UNIVERSIDADE FEDERAL
DE ALAGOAS

Universidade Federal de Alagoas
Instituto de Matemática
Curso de Licenciatura em Matemática

Marcos André dos Santos Silva

Ordenando o Grupo de Tranças no Disco

Maceió
Setembro de 2020

Marcos André dos Santos Silva

Ordenando o Grupo de Tranças no Disco

Trabalho de conclusão de curso apresentado ao corpo docente do Curso de Matemática Licenciatura da Universidade Federal de Alagoas - UFAL, *Campus* A.C. Simões, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Orientadora: Prof.ª Dra. Juliana Roberta Theodoro de Lima

Maceió
Setembro de 2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária: Taciana Sousa dos Santos – CRB-4 – 2062

S586o Silva, Marcos André dos Santos.
Ordenando o grupo de tranças no disco / Marcos André dos Santos Silva. – 2020.
88 f. : il., figs.

Orientadora: Juliana Roberta Theodoro de Lima.
Monografia (Trabalho de Conclusão de Curso em Matemática : Licenciatura) – Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2020.

Bibliografia: f. 83-84.
Apêndice: f. 85-86.
Índice remissivo: f. 87-88.

1. Teoria dos grupos. 2. Grupo de tranças Artin. 3. Ordenação (Matemática). I. Título.

CDU: 515.14

Marcos André dos Santos Silva

Ordenando o Grupo de Tranças no Disco

Trabalho de conclusão de curso aprovado pelo corpo docente do Curso de Matemática Licenciatura da Universidade Federal de Alagoas - UFAL, *Campus* A.C. Simões, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Banca Examinadora:

Prof.ª Dra. Juliana Roberta Theodoro de Lima
Instituto de Matemática - IM/UFAL, Maceió
Orientadora

Prof. Dr. André Luís Flores
Instituto de Matemática - IM/UFAL, Maceió
Examinador

Prof. Dr. Marcio Cavalcante de Melo
Instituto de Matemática - IM/UFAL, Maceió
Examinador

Maceió, 04 de Setembro de 2020

Aos meus pais José Marcos e Josefa Maria
e minha querida avó Maria de Lourdes.

Agradecimentos

À Deus, Autor da minha história, por ter me dado força, direção e a sabedoria para concluir tudo isso. Sem Ele eu não teria conseguido. O Senhor realmente é maravilhoso!

À minha orientadora e amiga Juliana Theodoro por ter acreditado em mim. Uma das melhores escolhas que fiz nessa graduação foi de ter me matriculado na turma de Estruturas Algébricas do bacharelado e conhecer uma professora que iria me acolher de uma forma muito carinhosa como filho acadêmico. Sempre me incentivando a acreditar nos meus sonhos, cada encontro que tínhamos nos seminários de iniciação científica não só eram momentos de muito aprendizado como também de alívio, conselhos e ótimas conversas.

À professora Viviane Oliveira, nossa querida coordenadora de curso, sempre pensando nos alunos. À professora Cláudia Lozada, pelas disciplinas pedagógicas lecionadas e aqueles conselhos no final da tarde em sua sala. Ao Diretor do Instituto, professor Isnaldo Barbosa. Aos professores Amauri Barros, Cícero Tiarlos, Wagner Ranter, Davi Lima, Luís Guilhermo e André Flores, que além de terem lecionados ótimos cursos da área de Matemática, ofereciam palavras de incentivo e força para nunca desistir e sempre melhorar.

À minha família, meu alicerce, que sempre me apoiaram e se esforçaram para me proporcionar condições de permanência na universidade. Gratidão.

Aos meus amigos Manasses, Sidney, Bárbara, Lara, Dandara, Joyce e Milena. Aos meus irmãos acadêmicos Alyson e Givaldo. Agradeço a paciência e companheirismo em todo momento de Lucas Carlos, ora ríamos, ora surtávamos e assim a gente ia encarando as barras que iam surgindo. À minha amigona Cristina Almeida por todo carinho e pelas inúmeras vezes em que fazíamos terapia ao conversar por horas ao telefone. A amizade de cada um destes é uma bênção em minha vida.

Aos funcionários do IM pela dedicação em nos atender e resolver nossos problemas. Em especial, a Karenn, nossa técnica em assuntos educacionais e a Deyse, que sempre cuidou do ambiente de estudos dos bolsistas PIBIC no CPMAT.

Agradeço aos servidores da Supervisão de Estatística e Avaliação da SEDUC AL, onde passei por uma experiência de estágio que foi incrível. Em especial, à Fátima Laranjeira e Alberto Vanderlei, com quem tive boas formações. Foram grandes companheiros de trabalho e bons amigos.

Aos meus professores da educação básica por terem sido dedicados e dispostos a nos

ensinar muito mais que os conteúdos curriculares e sim aprendizagens para a vida.

À todos que apoiam e defendem a educação pública de qualidade para todos, pois sem ela muitos alunos, assim como eu, não conseguiriam prosseguir os estudos.

Aos professores da banca examinadora pela leitura e correção deste trabalho.

"O amor explicou cada coisa. O amor resolveu tudo para mim. É por isso que admiro o amor onde quer que se encontre. Talvez a vida seja uma onda de surpresas... Uma onda maior do que a morte. Não tenha medo. Nunca!"

São João Paulo II

Resumo

Neste trabalho, estudaremos os grupos de tranças Artin sobre n cordas B_n, bem como sua apresentação de acordo com o Teorema da Apresentação de Artin. Além disso, iremos demonstrar que B_n não é bi-ordenável, mas que admite uma ordem total invariante à esquerda chamada σ-ordenação de Dehornoy. Mostraremos também que o grupo de tranças puras sobre n cordas PB_n é bi-ordenável, ou seja, admite uma ordem total bi-invariante.

Palavras-chave: teoria dos grupos, grupo de tranças Artin, ordenação.

Abstract

In this work we study the groups of Artin braids on n strings, namely B_n, as well as their presentation according to Artin's Presentation Theorem. In addition, we show that B_n is not bi-orderable, but that it admits a total invariant order on the left called Dehornoy σ-ordering. We will also show that the group of pure braids on n strings, namely PB_n, is bi-orderable, that is, it admits a total bi-invariant order.

Keywords: groups theory, group of Artin braids, ordering.

Lista de Figuras

Lista de Símbolos

$G, H, K \ldots$	Grupos, conjuntos, anéis ...
x^y	$y^{-1}xy$
$[x, y]$	$x^{-1}y^{-1}xy$
$G \cong H$	G é isomorfo a H
$H \leq G$	H é sugbrupo de G
$H \lhd G$	H é subgrupo normal de G
$\langle S \rangle$	Subgrupo gerado por S
$\|G\|$	Cardinalidade do conjunto G
$C_G(H), N_G(H)$	Centralizador, normalizador de H em G
$Aut(G)$	Grupo dos automorfismo de G
$K \ltimes H, H \rtimes K$	Produto semidireto de K por H
$Z(G)$	Centro de G
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$	Conjunto dos números naturais, inteiros, racionais e reais
$\mathbb{Z}_n$	$\mathbb{Z}/n\mathbb{Z}$
B_n	Grupo de tranças sobre n cordas
PB_n	Grupo de tranças puras sobre n cordas
$\beta \in B_n$	Trança sobre n cordas
$\mathscr{A}_i$	$i-$ésimo arco da trança β
B_∞	Grupo de tranças sobre infinitas cordas
$F(X)$	Grupo livre sobre a base X
$\mu(w)$	Expansão de Magnus de w
σ_i	$i-$ésima trança elementar geradora de B_n
$G = \langle X \| R \rangle$	Apresentação do grupo G
τ_n	Permutação da trança
r_n	Homomorfismo esquecimento
$R[G]$	Anel de grupo sobre R

Sumário

Apêndices

Introdução

Em 1925, o matemático alemão Emil Artin publicou o artigo *"Theorie de Zöpfe"* [1] onde formalizou o estudo algébrico e topológico de certos objetos que tinham um comportamento de entrelaçamentos no espaço euclidiano tridimensional $\mathbf{E}^3$ e que cumpriam rigorosamente algumas condições. Tais objetos foram denominados tranças , além disso demostrou que o conjunto B_n das classes de equivalência das tranças sobre n cordas (ou seja, mantendo o número de cordas fixo), munido de uma operação binária, tem estrutura algébrica de grupo. Artin, em seu Teorema da Apresentação , calculou uma apresentação por meio de geradores e relatores para B_n e demonstrou que quaisquer outras relações que os geradores de B_n satisfazem, derivam-se das relações por ele encontrada.

Os grupos de tranças foram cada vez mais sendo estudados e novos resultados e questionamentos sendo divulgados. Dentre eles, podemos perguntar se é possível ordenar o grupo de tranças Artin sobre n cordas? Temos como objeto de estudo essa pergunta e como resposta o fato de que o grupo de tranças B_n não é bi-ordenável, mas pode ser ordenado à esquerda munido de uma relação de ordem dada em [4]. Iremos mostrar que podemos representar as tranças por palavras em relação à seus elementos geradores e partir daí, utlizar a σ-ordenação de Dehornoy. Além disso, quando consideramos o conjunto PB_n das n tranças cuja permutação é trivial temos que ele é um grupo bi-ordenável, ou seja, é possível muní-lo de uma ordem total que é bi-invariante. Para isto, como a ordenabilidade é um invariante algébrico, estudaremos os grupos livres e mostraremos que eles são bi-ordenáveis e a ordenabilidade de PB_n será dada mostrando que ele é isomorfo a um produto semidireto de grupos livres, onde tal isomorfismo é chamado de Sequência Normal de Artin.

No capítulo 1 faremos um estudo dos pré-requisitos básicos da Teoria de grupos que é normalmente estudado nos cursos de graduação em Matemática. Definiremos o que é um grupo, dando exemplos, apresentando teoremas e resultados relevantes que darão auxílio ao trabalho. As duas últimas seções desse capítulo trarão o conceito de produto direto e semidireto de grupos e sequências exatas curtas onde serão muito importantes pois fornecerão suporte teórico para a demonstração da bi-ordenabilidade do PB_n. As referências desse capítulo são [5], [6] e [11].

O capítulo 2, cujas referências são [3], [8], [10] e [12], traremos a Teoria Combinatória de Grupos por meio do estudo dos grupos livres, ou seja, grupos cujos geradores satisfazem

somente as relações da definição de grupo. Esse capítulo é de extrema importância, pois a Propriedade Universal dos Grupos Livres nos permitem descrever grupos por meio de geradores e relações que esses geradores satisfazem. Tal método é denominado apresentação de grupos e será muito importante para a descrição algébrica do grupo de tranças e os demais resultados dos capítulos seguintes.

O capítulo 3 trará a descrição geométrica do grupo de tranças Artin sobre n cordas. As Figuras 3.8, 3.2 e 3.13 são encontradas em [13]. As demais figuras deste capítulos estão em [7]. Apresentaremos a definição de tranças sobre n cordas no espaço $\mathbf{E}^3$ e definir quando que as tranças são equivalentes, isto se dará por meio de uma relação de equivalência chamada de isotopia ambiente ou simplesmente isotopia. O conjunto das classes de equivalência sobre n cordas B_n será munido com uma operação binária $\cdot : B_n \times B_n \longrightarrow B_n$ e mostraremos que o par $(B_n, \cdot)$ satisfaz os axiomas da definição de grupos.

No capítulo 4, apresentaremos o que é uma ordem e quando que um grupo é ordenado. Demonstraremos que B_n não é bi-ordenável, mas possui uma ordem total que é invariante à esquerda.

No capítulo 5, concluímos o estudo deste trabalho. Será feita a ordenação de Magnus para o produto semidireto de grupos livres e escreveremos PB_n na forma normal de Artin, ou seja, como um isomorfismo do produto semidireto de grupos livres. As principais referências desses capítulos são [4], [9], [12] e [15].

As referências consultadas para a elaboração desta monografia são de domínio público.

1

Teoria Básica de Grupos

Neste capítulo, faremos um estudo da teoria básica de grupos. Iremos apresentar definições e resultados importantes de grupos que darão base para o desenvolvimento do trabalho. Este capítulo está divido nas secções 1,2 e 3 que tratam de grupos e subgrupos, produto direto e semidireto de grupos e sequências exatas, respectivamente. Como este conteúdo é visto nas disciplinas de Introdução às Estruturas Algébricas do bacharelado ou Álgebra 1 da Licenciatura em Matemática, estamos assumindo que o leitor está bem familiarizado com tais conceitos e resultados.

Para um aprofundamento da teoria e demonstrações de resultados que foram omitidos recomendamos os autores [5], [6] e [11] da referência.

1.1 Grupos e Subgrupos

Definição 1.1. Um grupo consiste de um par $(G, \star)$, onde G é um conjunto não vazio e $\star : G \times G \to G$ uma operação binária denotada simplesmente por

$$(a, b) \in G \times G \mapsto a \star b \in G$$

satisfazendo os seguintes axiomas:

1. $(a \star b) \star c = a \star (b \star c)$.
2. $\exists e \in G$ tal que $e \star a = a \star e = a, \forall a \in G$.
3. $\forall a \in G, \exists a^{-1}$ tal que $a \star a^{-1} = a^{-1} \star a = e$.

Observação 1.1. O segundo axioma garante a existência de um elemento neutro que é único. De fato, suponhamos que $e, e' \in G$ sejam elementos neutros de G, sendo assim $e = e \star e' = e'$.

Observação 1.2. O elemento inverso, definido no terceiro e último axioma, é único. Com efeito, se dado $a \in G$ com $a^{-1}, \overline{a} \in G$ são dois elementos inversos de a em G então $a^{-1} = a^{-1} \star e = a^{-1} \star (a \star \overline{a}) = (a^{-1} \star a) \star \overline{a} = \overline{a}$.

Observação 1.3. Para facilitar a escrita, escreveremos simplesmente G ao invés de $(G, \star)$ sempre que a operação binária ficar clara. Além disso, faremos ab ao invés de $a \star b$ quando não houver perigo de ambiguidade.

Observação 1.4. A Definição 1.1 de grupos dada foi feita utilizando a notação multiplicativa. Contudo, dado um conjunto G não vazio, podemos reescrever tal definição na notação aditiva, ou seja, a operação binária é dada por $+ : G \times G \longrightarrow G$ tal que $(a, b) \in G \times G \mapsto a + b \in G$. Sendo assim, o elemento neutro de $(G, +)$ será denotado por 0_G e dado um elemento $a \in G$ qualquer seu inverso aditivo será $-a \in G$.

Exemplos de grupos

Exemplo 1.1. *(O grupo aditivo e multiplicativo de um corpo)* Seja $(K, +, \cdot)$ um *corpo* qualquer. Então, $(K, +)$ e $(K - \{0_K\}, \cdot)$ são os grupos aditivo e multiplicativo do corpo K, respectivamente.

Exemplo 1.2. *(O grupo geral linear)* Seja $G = GL_n(K)$, o conjunto das matrizes invertíveis com entradas num corpo K. Claramente, G é um grupo com a operação de multiplicação usual de matrizes.

Exemplo 1.3. *(O grupo das permutações de um conjunto)* Seja X um conjunto não vazio qualquer. Vamos chamar de $B_{ij}(X)$ o conjunto das funções $f : X \to X$ que são bijetoras. Assim, $(B_{ij}(X), \circ)$ é um grupo onde a operação binária $\circ$ é a composição de funções. Quando X é finito, isto é, possui n elementos, denotaremos $B_{ij}(X)$ por S_n e será chamado de *grupo das permutações de n letras* ou *grupo simétrico*.

Exemplo 1.4. *(O grupo da circunferência unitária)* Tomando $G = S^1$, o conjunto dos números complexos z tais que $|z| = 1$, munido da multiplicação usual de números complexos é um grupo.

Definição 1.2. Dizemos que um grupo G é *abeliano* ou *comutativo* se dados $a, b \in G$ quaisquer temos $ab = ba$.

Exemplo 1.5. $(\mathbb{Z}, +)$ é um grupo abeliano.

Definição 1.3. Um subconjunto H não vazio de um grupo $(G, \star)$ é um subgrupo de G, onde denotamos $H \leq G$, se cumpre as seguintes condições:

1. $h_1 \star h_2 \in H, \forall h_1, h_2 \in G$.
2. $h_1 \star (h_2 \star h_3) = (h_1 \star h_2) \star h_3, \forall h_1, h_2, h_3 \in H$.

3. $\exists e_H \in H$ tal que $h \star e_H = e_H \star h = h, \forall h \in H$.

4. $\forall h \in H, \exists h^{-1} \in H$ tal que $h \star h^{-1} = h^{-1} \star h = e_H$.

Observação 1.5. O elemento neutro e_H de H e o inverso h^{-1} de $h \in H$ são, respectivamente, o elemento neutro e de G e o inverso de h em G.

Exemplo 1.6. $\{e\}$ e G são, claramente, subgrupos de um grupo G chamados de *subgrupos triviais*.

Exemplo 1.7. Seja $n\mathbb{Z} = \{nx; x \in \mathbb{Z}\}$ então $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$.

Exemplo 1.8. Sejam $SL_n(K)$ o conjunto das matrizes $n \times n$ com entradas num corpo K cujo determinante é igual a 1 e $SO_n(K)$ o conjunto das matrizes $n \times n$ ortogonais, isto é, se $A \in SO_n(K)$ então $AA^t = I$ (onde A^t é a transposta de A e I é a matriz identidade). Então,

$$SO_n(K) \leq SL_n(K) \leq GL_n(K).$$

Exemplo 1.9. Seja G um grupo e denotemos $C_G(x) = \{x \in G; xy = yx, \forall y \in G\}$, ou seja, o conjunto dos elementos $y \in G$ que comutam com x. Então $C_G(x) \leq G$ onde o chamamos de *centralizador* de x em G.

Exemplo 1.10. Seja G um grupo qualquer. O subconjunto $Z(G) = \{x \in G; xy = yx, \forall y \in G\}$ é um subgrupo chamado de *centro* de G.

Exemplo 1.11. Seja G um grupo, $H \leq G$ e $g \in G$ fixo. Então, o conjunto $H^g \leq \{h^g; h \in H\}$ é um subgrupo de G chamado de *subgrupo conjugado de H por g*.

Exemplo 1.12. Seja H um subgrupo do grupo G. Defina o conjunto $N_G(H) = \{g \in G; H^g = H\}$. Então $N_G(H) \leq G$, onde o chamamos de *normalizador* de G.

Veja que, em outras palavras, a Definição 1.3 diz que um subconjunto H de um grupo G é um subgrupo se com a operação binária de G, H também é um grupo. Para facilitar os cálculos, o teorema abaixo fornece uma condição necessária e suficiente para que um subconjunto de um grupo seja um subgrupo.

Teorema 1.1. *Seja G um grupo e H um subconjunto não vazio de G. Então, H é um subgrupo de G se, e somente se, satisfaz:*

1. $\forall a, b \in H$, temos $ab \in H$.

2. $\forall a \in H$ temos $a^{-1} \in H$.

Prova: ($\Rightarrow$) Vamos demonstrar que H é um grupo. Por hipótese, $H \neq \varnothing$. O item 1 nos diz que H é fechado em relação a operação binária $\star$. Este fato assegura a associatividade de $\star$ sobre os elementos de H. Por fim, dado qualquer elemento $a \in H$, pelo item 2, existe $a^{-1} \in H$, portanto, garante que cada elemento de H possui inverso. ($\Leftarrow$) Se H satisfaz as condições (1) e (2) então o resultado é imediato. □

Observação 1.6. Neste trabalho, se A e B são subgrupos do grupo G então iremos denotar por AB, BA e A^{-1} como os conjuntos $\{ab\,; a \in A\, e\, b \in B\}$, $\{ba; b \in BeA \in A\}$ e $\{a^{-1}; a \in A\}$, respectivamente. Contudo, não podemos afirmar que AB sempre será um subgrupo de G mesmo que A e B sejam! Em breve iremos oferecer condições para quando o produto de tais grupos será um grupo.

Definição 1.4. Seja S um subconjunto não vazio de um grupo G. Então, chamamos o conjunto

$$\langle S\rangle = \bigcap\{H : H \leq G, S \subseteq H\}$$

de **subgrupo gerado por** S.

A proposição a seguir caracteriza o subgrupo $\langle S\rangle$ de um grupo G.

Proposição 1.1. *Seja G um grupo e S um subconjunto de G não vazio. Então*

$$\langle S\rangle = \{a_1a_2\ldots a_n : a_j \in S \text{ ou } a_j^{-1} \in S, n \geq 1\}.$$

é um subgrupo de G.

Prova: Claramente, o conjunto do lado esquerdo está contido no conjunto do lado direito. Além disso, o conjunto $\{a_1a_2\ldots a_n : a_j \in S \text{ ou } a_j^{-1} \in S, n \geq 1\}$ é um subgrupo de G que contém S logo contém $\langle S\rangle$. □

Observação 1.7. Quando o conjunto não vazio $S = \{s_1, s_2, \ldots, s_n\}$ pertencente ao grupo G for finito, denotaremos $\langle S\rangle$ por $\langle s_1, s_2, \ldots, s_n\rangle$ para nos referirmos ao conjunto $\langle\{s_1, s_2, \ldots, s_n\}\rangle$. Conforme a Proposição 1.1 temos que se $a \in G$ então $\langle a\rangle \doteq \{\ldots, (a^{-1})^2, a^{-1}, e, a, a^2, \ldots\}$. De modo prático, escrevemos $\langle a\rangle = \{a^k; k \in \mathbb{Z}\}$.

Definição 1.5. Um grupo G é chamado de *cíclico* quando é gerado por um elemento. Em outras palavras, se existe um $g \in G$ tal que $\langle g\rangle = G$. Neste caso, g é dito ser um *gerador* para G.

Exemplo 1.13. O grupo aditivo dos inteiros é gerado por $\{1\}$, ou seja, $\mathbb{Z} = \langle 1\rangle$.

Exemplo 1.14. Seja $U_n = \{1, e^{\frac{2\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\}$ o grupo multiplicativo das raízes do polinômio $p : \mathbb{C} \longrightarrow \mathbb{C}$, $p(z) = x^n + 1$ (ou seja, as n-ésimas raízes da unidade) munido da multiplicação usual de números complexos. Então, $U_n = \langle e^{\frac{2\pi i}{n}}\rangle$.

Definição 1.6. Seja G um grupo. O conjunto $\langle\{xyx^{-1}y^{-1}; x, y \in G\}\rangle$ é chamado de *subgrupo dos comutadores* de G.

Definição 1.7. Dizemos que a ordem de um grupo G é a cardinalidade do conjunto G e denotamos por $|G|$. Se $g \in G$ então denotaremos a ordem de g por $O(g)$, ou ainda, $|g|$ como a ordem do subgrupo gerado por g. Os elementos de um grupo que tem ordem 2 são chamados de *involuções*.

Exemplo 1.15. Temos que $|\mathbb{Z}| = \infty$, $|\frac{\mathbb{Z}}{n\mathbb{Z}}| = n$ e $|S_n| = n!$.

Definição 1.8. Um *grupo de torsão, ou grupo periódico* é um grupo G onde todos os seus elementos possuem ordem finita, ou seja, para todo $g \in G$ temos que $|g| = n$ é finito. Um grupo G é *livre de torsão* se, com excessão do elemento identidade e_G, todos os elementos possuem ordem infinita.

1.1.1 Classes Laterais e o Teorema de Langrange

Tomemos G um grupo e H um subgrupo de G. Vamos definir a seguinte relação de equivalência $\mathcal{R}_E$ sobre G. Com efeito, dados $a, b \in G$ temos que

$$b\mathcal{R}_E a \Leftrightarrow \exists h \in H \, tal \; que \, b = ah.$$

É de fácil verificação que $\mathcal{R}_E$ é uma relação de equivalência. Com efeito, para quaisquer $a, b, c \in G$ a relação $\mathcal{R}_E$ cumpre as seguintes propriedades

1. **Reflexividade:** $a\mathcal{R}_E a \Leftrightarrow \exists h \in H$ tal que $a = ah$. Basta tomar $h \doteq e$, onde e é o elemento neutro de G.

2. **Simetria:** $a\mathcal{R}_E b \Leftrightarrow \exists h \in H$ tal que $a = bh \Leftrightarrow ah^{-1} = b \Leftrightarrow b\mathcal{R}_E a$.

3. **Transitividade:** $a\mathcal{R}_E b$ e $b\mathcal{R}_E c \Leftrightarrow \exists h_1, h_2 \in H$ tais que $a = bh_1$ e $b = ch_2 \Leftrightarrow a = bh_1 = ch_2h_1 = c(h_2h_1) \Leftrightarrow a\mathcal{R}_E c$.

Observação 1.8. De maneira similiar, podemos definir a relação de equivalência ${\mathcal{R}'}_E$ fazendo $a{\mathcal{R}'}_E b \Leftrightarrow \exists h \in H$ tal que $a = hb$.

Definição 1.9. A classe de equivalência, segundo a relação $\mathcal{R}_E$, que contém o elemento a é chamada de *classe lateral à direita* de H em G donde

$$\overline{a} = Ha = \{b \in G; b\mathcal{R}_E a\} = \{ha; h \in H\}.$$

Da mesma forma, podemos definir a classe lateral à esquerda de H em G, segundo a relação $\mathcal{R}_E$, que contém a como

$$\overline{a} = aH = \{b \in G; b\mathcal{R}_E a\} = \{ah; h \in H\}.$$

Observação 1.9. Note que se H é um subgrupo de um grupo G então $aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}$. Além disso, é fácil ver que $\forall a \in G$ a bijeção $h \mapsto xh$ de H em xH nos fornece que H tem a mesma cardinalidade que xH. Também podemos concluir que a união de todas as classes laterais à esquerda (respectivamente, à direita) resulta em G.

Definição 1.10. Dizemos que a cardinalidade do conjunto das classes laterais é o índice de H em G, onde será denotado por $(G : H)$.

Definição 1.11. Um subconjunto T de um grupo G, que contém um e somente um elemento de cada classe lateral de H em G é chamado de *conjunto de representantes de classes laterais* ou *transversal*. Evidentemente, a existência de T depende do Axioma da Escolha.

Exemplo 1.16. Se $G = \mathbb{Z}$, o grupo aditivo dos inteiros, e $H = \langle m \rangle$ o subgrupo múltiplo dos inteiros $m > 1$. Temos então m classes laterais distintas, a saber,

$$[0], [1], \ldots, [m-1].$$

Logo, um transversal seria $T = \{0, 1, 2, \ldots, (m-1)\}$.

Teorema 1.2. *(Teorema de Lagrange) Se G é um grupo finito e H um subgrupo de G então*

$$|G| = |H|(G : H).$$

Prova: Como H é subgrupo G então $|H| \leq |G|$. A observação 1.9 garante que as classes laterais possuem a mesma cardinalidade que H, ou seja, $|H| = |Ha|, \forall a \in G$. Além disso, temos que $(G : H) \leq |G|$. Sabemos que $G = \bigcup_{a \in G} Ha$, então podemos dizer que

$$|G| = \sum_{a \in G} |Ha|.$$

Sendo assim, concluímos que $|G| = |H|(G : H)$. □

Corolário 1. Seja H um subgrupo de um grupo finito G. Então a ordem de H divide a ordem de G

Corolário 2. Se G é um grupo cíclico, finito de ordem p prima então seus subgrupos são somente os subgrupos triviais.

