UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

**O grupo de homotopia de tranças puras no disco é
bi-ordenável**

Mirianne Andressa Silva Santos

Dissertação de Mestrado do Programa de Pós-Graduação em
Matemática (PPG-Mat)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Mirianne Andressa Silva Santos

O grupo de homotopia de tranças puras no disco é bi-ordenável

Dissertação apresentada ao Instituto de Ciências
Matemáticas e de Computação – ICMC-USP,
como parte dos requisitos para obtenção do título
de Mestra em Ciências – Matemática. *VERSÃO
REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. José Eduardo Prado Pires
de Campos

USP – São Carlos
Dezembro de 2018

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

S237g Santos, Mirianne Andressa Silva
O grupo de homotopia de tranças puras no disco é
bi-ordenável / Mirianne Andressa Silva Santos;
orientador José Eduardo Prado Pires de Campos. --
São Carlos, 2018.
103 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Matemática) -- Instituto de Ciências Matemáticas
e de Computação, Universidade de São Paulo, 2018.

1. grupo de tranças . 2. isotopia. 3. homotopia.
4. ordenação. I. Pires de Campos, José Eduardo
Prado, orient. II. Título.

Mirianne Andressa Silva Santos

The homotopy group of braids over a disc is bi-orderable

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. José Eduardo Prado Pires de Campos

USP – São Carlos
December 2018

Dedico este trabalho a todos que fizeram parte da minha caminhada até aqui.

AGRADECIMENTOS

Não cabem aqui todos os nomes daqueles que me ajudaram a percorrer esse caminho até essa etapa de minha carreira, mas devo agradecer a minha família e amigos que estiveram do meu lado sempre que precisei de um abraço, de uma palavra amiga, de algo que me fortalecesse. Agradeço em especial a Arianne que conviveu comigo neste período, ao David que com muita paciência me deu aulas e tirou minhas dúvidas sempre que precisei e principalmente ao meu namorado Marcos que me incentivou e me auxiliou da melhor maneira possível em todos os momentos de incertezas e medos.

Também gostaria de agradecer ao meu orientador que se dispôs a me orientar para eu obter esse título de grande significado para mim. Também ao Instituto de Ciências Matemáticas e de Computação (ICMC) pela infraestrutura de qualidade disponível e excelentes funcionários, que permitiu que tivesse um ambiente organizado e agradável para eu realizar meus estudos.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. E também com o apoio do Projeto Temático FAPESP nº 2016/24707 – 4.

*“O êxito da vida não se mede pelo caminho que você conquistou,
mas sim pelas dificuldades que você superou no caminho.”
(Abraham Lincoln)*

RESUMO

SANTOS, M. A. S. **O grupo de homotopia de tranças puras no disco é bi-ordenável.** 2018. 103 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

Em [Artin \(1925\)](#), Artin introduziu o estudo do grupo de tranças, o qual está intimamente relacionado ao estudo de nós e enlaçamentos. Em seu outro artigo “Theory of Braids” [Artin \(1947\)](#), ele questionou se as noções de isotopia e homotopia de tranças são as mesmas ou diferentes. Tal questão foi respondida muito mais tarde em [Goldsmith \(1974\)](#), onde a autora apresenta um exemplo de trança que é homotópica à trança trivial mas não é equivalente à trança trivial, caracterizando, além disso, o grupo de classes de homotopia de tranças puras no disco como um certo quociente do grupo de tranças puras original. Uma área de pesquisa mais recente nesta teoria é o estudo da ordenação destes grupos de tranças. Em [Habegger e Lin \(1990\)](#) os autores mostram que o grupo de classes de homotopia de tranças puras no disco é nilpotente e livre de torção. Resulta que ele é bi-ordenado. Em [Yurasovskaya \(2008\)](#) a autora fornece uma ordem explícita e calculável para este grupo. Neste trabalho discutiremos e apresentaremos os principais resultados neste contexto.

Palavras-chave: grupo de tranças, isotopia, homotopia, ordenação.

ABSTRACT

SANTOS, M. A. S. **The homotopy group of braids over a disc is bi-orderable.** 2018. 103 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

In [Artin \(1925\)](#), Artin introduced the study of braid groups, which is closely related to the study of knots and links. In his other paper “Theory of Braids” [Artin \(1947\)](#), he asked if the notions of isotopy and homotopy of braids are different or the same. Such question was answered much later in [Goldsmith \(1974\)](#), where the author presents an example of braid that is homotopic to the trivial braid, but it is not equivalent to the trivial braid, characterizing, beyond that, the group of homotopy classes of braids as a certain quotient of the original braid group. One more recent research area on this theory is the study of ordenation of braid groups. In [Habegger e Lin \(1990\)](#) the authors show that the homotopy group classes of pure braids is nilpotent and torsion free. It follows that it is bi-orderable. In [Yurasovskaya \(2008\)](#) the author provides one explicit and evaluable order for this group. In this work, we will discuss and present the main results involved on this context.

Keywords: braid groups, isotopy, homotopy, ordenation.

LISTA DE ILUSTRAÇÕES

Figura 1 – Uma trança geométrica com n cordas.	46
Figura 2 – Trança trivial.	46
Figura 3 – Movimento elementar.	47
Figura 4 – Representação geométrica de um cruzamento.	48
Figura 5 – Produto de duas tranças.	49
Figura 6 – A associatividade em $\mathcal{B}_n$	50
Figura 7 – O elemento neutro em $\mathcal{B}_n$	50
Figura 8 – A trança inversa em $\mathcal{B}_n$	50
Figura 9 – Uma partição de β	51
Figura 10 – Trança elementar σ_i	51
Figura 11 – Trança elementar inversa σ_i^{-1}	52
Figura 12 – A relação (2.5).	52
Figura 13 – A relação (2.6).	53
Figura 14 – Inclusão de $\mathbb{B}_m$ em $\mathbb{B}_n$ com $1 \leq m \leq n$	53
Figura 15 – Trança pura em (2.14).	56
Figura 16 – Trança β	58
Figura 17 – Tranças equivalentes.	59
Figura 18 – Exemplos de enlaçamentos de intervalos de 1 e 2 intervalos, respectivamente.	60
Figura 19 – Movimento elementar de homotopia.	61
Figura 20 – Enlaçamento de intervalos homotópico à trança σ_1^2	61
Figura 21 – Trança β que é homotopicamente trivial.	63
Figura 22 – Sequência de movimentos elementares de homotopia em β	63
Figura 23 – $\pi_1(\mathbb{D} \setminus \{P_1, \dots, P_n\})$	65
Figura 24 – Representação dos meridianos.	65
Figura 25 – Exemplo de nó.	66
Figura 26 – Um exemplo de nó em $\mathbb{R}^3$	67
Figura 27 – Representação das relações em (3.24).	68
Figura 28 – Cruzamento em que foi aplicada a homotopia.	68

SUMÁRIO

1	CONCEITOS PRELIMINARES	19
1.1	Introdução	19
1.2	Grupo residualmente nilpotente	20
1.3	Grupos livres	21
1.3.1	<i>Construção de um grupo livre</i>	23
1.3.2	<i>Apresentação de um grupo</i>	32
1.4	Produto semidireto	34
1.4.1	<i>Ação de grupos e produto semidireto</i>	35
1.4.2	<i>Produto semidireto e sequência exata</i>	36
1.5	Anéis, ideais e grupo das unidades	37
1.6	Ordenação de grupos	39
1.6.1	<i>Propriedades de grupos ordenáveis</i>	43
2	GRUPO DE TRANÇAS	45
2.1	Grupos de tranças	48
2.2	Apresentação do grupo de tranças	51
2.3	Apresentação do grupo das tranças puras	55
2.4	Isotopia de tranças	56
3	GRUPO DE HOMOTOPIA DE TRANÇAS PURAS NO DISCO	57
3.1	Representação de tranças por automorfismos de grupos livres	57
3.2	Homotopia de tranças	60
3.3	Homotopia e o grupo reduzido de um enlaçamento de intervalos	66
3.4	Uma apresentação de $\hat{\mathcal{PB}}_n(\mathbb{D})$	69
4	UMA ORDEM NO GRUPO DE TRANÇAS E NO GRUPO DE TRANÇAS PURAS	71
4.1	Uma ordem no grupo de tranças	71
4.1.1	<i>Algumas propriedades da ordem de Dehornoy</i>	73
4.2	Uma ordem no grupo de tranças puras	75
4.2.1	<i>Expansão de Magnus e uma ordem no grupo livre</i>	75
4.2.2	<i>Ordem no grupo de tranças puras</i>	79

5	O GRUPO DE HOMOTOPIA DE TRANÇAS PURAS NO DISCO É BI-ORDENÁVEL	85
5.1	Grupo livre reduzido	85
5.2	Expansão de Magnus e comutadores básicos com repetição	88
5.2.1	<i>Expansão de Magnus reduzida</i>	90
5.3	$\hat{\mathbb{P}\mathbb{B}}_n(\mathbb{D})$ é bi-ordenável	93
5.3.1	<i>Ordenando $RF(n)$</i>	93
5.3.2	<i>Automorfismos de $RF(n)$ e uma ordem em $\hat{\mathbb{P}\mathbb{B}}_n(\mathbb{D})$</i>	96
	REFERÊNCIAS	99
	ÍNDICE REMISSIVO	101

CONCEITOS PRELIMINARES

1.1 Introdução

A teoria de tranças tem sido um assunto bastante discutido nas últimas décadas não só por estabelecer uma relação intrínseca entre Topologia e Álgebra, mas também pela variedade de aplicações em áreas distintas da Matemática como em Biologia Molecular ([Francis \(2014\)](#)), Física Matemática ([Ricca \(2000\)](#)) e Computação Quântica ([Delaney, Rowell e Wang \(2016\)](#)).

Em [Artin \(1925\)](#), Artin introduziu o estudo do grupo de tranças, o qual está intimamente relacionado ao estudo de nós e enlaçamentos. Em seu outro trabalho, “Theory of Braids” ([Artin \(1947\)](#)), ele propôs a questão se as noções de isotopia e homotopia de tranças são coincidentes. Tal questão foi respondida bem mais tarde em [Goldsmith \(1974\)](#), onde a autora apresenta um exemplo de trança que é homotópica à trança trivial, mas que não é equivalente à trança trivial.

Graças a um resultado apresentado em [Habegger e Lin \(1990\)](#), o grupo de classes de homotopia de enlaçamentos de intervalos sobre o disco $\mathbb{D}$ pode ser considerado como o grupo de classes de homotopia de tranças puras no disco, visto que todo enlaçamento de intervalos é homotópico a uma trança pura.

Uma área de pesquisa recente é o estudo da ordenação de grupos de tranças. Em [Habegger e Lin \(1990\)](#) os autores mostram que o grupo de classes de homotopia de tranças puras é nilpotente e livre de torção. Disto resulta que tal grupo é bi-ordenável (veja [Dehornoy *et al.* \(2008, p. 264\)](#)). Em [Yurasovskaya \(2008\)](#) a autora fornece uma ordem explícita e calculável para este grupo, a qual será exibida no [Capítulo 5](#). Também discutimos e apresentamos os principais resultados que aparecem nesse contexto.

No presente [Capítulo 1](#) introduzimos alguns resultados preliminares para esse estudo bem como alguns conceitos da teoria combinatória de grupos que serão essenciais no decorrer do trabalho, tais como a definição de grupo livre e como estabelecer uma apresentação para um grupo. Além disso, recordamos algumas definições e propriedades de produto semidireto,

sequência exata de grupos, anel, ideal, ordem e algumas consequências relevantes de grupos que possuem uma ordenação.

No [Capítulo 2](#) introduzimos o conceito matemático de tranças e a apresentação do grupo de tranças em termos dos geradores de Artin. Além disso, caracterizamos o subgrupo das tranças puras que tem bastante relevância no estudo aqui desenvolvido. E também definimos a relação de equivalência denominada isotopia que divide o conjunto de todas as tranças em um grupo de classes de equivalência sob tal relação.

No início do [Capítulo 3](#) apresentamos um teorema interessante que relaciona o grupo de tranças no disco a um subgrupo do grupo dos automorfismos de um grupo livre. Posteriormente definimos uma nova relação de equivalência no conjunto de todas as tranças, denominada homotopia. E também mostramos que as duas relações, isotopia e homotopia, são de fato diferentes. Aqui o grupo de classes de homotopia de tranças puras é caracterizado como um certo grupo quociente do grupo de tranças puras definido no capítulo anterior.

Já no penúltimo capítulo abordamos a ordem de Dehornoy, a qual é uma ordem total invariante à esquerda no grupo de tranças com a relação de isotopia. Mostramos que o grupo de tranças puras é isomorfo ao produto semidireto de grupos livres, o qual pode ser munido de uma ordem bi-invariante. A construção de tal ordem bi-invariante é interessante pois utiliza a ordenação de Magnus, uma construção elegante de uma ordem para um grupo livre.

No último e mais importante capítulo apresentamos uma ordenação bi-invariante para o grupo de homotopia de tranças puras sobre o disco. A sua bi-ordenação é parecida com a ordem do grupo de tranças puras apresentada no [Capítulo 4](#), mas agora utilizamos o fato de que o grupo de homotopia de tranças puras é isomorfo ao produto semidireto de grupos livres reduzidos que são bi-ordenados com a ordem de Magnus reduzida construída a partir da expansão de Magnus reduzida.

1.2 Grupo residualmente nilpotente

As definições e resultados apresentados nesta seção podem ser encontrados em [Magnus, Karrass e Solitar \(1966\)](#).

Definição 1. Sejam x e y elementos de um grupo G . O *comutador de x e y* é o elemento $[x, y] = x^{-1}y^{-1}xy$.

Definição 2. Dados dois subconjuntos K e H de um grupo G , denotaremos por $[K, H]$ o subgrupo de G gerado pelo conjunto $\{[k, h]; k \in K, h \in H\}$.

Em particular, o grupo $G' = [G, G]$ chama-se *subgrupo comutador* ou *subgrupo derivado* de G .

Definição 3. A *série central inferior* de um grupo F é a sequência de subgrupos de F , $F = F_1 \supseteq F_2 \supseteq F_3 \supseteq F_4 \supseteq \dots$ definida recursivamente por $F_1 = F$ e $F_{i+1} = [F_i, F]$, para $i \geq 1$, isto é, o subgrupo gerado pelo conjunto $\{[k, h]; k \in F_i, h \in F\}$.

Observação 1. Os subgrupos F_i que compõem a série central inferior da definição anterior são normais a F e os grupos quocientes F_n/F_{n+1} são abelianos.

Definição 4. Seja F um grupo e considere (F_n) sua série central inferior. Se existir r inteiro tal que $F_r = 1$ então F é dito *nilpotente*.

Definição 5. Um grupo F é dito ser *residualmente nilpotente* se para todo $g \in F$, tal que $g \neq 1_F$, existe um grupo nilpotente Q_g e um homomorfismo $\phi_g: F \rightarrow Q_g$ com $\phi_g(g) \neq 1_{Q_g}$.

Proposição 1. Considere F um grupo residualmente nilpotente, então a Definição 5 é equivalente a cada uma das seguintes afirmações:

- (a) Para todo $g \neq 1_F$ em F existe um subgrupo N_g normal em F e tal que F/N_g é nilpotente e $g \notin N_g$;
- (b) A interseção de todos os subgrupos normais R de F tais que F/R é nilpotente é igual a 1_F , ou seja, $RN_F = \bigcap_{R \trianglelefteq F; F/R \text{ é nilpotente}} R = \{1_F\}$.

Demonstração. Primeiramente mostremos que a Definição 5 equivale à afirmação (a). Se $g \neq 1_F$, como F é residualmente nilpotente existe um grupo nilpotente Q_g e um homomorfismo $\phi_g: F \rightarrow Q$ tal que $\phi_g(g) \neq 1_F$. Tomando $N_g = \ker(\phi_g)$, então $\ker(\phi_g)$ é um subgrupo normal de F e $F/\ker(\phi_g)$ é nilpotente, já que pelo Teorema do Homomorfismo, é isomorfo a $\text{Im}(\phi_g) \subset Q$, e g não está em N_g .

Reciprocamente, suponha que a afirmação (a) seja satisfeita. Considere $g \neq 1_F$ em F e a projeção canônica $\pi: F \rightarrow F/N_g$. Como $g \notin N_g$, $\pi(g) \neq 1_{F/N_g}$ e π é um homomorfismo em F/N_g que é nilpotente, logo vale a Definição 5;

(a) $\Rightarrow$ (b) Suponha que $RN_F \neq \{1_F\}$, então existe $g \in RN_F$, tal que $g \neq 1_F$. Logo g está em todo subgrupo normal R de F e tal que F/R é nilpotente, o que contradiz (a);

(b) $\Rightarrow$ (a) Suponha que $RN_F = \{1_F\}$, então para todo $g \neq 1_F \in F$ existe um subgrupo normal N_g de F tal que F/N_g é nilpotente e $g \notin N_g$. $\square$

Em Magnus, Karrass e Solitar (1966, p. 349) um grupo é dito ser *residualmente nilpotente* se, e somente se, a interseção de todos os subgrupos da série central inferior é a identidade.

1.3 Grupos livres

Todos os resultados a respeito de grupos livres a seguir foram baseados em Cohen (1989).

Seja X um conjunto gerador de um grupo G , então qualquer elemento $g \in G$ pode ser escrito como um produto finito de elementos de X e seus inversos, ou seja, $g = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$, onde $\epsilon_k \in \{\pm 1\}$ e $x_{i_k} \in X$ para todo $k \in \{1, \dots, n\}$.

Dizemos que um grupo G é livre, em um conjunto X , se toda função $f: X \rightarrow H$, onde H é um grupo qualquer, pode ser estendida a um único homomorfismo $\varphi: G \rightarrow H$. Formalmente, temos:

Definição 6. Sejam X um conjunto, G um grupo e $i: X \rightarrow G$ uma aplicação. Dizemos que (G, i) é livre em X se para todo grupo H e uma função qualquer $f: X \rightarrow H$ existe um único homomorfismo $\varphi: G \rightarrow H$ tal que $f = \varphi \circ i$.

Observe que a definição anterior nos diz que o seguinte diagrama é comutativo.

$$\begin{array}{ccc} X & \xrightarrow{f} & H \\ \downarrow i & \searrow \varphi & \\ G & & \end{array}$$

A seguinte proposição garante que dado um conjunto X , o grupo livre sobre X , se existir, será único, a menos de isomorfismo.

Proposição 2. Sejam (G_1, i_1) e (G_2, i_2) grupos livres em X . Então existe um isomorfismo $\varphi: G_1 \rightarrow G_2$ tal que $\varphi \circ i_1 = i_2$.

Demonstração. Como (G_1, i_1) é livre em X , dado $i_2: X \rightarrow G_2$ existe um único homomorfismo $\varphi: G_1 \rightarrow G_2$ tal que $\varphi \circ i_1 = i_2$. E, sendo (G_2, i_2) livre em X , dado $i_1: X \rightarrow G_1$ existe um único homomorfismo $\psi: G_2 \rightarrow G_1$ tal que $\psi \circ i_2 = i_1$.

$$\begin{array}{ccc} X & \xrightarrow{i_2} & G_2 \\ \downarrow i_1 & \searrow \varphi & \\ G_1 & & \end{array}$$

$$\begin{array}{ccc} X & \xrightarrow{i_1} & G_1 \\ \downarrow i_2 & \searrow \psi & \\ G_2 & & \end{array}$$

Assim, temos que

$$\varphi \circ i_1 = i_2 \text{ e } \psi \circ i_2 = i_1. \quad (1.1)$$

De (1.1) segue que

$$\psi \circ \varphi \circ i_1 = i_1 \text{ e } \varphi \circ \psi \circ i_2 = i_2. \quad (1.2)$$

Por outro lado, dado $i_1: X \rightarrow G_1$ o homomorfismo $Id_{G_1}: G_1 \rightarrow G_1$ satisfaz $Id_{G_1} \circ i_1 = i_1$ e dado $i_2: X \rightarrow G_2$, o homomorfismo $Id_{G_2}: G_2 \rightarrow G_2$ satisfaz $Id_{G_2} \circ i_2 = i_2$ (ver diagramas adiante). Ainda por (1.2), como os homomorfismos que estendem i_1 e i_2 são únicos, segue que $\psi \circ \varphi = Id_{G_1}$ e $\varphi \circ \psi = Id_{G_2}$. Portanto, φ é um isomorfismo. $\square$

Veremos que é possível obter um resultado um pouco mais geral na [Proposição 5](#), onde é necessário apenas que as cardinalidades das bases coincidam.

A proposição a seguir mostra que se (G, i) é um grupo livre, então $i: X \rightarrow G$ é injetiva:

Proposição 3. Seja (F, i) um grupo livre em X . São válidas as seguintes afirmações:

- (a) Se existir um grupo G tal que existe $f: X \rightarrow G$ injetiva, então i é injetiva;
- (b) Existe um grupo G com uma função $g: X \rightarrow G$ injetiva;
- (c) i é injetiva.

Demonstração. (a) Como (F, i) é um grupo livre em X , dada $f: X \rightarrow G$ existe um único homomorfismo $\varphi: F \rightarrow G$ tal que $\varphi \circ i = f$. Dados x e y em X tal que $i(x) = i(y)$ temos que $\varphi \circ i(x) = \varphi \circ i(y)$ o que implica que $f(x) = f(y)$, logo $x = y$, pois f é injetiva;

(b) Considere o conjunto $\mathbb{Z}^X = \{f: X \rightarrow \mathbb{Z}\}$. Tal conjunto é um grupo com a operação

$$\begin{aligned} +: \mathbb{Z}^X \times \mathbb{Z}^X &\rightarrow \mathbb{Z}^X \\ (\alpha, \beta) &\mapsto (\alpha + \beta)(x) = \alpha(x) + \beta(x), \end{aligned}$$

para todo $x \in X$. Defina

$$\begin{aligned} g: X &\rightarrow \mathbb{Z}^X \\ x &\mapsto g(x) = \alpha_x, \text{ onde } \begin{cases} \alpha_x(x) = 1, \\ \alpha_x(y) = 0 \text{ se } y \neq x. \end{cases} \end{aligned}$$

Tal função é injetora;

(c) Segue de (b) e (a). □

1.3.1 Construção de um grupo livre

Uma questão natural que surge é a seguinte: dado um conjunto X , qualquer, é possível obter um grupo livre sobre ele?

Para responder a essa questão é necessário construir alguns objetos auxiliares.

Seja X um conjunto qualquer e considere o conjunto $M(X)$ de todas as sequências finitas $(x_{i_1}, \dots, x_{i_n})$, onde $n \geq 0$ e $x_{i_k} \in X$ para $k \in \{1, \dots, n\}$.

Podemos munir $M(X)$ de uma estrutura de monoide definindo o produto da seguinte maneira:

$$(x_{i_1}, \dots, x_{i_n})(x_{j_1}, \dots, x_{j_m}) = (x_{i_1}, \dots, x_{i_n}, x_{j_1}, \dots, x_{j_m}).$$

Neste caso o elemento neutro é dado pela sequência vazia $()$, ou seja, com $n = 0$ e será denotado por 1 . Tal monoide é denominado *monoide livre* sobre X . Utilizando a identificação $x \mapsto (x)$ iremos a partir de agora representar a sequência $(x_{i_1}, \dots, x_{i_n})$ apenas por $x_{i_1}x_{i_2} \cdots x_{i_n}$.

Definição 7. Sejam $X = \{x_1, x_2, \dots, x_n\}$, $M(X)$ o monoide livre sobre X e $w \in M(X)$. Então w é um produto de elementos de X e o morfismo $l: M(X) \rightarrow \mathbb{N}$, que associa a cada $w \in M(X)$ o número de elementos de X em sua expansão é chamado *função comprimento*. Note que o morfismo envia x_i em 1 , para todo $x_i \in X$. Vemos que $l(1) = 0$ e $l(ww') = l(w) + l(w')$, para todo $w, w' \in M(X)$.

Definição 8. Dado $w = x_{i_1} \cdots x_{i_n}$ um elemento em $M(X)$, dizemos que $x_{i_r}x_{i_{r+1}} \cdots x_{i_s}$ para $1 \leq r \leq s \leq n$ é um *segmento* de w . Se $r = 1$, o segmento é *inicial* e se $s = n$ o segmento é *final*.

Vamos agora construir um grupo livre sobre X . Considere um conjunto que denotaremos por X^{-1} , tal que existe uma bijeção $f: X \rightarrow X^{-1}$ onde $f(x) = x^{-1}$ e $X \cap X^{-1} = \emptyset$.

Definição 9. O elemento $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ em $M(X \cup X^{-1})$, onde $n \geq 0$, $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$ para todo $r \in \{1, \dots, n\}$, é denominado uma *palavra* em X onde $x_{i_r}^{\varepsilon_r}$ é uma *letra* de w .

Definição 10. Seja $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ uma palavra em X , dizemos que w é *reduzida* se para todo $r \in \{1, \dots, n-1\}$, $i_{r+1} \neq i_r$ ou se $i_{r+1} = i_r$ tivermos $\varepsilon_{r+1} \neq -\varepsilon_r$.

Note que a palavra vazia é obviamente reduzida e também que se w não é uma palavra reduzida então existe $r \in \{1, \dots, n-1\}$ tal que $i_{r+1} = i_r$ e $\varepsilon_{r+1} = -\varepsilon_r$.

Definição 11. Seja w uma palavra em X que não é reduzida e seja $r \in \{1, \dots, n-1\}$ tal que $i_{r+1} = i_r$ e $\varepsilon_{r+1} = -\varepsilon_r$, uma *redução elementar* de w consiste em excluir o par $x_{i_r}^{\varepsilon_r}x_{i_{r+1}}^{\varepsilon_{r+1}}$, obtendo uma nova palavra w' . Neste caso diremos que w' vem de w por uma redução elementar.

Definição 12. Dizemos que w'' é uma *redução* de w se ela é obtida após uma sequência de reduções elementares em w . Ou seja, existe uma sequência de palavras $w_1, \dots, w_k$ tais que $w_1 = w$, $w_k = w''$ e para todo $j \in \{1, \dots, k-1\}$, w_{j+1} vem de w_j por uma redução elementar.

Vamos agora considerar no conjunto $M(X \cup X^{-1})$ a seguinte relação $w \sim w' \Leftrightarrow w = w'$, ou existe uma sequência de palavras $w_1, \dots, w_k$ para algum k tal que $w_1 = w$, $w_k = w'$ e para cada $1 \leq j < k$, uma das palavras w_{j+1} ou w_j provém da outra por uma redução elementar.

Denotaremos a classe de equivalência de $w \in M(X \cup X^{-1})$ por $[w]$ e o conjunto quociente de $M(X \cup X^{-1})$ por tal relação de equivalência por $F(X)$, o qual é um grupo com a seguinte

operação

$$[u][w] = [uw],$$

onde o elemento neutro é a classe da palavra vazia e, dado $w = [x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}]$, o elemento inverso é dado por $w^{-1} = [x_{i_n}^{-\varepsilon_n} \cdots x_{i_1}^{-\varepsilon_1}]$.

Considerando a função $i: X \rightarrow F(X)$, tal que

$$i(x) = [x],$$

temos que $F(X)$ é gerado por $i(X)$. De fato, dado um elemento z em $F(X)$, então existe $w \in M(X \cup X^{-1})$, $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$, $x_{i_r} \in X$ e $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$, tal que $z = [w]$ e então,

$$z = [x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}] = [x_{i_1}]^{\varepsilon_1} \cdots [x_{i_n}]^{\varepsilon_n} = i(x_1)^{\varepsilon_1} \cdots i(x_{i_n})^{\varepsilon_n},$$

implicando que todo elemento em $F(X)$ se escreve como combinação de elementos em $i(X)$.

Teorema 1. O par $(F(X), i)$ é livre em X .

Demonstração. Sejam H um grupo livre e $f: X \rightarrow H$ uma função. Defina

$$\begin{aligned} \bar{f}: M(X \cup X^{-1}) &\rightarrow H \\ w &\mapsto \bar{f}(w) = f(x_{i_1})^{\varepsilon_1} \cdots f(x_{i_n})^{\varepsilon_n}, \end{aligned} \quad (1.3)$$

onde $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$.

Considere $\varphi: F(X) \rightarrow H$ definida por $\varphi([w]) = \bar{f}(w)$. Temos que φ está bem definida e é o único homomorfismo que satisfaz $\varphi \circ i(x) = f(x)$, para todo $x \in X$. De fato:

- i) Sejam $[w], [w'] \in F(X)$ tais que $[w] = [w']$ de onde temos que $w \sim w'$. É imediato que se w'' provém de w por uma redução elementar, então w e w'' têm a mesma imagem. Segue que se $w \sim w'$, então $\varphi([w]) = \bar{f}(w) = \bar{f}(w') = \varphi([w'])$.
- ii) φ é um homomorfismo que estende f . Considere $[w_1]$ e $[w_2]$ em $F(X)$, com $w_1 = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ e $w_2 = x_{j_1}^{\delta_1} \cdots x_{j_m}^{\delta_m}$ temos que

$$\begin{aligned} \varphi([w_1][w_2]) &= \varphi([w_1 w_2]) \\ &= \bar{f}(w_1 w_2) \\ &= \bar{f}(x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n} x_{j_1}^{\delta_1} \cdots x_{j_m}^{\delta_m}) \\ &= f(x_{i_1})^{\varepsilon_1} \cdots f(x_{i_n})^{\varepsilon_n} f(x_{j_1})^{\delta_1} \cdots f(x_{j_m})^{\delta_m} \\ &= \bar{f}(w_1) \bar{f}(w_2) \\ &= \varphi([w_1]) \varphi([w_2]) \end{aligned}$$

e, portanto, φ é um homomorfismo.

Além disso, dado $x \in X$, $\varphi \circ i(x) = \varphi(i(x)) = \varphi([x]) = \bar{f}(x) = f(x)$.

iii) Queremos garantir agora que φ é o único homomorfismo que estende f . Seja $\psi: F(X) \rightarrow H$ tal que $\psi \circ i = f$. Dado $[w]$ em $F(X)$ segue que $[w] = i(x_{i_1})^{\varepsilon_1} \cdots i(x_{i_n})^{\varepsilon_n}$, visto que $F(X) = \langle i(X) \rangle$. Então

$$\begin{aligned}
 \psi([w]) &= \psi(i(x_1)^{\varepsilon_1} \cdots i(x_{i_n})^{\varepsilon_n}) \\
 &= \psi(i(x_1)^{\varepsilon_1}) \cdots \psi(i(x_{i_n})^{\varepsilon_n}) \\
 &= (\psi \circ i)(x_1^{\varepsilon_1}) \cdots (\psi \circ i)(x_{i_n}^{\varepsilon_n}) \\
 &= f(x_{i_1}^{\varepsilon_1}) \cdots f(x_{i_n}^{\varepsilon_n}) \\
 &= (\varphi \circ i)(x_1^{\varepsilon_1}) \cdots (\varphi \circ i)(x_{i_n}^{\varepsilon_n}) \\
 &= \varphi(i(x_1)^{\varepsilon_1}) \cdots \varphi(i(x_{i_n})^{\varepsilon_n}) \\
 &= \varphi(i(x_1)^{\varepsilon_1} \cdots i(x_{i_n})^{\varepsilon_n}) \\
 &= \varphi([w]).
 \end{aligned}$$

Logo, $\varphi = \psi$.

□

Teorema 2 (Teorema da forma normal para grupos livres). Existe somente uma palavra reduzida em cada classe de equivalência.

Demonstração. Ver [Cohen \(1989, p. 5\)](#).

□

Corolário 1. A aplicação $i: X \rightarrow F(X)$ é injetiva.

Demonstração. Sejam $x, y \in X$, tais que $x \neq y$, então x e y são palavras reduzidas distintas e consequentemente $[x]$ e $[y]$ são classes de equivalência distintas.

□

Definição 13. Seja G um grupo, dizemos que G é *residualmente finito* se para todo $g \in G$, com $g \neq 1$, existe um subgrupo normal N de G tal que $g \notin N$ e G/N é finito.

Proposição 4. Todo grupo livre é residualmente finito.

Demonstração. Ver [Cohen \(1989, p. 11\)](#).

□

Definição 14. Dizemos que um grupo G é *Hopfiano* se todo epimorfismo de G em G é um automorfismo.

