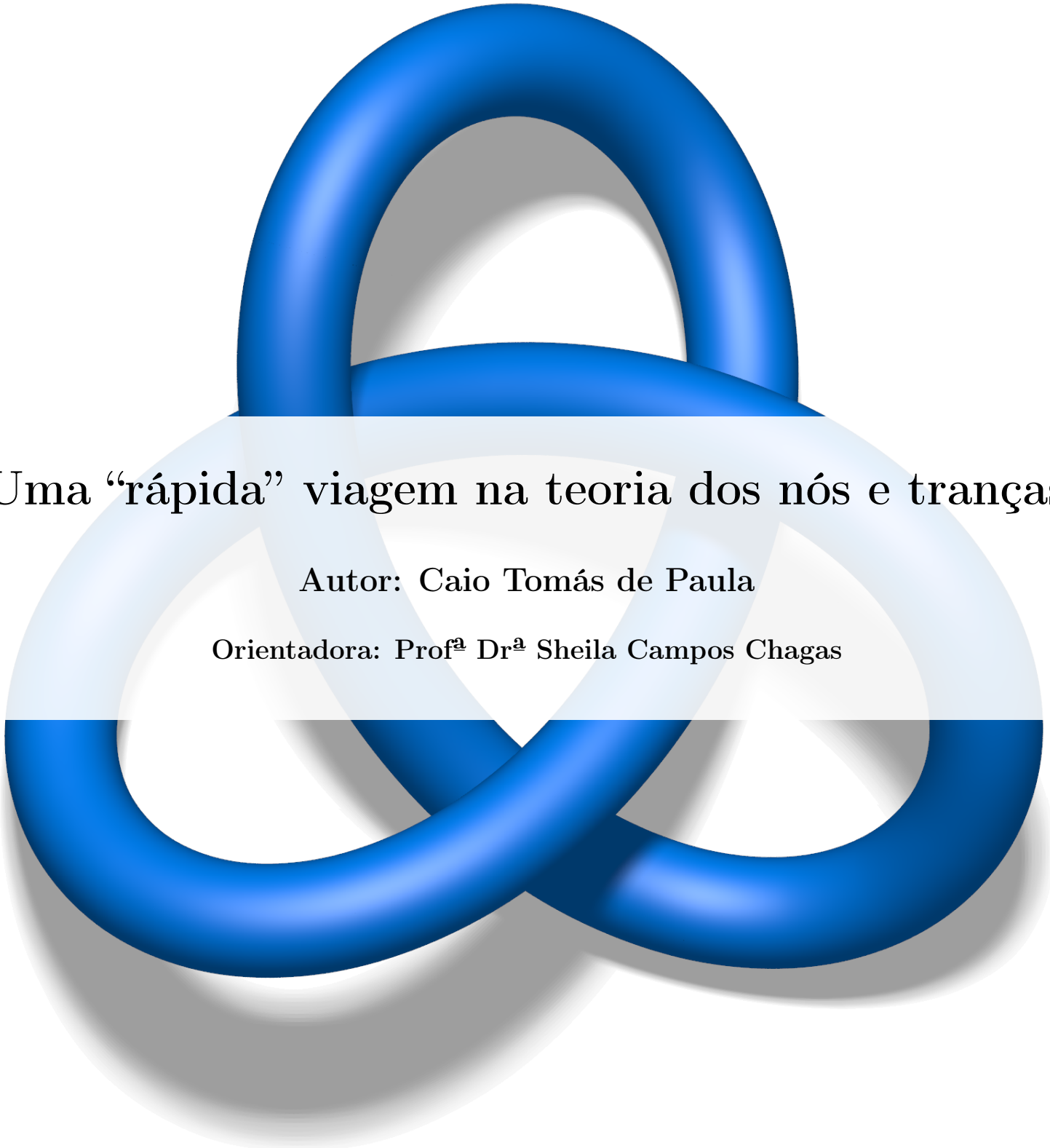


Uma “rápida” viagem na teoria dos nós e tranças

Autor: Caio Tomás de Paula

Orientadora: Profª Drª Sheila Campos Chagas

Sumário

I Preparando as malas — Preliminares de Álgebra Abstrata 4

Teoria de Grupos **5**
- Grupos . . . 5
- Grupos de permutação . . . 13
- Isomorfismos . . . 18
- Classes laterais . . . 23
- Produto direto externo de grupos . . . 29
- Subgrupos normais e grupo quociente . . . 38
- Homomorfismos . . . 42