Corolário 3. Seja G um grupo finito de ordem k. Então $g^k = e$ para todo $g \in G$.

Observação 1.10. É fácil perceber que a recíproca do Teorema de Lagrange é falsa. Contudo, se o grupo em questão for abeliano então torna-se válida.

1.1.2 Subgrupos Normais e Grupos Quocientes

Havíamos observado que dados K, H subgrupos de um grupo G nem sempre os conjuntos KH e HK poderiam ser também subgrupos de G. Veremos que se um destes subgrupos possuir uma determinada propriedade, então o produto entre eles será sempre um subgrupo. Essa questão e outros resultados importantes serão estudados nesta seção. Vamos definir e estudar os *subgrupos normais*: aqueles que são preservados por conjugação. Tais subgrupos possuem uma grande importância para a Álgebra, pois construímos com eles os *grupos quocientes*, revelando resultados incríveis para o estudo de grupos.

Proposição 1.2. *Se H e K são subgrupos de G, HK é um subgrupo de G se, e somente se, $KH = HK$. Neste evento $HK = \langle H, K\rangle = KH$.*

Prova: ($\Rightarrow$) Suponha que $HK \leq G$ então $H \leq HK$ e $K \leq HK$, assim $KH \subseteq HK$. De maneira análoga concluímos que $HK \subseteq KH$, donde temos $KH = HK$. Além disso, $\langle H, K\rangle \leq HK$ desde que $HK \leq G$, enquanto $HK \subseteq \langle H, K\rangle$ é sempre verdade; portanto $HK = \langle H, K, \rangle$. ($\Leftarrow$) Reciprocamente, suponha que $HK = KH$. Se $h_i \in H$ e $k_i \in K$, onde $i \in \{1, 2\}$, então

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1}.$$

Veja que, $(k_1k_2^{-1}) = h_3k_3$ onde $h_3 \in H$ e $k_3 \in K$. Consequentemente, $h_1k_1(h_2k_2)^{-1} = (h_1k_3)k_3 \in HK$ o que implica $HK \leq G$, conforme o Teorema 1.3. □

Definição 1.12. Um subgrupo H de um grupo G é chamado de *subgrupo normal* de G, denotado por $H \lhd G$, se satisfaz uma (e, portanto, todas) das condições abaixo:

1. A operação induzida sobre as classes laterais de H em G é bem definida.
2. $xHx^{-1} = H$ para todo $x \in G$.
3. $xHx^{-1} \subseteq H$ para todo $x \in G$.
4. $xH = Hx$ para todo $x \in G$.

Observação 1.11. Independente do grupo G, os subgrupos $\{e\}$ e G são subgrupos normais de G. Quando um grupo possui como subgrupo normais apenas $\{e\}$ e G então o chamamos de *grupo simples*.

Exemplo 1.17. Todo subgrupo H de um grupo abeliano G é automaticamente normal. Contudo, a recíproca **não** é verdadeira.

Exemplo 1.18. $(n\mathbb{Z}, +)$ é um subgrupo normal de $\mathbb{Z}$.

Exemplo 1.19. Se G é um grupo então $Z(G) \lhd G$. Além disso, todo subgrupo H de $Z(G)$ é normal a G.

Teorema 1.3. *Se H é um subgrupo normal de um grupo G, então o conjunto das classes laterais, denotado por G/H, tem estrutura de grupo relativamente ao produto natural*

$$(xH)(yH) = xyH$$

onde o elemento neutro é a classe lateral $eH = H$ e o inverso da classe lateral xH é a classe lateral $x^{-1}H$.

Prova: A associatividade de G/H segue de G. Para toda classe lateral xH de G/H temos que $(xH)H = (xH)(eH) = xeH = xH$.

E por fim, se yH é uma classe lateral qualquer de G/H então tomando a classe lateral $x^{-1}H$ de G/H temos $(xH)(x^{-1}H) = xx^{-1}H = eH = H$. □

Definição 1.13. Seja H um subgrupo normal de um grupo G. Então o conjunto das classes laterais com a operação induzida de G é chamado de *grupo quociente* de G por H. Usaremos a notação G/H ou $\frac{G}{H}$.

Observação 1.12. Se o grupo G for finito, o teorema 1.2 garante que

$$|G/H| = \frac{|G|}{|H|}.$$

Proposição 1.3. *Sejam H, K dois subgrupos de G. Então HK é um subgrupo normal de G se, e somente se, $HK = KH$.*

Observação 1.13. Se H e K são subgrupos de um grupo G e algum deles é normal a G então HK é um subgrupo de G.

Definição 1.14. Seja X um subconjunto não vazio de um grupo G. Definimos por *fecho normal* de X em G a intersecção de todos os subgrupos normais de G que contém G onde será denotado da seguinte maneira

$$\langle X \rangle^G = \bigcup_{\lambda \in \Gamma} H_\lambda,\ H_\lambda \lhd G,\ \forall \lambda \in \Gamma.$$

Note que este é o menor subgrupo normal de G que contém X e pode ser caracterizado como

$$\langle X \rangle^G = \langle \{gxg^{-1}; g \in G \text{ e } x \in X\} \rangle.$$

1.1.3 Homomorfismos de Grupos

Definição 1.15. Sejam $(G, \star)$ e $(K, \cdot)$ dois grupos. Então dizemos que a aplicação $f : G \to K$ é um homomorfismo se ela cumpre a condição abaixo

$$f(a \star b) = f(a) \cdot f(b), \forall a, b \in G$$

.

Exemplo 1.20. $I_d : (G, \star) \to (G, \star)$ dado por $I_d(g) = g$ é um homomorfismo chamado de *identidade* de G.

Exemplo 1.21. Seja $(G, \star)$ um grupo abeliano e $n \in \mathbb{Z}$ fixo. Então $\phi : G \to G$ dada por $\phi_n(g) = g^n$ é um homomorfismo.

Exemplo 1.22. Sejam G um grupo e H um subgrupo normal de G. A aplicação

$$\pi : G \to G/H$$

$$g \mapsto \pi(g) = gH$$

é um homomorfismo chamado *projeção canônica*.

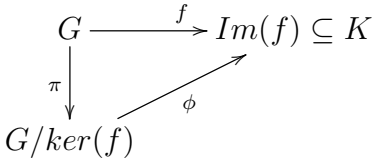
Definição 1.16. Seja $f : G \to K$ um homomorfismo de grupos. Os conjuntos $ker(f) = \{g \in G; f(g) = e_G\}$ e $Im(f) = \{f(g) \in K; g \in G\}$ são subgrupos de G e K, respectivamente, chamados de *núcleo* e *imagem* de f.

Observação 1.14. Note que $ker(f) \lhd G$, pois como consequência da definição de homomorfismo temos que $f(e_G) = e_K$ o que implica $e_G \in ker(f)$. Dados $x, y \in ker(f)$ temos que $f(x) = f(y) = e_K$ daí $f(xy^{-1}) = f(x) \cdot f(y)^{-1} = e_K \cdot e_K^{-1} = e_K$. Portanto, $ker(f)$ é um subgrupo de G. A normalidade segue de que se $a \in ker(f)$ e $g \in G$ é um elemento arbitrário, temos que $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)f(g^{-1}) = e_K$. Logo, $gker(f)g^{-1} \subseteq ker(f)$ satisfazendo um dos itens (portanto, todos) da definição 1.12.

Definição 1.17. Um homomorfismo de grupos $f : G \to K$ é chamado de

1. *Monomorfismo* quando f é injetor, ou seja, $f(a) = f(b)$ então $a = b$.
2. *Epimorfismo* quando f é sobrejetor, ou seja, se $Im(f) = K$.
3. *Isomorfismo* quando f é injetor e sobrejetor.

Teorema 1.4. *(Teorema do Isomorfismo I) Seja $f : G \to K$ um homomorfismo de grupos. Então, $ker(f)$ é um subgrupo normal de G e existe um único isomorfismo $\phi : G/ker(f) \longrightarrow Im(f)$ tal que $\phi \circ \pi = f$, ou seja, faz comutar o diagrama abaixo:*



Prova: Na Observação 1.14 fizemos a verificação de que $ker(f) \lhd G$. Para provar a existência de ϕ defina a aplicação $\phi : G/ker(f) \longrightarrow Im(f) \subseteq K$ dada por

$$\phi(ker(f)g) = f(g).$$

Tal aplicação é bem definida e independe do representanmte da classe lateral tomada.

Dados dois elementos quaisquer $(ker(f)g, (ker(f)h) \in G/ker(f)$ temos que

$$\begin{aligned}\phi((ker(f)g(ker(f)h)) &= f((ker(f)g(ker(f)h)\\ &= f(ker(f)g)f(ker(f)h)\\ &= f(g)f(h)\\ &= \phi(g)\phi(h)\end{aligned}$$

Se $\phi((ker(f)g) = e_K$ então $f(g) = e_K$. Portanto, ϕ é injetora. A verificação da unicidade da aplicação ϕ e sua sobrejetividade é dada por construção. □

O resultado acima nos permite fazer a descrição de grupos quociente por meio de isomorfismos.

Exemplo 1.23. Seja o homomorfismo de grupos $f : \mathbb{R} \to S^1$, onde $f(x) = e^{2\pi ix}$. Temos que $ker(f) = \mathbb{Z}$ então $\mathbb{R}/\mathbb{Z} \cong S^1$.

Exemplo 1.24. Seja $det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ o homomorfismo determinante, que a cada matriz $A \in GL_n(\mathbb{R})$ associa seu determinante $det(A) \in \mathbb{R}^*$ então $ker(det) = SL_n(\mathbb{R})$ e, portanto, $GL_n\mathbb{R}/SL_n\mathbb{R} \cong \mathbb{R}^*$.

Teorema 1.5. *(Teorema do Isomorfismo II) Sejam H e K subgrupos de G com $H \lhd G$. Então $H \cap K \lhd K$ e $K/(H \cap K) \cong KH/H$.*

Prova: A aplicação $\alpha : KH \longrightarrow KH/H$ dada por $\alpha(x) = Hx, x \in KH$ é um epimorfismo de H em KH/H cujo kernel é $H \cup K$. Pelo Teorema do Isomorfismo I temos que $K/(H \cup K) \cong KH/H$. □

Observação 1.15. Se G for finito, o teorema de Lagrange nos fornece que $\frac{|K|}{|K \cap H|} = \frac{|KH|}{|H|}$.

Teorema 1.6. *(Teorema do Isomorfismo III) Sejam H e K subgrupos normais de um grupo G. Então $\frac{G/K}{H/K} \cong G/H$.*

Prova: Defina a aplicação $\alpha : G/K \longrightarrow G/H$ por $\alpha(Kg) = Hg, g \in G$. Como K e H são subgrupos normais de G a aplicação é bem definida e claramene é um epimorfismo cujo kernel é H/K. Sendo assim, $\frac{G/K}{H/K} \cong G/H$. □

Observação 1.16. O teorema acima nos garante, quando G for finito, que $(G : H) = (G : K)(H : K)$. Contudo, para este resultado, a condição da normalidade de H e K não são necessárias.

Definição 1.18. Seja $(G, \star)$ um grupo. Se $f : G \to G$ é um isomorfismo então o chamaremos de automorfismo. Denotaremos por $Aut(G)$ ao conjunto de todos os automorfismos de G.

Exemplo 1.25. $Aut(\mathbb{Z}) = \{I_d, -I_d\}$.

Definição 1.19. Sejam x, g elementos de um grupo G. Escreveremos x^g para detonar o conjugado de x por g, ou seja,

$$x^g = g^{-1}xg.$$

Além disso, a função $\theta_g : G \longrightarrow G$ dada por $\theta_g(x) = x^g$ é um automorfismo chamado de *automorfismo interior* de G por g. O conjunto de todos os automorfismos interiores de G é denotado por $Inn(G)$.

1.2 Produto Direto e Semidireto de Grupos

Nesta seção, faremos a definição de produto direto e semidireto de grupos. Queremos escrever um grupo G em termos de grupos menos complexos. Esse conteúdo será de grande importância para o desenvolvimento do trabalho e para a conclusão do resultado final a ser demonstrado, pois o grupo de tranças puras PB_n se escreve como o produto semidireto de grupos chamados livres.

Definição 1.20. Sejam G e H grupos cujas identidades são 1_G e 1_H, respectivamente. O conjunto $G \times H = \{(g, h); g \in G, h \in H\}$ munido da operação abaixo

$$\cdot : (G \times H) \times (G \times H) \longrightarrow (G \times H)$$

$$((a, b), (c, d)) \longmapsto (ac, bd), \forall a, b \in G \, e \, \forall c, d \in H$$

é um grupo e o chamamos de *o produto direto* de G por H. O elemento neutro do grupo $(G \times H, \cdot)$ é $(1_G, 1_H)$ e se $(a, b) \in (G \times H, \cdot)$ então seu elemento inverso será (a^{-1}, b^{-1}).

Observação 1.17. A definição acima pode ser generalizada para um número finito de grupos. Com efeito, seja $\{G_\lambda\}_{1 \leq \lambda \leq n}$ uma família não vazia de grupos multiplicativos quaisquer. Seja $G \doteq G_1 \times G_2 \times \ldots \times G_n$ o produto cartesiano dos conjuntos $G_1, G_2, \ldots, G_n$ e para quaisquer dois elementos $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in G$ defina a seguinte operação

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

Então, $(G, \cdot_\lambda)$ é um grupo. É fácil ver que o elemento neutro de G é $e_G = (e_1, e_2, \ldots, e_n)$, onde $e_\lambda \in G_\lambda$, para $\lambda \in \{1, 2, \ldots, n\}$. Se $(a_1, a_2, \ldots, a_n)$ é um elemento de G enão seu inverso $(a_1, a_2, \ldots, a_n)^{-1}$ será $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.

Proposição 1.4. *$G \doteq G_1 \times \ldots \times G_n$ é abeliano se, e somente se, cada grupo $G_1, \ldots, G_n$ é abeliano.*

Prova: ($\Rightarrow$) Se G é abeliano então para quaisquer elementos $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G$ temos que $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (b_1, \ldots, b_n) \cdot (a_1, \ldots, a_n)$. O que nos fornece

$(a_1b_1, \ldots, a_nb_n) = (b_1a_1, \ldots, b_na_n)$. ($\Leftarrow$) Reciprocamente, seja G_i abeliano $\forall i \in \{1, 2, \ldots, n\}$. Sendo assim, dados $a_i, b_i \in G_i$ temos $a_ib_i = a_ib_i$. Portanto,

$$\begin{aligned}(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) &= (a_1b_1, \ldots, a_nb_n) \\ &= (b_1a_1, \ldots, b_na_1) \\ &= (b_1, \ldots, b_n) \cdot (a_1, \ldots, a_n)\end{aligned}$$

□

Observação 1.18. Quando $G_i, \forall i \in \{1, 2, \ldots, n\}$ for um grupo aditivo é comum chamarmos o produto direto de *soma direta*, onde substituímos a notação multiplicativa pela aditiva. Ou seja, em vez de $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n)$ fazemos $(a_1, \ldots, a_n) + (b_1, \ldots, b_n)$.

A partir de agora vamos construir uma estrutura algébrica que é uma generalização do produto direto entre dois grupos. Relembre que denotamos por $Aut(G)$ o conjunto dos automorfismo de G. Sobre esse conjunto vamos definir a seguinte operação binária

$$\begin{aligned}\bullet : Aut(G) \times Aut(G) &\longrightarrow Aut(G) \\ (\alpha, \beta) &\longmapsto \alpha \bullet \beta \doteq \beta \circ \alpha : G \to G.\end{aligned}$$

Nessas condições, $(Aut(G), \bullet)$ tem estrutura de grupo, donde seu elemento identidade é o automorfismo $I_d : G \to G$ e dado $\alpha \in Aut(G)$ seu inverso será $\alpha^{-1} : G \to G$.

Definição 1.21. Dado um grupo K, dizemos que dois subgrupos A e B de K são *complementos* um do outro (ou que são subgrupos complementares) em K se cumprem:

1. $K = AB = \{ab \,;\, a \in A \, e \, b \in B\}$.
2. $A \cap B = \{1_K\}$.

Definição 1.22. Se K e H são subgrupos de um grupo G tais que $H \lhd G, H \cap K = e_G$ e $G \doteq KH = \{kh \,;\, k \in K \, e \, h \in H\}$, dizemos que G é o *produto semidireto interno* de K por H, denotado por $G = K \ltimes H$, ou também, $G = H \rtimes K$.

Observação 1.19. Podemos observar que na Definição 1.22 K e H são subgrupos complementares de G.

Teorema 1.7. *Sejam H e K dois grupos, $\phi : K \to Aut(H)$ um homomorfismo e $\cdot_\phi$ a operação definida sobre $H \times K$ dada por $(h_1, k_1) \cdot_\phi (h_2, k_2) := (h_1\phi(k_1)h_2, k_1k_2)$. Então, $(H \times K, \cdot_\phi)$ é um grupo.*

Prova: Vamos mostrar que o par $(H \times K, \cdot_\phi)$ satisfaz os axiomas da Definição 1.1. Com efeito,

i.) Sejam $(h_1, k_1), (h_2, k_2)$ e (h_3, k_3) elementos de $H \times K$ então

$$\begin{aligned}[(h_1, k_1) \cdot_\phi (h_2, k_2)] \cdot_\phi \cdot_\phi (h_3, k_3) &= (h_1\phi(k_1)h_2, k_1k_2) \cdot_\phi (h_3, k_3) \\ &= (h_1\phi(k_1)h_2\phi(k_1k_2), k_1k_2k_3) \qquad (1.1)\end{aligned}$$

Analogamente,

$$\begin{aligned}(h_1, k_1) \cdot_\phi [(h_2, k_2) \cdot_\phi \cdot_\phi (h_3, k_3)] &= (h_1, k_1) \cdot_\phi (h_2\phi(k_2)h_3, k_2k_3) \\ &= (h_1\phi(k_1)h_2\phi(k_2)h_3, k_1k_2k_3) \qquad (1.2)\end{aligned}$$

A operação $\cdot_\phi$ é associativa em $H \times K$.

ii.) (e_H, e_K) é o elemento neutro de $(H \times K, \cdot_\phi)$, onde e_H e e_K denotam os elementos neutros de H e K, respectivamente. De fato, para todo $(h, k) \in H \times K$ temos que $(e_H, e_K) \cdot_\phi (h, k) = (e_H\phi(e_K)h, e_Kk) = (h, k)$.

iii.) Finalmente, o inverso de todo elemento $(h, k) \in H \times K$ é dado por $(\phi(k^{-1})(h^{-1}), k^{-1})$. De fato,

$$\begin{aligned}(h, k) \cdot_\phi (\phi(k^{-1})(h^{-1}), k^{-1}) &= (h\phi(k)\phi(k^{-1}(h^{-1}), kk^{-1}) \\ &= (h\phi(k)\phi(k)^{-1}h^{-1}, e_K) \\ &= (he_Hh^{-1}, e_K) = (e_H, e_K) \qquad (1.3)\end{aligned}$$

□

Definição 1.23. O grupo $(H \times K, \cdot_\phi)$ é chamado de *produto semidireto externo* de H por K com respeito ao homomorfismo $\phi : K \to Aut(H)$. onde denotamos por $K \ltimes_\phi H$, e também $H \rtimes_\phi K$.

Observação 1.20. Se na definição anterior $\phi : K \longrightarrow Aut(H)$ for trivial, ou seja, associe qualquer elemento $k \in K$ no homomorfismo identidade $id : H \longrightarrow H$ então o produto semidireto coincide com o produto direto.

Observação 1.21. Observe que se $\phi : K \to Aut(H)$ não for trivial, então $K \ltimes_\phi H$ não será abeliano. De fato, existirão $h \in H$ e $k \in K$ tais que $\phi(k)(h) \neq h$, o que implica, $(h, e_K) \cdot_\phi (e_H, k) = (h, k)$ e $(e_H, k) \cdot_\phi (h, e_K) = (\phi(k)h, k)$. Consequentemente, por meio do produto semidireto, obtemos uma ferramenta para a construção de grupos não abelianos.

Lema 1.1. *Sejam A e B sugrupos de um grupo G tais que $A \lhd G$, $A \cap B = \{e_G\}$ e $G = AB$. Então $G \cong B \ltimes_\theta A$, onde θ é a conjugação por um elemento de B.*

Exemplo 1.26. Seja $G = GL_2(\mathbb{R}), H = SL_2((R)) \lhd G$ e K é o subgrupo das matrizes diagonais $M(a)$ de G. Então, $\theta : K \longrightarrow Aut(SL_2(\mathbb{R}))$ é o homomorfismo que associa

$M(a)$ no automorfismo de $SL_2(\mathbb{R})$ dado pela conjugação por $M(a)$:

$$C \in SL_2(\mathbb{R}) \mapsto M(a)PM(1/a) \in SL_2(\mathbb{R}),$$

e, pelo lema acima,

$$GL_2(\mathbb{R}) \cong K \ltimes_\theta SL_2(\mathbb{R}).$$

Teorema 1.8. *Sejam H e K dois grupos e $\theta_1, \theta_2 : K \longrightarrow Aut(H)$ dois homomorfismos. Então*

1. *Se existir $\sigma \in Aut(H)$ tal que $\theta_2(k) = \sigma\theta_1(k)\sigma^{-1}$, para todo $k \in K$, então*

$$K \ltimes_{\theta_1} H \cong K \ltimes_{\theta_2} H.$$

2. *Se $\theta_1 = \theta_2 \circ \beta$, para algum $\beta \in Aut(K)$, então $K \ltimes_{\theta_1} H \cong K \ltimes_{\theta_2} H$.*

Prova: Vamos construir um isomorfismo de $K \ltimes_{\theta_1} H$ em $K \ltimes_{\theta_2} H$. Com efeito, defina a seguinte aplicação

$$\psi : K \ltimes_{\theta_1} H \longrightarrow K \ltimes_{\theta_2} H$$

$$(h, k) \mapsto (\sigma(h), k)$$

.

- ψ é um homomorfismo. De fato, dados $(h_1, k_1), (h_2, k_2) \in K \ltimes_{\theta_1} H$ então $(h_1, k_1)(h_2, k_2) = (h_1\theta_1(k_1)(h_2), k_1k_2) \mapsto (\sigma(h_1)\sigma(\theta_1(k_1)(h_2)), k_1k_2)$. Por outro lado,

$$\begin{aligned} \psi((\sigma(h_1), k_1))\psi((\sigma(h_2), k_2)) &= (\sigma(h_1)\theta_2(k_1)(\sigma(h_2)), k_1k_2) \\ &= (\sigma(h_1)(\sigma \circ \theta_1(k_1) \circ \sigma^{-1})(\sigma(h_2))), k_1k_2) \\ &= \psi((\sigma(h_1)\sigma(\theta_1(k_1)(h_2)), k_1k_2)) \end{aligned}$$

- O fato de que ψ é uma bijeção é imediato.

Com isso está provado o item 1. De maneira análoga, para o item 2, fazemos

$$\phi : K \ltimes_{\theta_1} H \longrightarrow K \ltimes_{\theta_2} H$$

$$(h, k) \mapsto (h, \beta(k))$$

.

- ϕ é um homomorfismo. Com efeito,

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1\theta_1(k_1)(h_2), k_1k_2) \mapsto (h_1\theta_1(k_1)(h_2)), \beta(k_1k_2)).$$

Também temos que

$$(h_1, \beta(k_1)) \cdot (h_2, \beta(k_2)) = (h_1\theta_2(\beta(k_1))(h_2), \beta(k_1)\beta(k_2)) = (h_1\theta_1(k_1)(h_2)), \beta(k_1k_2)).$$

- o fato de ϕ ser uma bijeção também é imediato.

Temos então a demonstração de 2. □

1.3 Sequências Exatas Curtas

Essa seção é de extrema importância para o capítulo final, pois utilizamos uma sequência exata curta para a demonstração de que o grupo de tranças puras no disco é o produto semidireto de grupos livres.

Definição 1.24. A sequência

$$G_0 \xrightarrow{\alpha_0} G_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-2}} G_{n-1} \xrightarrow{\alpha_{n-1}} G_n$$

onde cada G_i é um grupo e cada α_i é um homomorfismo, para todo $i = 1, 2, \cdots, n-1, n$, é dita ser uma *sequência exata* se $Im(\alpha_{i-1}) = Ker(\alpha_i)$, $\forall i \in [1, n-1]$.

Observação 1.22. Quando $G_0 = G_n = 1$, ou seja, são triviais, com $n = 4$ obtemos a seguinte sequência exata

$$1 \longrightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \longrightarrow 1$$

que será chamada de *sequência exata curta*. É imediato que os monomorfismos $1 \longrightarrow G_1$ e $G_3 \longrightarrow 1$ são os únicos possíveis. A exatidão em G_1 e G_3 nos fornecem informações importantes, pois $ker(f) = \{1\}$ nos diz que f é injetora (monomorfismo) e $Im(g) = \{1\}$ então g é sobrejetora (epimorfismo). Por fim, a exatidão de G_2 garante que $f(G_1) = Im(f) \lhd G_2$.

Exemplo 1.27. Sejam G um grupo, H um subgrupo normal de G e G/H o grupo quociente. Então, a sequência

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow 1$$

é uma sequência exata curta, onde as aplicações $i : H \longrightarrow G$ e $\pi : G \longrightarrow G/H$ são a inclusão e a projeção canônica, respectivamente.

Exemplo 1.28. Considere a sequência exata abaixo

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1\,.$$

Temos então que com os isomorfismos $f' : H \longrightarrow f(H)$ e $\overline{g} : G/f(H) \longrightarrow K$ fazemos o diagrama abaixo comutar

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{f} & G & \xrightarrow{g} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle id_G} & & \downarrow{\scriptstyle \overline{g}^{-1}} & & \\ 1 & \longrightarrow & f(H) & \xrightarrow[i]{} & G & \xrightarrow[\pi]{} & G/f(H) & \longrightarrow & 1 \end{array}$$

,isto é, $i \circ f' = id \circ f$ e $\pi \circ id = \overline{g}^{-1} \circ g$.

Definição 1.25. Dizemos que a sequência exata curta

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1$$

de homomorfismos e grupos *cinde* se existir um homomorfismo $i : K \longrightarrow G$ satisfazendo $g(i(k)) = k$ para todo $k \in K$.

Observação 1.23. Em outras palavras, estamos dizendo que uma sequência exata curta cinde quando conseguimos "voltar"ao longo da sequência.

Lema 1.2. *Consideremos a sequência exata curta*

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1 \, .$$

Suponhamos que cinda via $\lambda : K \longrightarrow G$. Então $G \cong K \ltimes H$.