Corolário 2. Grupos livres finitamente gerados são Hopfianos.

Demonstração. Ver [Cohen \(1989, p. 12\)](#).

□

Proposição 5. Sejam $(F(X), i_1)$ livre em X e $(F(Y), i_2)$ livre em Y . Então $F(X)$ é isomorfo a $F(Y)$ se, e somente se, $|X| = |Y|$.

Demonstração. Primeiramente suponha que $F(X)$ é isomorfo a $F(Y)$.

Recorde que para cada função $f: X \rightarrow \mathbb{Z}_2$, por $(F(X), i)$ ser livre sobre X , existe um único homomorfismo $\varphi: F(X) \rightarrow \mathbb{Z}_2$ tal que $\varphi \circ i = f$. Então

$$|\{f: X \rightarrow \mathbb{Z}_2\}| = |\{\varphi: F(X) \rightarrow \mathbb{Z}_2; \varphi \text{ é homomorfismo}\}| = 2^{|X|}.$$

De maneira análoga obtemos

$$|\{f: Y \rightarrow \mathbb{Z}_2\}| = |\{\varphi: F(Y) \rightarrow \mathbb{Z}_2; \varphi \text{ é homomorfismo}\}| = 2^{|Y|}.$$

Como $F(X) \cong F(Y)$ temos que $2^{|X|} = 2^{|Y|}$. E no caso em que X ou Y é finito então $|X| = |Y|$.

Agora suponha que X e Y possuem infinitos elementos. Neste caso, pode-se mostrar que

$$|M(X \cup X^{-1})| = |X \cup X^{-1}| = |X|$$

e como $F(X)$ é um conjunto de classes de $M(X \cup X^{-1})$ segue que $|F(X)| \leq |X|$. Como $X \subset F(X)$ então $|X| \leq |F(X)|$, logo $|X| = |F(X)|$ e de maneira análoga temos que $|Y| = |F(Y)|$. Desde que $F(X) \cong F(Y)$ temos que $|F(X)| = |F(Y)|$, portanto $|X| = |Y|$.

Agora suponha que $|X| = |Y|$, então existe uma bijeção $f: X \rightarrow Y$.

Como $(F(X), i_1)$ é livre em X , a função $i_2 \circ f: X \rightarrow F(Y)$ se estende a um único homomorfismo $\varphi: F(X) \rightarrow F(Y)$ tal que $\varphi \circ i_1 = i_2 \circ f$.

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{i_2} & F(Y) \\ i_1 \downarrow & & & \nearrow \varphi & \\ F(X) & & & & \end{array}$$

Como $(F(Y), i_2)$ é livre em Y , a função $i_1 \circ f^{-1}: Y \rightarrow F(X)$ se estende a um único homomorfismo $\psi: F(Y) \rightarrow F(X)$ tal que $\psi \circ i_2 = i_1 \circ f^{-1}$.

$$\begin{array}{ccccc} Y & \xrightarrow{f^{-1}} & X & \xrightarrow{i_1} & F(X) \\ i_2 \downarrow & & & \nearrow \psi & \\ F(Y) & & & & \end{array}$$

Resulta que

$$\psi \circ \varphi \circ i_1 = \psi \circ i_2 \circ f = i_1 \circ f^{-1} \circ f = i_1 \text{ e } \varphi \circ \psi \circ i_2 = \varphi \circ i_1 \circ f^{-1} = i_2 \circ f \circ f^{-1} = i_2.$$

Recorde que dado $i_1: X \rightarrow F(X)$ temos que a aplicação $Id_{F(X)}$ é tal que $Id_{F(X)} \circ i_1 = i_1$ e dado $i_2: Y \rightarrow F(Y)$ temos que aplicação $Id_{F(Y)}$ é tal que $Id_{F(Y)} \circ i_2 = i_2$.

Pela unicidade da extensão, obtemos $\psi \circ \varphi = Id_{F(X)}$ e $\varphi \circ \psi = Id_{F(Y)}$ e, portanto, $F(X) \cong F(Y)$. $\square$

Definição 15. Dado G um grupo, se existir um isomorfismo $j: F(X) \rightarrow G$ para algum conjunto X diremos que G é livre e que $j(X)$ é base de G .

Proposição 6. Seja G um grupo, $\varphi: G \rightarrow G$ um automorfismo e A uma base de G . Então $\varphi(A)$ também é base de G .

Demonstração. Por definição, se A é base de G então $A = j(X)$ para um isomorfismo $j: F(X) \rightarrow G$. Como $\varphi: G \rightarrow G$ é um automorfismo, então $\varphi \circ j: F(X) \rightarrow G$ é um isomorfismo, logo $\varphi \circ j(X) = \varphi(A)$ é base de G . $\square$

Proposição 7. Sejam A e B bases distintas de um grupo G . Então $|A| = |B|$.

Demonstração. Se A e B são bases de G então $A = j(X)$ e $B = h(Y)$, onde $j: F(X) \rightarrow G$ e $h: F(Y) \rightarrow G$ são isomorfismos.

Portanto, $F(X)$ é isomorfo a $F(Y)$, pois basta considerar $h^{-1} \circ j$. Pela [Proposição 5](#), $|X| = |Y|$ e como $|j(X)| = |X|$ e $|h(Y)| = |Y|$, segue que $|A| = |B|$. $\square$

Proposição 8. Sejam G um grupo, A e B bases de G e $f: A \rightarrow B$ uma bijeção, então existe um automorfismo $\varphi: G \rightarrow G$ tal que $\varphi|_A = f$, ou seja, φ estende f .

Demonstração. Temos que $|A| = |B|$ e, pela [Proposição 5](#), existe um automorfismo de G . $\square$

Definição 16. O posto de um grupo livre G é a cardinalidade de X , tal que existe um isomorfismo $i: F(X) \rightarrow G$.

Proposição 9. Seja X um subconjunto de um grupo G . Então as seguintes afirmações são equivalentes:

- i) G é um grupo livre com base X ;
- ii) Todo elemento de G pode ser escrito de maneira única como $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ para algum $n \geq 0$, onde $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$ e $\varepsilon_{r+1} \neq -\varepsilon_r$ se $i_{r+1} = i_r$ para $r \in \{1, \dots, n-1\}$;
- iii) X gera G e 1 não pode ser escrito da forma $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$, para nenhum $n > 0$, $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$ e $\varepsilon_{r+1} \neq -\varepsilon_r$ se $i_{r+1} = i_r$ para $r \in \{1, \dots, n-1\}$.

Demonstração. (ii) $\Rightarrow$ (iii) Segue da definição de conjunto gerador;

(iii) $\Rightarrow$ (ii) Como X gera G , qualquer elemento de G é escrito da forma $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ para $n \geq 0$, $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$ e $\varepsilon_{r+1} \neq -\varepsilon_r$ se $i_{r+1} = i_r$ para $r \in \{1, \dots, n-1\}$. Agora suponha que um elemento de G possua duas representações, multiplicando uma pelo inverso da outra e fazendo todas as possíveis reduções, obtemos uma maneira de escrever 1 como um produto não-trivial, o que contradiz (iii);

(i) $\Rightarrow$ (ii) e (iii) Se G é livre em X , já temos que $F(X)$ é livre em X , portanto $F(X) \cong G$. Assim, se $F(X)$ possui essa propriedade, G também deve satisfazer;

(ii) e (iii) $\Rightarrow$ (i) Se G possui as propriedades apresentadas em (ii) e (iii) temos que dada a inclusão $j: X \rightarrow G$ existe um único homomorfismo $\alpha: F(X) \rightarrow G$ que estende j . E α é sobrejetora já que X gera G . Além disso, α é injetora, desde que se $\alpha(w) = 1$ então $w = 1$, visto que se $w = x_{i_1}^{\delta_1} \cdots x_{i_n}^{\delta_n}$ com $n > 0$ então $\alpha(w) = \alpha(x_{i_1}^{\delta_1} \cdots x_{i_n}^{\delta_n}) = \alpha(x_{i_1})^{\delta_1} \cdots \alpha(x_{i_n})^{\delta_n} = \alpha(j(x_{i_1}))^{\delta_1} \cdots \alpha(j(x_{i_n}))^{\delta_n} = j(x_{i_1})^{\delta_1} \cdots j(x_{i_n})^{\delta_n} = x_{i_1}^{\delta_1} \cdots x_{i_n}^{\delta_n} = 1$ o que contraria a hipótese de (iii). $\square$

Corolário 3. Seja X um conjunto gerador de um grupo G e seja $\varphi: G \rightarrow H$ um homomorfismo tal que $\varphi|_X$ é injetor e $\varphi(G)$ é livre com base $\varphi(X)$. Então G é livre com base X .

Demonstração. Temos que X gera G , assim resta mostrar que 1 não pode ser escrito da forma $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$, $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$ e $\varepsilon_{r+1} \neq -\varepsilon_r$ se $i_{r+1} = i_r$ para todo $r \in \{1, \dots, n-1\}$ para nenhum $n > 0$. Supondo que 1 possa ter a representação anterior, teríamos

$$1 = \varphi(1) = \varphi(x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}) = \varphi(x_{i_1})^{\varepsilon_1} \cdots \varphi(x_{i_n})^{\varepsilon_n},$$

o que contradiz o fato de $\varphi(G)$ ser livre em $\varphi(X)$.

Portanto G satisfaz a condição (iii) da [Proposição 9](#) e, assim, pela condição (i) segue que G é livre com base X . $\square$

Corolário 4. Sejam G um grupo livre com base X , e $Y \subset X$. Então o subgrupo $\langle Y \rangle$ de G é livre com base Y .

Demonstração. A condição (iii) da [Proposição 9](#) permanece válida para $\langle Y \rangle$, pois vale para G . Portanto, $\langle Y \rangle$ é livre com base Y . $\square$

Corolário 5. Sejam $F(X)$ um grupo livre com base $X = \{x, y\}$ e $\varphi: F(X) \rightarrow \mathbb{Z}$ uma aplicação que satisfaz $\varphi(x) = 1$ e $\varphi(y) = 0$. Então $\ker(\varphi)$ é livre com base $A = \{x^{-i}yx^i, \forall i \in \mathbb{Z}\}$.

Demonstração. Temos que $A \subset \ker(\varphi)$ já que $\varphi(x^{-i}yx^i) = -i\varphi(x) + \varphi(y) + i\varphi(x) = 0$. Logo $\langle A \rangle \subseteq \ker(\varphi)$.

Seja agora $w \in F(X)$, então $w = x^{a_1}y^{b_1} \cdots x^{a_n}y^{b_n}$ onde $a_1 \geq 0$ e $b_n \geq 0$. Temos que

$$\begin{aligned} w &= x^{a_1}y^{b_1}x^{-a_1}x^{a_1}x^{a_2}y^{b_2}x^{a_3} \cdots x^{a_n}y^{b_n} \\ &= (x^{a_1}y^{b_1}x^{-a_1})x^{(a_1+a_2)}y^{b_2}x^{a_3} \cdots x^{a_n}y^{b_n} \\ &= (x^{a_1}y^{b_1}x^{-a_1})(x^{(a_1+a_2)}y^{b_2}x^{-(a_1+a_2)})x^{(a_1+a_2)}x^{a_3} \cdots x^{a_n}y^{b_n} \\ &= z_1 z_2 x^{(a_1+a_2+a_3)} \cdots x^{a_n}y^{b_n} \\ &= z_1 z_2 \cdots z_n x^{(a_1+a_2+\cdots+a_n)}, \end{aligned}$$

onde $z_i \in A$ para todo $i \in \{1, \dots, n\}$. Logo, todo elemento de $F(X)$ pode ser escrito como ux^n , $u \in \langle A \rangle$ e $n \in \mathbb{Z}$. Assim, dado $w = ux^n \in F$,

$$\varphi(w) = 0 \Leftrightarrow \varphi(ux^n) = 0 \Leftrightarrow \varphi(u) + n\varphi(x) = 0 \Leftrightarrow n = 0. \quad (1.4)$$

Portanto, $w \in \ker(\varphi)$ somente se $w = u \in A$, donde $\ker(\varphi) \subseteq \langle A \rangle$ e segue a igualdade.

Agora iremos mostrar que 1 não pode ser escrito com uma palavra reduzida não-trivial. Considere $x_i = x^{-i}yx^i$, então tome $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n} = 1 \in \ker(\varphi)$ com $n > 0$. Temos que

$$\begin{aligned} w &= (x^{-i_1}yx^{i_1})^{\varepsilon_1} (x^{-i_2}yx^{i_2})^{\varepsilon_2} \cdots (x^{-i_n}yx^{i_n})^{\varepsilon_n} \\ &= x^{j_1}y^{\varepsilon_1}x^{j_2}y^{\varepsilon_2}x^{j_3} \cdots x^{j_n}y^{\varepsilon_n}x^{j_{n+1}}, \end{aligned}$$

onde $j_k = i_{k-1} - i_k$ com $k \in \{1, \dots, n\}$ considerando $i_0 = i_{n+1} = 0$. Tal produto não pode ser igual a 1 visto que $F(X)$ é livre em X . Segue de (iii) que $\ker(\varphi)$ é livre sobre A . $\square$

Definição 17. Seja g um elemento de $F(X)$. Pelo Teorema 2, g tem um único representante que é uma palavra reduzida. O número de letras deste representante é chamado de *comprimento* de g e é denotado por $|g|$.

Definição 18. Sejam $g_1, g_2, \dots, g_k, k \geq 0$, palavras reduzidas em $F(X)$. Se $g_1g_2 \cdots g_k$ é reduzida, dizemos que $g_1g_2 \cdots g_k$ é *reduzida como escrita*.

Segue da definição que:

1. $|gh| \leq |g| + |h|$ e só é válido $|gh| = |g| + |h|$ se a palavra gh é reduzida como escrita;
2. A primeira letra de gh é a primeira letra de g ou g é cancelada completamente na redução de gh a uma palavra reduzida k equivalente a ela, então $h = g^{-1}k$. E também dizemos que gh termina com a última letra de h ou h é cancelada completamente na redução de gh a uma palavra reduzida k , então $g = kh^{-1}$.

Definição 19. Seja $g \in F(X)$ uma palavra reduzida, então g se escreve como $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ para algum $n \geq 0$, $x_{i_r} \in X$, $\varepsilon_r \in \{\pm 1\}$, para todo $r \in \{1, \dots, n\}$ e $i_{r+1} \neq i_r$ ou $i_{r+1} = i_r$ mas $\varepsilon_{r+1} \neq -\varepsilon_r$, para todo $r \in \{1, \dots, n-1\}$. Dizemos que g é *ciclicamente reduzida* se $i_n \neq i_1$ ou $i_n = i_1$, mas $\varepsilon_n \neq -\varepsilon_1$.

É fácil verificar que g é ciclicamente reduzida se, e somente se, gg é reduzida como escrita. Por indução é possível ainda mostrar que g é ciclicamente reduzida se, e somente se, g^n é reduzida como escrita.

Segue que se g^n é reduzida como escrita então $|g^n| = n|g|$. E que se $g = u^{-1}vu$, reduzida como escrita, e v é ciclicamente reduzida, então $g^n = u^{-1}v^nu$ é reduzida como escrita.

Definição 20. Seja $g = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n} \in F(X)$ uma palavra reduzida, então

$$x_{i_r}^{\varepsilon_r} \cdots x_{i_n}^{\varepsilon_n} x_{i_1}^{\varepsilon_1} \cdots x_{i_{r-1}}^{\varepsilon_{r-1}},$$

onde $r \in \{1, \dots, n\}$, é uma permutação cíclica de g .

Proposição 10. As seguintes afirmações são válidas:

- (i) Qualquer elemento de $F(X)$ é conjugado de uma palavra ciclicamente reduzida;
- (ii) Qualquer permutação cíclica de uma palavra ciclicamente reduzida é ciclicamente reduzida;
- (iii) Duas palavras ciclicamente reduzidas são conjugadas se, e somente se, elas são permutações cíclicas uma da outra.

Demonstração. Ver [Cohen \(1989, p. 15\)](#). □

Definição 21. Seja G um grupo. O conjunto $Tor(G) = \{g \in G; \exists n \in \mathbb{N} \text{ tal que } g^n = 1_G\}$ é chamado *subgrupo de torção*. Se $Tor(G) = 1_G$, o grupo G é chamado *livre de torção*.

Proposição 11. Grupos livres são livres de torção.

Demonstração. Seja $g \in F(X)$, onde $F(X)$ é livre sobre um conjunto X e $g \neq 1$. Considerando o conjugado, se necessário, podemos assumir que g é ciclicamente reduzida. Então como $|g^n| = n|g| \neq 0$, segue que $g^n \neq 1$. □

Proposição 12. Seja $F(X)$ grupo livre sobre X , então $F(X)$ possui raízes únicas, isto é, dados $g, h \in F(X)$. Se $g^k = h^k$ para algum $k \neq 0$, então $g = h$.

Demonstração. Assuma que $k > 0$. Tomando o conjugado, se necessário, também podemos assumir que g é ciclicamente reduzida, então g^k também o é. Se h não é ciclicamente reduzida então h^k não é ciclicamente reduzida, daí $g^k \neq h^k$. Se h é ciclicamente reduzida então h^k também é ciclicamente reduzida como escrita. Consequentemente g^k consiste do elemento g repetido k vezes, e similarmente h^k consiste de h repetido k vezes, então $g^k = h^k$ se $h = g$. □

Proposição 13. Sejam $F(X)$ um grupo livre sobre X e $g, h \in F(X)$. Se $gh = hg$ então $\langle g, h \rangle$ é cíclico, isto é, existem $u \in F(X)$ e inteiros r e s tais que $g = u^r$ e $h = u^s$.

Demonstração. Provaremos por indução sobre $|g| + |h|$, o caso em que $|g| + |h| \leq 2$ é imediato. Considerando se necessário o seu conjugado, podemos assumir (sem aumentar $|g| + |h|$) que g é ciclicamente reduzida.

Suponha que gh é reduzida como escrita, então $|gh| = |g| + |h|$ e portanto $|hg| = |h| + |g|$. Logo, hg também é reduzida como escrita. Então g é o segmento inicial de gh e h é o segmento inicial

de hg . Como $hg = gh$, um dos segmentos g ou h deve ser o segmento inicial do outro. Isto é, mudando o lugar de g e h se necessário, temos $g = hw$, para algum w em $F(X)$, reduzida como escrita. Além disso, de $gh = hg$ temos que $hwh = hhw$, de onde temos que $wh = hw$. E o resultado segue por indução.

Se gh não é reduzida como escrita, então $g = vx^\varepsilon$ e $h = x^{-\varepsilon}t$ ambas reduzidas como escritas em $F(X)$. Agora hg começa com a primeira letra de h , que é $x^{-\varepsilon}$, a menos que h seja completamente cancelada no produto. Então gh começa com a primeira letra de g a menos que g cancela completamente no produto. Desde que g é ciclicamente reduzida e termina em x^ε , então g não pode começar com $x^{-\varepsilon}$. Então gh e hg são diferentes a menos que g seja cancelada completamente em gh ou h seja cancelado completamente em hg . Consequentemente, $h = g^{-1}w$ ou $g = h^{-1}w$, reduzida como escrita em ambos os casos, para algum w em $F(X)$. O resultado segue agora por indução. $\square$

Observação 2. Para simplificar a notação escreveremos somente F para indicar $F(X)$ sempre que não for necessário especificar o conjunto gerador. E também quando quisermos especificar a quantidade de geradores de F colocaremos entre parênteses a quantidade de elementos de seu conjunto gerador, por exemplo, se $X = \{x_1, \dots, x_n\}$ é o conjunto gerador, escrevemos $F(n)$.

1.3.2 Apresentação de um grupo

Proposição 14. Qualquer grupo G é quociente de um grupo livre.

Demonstração. Considere a aplicação identidade $Id: G \rightarrow G$. Tome $F(G)$ o grupo livre sobre G , então existe um único homomorfismo $\varphi: F(G) \rightarrow G$ definido por $\varphi(w) = \varphi(g_{i_1}^{\varepsilon_1} \cdots g_{i_n}^{\varepsilon_n}) = Id(g_{i_1})^{\varepsilon_1} \cdots Id(g_{i_n})^{\varepsilon_n} = g_{i_1}^{\varepsilon_1} \cdots g_{i_n}^{\varepsilon_n}$, para todo $w = g_{i_1}^{\varepsilon_1} \cdots g_{i_n}^{\varepsilon_n} \in F(G)$. Temos que φ é sobrejetora e assim, pelo Teorema do Homomorfismo, o quociente $F(G)/\ker(\varphi)$ é isomorfo à $Im(\varphi)$, que neste caso é G . Portanto, G é quociente de um grupo livre. $\square$

Definição 22. Sejam X um conjunto, G um grupo e $\varphi: F(X) \rightarrow G$ um epimorfismo. Então X é chamado um *conjunto de símbolos geradores para G* e a família $\{\varphi(x); x \in X\}$ é chamada *família de geradores de G* .

Definição 23. Sejam X um conjunto, G um grupo e $\varphi: F(X) \rightarrow G$ um epimorfismo. Então $\ker(\varphi)$ é chamado *conjunto de relatores de G* .

Definição 24. Sejam H um grupo e $S \subset H$ um subconjunto. Então o fecho normal de S em H , que denotaremos por $\langle S \rangle^H$, é chamado *conjunto das consequências de S em H* .

Definição 25. Sejam X um conjunto, G um grupo e $\varphi: F(X) \rightarrow G$ um epimorfismo. Um subconjunto R de $F(X)$ tal que $\ker(\varphi) = \langle R \rangle^{F(X)}$ é chamado de *conjunto de relatores definidores de G* .

Definição 26. Uma *apresentação de um grupo* G consiste de um conjunto X , um epimorfismo $\varphi: F(X) \rightarrow G$ e um conjunto de relatores definidores R de G .

Denotaremos uma apresentação por $\langle X; R \rangle^\varphi$.

Observação 3. Em alguns casos é conveniente escrever a relação $r = 1$ em vez do relator r .

Exemplo 1. Seja G um grupo abeliano gerado por um conjunto X . Em vez de escrevermos os relatores $x^{-1}y^{-1}xy$, utilizamos a relação $xy = yx$, para todo $x, y \in X$.

Definição 27. Seja $\langle X; R \rangle^\varphi$ uma apresentação de G . Se X e R forem finitos, dizemos que $\langle X; R \rangle^\varphi$ é uma *apresentação finita* e G é um *grupo finitamente apresentado*.

Exemplo 2. O grupo livre em X tem uma apresentação $\langle X; R \rangle^\varphi$, com $R = \emptyset$.

De fato, considere a aplicação identidade $\varphi = Id_{F(X)}: F(X) \rightarrow F(X)$. Temos que φ é um epimorfismo e $\ker(\varphi) = \langle R \rangle^{F(X)} = \{1\}$, com $R = \emptyset$. Portanto, $F(X) = \langle X; \emptyset \rangle^\varphi$.

Exemplo 3. A apresentação $\langle a, b; a^{-1}ba = b^2, b^{-1}ab = a^2 \rangle$ representa o grupo trivial.

Temos que $X = \{a, b\}$ e suponha que $\langle a, b; a^{-1}ba = b^2, b^{-1}ab = a^2 \rangle$ é uma apresentação de G . Utilizando as relações dadas temos que $a = a^{-1}b^{-1}ab$ e $b = b^{-1}a^{-1}ba$. Assim, $ab = (a^{-1}b^{-1}ab)(b^{-1}a^{-1}ba) = 1$ e $a = b^{-1}$. Substituindo nas relações temos que $b^2 = b$ e $a^2 = a$, portanto $a = b = 1$. Assim, $X = \{1\}$ e então $F(X) = \{1\}$. Como $\varphi: F(X) \rightarrow G$ é um homomorfismo sobrejetor, segue que $G = \{1_G\}$.

Teorema 3 (Teorema de Von Dick). Sejam $\langle X; R \rangle^\varphi$ uma apresentação de um grupo G , H um grupo qualquer, $f: X \rightarrow H$ uma aplicação e $\theta: F(X) \rightarrow H$ o homomorfismo correspondente. Se $\theta(r) = 1$ para todo $r \in R$, então existe um homomorfismo $\psi: G \rightarrow H$ tal que $f(x) = \psi \circ \varphi(x)$ para todo $x \in X$. Além disso, se $f(X)$ gera H , então ψ é um epimorfismo.

Demonstração. Por hipótese, $\theta(r) = 1$ para todo $r \in R$ donde $R \subset \ker(\theta)$. Como $\ker(\varphi) = \langle R \rangle^{F(X)}$ temos que $\ker(\varphi) \subset \ker(\theta)$.

Defina $\psi: G \rightarrow H$ por $\psi(g) = \theta(w)$, onde $\varphi(w) = g$. Note que para todo $x \in X$, $\psi(\varphi(x)) = \theta(x)$, então $\psi(\varphi(x)) = f(x)$.

Temos que ψ está bem definida. De fato, suponha que existam w_1 e w_2 em $F(X)$ tais que $\varphi(w_1) = \varphi(w_2) = g$. Temos que

$$\begin{aligned} \varphi(w_1 w_2^{-1}) = 1 &\Rightarrow w_1 w_2^{-1} \in \ker(\varphi) \\ &\Rightarrow w_1 w_2^{-1} \in \ker(\theta) \\ &\Rightarrow \theta(w_1 w_2^{-1}) = 1 \\ &\Rightarrow \theta(w_1) = \theta(w_2). \end{aligned}$$

Se $\langle f(X) \rangle = H$, então o homomorfismo induzido $\theta: F(X) \rightarrow H$ é sobrejetor e portanto $\psi: G \rightarrow H$ também é sobrejetor. De fato, se $h \in H$ existe $w \in F(X)$ tal que $\theta(w) = h$, e suponha que $\varphi(w) = w'$ da maneira em que definimos ψ , temos $\psi(w') = \theta(w) = h$. $\square$

Utilizando o mesmo argumento da demonstração do teorema anterior temos o seguinte resultado:

Proposição 15. Sejam R um subconjunto de um grupo A , H um grupo qualquer e $\theta: A \rightarrow H$ um homomorfismo tal que $\theta(R) = \{1\}$. Então existe um homomorfismo $\psi: A/\langle R \rangle^A \rightarrow H$ tal que $\theta = \psi \circ \pi$, onde π é o epimorfismo canônico de A em $A/\langle R \rangle^A$.

Exemplo 4. O grupo $\mathbb{Z}_n$ tem apresentação $\langle x; x^n \rangle$.

De fato, seja $G = \langle x; x^n \rangle$. A aplicação $f: \{x\} \rightarrow \mathbb{Z}_n$ dada por $f(x) = 1$ se estende a um homomorfismo $\theta: F(\{x\}) \rightarrow \mathbb{Z}_n$ que é um epimorfismo pois $\theta(x) = 1$ gera $\mathbb{Z}_n$. Como $x^n \in \ker(\theta)$, temos um epimorfismo de G em $\mathbb{Z}_n$. Logo, basta provar que G não tem mais que n elementos. Utilizando o algoritmo da divisão de Euclides, vê-se que todo elemento de G pertence ao conjunto $\{1, x, x^2, \dots, x^{n-1}\}$, já que $x^n = 1$.

1.4 Produto semidireto

Esta seção terá como principais referências [Melocro \(2016\)](#) e [Sgobbi \(2017\)](#).

Definição 28. Sejam H e Q grupos, com 1_H e 1_Q denotando, respectivamente, seus elementos identidades. O conjunto $H \times Q = \{(h, q); h \in H \text{ e } q \in Q\}$ munido da operação

$$\begin{aligned} \cdot: (H \times Q) \times (H \times Q) &\rightarrow H \times Q \\ ((h_1, q_1), (h_2, q_2)) &\mapsto (h_1 h_2, q_1 q_2), \end{aligned} \quad (1.5)$$

para todo $h_1, h_2 \in H$ e $q_1, q_2 \in Q$, é um grupo onde dado $(h, q) \in H \times Q$ o seu inverso é (h^{-1}, q^{-1}) e $(1_H, 1_Q)$ é a identidade. Tal grupo é chamado *produto direto* de H por Q .

Seja H um grupo, então $\text{Aut}(H)$ é o grupo dos automorfismos de H com a operação composição natural.

Definição 29. Sejam H e Q grupos e $\sigma: Q \rightarrow \text{Aut}(H)$ um homomorfismo. O produto semidireto (externo) de H por Q , que denotaremos por $H \rtimes_\sigma Q$ é o conjunto $H \times Q$ munido da operação

$$\begin{aligned} *_\sigma: (H \times Q) \times (H \times Q) &\rightarrow (H \times Q) \\ ((h_1, q_1), (h_2, q_2)) &\mapsto (h_1 \sigma(q_1)(h_2), q_1 q_2) \end{aligned} \quad (1.6)$$

onde $\sigma(q_1)(h_2)$ é a imagem de h_2 através de $\sigma(q_1) \in \text{Aut}(H)$. Com esta operação, $H \rtimes_\sigma Q$ é um grupo com identidade $(1, 1)$ e dado $(h, q) \in H \rtimes_\sigma Q$ o seu inverso é $(\sigma(q^{-1})(h^{-1}), q^{-1})$.

Observação 4. Se, na definição anterior, $\sigma: Q \rightarrow \text{Aut}(H)$ é o homomorfismo trivial, isto é, que leva todo elemento de Q na identidade de $\text{Aut}(H)$, obtemos o produto direto de G e H .

Definição 30. Sejam G um grupo e H e Q subgrupos de G . Dizemos que H e Q são complementos um do outro em G se $G = HQ = \{hq; h \in H \text{ e } q \in Q\}$ e $H \cap Q = \{1_G\}$. Neste caso, $G \cong H \times Q$ (a saber, pelo isomorfismo $(h, k) \rightarrow hk$).

Definição 31. Considere um grupo G e subgrupos H e Q de G . Dizemos que G é o *produto semidireto interno de H por Q* , quando:

- i) $H \leq G$ é normal;
- ii) $H \cap Q = 1$;
- iii) $HQ = G$.

Proposição 16. Se G é o produto semidireto interno de H por Q , então $G \cong H \rtimes Q$, onde a operação do produto semidireto externo é dada pela conjugação $\sigma(q)(h) = q^{-1}hq$. Reciprocamente, um produto semidireto $H \rtimes Q$ é produto semidireto interno de dois de seus subgrupos $(H \rtimes \{1\})$ por $\{1\} \rtimes Q$.

Demonstração. Ver Sgobbi (2017), Proposição 1.8. □

Segue da última proposição que todo produto semidireto interno é um produto semidireto (externo). Iremos a partir de agora confundir os dois conceitos e eventualmente escrever $G = H \rtimes Q$ ou $G \cong H \rtimes Q$.

1.4.1 Ação de grupos e produto semidireto

Definição 32. Sejam G um grupo e S um conjunto não vazio. Uma *ação à direita* de G sobre S é uma função $*$: $S \times G \rightarrow S$, onde $*(x, g) = x \cdot g$, satisfazendo as seguintes condições:

- (1) (Compatibilidade) $(x, gh) \mapsto x \cdot (gh) = (x \cdot g) \cdot h, \forall x \in S, \forall g, h \in G$;
- (2) (Identidade) $(x, 1_G) \mapsto x \cdot 1_G = x, \forall x \in S$ e 1_G é o elemento identidade de G .

Dizemos que G *age sobre S* e para simplificar a notação escrevemos xg no lugar de $x \cdot g$.