Grupos livres **52**
- Introdução . . . 52
- Apresentações de produtos diretos . . . 62
- Grupos abelianos finitamente gerados . . . 62
- Alguns subgrupos importantes de um grupo abeliano . . . 71
- Subgrupos de Sylow . . . 74
- Abelianização de um grupo . . . 75
- Algumas propriedades de grupos livres . . . 78
- Grupos, isometrias e polinômios . . . 81

II Começando a viagem — Tranças e Nós 85

A Teoria das Tranças **86**
- Introdução . . . 86
- Propriedades de B_n e o grupo de tranças puras . . . 98
- Centro de B_n . . . 103
- Tranças como espaços de configuração . . . 106
- Diagrama de van Kampen . . . 117
- Tranças como discos perfurados . . . 120

A Teoria dos Nós **127**
- Conexões entre tranças e nós . . . 127
- Algumas aplicações do Teorema de Markov . . . 135
- Grupos de nó . . . 137
- Representação de Burau e os polinômios de Alexander e Jones . . . 144
- O grupo de Alexander . . . 177

Curiosidades finais **182**
O problema da palavra em $B_n(\mathbb{R}^2)$ – uma breve introdução 182
O *linking number* 184
Tranças, nós e protetores solares de para-brisa 186

Referências Bibliográficas **190**

Índice Remissivo **192**

Introdução

"You know also that the beginning is the most important part of any work"
— Plato's Republic

O que é esse texto?

O presente texto é resultado de um projeto de PIBIC – Programa Institucional de Bolsas de Iniciação Científica – realizado no período de Agosto de 2019 a Setembro de 2020 sob orientação da profª Sheila Campos Chagas da Universidade de Brasília.

Nele, busquei registrar tudo que estudei e aprendi ao no projeto, assim como os *insights* e entendimentos que eu mesmo tive durante os estudos e discussões ao longo da pesquisa. Gostaria de deixar registrados os meus agradecimentos à professora Sheila, que me aceitou para participar do projeto ainda que eu não tivesse, a rigor, os pré-requisitos necessários. Agradeço também ao professor Igor dos Santos, que foi a ponte entre mim e a professora Sheila.

O que você encontrará nele?

Os meus principais objetos de estudo ao longo do projeto foram as tranças e os nós. Como, na época, eu não havia feito nenhum curso de Álgebra Abstrata ainda, o primeiro passo foi estudar todos os pré-requisitos de Teoria dos Grupos que eram necessários para entender a Teoria das Tranças e a Teoria dos Nós. Nessa primeira etapa, as principais referências foram [6, 7]. A primeira parte do livro se ocupa em tratar desses pré-requisitos, dividida em dois capítulos: o primeiro sobre a Teoria de Grupos "genérica", tratada em cursos iniciais de Álgebra Abstrata, e o segundo sobre grupos livres e alguns outros tópicos mais avançados da Teoria de Grupos.

Estudados os pré-requisitos necessários, avançamos para o estudo das tranças e dos nós. Nesta etapa, as principais referências foram [1, 3, 13]. A segunda parte do livro divide-se, então, em 3 capítulos: o primeiro introduz os tópicos que serão estudados nesta etapa e trata das principais propriedades (mais básicas) das tranças, de sua estrutura algébrica e das diferentes formas pelas quais podemos enxergá-las; o segundo foca nos nós, utilizando a Teoria das Tranças

desenvolvida anteriormente para construir essa nova teoria; e o terceiro e último capítulo traz, a título de curiosidade, alguns tópicos interessantes e correlacionados com os temas tradados ao longo do livro.