Prova: Por definição, como a sequência cinde via λ então $\lambda \circ g = id_H$. Basta verificar que $G = Im(\lambda) \ltimes Im(f)$, pois $H \cong Im(\lambda)$ e $N \cong Im(f)$. Com efeito,

- Note que, $Im(f) = Ker(g) \lhd G$.
- Tome $x \in Im(\lambda) \cap Im(f)$ então $g(x) = e_G$. Se $h \in H$ então $\lambda(h) = x$, ou seja, $e_G = g(x) = h$. Logo, $x = e_G$.
- Se $x \in G$ então vamos fazer $x = (\lambda \circ g(x))(\lambda \circ g(x))^{-1}x$. Claramente, $\lambda \circ g(x) \in Im(\lambda)$ e $(\lambda \circ g(x))^{-1}(x) \in Im(f)$.

Logo, pela Definição 1.22 concluímos a demonstração. □

Lema 1.3. *(Lema dos Cinco) Seja o diagrama comutativo abaixo cujas linhas são sequências exatas*

$$\begin{array}{ccccccccc} A_0 & \xrightarrow{\alpha_0} & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 \\ \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \downarrow{\scriptstyle \phi_4} \\ B_0 & \xrightarrow[\beta_0]{} & B_1 & \xrightarrow[\beta_1]{} & B_2 & \xrightarrow[\beta_2]{} & B_3 & \xrightarrow[\beta_3]{} & B_4 \end{array}$$

Se ϕ_0, ϕ_1, ϕ_3 e ϕ_4 são isomorfismos então ϕ_2 também o é.

Prova: Veja [10].

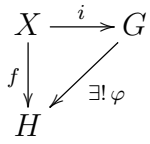
2

Teoria Combinatória de Grupos

Neste capítulo aprenderemos um método de descrever e estudar as propriedades dos grupos de uma forma diferente da que foi feita no capítulo anterior. Iremos introduzir o método de apresentação de grupos por geradores e relatores que é uma ferramenta de grande importância da Teoria Combinatória de Grupos e que é usada nas demais áreas como a Topologia Algébrica. Para isto, faremos a definição de grupos livres sob uma base arbitrária e mostraremos que a Propriedade Universal de tais grupos garante que conseguimos uma apresentação para grupos arbitrários. A importância desse conteúdo pode ser vista por alguns exemplos, a saber, todo grupo G é isomorfo a um quociente de um grupo livre, e mais ainda, todo grupo admite uma apresentação por meio de geradores e relatores. A teoria aqui desenvolvida, definições e demonstrações, estão contidas em [3], [8], [10] e [12].

2.1 Grupos Livres

Definição 2.1. Sejam X um conjunto, G um grupo e $i : X \longrightarrow G$ uma aplicação. O par (G, i) é dito ser livre sobre X se para todo grupo H e aplicação $f : X \longrightarrow H$ existe um único homomorfismo $\varphi : G \longrightarrow H$ tal que $\varphi \circ i = f$, ou seja, o diagrama abaixo comuta.



Observação 2.1. A propriedade descrita na Definição 2.1 é também conhecida por *Propriedade Universal dos Grupos Livres.*

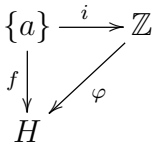
Exemplo 2.1. O grupo trivial $\{1\}$ é livre sobre o conjunto vazio $\varnothing$.

Exemplo 2.2. O grupo aditivo dos inteiros é livre sobre qualquer conjunto que contenha um único elemento. De fato, conforme a definição 2.1, sejam $G = \mathbb{Z}$ e $X = \{a\}$. Tome

a aplicação $i : \{a\} \longrightarrow \mathbb{Z}$ dada por $i(a) = 1$. Se H é um grupo qualquer e $f : X \longrightarrow H$ uma aplicação, então $f(a) = b$ onde $b \in H$, então a aplicação $\varphi : G \longrightarrow H$ dada por $n \mapsto \varphi(n) = [f(a)]^n$ é um homomorfismo. Além disso,

$$(\varphi \circ i)(a) = \varphi i(a) = \varphi(1) = b^1 = b = f(a).$$

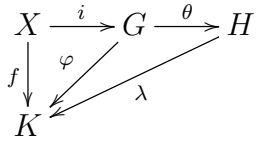
Sendo assim, obtivemos o seguinte diagrama comutativo



Se existir outro homomorfismo $\lambda : G \longrightarrow H$ tal que satisfaça $\lambda \circ i = f$ teríamos $\lambda(a) = (\lambda \circ i)(a) = f(a) = b = f(a) = (\varphi \circ i)(a) = \varphi(1)$. Portanto, $\varphi = \lambda$.

Proposição 2.1. *Seja (G, i) livre sobre X e H um grupo qualquer. Se $\theta : G \longrightarrow H$ for um isomorfismo, então $(H, \theta \circ i)$ também é livre sobre X.*

Prova: Para provarmos o teorema devemos mostrar que para qualquer grupo K e aplicação $f : X \longrightarrow K$ existe um único homomorfismo $\lambda : H \longrightarrow K$ tal que $\lambda \circ (\theta \circ i) = f$, ou seja, o diagrama



Com efeito, defina $\theta : H \longrightarrow K$ por $\theta = \varphi \circ \theta^{-1}$. Então,

- λ é um homomorfismo, pois foi definido pela composição dos homomorfismos θ^{-1} e φ.
- $\lambda \circ \theta \circ i = f$, pois $\lambda \circ (\theta \circ i) = (\varphi \circ \theta^{-1}) \circ (\theta \circ i) = \phi \circ (\theta^{-1} \circ \theta) \circ i = \varphi \circ Id_G \circ i = f$.
- O homomorfismo λ é o único que satisfaz a Propriedade Universal de Grupos Livres, pois suponhamos que houvesse um outro homomorfismo $\lambda' : H \longrightarrow K$ tal que $\lambda' \circ (\theta \circ i) = f$. Sendo assim, se $\omega : G \longrightarrow K$ é um homomorfismo dado por $\lambda \circ \theta$ teríamos $\omega \circ i = \lambda \circ (\theta \circ i) = f$. Mas por hipótese, $\varphi : G \longrightarrow K$ é o único que cumpre $\varphi \circ i = f$. Portanto, $\lambda = \lambda'$.

□

A proposição seguinte afirma que se um grupo é livre sobre um determinado conjunto, então ele é único a menos de isomorfismo!

Proposição 2.2. *Sejam (G_1, i_1) e (G_2, i_2) grupos livres sobre X. Então existe um isomorfismo $\varphi : G_1 \longrightarrow G_2$ tal que $\varphi \circ i_1 = i_2$.*

Prova: Sejam (G_1, i_1) e (G_2, i_2) grupos livres sobre X, então existem únicos homomorfismos $\varphi_1 : G_1 \longrightarrow G_2$ e $\varphi_2 : G_2 \longrightarrow G_1$ cumprindo a condição de que $\varphi_1 \circ i_1 = i_2$ e $\varphi_2 \circ i_2 = i_1$, ou sejam, os diagramas abaixo

$$\begin{array}{ccc} X & \xrightarrow{i_1} & G_1 \\ {\scriptstyle i_2}\downarrow & \swarrow{\scriptstyle \exists!\,\varphi_1} & \\ G_2 & & \end{array}$$

e

$$\begin{array}{ccc} X & \xrightarrow{i_2} & G_2 \\ {\scriptstyle i_1}\downarrow & \swarrow{\scriptstyle \exists!\,\varphi_2} & \\ G_1 & & \end{array}$$

são comutativos. Assim, observe que

$$\varphi_1 \circ i_1 = (\varphi_1 \circ \varphi_2) \circ i_2 = i_2.$$

Analogamente,

$$\varphi_2 \circ i_2 = (\varphi_2 \circ \varphi_1) \circ i_1 = i_1.$$

Concluímos então que $\varphi_1 \circ \varphi_2 = Id_2$ e $\varphi_2 \circ \varphi_1 = Id_1$, ou seja, as aplicações φ_1 e φ_2 são simultaneamente a inversa uma da outra. Sendo assim, $G_1 \cong G_2$.

Proposição 2.3. *Seja (F, i) um grupo livre sobre X.*

1. *Se existem um grupo G e uma função injetiva de X para G então $i : X \longrightarrow F$ é injetiva.*
2. *$(\mathbb{Z}^X, +)$ é um grupo tal que $\mathbb{Z}^X = \{\lambda : X \longrightarrow X; \lambda \text{ é função}\}$ e $(\varphi + \theta)(x) = \varphi(x) + \theta(x), \forall x \in X$ e existe uma função injetiva $f : X \longrightarrow \mathbb{Z}^X$.*
3. *$i : X \longrightarrow F$ é injetiva.*

Prova:

1. Pela definição de grupo livre, para o grupo G e a aplicação $f : X \longrightarrow G$, existe um único homomorfismo $\varphi : F \longrightarrow G$ tal que $\varphi \circ i = f$ o que resulta no seguinte diagrama comutativo

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle \exists!\,\varphi} & \\ G & & \end{array}$$

   Por hipótese, f é injetiva, então $f(x) \neq f(y)$ sempre que $x \neq y, \forall x, y \in X$. Portanto, $f(x) = (\varphi \circ i)(x) \neq (\varphi \circ i)(y) = f(y), \forall x, y \in X$.

2. Os axiomas da Definição 1.1 são verificados facilamente. Com efeito, a associantividade de $(\mathbb{Z}^X, +)$ segue da adição em $\mathbb{Z}$. Veja que $\alpha_0 : X \longrightarrow \mathbb{Z}^X$ dada por $\alpha_0(x) = 0, \forall x \in X$ é o elemento neutro. Por fim, se $\alpha \in \mathbb{Z}^X$ então seu elemento inverso é $-\alpha : X \longrightarrow \mathbb{Z}^X$ dada por $(-\alpha)(x) = -x, \forall x \in X$. Portanto, $(\mathbb{Z}^X, +)$ é um grupo. Vamos agora exibir uma função $f : X \longrightarrow \mathbb{Z}^X$ injetiva. Com efeito, seja

$$\begin{aligned} f : X &\longrightarrow \mathbb{Z}^X \\ x &\longmapsto f(x) = \alpha_x : X \longrightarrow \mathbb{Z}^X \end{aligned}$$

onde α_x é definida da seguinte forma, para todo x em X:

$$\alpha_x(y) = \begin{cases} 1, & se\, x = y \\ 0, & se\, x \neq y \end{cases}$$

Claramente, $\alpha_x(y) \neq \alpha_y(x), \forall x, y \in X$ onde $x \neq y$. Logo, $f(x) \neq f(y)$ sempre que $x \neq y, \forall x, y \in X$.

3. Sai de imediato fazendo $G = \mathbb{Z}^X$ e tomando f como no item 2, acima.

□

2.2 Construção de Grupos Livres e Suas Propriedades

Seja X um conjunto qualquer. Denotaremos por

$$M(X) = \{(x_{i_1}, ..., x_{i_n});\ x_{i_k} \in X, k = 1, ..., n\}$$

o conjunto das sequências finitas $(x_{i1}, \ldots, x_n)$ de elementos de X, para $n \geq 0$ (o caso $n = 0$ corresponde a sequência vazia ( )). Agora, defina a operação de multiplicação $\cdot : M(X) \times M(x) \longrightarrow M(X)$ da seguinte forma

$$(x_{i_1}, \ldots, x_{i_n}) \cdot (x_{j_1}, \ldots, x_{j_k}) = (x_{i_1}, \ldots, x_{i_n}, x_{j_1}, \ldots, x_{j_k}).$$

Chamaremos essa operação de concatenação. É fácil perceber que a multiplicação é associativa. A sequência vazia ( ), que denotaremos por 1, atua como elemento neutro. Com essas duas propriedades $(M(X), \cdot)$ torna-se um *monóide*, onde o chamaremos de *monóide livre* sobre X.

A correspondência $x \mapsto (x)$ é, obviamente, injetora. Sendo assim, podemos escrever os elementos de $M(X)$ de uma maneira única como um produto $x_{i_1} \ldots x_{i_n}$ para todo n. Dizemos que um *segmento* de $x_{i_r} \ldots x_{i_s}$, com $1 \leq r \leq s \leq n$, é um *segmento inicial* quando $r = 1$; *segmento final* quando $s = n$; e *segmento próprio* quando $r = 1$ e $s = n$.

2.2.1 O grupo livre gerado por X

Nós agora procederemos para a construção do grupo livre sobre X. Tome um conjunto X^{-1} de mesma cardinalidade que o conjunto X, de modo que $X \cap X^{-1} = \varnothing$. Sendo assim, existe uma bijeção entre os elementos $x \in X$ para $x^{-1} \in X^{-1}$ (Obviamente, x^{-1} é apenas um símbolo adotado). Com isso, consideramos o conjunto $M(X \cup X^{-1})$ como o *monóide livre* gerado por $X \cup X^{-1}$, cujos elementos são chamados de *palavras sobre* X. Seja w a palavra $x_{i_1}^{\epsilon^1} \cdots x_{i_n}^{\epsilon^n}$ em $M(X \cup X^{-1})$, então dizemos que n é o *comprimento* de w onde denotamos por $l(w)$ ou ainda $|w|$. Nós chamamos os elementos $x_{i_r}^{\epsilon_r}$ de *letras* de w. A palavra w é chamada de *reduzida* se, para $1 \leq r \leq n-1$, temos $i_{r+1} \neq i_r$ ou $i_{r+1} = i_r$, mas $\epsilon_{r+1} \neq -\epsilon_r$. Convencionamos que a sequência vazia ( ) é reduzida.

Observação 2.2. Dizemos que as palavras $u = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ e $v = x_{j_1}^{\delta_1} \dots x_{j_r}^{\delta_r}$ com $x_{i_k}, x_{j_l} \in X$ e $\epsilon_k, \delta_l = \pm 1$ são iguais se, e só se, ambas forem a palavra vazia ou $m = n$ e $x_{i_k} = x_{j_l}, \epsilon_k = \delta_k$, para todo $k = 1, 2, \dots, n$.

Suponha que $w = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ não seja uma palavra reduzida e seja r tal que $i_{r+1} = i_r$ e $\epsilon_{r+1} = -\epsilon_r$. Então w' é a palavra obtida de w deletando os pares de letras adjascentes $x_{i_r}^{\epsilon} r$ e $x_{i_{r+1}}^{\epsilon_{r+1}}$. Nós dizemos que w' foi obtida de w por uma *redução elementar*. Se a palavra w'' sobre é obtida de w por uma sequência de reduções nós diremos então que w'' é obtida por *redução*.

Exemplo 2.3. As palavras $zzy^{-1}y$ e $zxx^{-1}z$ são obtidas de $zxx^{-1}zy^{-1}y$ por meio de redução elementar. Já a palavra zz resulta de uma redução.

Exemplo 2.4. Podemos obter a palavra zxy a partir da palavra $zxx^{-1}xy$ por redução elementar de duas formas diferentes. Na primeira podemos retirar os pares de letras xx^{-1}, enquanto na segunda retiramos $x^{-1}x$.

Diremos que as palavras w e w' são *equivalentes* e escrevemos $w \approx w'$ se, e somente se, $w = w'$ ou existe uma sequência de palavras $w_1, \dots, w_k$ onde para cada k temos que $w_1 = w$ e $w_k = w'$ e para cada $j < k$, w_{j+1} é obtida de w_j por redução elementar. Veja que $\approx$ define uma relação de equivalência sobre $M(X \cup X^{-1})$. Faremos a seguir a verificação das três propriedades de relação de equivalência.

- **Reflexividade:** Dado $w \in M(X \cup X^{-1})$ então $w = w$, portanto $w \approx w$.
- **Simetria:** Dadas as palavras w e w' em $M(X \cup X^{-1})$ tais que $w \approx w'$ então $w' \approx w$. Do contrário, existiria uma sequência de palavras $w_1, \dots, w_k$ tal que $w' = w$, $w_k = w'$ e para cada $j < k$ a palavra w_{j+1} é obtida de w_j por redução elementar. Para cada $j \in [1, \dots, k]$, considerando a palavra $v_j = w_{k-(j-1)}$ obtemos as palavras v_i, com

$i \in [1, \ldots, k]$, satisfazendo as equações abaixo

$$\begin{aligned} v_1 &= w_k = w', \\ v_2 &= w_{k-1}, \\ v_3 &= w_{k-2}, \ldots, v_{k-1}, \end{aligned}$$

onde os termos consecutivos v_i e v_{i+1} diferem por redução elementar para cada $i \in [1, \ldots, k]$. Logo, $w' \approx w$.

- **Transitividade:** Dadas as palavras $w, w', w'' \in F(X)$ tal que $w \approx w'$ e $w' \approx w''$ então $w \approx w''$.

A partir de agora denotaremos por $F(X)$ o conjunto das classes de quivalência pela relação $\approx$ em $M(X \cup X^{-1})$, ou seja, $F(X) = \{[w] \; ; \; w \in M(X \cup X^{-1})\}$ onde $[w] = \{w' \in M(X \cup X^{-1}) \; ; \; w \approx w'\}$.

Proposição 2.4. *O conjunto $F(X)$ munido da seguinte aplicação binária*

$$\begin{aligned} \cdot : F(X) \times F(X) &\longrightarrow F(X) \\ ([u], [v]) &\longmapsto [u].[v] = [u.v]. \end{aligned} \tag{2.1}$$

é um grupo.

Prova: Em primeiro lugar, como estamos trabalhando com classes de equivalência, devemos verificar se a operação definida em 2.1 é bem definida. Com efeito, sejam $u, v, w, w' \in F(X)$. Então, temos que

1. $w \approx w'$ implica $uwv \approx uw'v$.

   De fato, suponhamos que $w_1, \ldots, w_k$ seja uma sequência de palavras sobre X tal que $w_1 = w$, $w_k = w'$ e se $j < k$ então w_{j+1} é obtida de w_j por redução elementar, para todo $j \in [1, \ldots, k]$. Daí, a sequência $uw_1v, \ldots, uw_kv$ nos mostra que $uwv \approx uw'v$.

2. Se $u \approx u'$ e $w \approx w'$ então $uw \approx u'w'$.

   De fato, ambas as palavras $u \approx u'$ e $w \approx w'$ são equivalentes a palavra uw'.

Com isso, o produto $\cdot$ é bem definido. Prosseguiremos com a verificação dos axiomas da Definição 1.1.

1. **Associatividade:** Sejam $[u], [v], [w] \in F(X)$ então

$$\begin{aligned}([u]\cdot[v])\cdot[w] &= ([uv])\cdot[w]\\ &= [(uv)w]\\ &= [u(vw)]\\ &= [u]\cdot[vw]\\ &= [u]\cdot([v]\cdot[w])\end{aligned}$$

2. **Elemento neutro:** A classe da palavra vazia ( ) é, evidentemente, o elemento neutro. Denotaremos por 1.

3. **Elemento Inverso:** Seja $[u] \in F(X)$ a classe da palavra $u = x_{i1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$. Tomemos por $[u^{-1}]$ a classe da palavra $u^{-1} = x_{i_1}^{-\epsilon_1} \dots x_{i_n}^{-\epsilon_n}$. Daí,

$$\begin{aligned}[u]\cdot[u^{-1}] &= [x_{i1}^{\epsilon_1}\dots x_{i_n}^{\epsilon_n}][x_{i_1}^{-\epsilon_1}\dots x_{i_n}^{-\epsilon_n}]\\ &= [(x_{i1}^{\epsilon_1}\dots x_{i_n}^{\epsilon_n})(x_{i_n}^{-\epsilon_n}\dots x_{i_1}^{-\epsilon_1}]\\ &= [(x_{i_1}\dots x_{i_{n-1}}^{\epsilon_{n-1}})(x_{i_n}^{\epsilon_n}x_{i_n}^{-\epsilon_n})(x_{i_{n-1}}^{-\epsilon_{n-1}}\dots x_{i_1}^{-\epsilon_1})]\\ &= [(x_{i_1}\dots x_{i_{n-1}}^{\epsilon_{n-1}})(\,)(x_{i_{n-1}}^{-\epsilon_{n-1}}\dots x_{i_1}^{-\epsilon_1})]\\ &= [(x_{i_1}\dots x_{i_{n-1}}^{\epsilon_{n-1}})(x_{i_{n-1}}^{-\epsilon_{n-1}}\dots x_{i_1}^{-\epsilon_1})]\\ &= \dots\\ &= [(\,)] = 1.\end{aligned}$$

Com isso, $(F(X), \cdot)$ é um grupo. □

Seja $w = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ uma palavra em X. Vamos definir a função $i : X \longrightarrow F(X)$ dada por $i(x) = [x]$. Por construção temos que $[w] = i(x_{i_1}^{\epsilon_1}) \dots i(x_{i_n}^{\epsilon_n})$, ou seja, $F(X)$ é gerado por $i(X)$.

Teorema 2.1. *$(F(X), i)$ é livre sobre X.*

Prova: Seja G um grupo qualquer e $f : X \longrightarrow G$ uma aplicação (dada arbitrariamente). Vamos estender f na aplicação

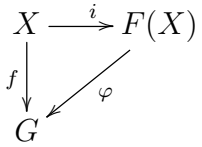
$$\begin{aligned}\overline{f} : M(X \cup X^{-1}) &\longrightarrow G\\ x_{i_1}^{\epsilon_1}\dots x_{i_n}^{\epsilon_n} &\longmapsto f(x_1)^{\epsilon_1}\dots f(x_n)^{\epsilon_n}\end{aligned}$$

Veja que se w' é obtida por redução elementar de uma palavra w, então $\overline{f}(w') = \overline{f}(w)$. Daí, segue que se $w \approx w''$ então $\overline{f}(w) = \overline{f}(w'')$. Consequentemente, nós temos que a

aplicação

$$\begin{aligned} \varphi : F(X) &\longrightarrow G \\ [u] &\longmapsto \varphi([u]) = \overline{f}(u) \end{aligned}$$

é um homomorfismo e que $\varphi \circ i = f$, ou seja, o diagrama



comuta. Como $i(X)$ gera $F(X)$ temos que φ torna-se o único homomorfismo que compre tal condição. Sendo assim, o grupo $(F(X), \cdot)$ satisfaz a Definição 2.1. □

É fácil perceber que as reduções elementares reduzem o comprimento de uma palavra. Contudo, quando obtemos uma palavra reduzida w podemos afirmar que ela é única? O resultado a seguir responde este questionamento.

Lema 2.1. *Se w é uma palavra reduzida distinta da palavra vazia $(\ ) = 1$ então $w1$, ou seja, $[w] \neq 1$.*

Prova: Seja w uma palavra reduzida distinta da palavra vazia e consideremos $S_n + 1$ o grupo das permutações dos elementos de $S = \{1, 2, \ldots, r, \ldots, n, n+1\}$. Existe um homomorfismo $\phi : F(X) \longrightarrow S_{n+1}$ tal que $\phi([w])$ não é a permutação identidade Id_S. Pelo fato de ϕ ser um homomorfismo temos que $\phi([1]) = Id_S$, caso contrário se $[w] = 1$, teríamos $\phi([w]) = \phi([1]) = Id_S$ o que seria um absurdo. □

Na demonstração do lema 2.1 usamos a afirmação de que existe um homomorfismo $\phi : F(X) \longrightarrow S_{n+1}$ tal que $\phi([w])$ não é a permutação identidade Id_S. A demonstração dessa afirmação é longa, mas pode ser encontrada em [12].

Teorema 2.2. *(Teorema da Forma Normal para grupos livres) Existe exatamente uma palavra reduzida em cada classe de equivalência em $F(X)$.*

Prova: Suponha por absurdo que existam palavras reduzidas u e v tais que $u \approx v$, ou seja, $[u] = [v]$. Temos então que $uv^{-1} = 1$. Consequentemente a palavra uv^{-1} não é reduzida, mas se u e v são diferentes é fácil ver que

$$uv^{-1} \approx w \neq 1.$$

Ou seja, obtivemos uma única palavra w reduzida diferente de 1. □

O resultado a seguir é consequência da demonstração do Teorema da Forma Normal para grupos livres.

Corolário 2.1. *$i : X \longrightarrow F(X)$ é injetiva.*

Observação 2.3. A partir de agora tomaremos X como um subconjunto de $F(X)$. A aplicação i será tomada como a inclusão $i : X \hookrightarrow F(X)$, por isso passaremos a omiti-la. Usualmente iremos identificar os elementos de $F(X)$ com as palavras reduzidas correspondentes.

Observação 2.4. Sejam u e v palavras reduzidas, então existe uma sequência de reduções elementares tais que uv torna-se uma palavra reduzida.

Observação 2.5. Podemos definir $F(X)$ como o conjunto das palavras reduzidas e o produto $\cdot$ de u por v como a palavra reduzida a partir da palavra uv.

2.2.2 Propriedades dos grupos livres

Proposição 2.5. *Grupos livres são residualmente finitos, ou seja, se F é livre e $1 \neq w \in F$ então existe um subgrupo normal N de F com $w \notin N$ e F/N finito.*

Prova: Seja w uma palavra reduzida não trivial. Sabemos que existe um homomorfismo φ de F em S_{n+1} tal que $\varphi(w)$ não é o elemento identidade, para todo n. □

Definição 2.2. Um grupo G é dito *hopfiano* se ele não é isomorfo a um grupo quociente próprio dele mesmo. Em outras palavras, se $G/H \cong G$, onde $H \lhd G$, então H é trivial.

