente, $f(x) = m_i x + n_i$, $a_i \leq x \leq a_{i+1}$, para cada $i = 0, 1, \ldots, r-1$, onde m_i é potência de 2 e n_i é um racional diádico.

Reciprocamente, se $f : [0,1] \to [0,1]$ é um homeomorfismo linear por partes que fixa 0 e 1 e tal que $f(x) = m_i x + n_i$, $a_i \leq x \leq a_{i+1}$, para $i = 0, 1, \ldots, r-1$, onde m_i são potências de 2 e n_i são racionais diádicos, então todas as derivadas de f são potências de 2 onde existem e f não é diferenciável justamente nos racionais diádicos $a_0, \ldots, a_r$.

Veja que, se $f \in F$, pelo que foi mostrado, f leva racional diádico em racional diádico, pois a soma de racionais diádicos é ainda um racional diádico.

Proposição 4.1.1. F é um grupo com a composição de funções.

Demonstração. Dados $f, g \in F$, tem-se que $f \circ g : [0,1] \to [0,1]$ é um homeomorfismo linear por partes que fixa 0 e 1. Como f e g são deriváveis exceto por um número finito de pontos racionais diádicos, o mesmo pode ser dito de $f \circ g$. Além disso, como as derivadas de f e de g são potências de 2 e f e g são lineares onde são diferenciáveis, as derivadas de $f \circ g$ são potências de 2. Consequentemente, $f \circ g \in F$.

A identidade $id : [0,1] \to [0,1]$ é o elemento neutro de F.

Se $f \in F$, então existe $f^{-1} : [0,1] \to [0,1]$ e esse é um homeomorfismo linear por partes, pois, se $0 = a_0 < \ldots < a_r = 1$ são os pontos onde f não é diferenciável e $f(x) = m_i x + n_i$, $a_i \leq x \leq a_{i+1}$, para $i = 0, \ldots, r-1$, então como $m_i > 0$, $f^{-1}(x) = \frac{1}{m_i}x - \frac{n_i}{m_i}$, $f(a_i) \leq x \leq f(a_{i+1})$. Cada m_i é da forma 2^{k_i}, logo, as derivadas de f^{-1}, onde existem, são da forma 2^{-k_i}. Além disso, f^{-1} não é derivável nos pontos $0 = f(a_0) < f(a_1) < \ldots < f(a_r) = 1$. Segue que $f^{-1} \in F$. $\square$

Definição 4.1.2. O Grupo F é chamado de *grupo de Thompson*.

Por simplicidade, podemos escrever apenas fg para denotar $f \circ g$.

Exemplo 4.1.3. Os homeomorfismos

$$X_0(x) = \begin{cases} \frac{x}{2}, & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{4}, & \frac{1}{2} \leq x \leq \frac{3}{4} \\ 2x - 1, & \frac{3}{4} \leq x \leq 1 \end{cases} \qquad X_1(x) = \begin{cases} x, & 0 \leq x \leq \frac{1}{2} \\ \frac{x}{2} + \frac{1}{4}, & \frac{1}{2} \leq x \leq \frac{3}{4} \\ x - \frac{1}{8}, & \frac{3}{4} \leq x \leq \frac{7}{8} \\ 2x - 1, & \frac{7}{8} \leq x \leq 1 \end{cases}$$

são exemplos de elementos de F.

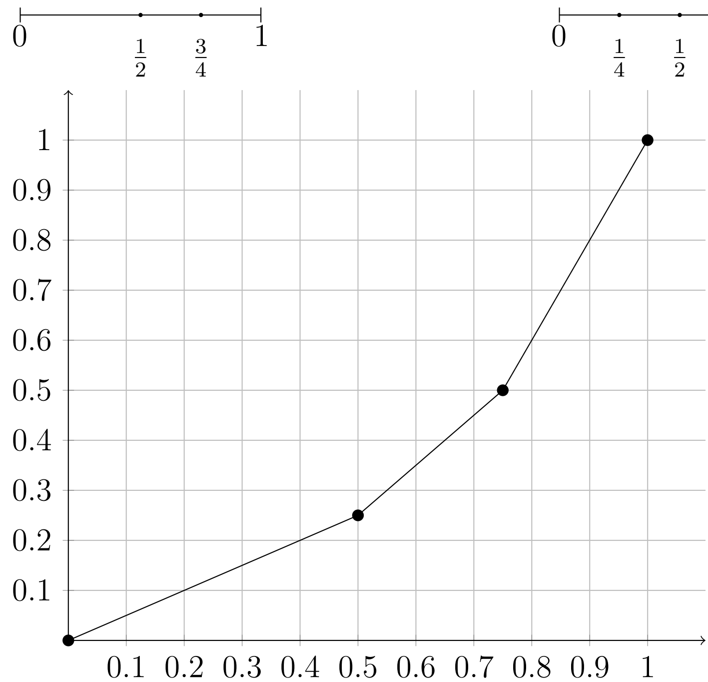
Proposição 4.1.4. O Grupo de Thompson é livre de torção.