É interessante comentar acerca das referências: todas listadas foram utilizadas de alguma maneira, seja como guia do estudo, seja apenas para uma breve consulta. Via de regra, as referências citadas ao longo do texto serviram de guia para alguma etapa do projeto, enquanto que as não citadas serviram para uma consulta breve.

Além disso, os pontos principais que eu gostaria que você, leitor(a), levasse para a casa são:

1. quando queremos formalizar um certo objeto, quanto mais "liberdade" ele tiver, mais difícil será o nosso trabalho;

2. os invariantes são ferramentas poderosas para se lidar com certos objetos, como os nós;

Todos que têm um pouco mais experiência e vivência matemática já sentiram, em algum momento, o primeiro item "na pele". Para aqueles que nunca pensaram nisso, as tranças devem ser o exemplo principal: para formalizar esse objeto matematicamente, precisamos recorrer a uma teoria algébrica pesada e, para analisar as propriedades deste objeto, precisamos de teorias mais rebuscadas ainda.

O segundo item merece um pouco mais de explicação. A discussão feita acerca dos polinômios de Alexander e Jones detectarem ou não o nó trivial é o germe dessa importância: os invariantes são uma das únicas ferramentas que nós temos para estudar e distinguir os nós (pelo menos por enquanto). A quantidade de invariantes é vasta[1], e citamos alguns abaixo:

- invariantes da teoria das tranças;
- invariantes tridimensionais;
- o polinômio de Alexander-Conway;
- o polinômio de Alexander multivariável;
- o determinante e a assinatura;
- o polinômio de Jones;
- os polinômios de Jones coloridos;
- o invariante A2;

[1]Essa lista foi obtida deste site

- o polinômio HOMFLY-PT;
- o polinômio de Kauffman;
- os invariantes de Vassiliev;
- homologia de Khovanov;
- homologia Floer de nós de Heegaard;
- invariantes de R-Matriz.

Alguns deles são algébricos, outros são geométricos e outros ainda são topológicos. Dependendo do problema que se tem em mãos, um deles pode ser mais adequado que os outros.

A noção de invariante também é relevante em outros problemas, como foi o caso da solução do 3º problema de Hilbert (não comentarei sobre a solução, mas quem se interessar pode ler mais sobre aqui.

Por isso, gostaria de finalizar esse texto incentivando o(a) leitor(a) a reconsiderar a importância dos invariantes (ou a considerar, se nunca o havia feito antes), e tê-los em mente como ferramentas importantes e muito úteis em vários contextos.

Boa leitura!

Parte I

Preparando as malas — Preliminares de Álgebra Abstrata

Capítulo 1

Teoria de Grupos

"Go down deep enough into anything and you will find mathematics."
— Dean Schlicter

1.1 Grupos

Definição 1.1.1 — Operação binária. Seja G um conjunto. Uma operação binária em G é uma função que associa, a cada par ordenado de elementos de G, um elemento de G.

■ **Exemplo 1.1.1** A adição, subtração e multiplicação de inteiros são exemplos de operações binárias, bem como a adição e multiplicação módulo n. ■

Definição 1.1.2 — Grupo. Seja G um conjunto munido de uma operação binária que, a cada par $(a, b) \in G \times G$, associa o elemento de G denotado por ab. Dizemos que G é um grupo sob essa operação se as seguintes condições são satisfeitas:

(i) a operação é associativa, ou seja, $(ab)c = a(bc)$ para todos $a, b, c \in G$;

(ii) existe um elemento $e \in G$, chamado identidade, tal que $ae = ea = a$ para todo $a \in G$;

(iii) para todo $a \in G$, existe $b \in G$ (chamado o inverso de a) tal que $ab = ba = e$.

Observação. É comum denotar a identidade simplesmente por 1 ao invés de e. Faremos isso sem cerimônia no decorrer do texto onde for conveniente.