Proposição 2.6. *Um grupo G é hopfiano se, e somente se, todo epimorfismo $\varphi : G \longrightarrow G$ é automorfismo.*

Prova: ($\Rightarrow$) Seja $f : G \longrightarrow G$ um epimorfismo. Então, pelo Teorema do Isomorfismo I temos que existe um único isomorfismo $\varphi : G/ker(f) \longrightarrow G$. Como $kernel(f)$ é trivial segue de imediato que φ é injetor. Portanto, um automorfismo. ($\Leftarrow$) Seja $H \lhd G$ e considere o homomorfismo $g : G/H \longrightarrow G$. Tomando a projeção canônica $\pi : G \longrightarrow G/H$, podemos definir um epimorfismo $f : G \longrightarrow G$ fazendo $f = g \circ \pi$. Note que

$$\begin{aligned} ker(\pi) &= \{g \in G; \pi(g) = e_G\} \\ &= \{g \in G; g = Hg\} = H \end{aligned}$$

Como f é um isomorfismo, π é injetor, consequentemente $ker(f) = H$ é trivial. Logo, G é hopfiano. □

Corolário 2.2. *Grupos livres finitamente gerados são hopfianos.*

Proposição 2.7. *$F(X)$ é isomorfo a $F(Y)$ se, e somente se, $|X| = |Y|$.*

Prova: Seja $f : X \longrightarrow Y$ uma bijeção. Então, f se estende a um homomorfismo $\phi : F(X) \longrightarrow F(Y)$ enquanto $f^{-1} : Y \longrightarrow X$ se estende para o homomorfismo $\psi : F(Y)] \longrightarrow F(X)$. Observe que as composições $f \circ f^{-1}$ e $f^{-1} \circ f$ se estendem para os homomorfismos

$\phi \circ \psi$ e $\psi \circ \phi$, ou seja, $Id_{F(Y)}$ e $Id_{F(X)}$, respectivamente. Portanto, $F(X) \cong F(Y)$. Reciprocramente, suponhamos que $F(X) \cong F(Y)$. O número de isomorfismos de $F(X)$ para $\mathbb{Z}_2$, o grupo cíclico de ordem 2, é o mesmo que o número de funções de X para $\mathbb{Z}_2$ que é $2^{|X|}$. Consequentemente, $2^{|X|} = 2^{|Y|}$. Segue de imediato que $|X| = |Y|$. □

Proposição 2.8. *Grupos livres são livres de torsão, ou seja, todo elemento de um grupo livre não possui ordem finita.*

Prova: Seja F um grupo livre e $g \in F$ diferente de 1. Tomando o conjugado se necessário, assumimos sem perda de generalidade que g é ciclicamente reduzida. Então,

$$|g^n| = n|g| \neq 0.$$

Portanto, $g^n \neq 1$. □

Proposição 2.9. *Seja F um grupo livre e sejam g e h elementos de F. Se $g^k = h^k$ para todo $k \neq 0$ então $g = h$.*

Prova: Vamos assumir que $k \geq 0$. Seja g um elemento de F. Tomando o conjugado se necessário, nós vamos assumir também que g é ciclicamente reduzida. Se h não é ciclicamente reduzida por escrito então h^k também não é, logo $g^k \neq h^k$. Se h é ciclicamente reduzida então h^k é ciclicamnete reduzida por escrito. Consequentemente, g^k consiste de g multiplicado k vezes, similarmente para h^k. Logo, $g^k = h^k$ e temos $g = h$. □

Proposição 2.10. *Todo grupo G é quociente de um grupo livre.*

Prova: Seja G um grupo qualquer e tome $Id_G : G \longrightarrow G$ a aplicação identidade de G. Existe um único homomorfismo $\varphi : F(G) \longrightarrow G$ tal que $\varphi \circ i = Id_G$, onde $i(g) = [g]$. Daí, o seguinte diagrama comuta

$$\begin{array}{ccc} G & \xrightarrow{Id_G} & G\,. \\ {\scriptstyle i}\downarrow & \nearrow_{\exists!\,\varphi} & \\ F(G) & & \end{array}$$

Consequentemente, φ é um epimorfismo e portanto $F(G)/ker(Id_G) \cong G$. □

Definição 2.3. Um grupo G é chamado de *grupo livre* se é isomorfo a $F(X)$ para algum conjunto X. Além disso, se $i : X \longrightarrow F(X)$ for um isomorfismo, então a imagem $i(X)$ é chamada de *base* de G. Nós também dizemos que G é livre sobre X.

Observação 2.6. Se A é uma base de G e $\alpha : G \longrightarrow G$ um automorfismo, então $\alpha(A)$ também será uma base de G.

Observação 2.7. Se A e B são bases de um mesmo grupo então $|A| = |B|$.

Observação 2.8. Toda bijeção entre as bases A e B se estende naturalmente para um automorfismo de G.

Definição 2.4. A cardinalidade da base de um grupo livre G é chamada de *rank* ou *posto* de G.

Exemplo 2.5. Seja $X = \{x, y\}$. Então, $\{x^{-1}, x^2y\}$ é uma base para o grupo livre $F(X)$. Para verificar isto basta tomar a aplicação

$$\begin{aligned} f : X &\longrightarrow F(X) \\ x &\longmapsto x^{-1} \\ y &\longmapsto x^2y \end{aligned}$$

e perceber que pela Propriedade Universal dos Grupos Livres existe um único homomorfismo $\varphi : F(X) \longrightarrow F(X)$. Como tal grupo livre é finitamente gerado, então $F(X)$ é hopfiano consequentemente φ é automorfismo. □

Proposição 2.11. *Seja X um subconjunto do grupo livre G. Então as seguintes afirmações são equivalentes:*

i). G é livre com base X.

ii). Todo elemento de G pode ser escrito de maneira única na forma $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ para cada $n \geq 0$,$x_{i_r} \in X$ e $\epsilon_r = \pm 1$ onde $\epsilon_{r+1} \neq -\epsilon_r$ se $i_{r+1} = i_r$.

iii). X gera G e 1 não é igual a qualquer produto $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$, com $n \geq 0$, $x_{i_r} \in X$, $\epsilon_r = \pm 1$ e $\epsilon_{r+1} \neq -\epsilon_r$ se $i_{r+1} = i_r$.

Prova: $(ii) \Rightarrow (iii)$ é imediato. $(iii) \Rightarrow (ii)$: Suponhamos que existisse uma forma de escrever um elemento $g \in G$ de duas maneiras diferentes, então multiplicando um pelo inverso do outro estaríamos escrevendo 1 como um produto não trivial de letras em X. (iii) e $(ii) \Leftrightarrow (i)$: Se G é livre sobre X então goza das propriedades da hipótese, uma vez que $F(X)$ é livre. Considere o homomorfismo $\alpha : F(X) \longrightarrow G$ que é induzido pela aplicação identidade de X. Note que α é sobrejetor, pois $i(X)$ gera G. Além disso, (iii) implica que α também é injetor. Portanto, $G \cong F(X)$ e tem-se demonstrada a proposição. □

Corolário 2.3. *Seja G gerado por X e $\varphi : G \longrightarrow H$ um homomorfismo injetor sobre X tal que $\varphi(G)$ é livre sobre $\varphi(X)$. Então G é livre com base X.*

Prova: A condição (iii) vale para X e G porque $\varphi(X)$ e $\varphi(G)$ a cumprem, sendo assim G é livre de acordo com a Proposição 2.11. □

Corolário 2.4. *Seja G livre com base X e seja $Y \subset X$. Então o subgrupo $\langle Y \rangle$ de G é livre com base Y.*

Prova: Veja que também decorre de imediato do item (iii) da Proposição 2.11. □

2.3 Apresentação de Grupos

Nesta subsecção iremos definir apresentação de grupos, consequência do estudo de grupos livres e da Propriedade Universal. Este método é o objetivo principal deste capítulo e um dos tópicos mais importantes da Teoria Combinatória de Grupos, pois permitirá descrever o grupo de tranças no disco por meio de elementos que geram o grupo e que satisfazem determinadas relações.

Definição 2.5. Seja G um grupo, X um conjunto e $\varphi : F(X) \longrightarrow G$ um epimorfismo.

i. X é chamado de *conjunto de símbolos geradores* de G.

ii. A família $\varphi(X) = \{\varphi(x); x \in X\}$ é chamada de *conjunto de geradores* para G.

iii. $ker(\varphi)$ é chamado de *conjunto de relatores* de G sob φ.

iv. Dada duas palavras $u \equiv x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ e $v \equiv x_{j_1}^{\delta_1} \dots x_{j_m}^{\delta_m}$ se $uv^{-1} \in ker(\varphi)$, fazendo $a_i = \varphi(x_i)$ dizemos que a equação $a_{i_1}^{\epsilon_1} \dots a_{i_n}^{\epsilon_n} = a_{j_1}^{\delta_1} \dots a_{j_m}^{\delta_m}$ é uma *relação* em G.

Definição 2.6. Para todo subconjunto S de um grupo G, o fecho normal $\langle S \rangle^G$ é chamado de *conjunto das consequências* de S em G.

Definição 2.7. Seja G um grupo, X um conjunto e $\varphi : F(X) \longrightarrow G$ um epimorfismo. Se $ker(\phi)$ é o conjunto das consequências de algum subconjunto R de $F(X)$, ou seja, $ker(\varphi) = \langle R \rangle^F(X)$, então chamamos R de *conjunto de relatores definidores* de G sob φ. Diremos que uma relação $u = v$ em G é uma *consequência* de relatores definidores se uv^{-1} é uma consequência de relatores definidores.

Definição 2.8. Uma *apresentação* de um grupo G consiste num conjunto X, um epimorfismo $\varphi : F(X) \longrightarrow G$ e de um conjunto R de relatores definidores de G sob φ e a denotamos por $G = \langle X|R \rangle^{\varphi}$. Quando X e R forem finitos diremos que $\langle X|R \rangle^{\varphi}$ é uma *apresentação finita* de G, ou que G é *finitamente apresentado*.

Observação 2.9. Omitiremos φ na notação quando φ for a aplicação natural de $F(X)$ em $F(X)/\langle R \rangle^{F(X)}$ ou se φ for injetora sobre X.

Observação 2.10. Todo grupo admite apresentação $\langle X|R \rangle$. De fato, seja G um grupo qualquer. Existe o epimorfismo $\varphi : F(X) \longrightarrow G$, onde X é um conjunto gerador para G. Para algum $R \subset G$ temos que $ker(\varphi) = \langle R \rangle^{F(X)}$. Tome $R = ker(\varphi) \lhd F(X)$. Claramente, $\langle ker(\varphi) \rangle^{F(X)} = ker(\varphi)$. Consequentemente obtemos $G = \langle X|R \rangle^{\varphi}$.

Exemplo 2.6. O grupo livre $F(X)$ é apresentado por $\langle X|R \rangle$ com $R = \varnothing$. De fato, seja $\varphi = Id_{F(X)}$. Consequentemente, $ker(\varphi) = \{1\} = \langle \varnothing \rangle^{F(X)}$. Portanto, $R = \varnothing$ e temos assim a apresentação de $F(X)$ conforme a definição 2.8.

Exemplo 2.7. O grupo aditivo dos inteiros $(\mathbb{Z}, +)$ é finitamente apresentado. De fato, consideremos a seguinte função sobrejetora

$$\begin{aligned} f : \{a\} &\longrightarrow \{1\} \\ a &\longmapsto 1 \end{aligned}$$

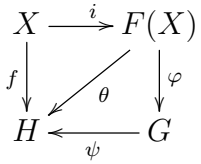
f se estende naturalmente ao epimorfismo $\varphi : F(X) \longrightarrow \mathbb{Z}$. Temos que $F(X) = \{a^n; n \in \mathbb{Z}\}$ e

$$\begin{aligned} ker(\varphi) &= \{a^n \in F(X);\ \varphi(a^n) = 0\} \\ &= \{a^n \in F(X);\ n\varphi(a) = 0\} \\ &= \{a^n;\ n = 0\} = \{1\} \end{aligned}$$

Logo, pela Definição 2.8, temos $(\mathbb{Z}, +) = \langle a|\varnothing\rangle^{\varphi}$.

Exemplo 2.8. O grupo cíclico $\mathbb{Z}_n$, de ordem n, tem apresentação $\langle x|x^n\rangle$.

Teorema 2.3. *(Teorema de Von Dyck) Seja G apresentado por $\langle X|R\rangle^{\varphi}$, $f : X \longrightarrow H$ uma função de X para um grupo qualquer H e $\theta : F(X) \longrightarrow H$ o correspondente homomorfismo que estende f. Se $\theta(r) = 1$ para todo $r \in R$, então existe um homomorfismo $\psi : G \longrightarrow H$ tal que $\varphi \circ \psi(x) = f(x)$ para todo $x \in X$. Além disso, se $f(X)$ gera H então ψ é um epimorfismo.*



Prova: Por hipótese, G é apresentado por $\langle X|R\rangle^{\varphi}$ onde $\varphi : F(X) \longrightarrow G$ é um epimorfismo e $R \subseteq F(X)$ é o conjunto de relatores definidores para G sob φ. Desde que $ker(\theta) \lhd F(X)$, então $R \subset ker(\theta)$ e segue que $ker(\varphi) \subseteq ker(\theta)$, pois $\theta(r) = 1, \forall r \in R$. Sendo $\varphi : F(X) \longrightarrow G$ um epimorfismo, existe $w \in F(X)$ tal que $\varphi(w) = g,\ g \in G$. Vamos definir

$$\begin{aligned} \psi : G &\longrightarrow H \\ g &\longmapsto \psi(g) = \theta(w), \forall w \in F(X), \varphi(w) = g. \end{aligned}$$

i. ψ é bem definida. Dados $w, w' \in F(X)$ tais que $\varphi(w) = \varphi(w')$. Daí, $\varphi(w - w') = 1_G$ o que implica $w - w' \in ker(\varphi) \subseteq ker(\theta)$, portanto $\theta(w - w') = 1_H$. Consequentemente, $\theta(w) = \theta(w')$.

ii. ψ é um homomorfismo. Tome $g_1, g_2 \in G$. Então, $\psi(g_1 \cdot g_2) = \theta(w), \forall w \in F(X)$ tal que $\varphi(w) = g_1 \cdot g_2$. Mas, note que $\psi(g_1) \cdot \psi(g_2) = \theta(u) \cdot \theta(v), \forall u, v \in F(X)$ tais que

$\varphi(u) = g_1$ e $\varphi(v) = g_2$. Consequentemente,

$$\varphi(w) = g_1 \cdot g_2 = \varphi(u)\varphi(v) = \varphi(u \cdot y). \tag{2.2}$$

Sendo assim, tome $w' = uv \in F(X)$. Pela equação 2.2 concluímos que

$$\psi(g_1 \cdot g_2) = \theta(u \cdot v) = \theta(u) \cdot \theta(v) = \psi(u) \cdot \psi(v). \tag{2.3}$$

iii. Para todo $x \in X$

$$(\psi \circ \varphi)(x) = \psi(\varphi(x)) = \psi(g) = \theta(x) = f(x). \tag{2.4}$$

Por fim, suponhamos que $H = \langle f(X) \rangle$, então tomando $h \in H$ temos que h será escrito da forma $f(x_{i_1})^{\epsilon_1} \dots f(x_{i_n})^{\epsilon_n}$, com $x_{i_r} \in X$, $\epsilon \mp 1$ e $n \geq 0$. Seja $w = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} \in F(X)$. Assim,

$$\begin{aligned} \varphi(w) &= \varphi(x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}) \\ &= \varphi(x_{i_1}^{\epsilon_1}) \dots \varphi(x_{i_n}^{\epsilon_n}) \\ &= \phi(x_{i_1})^{\epsilon_1} \dots \varphi(x_{i_n})^{\epsilon_n} \end{aligned} \tag{2.5}$$

Concluímos então que $h \in H$, logo existe $g \in G$, conforme a equação 2.5, tal que

$$\begin{aligned} \psi(g) &= \psi(\varphi(g)) && (2.6) \\ &= \psi(\varphi(x_{i_1})^{\epsilon_1} \dots \varphi(x_{i_n})^{\epsilon_n}) \\ &= ((\psi \circ \varphi)(x_{i_1}))^{\epsilon_1} \dots ((\psi \circ \varphi)(x_{i_n}))^{\epsilon_n} \\ &= f(x_{i_1})^{\epsilon_1} \dots f(x_{i_n})^{\epsilon_n} \\ &= h. && (2.7) \end{aligned}$$

Sendo assim, ψ é epimorfismo. □

Observação 2.11. Uma consequência do Teorema de Von Dyck é de que a inclusão $\overline{i} : X \longrightarrow X \cup Y$ induz um homomorfismo de $\langle X|R \rangle$ para $\langle X \cup Y | R \cup S \rangle^{\varphi}$ para qualquer subconjunto S de $F(X \cup Y)$.

Teorema 2.4. *Seja R um subconjunto de um grupo A e seja $\theta : A \longrightarrow H$ um homomorfismo tal que $\theta(R) = \{1\}$. Então, existe um homomorfismo $\psi : A/\langle R \rangle^A \longrightarrow H$ tal que $\theta = \pi \circ \psi$, onde π é a projeção de A para $A/\langle R \rangle^A$.*

Prova: Sabemos que existem $X \subset A$ tal que $A = \langle X \rangle$ e um epimorfismo $\varphi : F(X) \longrightarrow A$, onde $F(X)$ é livre gerado por X. Seja $\psi : A/\langle X \rangle^A \longrightarrow H$ dada por

$$[a] \mapsto \psi([a]) = \theta(a), \forall a \in A.$$

É fato que, se $a \in [b] = b \cdot \langle R \rangle^A$ então $ab^{-1} \in \langle \{a^{-1}ra;\ a, r \in R\} \rangle$. Assim,

$$ab^{-1} = a_{i_1}^{-1} r_{i_1} a_{i_1} \dots a_{i_n}^{-1} r_{i_n} a_{i_n},\ a_{i_k} \in A, r_{i_k} \in R,\ k = 1, \dots, n. \tag{2.8}$$

ALém disso, sendo $\varphi : F(X) \longrightarrow A$ um epimorfismo e $\langle R \rangle^A \subset A$, existe $w = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ tal que $\varphi(w) = ab^{-1}$. Logo,

$$ab^{-1} = \varphi(w) = \varphi(x_{i_1}^{\epsilon_1}) \dots \varphi(x_{i_n}^{\epsilon_n}) \tag{2.9}$$

onde $\phi(x_{i_1}^{\epsilon_1}) = a_{i_k}^{-1} r_{i_k} a_{i_k},\ a_{i_k} \in A,\ r_{i_k} \in R$, para todo $k = 1, \dots, n$. Daí, temos

$$\begin{aligned} \theta(a)\theta(b)^{-1} &= \theta(\varphi(x_{i_1}^{\epsilon_1}) \dots \varphi(x_{i_n}^{\epsilon_n}) \\ &= \theta(a_{i_1}^{-1} r_{i_1} a_{i_1}) \dots \theta(a_{i_1}^{-1} r_{i_n} a_{i_n}) \\ &= \theta(a_{i_1}^{-1})\theta(r_{i_1})\theta(a_{i_1}) \dots \theta(a_{i_n}^{-1})\theta(r_{i_n})\theta(a_{i_n}) \\ &= \theta(a_{i_1})^{-1}\theta(a_{i_1}) \dots \theta(a_{i_n})^{-1}\theta(a_{i_n}) \Rightarrow \theta(a)\theta(b) = \psi([a])\psi([b]). \end{aligned} \tag{2.10}$$

Isto prova que ψ é bem definido. Para todo $[a], [b] \in A/\langle R \rangle^A$ temos

$$\psi([a][b]) = \psi([a \cdot b]) = \theta(a \cdot b) = \theta(a)\theta(b) = \psi([a])\psi([b]). \tag{2.11}$$

Portanto, ψ é um homomorfismo que satisfaz $(\psi \circ \pi)(a) = \theta(a)$, para todo $a \in A$. □

Observação 2.12. Quando dois grupos possuem a mesma apresentação $\langle X|R \rangle$, então eles são isomorfos. De fato, sejam G e H grupos apresentados por $\langle X|R \rangle^{\varphi}$ e $\langle X|R \rangle^{\psi}$ sob os epimorfismos $\varphi : F(X) \longrightarrow G$ e $\psi : F(X) \longrightarrow H$, respectivamente. Consequentemente, temos que $\langle R \rangle^{F(X)} = ker(\varphi)$ e $\langle R \rangle^{F(X)} = ker(\psi)$. Como $ker(\varphi) = ker(\psi)$, do Teorema do Isomorfismo I vem que

$$G \cong \frac{F(X)}{ker(\varphi)} \cong \frac{F(X)}{ker(\psi)} \cong H. \tag{2.12}$$

□

Claramente, um grupo G pode ter muitas apresentações mesmo para um determinado X e ϕ dado. Para comparar essas apresentações e resolver este problema vamos estudar as *transformações de Tietze* e concluir que é possível deduzir uma determinada apresentação com uma já dada.

Seja G um grupo com apresentação $\langle X|R \rangle^{\varphi}$. Então, $\langle X|R \cup S \rangle^{\varphi}$ também é uma apresentação de G para todo subconjunto S de $\langle R \rangle^{F(X)}$. Sendo assim, diremos que $\langle X|R \cup S \rangle^{\varphi}$ foi obtida de $\langle X|R \rangle^{\phi}$ por uma *transformação de Tietze do tipo I* e que $\langle X|R \rangle^{\varphi}$ provém de uma *transformação geral de Tietze do tipo I'*. Se $|S| = 1$ diremos *transformação de*

Tietze simples.

Seja Y um conjunto tal que $X \cap Y = \varnothing$ e seja u_y o elemento de $F(X)$ fara cada $y \in Y$. Então $\langle X \cup Y | R \cup \{yu_y^{-1}, \forall y \in Y\}\rangle^{\psi}$ também apresenta G quando $\psi(x) = \varphi(x)$ e $\psi(y) = \varphi(u_y)$. De fato, seja $N = \langle R \cup \{yu_y^{-1}\}\rangle^{F(X)}$. Então, ψ induz o epimorfismo $\pi : F(X \cup Y)/N \to G$, dado por $wN \mapsto \varphi(w)$ onde $\phi(R \cup \{yu_y^{-1}\}) = \{1\}$. Daí, o teorema de von Dyck garante que existe um epimorfismo $\rho : G \longrightarrow F(X \cup Y)/N$ com $\rho \circ \varphi(x) = xN$. Claramente, $\pi \circ \rho$ é a aplicação identidade. Além disso, note que

$$\rho \circ \pi(yN) = \rho\psi(y) = \rho\phi(u_y)u_yN = y_N. \tag{2.13}$$

Portanto, a composição $\rho \circ \pi$ resulta na identidade e temos provado o resultado. Nós dizemos que $\langle X \cup Y | R \cup \{yu_y^{-1}, \forall y\}\rangle^{\psi}$ resulta de $\langle X|R\rangle^{\varphi}$ por uma *transformação geral de Tietze do tipo II* e que $\langle X|R\rangle^{\varphi}$ resulta de $\langle X \cup Y | R \cup \{yu_y^{-1}, \forall y\}\rangle^{\psi}$ por uma *transformação geral de Tietze do Tipo II'*. Quando $|Y| = 1$ nos referimos a uma *transformação de Tietze simples.*

Os seguintes resultados serão assumidos sem demonstrações, contudo poderão ser encontradas em [3] da referência.

Teorema 2.5. *Duas apresentações de um mesmo grupo podem ser obtidas uma da outra mediante uma sequência de transformações de Tietze. Se ambas as apresentações são finitas então poderão ser obtidas uma da outra mediante transformações de Tietze simples.*

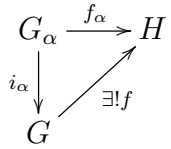
Proposição 2.12. *Seja G um grupo finitamente gerado e seja $\langle Y|S\rangle^{\psi}$ uma apresentação de G. Então, existe um subconjunto finito X de Y que gera G.*

Proposição 2.13. *Seja G apresentado por $\langle X|R\rangle^{\varphi}$ e $\langle Y|S\rangle^{\psi}$. Se X, R e Y são finitos então existe um subconjunto S_1 de S tal que G é apresentado por $\langle Y|S_1\rangle^{\psi}$.*

2.4 Produtos Livres

Nesta última secção do Capítulo 2 iremos definir um novo tipo de grupo chamado de Produto Livre que é a generalização do conceito de grupo livre.

Definição 2.9. Sejam $\{G_\alpha\}$ uma família de grupos, G um grupo e $i_\alpha : G_\alpha \longrightarrow G$ um homomorfismo. Então, $(G, \{i_\alpha\})$ é chamado o *produto livre* dos grupos G_α se para todo grupo H e homomorfismo $f_\alpha : G_\alpha \longrightarrow H$ existir um único homomorfismo $f : G \longrightarrow H$ tal que $f_\alpha = f \circ i_\alpha$, para todo α.



Observação 2.13. A propriedade descrita na Definição 2.9 é também conhecida como *Propriedade Universal para Produtos Livres.*

Assim como fizemos com os grupos livres podemos nos perguntar se quando o produto livre existe ele é único, mais ainda se as aplicações i_α são monomorfismos. Essa questão é respondida na proposição abaixo cuja demonstração é omitida por ser a generalização imediata da demonstração da Proposição 2.2.

Proposição 2.14. *Se $(G, \{i_\alpha\})$ e $(H, \{j_\alpha\})$ são ambos produto livre de uma mesma família de grupos $\{G_\alpha\}$ então existe um único isomorfismo $f : G \longrightarrow H$ tal que $f \circ i_\alpha = j_\alpha$, para todo α.*

Proposição 2.15. *Toda família de grupos G_α tem um produto livre.*

Prova: Suponha que para cada α, o grupo G_α é apresentado por $\langle X|R_\alpha\rangle^{\varphi_\alpha}$. Além disso, sem perda de generalidade, vamos supor que $X_\alpha \cap X_\beta = \varnothing$ sempre que $\alpha \neq \beta$. Seja

$$G = \frac{F(\underset{\alpha}{\cup} X_\alpha)}{\langle \underset{\alpha}{\cup} R_\alpha \rangle^{F(\underset{\alpha}{\cup} X_\alpha)}}.$$

Então G é apresentado por $\langle \underset{\alpha}{\cup} X_\alpha | \underset{\alpha}{\cup} R_\alpha \rangle^{\varphi}$ onde $\varphi : F(\underset{\alpha}{\cup} X_\alpha) \longrightarrow G$ é a aplicação natural. Agora, veja que pela observação 2.11, que é consequência do Teorema de Von Dyck, a inclusão $\bar{i}_\alpha : X_\alpha \longrightarrow \underset{\alpha}{\cup} X_\alpha$ induz um homomorfismo $i_\alpha : G_\alpha \longrightarrow G$. Nosso trabalho será mostrar que $(G, \{i_\alpha\})$ é o produto livre da família $\{G_\alpha\}$.

Seja H um grupo qualquer. Considere para cada α o homomorfismo $f_\alpha : G_\alpha \to H$. Claramente, f_α induz um homomorfismo

$$\psi_\alpha = f_\alpha \circ \varphi : F(X) \to H$$

tal que $\psi_\alpha(R_\alpha) = \{1\}$, para todo α. Defina o homomorfismo

$$\psi : F(\underset{\alpha}{\cup} X_\alpha) \to H$$

por $\psi(x) = \psi_\alpha(x)$, $\forall x \in X_\alpha$. É óbvio que $\psi(\underset{\alpha}{\cup} R_\alpha) = \{1\}$. Sendo assim, o teorema de Von Dyck nos garante a existência de um homomorfismo $f : G \to H$ tal que o diagrama abaixo comuta

$$\begin{array}{ccc} F(\underset{\alpha}{\cup} X_\alpha) & \xrightarrow{\psi} & H \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\exists!\, f} & \\ G & & \end{array} \tag{2.14}$$

Agora, para cada α, temosd que $(i_\alpha \circ \varphi_\alpha)(x_\alpha) = \varphi(x_\alpha)$, para todo $x_\alpha \in X_\alpha$. Obtemos

então o diagrama

$$\begin{array}{ccccc} F(X_\alpha) & \xrightarrow{\varphi_\alpha} & G_\alpha & \xrightarrow{f_\alpha} & H \\ \downarrow & & \downarrow{\scriptstyle i_\alpha} & \nearrow{\scriptstyle f} & \\ F(\bigcup_\alpha X_\alpha) & \xrightarrow{\varphi} & G & & \end{array} \tag{2.15}$$

Concluindo, temos

$$\begin{aligned} f(i_\alpha(\varphi_\alpha(x_\alpha))) &= f(\varphi(x_\alpha)) \\ &= \psi(x_\alpha) \\ &= \psi_\alpha(x_\alpha) \\ &= f_\alpha(\varphi_\alpha(x_\alpha)), \forall x_\alpha \in X_\alpha \end{aligned} \tag{2.16}$$

Conforme a definição 2.9 de produtos livres, encontramos um homomorfismo f que satisfaz a Propriedade Universal. □

Observação 2.14. O produto livre de uma família de grupos $\{G_\alpha\}$ é denotado por $G = *G_\alpha$. Denotamos por $G = G_1 * \ldots * G_n$ o produto livre da família de grupos $\{G_\alpha\}$ quando $\alpha \in \{1, \ldots, n\}$.