Observação 5. Na Definição 29, dados grupos H, Q e um homomorfismo arbitrário

$$\begin{aligned} \sigma: Q &\rightarrow \text{Aut}(H) \\ q &\mapsto \sigma(q): H \rightarrow H \\ h &\mapsto \sigma(q)(h), \end{aligned} \tag{1.7}$$

para todo $h \in H$ e $q \in Q$, observemos que dados q_1 e q_2 em Q , temos que $q_1 q_2 \in Q$ e o automorfismo $\sigma(q_1 q_2): H \rightarrow H$ é definido por $\sigma(q_1 q_2)(h) = (\sigma(q_2) \circ \sigma(q_1))(h)$ para todo $h \in H$. Além disso, para $1_Q \in Q$, temos $\sigma(1_Q) = \text{Id}_H: H \rightarrow H$, para todo $h \in H$. Assim, $\sigma(qq^{-1}) = \sigma(q^{-1}q) = \sigma(1_Q) = \text{Id}_H$, para todo $q \in Q$. O homomorfismo $\sigma: Q \rightarrow \text{Aut}(H)$ determina uma ação à direita de Q em H , definida por

$$\begin{aligned} *_\sigma: H \times Q &\rightarrow H \\ (h, q) &\mapsto h \cdot q = hq = \sigma(q)(h), \end{aligned} \tag{1.8}$$

ou seja, a ação leva o par (h, q) na imagem de h pelo automorfismo $\sigma(q)$. Assim, desde que $\sigma(q)$ é um automorfismo para todo $h \in H$ temos, para quaisquer $q_1, q_2 \in Q$ que

- (i) $h \cdot 1_Q = \sigma(1_Q)(h) = Id_H(h) = h$;
- (ii) $(h \cdot q_1) \cdot q_2 = \sigma(q_2)(\sigma(q_1)(h)) = \sigma(q_2)(hq_1) = (hq_1)q_2 = hq_1q_2 = \sigma(q_1q_2)(h) = h \cdot (q_1q_2)$.

Observação 6. Sempre iremos nos referir ao homomorfismo σ como segue. Para cada $q \in Q$, definimos a aplicação que associa a cada h o automorfismo interno

$$\begin{aligned} \sigma: Q &\rightarrow Aut(H) \\ q &\mapsto \sigma_q: H \rightarrow H \\ h &\mapsto \sigma_q(h) = h^q = q^{-1}hq, \end{aligned} \quad (1.9)$$

para todo $h \in H$ e $q \in Q$, satisfazendo, para todo $h \in H$ e todo $q, r \in Q$:

$$\begin{aligned} (\sigma_q \circ \sigma_{q^{-1}})(h) &= \sigma_{q^{-1}q}(h) = (q^{-1}q)^{-1}h(q^{-1}q) = h = (\sigma_{q^{-1}} \circ \sigma_q)(h), \\ (\sigma_q \circ \sigma_r)(h) &= \sigma_q(\sigma_r(h)) = \sigma_q(r^{-1}hr) = q^{-1}(r^{-1}hr)q, \\ \sigma_{rq}(h) &= (rq)^{-1}h(rq) = q^{-1}r^{-1}hrq = q^{-1}(r^{-1}hr)q. \end{aligned} \quad (1.10)$$

O homomorfismo $\sigma: Q \rightarrow Aut(H)$ determina uma ação à direita de Q em H , definida por

$$\begin{aligned} *: H \times Q &\rightarrow H \\ (h, q) &\mapsto \sigma_q(h) = h^q = q^{-1}hq, \end{aligned} \quad (1.11)$$

ou seja, a ação leva o par (h, q) em $q^{-1}hq$, denominada *ação por conjugação*. Logo, σ_q é um automorfismo de grupos e σ é um homomorfismo de grupos denominado *homomorfismo por conjugação*.

1.4.2 Produto semidireto e sequência exata

Definição 33. Uma *sequência exata curta* (de grupos) é uma sequência de homomorfismos de grupos

$$1 \xrightarrow{\varphi} N \xrightarrow{\alpha} G \xrightarrow{\beta} H \xrightarrow{\psi} 1, \quad (1.12)$$

onde 1 representa o grupo trivial $\{1\}$, N, G e H são grupos quaisquer, as setas são homomorfismos de grupos e valem as seguintes igualdades: $Im(\varphi) = Ker(\alpha)$, $Im(\alpha) = Ker(\beta)$ e $Im(\beta) = Ker(\psi)$.

Observação 7. Seja N um subgrupo normal de um grupo G , pode-se considerar a sequência exata curta $1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \rightarrow 1$ onde i é a inclusão e π é a projeção canônica.

Proposição 17. Se $G = N \rtimes H$, então temos uma sequência exata curta

$$1 \rightarrow N \rightarrow N \rtimes H \rightarrow H \rightarrow 1. \quad (1.13)$$

Definição 34. Dizemos que uma sequência exata $1 \rightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ *cinde* quando existe um homomorfismo $\gamma: H \rightarrow G$ tal que $\beta \circ \gamma = Id_H$.

Exemplo 5. Toda sequência exata $1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$, onde H é um grupo livre, *cinde*. De fato, tome X a base de H . Dado $x \in X$, como β é sobrejetor, defina $\varphi: X \rightarrow G$ por $\varphi(x) = \beta^{-1}(x)$ onde $\beta^{-1}(x)$ é um elemento fixado da imagem inversa de x . Como H é um grupo livre existe uma extensão $\bar{\varphi}: H \rightarrow G$, tal que $\bar{\varphi} \circ i(x) = \varphi(x)$, ou seja, $\bar{\varphi}(x) = \beta^{-1}(x)$ para todo $x \in X$. Então $\beta(\bar{\varphi}(x)) = \beta(\beta^{-1}(x)) = x$, para todo $x \in X$. Portanto o mesmo vale para todo elemento de H e temos que $\beta \circ \bar{\varphi} = Id_H$.

Proposição 18. Se uma sequência exata curta $1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ *cinde*, então $G \cong N \rtimes H$.

Demonstração. Considere o homomorfismo $\gamma: H \rightarrow G$ tal que $\beta \circ \gamma = Id_H$. Na verdade, provaremos que G é produto semidireto de $Im(\gamma) \cong H$ e $Im(\alpha) \cong N$ (γ e α são injetoras). Temos que $Im(\alpha) = ker(\beta) \trianglelefteq G$. Basta então provar que $Im(\gamma) \cap Im(\alpha) = \{1\}$ e $G = Im(\gamma)Im(\alpha)$. Para a primeira igualdade, seja $g \in Im(\gamma) \cap Im(\alpha)$. Então, como $Im(\alpha) = Ker(\beta)$, temos $\beta(g) = 1$. Por outro lado, $\gamma(h) = g$ para $h \in H$. Daí $1 = \beta(g) = \beta(\gamma(h)) = h$ e, portanto, $g = \gamma(1) = 1$. Para a segunda igualdade, tome $g \in G$ qualquer e escreva $g = (\gamma \circ \beta(g))(\gamma \circ \beta(g))^{-1}(g)$. Agora note que a parte da direita $\gamma \circ \beta(g) = \gamma(\beta(g)) \in Im(\gamma)$ e a parte restante da esquerda $(\gamma \circ \beta(g))^{-1}(g) \in Im(\alpha) = ker(\beta)$, pois $\beta((\gamma \circ \beta(g))^{-1}(g)) = \beta((\gamma \circ \beta(g))^{-1})\beta(g) = \beta(g)^{-1}\beta(g) = 1$. $\square$

1.5 Anéis, ideais e grupo das unidades

As definições desta seção se encontram em [Garcia e Lequain \(2012\)](#) e [Tengan e Borges \(2015\)](#).

Definição 35. Um *anel* ou *anel comutativo* $(A, +, \cdot)$ é um conjunto A com pelo menos dois elementos, munido de uma operação denotada por $+$ (chamada adição) e de outra operação denotada por $\cdot$ (chamada multiplicação) que satisfazem as condições seguintes:

A1) A adição é associativa, isto é,

$$\forall x, y, z \in A, \quad (x + y) + z = x + (y + z).$$

A2) Existe um elemento neutro com respeito à adição, isto é,

$$\exists 0 \in A \quad \text{tal que, } \forall x \in A, \quad 0 + x = x \quad \text{e} \quad x + 0 = x.$$

A3) Todo elemento de A possui um inverso com respeito à adição, isto é,

$$\forall x \in A, \exists z \in A \quad \text{tal que} \quad x + z = 0 \quad \text{e} \quad z + x = 0.$$

A4) A adição é comutativa, isto é,

$$\forall x, y \in A, \quad x + y = y + x.$$

M1) A multiplicação é associativa, isto é,

$$\forall x, y, z \in A, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

M2) Existe um elemento neutro com respeito à multiplicação, isto é,

$$\exists 1 \in A \text{ tal que, } \forall x \in A, \quad 1 \cdot x = x \text{ e } x \cdot 1 = x.$$

M3) A multiplicação é comutativa, isto é,

$$\forall x, y \in A, \quad x \cdot y = y \cdot x$$

M4) A multiplicação é distributiva em relação à adição, isto é,

$$\forall x, y, z \in A, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$$

Se todas as condições são satisfeitas com exceção de M3), então $(A, +, \cdot)$ é chamado *anel não comutativo*.

Exemplo 6. O conjunto dos números inteiros $\mathbb{Z}$ com as operações de adição e multiplicação usuais é um anel.

Definição 36. Dado um grupo G e um anel R , o *anel de grupo* RG é o conjunto de todas as expressões da forma

$$\alpha = \sum_{g \in G} a_g g$$

onde $a_g \in R$ e somente um número finito dos elementos a_g são não nulos, com operações definidas por:

$$\alpha + \beta = \left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g;$$

$$\alpha \beta = \left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) (gh).$$

Observação 8. 1. Podemos escrever o produto $\alpha \beta$ como $\sum_{u \in G} C_u u$, onde $C_u = \sum_{gh=u} a_g b_h$;

2. RG é um anel;

3. Dados $\alpha \in RG$ e $\lambda \in R$, escrevemos uma multiplicação

$$\lambda \cdot \alpha = \lambda \sum_{g \in G} a_g g = \sum_{g \in G} (\lambda a_g) g.$$

Definição 37. Seja A um anel. Um elemento $u \in A$ é uma *unidade* se possui inverso multiplicativo em A , ou seja, se existe um elemento $v \in A$ tal que $uv = vu = 1$. O conjunto de todas as unidades de A

$$A^* = \{u \in A; \exists v \in A \text{ tal que } uv = vu = 1\}$$

forma um grupo $(A^*, \cdot)$, chamado *grupo das unidades de A* .

Exemplo 7. O grupo das unidades de RG é dado por:

$$RG^* = \{\alpha \in RG; \exists \beta \in RG \text{ tal que } \alpha\beta = \beta\alpha = 1\}.$$

Definição 38. Seja A um anel. Um elemento $a \in A$ é chamado

- *divisor de zero* se existe $b \neq 0$ tal que $ab = 0$.
- *nilpotente* se possui alguma potência nula, isto é, $a^n = 0$ para algum $n \in \mathbb{N}$.

Definição 39. Seja $(A, +, \cdot)$ um anel e seja I um subconjunto não vazio de A . Dizemos que I é um *ideal à esquerda de A* se,

1. $x + y \in I, \forall x, y \in I$;
2. $ax \in I, \forall x \in I, \forall a \in A$ (ou simbolicamente $A \cdot I \subset I$).

Analogamente definimos um *ideal à direita J de A* se,

1. $x + y \in J, \forall x, y \in J$;
2. $xa \in J, \forall x \in J, \forall a \in A$ (ou simbolicamente $J \cdot A \subset J$).

Se I é um ideal simultaneamente à direita e à esquerda de um anel A dizemos que I é um *ideal bilateral de A* ou simplesmente *ideal de A* , isto é, $A \cdot I \subset I$ e $I \cdot A \subset I$.

1.6 Ordenação de grupos

Veremos aqui algumas definições e propriedades de grupos ordenáveis. Para mais detalhes, ver [Kassel e Turaev \(2008\)](#).

Definição 40. Seja X um conjunto. Uma *ordem* em X é uma relação binária entre os elementos de X que denotaremos por $\leq$, satisfazendo as seguintes propriedades:

- 1) Reflexividade: $x \leq x$;
- 2) Antissimetria: Se $x \leq y$ e $y \leq x$, então $x = y$;
- 3) Transitividade: Se $x \leq y$ e $y \leq z$, então $x \leq z$;

para todo $x, y, z \in X$.

O conjunto X munido da ordem $\leq$ é dito ser um *conjunto ordenado* e o mesmo é denotado pelo par $(X, \leq)$.

Definição 41. Uma *ordem estrita* em um conjunto X é uma relação binária entre os elementos de X , que denotaremos por $<$, satisfazendo as seguintes propriedades:

- 1) $\forall x \in X$, tem-se $x \not< x$;
- 2) $\forall x, y \in X$, se $x < y$ então $y \not< x$;
- 3) $\forall x, y, z \in X$, se $x < y$ e $y < z$ então $x < z$.

Observação 9. Note que se $(X, \leq)$ é um conjunto ordenado, a relação $x < y \Leftrightarrow x \leq y$ e $x \neq y$ é uma ordem estrita em X .

Definição 42. Uma ordem em um conjunto X é dita ser *total* se para todo $x, y \in X$, tivermos $x = y$, $x < y$ ou $x > y$.

Definição 43. Sejam $(X, \leq)$ e $(X', \leq')$ conjuntos ordenados e $f: X \rightarrow X'$ uma aplicação. Dizemos que f *preserva ordem* se $f(x) \leq' f(y)$ para todo $x, y \in X$, tal que $x \leq y$.

Definição 44. Considere G um grupo e $\leq$ uma ordem no conjunto G . Dizemos que $\leq$ é uma *ordem invariante à esquerda* se dados $x, y, z \in G$ tal que $x \leq y$ temos que $zx \leq zy$.

Definição 45. Considere G um grupo e $\leq$ uma ordem no conjunto G . Dizemos que $\leq$ é uma *ordem invariante à direita* se dados $x, y, z \in G$ tal que $x \leq y$ temos que $xz \leq yz$.

Definição 46. Um grupo G é *ordenável* se ele possui uma ordem $\leq$ total invariante à esquerda. Neste caso, $(G, \leq)$ é um *grupo ordenado*.

Definição 47. Seja G um grupo e $\leq$ uma ordem no conjunto G . Dizemos que $\leq$ é uma *ordem bi-invariante* se for invariante à esquerda e à direita.

Definição 48. Um grupo G é *bi-ordenável* se ele possui uma ordem total bi-invariante.

Note que se um grupo G tem uma ordem total invariante à esquerda então G admite também uma ordem total invariante à direita $\leq'$ definida por $x \leq' y$ se $x^{-1} \leq y^{-1}$ para todo $x, y \in G$.

Exemplo 8. O conjunto dos números reais é um grupo ordenável, pois basta considerá-lo munido da ordem padrão.

Definição 49. Sejam $(G_i, \leq_i)$ grupos ordenados e considere $G = G_1 \times G_2 \times \cdots \times G_r$. Definimos uma ordem $\leq$ em G da seguinte forma: dados $x = (x_1, \dots, x_r)$ e $y = (y_1, \dots, y_r)$, $x \leq y$ se uma das seguintes condições ocorrer: $x_i = y_i$ para todo $i \in \{1, \dots, r\}$ ou se existir $k \in \{1, \dots, r\}$ tal que $x_i = y_i$ para todo $i < k$ e $x_k <_k y_k$. A ordem $\leq$ assim definida é denominada *ordem lexicográfica*.

Lema 1. Sejam $(G_i, \leq_i)$ grupos ordenados para $i = 1, \dots, r$. Então o produto direto $G = G_1 \times G_2 \times \cdots \times G_r$ é ordenável.

Demonstração. Considere $\leq$ a ordem lexicográfica em G . Devemos mostrar que tal ordem é total invariante à esquerda. A ordem $\leq$ é total, pois a ordem $\leq_i$ de G_i é total para todo $i \in \{1, \dots, r\}$. Provemos que é invariante à esquerda, de fato, sejam $x = (x_1, \dots, x_r)$, $y = (y_1, \dots, y_r)$ e $z = (z_1, \dots, z_r)$ em G . Suponha que $x \leq y$, então $x_i = y_i$ para todo $i \in \{1, \dots, r\}$ ou existe $k \in \{1, \dots, r\}$ tal que $x_i = y_i$ para todo $i < k$ e $x_k <_k y_k$. No primeiro caso temos que $x = y$, logo $zx = zy$ e no segundo caso temos que $z_i x_i = z_i y_i$ para todo $i < k$ e $z_k x_k <_k z_k y_k$ e utilizando a invariância à esquerda de $\leq_k$, portanto, $zx \leq zy$. $\square$

Lema 2. Sejam G um grupo e H um subgrupo normal de G . Se H e G/H têm ordens totais invariantes à esquerda, então G possui uma única ordem total invariante à esquerda tal que as aplicações inclusão $i: H \rightarrow G$ e projeção canônica $p: G \rightarrow G/H$ preservam a ordem. Além disso, se as ordens de H e G/H são bi-invariantes e $zxz^{-1} > 1$ para todo $z \in G$ e $x \in H$ com $x > 1$, então a ordem em G é bi-invariante.

Demonstração. Como H e G/H por hipótese possuem uma ordem total invariante à esquerda, temos que são conjuntos ordenados e os denotamos por $(H, \leq_H)$ e $(G/H, \leq_{G/H})$. Podemos definir uma ordem $\leq_G$ total invariante à esquerda em G da seguinte forma:

Dados $x, y \in G$ dizemos que $x \leq_G y$ se

$$p(x) <_{G/H} p(y) \text{ ou se } p(x) = p(y) \text{ e } 1 \leq_H x^{-1}y, \quad (1.14)$$

onde p é a projeção canônica de G em G/H .

De fato, se $\leq_G$ preserva a ordem na inclusão $i: H \rightarrow G$ e na projeção $p: G \rightarrow G/H$, então tal ordem necessariamente satisfaz (1.14).

Agora assumamos que as ordens $\leq_H$ e $\leq_{G/H}$ são bi-invariantes e ainda vale que se $1 <_H x$ então $1 <_G zxz^{-1}$ para todo $z \in G$. Vamos provar que $\leq_G$ é invariante à direita.

Seja $x \leq_G y$, então $p(x) <_{G/H} p(y)$ ou $p(x) = p(y)$ e $1 \leq_H x^{-1}y$. No primeiro caso, usando a invariância à direita da ordem em G/H temos que $p(xy) = p(x)p(z) <_{G/H} p(y)p(z) = p(yz)$, para todo $z \in G$. Já no segundo caso, usando novamente a invariância à direita de $\leq_{G/H}$ temos que $p(xz) = p(x)p(y) = p(y)p(z) = p(yz)$ e como por hipótese a conjugação por um elemento de H positivo ainda é positiva, segue que $(xz)^{-1}(yz) = z^{-1}(x^{-1}y)z \geq_G 1$. Então de ambos os casos temos que $xz \leq_G yz$. $\square$

Definição 50. Seja G um grupo e $\mathcal{P}$ um subconjunto de G . Definimos $\mathcal{P}^{-1} = \{x \in G; x^{-1} \in \mathcal{P}\}$ e $\mathcal{P}^2 = \{z \in G; \text{existem } x, y \in \mathcal{P} \text{ com } z = xy\}$.

Lema 3. Dado qualquer subconjunto $\mathcal{P}$ de um grupo G , temos que $\mathcal{P} \cap \{1\} = \emptyset$ se, e somente se, $\mathcal{P}^{-1} \cap \{1\} = \emptyset$. E se tivermos $\mathcal{P} \cap \mathcal{P}^{-1} = \emptyset$ então $\mathcal{P} \cap \{1\} = \emptyset$. Além disso, se $\mathcal{P}^2 \subset \mathcal{P}$ e $\mathcal{P} \cap \{1\} = \emptyset$ então $\mathcal{P} \cap \mathcal{P}^{-1} = \emptyset$.

Demonstração. Ver [Kassel e Turaev \(2008\)](#), Lema 7.2. □

Lema 4. Seja $\leq$ uma ordem invariante à esquerda em um grupo G e seja $\mathcal{P} = \{x \in G; x > 1\}$. Então $\mathcal{P}^{-1} = \{x \in G; x < 1\}$, $\mathcal{P}^2 \subset \mathcal{P}$ e $\mathcal{P} \cap \{1\} = \mathcal{P}^{-1} \cap \{1\} = \mathcal{P} \cap \mathcal{P}^{-1} = \emptyset$. Se a ordem $\leq$ é total, então $\mathcal{P} \cup \{1\} \cup \mathcal{P}^{-1} = G$.

Demonstração. Ver [Kassel e Turaev \(2008\)](#), Lema 7.3. □

Definição 51. Um subconjunto $\mathcal{P}$ de um grupo G é dito ser um *cone positivo* em G se $\mathcal{P}^2 \subset \mathcal{P}$ e $G \setminus \{1\}$ é a união de $\mathcal{P}$ e $\mathcal{P}^{-1}$.

Assim, podemos dizer que $\mathcal{P} = \{x \in G; x > 1\}$ é um cone positivo de G , no caso em que a ordem $\leq$ é total.

Teorema 4. Seja $\mathcal{P}$ um subconjunto de um grupo G tal que $\mathcal{P}^2 \subset \mathcal{P}$ e $1 \notin \mathcal{P}$. Então G tem uma única ordem invariante à esquerda $\leq$ tal que $\mathcal{P} = \{x \in G; x > 1\}$. Se $z\mathcal{P}z^{-1} \subset \mathcal{P}$ para todo $z \in G$, então a ordem $\leq$ é bi-invariante. Se $\mathcal{P} \cup \{1\} \cup \mathcal{P}^{-1} = G$, então a ordem é total.

Demonstração. Mostraremos a unicidade. Observe que dados x, y em G tais que $x < y$, utilizando a invariância à esquerda da ordem em G temos que $x^{-1}x < x^{-1}y$, o que equivale a afirmar que $1 < x^{-1}y$, ou seja, $x^{-1}y \in \mathcal{P}$.

Logo, definiremos uma ordem invariante à esquerda em G com um cone positivo $\mathcal{P}$ da seguinte forma: Dados $x, y \in G$, diremos que $x \leq y$ se

$$x = y \text{ ou } x^{-1}y \in \mathcal{P}. \quad (1.15)$$

É fácil ver que realmente se trata de uma ordem invariante à esquerda. Pelo [Lema 3](#), se $\mathcal{P}^2 \subset \mathcal{P}$ e $1 \notin \mathcal{P}$, então $\mathcal{P} \cap \{1\} = \mathcal{P}^{-1} \cap \{1\} = \mathcal{P} \cap \mathcal{P}^{-1} = \emptyset$.

A partir desta informação podemos verificar se a ordem definida em (1.15) satisfaz a [Definição 40](#). A reflexividade segue direto da definição. Se $x \leq y$ e $y \leq x$, então $x = y$ ou $x^{-1}y$ e $y^{-1}x$ estão em $\mathcal{P}$. Desde que $y^{-1}x = (x^{-1}y)^{-1}$, obtemos que $x^{-1}y \in \mathcal{P} \cap \mathcal{P}^{-1} = \emptyset$, contradição. Portanto, $x = y$ e a relação é antissimétrica. Agora suponha que $x \leq y$ e $y \leq z$ então $x = y$ ou $x^{-1}y$ e $y^{-1}z$ estão em $\mathcal{P}$ e neste caso $x^{-1}z = (x^{-1}y)(y^{-1}z) \in \mathcal{P}^2 \subset \mathcal{P}$. Logo, $x \leq z$ e segue que a relação também é transitiva.

Assim, agora podemos verificar se tal ordem é invariante à esquerda. Escolha x, y em G , tal que $x \leq y$, ou seja, $x = y$ ou $x^{-1}y \in \mathcal{P}$. Caso $x = y$, então $zx = zy$ para todo $z \in G$. No caso que $x^{-1}y \in \mathcal{P}$, então $x^{-1}z^{-1}zy = (zx)^{-1}(zy) = x^{-1}y \in \mathcal{P}$ e segue que $zx \leq zy$ para todo $z \in G$.

Agora suponha que $z\mathcal{P}z^{-1} \subset \mathcal{P}$ para todo $z \in G$ e considere x, y em G tais que $x \leq y$. Então

$x = y$ ou $x^{-1}y \in \mathcal{P}$. No caso em que $x = y$ temos que $xz = yz$ para todo $z \in G$ e se $x^{-1}y \in \mathcal{P}$, $z^{-1}x^{-1}yz = (xz)^{-1}yz \in \mathcal{P}$ e, portanto, $xz \leq yz$ para todo $z \in G$ e a ordem é invariante à direita. Se $\mathcal{P} \cup \{1\} \cup \mathcal{P}^{-1} = G$, então para todo $x, y \in G$, $x^{-1}y \in \mathcal{P}$, $x^{-1}y \in \mathcal{P}^{-1}$ ou $x^{-1}y = 1$. Se $x^{-1}y \in \mathcal{P}$, então $x < y$ e se $x^{-1}y \in \mathcal{P}^{-1}$ tem-se que $(x^{-1}y)^{-1} = y^{-1}x \in \mathcal{P}$ e daí $y < x$. Ainda, se $x^{-1}y = 1$, temos que $x = y$. Portanto, a ordem é total. $\square$

1.6.1 Propriedades de grupos ordenáveis

A ordenabilidade implica em consequências relevantes sobre o grupo. A seguir apresentamos algumas dessas consequências, as quais estão presentes em [Kassel e Turaev \(2008\)](#):

Proposição 19. Seja $(G, \leq)$ um grupo ordenável, então G é livre de torção.

Demonstração. Dados $g \in G \setminus \{1_G\}$ e um inteiro $n \geq 1$ devemos mostrar que $g^n \neq 1_G$. Suponha que $1 < g$, então pela invariância à esquerda de $\leq$ temos que

$$g^{n-1}1 < g^{n-1}g = g^n \quad (1.16)$$

para qualquer $n \geq 1$. Por indução, obtemos que $1 < g < g^n$, consequentemente $g^n \neq 1$. Caso $g < 1$, então $1 < g^{-1}$ e $g^{-n} = (g^{-1})^n \neq 1$. Consequentemente $g^n \neq 1$ para todo $n \geq 1$. $\square$

Proposição 20. Se $(G, \leq)$ é um grupo ordenável e R é um anel sem divisores de zero, então o anel de grupo sobre R , $R[G]$ não tem divisores de zero.

Demonstração. Sejam $w = \sum_{i=1}^p r_i g_i$ e $w' = \sum_{j=1}^q s_j h_j$ elementos não nulos de $R[G]$, ou seja, $g_1, \dots, g_p, h_1, \dots, h_q$ são elementos de G e $r_1, \dots, r_p, s_1, \dots, s_q$ são elementos de R que iremos assumir sendo todos não nulos. Também podemos supor que os elementos h_i são numerados de tal forma que $h_1 < h_2 < \dots < h_q$.

O produto de w por w' é dado por

$$w \cdot w' = \sum_{i=1}^p \sum_{j=1}^q (r_i s_j) g_i h_j. \quad (1.17)$$

Pela invariância à esquerda de $\leq$ temos que $g_i h_1 < g_i h_j$ para $i \in \{1, 2, \dots, p\}$ e $j \in \{2, \dots, q\}$. Utilizando a totalidade da ordem encontramos um único i_0 tal que $g_{i_0} h_1 < g_i h_1$ para todo $i \neq i_0$. Afirmamos que $(i_0, 1)$ é o menor e único par (i, j) tal que $g_{i_0} h_1 = g_i h_j$ em G . De fato, observamos que $g_{i_0} h_1 < g_{i_0} h_j$ para todo $j \neq 1$ e, se $i \neq i_0$, obtemos $g_{i_0} h_1 < g_i h_1 < g_i h_j$. Portanto, o coeficiente de $g_{i_0} h_1$ em $ww' \in R[G]$ é $r_{i_0} s_1$, que é não nulo, desde que R não tem divisores de zero. Consequentemente, $ww' \neq 0$. $\square$

Proposição 21. Seja $(G, \leq)$ um grupo bi-ordenável. Então G possui raízes únicas, isto é, para todo $x, y \in G$ e todo $n \in \mathbb{Z}$, $x^n = y^n$ somente quando $x = y$.

Demonstração. Em um grupo bi-ordenável se tivermos $x < y$ e $x' < y'$ temos $xx' < yy'$. De fato, pela invariância à direita $x < y$ implica que $xx' < yx'$ e pela invariância à esquerda $x' < y'$ implica que $yx' < yy'$, assim, pela transitividade de $\leq$ obtemos $xx' < yy'$. E por indução temos que se $x < y$ então $x^n < y^n$ para qualquer inteiro n .

Agora sejam $x, y \in G$ tais que $x^n = y^n$. Desde que a ordem $\leq$ é total, temos que $x = y$, $x < y$ ou $y < x$.

Pela observação feita no primeiro parágrafo, devemos ter $x = y$. □

GRUPO DE TRANÇAS

Neste capítulo introduzimos o conceito de trança geométrica, construímos o grupo de tranças e estabelecemos uma apresentação deste grupo. Além disso, damos uma apresentação de um subgrupo especial, o subgrupo das tranças puras. A maioria das demonstrações serão omitidas, mas podem ser encontradas em [Murasugi e Kurpita \(1999\)](#).

Também nos dedicamos a apresentar alguns invariantes e a relação de isotopia ambiente.

Definição 52. Sejam X, Y espaços topológicos e uma função contínua injetiva $f: X \rightarrow Y$. Dizemos que f é um *mergulho* se é um homeomorfismo de X em $f(X)$.

Definição 53. Um *arco* no espaço euclidiano $\mathbb{R}^3$ é a imagem de um mergulho $d: I \rightarrow \mathbb{R}^3$ do intervalo unitário $I = [0, 1]$ em $\mathbb{R}^3$. Usaremos a mesma notação para arco e para o correspondente mergulho.

Definição 54. Considere o espaço euclidiano $\mathbb{R}^3$ e o cubo unitário $\mathbb{D} = \{(x, y, z) \in \mathbb{R}^3; 0 \leq x, y, z \leq 1\}$. Tome n pontos $P_1 = (\frac{1}{2}, \frac{1}{n+1}, 1), P_2 = (\frac{1}{2}, \frac{2}{n+1}, 1), \dots, P_n = (\frac{1}{2}, \frac{n}{n+1}, 1)$ na face superior, n pontos $\bar{P}_1 = (\frac{1}{2}, \frac{1}{n+1}, 0), \bar{P}_2 = (\frac{1}{2}, \frac{2}{n+1}, 0), \dots, \bar{P}_n = (\frac{1}{2}, \frac{n}{n+1}, 0)$ na face inferior e arcos $d_1, d_2, \dots, d_n$ mergulhados em $\mathbb{R}^3$ unindo os pontos P_i na face superior e $\bar{P}_{\pi(i)}$ na face inferior, onde π é uma permutação de $\{1, 2, \dots, n\}$, satisfazendo:

- (1) $d_i \cap d_j = \emptyset$ para todo $i \neq j$ onde $i, j \in \{1, 2, \dots, n\}$;
- (2) O arco d_i liga P_i a um único ponto $\bar{P}_{\pi(i)}$, onde π é uma permutação de $\{1, 2, \dots, n\}$;
- (3) O plano $z = s$, $0 \leq s \leq 1$, que denotaremos por E_s , é tal que $E_s \cap d_i$ consiste de um único ponto, então o conjunto de arcos $\{d_1, d_2, \dots, d_n\}$ intercepta cada plano E_s em exatamente n pontos distintos.

Cada arco d_i é denominado uma *corda* e o conjunto de arcos satisfazendo as propriedades anteriores é denominado uma *trança geométrica com n cordas*.

Observação 10. Da maneira como definimos, os segmentos deveriam ser poligonais, mas para facilitar a visualização dos diagramas, vamos desenhar estes arcos, como na próxima representação, sendo curvas suaves.

Figura 1 – Uma trança geométrica com n cordas.

Definição 55. Seja β uma trança. Vimos na Definição 54 que a i -ésima corda d_i de β une P_i a $\bar{P}_{\pi(i)}$ para $i = 1, 2, \dots, n$. E π é uma permutação de $\{1, 2, \dots, n\}$. Tal permutação é chamada a *permutação da trança* β .

Denotaremos por 1_n a *trança trivial*, a qual é a trança onde cada arco d_i conecta P_i a $\bar{P}_i$, para todo $i \in \{1, 2, \dots, n\}$, sem cruzamento, como é representado na Figura 2 e por $\mathcal{B}_n$ o conjunto de todas as tranças geométricas com n cordas.

Figura 2 – Trança trivial.

É interessante determinar quando duas tranças podem ser consideradas iguais. Para isso dividiremos $\mathcal{B}_n$ em classes de equivalência, ou seja, duas tranças β e β' serão ditas *as mesmas* se pertencerem à mesma classe de equivalência.

Definição 56. Seja $\mathbb{D}$ um cubo unitário e considere uma trança formada por n cordas d_i , como na Definição 54 (Para fazer sentido esta definição, precisamos trabalhar com as imagens poligonais das cordas). Seja AB uma aresta da corda d e considere C um outro ponto satisfazendo:

- (1) O triângulo $\triangle ABC$ intercepta d somente em AB e não intercepta qualquer outra corda;
- (2) $(AC \cup CB) \cap E_s$ consiste de no máximo um ponto, para todo $s \in [0, 1]$.