■ **Exemplo 1.1.2** Os conjuntos dos inteiros, dos racionais e dos reais são todos grupos sob a operação de adição. Em cada um dos casos, a identidade é o 0 e o inverso de a é $-a$. Além disso, $a + b = b + a$ para todos a, b no respectivo conjunto e, por isso, dizemos que o grupo é abeliano. ■

■ **Exemplo 1.1.3** O conjunto dos inteiros sob a multiplicação ordinária não é um grupo. De fato, não existe nenhum inteiro b tal que $5b = 1$. ■

Propriedades elementares de grupos

Teorema 1.1.1 O elemento identidade de um grupo é único.

Demonstração. Suponha que e e e' são identidades em G. Então, temos

$$e' = e'e = e$$

e, portanto, a identidade é única. ■

Teorema 1.1.2 Dados um grupo G e $a, b, c \in G$ quaisquer, temos que

1. $ba = ca \implies b = c$;
2. $ab = ac \implies b = c$.

Demonstração. Suponha $ba = ca$ e seja a^{-1} o inverso de a. Multiplicando à direita, temos

$$(ba)a^{-1} = (ca)a^{-1} \iff b(aa^{-1}) = c(aa^{-1}) \iff b = c.$$

De maneira análoga, mostra-se que $ab = ac$ implica $b = c$ multiplicando-se por a^{-1} à esquerda. ■

Teorema 1.1.3 Para cada $a \in G$, existe um único $b \in G$ tal que $ab = ba = e$.

Demonstração. Suponha que b e c são inversos de a. Então $ab = e = ac$ e, portanto, $b = c$. ■

Teorema 1.1.4 Dados um grupo G e $a, b \in G$, temos $(ab)^{-1} = b^{-1}a^{-1}$.

Demonstração. Note que

$$(ab)(ab)^{-1} = e$$

e

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e,$$

donde segue, pelo teorema anterior, que $(ab)^{-1} = b^{-1}a^{-1}$. ■

Subgrupos

Definição 1.1.3 — Ordem de grupo. A ordem de um grupo finito G é o número de elementos que ele contém, denotada por $|G|$ ou $\sharp G$.

Definição 1.1.4 — Ordem de elemento. A ordem de um elemento g de um grupo G é o menor inteiro positivo n tal que $g^n = e$. Se um tal inteiro não existir, dizemos que g tem ordem infinita. Denotamos a ordem de g por $|g|$.

■ **Exemplo 1.1.4** Considere $\mathbb{Z}_{10}$ sob a adição módulo 10. Como $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$ e $5 \cdot 2 = 0$, sabemos que $|2| = 5$. ■

■ **Exemplo 1.1.5** Considere $\mathbb{Z}$ sob a adição. Todo elemento não nulo tem ordem infinita, já que a sequência $a, 2a, 3a, \ldots$ não inclui o 0 se $a \neq 0$. ■

Definição 1.1.5 — Subgrupo. Se um subconjunto H de um grupo G é também um grupo sob a operação de G, dizemos que H é um subgrupo de G, e denotamos $H \leq G$ ou $H < G$ se $H \subseteq G$ e $H \subset G$, respectivamente.

Testes de subgrupos

Teorema 1.1.5 Sejam G um grupo e $H \neq \varnothing$ um subconjunto de G. Se $ab^{-1} \in H$ sempre que $a, b \in H$, então $H \leq G$.

Demonstração. Como a operação de H é a mesma de G, é claro que ela é associativa. Vamos mostrar que $e \in H$.

Como $H \neq \varnothing$, existe $x \in H$. Daí, tomando $a = x = b$, temos que $e = xx^{-1} = ab^{-1} \in H$.

Para checar que $x^{-1} \in H$ sempre que $x \in H$, basta tomarmos $a = e$ e $b = x$.