Exemplo 2.9. O grupo livre $F(X)$ é o produto livre da família de grupos cíclicos $\{\langle x \rangle;\ x \in X\}$.

Os seguintes resultados serão assumidos sem demonstrações. O primeiro é a versão do Teorema da Forma Normal para o produto livre e o segundo também é análogo ao que foi feito para grupos livres.

Teorema 2.6. *(Teorema da Forma Normal para Produtos Livres) Seja $(G, \{i_\alpha\})$ o produto livre da família de grupos $\{G_\alpha\}$. Então,*

1. *Cada i_α é um monomorfismo;*
2. *Considerando i_α como a inclusão, todo elemento de G pode ser escrito unicamente da forma $g_a \ldots g_n$, com $n \geq 0$, $g_i \in G$ para cada $\alpha_i, g_i \neq 1$ e $\alpha_r \neq \alpha_{r+1}$ para $r < n$.*

Proposição 2.16. *Seja G_α subgrupos de um grupo G. Então as seguintes afirmações são equivalentes.*

i. G é o produto livre dos subgrupos G_α.

ii. Todo elemento de G pode ser escrito unicamente como $g_1 \ldots g_n$, com $n \geq 0$,$g_i \in G_{\alpha_i}$, $g_i \neq 1$ e $\alpha_i \neq \alpha_{i+1}$.

iii. G é gerado pelos subgrupos G_α e 1 não pode ser escrito como um produto $g_1 \ldots g_n$ com $n > 0$, $g_i \in G_{\alpha_i}$, $g_i \neq 1$ e $\alpha \neq \alpha_{i+1}$.

2.5 Apresentação de Produtos diretos, Semidiretos e Extensões de Grupos

Nesta última secção iremos calcular a apresentação dos produtos direto e semidireto de grupos bem como das extensões de grupos. Para isto, também vamos calcular uma apresentação para extensões de grupos. Cabe ressaltar a importância desta secção para o trabalho, pois pretendemos escrever o grupo de tranças puras PB_n como o produto semidireto de grupos livres. Os resultados aqui expostos estão contidos em [8].

Proposição 2.17. *Sejam G e H grupos apresentados por $\langle X|R\rangle$ e $\langle Y|S\rangle$, respectivamente. Então o produto direto $G\times H$ tem a apresentação $\langle X,Y|R,S,[X,Y]\rangle$, onde $[X,Y]$ denota o subgrupo dos comutadores $\{x^{-1}y^{-1}xy;\ x\in X, y\in Y\}$.*

Prova: Sejam D um grupo que possui apresentação $\langle X,Y|R,S,[X,Y]\rangle$ e $i_X : X \longrightarrow D$, $i_Y : Y \longrightarrow D$ inclusões. O Teorema de Von Dick garante que estas inclusões induzem homomorfismos $\bar{i}_X : G \longrightarrow D$ e $\bar{i}_Y : H \longrightarrow D$, respectivamente.

Observe que os relatores $[X,Y]$ garantem que os elementos da imagem de $\bar{i}_X$ comutam com os elementos da imagem de $\bar{i}_Y$ em D. Seja aplicação $\alpha : G\times H \longrightarrow D$ definida por $\alpha(g,h) = \bar{i}_X(g)\bar{i}_Y(h)$. Claramente, α é um homomorfismo, basta verificar que é um isomorfismo. De fato, $\alpha(x,1) = x, \forall x\in X$ e $\alpha(1,y) = y, \forall y\in Y$. Enfim, considere a aplicação $: X\cup Y \longrightarrow G\times H$ dada por $(x) = (x,1)$ e $(y) = (1,y)$. Logo, pelo Teorema de Von Dyck, existe um homomorfismo $\beta : D \longrightarrow G\times H$ que estende . Como $\beta\circ\alpha$ e $\alpha\circ\beta$ fixam os geradores de D e de $G\times H$, concluímos que β é o inverso de α. Consequentemente, α é um isomorfismo e pela observação 2.12 encontramos uma apresentação para $G\times H$. □

Definição 2.10. Sejam $G, \tilde{G}, A$ grupos. Dizemos que $\tilde{G}$ é uma extensão do grupo G por A se existir um subgrupos normal N de $\tilde{G}$ tal que A é isomorfo a N e o quociente $\tilde{G}/N$ é isomorfo a G, ou seja, $A \overset{\alpha}{\cong} N$ e $\tilde{G}/N \overset{\beta}{\cong} G$, onde α e β são isomorfismos, respectivamente.

A seguir, iremos dar exemplos de casos em que surgem extensões de grupos.

1. Seja $l : A \longrightarrow \tilde{G}$ um mergulho normal. Então, $Im\, l \lhd \tilde{G}$. Assim, defina $N = Im\, l$ e $G = \tilde{G}/Im\, l$. Portanto, $A \overset{\alpha}{\cong} Im\, l$ e consequentemente $\tilde{G}/Im\, l \overset{\beta}{\cong} G$.

2. Seja $\vartheta : \tilde{G} \longrightarrow G$ um epimorfismo. Vamos definir $A = ker\vartheta$. Assim, Pelo Teorema do Isomorfismo I temos que $ker\vartheta \lhd \tilde{G}$ e $\tilde{G}/ker\vartheta \cong G$. Sendo assim, $\tilde{G}$ é uma extensão de G por A.

Veja que podemos ilustrar a extensão de grupos pelos diagramas

$$A \xrightarrow{\alpha} N \xrightarrow{i} \tilde{G}$$

$$\tilde{G} \xrightarrow{p} \tilde{G}/N \xrightarrow{\beta} G$$

Aqui, l é um homomorfismo injetor, ou seja, $ker\ l = \{1\}$, ϑ é um homomorfismo sobrejetor, ou seja, $Im\theta = G$ e por fim, $Im\ l = ker\vartheta$.

Observação 2.15. Conforme as considerações acima, pela Definição 1.24 podemos pensar a extensão de grupos como uma sequência exata curta

$$1 \longrightarrow A \xrightarrow{l} \tilde{G} \xrightarrow{\vartheta} G \longrightarrow 1$$

Suponha que seja dada a extensão

$$1 \longrightarrow A \xrightarrow{l} \tilde{G} \xrightarrow{\vartheta} G \longrightarrow 1$$

onde os grupos G e A são apresentados por $\langle X|R\rangle$ e $\langle Y|S\rangle$, respectivamente. Vamos buscar uma apresentação para a extensão $\tilde{G}$. Para isto, seguiremos três passos abaixo.

i. Considere os conjuntos $\tilde{Y} = \{\tilde{y} = l(y); y \in Y\}$ e $\tilde{S} = \{\tilde{s}; s \in S\}$. $\tilde{S}$ é o conjunto das palavras em $\tilde{Y}$ obtidas de S substituindo y por $\tilde{y}$ quando y aparecer. Seja $\tilde{X} = \{\tilde{x}; x \in X\}$ os membros do transversal para $Im\ l$ em G tal que $\vartheta(\tilde{x}) = x$, para todo $x \in X$.

ii. Para cada $r \in R$, seja $\tilde{r}$ a palavra em $\tilde{X}$ obtida de r pela substituição de cada x por $\tilde{x}$. Veja que $\vartheta(\tilde{r}) = 1_G$, logo para cada $r \in R$ temos que $\tilde{r} \in ker\vartheta = Im\ l$. Desde que $Im\ l = \langle\tilde{Y}\rangle$, cada $\tilde{r}$ pode ser escrito como uma palavra, a saber, $\theta_r \in \tilde{Y}$. Assim, seja $R = \{\tilde{r}\theta_r^{-1};\ r \in R\}$.

iii. Como $Im\ l \lhd G$ cada conjugado $\tilde{x}^{-1}\tilde{y}x$, $\tilde{x} \in \tilde{X}$, $\tilde{y} \in \tilde{Y}$ pertence a $Im\ l$ e assim é uma palavra, a saber, $w_{x,y}$ em $\tilde{Y}$. Seja $\tilde{T} = \{\tilde{x}^{-1}\tilde{y}\tilde{x}\tilde{w}_{x,y}^{-1};\ x \in X, y \in Y\}$.

Teorema 2.7. *Com as notações anteriores, o grupo $\tilde{G}$ tem apresentação $\langle\tilde{X}, \tilde{Y}|\tilde{R}, \tilde{S}, \tilde{T}\rangle$.*

Prova: Vamos supor que o grupo D possua a apresentação $\langle\tilde{X}, \tilde{Y}|\tilde{R}, \tilde{S}, \tilde{T}\rangle$. Pelo teorema de Von Dyck existe um homomorfismo

$$\begin{aligned} \theta : D &\to \tilde{G} \\ d &\mapsto \theta(d) = \begin{cases} \tilde{x} & se\ d = \tilde{x} \\ \tilde{y} & se\ d = \tilde{y} \end{cases} \end{aligned} \tag{2.17}$$

Quando restringimos θ ao gerado por $\tilde{Y}$ temos o homomorfismo

$$\theta_1 : \langle\tilde{Y}\rangle \to Im\ l \cong A$$

onde $\theta_1(\tilde{y}) = y$. Sabemos que as relações definidoras S de A são satisfeitas em $\langle \tilde{Y} \rangle \geq D$. Portanto, θ_1 é uma bijeção. Além disso, $\langle \tilde{Y} \rangle$ é um subgrupo normal de D, sendo assim, obtemos

$$\theta_2 : \frac{D}{\langle \tilde{Y} \rangle} \to \frac{\tilde{G}}{Im\ l} \cong G \tag{2.18}$$

que é dado por $\theta_2(\tilde{x}\langle \tilde{Y} \rangle) = x$. Temos então que θ_2 é uma bijeção.

Com isso, chegamos ao seguinte diagrama comutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & < \tilde{Y} > & \xrightarrow{i} & D & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta_2} & & \\ 1 & \longrightarrow & A & \xrightarrow[l]{} & \tilde{G} & \xrightarrow[\vartheta]{} & G & \longrightarrow & 1 \end{array}$$

cujas linhas são exatas. Sendo θ_1 e θ_2 isomorfismos, pelo Lema dos Cinco temos que θ é isomorfismo. Portanto os grupos D e $\tilde{G}$ são isomorfos e possuem a mesma apresentação. □

Corolário 2.5. *Sejam $G = \langle X|R \rangle$ e $A = \langle Y|S \rangle$ grupos e $\alpha : G \longrightarrow Aut(A)$ um homomorfismo tal que $\alpha(x)y = w_{x,y}$, onde $w_{x,y} \in Y^{\mp 1}$, com $x \in X$, $y \in Y$. Então o produto semidireto tem a apresentação*

$$G \ltimes_\alpha A = \langle X, Y | R, S, \{x^{-1}yxw_{x,y}^{-1}; x \in X, y \in Y\} \rangle$$

.

Corolário 2.6. *Sejam G e A grupos finitamente apresentados. Então a extensão $\tilde{G}$ de G por A é também finitamente apresentada.*

3

Tranças e Grupo de Tranças

Neste capítulo faremos um estudo dos resultados mais importantes sobre tranças e o grupo de tranças. Faremos a definição de uma trança geométrica sobre n cordas no espaço euclidiano tridimensional como foi dada por Emil Artin [1] em 1925.

Iremos definir o conceito de equivalência entre tranças por meio de uma *isotopia*, ou seja, um homeomorfismo que preserva os axiomas da definição de trança. Com isso, vamos demonstrar que o conjunto das classes de equivalência das tranças sobre n cordas, munido de uma operação binária, cumpre a Definição 1.1 de grupo. Tal grupo será chamado de *grupo de tranças Artin sobre n cordas* ou simplesmente *grupo de tranças no disco* que será denotado por B_n. Veremos que quando a permutação das cordas for trivial B_n admitirá um subgrupo que será chamado de *grupo de tranças puras sobre n cordas* ou *grupo de tranças puras no disco* e será denotado por PB_n. Estudaremos também o Teorema da Apresentação de Artin que define B_n em termos de geradores e relatores, ou seja, uma apresentação para B_n e consequentemente para PB_n.

Todo conteúdo aqui apresentado foi baseado nos seguintes autores da referência [4], [7], [12] e [13].

3.1 Tranças Geométricas

Seja $\mathbb{E}^3$ o espaço euclidiano de dimensão 3. Nós faremos a identificação de $\mathbb{E}^3$ com o espaço vetorial real $\mathbb{R}^3$, consistindo do sistema de coordenadas (x, y, z) tal que o eixo z aponta no seu sentido positivo para baixo conforme a figura 1.

Consideremos os planos paralelos $z = z_0$ e $z = z_1$ em $\mathbb{E}^3$, com $z_0 < z_1$, onde o chamaremos de *plano superior* e *plano inferior*, respectivamente. Sobre o plano superior marquemos n pontos $P_1, \ldots, P_n$ distintos e colineares e consideremos os pontos $P_1' \ldots, P_n'$ suas projeções ortogonais no plano inferior.

Definição 3.1. Uma trança geométrica sobre n cordas (ou uma n-trança) β é um sistema de n arcos $\mathscr{A} = \{\mathscr{A}_0, \ldots, \mathscr{A}_n\}$ mergulhados em $\mathbb{E}^3$, onde o i-ésimo arco $\mathscr{A}_i$ conecta o ponto

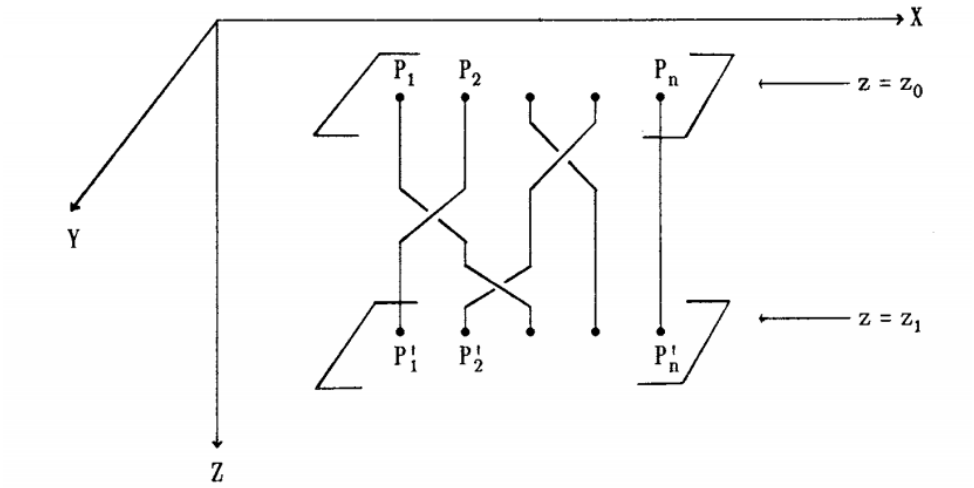
P_i no plano superior ao ponto $P'_{\tau(i)}$ no plano inferior para cada permutação $\tau \in \{1, \ldots, n\}$, satisfazendo os seguintes axiomas:

(i) Cada arco $\mathscr{A}$ intercepta cada plano paralelo intermediário aos planos superior e inferior exatamente uma vez.

(ii) Os arcos $\mathscr{A}_0, \ldots, \mathscr{A}_n$ interceptam cada plano parelelo intermediário aos planos superior e inferior em exatamente n pontos distintos.

A permutação τ é chamada de permutação da trança. O arco $\mathscr{A}_i$ é chamado de i-ésima corda ou i-ésimo fio da trança. Quando for conveniente escreveremos $(\mathscr{A}, \tau)$ para destacar o sistema de arcos e a permutação referente.

Figura 3.1: Representação de uma trança geométrica



Fonte: [7]

Observação 3.1. Podemos pensar num arco em $\mathbb{E}^3$ como a imagem de um mergulho $\mathscr{A}_i : [0,1] \to \mathbb{E}^3$, ou seja, como um caminho injetor do intervalo unitário $[0,1]$ em $\mathbb{E}^3$.

A seguir faremos a definição de tranças equivalentes. De maneira informal diremos que duas n-tranças β_1 e β_2 são equivalentes se pudermos deformar seus fios continuamente uma na outra, de forma que em cada passo as condições da definição 3.1 sejam obedecidas.

Definição 3.2. Duas n-tranças $\mathscr{A}^0 = \{\mathscr{A}_1^0, \ldots, \mathscr{A}_n^1\}$ e $\mathscr{A}^1 = \{\mathscr{A}_1^1, \ldots, \mathscr{A}_n^1\}$ com a mesma permutação τ são ditas *equivalentes* (ou *isotópicas*) se existe uma *isotopia ambiente*, ou simplemente *isotopia*, entre as tranças geométricas com permutação τ de $\mathscr{A}^0$ para $\mathscr{A}^1$, em outras palavras, se existirem n aplicações contínuas

$$F_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3, \ 1 \leq i \leq n$$

tal que

$$\begin{cases} F_i(t,0) = \mathscr{A}_i(t) \\ \qquad\qquad 0 \leq t \leq 1,\ 1 \leq i \leq n \\ F_i(t,1) = \mathscr{A}'_i(t) \end{cases} \tag{3.1}$$

$$\begin{cases} F_i(0,s) = P_i \\ \qquad\qquad 0 \leq s \leq 1,\ 1 \leq i \leq n \\ F_i(1,s) = P'_{\tau(i)} \end{cases} \tag{3.2}$$

de modo que se nós definimos $\mathscr{A}_i^s : [0,1] \longrightarrow \mathbb{E}^3$ por $\mathscr{A}_i^s(t) = F_i(t,s)$, então $\mathscr{A}^s = \{\mathscr{A}_1^s, \ldots, \mathscr{A}_n^s\}$ é ainda uma n-trança geométrica (com permutação τ) para cada $0 \leq s \leq 1$.

Observação 3.2. De fato, a relação de equivalência de tranças enunciada na definição 3.2 é uma relação de equivalência. Com efeito, temos satisfeitas as propriedades de

i.) **Reflexividade**: Seja $(\mathscr{A}, \tau)$ uma n-trança. Então para cada $1 \leq i \leq n$ temos que a aplicação $F_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ dada por $F_i(t,s) = A_i(t)$, $\forall t, s \in [0,1]$ satisfaz

$$\begin{cases} F_i(t,0) = \mathscr{A}_i(t) \\ \\ F_i(t,1) = \mathscr{A}_i(t) \end{cases} \tag{3.3}$$

$$\begin{cases} F_i(0,s) = P_i \\ \\ F_i(1,s) = P'_{\tau(i)} \end{cases} \tag{3.4}$$

Ou seja, temos que $(\mathscr{A}, \tau) \sim (\mathscr{A}, \tau)$,

ii.) **Simetria**: Sejam $(\mathscr{A}^0, \tau) \sim (\mathscr{A}^1, \tau)$ duas n-tranças. Então existem n aplicações $F_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$, onde $1 \leq i \leq n$, tais que

$$\begin{cases} F_i(t,0) = \mathscr{A}_i^0(t) \\ \\ F_i(t,1) = \mathscr{A}^1(t)_i \end{cases} \tag{3.5}$$

$$\begin{cases} F_i(0,s) = P_i \\ \\ F_i(1,s) = P'_{\tau(i)} \end{cases} \tag{3.6}$$

Para cada $i \in \{1, \ldots, n\}$ defina a aplicação $G_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ dada por $G_i(t,s) = F_i(t, 1-s)$ com $0 \leq t$ e $s \leq 1$. Sendo assim, note que

$$\begin{cases} G_i(t,0) = F_i(t,1) = A_i^1(t) \\ \\ G_i(t,1) = F_i(t,0) = \mathscr{A}_i^0(t) \end{cases} \tag{3.7}$$

$$\begin{cases} G_i(0,s) = F_i(0,1-s) = P_i \\ \\ G_i(1,s) = F_i(1,1-s) = P'_{\tau(i)} \end{cases} \tag{3.8}$$

Logo, $(A^1, \tau) \sim (\mathscr{A}^0, \tau)$.

iii.) **Transitividade:** Sejam as n-tranças $(\mathscr{A}^0, \tau), (\mathscr{A}^1, \tau)$ e $(\mathscr{A}^2, \tau)$ tais que $(\mathscr{A}^0, \tau) \sim (\mathscr{A}^1, \tau)$ e $(\mathscr{A}^1, \tau) \sim (\mathscr{A}^2, \tau)$. Então existem aplixações $F_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ e $G_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ satisfazendo a definição 3.2. Vamos definir $H_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ por

$$H_i(t,s) = \begin{cases} F_i(t,2s), & 0 \leq s \leq 1/2, \\ \\ G_i(t,2s-1), & 1/2 \leq s \leq 1 \end{cases} \tag{3.9}$$

Veja que H_i é contínua para todo $i \in \{1, \ldots, n\}$, então

$$\begin{cases} H_i(t,0) = F_i(t,0) = \mathscr{A}_i^0, & 0 \leq s \leq 1/2, \\ \\ H_i(t,1) = G_i(t,1) = A_i^1, & 1/2 \leq s \leq 1 \end{cases} \tag{3.10}$$

$$H_i(0,s) \;\; = \;\; \begin{cases} F_i(0,2s) = P_i, & 0 \leq s \leq 1/2 \\ G_i(0,2s-1) = P_i, & 1/2 \leq s \leq 1 \end{cases} \tag{3.11}$$

$$H_i(1,s) \;\; = \;\; \begin{cases} F_i(1,2s) = P'_\tau(i), & 0 \leq s \leq 1/2 \\ G_i(1,2s-1) = P'_\tau(i), & 1/2 \leq s \leq 1 \end{cases} \tag{3.12}$$

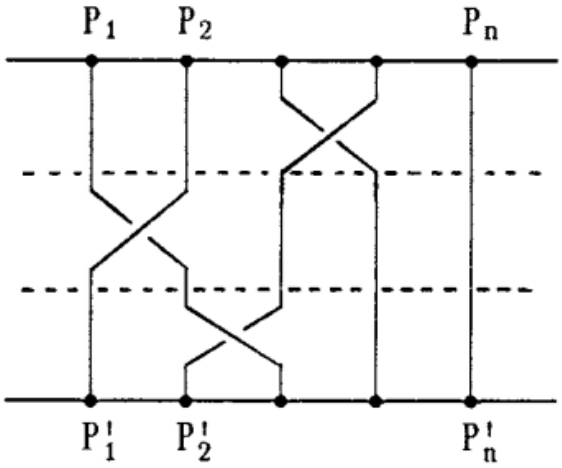
Sendo assim, concluímos que $(\mathscr{A}^0, \tau) \sim (\mathscr{A}^2, \tau)$.

Observação 3.3. Neste trabalho, em termos de notação, devido a relação de isotopia de tranças, não faremos distinção entre a trança β e sua classe de equivalência $[\beta]$. Além

disso, também usaremos, quando for conveniente, a notação $\beta = (\beta_1, \ldots, \beta_n)$ para denotar a classe de equavalência de uma trança β.

Observação 3.4. Podemos visualizar uma trança projetando-a num plano em $\mathbb{E}^3$ contendo os pontos $P_1, \ldots, P_n, P'_1, \ldots, P'_n$ como um sistema de arcos poligonais cujo cruzamentos entre os arcos são transversais. Veja que cada cruzamento pode ser visto em diferentes níveis, eles serão indicados quando os arcos se cruzam por cima ou por baixo um dos outros.

Figura 3.2: Projeção padrão de uma n-trança



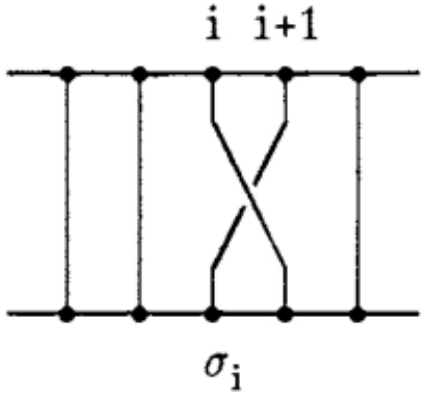
Fonte: [7]

3.2 Geradores de Artin

A figura 3.2 nos permite decompor uma trança em várias outras tranças chamadas *tranças elementares*. Veremos como que uma trança pode ser escrita como um produto dessas tranças elementares e a partir daí estudar relações que são satisfeitas por tais. O intuito é de estudar uma apresentação para o grupo de tranças, que será descrito em breve, e de enunciar o Teorema da Apresentação de Artin. A partir de agora o conjunto das classes de equivalência de uma n-trança β será denotado por B_n.

Definição 3.3. Para cada $1 \leq i \leq n-1$ vamos denotar denotar por σ_i a n-trança geométrica elementar quando i-ésimo arco da trança cruzar por cima o $(i+1)$-ésimo arco uma única vez e as demais cordas ligam os pontos $P_1, \ldots, P_n, P'_1, \ldots, P'_n$ sem se cruzarem.

Figura 3.3: n-trança geométrica elementar



Fonte: [7]

Exemplo 3.1. Se olharmos a trança da figura 3.2 como uma 5-trança β podemos escrevê-la como um produto de tranças elementares, a saber, $\beta = \sigma_3^{-1} \cdot \sigma_1^{-1} \cdot \sigma_2$.

A partir de agora vamos definir uma operação em B_n afim de demonstrar que o conjunto das n-tranças geométricas possue estrutura de grupo.

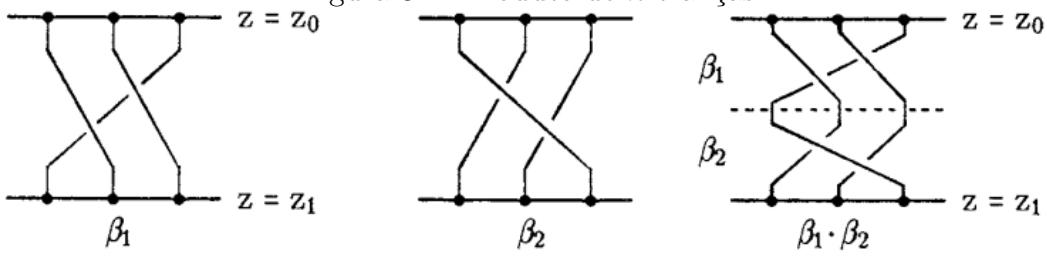
Definição 3.4. Sejam β_1 e β_2 duas n-tranças geométricas. Então nós definimos o produto (composição) das tranças β_1 e β_2, denotado por $\beta_1 \cdot \beta_2$, da seguinte forma:

i.) Identificamos o plano superior de β_2 com o plano inferior de β_1 de modo que os pontos finais e inicias de tais tranças coincidam.

ii.) Removemos os planos coincidentes e consideramos como plano superior $z = z_0$ e plano inferior $z = z_1$ os tais planos de β_1 e β_2, respectivamente.

iii.) Comprimimos de modo contínuo a n-trança resultante dos passos anteriores.