Demonstração. Dado $f \in F \backslash \{id\}$, como $[0,1]$ é compacto, podemos tomar $x_0 = \inf\{t \in [0,1] : f(t) \neq t\}$. Tem-se que $f(x_0) = x_0$ e x_0 é um ponto onde f não é diferenciável. A derivada à direita de f em x_0 é $f'_+(x_0) = 2^m$, para algum m inteiro não nulo.

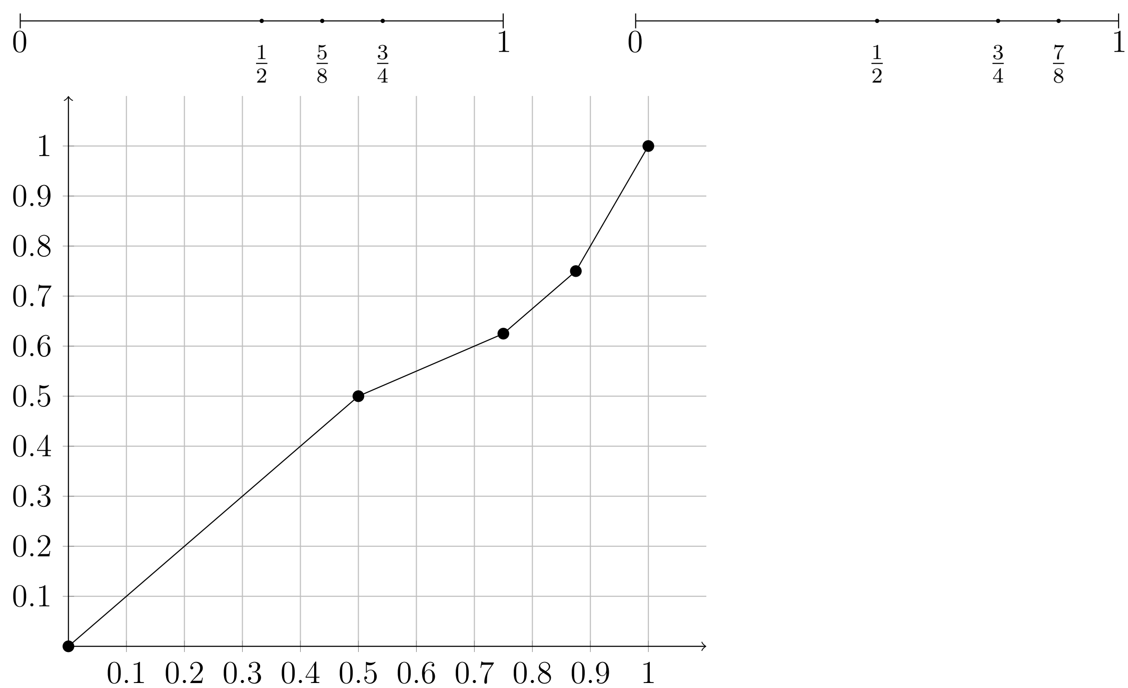
Pela regra da cadeia, $(f^2)'_+(x_0) = f'_+(f(x_0))f'_+(x_0) = f'_+(x_0)f'_+(x_0) = 2^{2m}$. Se $(f^{n-1})'_+(x_0) = 2^{(n-1)m}$, então $(f^n)'_+(x_0) = (f^{n-1})'_+(f(x_0))f'_+(x_0) = 2^{nm}$. Assim, $f^n \neq id$, $\forall n \in \mathbb{N}$. $\square$

Dadas duas subdivisões diádicas $\mathcal{D}, \mathcal{E}$ com o mesmo número de cortes, podemos encontrar um homeomorfismo linear por partes $f : [0,1] \to [0,1]$ que leva cada intervalo de $\mathcal{D}$ no seu respectivo intervalo em $\mathcal{E}$.