Então o *movimento elementar* de uma trança consiste do seguinte procedimento: Substituir AB pelas arestas $AC \cup CB$ ou o contrário como representado na Figura 3. Denotaremos o movimento elementar por Ω e o movimento inverso por Ω^{-1} .

Figura 3 – Movimento elementar.

Observe que os extremos das cordas não são movidos pelo movimento elementar.

Definição 57. Sejam β e β' em $\mathcal{B}_n$. Dizemos que β é *equivalente* a β' se existe uma sequência finita de movimentos elementares ou seus inversos em que β é transformada em β' . Em outros termos,

$$\beta = \beta_0 \xrightarrow{\Omega^{\pm 1}} \beta_1 \xrightarrow{\Omega^{\pm 1}} \beta_2 \xrightarrow{\Omega^{\pm 1}} \dots \xrightarrow{\Omega^{\pm 1}} \beta_m = \beta', \quad (2.1)$$

onde temos que β_i é obtida de β_{i-1} por aplicação de Ω ou Ω^{-1} .

Para indicar que β é equivalente a β' utilizaremos a notação $\beta \sim \beta'$.

Definição 58. A relação $\sim$ definida anteriormente é uma relação de equivalência. O quociente $\mathcal{B}_n / \sim$ é o *conjunto de todas as classes de tranças com n cordas*, o qual é denotado por $\mathbb{B}_n$.

No caso em que suspeitamos que duas tranças β e β' dadas não são equivalentes podemos utilizar a noção de invariante de trança. Calculamos o “valor” em cada trança e se forem diferentes podemos concluir que as tranças não são equivalentes, pois vale a seguinte definição:

Definição 59. Considere $f: \mathcal{B}_n \rightarrow C$, onde C é algum objeto algébrico. Se f satisfaz a propriedade

$$\beta \sim \beta' \Rightarrow f(\beta) = f(\beta'), \quad (2.2)$$

então f é dito ser um *invariante de trança*.

Uma trança com n cordas não é equivalente a uma trança com m cordas se $n \neq m$. De fato, basta notar que em um movimento elementar não é possível acrescentar ou excluir uma corda. Então a quantidade de cordas é um invariante que nos permite dizer que duas tranças não são equivalentes, caso elas tenham um número distinto de cordas.

Além disso, qualquer trança com uma corda é equivalente a uma trança formada por um ponto P_1 na face superior e um ponto $\bar{P}_1$ na face inferior e um segmento de reta de P_1 a $\bar{P}_1$, ou seja, à trança trivial com uma corda.

Definição 60. Seja β uma trança. Podemos obter uma *projeção regular* $p(\beta)$ de β da seguinte maneira: Consideremos a projeção ortogonal de β sobre o plano contendo os pontos $P_1, \dots, P_n, \bar{P}_1, \dots, \bar{P}_n$. É possível mostrar que, aplicando-se um número finito de movimentos elementares pode-se obter um conjunto de curvas $\hat{d}_i$ satisfazendo as seguintes condições:

- (1) Há entre os $\hat{d}_i$, no máximo, um número finito de interseções;
- (2) Se Q é um *ponto de interseção*, então $p^{-1}(Q) \cap \beta$ é exatamente dois pontos, Q também é dito um *ponto duplo*;
- (3) Cada ponto $P_1, \dots, P_n, \bar{P}_1, \dots, \bar{P}_n$ de β nunca é aplicado em um ponto duplo.

Temos que $p(\beta) = \cup \hat{d}_i$ representa a trança β a menos dos pontos duplos. Utilizaremos uma modificação em $p(\beta)$ retirando um pedaço da corda que passa por baixo próximo ao ponto duplo como na próxima figura para indicar qual corda passa por cima e qual passa por baixo.

Figura 4 – Representação geométrica de um cruzamento.

2.1 Grupos de tranças

Recorde que denotamos o conjunto de todas as tranças com n cordas por $\mathcal{B}_n$ e o conjunto de todas as classes de tranças com n cordas por $\mathbb{B}_n$.

Observação 11. Para facilitar a visualização, as próximas representações serão dadas em termo das projeções dos objetos citados.

Definição 61. Sejam $\beta_1, \beta_2 \in \mathcal{B}_n$. O *produto* $\beta_1 \beta_2$ é uma terceira trança com n cordas que dizemos ser o produto de β_1 por β_2 e é obtido através dos seguintes passos:

- 1º) Sejam β_1 e β_2 duas tranças com n cordas e tome os cubos U_1 e U_2 contendo as respectivas tranças em $\mathcal{B}_n$;
- 2º) Identifique o plano inferior de U_1 com o plano superior de U_2 ;
- 3º) Remova o plano de interseção entre os cubos U_1 e U_2 , obtendo U , cubo contendo $\beta_1\beta_2$.

Veja a [Figura 5](#).

Figura 5 – Produto de duas tranças.

Proposição 22. Sejam $\beta, \beta', \bar{\beta}, \bar{\beta}'$ tranças em $\mathcal{B}_n$ tais que $\beta \sim \beta'$ e $\bar{\beta} \sim \bar{\beta}'$. Então $\beta\bar{\beta} \sim \beta'\bar{\beta}'$.

Demonstração. Como $\beta \sim \beta'$, existe uma sequência finita

$$\beta = \beta_0 \xrightarrow{\Omega^{\pm 1}} \beta_1 \xrightarrow{\Omega^{\pm 1}} \dots \xrightarrow{\Omega^{\pm 1}} \beta_m = \beta'.$$

Multiplicando à direita todos os elementos da sequência anterior pelo termo $\bar{\beta}$ temos uma segunda sequência,

$$\beta\bar{\beta} = \beta_0\bar{\beta} \xrightarrow{\Omega^{\pm 1}} \beta_1\bar{\beta} \xrightarrow{\Omega^{\pm 1}} \dots \xrightarrow{\Omega^{\pm 1}} \beta_m\bar{\beta} = \beta'\bar{\beta}.$$

Assim, $\beta\bar{\beta} \sim \beta'\bar{\beta}$.

Como $\bar{\beta} \sim \bar{\beta}'$, por um processo análogo ao anterior, obtemos $\beta'\bar{\beta} \sim \beta'\bar{\beta}'$.

Utilizando a transitividade segue que $\beta\bar{\beta} \sim \beta'\bar{\beta}'$. □

Proposição 23. Sejam β_1, β_2 e β_3 em $\mathcal{B}_n$. Então $(\beta_1\beta_2)\beta_3 \sim \beta_1(\beta_2\beta_3)$, ou seja, no produto de tranças vale a propriedade associativa.

Figura 6 – A associatividade em $\mathcal{B}_n$.

Proposição 24. Dada qualquer trança β em $\mathcal{B}_n$, é válido que $\beta 1_n \sim \beta$ e $\beta \sim \beta 1_n$.

Figura 7 – O elemento neutro em $\mathcal{B}_n$.

Definição 62. Seja β uma trança em $\mathcal{B}_n$ e considere β^{-1} a imagem refletida de β em relação a um plano horizontal $z = 0$. Então β^{-1} é dita a *trança inversa* de β .

Figura 8 – A trança inversa em $\mathcal{B}_n$.

Proposição 25. Para cada trança $\beta \in \mathcal{B}_n$, $\beta \beta^{-1} \sim 1_n$ e $\beta^{-1} \beta \sim 1_n$.

Note que na [Definição 61](#) estabelecemos uma operação no conjunto de todas as tranças geométricas com n cordas $\mathcal{B}_n$, e a partir dela podemos introduzir uma operação no conjunto de todas as classes de tranças com n cordas ($\mathbb{B}_n$) dada por

$$[\beta_1][\beta_2] = [\beta_1\beta_2], \quad (2.3)$$

a qual, pela [Proposição 22](#), está bem definida e, pelas [Proposições 23, 24 e 25](#) temos que tal operação é associativa, admite elemento neutro e inverso. Assim, temos a validade do seguinte teorema:

Teorema 5. $\mathbb{B}_n$ munido da operação definida em (2.3), é um grupo, denominado o *grupo das tranças no disco*.

Observação 12. $\mathbb{B}_1$ é o grupo trivial.

2.2 Apresentação do grupo de tranças

Daremos aqui uma apresentação em termos dos geradores de Artin, representados na [Figura 10](#) e na [Figura 11](#). Artin provou que o grupo de tranças possui uma apresentação como no [Teorema 6](#).

Dada uma trança $\beta \in \mathbb{B}_n$, realizando um ou mais movimentos elementares é possível obter uma partição de β em que cada nível contenha um único ponto duplo como representado a seguir.

Figura 9 – Uma partição de β .

Consideremos as tranças σ_i e σ_i^{-1} ($i = 1, \dots, n-1$) a seguir, chamadas de *tranças elementares*.

Figura 10 – Trança elementar σ_i .

Figura 11 – Trança elementar inversa σ_i^{-1} .

Proposição 26. Dado $\beta \in \mathbb{B}_n$ então $\beta = \sigma_{i_1}^{\varepsilon_1} \sigma_{i_2}^{\varepsilon_2} \cdots \sigma_{i_k}^{\varepsilon_k}$, onde $1 \leq i_1, i_2, \dots, i_k \leq n-1$ e $\varepsilon_i \in \{\pm 1\}$ para $i \in \{1, \dots, k\}$.

A proposição anterior nos diz que o conjunto das tranças elementares $\{\sigma_1, \sigma_2, \dots, \sigma_{n-1}\}$ gera o grupo $\mathbb{B}_n$ e seus elementos são denominados *geradores de Artin*. Assim, chamamos $\mathbb{B}_n$ de *grupo das tranças de Artin com n cordas* ou simplesmente *grupo das tranças no disco*.

Observação 13. (i) Qualquer trança em $\mathbb{B}_2$ é escrita da forma σ_1^k , onde $k \in \mathbb{Z}$, ou seja, σ_1 gera $\mathbb{B}_2$.

(ii) Qualquer trança em $\mathbb{B}_3$ é escrita da forma $\sigma_1^{a_1} \sigma_2^{b_1} \sigma_1^{a_2} \sigma_2^{b_2} \cdots \sigma_1^{a_m} \sigma_2^{b_m}$, onde $a_2, a_3, \dots, a_m, b_1, b_2, \dots, b_{m-1} \in \mathbb{Z} \setminus \{0\}$, e a_1, b_m são inteiros que podem ser iguais a zero.

Uma representação em termos dos geradores de Artin pode não ser única, mais precisamente, vale o seguinte teorema:

Teorema 6. O grupo $\mathbb{B}_n$ para qualquer $n \geq 1$ possui a seguinte apresentação:

$$\mathbb{B}_n = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \left| \begin{array}{ll} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, & 1 \leq i \leq n-2 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & 1 \leq i, j \leq n-1 \text{ e } |j-i| \geq 2 \end{array} \right. \right\rangle. \quad (2.4)$$

As relações da apresentação anterior podem ser visualizadas nas seguintes figuras:

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \text{ se } 1 \leq i \leq n-2. \quad (2.5)$$

Figura 12 – A relação (2.5).

$$\sigma_i \sigma_j = \sigma_j \sigma_i, \text{ se } 1 \leq i, j \leq n-1 \text{ e } |i-j| \geq 2. \quad (2.6)$$

Figura 13 – A relação (2.6).

Note que na Figura 13 o par de cordas i e $i+1$ não interage com o par de cordas j e $j+1$.

Assim, Artin apresentou quais são as relações que definem $\mathbb{B}_n$, isto é, qualquer relação no grupo das tranças é consequência destas duas relações.

O grupo de tranças com infinitas cordas é denotado por $\mathbb{B}_\infty$ e possui uma apresentação com um conjunto infinito de geradores $\{\sigma_1, \sigma_2, \dots\}$ sujeito às mesmas relações.

Observação 14. Utilizando as relações de $\mathbb{B}_n$, temos que $\sigma_i \sigma_{i+1}^l \sigma_i^{-1} = \sigma_{i+1}^{-1} \sigma_i^l \sigma_{i+1}$, com $l \in \mathbb{Z}$.

Dada uma trança com m cordas, se adicionarmos k cordas retas unindo os pontos P_{m+j} à $\bar{P}_{m+j}$ onde $j \in \{1, \dots, k\}$ ainda teremos uma trança, agora com $m+k$ cordas. Para formalizar essa ideia considere a seguinte proposição:

Proposição 27. Se $1 \leq m \leq n$, a aplicação $\psi: \mathbb{B}_m \rightarrow \mathbb{B}_n$ definida por $\psi(\sigma_i) = \sigma_i$, para $i = 1, 2, \dots, m-1$, é um homomorfismo injetor de $\mathbb{B}_m$ em $\mathbb{B}_n$. Assim, $\mathbb{B}_m$ é um subgrupo de $\mathbb{B}_n$.

Figura 14 – Inclusão de $\mathbb{B}_m$ em $\mathbb{B}_n$ com $1 \leq m \leq n$.

Demonstração. Temos que

$$\mathbb{B}_m = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{m-1} \mid \begin{array}{ll} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, & 1 \leq i \leq m-2 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & 1 \leq i, j \leq m-1 \text{ e } |j-i| \geq 2 \end{array} \right\rangle \quad (2.7)$$

e

$$\mathbb{B}_n = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, & 1 \leq i \leq n-2 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & 1 \leq i, j \leq n-1 \text{ e } |j-i| \geq 2 \end{array} \right\rangle. \quad (2.8)$$

Para ψ ser um homomorfismo basta mostrar que toda relação em $\mathbb{B}_m$ permanece válida em $\mathbb{B}_n$, mas por (2.7) e (2.8) isto é válido. Agora mostremos que ψ é injetora. Suponha que $\beta \in \mathbb{B}_m$ é tal que $\psi(\beta) = 1_n$, assim, adicionando $n - m$ cordas simples, a trança é equivalente à trivial. Então existe uma sequência finita

$$\psi(\beta) = \beta_0 \xrightarrow{\Omega^{\pm 1}} \beta_1 \xrightarrow{\Omega^{\pm 1}} \beta_2 \xrightarrow{\Omega^{\pm 1}} \dots \xrightarrow{\Omega^{\pm 1}} \beta_k = 1_n, \quad (2.9)$$

sendo β_i uma trança em $\mathbb{B}_n$ para todo $i \in \{1, \dots, k\}$ e β_{i+1} é obtida de β_i por um movimento elementar.

Observe que se removermos as $n - m$ últimas cordas de cada uma das tranças β_i , obtemos tranças com m cordas as quais serão denotadas por $\bar{\beta}_i$, obtendo assim a seguinte sequência

$$\beta = \bar{\beta}_0 \xrightarrow{\Omega^{\pm 1}} \bar{\beta}_1 \xrightarrow{\Omega^{\pm 1}} \bar{\beta}_2 \xrightarrow{\Omega^{\pm 1}} \dots \xrightarrow{\Omega^{\pm 1}} \bar{\beta}_k = 1_m, \quad (2.10)$$

onde ou $\bar{\beta}_{i+1}$ é obtida aplicando um movimento elementar em $\bar{\beta}_i$ ou é idêntica a $\bar{\beta}_i$. Esta última afirmação ocorre se o movimento elementar foi aplicado na l -ésima corda de β_i , com $m < l \leq n$, da sequência (2.9).

Portanto, $\beta \sim 1_m$ e temos que $\ker(\psi) = \{1_m\}$. □

Como existe um homomorfismo injetor de $\mathbb{B}_n$ em $\mathbb{B}_{n+1}$ podemos identificar $\mathbb{B}_n$ como um subgrupo de $\mathbb{B}_\infty$ gerado por $\sigma_1, \dots, \sigma_{n-1}$.

Proposição 28. Para todo $i \in \{1, \dots, n-1\}$, $\sigma_i \in \mathbb{B}_n$ tem ordem infinita, ou seja, para todo inteiro estritamente positivo k temos $\sigma_i^k \neq 1$.

Demonstração. Como vimos na [Observação 13](#), $\mathbb{B}_2$ é gerado por σ_1 e assim, pelo [Teorema 6](#), $\langle \sigma_1 | - \rangle$ é sua apresentação. Neste caso, como $\mathbb{B}_2$ tem ordem infinita, podemos dizer que $|\sigma_1| = \infty$. Pela [Proposição 27](#) sabemos que para qualquer $n \geq 2$, $\mathbb{B}_n$ contém o grupo $\mathbb{B}_2$. Logo σ_1 é um elemento de $\mathbb{B}_n$ que tem ordem infinita.

Suponha que exista um inteiro estritamente positivo l tal que $\sigma_2^l = 1_n$, ou seja, que σ_2 tem ordem finita. Consequentemente,

$$(\sigma_1 \sigma_2 \sigma_1) \sigma_2^l (\sigma_1 \sigma_2 \sigma_1)^{-1} = 1_n. \quad (2.11)$$

Utilizando a relação dada na [Observação 14](#), obtemos $(\sigma_1 \sigma_2 \sigma_1) \sigma_2^l (\sigma_1 \sigma_2 \sigma_1)^{-1} = \sigma_1^l$, e de (2.11) segue que $\sigma_1^l = 1$, o que contradiz o fato de que a ordem de σ_1 é infinita.

Assuma que para $j \in \{1, 2, \dots, i-1\}$, σ_j tem ordem infinita. Suponha que exista um inteiro estritamente positivo k tal que $\sigma_i^k = 1_n$, então utilizando processo análogo ao realizado para σ_2 temos que $\sigma_{i-1}^k = 1_n$, o que contradiz nossa hipótese.

Portanto σ_i tem ordem infinita para todo $i \geq 1$. □

Observação 15. Tranças equivalentes têm mesma permutação (ver [Definição 55](#)), assim temos uma aplicação $p: \mathbb{B}_n \rightarrow \mathbb{S}_n$, onde $\mathbb{S}_n$ é o grupo das permutações de $\{1, 2, \dots, n\}$.

Definição 63. Uma trança $\beta \in \mathbb{B}_n$ é dita *pura* se sua permutação é trivial.

Proposição 29. Seja $\mathbb{B}_n$ o grupo das tranças com n cordas, onde $n \geq 1$. O conjunto de todas as tranças puras, denotado por $\mathbb{P}_n$, é um subgrupo de $\mathbb{B}_n$. Além disso, existe um isomorfismo entre o grupo quociente $\mathbb{B}_n/\mathbb{P}_n$ e $\mathbb{S}_n$ e, conseqüentemente, $[\mathbb{B}_n : \mathbb{P}_n] = n!$.

Demonstração. Considere a seguinte aplicação

$$\begin{aligned} p: \mathbb{B}_n &\rightarrow \mathbb{S}_n \\ \beta &\mapsto p(\beta), \end{aligned}$$

onde $p(\beta)$ é a permutação de β . Temos que $\ker(p) = \mathbb{P}_n$ e portanto $\mathbb{P}_n$ é um subgrupo normal de $\mathbb{B}_n$. Além disso, p é um homomorfismo sobrejetor. Portanto, pelo Teorema do Homomorfismo, o quociente $\mathbb{B}_n/\mathbb{P}_n$ é isomorfo à imagem de p , que é $\mathbb{S}_n$. E como $\mathbb{P}_n$ é um subgrupo normal de $\mathbb{B}_n$ resulta que $[\mathbb{B}_n : \mathbb{P}_n] = |\mathbb{B}_n/\mathbb{P}_n| = |\mathbb{S}_n| = n!$. $\square$

Como o grupo das tranças puras é normal ao grupo de todas as tranças, ou seja, $\mathbb{P}_n \trianglelefteq \mathbb{B}_n$ e vale que $\mathbb{B}_n/\mathbb{P}_n \cong \mathbb{S}_n$, podemos construir a seguinte sequência exata curta

$$1 \rightarrow \mathbb{P}_n \xrightarrow{i} \mathbb{B}_n \xrightarrow{p} \mathbb{S}_n \rightarrow 1. \quad (2.12)$$

2.3 Apresentação do grupo das tranças puras

Uma apresentação de $\mathbb{P}_n$ pode ser encontrada utilizando-se o método de Reidemeister-Schreier que pode ser visto em [Murasugi e Kurpita \(1999\)](#).

Teorema 7. O grupo das tranças puras $\mathbb{P}_n$ é um grupo com geradores $A_{i,j}$ para $1 \leq i < j \leq n$ e relações:

$$A_{r,s}^{-1} A_{i,j} A_{r,s} = \begin{cases} A_{i,j}, & \text{se } s < i \text{ ou } i < r < s < j, \\ A_{r,j} A_{i,j} A_{r,j}^{-1}, & \text{se } s = i, \\ A_{r,j} A_{s,j} A_{i,j} A_{s,j}^{-1} A_{r,j}^{-1}, & \text{se } i = r < s < j, \\ A_{r,j} A_{s,j} A_{r,j}^{-1} A_{s,j}^{-1} A_{i,j} A_{s,j} A_{r,j} A_{s,j}^{-1} A_{r,j}^{-1}, & \text{se } r < i < s < j. \end{cases} \quad (2.13)$$

Definimos uma trança pura com n cordas da forma $A_{i,j}$, para $1 \leq i < j \leq n$, como

$$A_{i,j} = (\sigma_{j-1} \sigma_{j-2} \cdots \sigma_{i+1}) \sigma_i^2 (\sigma_{i+1}^{-1} \cdots \sigma_{j-2}^{-1} \sigma_{j-1}^{-1}), \quad (2.14)$$

onde $A_{j,j} = 1$.

2.4 Isotopia de tranças

Definição 64. Sejam β e β' em $\mathcal{B}_n$. Uma *isotopia ambiente* é um homeomorfismo

$$\begin{aligned} H: \mathbb{D} \times [0, 1] &\rightarrow \mathbb{D} \times [0, 1] \\ (x, t) &\mapsto H(x, t) = (h_t(x), t) \end{aligned} \quad (2.15)$$

onde h_t , com $t \in [0, 1]$, são homeomorfismos de $\mathbb{D}$ em $\mathbb{D}$, tal que $h_t|_{\partial\mathbb{D}} = Id: \partial\mathbb{D} \rightarrow \partial\mathbb{D}$, $h_0 = Id: \mathbb{D} \rightarrow \mathbb{D}$ e $h_1(\beta) = \beta'$.

Neste caso dizemos que β é *isotópica ambiente* a β' e denotamos por $\beta \simeq \beta'$.

Se, além das hipóteses acima tivermos que $h_t(\beta)$ é uma trança em $\mathcal{B}_n$ para todo $t \in [0, 1]$, então H é dito ser uma *isotopia forte* ou *s-isotopia* e dizemos que β é *s-isotópica* a β' e denotamos por $\beta \stackrel{s}{\simeq} \beta'$.

As relações de “ser isotópico à” e “s-isotópico à” são relações de equivalência.

Teorema 8. As seguintes afirmações são equivalentes:

- (1) β é equivalente à β' ;
- (2) β é isotópica ambiente à β' ;
- (3) Existe um homeomorfismo $h: \mathbb{D} \rightarrow \mathbb{D}$ tal que
 - (i) $h(\beta) = \beta'$;
 - (ii) $h|_{\partial\mathbb{D}} = Id$;
- (4) $\beta \stackrel{s}{\simeq} \beta'$.

O Teorema anterior fornece várias interpretações para quando podemos dizer que β e β' representam a mesma trança.

GRUPO DE HOMOTOPIA DE TRANÇAS PURAS NO DISCO

Neste capítulo introduzimos o conceito de homotopia e a questão de Artin se dadas duas tranças β e β' homotópicas, as mesmas também são equivalentes (isotópicas ambiente). Em [Goldsmith \(1974\)](#) obtemos a resposta, onde a autora descreve o grupo de classes de homotopia de tranças puras no disco como um certo quociente do grupo de tranças puras discutido na [Seção 2.3](#).

Na próxima seção será definido um invariante completo no grupo de tranças, denominado o conjunto de palavras associado a uma trança.

3.1 Representação de tranças por automorfismos de grupos livres

Seja $F(n)$ um grupo livre (relembre a notação estabelecida na [Observação 2](#), onde $X = \{x_1, \dots, x_n\}$ é o conjunto de geradores). Em [Artin \(1947\)](#), temos que o grupo de tranças no disco $\mathbb{B}_n$ é isomorfo ao subgrupo do grupo dos automorfismos $h \in \text{Aut}(F(n))$ da forma $h(x_i) = w_j x_j w_j^{-1}$, onde w_j é uma palavra em $F(n)$, satisfazendo $h(x_1 x_2 \cdots x_n) = x_1 x_2 \cdots x_n$.

Teorema 9 (Teorema de Representação de Artin). Sejam $F(n)$ um grupo livre, onde $X = \{t_1, \dots, t_n\}$ é o conjunto de geradores com $n \geq 1$ fixo, e $\text{Aut}(F(n))$ o grupo dos automorfismos de $F(n)$. Então $\mathbb{B}_n$ é isomorfo ao subgrupo de $\text{Aut}(F(n))$ formado por todos os automorfismos $\bar{\beta}$ de $F(n)$ tais que

$$(1) \quad \bar{\beta}(t_i) = w_i t_{\pi(i)} w_i^{-1}, \text{ para } 1 \leq i \leq n,$$

$$(2) \quad \bar{\beta}(t_1 \cdots t_n) = t_1 \cdots t_n,$$

onde π é uma permutação em $\mathbb{S}_n$ e cada w_i é um elemento de $F(n)$.

Seja $\phi: \mathbb{B}_n \rightarrow \text{Aut}(F(n))$ definido nos geradores σ_k e em seus inversos σ_k^{-1} para $1 \leq k \leq n-1$ por:

$$\overline{\sigma}_k = \phi(\sigma_k): \begin{cases} t_i & \mapsto t_i, \text{ se } i \neq k, k+1 \text{ com } 1 \leq i \leq n, \\ t_k & \mapsto t_{k+1}, \\ t_{k+1} & \mapsto t_{k+1}t_k t_{k+1}^{-1}, \end{cases} \quad (3.1)$$

e

$$\overline{\sigma}_k^{-1} = \phi(\sigma_k^{-1}): \begin{cases} t_i & \mapsto t_i, \text{ se } i \neq k, k+1, \text{ com } 1 \leq i \leq n, \\ t_k & \mapsto t_k t_{k+1} t_k^{-1}, \\ t_{k+1} & \mapsto t_k. \end{cases} \quad (3.2)$$

Não faremos a demonstração detalhada de que ϕ é um isomorfismo (para uma demonstração, veja [Birman \(1974\)](#)), notemos, no entanto, que $X = \{\sigma_1, \sigma_2, \dots, \sigma_{n-1}\}$ gera $\mathbb{B}_n$ e que as relações $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ para $i = 1, \dots, n-2$ e $\sigma_i \sigma_j = \sigma_j \sigma_i$, $1 \leq i, j \leq n-1$ e $|j-i| \geq 2$ continuam valendo para os automorfismos $\overline{\sigma}_k = \phi(\sigma_k)$.

De fato, temos que se $j \neq i, i+1$

$$\begin{aligned} \overline{\sigma_i \sigma_{i+1} \sigma_i} &= \phi(\sigma_i \sigma_{i+1} \sigma_i): t_j \xrightarrow{\sigma_i} t_j \xrightarrow{\sigma_{i+1}} t_j \xrightarrow{\sigma_i} t_j \\ \overline{\sigma_{i+1} \sigma_i \sigma_{i+1}} &= \phi(\sigma_{i+1} \sigma_i \sigma_{i+1}): t_j \xrightarrow{\sigma_{i+1}} t_j \xrightarrow{\sigma_i} t_j \xrightarrow{\sigma_{i+1}} t_j \end{aligned} \quad (3.3)$$

e para $j = i$ e $j = i+1$, temos

$$\begin{aligned} \overline{\sigma_i \sigma_{i+1} \sigma_i} &= \phi(\sigma_i \sigma_{i+1} \sigma_i): t_i \xrightarrow{\sigma_i} t_{i+1} \xrightarrow{\sigma_{i+1}} t_{i+2} \xrightarrow{\sigma_i} t_{i+2} \\ \overline{\sigma_{i+1} \sigma_i \sigma_{i+1}} &= \phi(\sigma_{i+1} \sigma_i \sigma_{i+1}): t_i \xrightarrow{\sigma_{i+1}} t_i \xrightarrow{\sigma_i} t_{i+1} \xrightarrow{\sigma_{i+1}} t_{i+2} \end{aligned} \quad (3.4)$$

$$\begin{aligned} \overline{\sigma_i \sigma_{i+1} \sigma_i} &= \phi(\sigma_i \sigma_{i+1} \sigma_i): t_{i+1} \xrightarrow{\sigma_i} t_{i+1}^{-1} t_i t_{i+1} \xrightarrow{\sigma_{i+1}} t_{i+2}^{-1} t_i t_{i+2} \xrightarrow{\sigma_i} t_{i+2}^{-1} t_{i+1} t_{i+2} \\ \overline{\sigma_{i+1} \sigma_i \sigma_{i+1}} &= \phi(\sigma_{i+1} \sigma_i \sigma_{i+1}): t_{i+1} \xrightarrow{\sigma_{i+1}} t_{i+2} \xrightarrow{\sigma_i} t_{i+2} \xrightarrow{\sigma_{i+1}} t_{i+2}^{-1} t_{i+1} t_{i+2}. \end{aligned} \quad (3.5)$$

De (3.3), (3.4) e (3.5) obtemos que $\phi(\sigma_i \sigma_{i+1} \sigma_i) = \phi(\sigma_{i+1} \sigma_i \sigma_{i+1})$ para $i = 1, \dots, n-2$ e de maneira análoga obtemos que $\phi(\sigma_i \sigma_j) = \phi(\sigma_j \sigma_i)$, sempre que $|j-i| \geq 2$, onde $1 \leq i, j \leq n-1$.

Exemplo 9. Seja β uma trança com 3 cordas dada por $\beta = \sigma_1 \sigma_2$, como na representação a seguir.

Figura 16 – Trança β .

Temos que

$$\phi(\sigma_1\sigma_2)(t_1) = \phi(\sigma_1)(\phi(\sigma_2)(t_1)) = \phi(\sigma_1)(t_1) = t_2, \quad (3.6)$$

$$\phi(\sigma_1\sigma_2)(t_2) = \phi(\sigma_1)(\phi(\sigma_2)(t_2)) = \phi(\sigma_1)(t_3) = t_3, \quad (3.7)$$

$$\phi(\sigma_1\sigma_2)(t_3) = \phi(\sigma_1)(\phi(\sigma_2)(t_3)) = \phi(\sigma_1)(t_3^{-1}t_2t_3) = t_3^{-1}t_2^{-1}t_1t_2t_3. \quad (3.8)$$

Logo $\phi(\beta)(t_1) = t_2$, $\phi(\beta)(t_2) = t_3$ e $\phi(\beta)(t_3) = t_3^{-1}t_2^{-1}t_1t_2t_3$.

Definição 65. Para qualquer trança β com n cordas, o conjunto $\omega_i = \phi(\beta)(t_i)$ para $i = 1, 2, \dots, n$ é o conjunto de *palavras associadas à trança* β . Denotaremos tal conjunto por $\omega(\beta)$.

Exemplo 10. O conjunto de palavras associadas à trança $\beta = \sigma_1\sigma_2$, representada na [Figura 17](#), é $\omega(\beta) = \{t_2, t_3, t_3^{-1}t_2^{-1}t_1t_2t_3\}$.

Note que pelo [Teorema 9](#), duas tranças β e β' são equivalentes se, e somente se, $\omega(\beta) = \omega(\beta')$. Portanto temos que $\omega(\beta)$ é um invariante completo de tranças.

Exemplo 11. Considere $\beta = \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$ e $\beta' = \sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$ em $\mathcal{B}_4$.

Figura 17 – Tranças equivalentes.

Note que $\omega(\beta) = \omega(\beta') = \{\omega_1, \omega_2, \omega_3, \omega_4\} = \{t_3, t_4, t_4^{-1}t_3^{-1}t_2t_3t_4, t_4^{-1}t_3^{-1}t_2^{-1}t_1t_2t_3t_4\}$.