Figura 3.4: Produto de n-tranças

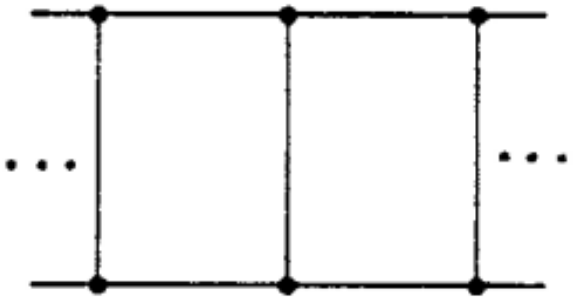


Fonte: [7]

Observação 3.5. Se substituirmos as tranças β_1 e β_2 por tranças homotópicas β_1' e β_2' temos que o produto $\beta_1' \cdot \beta_2'$ é isotópica a $\beta_1 \cdot \beta_2$. Assim, o produto no conjunto das classes de equivalência de n-tranças, feito na definição 3.4, é bem definido.

Definição 3.5. A n-trança trivial ϵ é a n-trança cujos fios ligam os pontos $P_1, \ldots, P_n, P'_1, \ldots, P'_n$ de forma ortogonal, ou seja, não se cruzam conforme a figura 3.5

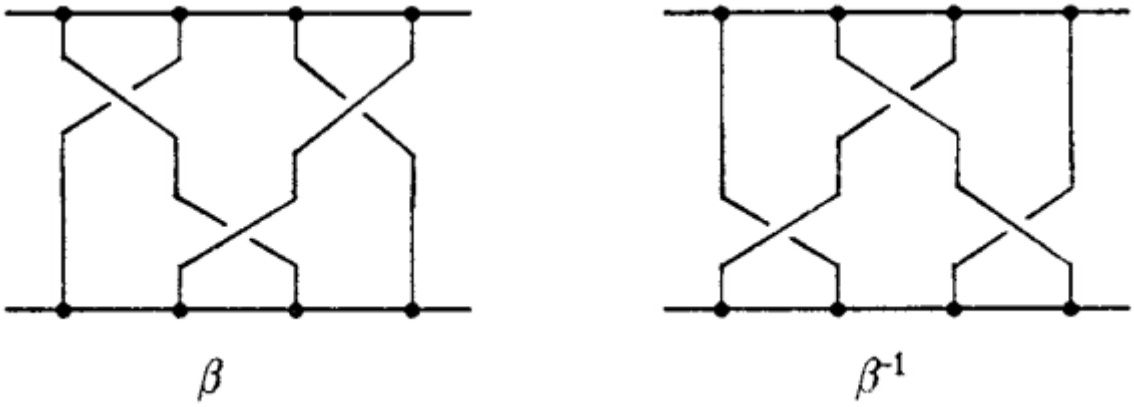
Figura 3.5: n-trança trivial



Fonte: [7]

Definição 3.6. A n-trança inversa β^{-1} de uma n-trança β é obtida pela imagem refletida de β num espelho horizontal no plano inferior.

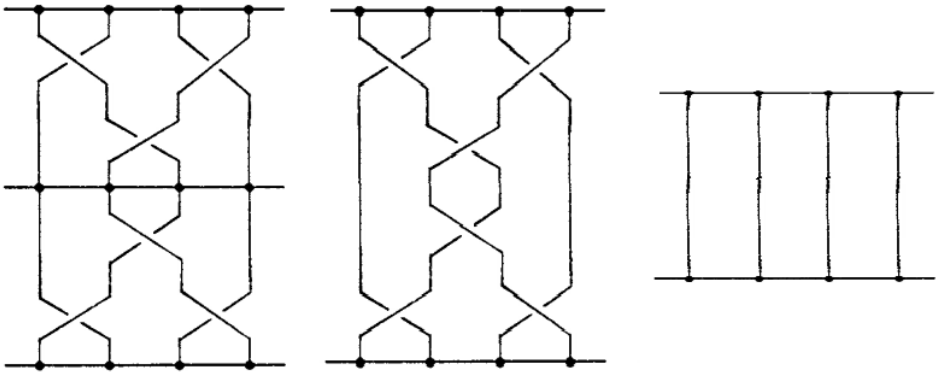
Figura 3.6: n-trança inversa β^{-1}



Fonte: [7]

Observação 3.6. Conforme a Definição 3.6 o produto das n-tranças β e β^{-1} é isotópico a n-trança trivial. Ilustramos abaixo o produto $\beta \cdot \beta^{-1}$.

Figura 3.7: Produto das n-tranças β e β^{-1}



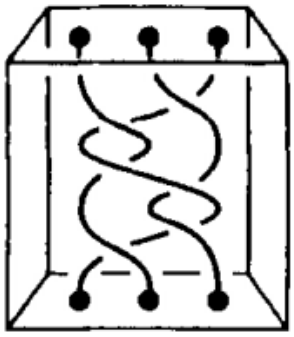
[7]

Observação 3.7. O produto de tranças em B_n é bem definido. Os elementos neutro e o inverso de uma trança serão a classe de equivalência da trança trivial ϵ e da trança inversa β^{-1}. A demonstração formal dessas afirmações são encontradas em [4].

Definição 3.7. O par $(B_n, \cdot)$ tem estrutura de grupo e será chamado de *Grupo de Trança de Artin sobre n cordas.*

Observação 3.8. Podemos ver uma n-trança geométrica definida num cubo onde os planos superior e inferior coincidem com as faces superior e inferior do cubo. Sendo assim, B_n também é conhecido como o *grupo de tranças no disco* pois as faces do cubo são homeomorfas ao disco.

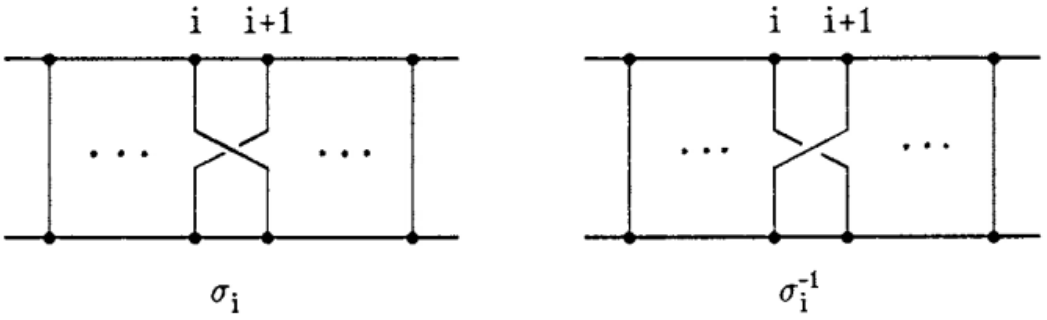
Figura 3.8: Trança representada no cilindro



Fonte: [13]

Observação 3.9. Para a trança elementar σ_i, $1 \leq i \leq n-1$, obtemos a trança inversa σ_i^{-1} é obtida pela mudança do cruzamento (conforme ilustrado na Figura 3.9) onde o $i+1$-arco passa a cruzar o i-ésimo arco por cima.

Figura 3.9: Obtenção da inversa de uma trança elementar



Fonte [7]

Observação 3.10. É intuitivo perceber, conforme a Figura 3.2, que uma classe de equivalência de uma n-trança geométrica pode ser escrita como um produto de tranças elementares σ_i com $1 \leq i \leq n-1$. Dessa forma, concluímos que os as tranças geométricas geram os elementos de B_n, ou seja, $B_n = \langle \{\sigma_i |\ 1 \leq i \leq n-1\} \rangle$. Logo, dizemos que o conjunto $\{\sigma_1, \ldots, \sigma_n\}$ é gerador de B_n.

3.3 Relações em B_n

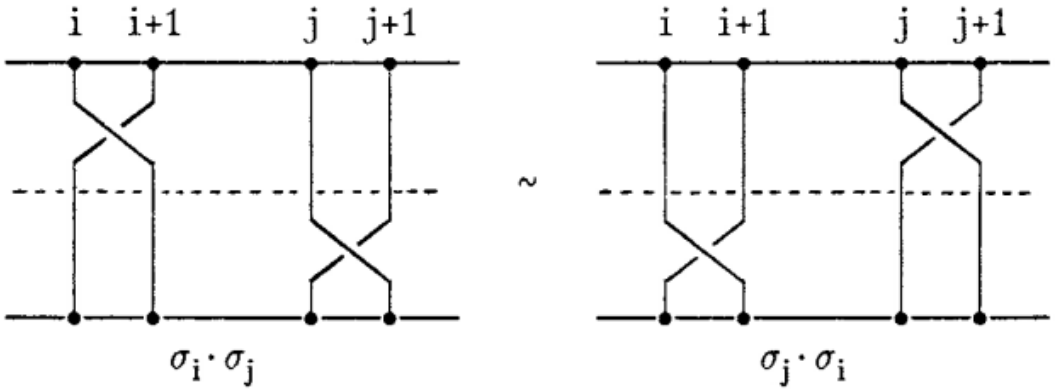
Na seção anterior mostramos que uma classe de equivalência de uma n-trança geométrica pode ser escrita como um produto de tranças elementares onde concluímos que são os geradores do grupo B_n. Agora, como pretendemos descrever B_n por meio de uma apresentação de grupos, estudaremos algumas relações que as tranças elementares satisfazem, isto será importante para enunciar o Teorema da Apresentação de Artin.

Sejam $\sigma_1, \ldots, \sigma_n$ os geradores de B_n.

1) Quando $|i-j| \geq 2$ e $1 \leq i, j \leq n-1$ temos que o par $i, i+1$ não intefere no par $j, j+1$, ou seja, obtemos a seguinte relação

$$\sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i, \ para\ |i-j| \geq 2, 1 \leq i, j \leq n-1. \tag{3.13}$$

Figura 3.10: Relação em B_n

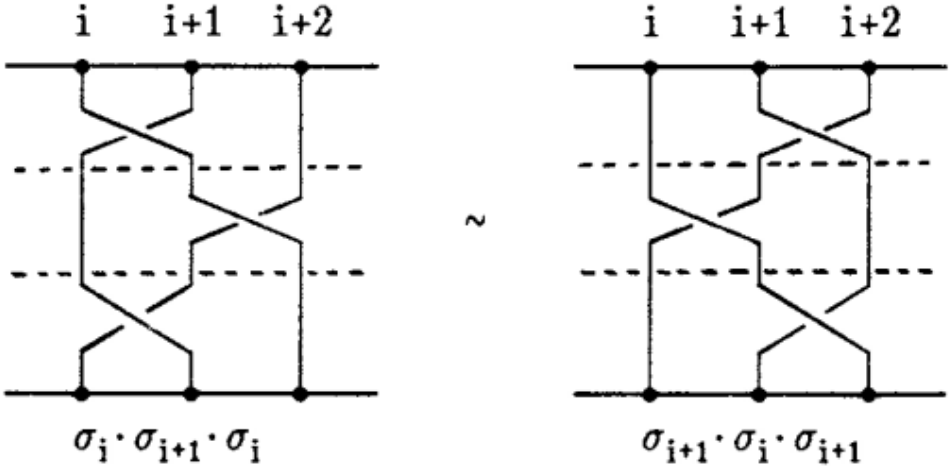


Fonte: [7]

2) Outra relação em B_n.

$$\sigma_i \cdot \sigma_{i+1} \cdot \sigma_i = \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1}, \text{ para } 1 \leq i \leq n-2. \tag{3.14}$$

Figura 3.11: Outra relação em B_n



Fonte: [7]

As relações estudadas nos itens 2 e 3 acima são as mais gerais que os elementos de B_n satisfazem, ou sejam, qualquer outra relação pode ser deduzida através destas apresentadas. Em [Artin], Emil Artin, pela primeira vez, demonstra este fato (que não é trivial). A seguir enunciamos o Teorema da Apresentação de Artin.

Teorema 3.1. *(Teorema da Apresentação de Artin) O grupo B_n de tranças geométricas sob n cordas admite apresentação com geradores $\sigma_1, \ldots, \sigma_n$ e relações*

(1) $\sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i$, *para* $|i-j| \geq 2, 1 \leq i, j \leq n-1$

(2) $\sigma_i \cdot \sigma_{i+1} \cdot \sigma_i = \sigma_i + 1 \cdot \sigma_i \cdot \sigma_{i+1}$, *para* $1 \leq i \leq n-2$.

Observação 3.11. De acordo com a notação adotada de apresentação de grupos também escrevemos a apresentação de B_n da seguinte forma:

$$B_n = \left\langle \sigma_1, \ldots, \sigma_n \middle| \begin{array}{cc} \sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i & |i-j| \geq 2,\ 1 \leq i, j \leq n-1 \\ \sigma_i \cdot \sigma_{i+1} \cdot \sigma_i = \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1} & 1 \leq i \leq n-2 \end{array} \right\rangle. \quad (3.15)$$

Exemplo 3.2. Pelo Teorema da Apresentação de Artin temos que $B_1 = \{1\}$. O grupo das 2-tranças B_2 tem apresentação $\langle \sigma_1 | \varnothing \rangle$, ou seja, é um grupo livre de *rank* 1 isomorfo ao grupo aditivo dos inteiros $\mathbb{Z}$. O grupo das 3-tranças B_3 admite a seguinte apresentação

$$\langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$$

E o grupo B_4 tem apresentação

$$\langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3, \sigma_1\sigma_3 = \sigma_3\sigma_1 \rangle.$$

Observação 3.12. A demonstração do Teorema da Apresentação de Artin requer o uso de ferramentas da Topologia Algébrica (grupo fundamental e espaços de configuração) que fogem do escorpo deste trabalho. Para tal recomendamos consultar o artigo *Theory of Braids* em [2] da referência.

Observação 3.13. O grupo de tranças com infinitas cordas é denotado por B_∞ e possui apresentação com infinitos geradores $\{\sigma_1, \sigma_2, \ldots\}$ e as mesmas relações satisfeitas em B_n.

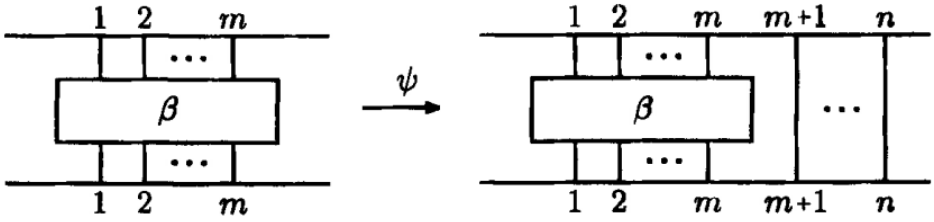
Observação 3.14. Com o Teorema da Apresentação de Artin podemos mostrar que os geradores $\{\sigma_1, \ldots, \sigma_n\}$ de B_n também satisfazem a relação $\sigma_i\sigma_{i+1}^k\sigma_i = \sigma_{i+1}^{-1}\sigma_i^k\sigma_{i+1}$, onde $k \in \mathbb{Z}$.

Proposição 3.1. *Para todo $i \in \{1, 2, \ldots, n\}$, σ_i tem ordem infinita.*

Prova: Pelo exemplo 3.2 temos claramente que os elementos de B_1 e B_2 tem ordem infinita. Para todo $n \geq 2$ o grupo B_n contém o grupo B_2, consequentemente σ_1 tem ordem infinita em B_n.
Suponha que exista um $k \in \mathbb{Z}$ tal que $\sigma_2^k = 1_n$. Então $(\sigma_1\sigma_2\sigma_1)\sigma_2^k(\sigma_1\sigma_2\sigma_1)^{-1} = 1_n$. Mas, como $(\sigma_1\sigma_2\sigma_1)\sigma_2^k(\sigma_1\sigma_2\sigma_1)^{-1} = \sigma_1$ então chegamos a conclusão de que σ_1 tem ordem finita, o que é um absurdo. □

Proposição 3.2. *Seja $1 \leq m \leq n$ então a aplicação $\psi : B_m \longrightarrow B_n$ é um monomorfismo. Consequentemente, B_m é um subgrupo de B_n.*

Figura 3.12: Inclusão de B_m em B_n



Fonte: [13]

Prova: Pelo Teorema da Apresentação de Artin temos que

$$B_m = \left\langle \sigma_1, \ldots, \sigma_m \middle| \begin{matrix} \sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i & |i-j| \geq 2,\ 1 \leq i,j \leq n-1 \\ \sigma_i \cdot \sigma_{i+1} \cdot \sigma_i = \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1} & 1 \leq i,j \leq m-2 \end{matrix} . \right\rangle. \quad (3.16)$$

e

$$B_n = \left\langle \sigma_1, \ldots, \sigma_n \middle| \begin{matrix} \sigma_i \cdot \sigma_j = \sigma_j \cdot \sigma_i & |i-j| \geq 2,\ 1 \leq i,j \leq n-1 \\ \sigma_i \cdot \sigma_{i+1} \cdot \sigma_i = \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1} & 1 \leq i,j \leq n-2 \end{matrix} . \right\rangle. \quad (3.17)$$

Para provar que ψ é um homomorfismo basta mostrar que toda relação de B_m é válida em B_n. Contudo, basta notar que isto é cumprido pelas apresentações de B_m e B_n acima. Agora, mostraremos que ψ é injetor, então teremos um monomorfismo.
Com efeito, suponha que temos $\beta \in B_m$ tal que $\psi(\beta) = 1_n$. Sendo assim, ao adicionar $n-m$ tranças simples obteremos uma trança equivalente a trança trivial. Formalizando a ideia, temos uma isotopia $F_i : [0,1] \times [0,1] \longrightarrow \mathbb{E}^3$ onde $\psi(\beta)$ é deformada continuamente em tranças β_i, para cada $i \in \{1, 2, \ldots, n\}$, na trança trivial 1_n. Quando removemos as $n-m$ últimas cordas da trança β_i obtemos tranças com m cordas, a saber, β_i'. Por construção, temos que $\psi(\beta_i') = 1_m$. Assim, $ker(\psi) = \{1_m\}$. □

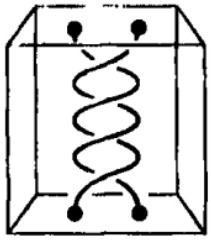
3.4 Grupo de Tranças Puras

De acordo com a Definição 3.2 temos que tranças equivalentes possuem a mesma permutação. Com isso, temos uma aplicação $\tau_n : B_n \longrightarrow S_n$, onde S_n é o grupo das permutações de n letras do conjunto $\{1, \ldots, n\}$.

Definição 3.8. Uma n-trança $\beta \in B_n$ é dita *pura* quando sua permutação é trivial.

Exemplo 3.3. A figura abaixo é uma trança pura sob 2 cordas.

Figura 3.13: 2-trança pura



Fonte: [13]

Definição 3.9. O conjunto de todas as tranças puras sobre n cordas é denotado por PB_n.

Proposição 3.3. *Seja B_n, $n \geq 1$, o grupo das tranças geométricas sob n cordas.*

i). O conjunto de todas as tranças puras sob n cordas é um subgrupo normal de B_n, ou seja, $PB_n \lhd B_n$.

ii). Existe um isomorfismo do grupo quociente B_n/PB_n no grupo das permutações S_n.

Prova: Vamos definir a aplicação

$$\begin{aligned} \tau_n : B_n &\longrightarrow S_n \\ \beta &\longmapsto \tau_n(\beta) \end{aligned} \tag{3.18}$$

onde $\tau_n(\beta)$ é a permutação de β. Veja que τ_n é um homomorfismo. Se tomarmos $\beta \in PB_n$ temos que $\tau_n(\beta) = 1$, onde 1 denota a permutação identidade, pois as tranças puras tem permutação trivial. Além disso, se tomarmos β_1 e β_1 em PB_n temos que $\tau_n(\beta_1\beta_2) = 1$. Este fato segue de que o produto de duas tranças puras ainda é uma trança pura. Logo, $ker(\tau) = PB_n$. Portanto, $PB_n \lhd B_n$. Com isso está provado $(i.)$. Veja que τ_n é sobrejetor e pelo Teorema do isomorfismo I temos que $B_n/PB_n \cong S_n$, o que demonstra o item $(ii.)$. Consequentemente temos que $(B_n : PB_n) = |B_n/PB_n| = n!$. □

Corolário 3.1. *A sequência* $1 \longrightarrow PB_n \xrightarrow{i} B_n \xrightarrow{\tau_n} S_n \longrightarrow 1$ *é exata.*

4

Uma Ordem no Grupo de Tranças B_n

Neste Capítulo, iremos mostrar que o Grupo de Tranças Artin com n cordas B_n admite uma ordem invariante à esquerda, mas não é bi-ordenável. Para isto, faremos a definição de ordem e estudaremos as propriedades de grupos ordenados e por consequências obter mais informações de propriedades algébricas de B_n. A ordenação de PB_n será tratada no Capítulo 5, pois difere grandemente da ordem que será dada em B_n,

Esse capítulo está baseado em [4], [9] e [15].

4.1 Grupos Ordenados

Nesta seção, iremos apresentar a definição de ordem e estudar os grupos ordenados. Aqui, iremos desenvolver o conceito de ordens estritas (ou linear) e invariantes por multiplicação. Todos os grupos serão escritos com a notação multiplicativa.

Definição 4.1. Uma ordem sobre um conjunto X é uma operação binária $\leq$ sobre os elementos de X satisfazendo as seguintes propriedades para todo $x, y, z \in X$.

(i.) (*Reflexividade*) $x \geq x$,

(ii.) (*Antissimetria*) $(x \geq y \text{ e } y \geq x) \Rightarrow x = y$,

(iii.) (*Transitividade*) $(x \geq y \text{ e } y \geq z) \Rightarrow x \geq z$.

Observação 4.1. Nós também escrevemos $y \leq x$ para denotar $x \geq y$. Escreveremos $x < y$ ou $y > x$ quando $x \geq y$ e $x \neq y$, neste caso $<$ é uma ordem *estrita*. É claro que não existem elementos $x, y \in X$ tais que aconteça $x < y$ e $y < x$ simultaneamente.

Definição 4.2. Uma ordem é dita ser *total* ou *linear* se para todo $x, y \in X$ temos que apenas uma das três situações ocorrem: $x = y$, $x \geq y$ ou $y \geq x$.

Definição 4.3. Sejam os pares $(X, \geq)$ e $(X', \geq')$ onde $\geq$ e $\geq'$ são uma ordem em X e X', respectivamente. Dizemos que a aplicação $f : X \longrightarrow X'$ *preserva ordem* se $x \geq y$ então $f(x) \geq' f(y)$ para todo $x, y \in X$.

Definição 4.4. Uma ordem $\geq$ sobre um grupo G é *invariante à esquerda* quando para todo $x, y, z \in G$ temos $x \geq y \Rightarrow zx \geq zy$. Analogamente, definimos uma ordem *invariante à direita*, onde $x \geq y \Rightarrow xz \geq yz$.

Definição 4.5. Uma ordem $\geq$ sobre um grupo G que é invariante à esquerda e à direita é chamada de *bi-ordenação*.

Definição 4.6. Um grupo G é *ordenável* se admite uma ordem $\geq$ invariante à esquerda ou à direita.

Observação 4.2. Note que se um grupo G admite uma ordem invariante à esquerda $\geq$ então podemos obter uma ordem invariante à direita $\leq'$ fazendo $x \leq' y \iff x^{-1} \geq y^{-1}$ para todo $x, y \in G$.

Exemplo 4.1. O conjunto dos números reais $\mathbb{R}$ é ordenável munido da ordem padrão conhecida.

Lema 4.1. *Se $G_1, \ldots, G_n$ são grupos ordenados então o produto direto deles também é ordenado.*

Prova: Seja $\geq_i$ a ordem total invariante à esquerda sobre G_i, onde $i = 1, \ldots, n$. Vamos definir a relação $\geq$ em $G = G_1 \times \ldots \times G_n$ da seguinte maneira: $(x_1, \ldots, x_n) \geq (y_1, \ldots, y_n)$ se cada $x_k = y_k$ conde $k \in \{1, \ldots, n\}$ ou existe um índice $r \in \{1, \ldots, n\}$ tal que $x_k = y_k$ quando $i < r$ e $x_r \geq_r y_r$. Claramente $\geq$ satisfaz a definição de ordem. Veremos agora que de fato a ordem é total e invariante à esquerda. Com efeito, desde que as ordens $\geq_i$ sobre G_i são totais então $\geq$ também é total. Sejam

$$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \; e \; z = (z_1, \ldots, z_n)$$

elementos de G. Se $x < y$ então existe um $r \in \{1, \ldots, n\}$ tal que $x_i = y_i$ quando $i < r$ e $x_r \geq_r y_r$. Consequentemente $z_i x_i = z_i y_i$ quando $i < r$ e $z_r x_r \geq_r z_r y_r$. □

Lema 4.2. *Seja G um grupo e H um subgrupo normal de G. Se H e G/H tem uma ordem total invariante à esquerda então a inclusão $i : H \longrightarrow G$ e a projeção canônica $\pi : G \longrightarrow G/H$ preserva ordem. Além disso, se a ordem total invariante à esquerda sobre H e G/H são bi-invariante e $zxz^{-1} > 1$ para todo $z \in G$ e $x \in H$ com $x > 1$ então a ordem invariante à esquerda associada a G é bi-invariante.*

Prova: Denotemos por $\geq_{G/H}$ e $\geq_H$ as ordens totais invariantes à esquerda de G/H e H, respectivamente. Vamos definir $\geq_G$ em G de forma que dados $x, y \in G$ temos $x \geq_G y$ se $\pi(x) <_{G/H} \pi(y)$ ou $\pi(x) = \pi(y)$ e $x^{-1}y > 1$. Observe que $x^{-}1y \in H$. De fato, $\geq_G$ é invariante à direita, pois $\pi(xz) = \pi(x)\pi(z) \geq_{G/H} \pi(yz) = \pi(y)\pi(z)$, $z \in G$. Além disso, $\pi(xz) = \pi(x)\pi(z) = \pi(y)\pi(z) = \pi(yz)$. Como, por hipótese, a conjugação por um elemento de H é positiva temos que $(xz)^{-1}(yz) = z^{-1}(x^{-1}y)z \geq_G 1$. Portanto $xz \leq_G yz$. □

Observação 4.3. Pelo Lema 4.1 e a ordenabilidade de $\mathbb{R}$ temos que todo espaço vetorial real de dimensão finita e seus subgrupos aditivos são ordenados. Nem todo grupo é ordenado.

Definição 4.7. Para um subconjunto $\mathcal{P}$ de um grupo G definiremos os conjuntos $\mathcal{P}^{-1} = \{x \in G \mid x^{-1} \in \mathcal{P}\}$ e $\mathcal{P}^2 = \{z \in G \mid existem\ x, y \in G\ tais\ que\ z = xy\}$.