Exemplo 4.1.5. A subdivisão diádica à direita é levada na subdivisão diádica à esquerda pela aplicação esboçada na figura abaixo, tal aplicação é a aplicação X_0.



A primeira subdivisão diádica abaixo é levada na segunda pelo homeomorfismo X_1.



Veja que os homeomorfismo obtidos dessa maneira são elementos de F.

Proposição 4.1.6. Para cada racional diádico i, existe $f \in F$ tal que $f(\frac{1}{2}) = i$.

Demonstração. Por definição, existem $a, b \in \mathbb{N}$ tais que $i = \frac{a}{2^b}$. Se $i = \frac{1}{2}$, basta tomar a identidade. Suponha que $i < \frac{1}{2}$. Considere então a seguinte subdivisão de $[0, i]$:

$$\left[0, \frac{1}{2^b}\right], \left[\frac{1}{2^b}, \frac{2}{2^b}\right], \ldots, \left[\frac{a-1}{2^b}, \frac{a}{2^b}\right]$$

Tal divisão parte $[0, i]$ em a partes. Denote-a por $\mathcal{E}_1$. Divida então $[0, \frac{1}{2}]$ em a partes da seguinte forma:

$$\left[0, \frac{1}{2^a}\right], \left[\frac{1}{2^a}, \frac{1}{2^{a-1}}\right], \ldots, \left[\frac{1}{2^2}, \frac{1}{2}\right].$$

Denote essa subdivisão por $\mathcal{D}_1$.

Considere a subdivisão $\mathcal{E}_2$ de $\left[\frac{a}{2^b}, 1\right]$ dada por

$$\left[\frac{a}{2^b}, \frac{a+1}{2^b}\right], \left[\frac{a+1}{2^b}, \frac{a+2}{2^b}\right], \ldots, \left[\frac{a + (2^b - a - 1)}{2^b}, 1\right].$$

Veja que $\mathcal{E}_2$ divide $\left[\frac{a}{2^b}, 1\right]$ em $2^b - a$ partes. Façamos então uma subdivisão $\mathcal{D}_2$ de $\left[\frac{1}{2}, 1\right]$ em $2^b - a = k$ partes:

$$\left[\frac{1}{2}, \frac{3}{4}\right], \left[\frac{3}{4}, \frac{7}{8}\right], \ldots, \left[\frac{2^{k+1} - 1}{2^{k+1}}, 1\right].$$

Sejam $\mathcal{D}$ e $\mathcal{E}$ as subdivisões diádicas formadas pelos intervalos de $\mathcal{D}_1, \mathcal{D}_2$ e $\mathcal{E}_1, \mathcal{E}_2$, respectivamente. Então, $\mathcal{D}$ e $\mathcal{E}$ têm o mesmo número de cortes e $\frac{1}{2}$ e $\frac{a}{2^b} = i$ são extremos superiores do a-ésimo intervalo de suas respectivas subdivisões diádicas. Assim, o homeomorfismo $f : [0,1] \to [0,1]$ que leva $\mathcal{D}$ em $\mathcal{E}$ é tal que $f(\frac{1}{2}) = i$.

O caso $i > \frac{1}{2}$ é análogo. $\square$

Corolário 4.1.7. Dados dois racionais diádicos i_1 e i_2, existe $f \in F$ tal que $f(i_1) = i_2$.

Demonstração. Existem $g, h \in F$ tais que $h(\frac{1}{2}) = i_1$ e $g(\frac{1}{2}) = i_2$. Tome $f = g \circ h^{-1}$. $\square$

Dados racionais diádicos i_1, i_2 tais que $i_1 < i_2$, pode-se mostrar que existe $f \in F$ tal que $f(\frac{1}{2}) = i_1$ e $f(\frac{3}{4}) = i_2$. A demonstração segue a ideia da Proposição 4.1.6. Como consequência, se $i_1, i_2, \bar{i}_1, \bar{i}_2$ são racionais diádicos tais que $i_1 < i_2$ e $\bar{i}_1 < \bar{i}_2$, existe $f \in F$ tal que $f(i_1) = \bar{i}_1$ e $f(i_2) = \bar{i}_2$.