De fato, para a trança β temos:

$$\begin{aligned} \omega_1 &= \tilde{\phi}(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2)(t_1) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(\phi(\sigma_2)(t_1))))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(t_1)))) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(t_1))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(t_2)) = \phi(\sigma_1)(t_3) = t_3, \end{aligned} \quad (3.9)$$

$$\begin{aligned} \omega_2 &= \tilde{\phi}(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2)(t_2) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(\phi(\sigma_2)(t_2))))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(t_3)))) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(t_4))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(t_4)) = \phi(\sigma_1)(t_4) = t_4, \end{aligned} \quad (3.10)$$

$$\begin{aligned} \omega_3 &= \tilde{\phi}(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2)(t_3) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(\phi(\sigma_2)(t_3))))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(t_3^{-1}t_2t_3)))) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(t_4^{-1}t_2t_4))) \\ &= \phi(\sigma_1)(\phi(\sigma_2)(t_4^{-1}t_2^{-1}t_1t_2t_4)) = \phi(\sigma_1)(t_4^{-1}t_3^{-1}t_1t_2t_3t_4) = t_4^{-1}t_3^{-1}t_2t_3t_4, \end{aligned} \quad (3.11)$$

$$\begin{aligned}
\omega_4 &= \tilde{\phi}(\sigma_1 \sigma_2 \sigma_1 \sigma_3 \sigma_2)(t_4) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(\phi(\sigma_2)(t_4))))) \\
&= \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(\phi(\sigma_3)(t_4)))) = \phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_1)(t_4^{-1} t_3 t_4))) \\
&= \phi(\sigma_1)(\phi(\sigma_2)(t_4^{-1} t_3 t_4)) = \phi(\sigma_1)(t_4^{-1} t_3^{-1} t_2 t_3 t_4) = t_4^{-1} t_3^{-1} t_2^{-1} t_1 t_2 t_3 t_4.
\end{aligned} \tag{3.12}$$

E para a trança β' temos:

$$\begin{aligned}
\omega'_1 &= \tilde{\phi}(\sigma_2 \sigma_3 \sigma_1 \sigma_2 \sigma_3)(t_1) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_3)(t_1))))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(t_1)))) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(t_1))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(t_2)) = \phi(\sigma_2)(t_2) = t_3,
\end{aligned} \tag{3.13}$$

$$\begin{aligned}
\omega'_2 &= \tilde{\phi}(\sigma_2 \sigma_3 \sigma_1 \sigma_2 \sigma_3)(t_2) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_3)(t_2))))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(t_2)))) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(t_3))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(t_3)) = \phi(\sigma_2)(t_4) = t_4,
\end{aligned} \tag{3.14}$$

$$\begin{aligned}
\omega'_3 &= \tilde{\phi}(\sigma_2 \sigma_3 \sigma_1 \sigma_2 \sigma_3)(t_3) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_3)(t_3))))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(t_4)))) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(t_4))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(t_4)) = \phi(\sigma_2)(t_4^{-1} t_3 t_4) = t_4^{-1} t_3^{-1} t_2 t_3 t_4,
\end{aligned} \tag{3.15}$$

$$\begin{aligned}
\omega'_4 &= \tilde{\phi}(\sigma_2 \sigma_3 \sigma_1 \sigma_2 \sigma_3)(t_4) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(\phi(\sigma_3)(t_4))))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(\phi(\sigma_2)(t_4^{-1} t_3 t_4)))) = \phi(\sigma_2)(\phi(\sigma_3)(\phi(\sigma_1)(t_4^{-1} t_3^{-1} t_2 t_3 t_4))) \\
&= \phi(\sigma_2)(\phi(\sigma_3)(t_4^{-1} t_3^{-1} t_2^{-1} t_1 t_2 t_3 t_4)) = \phi(\sigma_2)(t_4^{-1} t_3^{-1} t_2^{-1} t_1 t_2 t_3 t_4) = t_4^{-1} t_3^{-1} t_2^{-1} t_1 t_2 t_3 t_4.
\end{aligned} \tag{3.16}$$

Portanto, β e β' são equivalentes.

3.2 Homotopia de tranças

Quando definimos uma trança com n cordas, pedimos que cada plano intermediário interceptasse a trança em somente n pontos. Agora introduzimos uma generalização do conceito de trança, usualmente chamado de *enlaçamento de intervalos*. As figuras adiante são representações de exemplos de enlaçamentos de um e dois intervalos, respectivamente.

Figura 18 – Exemplos de enlaçamentos de intervalos de 1 e 2 intervalos, respectivamente.

Definição 66. Seja $\mathbb{D} = \{(x, y, z) \in \mathbb{R}^3; 0 \leq x, y, z \leq 1\}$ o cubo unitário e tome n pontos $P_1, P_2, \dots, P_n$ em sua face superior e n pontos $\bar{P}_1, \bar{P}_2, \dots, \bar{P}_n$ na face inferior. Um conjunto de arcos simples, mutuamente disjuntos, $d_1, d_2, \dots, d_n$ em $\mathbb{D}$ que unem os pontos $P_1, P_2, \dots, P_n$ aos pontos $\bar{P}_1, \bar{P}_2, \dots, \bar{P}_n$, respectivamente, é chamado um *enlaçamento de n intervalos*.

Uma trança pura é um caso particular de enlaçamento de intervalos em que cada plano E_s , entre as faces superior e inferior do cubo, intercepta os segmentos de arcos em somente n pontos.

Definição 67. Seja γ um enlaçamento de n intervalos em $\mathbb{D}$. Considere também A e B dois pontos em um arco d_i de γ , que determina um segmento de arco AB e seja C um ponto de $\mathbb{D}$, tal que o triângulo $\triangle ABC$ intercepta d_i em AB e pode interceptar d_i em um ponto em seu interior, mas não intercepta qualquer outro intervalo de γ . Então a operação Γ (e sua inversa Γ^{-1}) definida por substituir AB por $AC \cup CB$ (respectivamente, substituir $AC \cup CB$ por AB) é chamada *movimento elementar de homotopia*.

Figura 19 – Movimento elementar de homotopia.

Observação 16. Note que a única condição extra das condições apresentadas na [Definição 56](#) de movimento elementar, é que o triângulo pode interceptar d_i em um ponto em seu interior. Assim a relação de homotopia é mais geral que a relação de isotopia, visto que há enlaçamentos de intervalos que não são isotópicos ambiente a nenhuma trança, mas são homotópicos. O enlaçamento de intervalos apresentado na [Figura 20](#) representa um exemplo que não é isotópico ambiente a uma trança mas é homotópico à trança σ_1^2 .

Essa condição de homotopia nos diz que podemos escolher entre passar por cima ou por baixo em um cruzamento, desde que estejamos tratando da mesma corda. Isso é o mesmo que afirmar que cada corda pode passar através dela mesma, mas não através das outras cordas.

Figura 20 – Enlaçamento de intervalos homotópico à trança σ_1^2 .

Definição 68. Sejam γ e γ' enlaçamentos de intervalos. Dizemos que γ é *homotópico a* γ' se existe uma sequência finita de enlaçamentos de intervalos (γ_i)

$$\gamma = \gamma_0 \rightarrow \gamma_1 \rightarrow \cdots \rightarrow \gamma_m = \gamma', \quad (3.17)$$

tal que γ_{i+1} é isotópico ambiente ou homotópico a γ_i , para todo $i \in \{1, \dots, m\}$.

Assim, dois enlaçamentos de intervalos γ e γ' são ditos *homotopicamente equivalentes* se um pode ser deformado no outro por uma sequência finita de movimentos elementares de homotopia. A relação “ser homotópico à” é uma relação de equivalência.

Uma outra definição equivalente à [Definição 68](#), dada em [Habegger e Lin \(1990\)](#) é a seguinte:

Definição 69. Dados dois enlaçamentos de intervalos σ e σ' , dizemos que eles são *homotópicos* se existe uma homotopia de suas cordas em $\mathbb{D} \times I$, fixando os extremos e deformando σ em σ' , tal que a imagem de cordas diferentes permanecem disjuntas durante esta deformação.

Como uma trança pura é em particular um enlaçamento de intervalos temos uma noção de equivalência homotópica utilizando a definição anterior para tranças puras β e β' em $\mathcal{B}_n$, ou seja, dizemos que β é *homotópica* à β' se existir uma sequência finita de enlaçamentos de intervalos $\beta = \gamma_0 \rightarrow \gamma_1 \rightarrow \dots \rightarrow \gamma_m = \beta'$, tal que γ_{i+1} é isotópico ambiente ou homotópico à γ_i , para todo $i \in \{1, \dots, m\}$. Sendo β homotópica à β' , como homotopia de tranças é uma relação de equivalência, diremos que β é *homotopicamente equivalente* à β' .

O conjunto de todas as classes de enlaçamentos de n intervalos sobre o disco com a relação de homotopia é um grupo denotado por $\hat{\mathbb{P}}\mathcal{B}_n(\mathbb{D})$, com o produto definido como em [\(2.3\)](#) para classes de isotopia de tranças e é chamado *grupo de classes de enlaçamentos de n intervalos sobre o disco*.

Graças ao seguinte resultado, todo enlaçamento de intervalos é homotópico à uma trança pura, ou seja, toda classe de enlaçamentos de intervalos possui um representante sendo uma trança pura, então podemos dizer que $\hat{\mathbb{P}}\mathcal{B}_n(\mathbb{D})$ é o *grupo de homotopia de tranças puras no disco*.

Teorema 10. Todo enlaçamento de n intervalos sobre $\mathbb{D}$ é homotópico a uma trança pura.

Demonstração. Ver em [Habegger e Lin \(1990, p. 399\)](#). □

O próximo exemplo trata de uma trança que é homotopicamente trivial, porém não é equivalente à trança trivial. Este exemplo se encontra esquematizado em [Goldsmith \(1974\)](#). Logo, os conceitos de isotopia ambiente e homotopia não são equivalentes.

Exemplo 12. A trança $\beta = \sigma_1 \sigma_2^2 \sigma_1^2 \sigma_2^{-2} \sigma_1^{-2} \sigma_2^2 \sigma_1^{-2} \sigma_2^{-2} \sigma_1$ em $\mathcal{B}_3$ representada na [Figura 21](#) é homotopicamente trivial, mas não é equivalente à trança trivial.

A afirmação de que é homotopicamente trivial é demonstrado na [Figura 22](#), entretanto, tal trança não é equivalente à trança trivial, como vemos no [Exemplo 13](#).

Figura 21 – Trança β que é homotopicamente trivial. Figura 22 – Sequência de movimentos elementares de homotopia em β .

Vimos que se duas tranças são isotópicas ambiente, então as mesmas são homotópicas. Assim, podemos afirmar que todo invariante homotópico é um invariante de trança, entretanto nem todo invariante de trança é um invariante homotópico, como o conjunto de palavras associadas a uma trança da [Definição 65](#).

Exemplo 13. Seja β uma trança em $\mathbb{B}_n$. Vimos que o conjunto de palavras $\omega(\beta)$ associada à β é um invariante de trança, porém não é um invariante homotópico. De fato, considere a trança em $\mathbb{B}_3$ representada na [Figura 21](#). Mostramos que tal trança é homotopicamente trivial, mas, utilizando a [Definição 65](#), obtemos que $\omega(\beta) = \{\omega_1, \omega_2, \omega_3\}$, com $\omega_i \neq t_i$.

Além da [Definição 66](#), podemos dar uma definição equivalente para um enlaçamento de intervalos em termos de um mergulho próprio linear por partes.

Definição 70. Sejam X e Y espaços topológicos. Uma função contínua $f: X \rightarrow Y$ é *própria* se a pré-imagem de um conjunto compacto em Y é um conjunto compacto em X .

Definição 71. Uma função f é *linear* se é definida pela lei de formação $f(x) = mx + b$ para m e b constantes, isto é, seu gráfico é uma reta.

Definição 72. Uma função é *linear por partes* se seu gráfico consiste de segmentos de retas.

Considere $\mathbb{D}$ o disco unitário no plano e $I = [0, 1]$ o intervalo real unitário. Tome $P = \{P_1, \dots, P_n\}$, conjunto formado por pontos distintos em $\mathbb{D}$. Sejam n cópias do intervalo unitário I , $\{I_1, \dots, I_n\}$ e considere a união disjunta $\bigsqcup_{i=1}^n I_i$.

Definição 73. Um *enlaçamento de n intervalos*, $n \geq 1$, sobre o disco $\mathbb{D}$ é um mergulho próprio linear por partes (ou diferenciável)

$$\sigma: \bigsqcup_{i=1}^n I_i \rightarrow \mathbb{D} \times I, \quad (3.18)$$

tal que $\sigma|_{I_i}(0) = P_i \times 0$ e $\sigma|_{I_i}(1) = P_i \times 1$, para todo $i \in \{1, \dots, n\}$.

A imagem de I_i é chamada o *i -ésimo intervalo* de σ .

Dado um enlaçamento de intervalos σ , denotamos por

$$Y = (\mathbb{D} \times I) \setminus \sigma \left(\bigsqcup_{i=1}^n I_i \right) \quad (3.19)$$

o complemento de todos os segmentos, e sejam

$$Y_1 = (\mathbb{D} \setminus \{P_1, \dots, P_n\}) \times 1 \quad (3.20)$$

e

$$Y_0 = (\mathbb{D} \setminus \{P_1, \dots, P_n\}) \times 0. \quad (3.21)$$

Observação 17. Considere um ponto Q_0 em $\mathbb{D} \times \{0\}$ e Q_1 um ponto em $\mathbb{D} \times \{1\}$. O grupo fundamental $\pi_1(Y_0, Q_0)$ pode ser identificado com o grupo livre $F(n)$ com conjunto gerador $X = \{x_1, x_2, \dots, x_n\}$ onde cada $x_i \in X$ é representado pelo laço em Y_0 com ponto base Q_0 que circula P_i uma vez no sentido anti-horário, analogamente se considerarmos $\pi_1(Y_1, Q_1)$. Observe a representação na [Figura 23](#).

Figura 23 – $\pi_1(\mathbb{D} \setminus \{P_1, \dots, P_n\})$.

Associamos à um enlaçamento de intervalos σ o grupo fundamental de Y , que será denotado por $G(\sigma)$.

Definimos um conjunto de *meridianos* $\{t_1, \dots, t_k\}$ escolhendo uma orientação em Y e considerando m_i um círculo orientado em $\mathbb{D} \times \{1\}$ em torno de uma vizinhança tubular $I \times D$ da corda de ponto base P_i . Seja Q_1 como anteriormente o ponto base em Y_1 e conecte a m_i por um caminho γ_i em Y . O meridiano t_i é um elemento de $G(\sigma)$ e é representado por $\gamma_i m_i \gamma_i^{-1}$ (ver Figura 24).

Figura 24 – Representação dos meridianos.

No caso de uma trança pura, as inclusões $Y_0 \rightarrow Y \leftarrow Y_1$ induzem isomorfismos

$$\pi_1(Y_0) \cong \pi_1(Y) \cong \pi_1(Y_1). \quad (3.22)$$

Seja $J(\sigma)$ o subgrupo normal de $G(\sigma)$ gerado pelos comutadores dos conjugados dos meridianos, ou seja, os elementos da forma $[t'_i, t''_i]$, onde t'_i e t''_i denotam conjugados de t_i . O grupo quociente $G(\sigma)/J(\sigma)$, denotado por $\hat{G}(\sigma)$, é denominado *grupo reduzido de σ* . Observe que tomar tal quociente é o mesmo que afirmar que os conjugados dos meridianos comutam.

Observação 18. Dizer que conjugados dos meridianos comutam é equivalente a afirmar que cada meridiano comuta com seu conjugado. Ou seja, $[t'_i, t''_i] = 1$ se, e somente se, $[t_i, t'''_i] = 1$, onde t'_i, t''_i e t'''_i são conjugados de t_i .

De fato, note que a primeira implicação é óbvia, pois em particular t_i é conjugado dele mesmo e a segunda segue de

$$\begin{aligned}
 [t'_i, t''_i] &= t'_i t''_i (t'_i)^{-1} (t''_i)^{-1} \\
 &= \xi t_i (\xi^{-1} t''_i \xi) t_i^{-1} (\xi^{-1} (t'_i)^{-1} \xi) \xi^{-1} \\
 &= \xi (t_i t''_i t_i^{-1} (t'_i)^{-1}) \xi^{-1} \\
 &= \xi [t_i, t'_i] \xi^{-1} = \xi \xi^{-1} = 1.
 \end{aligned}$$

3.3 Homotopia e o grupo reduzido de um enlaçamento de intervalos

O Teorema 12 nos diz que o grupo reduzido $\hat{G}(\sigma)$ é um invariante por homotopia de enlaçamento de intervalos. Para demonstrá-lo utilizamos o Teorema da Apresentação de Wirtinger (Teorema 11) que descreve um procedimento para determinar a apresentação do grupo de um nó K em $\mathbb{R}^3$ (ou S^3). Neste sentido, a seguir consideramos alguns resultados da teoria de nós.

Podemos pensar em um enlaçamento como um mergulho de uma reunião disjunta de vários círculos S^1 em $\mathbb{R}^3$ (ou S^3 , a qual é obtida através de uma compactificação de $\mathbb{R}^3$). Basta notar que um círculo S^1 pode ser olhado como um intervalo $[0, 2\pi]$ onde identificamos os seus extremos. Tal intervalo é homeomorfo ao intervalo $[0, 1]$. Quando estivermos no caso em que tomamos somente um mergulho de S^1 em $\mathbb{R}^3$ (ou S^3), diremos que se trata de um nó. Assim, em resumo, um nó é uma curva poligonal fechada e simples em $\mathbb{R}^3$ (ou S^3).

Formalmente temos a seguinte definição:

Definição 74. Um *enlaçamento* é um mergulho linear por partes $k: S^1_1 \sqcup \cdots \sqcup S^1_r \rightarrow S^3$, onde cada S^1_i é homeomorfa a S^1 . Se $r = 1$ o enlaçamento é chamado *nó*.

Figura 25 – Exemplo de nó.

Em geral já vimos que podemos colocar os enlaçamentos em classes de equivalência e, neste caso, devemos dizer qual a relação de equivalência que podemos dar ao conjunto de nós.

Definição 75. Sejam $f_0, f_1: S^1 \hookrightarrow S^3$ dois nós. Se existir uma deformação linear por partes

$$\begin{aligned} H: S^3 \times I &\rightarrow S^3 \times I \\ (y, t) &\mapsto (h_t(y), t), \end{aligned} \quad (3.23)$$

onde $h_0 = Id_{S^3}$ e $f_1 = h_1 \circ f_0$, dizemos que f_0 é *ambientalmente isotópico* a f_1 ou que f_0 e f_1 são *ambiente isotópicos*.

Por abuso de notação podemos nos referir ao mergulho $f_0: S^1 \hookrightarrow S^3$ como sendo $K_0 = f_0(S^1)$, ou seja, utilizamos somente sua imagem.

Pensamos na isotopia ambiente como um movimento em S^3 em que o nó $K_0 = f_0(S^1)$ é continuamente levado ao nó $K_1 = f_1(S^1)$.

Definição 76. Dois nós são equivalentes se eles são ambiente isotópicos.

Proposição 30. Sejam K e K' dois nós em S^3 . As seguintes afirmações são equivalentes:

- (i) Existe um homeomorfismo preservando orientação $f: S^3 \rightarrow S^3$ que leva K a K' , isto é, $f(K) = K'$.
- (ii) K e K' são ambiente isotópicos.

Demonstração. Ver Santos (2002), Proposição 2.0.6. □

Com estas ideias básicas já podemos introduzir o que vem a ser a Apresentação de Wirtinger. As próximas definições são encontradas em Rolfsen (1976).

Considere K uma união de arcos conexos $\alpha_1, \alpha_2, \dots, \alpha_n$ com uma orientação dada como na figura a seguir.

Figura 26 – Um exemplo de nó em $\mathbb{R}^3$.

As setas indicadas por x_i passando sob cada α_i foram traçadas da direita para a esquerda. E agora podemos representar um caminho fechado no complementar de K . Tome $y = (0, 0, 1)$

como ponto base e denote por x_i o caminho fechado que consiste no triângulo orientado de y até o início de x_i , depois percorrendo x_i até o final na direção da seta e retornando a y .

Temos n relações entre os x_i , com $i = 1, 2, \dots, n$, sendo duas as possibilidades:

Figura 27 – Representação das relações em (3.24).

$$x_k x_i = x_{i+1} x_k \quad \text{e} \quad x_i x_k = x_k x_{i+1}, \quad (3.24)$$

denote por r_i tais relações que serão utilizadas na demonstração do Teorema 12.

Teorema 11 (Teorema da Apresentação de Wirtinger). O grupo $\pi_1(\mathbb{R}^3 \setminus K)$ é gerado pela classe de homotopia de x_i e tem apresentação

$$\pi_1(\mathbb{R}^3 \setminus K) = \{x_1, x_2, \dots, x_n; r_1, \dots, r_n\}. \quad (3.25)$$

Além disso, qualquer uma das relações r_i pode ser omitida e o resultado permanece válido.

Demonstração. Ver Rolfsen (1976, p. 57). □

Teorema 12. Dados σ e σ' dois enlaçamentos homotópicos, então seus grupos reduzidos $\hat{G}(\sigma)$ e $\hat{G}(\sigma')$ são isomorfos.

Demonstração. Pela Definição 68 sabemos que dois enlaçamentos são homotópicos se existe uma sequência de enlaçamentos tal que um difere do outro por uma isotopia ambiente ou por uma mudança de cruzamento.

Temos que uma isotopia ambiente deixa invariante o grupo fundamental $G(\sigma)$ e, consequentemente, o grupo reduzido $\hat{G}(\sigma)$.

Consideremos então somente o caso em que σ e σ' estão relacionados apenas por uma mudança de cruzamento na corda j . Para mudanças em mais de uma corda, o resultado segue por recorrência. Considere a apresentação de Wirtinger relacionada ao cruzamento a seguir.

Figura 28 – Cruzamento em que foi aplicada a homotopia.

Nas figuras, as setas A, B, C e D representam laços que são conjugados do meridiano t_j . Pelas relações de Wirtinger, resulta que

$$AC = DB, \quad (3.26)$$

$$A = B, \quad (3.27)$$

$$C = D, \quad (3.28)$$

o que nos diz que $AC = CA, AD = DA, BC = CB, \dots$, ou seja, um conjunto de relações dizendo que conjugados dos meridianos t_j comutam. Mas isto não tem efeito no grupo livre reduzido, o que implica que $\hat{G}(\sigma)$ e $\hat{G}(\sigma')$ são isomorfos. $\square$

3.4 Uma apresentação de $\hat{\mathbb{PB}}_n(\mathbb{D})$

Faremos uso da descrição presente em [Goldsmith \(1974\)](#) para $\hat{\mathbb{PB}}_n(\mathbb{D})$ apresentada a seguir.

Denote por $\mathbb{H}_n$ o conjunto das tranças que são homotópicas à trança trivial.

Lema 5. O conjunto $\mathbb{H}_n$ é subgrupo normal de $\mathbb{P}_n$.

Demonstração. Sejam β_1 e β_2 duas tranças homotópicas à trança trivial. Então utilizando as homotopias H_1 de β_1 à 1_n e H_2 de β_2 à 1_n , obtemos que $\beta_1\beta_2$ é homotópico à 1_n . Além disso, se β é homotópica à trança trivial então β^{-1} também o é.

Sejam $\gamma \in \mathbb{P}_n$ e $\beta \in \mathbb{H}_n$, então $\gamma\beta\gamma^{-1}$ é homotópica à trança trivial. $\square$

Recorde que $\hat{\mathbb{PB}}_n(\mathbb{D})$ o grupo formado por todas as *classes de homotopia de tranças puras sobre o disco* com a mesma operação que foi definida em (2.3) para o produto de classes de isotopia. Lembre que, pelo [Teorema 10](#), toda classe possui um representante que é uma trança pura.

Proposição 31. O grupo $\hat{\mathbb{PB}}_n(\mathbb{D})$ é isomorfo ao grupo quociente de $\mathbb{P}_n$ por $\mathbb{H}_n$.

Demonstração. Considere a aplicação

$$\begin{aligned} \mu: \mathbb{P}_n &\rightarrow \hat{\mathbb{PB}}_n(\mathbb{D}) \\ \beta &\mapsto [\beta]. \end{aligned} \quad (3.29)$$

Se a trança β é homotopicamente trivial, então β está no núcleo de μ , o qual é exatamente o subgrupo $\mathbb{H}_n$ de $\mathbb{P}_n$. Então, pelo Teorema do Homomorfismo, resulta que

$$\hat{\mathbb{PB}}_n(\mathbb{D}) \cong \frac{\mathbb{P}_n}{\mathbb{H}_n}. \quad (3.30)$$

$\square$

Recorde que $A_{j,k} = (\sigma_{k-1}\sigma_{k-2}\cdots\sigma_{j+1})\sigma_j^2(\sigma_{j+1}^{-1}\cdots\sigma_{k-2}^{-1}\sigma_{k-1}^{-1})$. A seguinte proposição nos apresenta tranças homotopicamente triviais.

Proposição 32. Seja β uma trança pura em $\mathbb{B}_n$ da forma

$$\beta = [A_{j,k}, gA_{j,k}g^{-1}], \quad (3.31)$$

onde $1 \leq j < k \leq n$ e g é um elemento do subgrupo $\mathbb{P}_G$ (de $\mathbb{P}_n$) gerado por $A_{1,k}, A_{2,k}, \dots, A_{k-1,k}$. Então, β é homotopicamente trivial, isto é, β é homotópica à trança trivial.

Demonstração. Ver [Goldsmith \(1974, p. 94\)](#). □

Proposição 33. Uma trança β em $\mathbb{B}_n$ é homotopicamente trivial se, e somente se, β pertence ao fecho normal do conjunto de todas as tranças da forma (3.31).

Demonstração. Ver [Goldsmith \(1974, p. 94\)](#). □

Assim podemos afirmar que o grupo $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ é isomorfo ao grupo de tranças puras com a relação adicional de que $A_{j,k} \rightleftharpoons gA_{j,k}g^{-1}$, onde $1 \leq j < k \leq n$, ou seja, possui a apresentação dada pelo seguinte teorema.

Teorema 13. O conjunto de todas as classes de homotopia de tranças puras forma um grupo, o qual estamos denotando por $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$. Além disso, $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ tem a seguinte apresentação:

$$\begin{aligned} &\text{geradores: } \sigma_1, \sigma_2, \dots, \sigma_{n-1}; \\ &\text{relações: } \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, i \in \{1, 2, \dots, n-2\}; \\ &\sigma_i\sigma_j = \sigma_j\sigma_i, \text{ para } |i-j| \geq 2 \text{ e } i, j \in \{1, 2, \dots, n-1\}; \\ &A_{j,k} \rightleftharpoons gA_{j,k}g^{-1}, \text{ onde } 1 \leq j < k \leq n, \end{aligned} \quad (3.32)$$

sendo g um elemento do subgrupo $\mathbb{P}_G$ de $\mathbb{P}_n$ gerado por $A_{1,k}, A_{2,k}, \dots, A_{k-1,k}$.

Observação 19. O símbolo $\rightleftharpoons$ indica que podemos trocar de posição as tranças relacionadas por ele.

UMA ORDEM NO GRUPO DE TRANÇAS E NO GRUPO DE TRANÇAS PURAS

Vimos que grupos ordenáveis possuem algumas propriedades especiais. Definimos aqui uma ordem sobre o grupo de tranças $\mathbb{B}_n$. Também mostramos que o grupo de tranças puras $\mathbb{P}_n$ possui uma ordem que é invariante sob a multiplicação de ambos os lados, ou seja, é bi-invariante. Um ponto crucial para que $\mathbb{P}_n$ seja bi-ordenado é o fato de que tal grupo é um produto semidireto de grupos livres, de acordo com a técnica de pentear de Artin.

As principais referências deste capítulo são [Dehornoy et al. \(2008\)](#) e [Kassel e Turaev \(2008\)](#).

4.1 Uma ordem no grupo de tranças

Consideramos agora uma ordem em $\mathbb{B}_n$, a saber, a ordem de Dehornoy, também chamada de σ -ordem e algumas de suas propriedades. Temos que a σ -ordem não é bi-invariante em $\mathbb{B}_n$, para $n \geq 3$, sendo bi-invariante somente quando restrita ao monoide de tranças positivas $\mathbb{B}_n^+$.

Utilizando alguns resultados apresentados no primeiro capítulo já podemos apresentar os seguintes exemplos, relacionados à inexistência de uma bi-ordenação em $\mathbb{B}_n$.

Exemplo 14. $\mathbb{B}_1 = \{1\}$ e $\mathbb{B}_2 \cong \mathbb{Z}$ são bi-ordenáveis.

Proposição 34. O grupo de tranças $\mathbb{B}_n$ com $n \geq 3$ não é bi-ordenável.

De fato, $\sigma_1 \sigma_2 \neq \sigma_2 \sigma_1$, porém $(\sigma_1 \sigma_2)^3 = (\sigma_2 \sigma_1)^3$. Então, pela [Proposição 21](#), $\mathbb{B}_n$ não é bi-ordenável se $n \geq 3$. Mas uma demonstração formal é encontrada em [Dehornoy et al. \(2008\)](#), Proposição 1.2.

Vimos que uma *palavra trança* é uma palavra no conjunto $\{\sigma_1, \dots, \sigma_{n-1}, \sigma_1^{-1}, \dots, \sigma_{n-1}^{-1}\}$. Toda palavra trança representa um elemento de $\mathbb{B}_n$.

Definição 77. Dada uma palavra trança não vazia $w = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_r}^{\varepsilon_r}$, onde $\varepsilon_k \in \{\pm 1\}$ e $i_k \in \{1, \dots, n-1\}$ para todo $k \in \{1, \dots, r\}$, dizemos que o *índice da palavra* w é o menor inteiro $i \in \{1, \dots, n-1\}$ tal que σ_i ou σ_i^{-1} aparece em w .

Observação 20. Uma palavra trança não vazia tem o mesmo índice de sua palavra inversa. Além disso, a palavra vazia não tem índice.

Definição 78. Dada uma palavra trança não vazia $w = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_r}^{\varepsilon_r}$, onde $\varepsilon_k \in \{\pm 1\}$ e $i_k \in \{1, \dots, n-1\}$ para todo $k \in \{1, \dots, r\}$, dizemos que w é σ_i -positiva se ela possui índice i e σ_i^{-1} não aparece em w . Dizemos que w é σ_i -negativa se seu inverso é σ_i -positivo.

Definição 79. Uma palavra trança é σ -positiva (resp. σ -negativa) se for σ_i -positiva (resp. σ_i -negativa) para algum $i \in \{1, \dots, n-1\}$.

Definição 80. Seja $\beta \in \mathbb{B}_n$, então β é σ -positiva (resp. σ -negativa) se ela é representada por uma palavra σ -positiva (resp. σ -negativa).

Observação 21. Uma trança $\beta \in \mathbb{B}_n$ pode ter mais de uma palavra associada, entretanto a definição anterior nos diz que basta que exista uma palavra associada σ -positiva ou σ -negativa para a trança ser considerada σ -positiva ou σ -negativa.

Exemplo 15. Considere β a trança $\sigma_1 \sigma_2 \sigma_1^{-1}$. A palavra trança $\sigma_1 \sigma_2 \sigma_1^{-1}$ não é σ -positiva e nem σ -negativa, porém é equivalente à $\sigma_2^{-1} \sigma_1 \sigma_2$. Logo, concluímos que β é uma trança σ -positiva.

Considere o subconjunto de $\mathbb{B}_n$ dado por

$$\mathcal{P} = \{\beta \in \mathbb{B}_n; \beta \text{ é } \sigma\text{-positiva}\}. \quad (4.1)$$

Lema 6. O subconjunto $\mathcal{P}^{-1} = \{\beta \in \mathbb{B}_n; \beta^{-1} \in \mathcal{P}\}$ de $\mathbb{B}_n$ é o conjunto de elementos σ -negativos e $\mathcal{P}^2 \subset \mathcal{P}$.

Lema 7. $1 \notin \mathcal{P}$.

Lema 8. Qualquer elemento $\beta \in \mathbb{B}_n$, distinto de 1, é σ -positivo ou σ -negativo. Em outras palavras, $\mathcal{P} \cup \{1\} \cup \mathcal{P}^{-1} = \mathbb{B}_n$.