Lema 4.3. *Para qualquer subconjunto $\mathcal{P}$ de um grupo G temos que*

$$\mathcal{P} \cap \mathcal{P}^{-1} = \varnothing \Leftrightarrow \mathcal{P} \cap \{1\} \neq \varnothing \Leftarrow \mathcal{P} \cap \{1\} = \varnothing.$$

Se $\mathcal{P}^2 \subset \mathcal{P}$ então $\mathcal{P} \cap \{1\} = \varnothing \Rightarrow \mathcal{P} \cap \mathcal{P}^{-1} = \varnothing$.

Prova: Se $1 \in \mathcal{P}$ então $1 = 1^{-1} \in \mathcal{P}^{-1}$. Consequentemente, $\mathcal{P}^{-1} \cap \{1\} = \varnothing \Rightarrow \mathcal{P} \cap \{1\} = \varnothing$. Substituindo $\mathcal{P}$ por $\mathcal{P}^{-1}$ nós provamos a recíproca.

Para provar que $\mathcal{P} \cap \mathcal{P}^{-1} = \varnothing \Rightarrow \mathcal{P} \cap \{1\} = \varnothing$ nós suponhamos que $\mathcal{P} \cap \{1\} \neq \varnothing$ e concluiremos que $\mathcal{P} \cap \mathcal{P}^{-1} \neq \varnothing$. Com efeito, se $\mathcal{P} \cap \{1\} \neq \varnothing$ então $1 \in \mathcal{P}$ e $1 \in \mathcal{P}^{-1}$ o que resulta em $\mathcal{P} \cap \mathcal{P}^{-1} \neq \varnothing$.

Em fim, vamos provar a última afirmação. Suponha que $\mathcal{P} \cap \mathcal{P}^{-1} \neq \varnothing$. Seja $x \in \mathcal{P} \cap \mathcal{P}^{-1}$ então $x^{-1} \in \mathcal{P} \cap \mathcal{P}^{-1}$. Consequentemente,

$$1 = xx^{-1} \in \mathcal{P}^2 \subset \mathcal{P}.$$

Portanto, $\mathcal{P} \cap \{1\} \neq \varnothing$. □

Lema 4.4. *Seja $\geq$ uma ordem invariante à esquerda sobre um grupo G. Seja o conjunto*

$$\mathcal{P} = \{x \in G \mid x > 1\}.$$

Então $\mathcal{P}^{-1} = \{x \in G \mid x < 1\}$,$\mathcal{P}^2 \subset \mathcal{P}$ e

$$\mathcal{P} \cap \{1\} = \mathcal{P}^{-1} \cap \{1\} = \mathcal{P} \cap \mathcal{P}^{-1} = \varnothing.$$

Se a ordem $\geq$ é total então $G = \mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\}$.

Prova: Se $x \in \mathcal{P}^{-1}$ então $x^{-1}\mathcal{P}$ desde que $1 < x^{-1}$. Multiplicando por x à esquerda nós obtemos $x < 1$. Similarmente, $x < 1$ implica que $1 = x^{-1}x < x^{-1}1 = x^{-1}$ desde que $x^{-1} \in \mathcal{P}$ e $x \in \mathcal{P}^{-1}$. Isto prova que $\mathcal{P}^{-1}$.

A propriedade de antissimetria de uma ordem implica que $\mathcal{P}$ e $\mathcal{P}^{-1} = \{x \in G \mid x < 1\}$ são disjuntos. E pela definição de $<$ temos que $\mathcal{P}$ e $\mathcal{P}^{-1}$ são distintos com $\{1\}$.

Se $x, y \in \mathcal{P}$ então $xy > x1 = x > 1$, com $xy \in \mathcal{P}$. Portanto $\mathcal{P}^2 \subset \mathcal{P}$.

Se a ordem *geq* é total então para cada $x \in G$, necessariamente, temos $x > 1$ ou $x = 1$ ou $x < 1$. Concluímos então que $G = \mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\}$. □

Definição 4.8. O subconjunto $\mathcal{P} = \{x > 1 \mid x \in G\}$ de um grupo G definido no Lema 4.4 é chamado de *cone positivo* associado a ordem $\geq$. Os elementos de G que pertencem a $\mathcal{P}$ são ditos serem *positivos* com respeito a $\geq$.

Veremos que uma ordem total invariante à esquerda $\geq$ sobre um grupo G pode ser reconstruída pelo cone positivo.

Teorema 4.1. *Seja $\mathcal{P}$ um subconjunto de um grupo G tal que $\mathcal{P}^2 \subset \mathcal{P}$ e $1 \notin \mathcal{P}$. Então G possui uma única ordem $\geq$ invariante à esquerda tal que $\mathcal{P} = \{x \in G \mid x > 1\}$. Se $z\mathcal{P}z^{-1} \subset \mathcal{P}$ então a ordem é bi-invariante. Se $\mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\} = G$ então a ordem é total.*

Prova: Seja $\mathcal{P}^2 \subset \mathcal{P}$ e $1 \notin \mathcal{P}$. Então pelo Lema 4.4 temos que

$$\mathcal{P} \cap \mathcal{P}^{-1} \cap \{1\} = \varnothing.$$

Daí, dados $x, y \in G$ definiremos $\geq$ tal que $x \geq y \Leftrightarrow x = y$ ou $x^{-1}y \in \mathcal{P}$. A reflexividade é imediata. Para verificar a antissimetria note que se $x \geq y$ e y então $x = y$ ou $x^{-1}y \in \mathcal{P}$ e $y^{-1}x \in \mathcal{P}$. Como $y^{-1}x = (x^{-1}y)^{-1}$ então $x^{-1}y \in \mathcal{P} \cap \mathcal{P}^{-1} = \varnothing$. Por fim, a transitividade se verifica observando que se $x^{-1}y, y^{-1}z \in \mathcal{P}$ então $x^{-1}z = x^{-1}yy^{-1}z \in \mathcal{P}^2 \subset \mathcal{P}$.

Agora vamos mostrar que a ordem $\geq$ é invariante á esquerda. Sejam $x, y \in G$ tais que $x \geq y$. Então $x = y$ ou $x^{-1}y \in \mathcal{P}$. Se $x = y$ então $zx = zy$ para todo $z \in G$. No segundo caso, se $x^{-1}y \in \mathcal{P}$ então $(zx)^{-1}(zy) = x^{-1}y \in \mathcal{P}$. Em ambos os casos $zx \geq zy$.

Vamos assumir que $z\mathcal{P}^{-1} \subset \mathcal{P}$, para todo $z \in G$. Então dados $x, y \in G$ se $x \geq y$ então $x = y$ ou $x^{-1}y \in \mathcal{P}$. Se $x = y$ então $zx = zy$ para todo $z \in G$. Se $x^{-1}y \in \mathcal{P}$ e $z \in G$ então $(xz)^{-1}(yz) = z^{-1}(x^{-1}y)z$ pertence a $z\mathcal{P}z^{-1}$ e consequentemente a $\mathcal{P}$. Logo, temos que $\geq$ é invariante à direita.

Por fim, se $\mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\} = G$ então para cada $x, y \in G$ temos que $x^{-1}y \in \mathcal{P}$ ou $x^{-1}y \in \mathcal{P}^{-1}$. No primeiro caso temos $x < y$ e no segundo caso temos $y^{-1}x = (x^{-1}y)^{-1} \in \mathcal{P}$ desde que $y < x$. O último caso seria $x = y$. Portanto, a ordem $\geq$ é total. □

4.1.1 Propriedade dos Grupos Ordenados

Proposição 4.1. *Todo grupo ordenado G é livre de torsão.*

Prova: Nós temos de mostrar que $x^n \neq 1$ para todo $n \in \mathbb{Z}$ e todo elemento $x \in G$ diferente de 1. Com efeito, suponha $x > 1$. Então pela invariância à esquerda temos

$$x^n = x^{n-1}x > x^{n-1}1 = x^{n-1}$$

para todo $n > 1$. Por indução, $x^n > x > 1$; consequentemente $x^n \neq 1$. Se $x < 1$, então $x^{-1} > 1$ e $x^{-n} = (x^{-1})^n \neq 1$. Portanto $x^n \neq 1$.

Definição 4.9. Sejam G um grupo e R um anel. O *anel de grupo* $R[G]$ é o conjunto de todas as expressões da forma $w = \sum_{g\in G} a_g g$ onde $a_g \in R$ e somente um número finito de a_g são não-nulos, com operações definidas por

$$\begin{aligned} w + w' &= \big(\sum_{g\in G} a_g g\big) + \big(\sum_{g\in G} b_g g\big) = \sum_{g\in G}(a_g + b_g)g \\ ww' &= \big(\sum_{g\in G} a_g g\big)\big(\sum_{h\in G} b_h h\big) = \sum_{g\in G}\sum_{h\in G}(a_g b_h)gh \end{aligned}$$

Proposição 4.2. *Se $(G, \geq)$ é um grupo ordenável e R é um anel sem divisores de 0 então o anel de grupo sobre R, $R[G]$, não tem divisores de 0.*

Prova: Sejam $w = \sum_{i=1}^{p} r_i g_i$ e $w' = \sum_{j=1}^{q} s_j h_j$ elementos não nulos de $R[G]$. Podemos supor que $h_1 < h_2 < \ldots < h_q$. Temos que

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

Pela invariância à esquerda da ordem $g_i h_i < g_i h_j$ para todo $i = 1, \ldots, p$ e $j = 2, \ldots, q$. Pela totalidade da ordem podemos encontrar um índice i_0 tal que $g_{i_0} h_1 < g_i h_1$ para $i \neq i_0$.

Afirmação: $(i_0, 1)$ é o único par (i, j) tal que $g_{i_0} h_i = g_i h_j$ em G.

De fato, observe que $g_{i_0} h_i < g_{i_0} h_j$ para todo $j \neq 1$ e se $i \neq i_0$ então $g_0 h_i < g_i h_1 < g_i h_j$. Portanto, o coeficiente de $g_{i_0} h_1$ em $ww' \in R[G]$ é $r_{i_0} s_1$, não nulo. Consequentemente, $ww \neq 0$. □

Definição 4.10. Um grupo G é *bi-ordenado* quando possui uma ordem total bi-invariante.

Exemplo 4.2. Todo grupo abeliano é bi-ordenável. Basta notar que toda ordem invariante à esquerda de um grupo abeliano é necessariamente bi-invariante.

Lema 4.5. *Grupos bi-ordenados possuem raízes únicas, ou seja, se dados $x, y \in G$ tivermos $x^n = y^n$, para algum inteiro n, então $x = y$.*

Prova: Observe que num grupo bi-ordenado se $x < y$ e $x' < y'$ implica que $xx' < yy'$. Como G é invariante à direita temos $xx' < yx'$. Mas também é invariante à esquerda, logo $yx' < yy'$. Pela transitividade de $\geq$ obtemos $xx' < yy'$. Por indução temos que $x < y$ então $x^n < y^n$.

Agora, suponhamos que dados $x, y \in G$ tenhamos $x^n = y^n$. Como a ordem $\geq$ é total então $x = y$ ou $x < y$ ou $y < x$. Os dois últimos casos são descartados, restando apenas $x = y$. □

4.2 A σ-ordenação de B_n

Nesta seção, mostraremos que o grupo de tranças Artin B_n não é bi-ordenável, mas pode ser ordenado por uma ordem total invariante à esquerda mediante uma construção chamada de *ordenação Dehornoy*. Para isto, iremos definir quando uma palavra trança w é σ-positiva ou σ-negativa.

Proposição 4.3. *Para $n \geq 3$, o grupo B_n não é bi-ordenável.*

Prova: Basta observar que os elementos $\sigma_1\sigma_2$ e $\sigma_2\sigma_1$ de B_n são distintos, mas satisfazem $(\sigma_1\sigma_2)^3 = (\sigma_2\sigma_1)^3$ o que contradiz o Lema 4.5. □

Definição 4.11. Uma palavra trança w é uma palavra sobre o conjunto

$$\{\sigma_1, \ldots, \sigma_n, \sigma_1^{-1}, \ldots, \sigma_n^{-1}\}.$$

Pelo Teorema da Apresentação de Artin toda palavra trança w representa um elemento de B_n. A palavra vazia representa o elemento neutro 1 de B_n

Definição 4.12. A inversa de uma palavra trança $w = \sigma_1^{\varepsilon_1} \ldots \sigma_r^{\varepsilon_r}$ não vazia é a palavra trança $w^{-1} = \sigma_r^{-r} \ldots \sigma_1^{-1}$.

Definição 4.13. Nós definimos *índice* de uma palavra trança w não vazia como o menor inteiro $i \in \{1, \ldots, n-1\}$ tal que σ_i ou σ_i^{-1} aparece em w.

Definição 4.14. Uma palavra trança não vazia $w = \sigma_{i_1}^{\varepsilon_1} \ldots \sigma_{i_n}^{\varepsilon_n}$ é dita ser *σ_i-positiva*, onde $\varepsilon_k \in \{\pm 1\}$ e $i_k \in \{1, \ldots, n-1\}$ para todo $k \in \{1, \ldots, n-1\}$, se ela possui índice i e σ_i^{-1} não aparece em w. Dizemos que a palavra trança é σ_i-negativa se sua inversa é σ_i-positiva.

Definição 4.15. Uma palavra trança é σ-positiva (respec. σ-negativa) se for σ_i-positiva (σ_i-negativa) para alguma $i \in \{1, \ldots, n\}$.

Definição 4.16. Um elemento β de B_n é σ-positivo (respc. negativo) se é σ_i-positivo (respec. σ-negativo).

Exemplo 4.3. Os geradores $\{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ de B_n são claramente σ-positivos.

Observação 4.4. Nem toda palavra trança representada por elementos σ-positivos de B_n é σ-positiva. De fato, tome a palavra trança $w = \sigma_1\sigma_2(\sigma_1^{-1})^N$, onde $n \geq 1$. Veja que o índice de w é 1, mas w não é σ-positiva e nem σ-negativa. Mesmo assim, representa uma σ-trança positiva $\beta \in B_n$. Fazendo de maneira análoga $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$ temos que $\sigma_2^N\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1^N$, para todo $N \geq 1$. Multiplicando 'à esquerda ambos os lados por σ_2^{-N} obtemos $\sigma_1\sigma_2 = \sigma_2^{-N}\sigma_2\sigma_1^N$. A palavra $\sigma_1\sigma_2$ representa uma trança σ-positiva, portanto β é σ-positiva.

Seja $\mathcal{P}$ o subconjunto de B_n que contém todas as tranças σ-positivas.

Lema 4.6. *O subconjunto de B_n consistindo de todas as tranças σ-negativas é $\mathcal{P}^{-1}$ e $\mathcal{P}^2 \subset \mathcal{P}$.*

Prova: Se β é um elemento σ-netgativo de B_n então é representado por uma palavra trança w que é σ-negativa. Sabemos, por definição, que w^{-1} é σ-positiva. Como $\beta^{-1} \in B_n$ então $\beta^{-1} \in \mathcal{P}$. Ou seja, $\beta \in \mathcal{P}^{-1}$. De maneira análoga provamos a outra inclusão. Agora, sejam $\beta_1, \beta_2 \in \mathcal{P}$. Por definição, tais tranças podem ser representadas, onde $i, j \in \mathbb{Z}$, por σ_i-palavra w_1 e σ_j-palavra w_2, respectivamente. Se $i < j$ então a palavra trança $w_1 w_2$ será σ_j-positiva. Caso contrário, temaremos $w_1 w_2$ uma palavra trança σ_i-positiva, ou seja, $\beta_1\beta_2$ sempre representa uma σ-trança positiva em B_n. Logo, $\mathcal{P}^2 \subset \mathcal{P}$. □

4.2.1 Definição da Ordem de Dehornoy

Essa seção contém um dos principais resultados desta monografia, pois mostraremos que B_n possui uma ordem total invariante à esquerda.

Lema 4.7. $1 \notin \mathcal{P}$.

Lema 4.8. *Todo elemento $\beta \in B_n$, distinto de 1, é σ-positivo ou σ-negativo. Em outras palavras, $\mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\} = B_n$.*

Teorema 4.2. *Para todo $n \geq 1$ o grupo de tranças Artin B_n admite uma ordem $\geq$ total invariante à esquerda tal que $1 \leq \beta$ se, e somente se, β é σ-positiva.*

Prova: Para todo $\beta, \gamma \in B_n$, $\beta \geq \gamma$ se $\beta = \gamma$ ou $\beta^{-1}\gamma \in \mathcal{P}$. Então pelo Teorema 4.1 temos que B_n é ordenado. □

Observação 4.5. Observe que pela Proposição 4.2 e pelo Teorema 4.1 temos que $Z[B_n]$ é um anel sem divisores de zero e que B_n é livre de torsão. Além disso, quando $n = 2$ temos que $B_n \cong \mathbb{Z}$ e a ordem de Dehernoy coincide com ardem natural dos inteiros.

Observação 4.6. A σ-ordenação de B_n não é invariante à direita. De fato, tome $\beta_1 = \sigma_1\sigma_2^{-1}$ e $\beta_2 = \sigma_1\sigma_2\sigma_1$ elementos de B_n. Como β_1 é σ_1-positiva então será σ-positiva. Agora, observe que

$$\beta_2^{-1}\beta_1\beta_2 = (\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1})(\sigma_1\sigma_2^{-1})(\sigma_1\sigma_2\sigma_1) = \sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2\sigma_1^{-1}$$

Claramente, $\beta_2^{-1}\beta_1\beta_2 = \sigma_2\sigma_1^{-1}$ é σ_1-negativa, ou seja, é σ-negativa. Logo, $\beta_1\beta_2 < \beta_2$.

4.2.2 Propriedades

Vamos discutir algumas propriedades que são consequências da σ-ordenação de Dehornoy em B_n.

Para a ordenação de Dehernoy vale

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

Proposição 4.4. *(a) σ_{n-1} é o menor elemento σ-positivo de B_n. (b) B_n não admite elementos mínimo e máximo.*

Prova: (a) Suponha que exista um elemento $\beta \in \mathcal{P}$ tal que $\beta < \sigma_{n-1}$. Equivalentemente $\beta^{-1}\sigma_{n-1} \in \mathcal{P}$. Seja w a palavra trança σ_i-positiva representante de β. Consequentemente 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_i-negativa o que é uma contradição. Portanto, $i = n-1$ implica $w = (\sigma_{n-1})^r$ para cada inteiro $r \geq 1$. Então se $r = 1$ temos $\beta^{-1}\sigma_{n-1} = 1$ e se $r > 1$, $\beta^{-1}\sigma_{n-1}$ estará contido em $\mathcal{P}$. Ainda assim obtemos contradições. Portanto, não existe elemento $\beta \in B_n$ que satisfaz $\beta < \sigma_{n-1}$.
(b) Como $\sigma_1 > 1 > \sigma_1^{-1}$ a invariância à esquerda da ordem implica que para todo $\beta \in B_n$ temos $\beta\sigma_1 > \beta > \beta\sigma_1^{-1}$. Logo, B_n não admite elementos maximal e minimal. □

Lema 4.9. *A inclusão $i : B_n \hookrightarrow B_\infty$ preserva ordem com respeito a ordem de Dehornoy, que é,*

$$\beta \geq \beta' \Rightarrow i(\beta) \geq_{n+1} i(\beta')$$

para todo $\beta, \beta' \in B_n$.

Seja $B_\infty = \bigcup_{n\geq 1} B_n$ o limite indutivo dos grupos B_n com respeito a inclusão i. Por definição, todo elemento de B_∞ está contido em algum dos conjuntos B_n. A estrutura de grupo de B_n se extende naturalmente à B_∞.

O lema a seguir fornecerá um caminho para demonstrarmos a próxima proposição e conluir que B_∞ é isomorfo a $\mathbb{Q}$ como conjuntos ordenados.

Lema 4.10. *(Cantor) Seja $(G, \geq)$ um conjunto ordenado não vazio e enumerável. Se (i) para todo $g \in G$ existir um $h \in G$ tal que $g < h$; (ii) para todo $g \in G$ existir um $h \in G$ tal que $h < g$ e (iii) para todo $g, h \in G$ existir um $k \in G$ tal que se $g < h$ implica $g < k < h$ então $(G, \geq)$ é isomorfo, como conjunto ordenado, ao conjunto dos números racionais $\mathbb{Q}$.*

Proposição 4.5. *Existe uma única ordem total invariante à esquerda em B_∞ tal que as inclusões $i : B_n \hookrightarrow B_\infty$ preserva ordem. Além disso, B_∞ é isomorfo ao conjunto dos racionais $\mathbb{Q}$ como conjuntos ordenados.*

Prova: (a) Sejam $\beta, \beta' \in B_\infty$. Por definição, existe um n tal que $\beta, \beta' \in B_n$. Façamos $\beta \leq_\infty \beta'$ se $\beta \leq_n \beta'$. Por construção temos que $\leq_\infty$ é a única ordem total invaiante à

esquerda sobre B_∞ e que a inclusão $i : B_n \hookrightarrow B_\infty$ preserva a ordem.
Como qualquer grupo gerado por um conjunto enumerável de geradores é enumerável temos que B_∞ é enumerável.
Se temos um elemento β máximo (resp. mínimo) em B_∞ então β também será um elemento máximo (resp. mínimo) de B_n, onde n é o índice do grupo de trança ao qual β pertence. Mas isso é uma contradição pela Proposição 4.4.
Enfim, para provarmos a última afirmação, basta observarmos que para todo $\beta \in B_\infty$ tal que $1 < \beta$ existe um α tal que $1 < \alpha < \beta$. De fato, para $\beta \in B_\infty$ tome $\alpha = i(\beta)\sigma_n^{-1} \in B_{n+1}$. Desde que o índice da palavra trança σ-positiva representante de β é $i < n$ a trança α é σ-positiva. Portanto, $1 < \alpha$ sobre B_{n+1} consequentemente sobre B_∞. Por outro lado $\alpha^{-1}\beta = \alpha_n$ em B_∞, ou seja, $\alpha^{-1}\beta$ é σ-positiva. Logo, $\alpha < \beta$ e o resultado segue do Lema de Cantor. □

5

A Bi-Ordenação de PB_n

Neste capítulo concluímos o estudo da ordenabilidade do Grupo de Tranças de Artin. Mostraremos que o grupo de tranças puras sobre n cordas, a saber PB_n, é bi-ordenável. A ordem que será definina no grupo de tranças puras será totalmente diferente da ordem definida em B_n. Para isto, iremos estudar a ordem de Magnus onde teremos que os grupos livres são bi-ordenáveis e que o produto semidireto de tais grupos também pode ser bi-ordenável via a ordenação lexicográfica apresentada anteriormente. O resultado será concluído provando que PB_n é isomorfo a um produto semidireto de grupos livres chamada *sequência normal de Artin*.

As referências desse capítulo são [4] [9], [12] e [15].

5.1 A Expansão de Magnus

Definição 5.1. Fixemos um conjunto finito não vazio $X = \{X_1, \ldots, X_2\}$ e seja $M(X) = M(X_1, \ldots, X_n)$ o monoide livre sobre X. Chamamos de *série formal de potências* sobre X a soma

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

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

Agora, vamos denotar por $\mathbb{Z}[[X]]$ o conjunto de todas as séries de potências formais sobre X. Dados dois elementos quaisquer $a = \sum_{U \in M(X)} f_U U$ e $b = \sum_{V \in M(X)} g_V V$ em $\mathbb{Z}[[X]]$ defina $a + b$ como a soma de cada coeficiente da mesma palavra. O produto $a.b$ é dado por

$$\left(\sum_{U \in M(X)} f_U U \right) \left(\sum_{V \in M(X)} g_V V \right) = \sum_{W} \left(\sum_{W = UV} f_U g_V \right) W.$$

Claramente, $\mathbb{Z}[[X]]$ é um grupo aditivo abeliano munido da soma definida. Já munido com o produto temos então um anel com unidade $1 \in \mathbb{Z}[[X]]$.

Definição 5.2. O conjunto $\mathbb{Z}[[X]]$ munido das operações de soma e produto definidas acima possui estrutura de anel e é chamado de *anel não-comutativo de séries formais em n indeterminadas X*

Definição 5.3. O comprimento de uma palavra W é chamado o *grau* do monômio $f_W W$. Nós dizemos que uma a série formal de potências $a = \sum_{W \in M(X)} f_W W \in \mathbb{Z}[[X]]$ tem grau $\geq r$, onde r é um inteiro positivo, se $f_W = 0$ para todo $W \in M(X)$ com $l(W) < r$.

Observação 5.1. Claramente, o produto de duas séries formais de potências $a.b$ com grau $\geq r$ e $\geq s$, respectivamente, resulta numa série de potência formal cujo grau é $\geq r + s$.

Observação 5.2. Para cada série formal de potência $a = \sum_{W \in M(X)} f_W W$, seja $\varepsilon(a) = n_1 \in \mathbb{Z}$ o coeficiente do elemento neutro $1 \in \mathbb{Z}[[X]]$. É de fácil verificação mostrar que a é invertível em $\mathbb{Z}[[\mathbb{X}]]$ se, e somente se, $\varepsilon(a) = \pm 1$. Por enquanto, para todo $x \in X$, $1 + x \in \mathbb{Z}[[X]]$ é invertível e seu inverso será a série formal de potência $\sum_{k \geq 0} (-1)^k x^k$.

Lema 5.1. *Para cada $x \in X$ e $k \in \mathbb{Z}$ existe uma série de potências formal $h_k(x)$ na variável x tal que*

$$(1 + x)^k = 1 + kx + x^2 h_k(x).$$

Definição 5.4. Denotaremos por $\mathcal{O}(k)$ o ideal de $\mathbb{Z}[[X]]$ formado pelas séries formais de potências de graus maior ou igual a k. Denotaremos por $o(k)$ os elementos de $\mathcal{O}(k)$.