Por fim, resta mostrarmos que H é fechado para a operação, ou seja, que se $x, y \in H$ então $xy \in H$. Ora, para tanto basta tomar $a = x$ e $b = y^{-1}$. ■

■ **Exemplo 1.1.6** Seja G um grupo abeliano com identidade e. Então $H = \{x \in G \mid x^2 = e\}$ é um subgrupo de G. De fato, temos $e^2 = e$, logo $e \in H$ e, portanto, $H \neq \varnothing$. Agora, suponha que $a, b \in H$, ou seja, $a^2 = e = b^2$. Queremos mostrar que $(ab^{-1})^2 = e$. Ora, mas como G é abeliano, então

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2(b^2)^{-1} = ee^{-1} = e.$$

Segue então do teorema anterior que $H \leq G$. ■

Teorema 1.1.6 Sejam G um grupo e $H \neq \varnothing$ um subconjunto de G. Se $ab \in H$ sempre que $a, b \in H$ e $a^{-1} \in H$ sempre que $a \in H$, então $H \leq G$.

Demonstração. Pelo Teorema 1.1.5, basta mostrar que se $a, b \in H$ então $ab^{-1} \in H$. Então, suponhamos $a, b \in H$. Por hipótese, H contém os inversos de a e de b, de modo que $ab^{-1} \in H$ pois H é fechado para a multiplicação por hipótese. ■

■ **Exemplo 1.1.7** Sejam G um grupo abeliano e $H = \{x \in G \mid |x| < \infty\}$. Vamos mostrar que $H \leq G$ usando o teorema acima. Primeiro, como $e^1 = e$, segue que $e \in H$, ou seja, $H \neq \varnothing$. Agora, assuma que $a, b \in H$ e sejam $|a| = m$ e $|b| = n$. Como G é abeliano, temos que

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e.$$

Portanto, $|ab| < \infty$ (não necessariamente $|ab| = mn$, cuidado!), ou seja, $ab \in H$. Por fim, como

$$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e,$$

então $a^{-1} \in H$ e, pelo teorema anterior, segue que $H \leq G$. ■

■ **Exemplo 1.1.8** Sejam G o grupo dos números reais não nulos com a multiplicação,

$$H = \{x \in G \mid x = 1 \text{ ou } x \in G \setminus \mathbb{Q}\}$$

e

$$K = \{x \in G \mid x \geq 1\}.$$

Note que $H \not\leq G$ pois $\sqrt{2} \in H$ mas $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Além disso, K também não é subgrupo de G pois $2 \in K$ mas $2^{-1} = 1/2 \notin K$. ■

Teorema 1.1.7 Seja $H \neq \varnothing$ um subconjunto finito de um grupo G. Se H é fechado sob a operação de G, então H é um subgrupo de G.

Demonstração. Do Teorema 1.1.6, para provarmos o resultado basta mostrar que $a^{-1} \in H$ sempre que $a \in H$.

Note que se $a = e$, então $a^{-1} = a$ e terminamos. Do contrário, considere a sequência $a, a^2, \ldots$ cujos elementos todos pertencem a H por hipótese. Pela finitude de H, segue que os elementos dessa sequência não são todos distintos, ou seja, existem $i, j \in \mathbb{N}$ tais que $a^i = a^j$ com $i > j$. Ora, então $a^{i-j} = e$ e, como $a \neq e$, devemos ter $i - j > 1$. Portanto, $a^{-1} = a^{i-j-1}$. Como $i - j - 1 \geq 1$, segue que $a^{i-j-1} \in H$ e terminamos. ■

Proposição 1.1.1 Se G é um grupo e $a \in G$, então $\langle a \rangle \leq G$. ■

Demonstração. Como $a \in \langle a \rangle$, temos $\langle a \rangle \neq \varnothing$. Sejam $a^n, a^m \in \langle a \rangle$. Então $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$ de modo que, pelo Teorema 1.1.5, temos $\langle a \rangle \leq G$. ■

■ **Exemplo 1.1.9** Em $\mathbb{Z}_{10}$, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$. ■

Definição 1.1.6 — Centro. O centro $Z(G)$ de um grupo G é o subconjunto dos elementos de G que comutam com todos os elementos de G. Em símbolos,

$$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}.$$

Teorema 1.1.8 O centro de um grupo G é um subgrupo de G.