As demonstrações destes 3 lemas podem ser encontradas em [Kassel e Turaev \(2008\)](#) e graças a eles podemos demonstrar o seguinte teorema que estabelece uma ordem no grupo de tranças conhecida como *ordem de Dehornoy*.

Teorema 14. Para qualquer $n \geq 1$, o grupo de tranças $\mathbb{B}_n$ tem uma ordem total $\leq$ invariante à esquerda, tal que $1 < \beta$ se, e somente se, β é σ -positiva.

Demonstração. Dadas quaisquer $\beta, \gamma \in \mathbb{B}_n$, então dizemos que $\beta \leq \gamma$, se $\beta = \gamma$ ou $\beta^{-1} \gamma \in \mathcal{P}$, onde $\mathcal{P} = \{\beta \in \mathbb{B}_n; \beta \text{ é } \sigma\text{-positiva}\}$.

Temos, pelos [Lemas 6, 7 e 8](#), que $\mathcal{P}$ satisfaz as condições do [Teorema 4](#), o que permite afirmar que $\mathbb{B}_n$ tem uma ordem total invariante à esquerda, ou seja, é ordenável. $\square$

Observação 22. Quando $n = 2$, qualquer palavra trança σ -positiva é necessariamente da forma σ_1^k para $k \geq 1$. Note que $\mathbb{B}_2$ é isomorfo a $\mathbb{Z}$ via a aplicação $\sigma_1^k \mapsto k$. A ordem de Dehornoy em $\mathbb{B}_2$ coincide com a ordem total padrão em $\mathbb{Z}$ via este isomorfismo.

O seguinte exemplo nos mostra que a σ -ordem não é invariante à direita.

Exemplo 16. Sejam $\beta = \sigma_1 \sigma_2^{-1}$ e $\gamma = \sigma_1 \sigma_2 \sigma_1$. A palavra $\sigma_1 \sigma_2^{-1}$ é σ -positiva, visto que é σ_1 -positiva, então $\beta > 1$.

Utilizando a [Observação 14](#) temos

$$\begin{aligned}
 \gamma^{-1} \beta \gamma &= \sigma_1^{-1} \sigma_2^{-1} \sigma_1^{-1} \sigma_1 \sigma_2^{-1} \sigma_1 \sigma_2 \sigma_1 \\
 &= (\sigma_1^{-1} \sigma_2^{-1} \sigma_1^{-1}) \sigma_1 (\sigma_1 \sigma_2 \sigma_1) (\sigma_1^{-1} \sigma_2^{-1} \sigma_1^{-1}) \sigma_2^{-1} (\sigma_1 \sigma_2 \sigma_1) \\
 &= \sigma_1^{-1} \sigma_2^{-1} (\sigma_1^{-1} \sigma_1) \sigma_1 \sigma_2 \sigma_1 \sigma_1^{-1} \sigma_2^{-1} (\sigma_1^{-1} \sigma_2^{-1} \sigma_1) \sigma_2 \sigma_1 \\
 &= \sigma_1^{-1} \sigma_2^{-1} \sigma_1 \sigma_2 \sigma_1 \sigma_1^{-1} (\sigma_2^{-1} \sigma_2) \sigma_1^{-1} (\sigma_2^{-1} \sigma_2) \sigma_1 \\
 &= \sigma_1^{-1} (\sigma_2^{-1} \sigma_1 \sigma_2) \sigma_1 \sigma_1^{-1} \sigma_1^{-1} \sigma_1 \\
 &= (\sigma_1^{-1} \sigma_1) \sigma_2 \sigma_1^{-1} (\sigma_1 \sigma_1^{-1}) (\sigma_1^{-1} \sigma_1) \\
 &= \sigma_2 \sigma_1^{-1}.
 \end{aligned}$$

Logo, $\gamma^{-1} \beta \gamma = \sigma_2 \sigma_1^{-1}$ é σ -negativa já que é σ_1 -negativa e, portanto, $\beta \gamma < \gamma$. Então $1 < \beta$ não implica que $\gamma < \beta \gamma$.

4.1.1 Algumas propriedades da ordem de Dehornoy

Para a ordem de Dehornoy, temos

$$\cdots > \sigma_1^3 > \sigma_1^2 > \sigma_1 > \cdots > \sigma_2^3 > \sigma_2^2 > \sigma_2 > \cdots > \sigma_{n-1}^3 > \sigma_{n-1}^2 > \sigma_{n-1}. \quad (4.2)$$

Basta notar que σ_i^r e $\sigma_{i+1}^s \sigma_i^r$, com $r \geq 1$ e $s \in \mathbb{Z}$ são elementos σ -positivos.

Proposição 35. O grupo $\mathbb{B}_n$ tem um menor elemento σ -positivo dado por σ_{n-1} . Em $\mathbb{P}_n$ o menor elemento σ -positivo é σ_{n-1}^2 . Similarmente prova-se que σ_{n-1}^{-1} e σ_{n-1}^{-2} são os maiores elementos de $\mathbb{B}_n$ e $\mathbb{P}_n$, respectivamente.

Demonstração. Suponha que exista $\beta \in \mathbb{B}_n$, σ -positivo, tal que $\beta < \sigma_{n-1}$. Por definição, isso equivale a dizer que $\beta^{-1} \sigma_{n-1} \in \mathcal{P}$. Seja w uma palavra σ_i -positiva representando β . Temos que a trança $\beta^{-1} \sigma_{n-1}$ é representada pela palavra $w^{-1} \sigma_{n-1}$. Se $i < n-1$, então $w^{-1} \sigma_{n-1}$ é σ -negativa. Logo, $i = n-1$ e $w = (\sigma_{n-1})^r$ para algum inteiro positivo $r \geq 1$. Assim, $\beta^{-1} \sigma_{n-1}$ é 1 se $r = 1$ e pertence a $\mathcal{P}^{-1}$ se $r > 1$, o que contraria a σ -positividade de $\beta^{-1} \sigma_{n-1}$. Portanto, não existe $\beta \in \mathcal{P}$ tal que $\beta < \sigma_{n-1}$.

A prova de que σ_{n-1}^2 é o menor elemento de $\mathbb{P}_n$ é feita de maneira análoga. $\square$

Proposição 36. O grupo $\mathbb{B}_n$ não tem elementos maximais e não tem elementos minimais.

Demonstração. Como $\sigma_1 > 1 > \sigma_1^{-1}$, a invariância da ordem implica que $\beta \sigma_1 > \beta > \beta \sigma_1^{-1}$, para cada $\beta \in \mathbb{B}_n$. Logo, $\mathbb{B}_n$ não tem elemento minimal nem maximal. $\square$

Lema 9. A inclusão $i: \mathbb{B}_n \hookrightarrow \mathbb{B}_{n+1}$ preserva a ordem com respeito a ordem de Dehornoy, ou seja, $\beta \leq_n \beta'$ implica que $i(\beta) \leq_{n+1} i(\beta')$, para todo $\beta, \beta' \in \mathbb{B}_n$.

Podemos pensar no grupo das tranças com infinitas cordas, $\mathbb{B}_\infty$ como sendo o limite indutivo dos grupos $\mathbb{B}_n$ para $n \geq 1$ com respeito as inclusões i , isto é, $\mathbb{B}_\infty = \bigcup_{n \geq 1} \mathbb{B}_n$.

Para demonstrar a próxima proposição faremos uso do seguinte resultado de Cantor que afirma quando um conjunto ordenado é isomorfo ao conjunto dos números racionais ($\mathbb{Q}$).

Teorema 15 (Cantor). Suponha que $(Y, \leq)$ é um conjunto não vazio enumerável tal que

- (a) Para todo $y \in Y$, existe $x \in Y$, tal que $y < x$;
- (b) Para todo $y \in Y$, existe $x \in Y$, tal que $x < y$;
- (c) Para todo $x, y \in Y$, se $x < y$ então existe $z \in Y$ tal que $x < z < y$.

Então $(Y, \leq)$ é isomorfo a $\mathbb{Q}$, como conjunto ordenado.

Note que o item (a) nos diz que Y não tem elementos maximais, (b) que não tem elementos minimais e o item (c) afirma que dados dois elementos distintos de Y , existe um outro elemento distinto deles que está entre eles com respeito à ordem de Y .

Proposição 37. O grupo $\mathbb{B}_\infty$ é munido de uma ordem tal que a inclusão $i: \mathbb{B}_n \hookrightarrow \mathbb{B}_\infty$ preserva a ordem. Como um conjunto ordenado, $\mathbb{B}_\infty$ é isomorfo a $\mathbb{Q}$.

Demonstração. Primeiramente mostraremos que a inclusão preserva a ordem. De fato, sejam β e β' em $\mathbb{B}_\infty$. Defina $\beta \leq_\infty \beta'$ se existir n tal que $\beta \leq_n \beta' \in \mathbb{B}_n$. Segue do Lema 9 a independência da escolha de n . Assim, temos uma relação de ordem bem definida em $\mathbb{B}_\infty$. É fácil verificar que $\leq_\infty$ é uma ordem invariante à esquerda, total e que as inclusões $\mathbb{B}_n \hookrightarrow \mathbb{B}_\infty$ preservam a ordem. O grupo $\mathbb{B}_\infty$ é enumerável, pois é gerado pelo conjunto $\{\sigma_1, \sigma_2, \dots\}$ e qualquer grupo com um conjunto enumerável de geradores é enumerável.

Se β fosse um elemento maximal de $\mathbb{B}_\infty$ com respeito à ordem $\leq_\infty$, então por definição β seria um elemento maximal de $\mathbb{B}_n$ para algum n , e o mesmo ocorre se $\mathbb{B}_\infty$ tivesse um elemento minimal. Logo, teríamos uma contradição com a Proposição 36.

Para provar que entre quaisquer dois elementos existe um outro elemento é suficiente (usando a invariância à esquerda) mostrar que $1 < \beta$ então existe α tal que $1 < \alpha < \beta$. Seja $\beta \in \mathbb{B}_n$ com $1 < \beta$.

Tome $\alpha = i(\beta) \sigma_n^{-1} \in \mathbb{B}_{n+1}$. Se w é uma palavra σ -positiva representando β em $\mathbb{B}_n$, então w possui um índice menor do que n . Então, $i(\beta)$ possui como representante uma palavra σ -positiva

com índice menor do que n , logo $\alpha = i(\beta)\sigma_n^{-1}$ é σ -positiva. Logo $\alpha > 1$ em $\mathbb{B}_{n+1}$ e portanto em $\mathbb{B}_\infty$.

Além disso, $\alpha^{-1}\beta = \sigma_n$ em $\mathbb{B}_\infty$, logo é σ -positiva, então $\alpha < \beta$. Portanto, $\mathbb{B}_\infty$ é enumerável, não tem elementos maximais e nem minimais. Além disso, dados quaisquer dois elementos existe um elemento entre eles e daí pelo [Teorema 15](#) temos que ele é isomorfo a $\mathbb{Q}$. $\square$

4.2 Uma ordem no grupo de tranças puras

Nesta seção introduzimos a expansão de Magnus e a partir dela mostramos que grupos livres são bi-ordenáveis, damos uma ideia da decomposição do grupo de tranças puras $\mathbb{P}_n$ como um produto semidireto de grupos livres e mostramos que tal produto semidireto é bi-ordenável utilizando a ordem lexicográfica. Com isso obtemos uma ordem total estrita no grupo de tranças puras $\mathbb{P}_n$ que é invariante pela multiplicação em ambos os lados.

4.2.1 Expansão de Magnus e uma ordem no grupo livre

Definição 81. Seja $X = \{X_1, X_2, \dots, X_n\}$ um conjunto finito e considere $M(X)$ o monoide livre sobre X . Por uma *série de potências formal sobre X* queremos dizer uma soma formal arbitrária

$$\sum_{W \in M(X)} f_W W, \quad (4.3)$$

onde $f_W \in \mathbb{Z}$.

Denote o conjunto de todas as séries de potência formais sobre X por $\mathbb{Z}[[X]]$. Dados $a = \sum_{U \in M(X)} f_U U$ e $b = \sum_{V \in M(X)} g_V V$, então considere a operação adição $a + b$ em $\mathbb{Z}[[X]]$ dada somando-se os coeficientes da mesma palavra e a operação de multiplicação $a \cdot b$ em $\mathbb{Z}[[X]]$ dada por $a \cdot b = (\sum_{U \in M(X)} f_U U)(\sum_{V \in M(X)} g_V V) = \sum_{W \in M(X)} (\sum_{UV=W} f_U g_V) W$. Com tais operações $\mathbb{Z}[[X]]$ é denominado o *anel não comutativo das séries de potências formais*.

Definição 82. Seja $a = \sum_{U \in M(X)} f_U U$ em $\mathbb{Z}[[X]]$. Dizemos que a tem *grau* maior do que ou igual a r , onde r é um inteiro positivo tal que $f_U = 0$ para todo $U \in M(X)$ com $l(U) < r$, sendo l a função comprimento dada na [Definição 7](#).

Observação 23. Denotaremos por $O(k)$ o ideal de $\mathbb{Z}[[X]]$ formado pelas séries de grau maior do que ou igual a k e por $o(k)$ um elemento de $O(k)$.

Proposição 38. Considere $\mathcal{G} = \{1 + o(1)\}$ subconjunto de $\mathbb{Z}[[X]]$ formado pelas séries de potências com termo constante igual a 1. Então $\mathcal{G}$ é um subgrupo de $\mathbb{Z}[[X]]$, munido da operação multiplicação.

Demonstração. Desde que o termo constante de um produto é o produto de todos os termos individuais constantes, segue que $\mathcal{G}$ é fechado para a multiplicação. Temos ainda que a multiplicação

é associativa em $\mathbb{Z}[[X]]$ e $1 = 1 + 0X_i \in \mathcal{G}$, então a associatividade e a existência de elemento identidade são válidas para $\mathcal{G}$. Agora resta mostrar que dado um elemento $a \in \mathcal{G}$, existe a^{-1} tal que $aa^{-1} = 1 = a^{-1}a$. Seja $a = 1 + h$ onde h é uma série envolvendo apenas monômios de grau maior ou igual a 1 então a^{-1} existe e é unicamente determinado por $a^{-1} = 1 - h + h^2 - h^3 + \dots$. De fato, desde que h tem termo constante igual a zero e

$$\begin{aligned} (1 + x_i)(1 - x_i + x_i^2 - x_i^3 + \dots + (-1)^n x_i^n + \dots) &= \\ (1 - x_i + x_i^2 + \dots + (-1)^n x_i^n + \dots) + (x_i - x_i^2 + \dots + (-1)^{n+1} x_i^{n+1} + \dots) &= \\ = 1, \end{aligned}$$

então $aa^{-1} = (1 + h)(1 - h + h^2 - h^3 + \dots + (-1)^n h^n + \dots) = 1$. Analogamente $a^{-1}a = 1$. $\square$

Denote por $\mathbb{Z}[[X]]^*$ o conjunto de todas as séries de potências formais $a \in \mathbb{Z}[[X]]$ que são invertíveis, ou seja, tais que $a \in \mathcal{G}$, denominado o grupo das unidades de $\mathbb{Z}[[X]]$.

Exemplo 17. Para qualquer $X_i \in X$, o polinômio $1 + X_i \in \mathbb{Z}[[X]]$ é invertível e seu inverso é a série de potências formal $\sum_{k \geq 0} (-1)^k X_i^k$, como vimos na demonstração da [Proposição 38](#).

Lema 10. Para qualquer $X_i \in X$ e $k \in \mathbb{Z}$ existe uma série de potências formal $h_k(X_i)$ tal que $(1 + X_i)^k = 1 + kX_i + X_i^2 h_k(X_i)$.

Demonstração. Segue por indução sobre k . $\square$

Definição 83. Sejam $X = \{x_1, \dots, x_n\}$ e $F(X)$ o grupo livre em X . A *expansão de Magnus de $F(X)$* é a aplicação

$$\mu: F(X) \rightarrow \mathbb{Z}[[X]] \quad (4.4)$$

definida no conjunto gerador X como segue:

$$\begin{aligned} \mu(x_i) &= 1 + X_i, \\ \mu(x_i^{-1}) &= 1 - X_i + X_i^2 - X_i^3 + \dots \end{aligned} \quad (4.5)$$

Exemplo 18. Considere $X = \{x, y\}$, $F(X)$ o grupo livre com base X e $w = x^2 y^2 \neq 1 \in F(X)$. Pela expansão de Magnus definida anteriormente temos que

$$\begin{aligned} \mu(w) &= \mu(x^2 y^2) = \mu(x^2) \mu(y^2) = \mu(x) \mu(x) \mu(y) \mu(y) \\ &= (1 + X)(1 + X)(1 + Y)(1 + Y) = (1 + 2X + X^2)(1 + 2Y + Y^2) \\ &= 1 + 2Y + Y^2 + 2X + 4XY + 2XY^2 + X^2 + 2X^2Y + X^2Y^2. \end{aligned} \quad (4.6)$$

Note que aparece somente um monômio expresso por XY e seu coeficiente é $4 = 2 \cdot 2$, o qual é dado pelo produto dos expoentes de x e y na palavra w . Utilizaremos esse fato na demonstração da [Proposição 39](#).

Exemplo 19. Dados $x_1, x_2 \in X$ temos que

$$\mu(x_1^{-1}x_2^{-1}x_1x_2) = 1 + (X_1X_2 - X_2X_1) + o(3) = 1 + o(2).$$

Demonstração. Basta ver que

$$\begin{aligned} \mu(x_1x_2x_1^{-1}x_2^{-1}) &= \\ &= (1 + X_1)(1 + X_2)(1 - X_1 + \cdots + (-1)^n X_1^n + \cdots)(1 - X_2 + \cdots + (-1)^n X_2^n + \cdots) \\ &= (1 + X_2 + X_1 + X_1X_2)(1 - X_2 + X_2^2 - X_1 + X_1X_2 + X_1^2 + o(3)) \\ &= 1 - X_2 + X_2^2 - X_1 + X_1X_2 + X_1^2 + X_2 - X_2^2 - X_2X_1 + X_1 - X_1X_2 - X_1^2 + X_1X_2 + o(3) \\ &= 1 - X_2X_1 + X_1X_2 + o(3) \\ &= 1 + o(2). \end{aligned}$$

□

Proposição 39. Seja X um conjunto e $F(X)$ o grupo livre sobre X . O homomorfismo de grupos $\mu: F(X) \rightarrow \mathbb{Z}[[X]]^*$ definido por $\mu(x_i) = 1 + X_i$ para todo $x_i \in X$ é injetivo.

Demonstração. Recorde da definição de grupo livre que se definirmos uma aplicação de X em G , digamos $f: X \rightarrow G$, existe um único homomorfismo $\varphi: F(X) \rightarrow G$, tal que $\varphi \circ i = f$ em X , onde i é a aplicação inclusão de X em $F(X)$. Portanto, μ existe e é único.

Agora mostremos que μ é injetiva. Seja $w \neq 1$, $w \in F$ e escreva na forma $w = x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r}$ onde $x_1, \dots, x_r \in X$ com $x_1 \neq x_2, x_2 \neq x_3, \dots, x_{r-1} \neq x_r$ e $k_i \neq 0$ para todo $i \in \{1, \dots, r\}$.

Temos que

$$\begin{aligned} \mu(w) &= \mu(x_1)^{k_1} \mu(x_2)^{k_2} \cdots \mu(x_r)^{k_r} \\ &= (1 + k_1 X_1 + X_1^2 h_{k_1}(X_1))(1 + k_2 X_2 + X_2^2 h_{k_2}(X_2)) \cdots (1 + k_r X_r + X_r^2 h_{k_r}(X_r)). \end{aligned}$$

Expandindo a série de potências formal do lado direito, vemos que ela contém um único monômio da forma $X_1 X_2 \cdots X_r$. O coeficiente deste monômio é $k_1 k_2 \cdots k_r \neq 0$. Portanto $\mu(w) \neq 1$. □

Dado $w \in F(X)$ a série de potências $\mu(w)$ é chamada *expansão de Magnus de w* .

Vamos agora munir um grupo livre de uma ordem total bi-invariante induzida de uma ordem na sua base.

Observação 24. Recordemos que na [Definição 7](#), a função comprimento $l: M(X) \rightarrow \mathbb{N}$ associa a cada $w \in M(X)$ o número do elementos de X em sua expansão.

Mostraremos que todo grupo livre é bi-ordenável, construindo um cone positivo (ver [Definição 51](#)), satisfazendo as condições do [Teorema 4](#), utilizando a expansão de Magnus.

Proposição 40. Seja $(X, \leq)$ um conjunto ordenado onde $\leq$ é uma ordem total e considere $F(X)$ o grupo livre sobre X . Então $F(X)$ pode ser munido de uma ordem total bi-invariante induzida pela ordem de X denominada *ordem de Magnus*.

Demonstração. Primeiramente iremos munir o monoide $M(X)$ de uma ordem $\leq^*$ induzida pela ordem $\leq$ em X . Estabelecemos tal ordem da seguinte maneira:

- (1) Os elementos de $X \subset M(X)$ são ordenados utilizando a ordem $\leq$ presente em X , ou seja, dados $x, y \in X$ temos que $x \leq^* y$ se, e somente se, $x \leq y$;
- (2) Dados W_1 e W_2 em $M(X)$ se $l(W_1) < l(W_2)$, diremos que $W_1 < W_2$;
- (3) Dados W_1 e W_2 em $M(X)$ se $l(W_1) = l(W_2)$, ordenamos lexicograficamente.

A ordem $\leq^*$ definida desta maneira é bi-invariante e total.

Pela [Proposição 39](#) a expansão de Magnus é uma aplicação injetiva e portanto dado $w \neq 1$ temos que $\mu(w) \neq 1$ em $\mathbb{Z}[[X]]$. Disso segue que $\mu(w) - 1 = \sum_W n_W W$ onde W são palavras não vazias em $M(X)$ e n_W são inteiros não nulos.

Considerando a ordem $\leq^*$ inserida em $M(X)$ podemos dizer que existe uma palavra V que é a menor dentre as palavras que aparecem na expansão de $\mu(w) - 1$, iremos denotá-la por V e seja $n(w) = n_V \neq 0$. Considere

$$\mathcal{P} = \{w \in F(X) \setminus \{1\}; n(w) > 0\}. \quad (4.7)$$

Então um elemento de $F(X) \setminus \{1\}$ está em $\mathcal{P}$ se, e somente se, é da forma $1 + n(w)V + \sum_{W > V} n_W W$ onde $V \neq 1$ e $n(w) > 0$.

Se $\mathcal{P}$ é um conjunto que satisfaz as condições do [Teorema 4](#) então ele define uma ordem total bi-invariante em $F(X)$. De fato, primeiramente note que da maneira como definimos $\mathcal{P}$ temos que $1 \notin \mathcal{P}$. Além disso, dados $w, w' \in \mathcal{P}$ temos $\mu(w) = 1 + n(w)V + \sum_{W > V} n_W W$ e $\mu(w') = 1 + n(w')V' + \sum_{W' > V'} n_{W'} W'$, onde $n(w)$ e $n(w') > 0$. Expandindo $\mu(ww') = \mu(w)\mu(w')$ e usando a bi-invariância da ordem de $M(X)$, obtemos

$$n(ww') = \begin{cases} n(w) & \text{se } V < V', \\ n(w') & \text{se } V > V', \\ n(w) + n(w') & \text{se } V = V'. \end{cases} \quad (4.8)$$

Então $n(ww') > 0$, ou seja, $ww' \in \mathcal{P}$. Portanto, $\mathcal{P}^2 \subset \mathcal{P}$.

Não é difícil verificar que $\mu(w^{-1}) = \mu(w)^{-1}$ e que $\mathcal{P}^{-1}$ é o conjunto de todos os $w \in F(X) \setminus \{1\}$ tal que $n(w) < 0$. Este fato junto com a injetividade de μ implicam que $\mathcal{P} \cup \{1\} \cup \mathcal{P}^{-1} = F(X)$. Se $f \in \mathbb{Z}[[X]]$ é uma série de potências formal sem termo constante, ou seja, $f \in O(1)$ e $W \in M(X)$ então $(1 + f)W(1 + f)^{-1} = W + \sum_{W' > V} n_{W'} W'$ onde $n_{W'} \in \mathbb{Z}$. Isto implica que $n(ww'w^{-1}) = n(w')$ para todo $w, w' \in F(X) \setminus \{1\}$ e assim obtemos $w\mathcal{P}w^{-1} \subset \mathcal{P}$ para todo $w \in F(X)$. $\square$

Corolário 6. Todo grupo livre é bi-ordenável.

4.2.2 Ordem no grupo de tranças puras

Vimos o que é um produto semidireto na [Definição 29](#) e pela [Observação 6](#), sabemos que o automorfismo de H que utilizamos na definição da operação inserida em $H \times Q$ é o automorfismo interno. Para ordenar o produto semidireto, faremos uso da *ordem lexicográfica* da seguinte forma:

Definição 84. Sejam $(H, \leq_H)$ e $(Q, \leq_Q)$ grupos bi-ordenados e tome o produto semidireto $H \rtimes Q$, temos que dados $hq, h'q' \in H \rtimes Q$,

$$hq < h'q' \Leftrightarrow q <_Q q' \text{ ou } q = q' \text{ e } h <_H h'. \quad (4.9)$$

Note que a comparação nesta ordem lexicográfica é feita da direita para a esquerda.

Como vimos se tivermos H, Q grupos bi-ordenáveis, então o produto direto $H \times Q$ é bi-ordenável, onde a ordem inserida nele é a ordem lexicográfica como vimos no [Lema 1](#). Entretanto não podemos dizer que a ordem lexicográfica em $H \rtimes Q$ é bi-invariante.

O seguinte lema nos dá uma condição necessária e suficiente para que a ordem lexicográfica do produto semidireto seja bi-invariante:

Lema 11. Sejam $(H, \leq_H)$ e $(Q, \leq_Q)$ grupos bi-ordenáveis. Então o produto semidireto $H \rtimes Q$ é bi-ordenado se, e somente se, a ação de Q sobre H preserva a ordem sobre H (equivalentemente $q^{-1} \mathcal{P}_H q \subset \mathcal{P}_H$, para todo $q \in Q$).

Demonstração. $\Rightarrow$) Considere $h \in \mathcal{P}_H$, então $(h, 1)$ está no cone positivo $\mathcal{P}_{H \rtimes Q}$. Note que

$$(1, q)(h, 1)(1, q^{-1}) = (h^q, q)(1, q^{-1}) = (h^q, 1). \quad (4.10)$$

Desde que $H \rtimes Q$ é um grupo bi-ordenado, sabemos que $(h^q, 1)$ está em $\mathcal{P}_{H \rtimes Q}$, isto é, $(1, 1) < (h^q, 1)$. Portanto $1 <_H h^q$, então h^q está no cone positivo $\mathcal{P}_H$.

$\Leftarrow$) Verificaremos se $\mathcal{P}_{H \rtimes Q}$ satisfaz as condições do [Teorema 4](#). Primeiramente sejam (h, q) e (h', q') elementos positivos em $H \rtimes Q$, então

- (a) Se $q \neq 1$ ou $q' \neq 1_Q$, então $1_Q < qq'$;
- (b) Se ambos q e q' são iguais a 1_Q , então $1_H < h(h')^q = hh'$.

Em ambos os casos $1 < (h, q)(h', q') = (h(h')^q, qq')$ logo o cone $\mathcal{P}_{H \rtimes Q}$ é fechado para a multiplicação.

Agora mostremos que a ordem em $H \rtimes Q$ é uma ordem total. Considere $(h, q) \in H \rtimes Q$, primeiro suponha que $q \neq 1_Q$. Desde que Q é bi-ordenável, q deve ser ou positivo ou negativo em Q , tornando (h, q) ou positivo ou negativo em $H \rtimes Q$. Agora assuma que $q = 1_Q$ então (h, q) é positivo ou negativo de acordo com o sinal de h , desde que H é bi-ordenado. Além disso, se tivermos que $h = 1_H$ obtemos a identidade de $H \rtimes Q$. Então vemos que qualquer elemento de

$H \rtimes Q$ é exatamente um elemento positivo, negativo ou a identidade.

Devemos mostrar que $\mathcal{P}_{H \rtimes Q}$ é fechado para a conjugação por qualquer (a, b) em $H \rtimes Q$. Seja (h, q) um elemento no cone positivo $\mathcal{P}_{H \rtimes Q}$, isto é, $(h, q) > 1$. Então

$$\begin{aligned} (a, b)(h, q)(a, b)^{-1} &= (a, b)(h, q)((a^{-1})^{b^{-1}}, b^{-1}) = (ah^b, bq)((a^{-1})^{b^{-1}}, b^{-1}) \\ &= (ah^b((a^{-1})^{b^{-1}})^{bq}, bq b^{-1}) = (ah^b(a^{-1})^q, bq b^{-1}). \end{aligned} \quad (4.11)$$

Se $q \neq 1$, sabemos que bqb^{-1} está no cone positivo $\mathcal{P}_Q$, visto que Q é bi-ordenável.

Se $q = 1$, então $ah^b(a^{-1})^q = (ab)h(b^{-1}a^{-1})$ está em $\mathcal{P}_H$ desde que ele é fechado para a conjugação por elementos de Q . Então $(a, b)\mathcal{P}_{H \rtimes Q}(a, b)^{-1} \subset \mathcal{P}_{H \rtimes Q}$ para todo (a, b) em $H \rtimes Q$. $\square$

Considere o homomorfismo $\rho_n: \mathbb{P}_n \rightarrow \mathbb{P}_{n-1}$, onde dado $b \in \mathbb{P}_n$, $\rho_n(b)$ é obtida a partir de b omitindo-se a n -ésima corda. Para $n \geq 2$ denote por U_n o núcleo de ρ_n . Utilizando a aplicação inclusão $i: U_n \rightarrow \mathbb{P}_n$ e $\rho_n: \mathbb{P}_n \rightarrow \mathbb{P}_{n-1}$ podemos construir a seguinte sequência exata curta

$$1 \rightarrow U_n \rightarrow \mathbb{P}_n \rightarrow \mathbb{P}_{n-1} \rightarrow 1. \quad (4.12)$$

E tal sequência cinde pois se considerarmos a aplicação $\psi: \mathbb{B}_{n-1} \rightarrow \mathbb{B}_n$ definida na [Proposição 27](#) restrita a $\mathbb{P}_{n-1}$ temos que $\rho_n \circ \psi|_{\mathbb{P}_{n-1}} = Id_{\mathbb{P}_{n-1}}$.

Teorema 16. Para todo $n \geq 2$, o grupo U_n é livre com $n - 1$ geradores $\{A_{i,n}\}_{1 \leq i \leq n-1}$, onde $A_{i,n} = (\sigma_{n-1}\sigma_{n-2} \cdots \sigma_{i+1})\sigma_i^2(\sigma_{i+1}^{-1} \cdots \sigma_{n-2}^{-1}\sigma_{n-1}^{-1})$.

Demonstração. Ver em [Kassel e Turaev \(2008\)](#), Teorema 1.16. $\square$

Observação 25. Como U_n é livre com uma base composta por $n - 1$ geradores e, portanto, pela [Proposição 5](#) temos que ele é isomorfo a $F(n - 1)$, um grupo livre com $n - 1$ geradores. Assim, obtemos a seguinte sequência exata curta presente em [Habegger e Lin \(1990\)](#)

$$1 \rightarrow F(n - 1) \xrightarrow{i} \mathbb{P}_n \xrightarrow{\rho_n} \mathbb{P}_{n-1} \rightarrow 1, \quad (4.13)$$

onde $\rho_n: \mathbb{P}_n \rightarrow \mathbb{P}_{n-1}$ é definida omitindo a n -ésima corda, como já mencionado.

Podemos pensar para cada $1 \leq i \leq n$ nos geradores de $F(i - 1)$ denotados por $x_{1,i}, x_{2,i}, \dots, x_{i-1,i}$. Onde cada $x_{j,i}$ para $1 \leq j \leq i - 1$ é um $A_{j,i}$ dado explicitamente em [\(2.14\)](#) e representado na [Figura 15](#).