Proposição 5.1. *Seja $\mathcal{G} = \{1 + o(1)\}$ o subconjunto de $\mathbb{Z}[[X]]$ formada pelas séries de potências com termo constante igual a 1. Então $\mathcal{G}$ é um subgrupo de $\mathbb{Z}[[X]]$ munido da operação de multiplicação.*

Prova: A associatividade e o fato de o elemento identidade $1+0x$ de $\mathbb{Z}[[X]]$ está em $\mathcal{G}$ são resultados imediatos. Quanto a existência do elemento inverso de $a = 1+h$, onde h é uma série formal envolvendo apenas monômios de grau ≥ 1, temos que $a^{-1} = 1-h+h^2-h^3+\ldots$. De fato, $a.a^{-1} = (1+h)(1-h+h^2-h^3+\ldots) = (1-h+h^2-h^3+\ldots+(-1)^n h^n+\ldots)+(h-h^2+h^3+\ldots+(-1)^n h^n+\ldots) = 1$. □

Proposição 5.2. *Seja F um grupo livre sobre X. O homomorfismo de grupos $\mu : F \longrightarrow \mathcal{G}$ definido por $\mu(x) = 1 + x$ é único para todo $x \in X$ e é injetor.*

Prova: A existência e unicidade de μ segue da definição de F. Quanto a demonstração da injetividade, tomemos um elemento w em F não trivial e escreva-o na forma

$$w = x_1^{k_1} \ldots x_r^{k_r},$$

onde $x_1^{k_1}, \ldots, x_n^{k_n} \in X$ satisfazendo $x_1 \neq x_2, x_2 \neq x_3, \ldots, x_{r-1} \neq x_r$, e os inteiros $k_1, \ldots, k_n$

são diferentes de 0. Então

$$\begin{aligned}\mu(w) &= (1+x_1)^{k_1}(1+x_2)^{k_2}\cdots(1+x_r)^{k_r}\\ &= (1+k_1x_1+x_1^2h_{k1}((x_1))(1+x_2k_2+x_2^2h_{k_2}(x_2)\\ \ldots &\ (1+k_rx_r+k_r^2k_{k_2}(x_r))\end{aligned}$$

Expandindo a série formal de potência do lado direito veremos que existe um único monômio da forma x_{1r}. O coeficiente deste monômio é $k_2k_{2r} > 0$. Consequentemente, $\mu(w) \neq 1$. □

Definição 5.5. A série formal de potência $\mu(w)$ definida na Proposição 5.2 é chamada de *expansão de Magnus* de F relativa a base X.

Exemplo 5.1. Para $w = x_1^{-1}x_2x_1$ nós obtemos

$$\begin{aligned}\mu(w) &= (1-X_2+X_1^2-X_1^3+\cdots)(1+X_2)(1+X_1),\\ &= 1+X_2-X1X_2+X_2X_1+X_1^2X_2-X_1X_2X_1\ mod\ \mathcal{O}(X^4).\end{aligned}$$

5.2 Grupos livres são bi-ordenáveis

Proposição 5.3. *Seja F o grupo livre gerado por X. Toda ordem total $\leq$ sobre X se estende para uma ordem total bi-invariante sobre F.*

Prova: Primeiramente, afirmamos que uma ordem total sobre X induz uma ordem $\geq$ sobre $M(X)$. De fato,

(i) Sobre $X \subset M(X)$, definiremos uma ordem $\leq_{M(X)}$ fazendo $x \leq_{M(X)} y$ se, e somente se, $x \leq y$.

(ii) Dados $W_1, W_2 \in M(X)$ satisfazendo $l(W_1) \leq l(W_2)$ então diremos que $W_1 \leq W_2$.

(iii) Se W_1 e W_2 em $M(X)$ tem o mesmo comprimento então nós ordenamos lexicograficamente da seguinte forma: Se $W_1 = x_1\cdots x_r$ e $W_2 = y_1\cdots y$ com $x_i, y_i \in X$, para todo i, então $W_1 \leq W_2$ desde que exista $k \leq r$ tal que $x_k \leq y_k$ e $x_i = y_i$ para todo $i \leq k$.

A ordem $\leq_{M(X)}$ é bi-invariante e total. Veja que $W_1 < W_2$ implica $WW_1 < WW_2$ e $W_1W < W_2W$ para todo $W \in M(X)$.
Pela Proposição 5.2, se $w \in F$ é um elemento distinto do elemento neutro 1 então $\mu(w) \neq 1$ em $\mathbb{Z}[[X]]$. Escreva

$$\mu(w) - 1 = \sum_W f_W W, \tag{5.1}$$

onde W não são palavras vazias em $M(X)$ e f_W são inteiros diferentes de 0.
Uma das palavras $V(w)$ é a menor dentre as palavras que aparecem na expansão $\mu(w)-1$ onde denotemos $f(w) = f_{V(w)} \neq 0$. Finalmente, definimos

$$\mathcal{P} = \{w \in F - \{1\} \mid f(w) > 0\}. \tag{5.2}$$

Claramente, um elemento $w \in F - \{1\}$ encontra-se em $\mathcal{P}$ se, e somente se, $\mu(w)$ é da forma

$$1 + f(w)V + \sum_{W>V} f_W W, \tag{5.3}$$

onde $V \neq 1$ e $f(w) > 0$.
Se tivermos um conjunto $\mathcal{P}$ conforme dado no Lema 4.4 então teremos definida uma ordem vi-invariante para F. Resulta das definições que $1 \notin \mathcal{P}$. Mostraremos agora que $\mathcal{P}^2 \subset \mathcal{P}$. Considere dois elementos $w, w' \in \mathcal{P}$ e suas respectivas extensões de Magnus

$$\mu(w) = 1 + f(w)V + \sum_{W>V} f_W W \tag{5.4}$$

e

$$\mu(w') = 1 + f(w')V' + \sum_{W>V'} f'_W W \tag{5.5}$$

onde $f(w) > 0$ e $f(w') > 0$. Expandindo $\mu(ww') = \mu(w)\mu(w')$ e sendo a ordem em $M(X)$ bi-invariante obtemos

$$f(ww') = \begin{cases} f(w), & V < V' \\ f(w'), & V > V' \\ f(w) + f(w'), & V = V' \end{cases} \tag{5.6}$$

Em todos os casos teremos $f(ww') > 0$, ou seja, $ww' \in \mathcal{P}$.
Claramente, $\mu(w^{-1}) = (\mu(w))^{-1}$ e $\mathcal{P}^{-1} = \{w \in F - \{1\} \mid f(w) < 0\}$. Pela injetividade de μ obtemos $\mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\} = F$.
Resta verificar que $w\mathcal{P}w^{-1} \subset \mathcal{P}$ para todo $w \in F$. Se $n \in \mathbb{Z}[[X]]$ é uma série de potências formal sem termo constante, ou seja, $n \in \mathcal{O}(1)$, então

$$(1+n)W(1+n)^{-1} = W + \sum_{W'>W} m_{W'} W' \tag{5.7}$$

para todo inteiro $m_{W'}$. Isto implica que

$$f(ww'w^{-1}) = f(w),$$

para todo $w, w' \in F - \{1\}$. Portanto, $w\mathcal{P}w^{-1} \subset \mathcal{P}$ para todo $w \in F$. □

Corolário 5.1. *Todo grupo livre é bi-ordenável.*

□

5.3 Ordenando o Grupo de Tranças Puras

Vimos neste trabalho que o produto direto $G \times H$ da Definição 1.20 de dois grupos bi-ordenados também é bi-ordenado mediante a definição de ordem lexicográfica apresentada no Lema 4.1. Veremos que no caso do produto semidireto esta afirmação nem sempre é verdadeira. Para ordenar o produto semidireto e concluir a bi-ordenabilidade do PB_n iremos recorrer também a ordem lexicográfico de uma forma diferente.

Definição 5.6. Seja $G \ltimes H$ o produto semidireto dos grupos bi-ordenados $(G, \leq_G)$ e $(H, \leq_H)$. Dados $hg, h'g' \in G \ltimes H$,

$$hg < h'g' \Leftrightarrow g <_G g' \text{ ou } g = g' \text{ e } h <_H h.$$

Proposição 5.4. *Sejam $(G, \leq_G)$ e $(H, \leq_H)$ grupos bi-ordenáveis. O produto semidireto $G \ltimes H$ é bi-ordenável se, e somente se, $g^{-1}\mathcal{P}_H g \subset \mathcal{P}_H$ para todo $g \in G$.*

Prova: ($\Rightarrow$) Seja $h \in \mathcal{P}_H$. Claramente, $(h, 1) \in \mathcal{P}_{G \ltimes H}$ e temos também

$$(1, g)(h, 1)(1, g^{-1}) = (h^g, 1).$$

Pela bi-ordenabilidade de $G \ltimes H$ temos que $(h^g, 1) \in \mathcal{P}_{G \ltimes H}$, ou seja, $(1, 1) < (h^g, 1)$. Portanto $1 <_H h^g$ o que implica $h^g \in \mathcal{P}_H$.
($\Leftarrow$) Temos que $g^{-1}\mathcal{P}_H g \subset \mathcal{P}$, para todo $g \in G$. Vamos mostrar que conseguimos verificar as hipóteses do Teorema 4.1.
Veja que dados $(h_1, g_1), (h_2, g_2) \in G \ltimes H$ elementos positivos então se g_1 ou g_2 são diferentes de 1_G então $g_1 g_2 > 1_G$. Note também que se $g_1 = g_2 = 1_G$ então $h_1 h_2 = h_1 g_1^{-1} h_2 g = h_1 h_2 > 1_H$. Com isso concluímos que $(h_1 g^{-1} h_2 g_1, g_1 g_2) = (h_1 h_2^g, g_1 g_2) = (h_1, g_1)(h_2, g_2) > 1$, ou seja, o cone $\mathcal{P}_{G \ltimes H}$ é fechado em relação à multiplicação.
A hipótese da bi-ordenabilidade dos grupos G e H nos permitem concluir que os elementos de $G \ltimes H$ serão exclusimante positivos ou negativos ou a identidade.
Afirmação: o cone $\mathcal{P}_{G \ltimes H}$ é fechado para a conjugação por qualquer elemento $(a, b) \in G \ltimes H$. Com efeito, tomando $(h, g) \in \mathcal{P}_{G \ltimes H}$ então

$$\begin{aligned} (a, b)(h, g)(a, b)^{-1} &= (a, b)(h, q)((a^{-1})^{-b}, b^{-1}) \\ &= (ah^b((a^{-1})^{-b})^{bg}, bgb^{-1}) = (ah^b(a^{-1})^g, bgb^{-1}). \end{aligned} \tag{5.8}$$

Tanto para $g = 1_G$ como $g \neq 1_G$ teremos que $(a, b)\mathcal{P}_{G \ltimes H}(a, b)^{-1} \subset \mathcal{P}_{G \ltimes H}$, para todo $(a, b) \in G \ltimes H$, pois $bgb^{-1} \in \mathcal{P}_G$ e $ah^b(a^{-1})^g \in \mathcal{P}_H$. □

Consideremos a aplicação $r_n : P_n \longrightarrow PB_{n-1}$ definida de forma que dada uma n-trança $\beta \in PB_n$ então $r_n(\beta)$ remove a primeira trança à direita de β, ou seja a n-ésima corda, tornando-se uma $(n-1)$-trança. Essa aplicação é conhecida como *homomorfismo esquecimento*.

A demontração do Lema 5.2 e do Teorema 5.1 a seguir estão contidas em [4] e serão omititas.

Lema 5.2. *A aplicação r_n é um homomorfismo de PB_n para PB_{n-1}. O kernel $F(n-1)$ de r_n é o conjunto das tranças puras sobre n-cordas que podem ser representadas por um diagrama com $n-1$ cordas e é um grupo livre de rank $n-1$.*

Veja que pelo Lema 5.2 obtemos uma sequência exata curta

$$1 \longrightarrow U_n \xrightarrow{i} PB_n \xrightarrow{\tau_n} PB_{n-1} \longrightarrow 1 \tag{5.9}$$

onde U_n é o kernel do homomorfismo r_n e $i : U_n \longrightarrow PB_n$ é a inclusão. Veja que tomando a aplicação $\psi : B_{n-1} \longrightarrow B_n$ conforme a Proposição 3.2 temos que a sequência acima cinde.

Teorema 5.1. *Para todo $n \geq 2$ o grupo U_n é livre com $n-1$ geradores $\{A_{i,n}\}_{1 \geq i \geq n-1}$, onde $A_{i,n} = (\sigma_{n-1}\sigma_{n-2}\cdots\sigma_{i+1})\sigma_i^2(\sigma_{i+1}^{-1}\cdots\sigma_{n-2}^{-1}\sigma_{n-1}^{-1})$.*

Proposição 5.5. *Para cada $n \leq 2$, o grupo de tranças puras PB_n é o produto semi-direto de PB_{n-1} por $F(n-1)$.*

Prova: Pelo Teorema 5.1 podemos afirmar que $U_n \cong PB_n$ e como a sequência exata 5.9 cinde pelo homomorfismo definido na Proposição 3.2, então pelo Lema 1.2 temos $PB_n \cong PB_{n-1} \ltimes F(n-1)$. □

O corolário abaixo é consequência imediata do raciocínio por indução na Proposição 5.5.

Corolário 5.2.

$$PB_n \cong F(1) \ltimes F(2) \ltimes \cdots \ltimes F(n-2) \ltimes F(n-1). \tag{5.10}$$

□

Observação 5.3. O isomorfismo dado em (5.10) é conhecido como *forma normal de Artin*.

Observação 5.4. Pela forma normal de Artin podemos escrever uma n-trança pura β na forma de produto

$$\beta_1 \cdots \beta_{n-1}, \tag{5.11}$$

onde $\beta_i \in F(n-i)$. As tranças β_i, para $i \in \{1, \ldots, n-1\}$, são chamadas de *coordenadas Artin*. Artin denonomiou o processo de escrever tranças como um produto em 5.11 como *técnica de pentear Artin*.

Lema 5.3. *Sejam $X = \{x_1, \ldots, x_n\}$ e F o grupo livre sobre X. Seja $\varphi : F \longrightarrow F$ um homomorfismo e considere a aplicação $\varphi_{ab} : F/[F,F] \longrightarrow F/[F,F]$, induzido pela abelianização de F. Se φ é a identidade, então a ordem de Margnus é invariante para φ.*

Prova: Mostraremos que se $1 < w$ então $1 < \varphi(w)$, para todo $w \in F$. Veja que $\mu([F,F]) \subset 1 + \mathcal{O}(2)$ em $\mathbb{Z}[[X_1, \ldots, X_n]]$.
Temos que

$$\begin{array}{rcl} \varphi_{ab} : F/[F,F] & \longrightarrow & F/[F,F] \\ x_i^{-1} + [F,F] & \mapsto & \varphi_{ab}(x_i^{-1} + [F,F]) = x_i^{-1} + [F,F]. \end{array} \tag{5.12}$$

Observe que

i.) $x_i^{-1} + [F,F] = \varphi(x_i^{-1}) + [F,F] \Leftrightarrow \varphi(x_i)x_i^{-1}$, para cada i.

ii.) $\mu([F,F]) \subset 1 + \mathcal{O}(2) \Rightarrow \mu(\varphi(x_i)x_i^{-1}) \in 1 + \mathcal{O}(2)$.

Sendo assim, pelos itens observados acima, podemos concluir que

$$\begin{array}{rcl} \mu(\varphi(x_i)x_i^{-1} & = & \mu(\varphi(x_i))\varphi(x_i^{-1}) = 1 + o(2) \\ \Rightarrow \mu(\varphi(x_i)) & = & (1 + o(2))\mu(x_i) = \mu(x_i) + o(2)\mu(x_i) = 1 + X_i + o(2). \end{array} \tag{5.13}$$

Tome $w \in F$ diferente de 1. Quando substituímos cada x_i por $\varphi(x_i)$ vemos como φ atua em w. A imagem da expansão de Magnus μ de w nos mostra que o primeiro termo não constante e não nulo de $\mu(w)$ e $\mu(\varphi(w))$ são coincidentes. Portanto, $1 < w$ então $1 < \varphi(w)$. □

Lema 5.4. *Dado $\beta \in B_{n-1}$ e $\varphi : F(n-1) \longrightarrow F(n-1)$ definido por $\varphi(x) = \beta^{-1}x\beta$ então existe $w_i \in F(n-1)$ que satisfaz*

$$\varphi(x_{i,n}) = w_i^{-1} x_{\tau_n(i),n} w_i, \tag{5.14}$$

onde τ_n é a permutação associada a trança β.

Prova: Seja $\sigma_i = \beta$ onde $1 \leq n-2$. De acordo com as relações dadas na Observação 3.14, temos

$$\varphi(x_{i,n}) = \sigma_i^{-1} x_{i,n} \sigma_i = x_{i,n} x_{i+1,n} x_{i,n}^{-1} \tag{5.15}$$

$$\varphi(x_{i+1}) = \sigma_i^{-1} x_{i+1,n} \sigma_i = x_{i,n} \tag{5.16}$$

$$\varphi(x_{j,n}) = \sigma_i^{-1} x_{j,n} \sigma_i = x_{j,n}, \text{ para } j \neq i,\ i+1. \tag{5.17}$$

Analogamente, para $\beta = \sigma_i^{-1}$, onde $i \leq n-2$, temos

$$\begin{aligned} \varphi(x_{i,n}) &= \sigma_i x_{i,n} \sigma_i^{-1} = x_{i+1,n} && (5.18) \\ \varphi(x_{i+1,n}) &= \sigma_i x_{i+1,n} \sigma_i^{-1} = x_{i+1,n}^{-1} x_{i,n} x_{i+1,n} && (5.19) \\ \varphi(x_{j,n}) &= \sigma_i x_{j,n} = x_{j,n}, \ \textit{para } j \neq i, i+1. && (5.20) \end{aligned}$$

Se $\beta \in B_{n-1}$ é uma trança arbitrária basta então seguir o raciocínio por indução no comprimento da palavra trança que representa β em termos dos geradores $\{\sigma_1, \ldots, \sigma_{n-2}\}$. □

Lema 5.5. *Sejam $\beta \in PB_n$ e $\varphi : F(n-1) \longrightarrow F(n-1)$ o autormorfismo dado por $\varphi(x) = \beta^{-1} x \beta$. Então a aplicação φ_{ab} é o automorfismo identidade.*

Prova: Basta mostrar que

$$\beta^{-1} x \beta + [F(n-1), F(n-1)] = x + [F(n-1), F(n-1)]. \tag{5.21}$$

Se verificarmos que $\beta^{-1} x^{-1} \in [F(n-1), F(n-1)]$, isto é, $\beta^{-1} x^{-1} \beta x = g^{-1} h^{-1} g h$, para todo $g, h \in F(n-1)$, teremos o resultado desejado.
Como $P_n \cong P_{n-1} \ltimes F(n-1)$ temos que se $\beta \in P_n$ então $\beta \in P_{n-1}$ ou $\beta \in F(n-1)$.
No primeiro caso, se $\beta \in P_{n-1}$, a permutação é a identidade, pelo Lema 5.4 existe $w_i \in F(n-1)$ tal que $\varphi(x_{i,n}) = w_i^{-1} x_{i,n} w_i$.
Se $\beta \in F(n-1)$ é imediato que $\beta = w_i \in F(n-1)$ e $\varphi(w_{i,n}) = w_i^{-1} x_{i,n} w_i$ o que implica $w_i^{-1} x_{i,j}^{-1} w_i x_{i,n} \in [F(n-1), F(n-1)]$.
Consequentemente,

$$\begin{aligned} \varphi_{ab}(x_{i,n} + [F(n-1), F(n-1)]) &= \varphi(x_{i,n}) + [F(n-1), F(n-1)] \\ &= x_{i,n} + [F(n-1), F(n-1)]. && (5.22) \end{aligned}$$

Logo, φ_{ab} é a identidade. □

Teorema 5.2. *O grupo de tranças puras PB_n é bi-ordenável para todo $n \geq 1$.*

Prova: Se $n = 1$ temos o grupo trivial $\{1\}$. Para $n = 2$ implica que $B_n \cong \mathbb{Z}$ que é bi-ordenável. Então, nos resta verificar para $n \geq 3$.
De acordo com o Corolário 5.10 da Proposição 5.5 podemos ver o grupo de tranças puras sob n cordas, PB_n, como um isomorfismo de grupos livres $F(i)$ para $i \in \{1, \ldots, n-1\}$, ou seja,

$$PB_n \cong F(1) \ltimes F(2) \ltimes \ldots \ltimes F(n-1). \tag{5.23}$$

Vamos mostrar que a ordem lexicográfica dada na Definição 5.6 é uma ordem total bi-invariante sobre PB_n.

De fato, suponha que PB_{n-1} seja bi-ordenável para todo $n \geq 3$, então pelo Lema 5.2 a sequência exata curta

$$1 \longrightarrow F(n-1) \xrightarrow{i} PB_n \xrightarrow{r_n} PB_{n-1} \longrightarrow 1 \tag{5.24}$$

cinde e $F(n-1)$ é bi-ordenável pela ordem de Magnus. Além disso $PB_{n-1} \cong PB_n/F(n-1)$ é bi-ordenável por hipótese de indução.
Veja que dados $f_1, f_2 \in F(n-1)$, tais que $f_1 < f_2$, então para todo $\beta \in PB_n$ temos que $\beta^{-1} f_1 \beta < \beta^{-1} f_2 \beta$, ou seja, PB_n age por conjugação em $F(n-1)$ preservando a ordem. Consequentemente, PB_n é bi-ordenável pelo Teorema 4.1. □

Teorema 5.3. *PB_∞ é bi-ordenável.*

Prova: A ordem de Magnus dada sobre PB_{n+1} estende a de PB_n. Com efeito, dizemos que dadas $\beta_1, \beta_2 \in PB_\infty$ então $\beta_2 \leq \beta_2$ se existir n tal que $\beta_1, \beta_2 \in PB_n$ e $\beta_1 \leq \beta_2$, onde $\leq$ é a ordem de PB_n. É evidente que a ordem dada em B_∞ é bi-invariante. □

Conclusão

Este trabalho possibilitou um amadurecimento e aprofundamento dos conhecimentos de Álgebra, que foram vistos na graduação, e conhecer teorias da Topologia Algébrica que não são contempladas nas disciplinas dos currículos de licenciatura e bacharelado em Matemática.

Como foi fruto de um trabalho de iniciação científica, esta monografia foi de grande contribuição para a consolidação de dois anos e meio como bolsista colaborador do Programa Institucional de Bolsas de Iniciação Científica (PIBIC) e estudante da Topologia Algébrica, onde expomos aqui o conceito de tranças geométricas, a estrutura de grupo de tais objetos e como estudá-los no ponto de vista algébrico.

Vimos que quando um grupo é ordenável então seguem-se observadas nele propriedades que não são vistas em grupos não ordenados. Essa pesquisa também fornece a base inicial e a motivação para prosseguir os estudos da teoria de tranças, pois a partir daí estuda-se a ordenabilidade do grupo de tranças em superfícies, orientáveis e não orientáveis, nós e enlaçamentos de intervalos (que tem uma ligação direta com as tranças) e problemas em aberto.

Referências Bibliográficas

E. Artin. Theorie der zöpfe. *Abhandlungen aus dem mathematichen Seminar der Universität Hamburg*, pages 47–72, 1925.

E. Artin. Theory of braids. *Annals of Mathematics 48*, pages 47–72, 1947.

D. COHEN. *Combinatorial group theory: a topological approach.* Cambrigde University Press, 1989. v.14.

I. DEHERNOY, P.; DYNNIKOV and B. WIEST. *Ordering Braids.* American Mathematical Society (AMS), Providence, RI, 2008. v.148.

J. S. R. DEREK. *A Course of the Theory of Groups.* Graduate Text in mathematics 80. Springer, New York, 1996.

A. GARCIA and Y. LEQUAIN. *Elementos de Álgebra.* IMPA, Rio de Janeiro, 2012. (Coleção Projeto Euclides).

V. HASEN. *Braids and Covering: selected topics.* Cambridge University Press, 1989.

D. JOHNSON. *Presentation of Groups.* Cambridge University Press, 1997. London Mathematical Society Student Text 15.

C. KASSEL and V. TURAEV. *Braids groups.* Springer, New York, 2008. (Graduate Text in Mathematics 247).

J. R. T. LIMA. Apresentação dos grupos de tranças em superfícies. Master's thesis, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2010.

P. A. MARTIN. *GRUPOS, CORPOS E TEORIA DE GALOIS.* Livraria da Física, São Paulo, 2010.

L. MELOCRO. Uma ordenação para o grupo de tranças puras. Master's thesis, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2016.

K. MURASUGI and B. KURPITA. *A Study of Braids.* Kluwer Academic Publisher Dordrecht, 1999.

P. J. H. Pizarro. Representação do grupo de tranças por automorfismos de grupos. Master's thesis, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2012.

M. SANTOS. O grupo de homotopia de tranças puras no disco é bi-ordenável. Master's thesis, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2018.

Apêndice A

Ações de grupos e o produto semidireto

O produto semidireto $G = H \ltimes K$ pode não fornecer informações suficientes do grupo G. Contudo, se considerarmos a ação do grupo K sobre H induzida por homomorfismos, poderemos obtê-las. Falando de forma direta, por [5] e [15] da referencia, iremos considerar homomorfismos que associam os elementos de K no grupo dos automorfismos $Aut(H)$.

Definição A.1. Dizemos que um grupo $(G, \star)$ age (à direita) num conjunto X quando existe uma função

$$\psi : G \times X \longrightarrow X$$

satisfazendo:

(A_1) *(Compatibilidade)* $\psi(x, \psi(g, h)) \mapsto \psi(x, gh) = x \star gh, \forall g, h \in G, \forall x \in X$.

(A_2) *(Identidade)* $\psi(x, e) \mapsto x, \forall x \in X$ (e é a identidade de G).

Analogamente podemos definir uma ação à esquerda do grupo G no conjunto X.

Agora, observe que na Definição 1.22 de produto semidireto externo de grupos, sejam H e K grupos arbitrários e $\phi : K \longrightarrow Aut(H)$ um homomorfismo qualquer dado da seguinte forma

$$\begin{array}{rccc} k \longmapsto \phi(k) : H & \longrightarrow & H \\ h & \longmapsto & \phi(k)(h) \end{array}$$

onde $h \in H$ e $k \in K$. Não é difícil perceber que o automorfismo ψ induz uma ação à direita dada por

$$\begin{array}{rccc} \cdot_\phi : H \times K & \longrightarrow & H \\ (h, k) & \longmapsto & \phi(k)h = hk \end{array}$$

de K em H. De fato,

i) $\cdot_\phi(h, \cdot_\phi(k_1, k_2) = \cdot_\phi(h, k_1k_2) = \phi(k_1k_2)h = h(k_1k_2)$.

ii) $\cdot_\phi(h, e_K) = \phi(e_k)h = h$.

Para trabalhar com o produto semidireto externo tomaremos o homomorfismo $\phi : K \longrightarrow Aut(H)$ como aquele tal que associa o elemento $k \in K$ ao homomorfismo interno, ou seja,

$$\begin{aligned} k \longmapsto \phi_k : H &\longmapsto H \\ h &\longmapsto \phi_k(h) = k^{-1}hk \end{aligned}$$

O homomorfismo ϕ induz uma ação de K em H que é dada por

$$\begin{aligned} \bullet : H \times K &\longrightarrow H \\ (h, k) &\longmapsto \bullet(h, k) = h^k = k^{-1}hk \end{aligned}$$

Veja que dados $h \in H$ e $k_1, k_2 \in K$ temos que

$$\bullet(h, k_1k_2) = h^{k_1k_2} = \phi_{k_1k_2} = (\phi_{k_1} \circ \phi_{k_2})(h) = \phi_{k_1}(\phi_{k_2}(h)) = (h^{k_1})^{k_2}.$$

Além disso, $\bullet(h, e) = \phi_e(h) = h^e = h$. A ação $\bullet$ é chamada de *ação por conjugação*. Veja que cada ϕ_k é um automorfismo. Logo, na ordenação do produto semidireto podemos usar o automorfismo interior na Definição 1.22.

Índice Remissivo