Em [6], foi mostrado que F tem apresentação

$$F = \langle X_0, X_1 | [X_0 X_1^{-1}, X_0^{-1} X_1 X_0], [X_0 X_1^{-1}, X_0^{-2} X_1 X_0^2] \rangle$$

na qual $X_0, X_1 \in F$ são os homeomorfismos definidos no Exemplo 4.1.3. Tem-se então que F é finitamente apresentável.

4.2 Aplicação

Vimos no Teorema 3.3.5 que, a fim de que $W \wr_X G$ seja finitamente apresentável, é suficiente que G e W sejam finitamente apresentáveis, que a ação de G em X tenha estabilizadores finitamente gerados e que o número de órbitas de G em $X \times X$ seja finito. Mostraremos que a ação de F no conjunto I dos racionais diádicos de $(0,1)$ satisfaz as duas últimas condições. Desse modo, $W \wr_I F$ é finitamente apresentável, sempre que W for finitamente apresentável.

Considere a ação natural do grupo de Thompson F em I. O estabilizador $F_{\frac{1}{2}} = \{f \in F : f(\frac{1}{2}) = \frac{1}{2}\}$ é tal que, para cada $f \in F$, as restrições $f|_{[0,\frac{1}{2}]} : [0,\frac{1}{2}] \to [0,\frac{1}{2}]$ e $f|_{[\frac{1}{2},1]} : [\frac{1}{2},1] \to [\frac{1}{2},1]$ são homeomorfismos lineares por partes que fixam $0, \frac{1}{2}$ e $\frac{1}{2}, 1$, respectivamente. Além disso, ambas as restrições são diferenciáveis, exceto nos pontos onde f não é diferenciável, respeitando-se o domínio de cada uma, e onde existe derivada em cada uma dessas restrições, tal derivada é uma potência de 2. Como consequência, $F_{[0,\frac{1}{2}]} = \{f|_{[0,\frac{1}{2}]} : f \in F_{\frac{1}{2}}\}$ e $F_{[\frac{1}{2},1]} = \{f|_{[\frac{1}{2},1]} : f \in F_{\frac{1}{2}}\}$ são isomorfos a F, pois $[0,\frac{1}{2}]$ e $[\frac{1}{2},1]$ são homeomorfos a $[0,1]$.

Com isso, podemos mostrar o seguinte resultado.

Proposição 4.2.1. $F_{\frac{1}{2}}$ é isomorfo a $F \times F$.

Demonstração. Defina $\alpha : F_{\frac{1}{2}} \to F_{[0,\frac{1}{2}]} \times F_{[\frac{1}{2},1]}$ por $\alpha(f) = (f_{[0,\frac{1}{2}]}, f|_{[\frac{1}{2},1]})$.

Pela sua escolha, α é uma aplicação injetiva. Veja que, se $f_1 \in F_{[0,\frac{1}{2}]}$ e $f_2 \in F_{[\frac{1}{2},1]}$ então

$$f(x) = \begin{cases} f_1(x), & 0 \leq x \leq \frac{1}{2} \\ f_2(x), & \frac{1}{2} \leq x \leq 1 \end{cases}$$

é um elemento de $F_{\frac{1}{2}}$ tal que $\alpha(f) = (f_1, f_2)$. Segue que α é bijeção.

Dados $f, g \in F_{\frac{1}{2}}$, tem-se que

$$\begin{aligned} \alpha(f \circ g) =& ((f \circ g)|_{[0,\frac{1}{2}]}, (f \circ g)|_{[\frac{1}{2},1]}) \\ =& (f|_{[0,\frac{1}{2}]} \circ g|_{[0,\frac{1}{2}]}, f|_{[\frac{1}{2},1]} \circ g|_{[\frac{1}{2},1]}) \\ =& (f|_{[0,\frac{1}{2}]}, f|_{[\frac{1}{2},1]}) \circ (g|_{[0,\frac{1}{2}]}, g|_{[\frac{1}{2},1]}) \\ =& \alpha(f) \circ \alpha(g) \end{aligned}$$

Assim, α é um isomorfismo. Portanto, $F_{\frac{1}{2}} \simeq F_{[0,\frac{1}{2}]} \times F_{[\frac{1}{2},1]} \simeq F \times F$. $\square$

Veja que não há nada de especial com $\frac{1}{2}$, poderíamos ter escolhido qualquer outro racional diádico. Segue que $F_i \simeq F \times F$, para todo $i \in I$. Como F é finitamente gerado, podemos concluir o seguinte resultado.