Por definição de sequência exata sabemos que $\ker(\rho_n) = \text{Im}(i) = F(n - 1)$, ou seja, o grupo livre com $n - 1$ geradores. Vimos que $F(n - 1)$ pode ser pensado como o grupo fundamental do disco menos os pontos $\{P_1, \dots, P_{n-1}\}$. Como tal sequência cinde, temos que

$$\mathbb{P}_n \cong F(n - 1) \rtimes \mathbb{P}_{n-1}. \quad (4.14)$$

O mesmo processo nos leva a concluir que

$$\mathbb{P}_{n-1} \cong F(n-2) \rtimes \mathbb{P}_{n-2} \quad (4.15)$$

e, assim, por indução obtemos a conhecida forma normal de Artin,

$$\mathbb{P}_n \cong F(n-1) \rtimes F(n-2) \rtimes \cdots \rtimes F(2) \rtimes F(1). \quad (4.16)$$

Então, toda trança pura sobre $\mathbb{D}$ pode ser escrita unicamente como um produto $\beta = \beta_1 \cdots \beta_{n-1}$, com $\beta_i \in F(n-i)$. As tranças $\beta_1, \dots, \beta_{n-1}$ são chamadas *coordenadas de Artin*.

Artin denominou o procedimento descrito anteriormente por “*pentear a trança*” e é conhecido como *técnica de pentear uma trança*.

Podemos concluir do [Exemplo 19](#) que:

Lema 12. O subgrupo $\mu([F, F])$ está incluído em $1 + O(2)$.

Lema 13. Sejam $X = \{x_1, \dots, x_n\}$ e F um grupo livre sobre X . Suponha que $\varphi: F \rightarrow F$ seja um automorfismo e considere a aplicação $\varphi_{ab}: F/[F, F] \rightarrow F/[F, F]$, automorfismo induzido na abelianização de F . Se φ_{ab} é a identidade, então a ordem de Magnus é invariante para φ .

Demonstração. Devemos provar que se $1 < w$, temos que $1 < \varphi(w)$, para todo $w \in F$. Temos pelo [Lema 12](#) que $\mu([F, F]) \subset 1 + O(2)$ em $\mathbb{Z}[[X_1, \dots, X_n]]$.

O automorfismo induzido pela abelianização de F é a identidade, então

$$\begin{aligned} \varphi_{ab}: F/[F, F] &\rightarrow F/[F, F] \\ x_i^{-1} + [F, F] &\mapsto \varphi_{ab}(x_i^{-1} + [F, F]) = x_i^{-1} + [F, F]. \end{aligned} \quad (4.17)$$

Como $x_i^{-1} + [F, F] = \varphi(x_i^{-1}) + [F, F]$ se, e somente se, $\varphi(x_i)x_i^{-1} \in [F, F]$ para cada i . E desde que $\mu([F, F]) \subset 1 + O(2)$, segue que $\mu(\varphi(x_i)x_i^{-1}) \in 1 + O(2)$, ou seja,

$$\begin{aligned} \mu(\varphi(x_i)x_i^{-1}) &= \mu(\varphi(x_i))\mu(x_i^{-1}) = 1 + o(2) \\ \Rightarrow \mu(\varphi(x_i)) &= (1 + o(2))\mu(x_i) = \mu(x_i) + o(2)\mu(x_i) = 1 + X_i + o(2). \end{aligned} \quad (4.18)$$

Agora dado $w \neq 1$ em F , para observar o efeito de φ em w substituímos cada x_i por $\varphi(x_i)$. A sua imagem sobre a expansão de Magnus μ substitui cada ocorrência de X_i por $X_i + o(2)$, o que implica que o primeiro termo não constante e não nulo de $\mu(w)$ e $\mu(\varphi(w))$ são iguais. Então, temos que se $1 < w$, segue que $1 < \varphi(w)$. $\square$

Observação 26. Dado $\beta \in \mathbb{B}_{n-1}$ e $\varphi: F(n-1) \rightarrow F(n-1)$ definido por $\varphi(x) = \beta^{-1}x\beta$ então existe $w_i \in F(n-1)$ que satisfaz

$$\varphi(x_{i,n}) = w_i^{-1}x_{\pi(i),n}w_i, \quad (4.19)$$

onde π é a permutação associada à trança β .

De fato, tome $\beta = \sigma_i$, onde $i \leq n-2$, então utilizando as relações presentes na apresentação de $\mathbb{B}_{n-1}$ e a relação presente na [Observação 14](#), obtemos que

$$\varphi(x_{i,n}) = \sigma_i^{-1} x_{i,n} \sigma_i = x_{i,n} x_{i+1,n} x_{i,n}^{-1}, \quad (4.20)$$

$$\varphi(x_{i+1,n}) = \sigma_i^{-1} x_{i+1,n} \sigma_i = x_{i,n}, \quad (4.21)$$

$$\varphi(x_{j,n}) = \sigma_i^{-1} x_{j,n} \sigma_i = x_{j,n}, \text{ para } j \neq i, i+1. \quad (4.22)$$

E por uma prova análoga obtemos para $\beta = \sigma_i^{-1}$, onde $i \leq n-2$, que

$$\varphi(x_{i,n}) = \sigma_i x_{i,n} \sigma_i^{-1} = x_{i+1,n}, \quad (4.23)$$

$$\varphi(x_{i+1,n}) = \sigma_i x_{i+1,n} \sigma_i^{-1} = x_{i+1,n}^{-1} x_{i,n} x_{i+1,n}, \quad (4.24)$$

$$\varphi(x_{j,n}) = \sigma_i x_{j,n} \sigma_i^{-1} = x_{j,n}, \text{ para } j \neq i, i+1. \quad (4.25)$$

O caso em que β é uma trança arbitrária segue por indução no comprimento da palavra trança representando β em $\mathbb{B}_{n-1}$ em termos dos geradores σ_i e seus inversos para $i \in \{1, \dots, n-2\}$.

Lema 14. Sejam $\beta \in \mathbb{P}_n$ e $\varphi: F(n-1) \rightarrow F(n-1)$ o automorfismo definido por $\varphi(x) = \beta^{-1} x \beta$. Então a aplicação φ_{ab} é o automorfismo identidade.

Demonstração. Recorde que se $\varphi: F(n-1) \rightarrow F(n-1)$ é um automorfismo tal que $\varphi(x) = \beta^{-1} x \beta$, então φ induz um automorfismo na abelianização

$$\begin{aligned} \varphi_{ab}: F(n-1)/[F(n-1), F(n-1)] &\rightarrow F(n-1)/[F(n-1), F(n-1)] \\ x + [F(n-1), F(n-1)] &\mapsto \beta^{-1} x \beta + [F(n-1), F(n-1)]. \end{aligned} \quad (4.26)$$

Logo, como queremos mostrar que φ_{ab} é o automorfismo identidade, devemos ter que

$$\beta^{-1} x \beta + [F(n-1), F(n-1)] = x + [F(n-1), F(n-1)] \quad (4.27)$$

e isto ocorre se, e somente se, $\beta^{-1} x^{-1} \beta x \in [F(n-1), F(n-1)]$, ou seja, existem $g, h \in F(n-1)$, tal que $\beta^{-1} x^{-1} \beta x = g^{-1} h^{-1} g h$. Pela [Observação 25](#), $\mathbb{P}_n = F(n-1) \rtimes \mathbb{P}_{n-1}$, logo se $\beta \in \mathbb{P}_n$ temos que $\beta \in F(n-1)$ ou $\beta \in \mathbb{P}_{n-1}$.

No caso em que $\beta \in F(n-1)$, então $\beta = w_i \in F(n-1)$ e para cada $i \in \{1, \dots, n-2\}$, $\varphi(x_{i,n}) = w_i^{-1} x_{i,n} w_i$, segue diretamente o que queríamos, ou seja, $w_i^{-1} x_{i,n}^{-1} w_i x_{i,n} \in [F(n-1), F(n-1)]$.

No segundo caso utilizamos a [Observação 26](#) e o fato de que se $\beta \in \mathbb{P}_n$, a permutação induzida é a identidade. Logo, para cada $i \in \{1, \dots, n-2\}$ existe $w_i \in F(n-1)$ tal que $\varphi(x_{i,n}) = w_i^{-1} x_{i,n} w_i$.

Em ambos os casos obtemos para cada $i \in \{1, \dots, n-2\}$

$$\begin{aligned} \varphi_{ab}(x_{i,n} + [F(n-1), F(n-1)]) &= \varphi(x_{i,n}) + [F(n-1), F(n-1)] \\ &= w_i^{-1} x_{i,n} w_i + [F(n-1), F(n-1)] \\ &= x_{i,n} + [F(n-1), F(n-1)], \end{aligned} \quad (4.28)$$

a última igualdade segue do fato que $w_i^{-1}x_{i,n}^{-1}w_ix_{i,n} \in [F(n-1), F(n-1)]$, visto que $w_i, x_{i,n} \in F(n-1)$. Portanto, φ_{ab} é a identidade. $\square$

Segue do [Lema 13](#) e do [Lema 14](#) a seguinte proposição.

Proposição 41. Para cada n , a ordenação de Magnus de $F(n-1)$ é invariante sob a conjugação por $\mathbb{P}_n$.

Observação 27. Note que pela [Observação 25](#) temos que $\mathbb{P}_n$ é isomorfo ao produto semidireto de grupos livres, os quais, pelo [Corolário 6](#) são bi-ordenáveis e, portanto, obtemos que $\mathbb{P}_n$ é bi-ordenado com a ordem lexicográfica da [Definição 84](#) pelo seguinte teorema:

Teorema 17. A ordem lexicográfica em

$$\mathbb{P}_n \cong F(n-1) \rtimes F(n-2) \rtimes \cdots \rtimes F(1) \quad (4.29)$$

é uma ordem bi-invariante para $n \geq 2$. Para comparar elementos $\beta_1 \cdots \beta_{n-1}$ e $\beta'_1 \cdots \beta'_{n-1}$ comparamos β_{n-i} e β'_{n-i} via a ordem de Magnus em $F(i)$ para $i = 1, \dots, n-1$, isto é, começando da direita.

Demonstração. Provaremos por indução sobre n .

Para $n = 2$, o resultado é claro, visto que, $\mathbb{P}_2 \cong F(1) \rtimes \mathbb{P}_1$, onde $\mathbb{P}_1$ é o grupo trivial e $F(1)$ é um grupo bi-ordenável pelo [Corolário 6](#). Logo, $\mathbb{P}_2$ é bi-ordenado.

Suponha que $\mathbb{P}_{n-1}$ é bi-ordenável para $n \geq 3$. Temos pela [Observação 25](#) a seguinte sequência exata curta

$$1 \rightarrow F(n-1) \xrightarrow{i} \mathbb{P}_n \xrightarrow{\rho_n} \mathbb{P}_{n-1} \rightarrow 1$$

e que $F(n-1)$ é bi-ordenado com a ordem de Magnus e $\mathbb{P}_{n-1} \cong \mathbb{P}_n / F(n-1)$ é bi-ordenado por hipótese de indução.

Como a ação por conjugação de $\mathbb{P}_n$ em $F(n-1)$ preserva ordem pela [Proposição 41](#), isto é, dados $f, f' \in F(n-1)$, tal que $f < f'$ temos para todo $g \in \mathbb{P}_n$ que $g^{-1}fg < g^{-1}f'g$, assim pelo [Lema 2](#), $\mathbb{P}_n$ é bi-ordenado. $\square$

Proposição 42. A ordem de Magnus de $\mathbb{P}_{n+1}$ estende a de $\mathbb{P}_n$, logo obtêm-se uma ordem bi-invariante em $\mathbb{P}_\infty$.

Demonstração. De fato, em $\mathbb{P}_\infty$ dizemos que $\beta \leq \beta'$ se existir n com $\beta, \beta' \in \mathbb{P}_n$, tal que $\beta \leq_n \beta'$. Para mostrar que $\leq$ é uma ordem bi-invariante, ver [Dehornoy et al. \(2008\)](#), Corolário 3.13. $\square$

O GRUPO DE HOMOTOPIA DE TRANÇAS PURAS NO DISCO É BI-ORDENÁVEL

Agora mostraremos também que o grupo de homotopia de tranças puras no disco $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ é bi-ordenável, ou seja, exibiremos uma ordenação para tal grupo que seja invariante pela multiplicação em ambos os lados, utilizando novamente a técnica de pentear de Artin juntamente com a expansão de Magnus reduzida para grupos livres reduzidos.

Além da tese [Yurasovskaya \(2008\)](#), podemos encontrar alguns desses resultados de maneira mais detalhada em [Habegger e Lin \(1990\)](#).

5.1 Grupo livre reduzido

Em [Levine \(1988\)](#) são apresentadas duas definições equivalentes de grupo livre reduzido, as quais serão enunciadas nesta seção.

Definição 85. Seja X o conjunto formado por n geradores $\{x_1, \dots, x_n\}$ e denote por F o grupo livre em X . O quociente do grupo F pela relação de equivalência que diz que x_i comuta com seus conjugados para todo $i \in \{1, \dots, n\}$ é chamado *grupo livre reduzido*.

Denotaremos um grupo livre reduzido por $RF(n)$.

Observação 28. Considere o subgrupo $J_1 = \langle [x'_i, x''_i]; 1 \leq i \leq n \rangle$ de F , onde x'_i e x''_i são conjugados de x_i . Na [Observação 18](#) vimos que dizer que cada termo comuta com seu conjugado é equivalente a dizer que todos os conjugados comutam entre si e assim podemos afirmar que o grupo livre reduzido da [Definição 85](#) coincide com o quociente F/J_1 , ou seja, $RF(n) = F/J_1$.

Para a outra definição de grupo livre reduzido introduzimos o conceito de *comutador com repetição*.

Primeiramente definimos comutadores em $X = \{x_1, \dots, x_n\}$ recursivamente:

- (1) Comutadores de peso 1 são os próprios geradores $x_1, \dots, x_n$;
- (2) Os comutadores de peso $k \geq 1$ são palavras $[C_1, C_2]$, onde C_1 e C_2 são comutadores distintos de peso k_1 e k_2 , respectivamente, tal que $k = k_1 + k_2$.

Os comutadores de peso 1 geram o grupo $F_1 = F$. O subgrupo normal gerado pelos comutadores $[x_i, x_j]$ com $1 \leq i \leq j \leq n$, de peso maior do que ou igual a 2, é denotado por F_2 . Seguindo o mesmo raciocínio obtemos para todo k , um subgrupo normal F_k de comutadores de peso maior do que ou igual a k .

Considere a série central inferior $F = F_1 \supseteq F_2 \supseteq F_3 \supseteq \dots$, como na [Definição 3](#). Sendo F um grupo livre, o mesmo é residualmente nilpotente (veja [Robinson \(1982, p. 59\)](#)), logo $\bigcap_{k \in \mathbb{N}} F_k = 1$.

Definição 86. Um conjunto de comutadores $\{C_i\}$ em $\{x_1, \dots, x_n\}$ ordenado de modo a satisfazer as seguintes propriedades, é chamado um *conjunto de comutadores básicos*:

- (1) $C_i = x_i$ se $i = 1, 2, \dots, n$;
- (2) $p(C_i) \leq p(C_j)$ se $i \leq j$ onde $p(C)$ é o peso do comutador C ;
- (3) Se $k > n$ então $C_k = [C_i, C_j]$ para algum $i < j < k$;
- (4) Se $C_j = [C_r, C_s]$ em (3) então $r \leq i$;
- (5) Todo comutador $C = [C_i, C_j]$, em que $i < j$, satisfazendo a condição (4) é um *comutador básico*.

Observação 29. Ordenamos arbitrariamente os comutadores de mesmo peso.

Exemplo 20. Considere F o grupo livre gerado por $\{x, y\}$.

Tomemos $C_1 = x$ e $C_2 = y$, com $x < y$.

Temos que $C_3 = [C_1, C_2] = [x, y]$, basta notar que C_3 satisfaz as propriedades (3) e (4) (pois $x < y$).

Ainda pelas condições (3) e (4) temos que $C_4 = [C_1, C_3] = [C_1, [C_1, C_2]] = [x, [x, y]]$. Assim, como $C_5 = [C_2, [C_1, C_2]] = [y, [x, y]]$ que também tem peso 3 e pode vir antes ou depois de C_4 .

Observe que até agora ordenamos de modo que a condição (5) seja satisfeita e obtemos a seguinte sequência

$$C_1 \leq C_2 \leq C_3 \leq C_4 \leq C_5. \quad (5.1)$$

Da mesma forma podemos determinar os demais comutadores.

Utilizaremos o seguinte teorema, conhecido como *Teorema de Hall*, na demonstração do [Teorema 19](#).

Teorema 18 (Hall). Existe um conjunto de comutadores básicos para qualquer m . Dado um conjunto de comutadores básicos $C_1 \leq C_2 \leq C_3 \leq \dots$, então cada elemento de F/F_q tem uma única representação como monômio $C_1^{e_1} C_2^{e_2} \dots C_n^{e_n}$, onde $C_1, C_2, \dots, C_n$ são todos os comutadores básicos de peso menor do que q .

Demonstração. Ver Magnus, Karrass e Solitar (1966), Teorema 5.13A. $\square$

Sejam $x_i \in X$ e C um comutador, denotaremos por r_i a quantidade de vezes em que x_i ocorre em C :

- i) Se $C = x_j$ então $r_i = 1$ se $i = j$ e $r_i = 0$ caso contrário;
- ii) Se $C = [C_1, C_2]$ então $r_i = r_1 + r_2$ onde r_k é a quantidade de vezes que x_i ocorre em C_k com $k \in \{1, 2\}$.

Definição 87. Dizemos que C é um *comutador com repetição* se existir $k \in \{1, \dots, m\}$, tal que x_k ocorre pelo menos duas vezes em C . Denotemos por J_2 o subgrupo gerado pelos comutadores com repetição.

Em Levine (1988) demonstra-se que $J_1 = J_2$. Apresentaremos a demonstração adiante no Teorema 19, o qual nos diz que as duas definições para grupo livre reduzido são equivalentes.

Proposição 43. Sejam F o grupo livre em $X = \{x_1, \dots, x_n\}$ e $\bar{N}_i$ o fecho normal de x_i em F para todo $i \in \{1, \dots, n\}$. Então o subgrupo $M = \langle [\bar{N}_i, \bar{N}_i]; 1 \leq i \leq n \rangle$ de F coincide com J_1 .

Demonstração. Segue do fato de que o fecho normal $\bar{N}_i$ de x_i em F pode ser pensado como o subgrupo gerado pelos conjugados de x_i , isto é, $\{g^{-1}x_i g; g \in F\}$. $\square$

Proposição 44. Seja C um comutador em que x_i ocorre, então $C \in \bar{N}_i$.

Demonstração. Seja n o peso de C . Se $n = 1$, então $C = x_i$ e segue que $C \in \bar{N}_i$. Suponha que o resultado seja válido para peso menor do que ou igual a n . Considere C um comutador de peso $n + 1$, temos que $C = [C_1, C_2]$ com C_k de peso n_k para $k \in \{1, 2\}$ com $n_1 + n_2 = n + 1$. Sem perda de generalidade suponha que $x_i \in C_1$. Então por hipótese de indução $C_1 \in \bar{N}_i$ e como $\bar{N}_i$ é normal, $C \in \bar{N}_i$. $\square$

Teorema 19. Sejam $X = \{x_1, \dots, x_m\}$ e F o grupo livre sobre X . O quociente do grupo F pelas relações que identificam todo comutador com repetição C com 1, ou seja, o quociente F/J_2 também é dito ser o *grupo livre reduzido*, isto é, é equivalente ao quociente F/J_1 apresentado na Definição 85.

Demonstração. A demonstração se reduz a mostrar que os subgrupos J_1 e J_2 dados na Observação 28 e Definição 87 são coincidentes.

Como cada comutador no qual aparece x_i está no fecho normal $\overline{N}_i$ de x_i em F , segue que se C é um comutador em que x_i repete, então $C \in [\overline{N}_i, \overline{N}_i] \subset J_1$ pela [Proposição 43](#).

Agora considere $[\alpha, \beta]$ em J_1 , então $\alpha, \beta \in \overline{N}_i$.

Como $\alpha \in \overline{N}_i \subset F$ pelo [Teorema de Hall](#), sabemos que α possui uma única representação na forma $W = C_1^{e_1} C_2^{e_2} \dots C_n^{e_n} \text{mod } F_{m+1}$.

Note que $F_{m+1} \subset J_2$, pois qualquer comutador com mais de m elementos deve ter repetição.

Tome C_k um comutador em W , então x_i ocorre em C_k .

De fato, considere o conjunto de comutadores em $\{x_1, \dots, x_m\}$ e tome o subconjunto formado pelos comutadores em que x_i não ocorre, ou seja, o conjunto dos comutadores em $\{x_1, \dots, \hat{x}_i, \dots, x_m\}$, onde $\hat{x}_i$ indica a supressão do gerador x_i . Considere o grupo $F' = F / \overline{N}_i$ livre em $\{x_1, \dots, \hat{x}_i, \dots, x_m\}$. Se C_k é um comutador em que x_i não ocorre então ele possui uma representação não trivial como um monômio nos comutadores básicos de F' , novamente pelo [Teorema de Hall](#). Desde que $\alpha \in \overline{N}_i$, isto viola a unicidade dada pelo [Teorema de Hall](#), neste caso aplicado a F' . Segue que x_i aparece em α e de maneira análoga mostra-se que x_i aparece em β , logo $C = [\alpha, \beta] \in J_2$.

Então $J_1 = J_2$ e segue o resultado. $\square$

5.2 Expansão de Magnus e comutadores básicos com repetição

Seja $\mathbb{Z}[[X]]$ o anel não comutativo das séries de potências formais em $X = \{X_1, \dots, X_n\}$ com coeficientes inteiros. Recordemos que a expansão de Magnus é um homomorfismo injetor do grupo livre F nos geradores $\{x_1, \dots, x_n\}$ em $\mathbb{Z}[[X]]$, dado por

$$\begin{aligned} \mu: F &\rightarrow \mathbb{Z}[[X]] \\ x_i &\mapsto 1 + X_i \\ x_i^{-1} &\mapsto 1 - X_i + (X_i)^2 - (X_i)^3 + (X_i)^4 - \dots \end{aligned}$$

Então a expansão de Magnus é um homomorfismo no grupo das unidades $\mathbb{Z}[[X]]^*$. Tal grupo é constituído pelas séries formais que podem ser escritas como $\pm 1 + p + h$, onde p é homogêneo de grau maior do que 0, e todo termo de h tem grau maior do que o grau de p que é denominado *parte principal*.

Observação 30. Recorde que o *grau total* de um polinômio p é o máximo das somas de todas as potências das variáveis em cada monômio de p .

Lema 15. Seja C um comutador de peso n em $X = \{x_1, x_2, \dots, x_n\}$, então a parte principal p de $\mu(C)$ é de grau n e, além disso, cada variável X_i ocorre em todo termo de p com grau total igual ao número de ocorrências de x_i em C .

Demonstração. Ver em [Levine \(1988, p. 365\)](#). $\square$

Exemplo 21. Seja $C = [x_2, [x_1, x_2]]$ um comutador de peso 3. Sabemos que $\mu(C)$ é um elemento de $\mathbb{Z}[[X]]$.

Temos que $C = [x_2, [x_1, x_2]] = x_2[x_1, x_2]x_2^{-1}[x_1, x_2]^{-1}$ e então

$$\mu(C) = \mu(x_2)\mu([x_1, x_2])\mu(x_2)^{-1}\mu([x_1, x_2])^{-1}. \quad (5.2)$$

Realizando as expansões separadamente, segue que

$$\mu(x_2) = 1 + X_2, \quad (5.3)$$

$$\begin{aligned} \mu([x_1, x_2]) &= \mu(x_1x_2x_1^{-1}x_2^{-1}) = \mu(x_1)\mu(x_2)\mu(x_1)^{-1}\mu(x_2)^{-1} \\ &= (1 + X_1)(1 + X_2)(1 + X_1)^{-1}(1 + X_2)^{-1} \\ &= 1 + X_1X_2 - X_2X_1 + X_2X_1^2 - X_1X_2^2 - X_1X_2X_1 + X_2X_1X_2 + o(4), \end{aligned} \quad (5.4)$$

$$\mu(x_2)^{-1} = 1 - X_2 + (X_2)^2 - (X_2)^3 + (X_2)^4 - \dots, \quad (5.5)$$

e

$$\begin{aligned} \mu([x_1, x_2])^{-1} &= \mu([x_1, x_2]^{-1}) = \mu([x_2, x_1]) = \mu(x_2x_1x_2^{-1}x_1^{-1}) \\ &= \mu(x_2)\mu(x_1)\mu(x_2)^{-1}\mu(x_1)^{-1} \\ &= (1 + X_2)(1 + X_1)(1 + X_2)^{-1}(1 + X_1)^{-1} \\ &= 1 - X_1X_2 + X_2X_1 - X_2X_1^2 + X_1X_2^2 + X_1X_2X_1 - X_2X_1X_2 + o(4). \end{aligned} \quad (5.6)$$

Substituindo as equações (5.3), (5.4), (5.5) e (5.6) em (5.2), obtemos

$$\mu(C) = 1 + 2X_2X_1X_2 - X_2^2X_1 - X_1X_2^2 + o(4), \quad (5.7)$$

onde $o(4)$ denota a soma dos termos de ordem maior ou igual à 4. E se assumimos que $x_1 < x_2 < x_3 < \dots$, então $[x_2, [x_1, x_2]]$ é um comutador básico.

A próxima proposição também se encontra em [Levine \(1988\)](#). Vamos reproduzi-la aqui apenas com o objetivo de entender as técnicas utilizadas.

Proposição 45. Sejam $\{C_1, C_2, \dots, C_n\}$ os comutadores básicos de peso $\leq q$ em X , tal que $C_1 < C_2 < \dots < C_n$ e um elemento $g \in J$ com representação $C_1^{e_1} \dots C_n^{e_n} \bmod F_{q+1}$. Nestas condições, se $e_i \neq 0$ então C_i é um comutador com repetição.

Demonstração. Se $g \in J \cap F_q$, então pelo [Teorema de Hall](#), g tem uma única representação $g = C_r^{e_r} \dots C_s^{e_s} \bmod F_{q+1}$ onde $C_r, \dots, C_s$ são comutadores básicos de peso q . A parte principal de $\mu(g)$ é $p = e_r p_r + \dots + e_s p_s$ onde p_i é a parte principal de $\mu(C_i)$. Uma propriedade de comutadores básicos é que $\{p_r, \dots, p_s\}$ forma um conjunto linearmente independente (veja em [Magnus, Karrass e Solitar \(1966\)](#)). Portanto, se $e_i \neq 0$ para algum C_i sem repetição, então pelo

Lema 15. p contém termos em que nenhuma variável tem grau total maior do que 1.

Se $f \in \overline{N}_i$, então todo termo de $\mu(f) - 1$ contém X_i com grau total maior do que 0, pois se $f \in \overline{N}_i$, então $f \in \langle \xi^{-1}x_i^e\xi : \xi \in F, e \in \{\pm 1\} \rangle$ e temos que:

Para o caso em que $e = 1$,

$$\begin{aligned}
 \mu(\xi^{-1}x_i\xi) &= \mu(\xi)^{-1}\mu(x_i)\mu(\xi) = \mu(\xi)^{-1}(1 + X_i)\mu(\xi) \\
 &= (\mu(\xi)^{-1} + \mu(\xi)^{-1}X_i)\mu(\xi) \\
 &= \mu(\xi^{-1})\mu(\xi) + \mu(\xi)^{-1}X_i\mu(\xi) \\
 &= \mu(\xi^{-1}\xi) + \mu(\xi)^{-1}X_i\mu(\xi) \\
 &= 1 + \mu(\xi)^{-1}X_i\mu(\xi),
 \end{aligned} \tag{5.8}$$

e para o caso em que $e = -1$,

$$\begin{aligned}
 \mu(\xi^{-1}x_i^{-1}\xi) &= \mu(\xi)^{-1}\mu(x_i^{-1})\mu(\xi) = \mu(\xi)^{-1}(1 - X_i + X_i^2 - \dots)\mu(\xi) \\
 &= (\mu(\xi)^{-1} - \mu(\xi)^{-1}X_i + \mu(\xi)^{-1}X_i^2 - \dots)\mu(\xi) \\
 &= \mu(\xi^{-1})\mu(\xi) - \mu(\xi)^{-1}X_i\mu(\xi) + \mu(\xi)^{-1}X_i^2\mu(\xi) - \dots \\
 &= \mu(\xi^{-1}\xi) - \mu(\xi)^{-1}X_i\mu(\xi) + \mu(\xi)^{-1}X_i^2\mu(\xi) - \dots \\
 &= 1 + \mu(\xi)^{-1}X_i\mu(\xi) + \mu(\xi)^{-1}X_i^2\mu(\xi) - \dots.
 \end{aligned} \tag{5.9}$$

Logo $\mu(\xi^{-1}x_i^e\xi) - 1$, possui o termo X_i com grau maior do que 0 e como isto é válido nos geradores de f , vale que $\mu(f) - 1$ contém X_i com grau total maior do que 0.

Como J é o subgrupo gerado por todo $[\overline{N}_i, \overline{N}_i]$, portanto se $g \in J$ então todo termo de $\mu(g) - 1$ deve conter alguma variável X_i com grau total maior do que 1. $\square$

Corolário 7. Sejam $\{C_1, C_2, \dots, C_n\}$ os comutadores básicos de peso menor do que ou igual a k em X , com $C_1 < C_2 < \dots < C_n$. Seja $f \in F$ com representação

$$C_1^{e_1} \dots C_n^{e_n} \text{ mod } F_{k+1}$$

onde k é o posto do grupo livre F . Então $f \in J$ se, e somente se, cada C_i é um comutador com repetição.

Demonstração. $\Rightarrow$) Segue do [Proposição 45](#).

$\Leftarrow$) Como F é um grupo livre de posto k , segue que $F_{k+1} \subset J$, desde que qualquer comutador de peso maior do que k deve ter repetição. $\square$

5.2.1 Expansão de Magnus reduzida

Inicialmente introduzimos e recordamos algumas notações. Temos que $\mathbb{Z}[[X]]$ denota o anel não comutativo das séries formais nas variáveis $X = \{X_1, \dots, X_n\}$ com coeficientes no anel dos números inteiros e a expansão de Magnus μ é uma aplicação do grupo livre de posto n no grupo das unidades $\mathbb{Z}[[X]]^*$.

Seja $\mathcal{R}$ o ideal bilateral de $\mathbb{Z}[[X]]$ gerado pelos monômios com repetição de alguma variável, $F_2 = [F, F]$ o subgrupo comutador e $\mathcal{D}_2$ o subgrupo multiplicativo do grupo das unidades $\mathbb{Z}[[X]]^*$ de $\mathbb{Z}[[X]]$, dado pelos elementos da forma $1 + o(2)$.

Os elementos de $1 + \mathcal{R}$ são da forma $1 +$ (monômio com repetição de uma variável).

Proposição 46. Seja F um grupo livre de posto n e tome $\mu: F \rightarrow U$ a expansão de Magnus. Então a imagem de F_2 é o subgrupo $\mathcal{D}_2$, ou seja, $\mu(F_2) = \mathcal{D}_2$.

Demonstração. Ver em Magnus, Karrass e Solitar (1966). □

Proposição 47. Seja F um grupo livre de posto n , tome $\mu: F \rightarrow U$ a expansão de Magnus e $f \in F$. Se $\mu(f) \in 1 + \mathcal{R}$, ou seja, cada termo da expansão de Magnus $\mu(f)$ tem repetição, então $f \in J$.

Demonstração. Suponha que $\mu(f) \in 1 + \mathcal{R}$, então $\mu(f) \in \mathcal{D}_2$ e pela Proposição 46, temos que $f \in F_2$.

Pelo Teorema de Hall f é expresso como um produto de comutadores de peso menor do que ou igual a n módulo F_{n+1} .

Tome o primeiro expoente não nulo para um comutador com peso i e obtemos a seguinte expressão de f

$$f = K_i K_{i+1} \cdots K_q, \quad (5.10)$$

onde cada K_j é o produto de potências de comutadores básicos de peso j , para todo $j \in \{i, \dots, q\}$. Então podemos tomar $K_j = C_{j,1}^{e_{j,1}} \cdots C_{j,r_j}^{e_{j,r_j}}$.

Suponha que f não está em J . Então pela Proposição 45 a representação (5.10) de f contém um termo de expoente não nulo para algum comutador básico sem repetição e digamos que o primeiro comutador básico sem repetição ocorre em f para os comutadores de peso m .

Agora aplique a expansão de Magnus μ para a expressão em (5.10), ou seja,

$$\mu(f) = \mu(K_i) \cdots \mu(K_{m-1}) \mu(K_m) \mu(K_{m+1}) \cdots \mu(K_q).$$

Note que para cada $j \in \{i, \dots, q\}$ temos $\mu(K_j) = 1 + p_j + h_j$ onde a parte principal é a soma dos monômios homogêneos de grau j e este é dado por $p_j = e_{j,1} p_{j,1} + \cdots + e_{j,r_j} p_{j,r_j}$, visto que $\mu(K_j) = \mu(C_{j,1}^{e_{j,1}} \cdots C_{j,r_j}^{e_{j,r_j}})$.

Cada K_j com $1 \leq j < m$ tem repetição e portanto cada termo p_j do produto $\mu(K_i) \cdots \mu(K_{m-1})$ tem repetição de algum elemento de X .

Note que pelo Lema 15 o termo p_m de $\mu(K_m)$ contém monômios de grau m sem repetição, podendo conter também termos de grau m com repetição.

Escreva o produto do restante $\mu(K_{m+1}) \cdots \mu(K_q)$ como $1 + o(m+1)$ onde $o(m+1)$ denota os termos de grau $m+1$ e maiores.

Agora multiplicamos todos os termos de $\mu(K_i) \cdots \mu(K_m) \cdots \mu(K_q)$ e obtemos a expansão de Magnus de f . A soma resultante contém termos de grau m com repetição que vem de $\mu(K_i) \cdots \mu(K_{m-1})$

e possivelmente de $\mu(K_m)$. E também contém termos sem repetição de uma variável que vem de $\mu(K_m)$. Estes termos não se cancelam, então $\mu(f)$ contém termos sem repetição de uma variável e não pode ser um elemento de $1 + \mathcal{R}$.

Logo devemos ter f em J . □

Note que se f é um termo de J então ele tem repetição e pelo [Lema 15](#) temos que $\mu(f) \in 1 + \mathcal{R}$.

Agora que estamos munidos dos resultados anteriores podemos finalmente definir a expansão de Magnus para o grupo livre reduzido $RF(n)$.

Considere Λ o quociente de $\mathbb{Z}[[X]]$ pelo ideal $\mathcal{R}$ dos monômios com repetição. Em outras palavras podemos descrever Λ como um anel de polinômios nas variáveis não comutativas $\{X_1, X_2, \dots, X_n\}$ tal que qualquer monômio com repetição de variáveis X_i para algum $1 \leq i \leq n$ é levado para o elemento identidade do anel.

A expansão de Magnus reduzida $\hat{\mu}$ é definida por

$$\begin{aligned} \hat{\mu}: RF(n) &\rightarrow \Lambda \\ \hat{x}_i &\mapsto 1 + X_i \\ \hat{x}_i^{-1} &\mapsto 1 - X_i, \end{aligned}$$

onde $\hat{x}_i$, para $i \in \{1, 2, \dots, n\}$, são os geradores de $RF(n)$.

Utilizando a [Proposição 47](#) podemos mostrar a injetividade de $\hat{\mu}$:

Teorema 20. A expansão de Magnus reduzida $\hat{\mu}: RF(n) \rightarrow \Lambda$ é injetiva.

Demonstração. Considere o seguinte diagrama com linhas exatas:

$$\begin{array}{ccccccc} 1 & \longrightarrow & J & \longrightarrow & F & \xrightarrow{p} & RF(n) \longrightarrow 1 \\ & & & & \downarrow \mu & & \downarrow \hat{\mu} \\ 1 & \longrightarrow & \mathcal{R} & \longrightarrow & \mathbb{Z}[[X]] & \xrightarrow{\pi} & \Lambda \longrightarrow 1 \end{array}$$

Observe que tal diagrama é comutativo. Seja x_i um gerador de F e note que

$$\hat{\mu} \circ p(x_i) = \hat{\mu}(\hat{x}_i) = 1 + X_i, \quad (5.11)$$

$$\pi \circ \mu(x_i) = \pi(1 + X_i) = 1 + X_i, \quad (5.12)$$

$$\hat{\mu} \circ p(x_i^{-1}) = \hat{\mu}(\hat{x}_i^{-1}) = 1 - X_i, \quad (5.13)$$

$$\pi \circ \mu(x_i^{-1}) = \pi(1 - X_i + X_i^2 - X_i^3 + \dots) = 1 - X_i. \quad (5.14)$$

Tome $\hat{f} \in RF(n)$ e suponha que $\hat{\mu}(\hat{f}) = 1_\Lambda$. Seja f uma pré-imagem de $\hat{f}$ por p . Como o diagrama é comutativo e Λ é o quociente de $\mathbb{Z}[[X]]$ por $\mathcal{R}$, temos que $\mu(f)$ é um elemento de $1 + \mathcal{R}$ e portanto pela [Proposição 47](#), $f \in J \subset \mathcal{R}$. Consequentemente $\hat{f} = p(f) = 1_{RF(n)}$. Assim, $\hat{\mu}$ é injetiva. □

5.3 $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ é bi-ordenável

Em [Mura e Rhemtulla \(1977\)](#) prova-se que todo grupo nilpotente livre de torção é bi-ordenável. Como vimos que $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ possui estas duas propriedades, então é possível mostrar que ele possui uma ordem bi-invariante.

Para construir uma ordem explícita em $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ utilizaremos o resultado dado no [Teorema 10](#), que nos diz que todo enlaçamento de intervalos é homotópico à uma trança pura, e também a expansão de Magnus reduzida.

5.3.1 Ordenando $RF(n)$

Determinaremos aqui uma ordem em Λ , o qual é o quociente do anel $\mathbb{Z}[[X]]$ pelo conjunto gerado pelos monômios com repetição $\mathcal{R}$. Utilizamos a expansão de Magnus reduzida $\hat{\mu}: RF(n) \rightarrow \Lambda$, definida por $\hat{\mu}(\hat{x}_i) = 1 + X_i$ e $\hat{\mu}(\hat{x}_i^{-1}) = 1 - X_i$ que é injetiva pelo [Teorema 20](#).

Definição 88. Sejam $f, g \in \Lambda$. Rearranje os monômios de f e g por grau e tome uma ordem alfabética nas variáveis $X_1, \dots, X_n$, isto é, considere que X_1 é a primeira letra, X_2 é a segunda letra e assim por diante. Dentro de cada grau arranje os monômios lexicograficamente. Compare cada monômio de f com os de g , grau por grau e termo por termo. Encontre o primeiro termo em que f e g diferem e olhe para os seus coeficientes ε_f e ε_g . Se $\varepsilon_f < \varepsilon_g$ diremos que $f < g$. Tal ordenação em Λ é chamada de *ordem de Magnus reduzida*.

Exemplo 22. Considere $f = 1 + X_1 + X_2 + X_3$ e $g = 1 + X_1 - X_3$, então

$$f = 1 + X_1 + X_2 + X_3 > 1 + X_1 + 0X_2 - X_3 = g. \quad (5.15)$$

Note que a ordem de Magnus reduzida não é invariante à esquerda em Λ , por exemplo, tomando 1 e $1 + X_1$ em Λ , então $1 < 1 + X_1$. Agora, considerando $-1 \in \Lambda$, temos que $(-1)1 > (-1)(1 + X_1)$.

Tome o seguinte subconjunto de Λ :

$$\mathcal{H} = \{1 + \text{monômios de grau maior do que } 0\}.$$

Observe que $\mathcal{H}$ é um subgrupo multiplicativo de Λ e, dado $g \in \mathcal{H}$, então $g = 1 + G$, onde G consiste de uma soma de monômios de grau não nulo, e seu inverso g^{-1} é dado por $1 - G + G^2 - G^3 + \dots + (-1)^n G^n$, pois $gg^{-1} = (1 + G)(1 - G + G^2 - G^3 + \dots + (-1)^n G^n) = 1 + (-1)^n G^{n+1} = 1$.

Recorde que qualquer monômio com grau maior do que n deve apresentar repetição de alguma variável X_i e, conseqüentemente, deve ser 1 no quociente Λ .

Proposição 48. O subconjunto $\mathcal{H}$ possui uma ordem bi-invariante induzida pela ordem de Magnus reduzida. Portanto, existe uma ordem bi-invariante no grupo livre reduzido $RF(n)$.

Demonstração. Dado $f \in \mathcal{H}$, arranje os monômios de f como definido na ordem de Magnus reduzida. Dizemos que f é positivo se o coeficiente do primeiro monômio de grau total não nulo é positivo. Chame tal coeficiente de *coeficiente líder de f* .

Como o coeficiente líder pode ser positivo ou negativo, obtemos que $\mathcal{P}_{\mathcal{H}} \cup \{1\} \cup \mathcal{P}_{\mathcal{H}}^{-1}$ é uma partição de $\mathcal{H}$.

Verifiquemos se $\mathcal{P}_{\mathcal{H}}$ satisfaz as condições do [Teorema 4](#):

- (i) Sejam f e g em $\mathcal{P}_{\mathcal{H}}$, então $f = 1 + F$ e $g = 1 + G$ onde F e G são compostos de uma soma de monômios com grau não nulo. Então

$$fg = (1 + F)(1 + G) = 1 + F + G + FG. \quad (5.16)$$

Temos que $fg \in \mathcal{P}_{\mathcal{H}}$. De fato, pois se $f = g$ seus coeficientes líderes coincidem, ou seja, $\varepsilon_f = \varepsilon_g$ e $\varepsilon_{fg} = \varepsilon_f + \varepsilon_g > 0$. E no caso $f \neq g$, então um dos coeficientes é maior do que o outro. Suponha que $\varepsilon_g < \varepsilon_f$ então $g < f$. Se g contém monômios de grau menor que aqueles de f , então ε_g é o coeficiente líder de fg . E se o menor grau é o mesmo para ambos f e g , então temos duas possibilidades: se lexicograficamente o menor monômio de f e g coincidem, então $\varepsilon_{fg} = \varepsilon_f + \varepsilon_g > 0$, caso contrário $\varepsilon_{fg} = \varepsilon_g > 0$ é o coeficiente líder de fg .

- (ii) $\mathcal{P}_{\mathcal{H}}$ é invariante pela conjugação de qualquer $g \in \mathcal{H}$. De fato, seja $f \in \mathcal{P}_{\mathcal{H}}$ e $g \in \mathcal{H}$ positivo, então

$$\begin{aligned} gfg^{-1} &= (1 + G)(1 + F)(1 - G + G^2 - G^3 + \cdots + (-1)^n G^n) \\ &= (1 + F + G + GF)(1 - G + G^2 - G^3 + \cdots + (-1)^n G^n) \\ &= 1 - G + G^2 + \cdots + (-1)^n G^n + F - FG + FG^2 + \cdots + F(-1)^n G^n + \\ &\quad + G - G^2 + \cdots + G(-1)^n G^n + GF - GFG + GFG^2 + \cdots + GF(-1)^n G^n \\ &= 1 + F - FG + FG^2 + \cdots + F(-1)^n G^n + GF - GFG + \cdots + GF(-1)^n G^n. \end{aligned}$$

Na expressão acima o coeficiente do termo de menor grau vem de F . Analogamente para g negativo temos:

$$\begin{aligned} g^{-1}fg &= (1 - G + G^2 - G^3 + \cdots + (-1)^n G^n)(1 + F)(1 + G) \\ &= (1 + F - G - GF + G^2 + G^2F + \cdots + (-1)^n G^n + (-1)^n G^n F)(1 + G) \\ &= 1 + G + F + FG - G - G^2 - GF - GFG + G^2 + G^3 + G^2F + G^2FG + \cdots + \\ &\quad + (-1)^n G^n + (-1)^n G^n FG \\ &= 1 + F + FG - GF + G^3 + G^2F + G^2FG + \cdots + (-1)^n G^n + (-1)^n G^n FG. \end{aligned}$$

Assim, temos também que o coeficiente do termo de menor grau vem de F . Então, como $f \in \mathcal{P}_{\mathcal{H}}$ temos que em ambos os casos $gfg^{-1} \in \mathcal{P}_{\mathcal{H}}$.

Portanto, $\mathcal{H}$ é bi-ordenável e como a expansão de Magnus reduzida $\hat{\mu}$ é injetiva podemos comparar os elementos de $RF(n)$ comparando os elementos de sua imagem em $\mathcal{H}$. $\square$

A seguinte proposição é a chave para a prova de Magnus de que grupos livres são residualmente nilpotentes:

Lema 16. O subgrupo $\hat{\mu}(RF(n)_k)$ está incluído em $1 + O(k)$.

Demonstração. Seja $o(2)$ a soma dos termos de grau 2 e maiores, $\mathcal{H}_2$ denota os elementos de $\mathcal{H}$ que são da forma $1 + o(2)$. A expansão de Magnus reduzida $\hat{\mu}$ aplica $RF(n)_2 = [RF(n), RF(n)]$ no subgrupo $\mathcal{H}_2$. Considere a e b elementos de $RF(n)$ e sejam $1 + A$ e $1 + B$ suas respectivas imagens inversas pela $\hat{\mu}$. Temos que $\hat{\mu}$ leva um comutador $aba^{-1}b^{-1}$ no subgrupo $\mathcal{H}_2$

$$\begin{aligned} \hat{\mu}(aba^{-1}b^{-1}) &= (1 + A)(1 + B)(1 - A + \dots + (-1)^n A^n + \dots)(1 - B + \dots + (-1)^n B^n + \dots) \\ &= (1 + A + B + o(2))(1 - A + o(2))(1 - B + o(2)) \\ &= (1 + B + o(2))(1 - B + o(2)) \\ &= 1 + o(2). \end{aligned}$$

Para a prova dos demais termos da série central procede-se por indução. $\square$

A próxima proposição, assim como sua demonstração, é análoga ao [Lema 13](#), só que neste caso consideramos o grupo livre reduzido:

Proposição 49. Suponha que $\varphi: RF(n) \rightarrow RF(n)$ seja um automorfismo e considere a aplicação $\varphi_{ab}: RF(n)_{ab} \rightarrow RF(n)_{ab}$, onde $RF(n)_{ab} = RF(n)/[RF(n), RF(n)]$, automorfismo induzido pela abelianização de $RF(n)$. Se φ_{ab} é a identidade, então a ordem de Magnus reduzida é preservada por φ .

Demonstração. É suficiente mostrar que se $1 < f$ temos que $1 < \varphi(f)$. Utilizando a hipótese de que φ_{ab} é a identidade em $RF(n)_{ab}$ e explorando a ação de φ nos geradores x_i , com $i \in \{1, \dots, n\}$, temos que $\varphi(x_i) = x_i C$, onde C é um elemento do subgrupo comutador $[RF(n), RF(n)]$, o que é equivalente a afirmar que $x_i^{-1} \varphi(x_i) \in [RF(n), RF(n)]$.

A imagem de $\varphi(x_i)$ pela expansão de Magnus reduzida $\hat{\mu}$ vem de

$$\hat{\mu}(\varphi(x_i)) = \hat{\mu}(x_i C) = (1 + X_i)(1 + o(2)) = 1 + X_i + o(2). \quad (5.17)$$

Para observar o efeito de φ na palavra f em $RF(n)$, substituímos cada x_i por $\varphi(x_i)$. A sua imagem sob a expansão de Magnus $\hat{\mu}$ substitui cada ocorrência de X_i por um elemento de $X_i + o(2)$, o que implica que o primeiro termo não constante e não nulo de $\hat{\mu}(f)$ e $\hat{\mu}(\varphi(f))$ são iguais. Então temos que se $1 < f$, segue que $1 < \varphi(f)$. $\square$

5.3.2 Automorfismos de $RF(n)$ e uma ordem em $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$

A seguinte construção é apresentada em [Habegger e Lin \(1990\)](#) e estabelece uma conexão entre enlaçamentos de intervalos e um subgrupo especial do grupo de automorfismos de $RF(n)$. Recorde a [Definição 66](#) que nos diz o que é um enlaçamento de intervalos, além disso, como foram definidos os conjuntos Y , Y_1 e Y_0 em (3.19), (3.20) e (3.21). Por um teorema de [Stallings \(1965\)](#) temos que as inclusões $Y_0 \rightarrow Y \leftarrow Y_1$ induzem isomorfismos nos quocientes dos grupos fundamentais pelos subgrupos das suas séries central inferior, ou seja,

$$\frac{\pi_1(Y_0)}{(\pi_1(Y_0))_m} \xrightarrow{\cong} \frac{\pi_1(Y)}{(\pi_1(Y))_m} \xleftarrow{\cong} \frac{\pi_1(Y_1)}{(\pi_1(Y_1))_m} \quad (5.18)$$

para todo m . Aqui G_m é o termo da série central inferior como definido na [Definição 3](#).

Note que $\pi_1(Y_0)$ e $\pi_1(Y_1)$ são grupos livres em n geradores. Mas, observe que quando permitimos que os segmentos de intervalos se enrolem sobre si mesmos e sobre outros segmentos, temos que $G(\sigma)$ pode não ser um grupo livre em n geradores. Entretanto, é verdade que um gerador de $G(\sigma)$ é um conjugado de um meridiano t_i , circulando a i -ésima corda para $1 \leq i \leq n$. Para ignorar os nós de σ introduzimos o grupo reduzido $\hat{G}(\sigma)$ de Y , em que os comutadores dos conjugados dos meridianos vão para 1.

Recordemos a definição alternativa do grupo livre reduzido $RF(n)$ como um quociente de um grupo livre F com n geradores pelo subgrupo normal J , gerado pelos comutadores com repetição de variável. Logo, $RF(n)$ é nilpotente, pois qualquer comutador com comprimento maior do que n deve necessariamente ser um comutador com repetição e portanto deve ser levado em 1.

Reescrevemos a relação (5.18) em termos dos grupos reduzidos

$$RF(n) \xrightarrow{\cong} \hat{G}(\sigma) \xleftarrow{\cong} RF(n). \quad (5.19)$$

O Teorema de Representação de Artin ([Teorema 9](#)) nos dá uma definição do grupo de tranças com n cordas $\mathbb{B}_n$ em termos de um subgrupo de $\text{Aut}(F(n))$, o grupo de automorfismos do grupo livre com n geradores. Estabelecemos um resultado similar considerando o quociente nilpotente $RF(n)$, introduzido em [Milnor \(1954\)](#). Então, dado qualquer enlaçamento de intervalos σ podemos obter um automorfismo de geradores $\{x_1, x_2, \dots, x_n\}$ de $RF(n)$ que satisfaz:

- (1) $\phi(x_i)$ é o conjugado de x_i , para $1 \leq i \leq n$;
- (2) $\phi(x_1 x_2 \cdots x_n) = x_1 x_2 \cdots x_n$.

Denote o conjunto de todos os automorfismos ϕ de $RF(n)$ satisfazendo as condições 1 e 2 anteriores por $\mathcal{A}_n$.

Lema 17. Os automorfismos ϕ induzem a identidade em $RF(n)_{ab}$.

Demonstração. Segue direto da definição de $\mathcal{A}_n$. □

Lema 18. Se σ e σ' são homotópicos, então $\phi_\sigma = \phi_{\sigma'}$.

Demonstração. Ver [Habegger e Lin \(1990\)](#), Lema 1.6. □

Note que o teorema anterior é semelhante ao [Teorema 9](#) que associa o grupo de tranças no disco ao grupo de automorfismos de um grupo livre.

O lema anterior mostra que a correspondência $\sigma \rightarrow \phi_\sigma$ induz um homomorfismo $\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D}) \rightarrow \mathcal{A}_n$.

Teorema 21. A aplicação

$$\begin{aligned} \hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D}) &\rightarrow \mathcal{A}_n \\ \sigma &\mapsto \phi_\sigma \end{aligned} \tag{5.20}$$

é um isomorfismo.

Demonstração. Ver [Habegger e Lin \(1990\)](#), Teorema 1.7. □

Lema 19. Existe uma sequência exata que cinde:

$$1 \rightarrow RF(n-1) \rightarrow \hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D}) \rightarrow \hat{\mathbb{P}}\mathbb{B}_{n-1}(\mathbb{D}) \rightarrow 1. \tag{5.21}$$

Demonstração. Ver [Habegger e Lin \(1990\)](#), Lema 1.8. □

Assim, obtemos de maneira análoga à realizada na [Observação 25](#) que nos diz que $\mathbb{P}_n \cong F(n-1) \rtimes F(n-2) \rtimes \cdots \rtimes F(2) \rtimes F(1)$, o fato que

$$\hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D}) \cong RF(n-1) \rtimes RF(n-2) \rtimes \cdots \rtimes RF(2) \rtimes RF(1). \tag{5.22}$$

Logo, cada classe de homotopia de enlaçamento de intervalos pode ser escrita unicamente como um produto

$$\tau = \tau_1 \cdots \tau_{n-1}, \tag{5.23}$$

onde $\tau_i \in RF(n-i)$, para $1 \leq i \leq n-1$.

Observação 31. Note que a aplicação canônica $\mathbb{P}_n \rightarrow \hat{\mathbb{P}}\mathbb{B}_n(\mathbb{D})$ é sobrejetora, visto que as projeções $F(i) \rightarrow RF(i)$, para $i = 1, \dots, n-1$ são sobrejetoras. Uma consequência disso é o que dizemos no [Teorema 10](#), ou seja, todo enlaçamento de n intervalos sobre $\mathbb{D}$ é homotópico a uma trança pura.

Combinando a [Definição 84](#), o [Lema 11](#), a [Proposição 48](#), a [Proposição 49](#), o [Teorema 21](#) e a decomposição dada em (5.22) obtemos o seguinte resultado:

Teorema 22. A ordem lexicográfica em

$$\hat{\mathbb{PB}}_n(\mathbb{D}) \cong RF(n-1) \rtimes RF(n-2) \rtimes \cdots \rtimes RF(1) \quad (5.24)$$

é uma ordem bi-invariante. Para comparar elementos $\tau_1 \cdots \tau_{n-1}$ e $\tau'_1 \cdots \tau'_{n-1}$ comparamos τ_{n-i} e τ'_{n-i} via a ordem de Magnus reduzida em $RF(i)$ para $i = 1, \dots, n-1$, isto é, começando da direita.

REFERÊNCIAS

ARTIN, E. Theorie der zöpfe. In: SPRINGER. **Abhandlungen aus dem mathematischen Seminar der Universität Hamburg**. [S.l.], 1925. v. 4, n. 1, p. 47–72. Citado nas páginas [11](#), [13](#) e [19](#).

_____. Theory of braids. **Annals of Mathematics**, JSTOR, p. 101–126, 1947. Citado nas páginas [11](#), [13](#), [19](#) e [57](#).

BIRMAN, J. Links, braids and mapping class groups. **Annals of Math. Studies**, n. 82, 1974. Citado na página [58](#).

COHEN, D. E. **Combinatorial group theory: a topological approach**. [S.l.]: Cambridge University Press, 1989. v. 14. Citado nas páginas [21](#), [26](#) e [31](#).

DEHORNOY, P.; DYNNIKOV, I.; ROLFSEN, D.; WIEST, B. **Ordering braids**. [S.l.]: Providence, RI: American Mathematical Society (AMS), 2008. v. 148. Citado nas páginas [19](#), [71](#) e [83](#).

DELANEY, C.; ROWELL, E. C.; WANG, Z. Local unitary representations of the braid group and their applications to quantum computing. **Revista Colombiana de Matemáticas**, Universidad Nacional de Colombia y Sociedad Colombiana de Matemáticas, v. 50, n. 2, p. 211–276, 2016. Citado na página [19](#).

FRANCIS, A. R. An algebraic view of bacterial genome evolution. **Journal of mathematical biology**, Springer, v. 69, n. 6-7, p. 1693–1718, 2014. Citado na página [19](#).

GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. 6. ed. Rio de Janeiro: IMPA, 2012. Citado na página [37](#).

GOLDSMITH, D. L. Homotopy of braids—in answer to a question of e. artin. In: SPRINGER. **Topology Conference**. [S.l.], 1974. p. 91–96. Citado nas páginas [11](#), [13](#), [19](#), [57](#), [62](#), [69](#) e [70](#).

HABEGGER, N.; LIN, X.-S. The classification of links up to link-homotopy. **Journal of the American Mathematical Society**, JSTOR, v. 3, n. 2, p. 389–419, 1990. Citado nas páginas [11](#), [13](#), [19](#), [62](#), [80](#), [85](#), [96](#) e [97](#).

KASSEL, C.; TURAEV, V. **Braid groups**. [S.l.]: Springer Science & Business Media, 2008. v. 247. Citado nas páginas [39](#), [42](#), [43](#), [71](#), [72](#) e [80](#).

LEVINE, J. P. An approach to homotopy classification of links. **Transactions of the American Mathematical Society**, v. 306, n. 1, p. 361–387, 1988. Citado nas páginas [85](#), [87](#), [88](#) e [89](#).

MAGNUS, W.; KARRASS, A.; SOLITAR, D. **Combinatorial Group Theory: Presentations of Groups in Terms of Generator and Relations**. [S.l.]: Interscience Publishers, 1966. Citado nas páginas [20](#), [21](#), [87](#), [89](#) e [91](#).

- MELOCRO, L. **Uma ordenação para o grupo de tranças puras**. Dissertação (Mestrado em Matemática) — Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2016. Citado na página 34.
- MILNOR, J. Link groups. **Annals of Mathematics**, JSTOR, p. 177–195, 1954. Citado na página 96.
- MURA, R. B.; RHEMTULLA, A. **Orderable groups**. [S.l.]: M. Dekker, 1977. Citado na página 93.
- MURASUGI, K.; KURPITA, B. **A Study of Braids, Mathematics and Its Applications 484**. [S.l.]: Kluwer Academic Publishers Dordrecht, 1999. Citado nas páginas 45 e 55.
- RICCA, R. L. Knots and braids on the sun. **Science and Art Sym.**, p. 263–268, 2000. Citado na página 19.
- ROBINSON, D. J. S. **A course in the theory of groups**. New York, U.S.A.: Springer-Verlag, 1982. v. 80. Citado na página 86.
- ROLFSEN, D. **Knots and links**. [S.l.]: American Mathematical Soc., 1976. v. 346. Citado nas páginas 67 e 68.
- SANTOS, H. A. **Enlaçamentos Bordantes**. Dissertação (Mestrado em Matemática) — Universidade de São Paulo, São Carlos, 2002. Citado na página 67.
- SGOBBI, W. C. **Solução do problema da conjugação para algumas extensões de grupos**. Dissertação (Mestrado em Matemática) — Universidade Federal de São Carlos, São Carlos, 2017. Citado nas páginas 34 e 35.
- STALLINGS, J. Homology and central series of groups. **Journal of Algebra**, Elsevier (Academic Press), San Diego, CA, v. 2, p. 170–181, 1965. ISSN 0021-8693. Citado na página 96.
- TENGAN, E.; BORGES, H. **Álgebra Comutativa em quatro movimentos**. Rio de Janeiro: IMPA, 2015. Citado na página 37.
- YURASOVSKAYA, E. **Homotopy string links over surfaces**. Tese (Doutorado) — University of British Columbia, 2008. Citado nas páginas 11, 13, 19 e 85.

ÍNDICE REMISSIVO

- Ação à direita, 35
- Ação por conjugação, 36
- Abelianização, 81
- Abelianização de um grupo, 95
- Anel, 37
- Anel de grupo, 38, 43
- Anel de séries formais, 75
- Anel não comutativo, 38
- Aplicação que preserva ordem, 40
- Apresentação de um grupo, 33
- Apresentação finita de um grupo, 33
- Arco, 45

- Base de um grupo livre, 28

- Coeficiente líder, 94
- Comprimento de uma palavra, 30
- Comutador, 20, 86
- Comutador básico, 86, 89
- Comutador com repetição, 85, 87
- Cone positivo, 42
- Conjunto de comutadores básicos, 86
- Conjunto de consequências, 32
- Conjunto de palavras de uma trança, 59, 63
- Conjunto de relatores, 32
- Conjunto de relatores definidores, 32
- Conjunto de símbolos geradores, 32
- Conjunto ordenado, 40
- Coordenadas de Artin, 81
- Corda da trança, 45

- Divisor de zero, 39

- Enlaçamento, 66
- Enlaçamento de n intervalos no disco, 60, 64

- Enlaçamentos de intervalos homotópicos, 62
- Expansão de Magnus, 76, 88, 90
- Expansão de Magnus reduzida, 92
- Expansão de Magnus reduzida, 93

- Família de geradores, 32
- Forma normal de Artin, 81
- Função comprimento, 24, 75, 77
- Função linear, 64
- Função linear por partes, 64
- Função própria, 64

- Geradores de Artin, 52
- Grau de uma série de potências formal, 75
- Grau total, 88
- Grupo bi-ordenável, 40, 43
- Grupo das tranças no disco, 51, 52
- Grupo das tranças puras, 55, 69
- Grupo das unidades de um anel, 39
- Grupo de homotopia de tranças puras, 62, 69, 70
- Grupo de tranças com infinitas cordas, 74
- Grupo de tranças puras, 75
- Grupo dos automorfismos, 34, 96
- Grupo finitamente apresentado, 33
- Grupo Hopfiano, 26
- Grupo livre, 22, 25, 28, 96
- Grupo livre de torção, 31, 43
- Grupo livre reduzido, 85, 87, 93
- Grupo nilpotente, 21, 96
- Grupo ordenável, 40, 43
- Grupo ordenado, 40
- Grupo reduzido de um enlaçamento, 65
- Grupo residualmente finito, 26

- Grupo residualmente nilpotente, 21, 86
- Homomorfismo por conjugação, 36
- I-ésimo intervalo de um enlaçamento, 64
- Ideal, 39, 75
- Ideal à direita, 39
- Ideal à esquerda, 39
- Invariante completo de tranças, 59
- Invariante de trança, 47
- Isotopia ambiente, 56
- Isotopia forte, 56
- Mergulho, 45
- Meridiano, 65
- Meridianos, 96
- Monoide livre, 24
- Movimento elementar, 47
- Movimento elementar de homotopia, 61
- Nó, 66
- Nós ambiente isotópicos, 67
- Nós equivalentes, 67
- Nilpotente, 39
- O índice de uma palavra, 72
- Ordem bi-invariante, 40, 83
- ordem bi-invariante, 98
- Ordem de Dehornoy, 72, 73
- Ordem de Magnus, 78, 81, 83
- Ordem de Magnus reduzida, 93, 95, 98
- Ordem de Magus reduzida, 93
- Ordem de um grupo livre, 78
- Ordem de um produto semidireto, 79
- Ordem em um conjunto, 39
- Ordem estrita em um conjunto, 40
- Ordem invariante à direita, 40
- Ordem invariante à esquerda, 40
- Ordem lexicográfica, 41, 79, 83, 98
- Ordem no grupo de homotopia, 98
- Ordem no grupo de tranças puras, 83
- Ordem total, 40
- Palavra, 24
- Palavra ciclicamente reduzida, 30, 31
- Palavra reduzida, 24
- Palavra reduzida como escrita, 30
- Palavra trança, 71
- Palavra trança σ -positiva, 72
- Palavra trança σ -negativa, 72
- Permutação cíclica de uma palavra, 31
- Permutação da Trança, 46
- Ponto duplo da projeção de uma trança, 48
- Posto de um grupo livre, 28, 90
- Produto de duas tranças, 48
- Produto direto, 34
- Produto semidireto, 34–36
- Projeção regular de uma trança, 48
- Redução de uma palavra, 24
- Redução elementar, 24
- Série central inferior, 20, 86, 96
- Série de potências formal, 75
- Segmento de uma palavra, 24
- Sequência exata curta, 36, 80, 97
- Sequência exata curta que cinde, 37
- Subgrupo comutador, 20
- Subgrupo derivado, 20
- Teorema da apresentação de Wirtinger, 67, 68
- Teorema da forma normal, 26
- Teorema de Cantor, 74
- Teorema de Hall, 87, 88
- Teorema de representação de Artin, 57, 96
- Teorema de Von Dick, 33
- Trança σ -positiva, 72
- Trança σ -negativa, 72
- Trança geométrica com n cordas, 45
- Trança inversa, 50
- Trança pura, 55
- Trança trivial, 46
- Trança trivial, 50

Tranças elementares, [51](#)

Tranças equivalentes, [47](#)

Tranças isotópicas, [56](#)

Unidade, [39](#)