Corolário 4.2.2. Os estabilizadores de F são finitamente gerados.

Lema 4.2.3. $F/F_{\frac{1}{2}}$ pode ser identificado com I.

Demonstração. Defina $\beta : F/F_{\frac{1}{2}} \to I$ por $\beta(fF_{\frac{1}{2}}) = f(\frac{1}{2})$. Se $fF_{\frac{1}{2}} = gF_{\frac{1}{2}}$, então $f^{-1}g \in F_{\frac{1}{2}}$, ou seja, $f^{-1}g(\frac{1}{2}) = \frac{1}{2}$. Logo, $f(\frac{1}{2}) = g(\frac{1}{2})$. Segue que β está bem definida.

Se $\beta(fF_{\frac{1}{2}}) = \beta(gF_{\frac{1}{2}})$, então $f(\frac{1}{2}) = g(\frac{1}{2})$, logo, $f^{-1}g \in F_{\frac{1}{2}}$. Segue que $fF_{\frac{1}{2}} = gF_{\frac{1}{2}}$.

Dado $i_1 \in I$, existe $f \in F$ tal que $f(\frac{1}{2}) = i_1$. Logo, $\beta(fF_{\frac{1}{2}}) = i_1$.

Segue que β é bijeção entre $F/F_{\frac{1}{2}}$ e I. $\square$

Vimos no Corolário 4.1.7 que a ação de F sobre I é transitiva. Entretanto, a ação de F sobre $I \times I$ não é transitiva. Apesar disso, essa ação possui apenas 3 órbitas, a saber

$$J_0 = \operatorname{diag}(I \times I) = \{(i,i) : \ i \in I\}$$
$$J_1 = \{(i_1, i_2) \in I \times I : \ i_1 < i_2\}$$
$$J_2 = \{(i_1, i_2) \in I \times I : \ i_1 > i_2\}.$$

De fato, $I \times I$ é a união disjunta desses 3 conjuntos. Além disso, J_0 é isomorfo a I. Como a ação de F sobre I é transitiva, segue que a ação de F sobre J_0 também é transitiva. Dados $(i_1, i_2), (\bar{i}_1, \bar{i}_2) \in J_1$, existe $f \in F$ que leva i_1 em $\bar{i}_1$ e i_2 em $\bar{i}_2$. Assim, a ação de F em J_1 é transitiva. Analogamente, dados $(i_1, i_2), (\bar{i}_1, \bar{i}_2) \in J_2$, existe $f \in F$ tal que $f(i_2) = \bar{i}_2$ e $f(i_1) = \bar{i}_1$.

Juntando esse fato ao Corolário 4.2.2, tem-se que F e o F-conjunto I satisfazem as condições do Teorema 3.3.5. Portanto,vale o

Teorema 4.2.4. Se W é um grupo não trivial finitamente apresentável, então $W \wr_I F$ é finitamente apresentável.

Corolário 4.2.5. $\mathbb{Z} \wr_I F$ é finitamente apresentável.

Corolário 4.2.6. $D_\infty \wr_I F$ é finitamente apresentável.

Bibliografia

[1] J. M Belk. “Thompson’s Group F”. Tese de doutoramento. Cornell University, 2004.

[2] D. E. Cohen. *Combinatorial Group Theory: A Topological Approach*. Mathematical Society Student Texts-London, 1989.

[3] Y. de Cornulier. “Finitely Presented Wreath Products And Double Coset Decompositions”. Em: *Geom. Dedicata* 102 (2006), pp. 89–108.

[4] D. S. Dummit e R. M. Foote. *Abstract Algebra*. John Wiley & Sons Canada - Limited, 2004.

[5] E. Green. “Graph products”. Tese de doutoramento. University of Leeds, 1990.

[6] W. R. Parry J. W. Cannon W. J. Floyd. “Introductory notes on Richard Thompson’s groups”. Em: *Eisengn. Math. (2) no 3-4* 42 (1996), pp. 215–256.

[7] D. J. S. Robinson. *A Course In The Theory Of Groups*. Springer-Verlag, New York, 1995.

[8] J. J. Rotman. *An Introduction To The Theory Of Groups*. Springer-Verlag, Berlin-Heidelberg-New York, 1994.

[9] J. P. Serre. *Trees*. Springer-Verlag, Berlin– New York, 1977.

Índice