Demonstração. Vamos mostrar esse resultado usando o Teorema 1.1.6. Como $eg = ge$ para todo $g \in G$, temos $e \in Z(G)$, de modo que $Z(G) \neq \varnothing$. Agora, suponha que $a, b \in Z(G)$. Então $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ para todo $x \in G$. Logo, $ab \in Z(G)$.

Por fim, suponha que $a \in Z(G)$, ou seja,

$$ax = xa \iff a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \iff exa^{-1} = a^{-1}xe \iff xa^{-1} = a^{-1}x.$$

Logo, $a^{-1} \in Z(G)$ e o resultado segue do Teorema 1.1.6. ■

Observe que $Z(G)$ é, por definição, abeliano, independentemente se G é ou não abeliano.

Definição 1.1.7 — Centralizador. Seja $a \in G$ um elemento fixado. O centralizador de $a \in G$, denotado $C_G(a)$, é o conjunto dos elementos de G que comutam com a. Em símbolos,

$$C_G(a) = \{g \in G \mid ga = ag\}.$$

Teorema 1.1.9 Para cada elemento a em um grupo G, o centralizador de a é um subgrupo de G.

Demonstração. A prova é similar àquela do Teorema 1.1.8 e é deixada ao leitor. ■

Observação. Note que, para todo elemento a de um grupo G, temos $Z(G) \subseteq C_G(a)$. Ademais, note que G é abeliano se, e somente se, $C_G(a) = G$ para todo $a \in G$. Equivalentemente, G é abeliano se, e somente se, $Z(G) = G$.

Propriedades de grupos cíclicos

Teorema 1.1.10 Sejam G um grupo e $a \in G$. Se a tem ordem infinita, então $a^i = a^j$ se, e somente se, $i = j$. Se a tem ordem finita n, então

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

e $a^i = a^j$ se, e somente se, $n \mid i - j$.

Demonstração. Se a tem ordem infinita, então não existe $n \neq 0$ tal que $a^n = e$. Como $a^i = a^j$ implica $a^{i-j} = e$, devemos ter $i = j$ e fica provada a primeira afirmação do teorema.

Agora, suponha que $|a| = n$. Vamos mostrar que $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. A inclusão $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$ é imediata. Para a inclusão no outro sentido, seja $a^k \in \langle a \rangle$ qualquer. Pelo algoritmo da divisão, existem inteiros q, r tais que

$$k = qn + r,\ 0 \leq r < n.$$

Sendo assim, temos

$$a^k = a^{qn+r} = (a^n)^q a^r = a^r,$$

ou seja, $a^k \in \{e, a, \ldots, a^{n-1}\}$ e fica provada a nossa afirmação.

Por fim, resta mostrar que $a^i = a^j \iff n \mid i - j$. Suponha, inicialmente, que $a^i = a^j$. Ora, então $a^{i-j} = e$ e, usando o algoritmo da divisão novamente, existem inteiros q, r tais que

$$i - j = qn + r,\ 0 \leq r < n.$$

Daí, segue que $e = a^{i-j} = a^r$. Como n é o menor inteiro positivo tal que $a^n = e$, devemos ter $r = 0$ e, portanto, $n \mid i - j$.

Reciprocamente, se $i - j = nq$ então $a^{i-j} = a^{nq} = e^q = e$, de modo que $a^i = a^j$. ■

Corolário 1.1.10.1 Para qualquer elemento a de um grupo, $|a| = |\langle a \rangle|$.

Corolário 1.1.10.2 Sejam G em grupo e $a \in G$ de ordem n. Se $a^k = e$, então $n \mid k$.

Demonstração. Como $a^k = e = a^0$, segue do Teorema 1.1.10 que $n \mid k - 0 = k$. ■

Teorema 1.1.11 Sejam a um elemento de ordem n de um grupo e k um inteiro positivo qualquer. Temos que

$$\langle a^k \rangle = \langle a^{\text{mdc}(n,k)} \rangle$$

e

$$|a^k| = \frac{n}{\text{mdc}(n,k)}.$$

Demonstração. Por simplicidade, vamos denotar $d = \text{mdc}(n, k)$. Escreva $k = dr$. Como $a^k = (a^d)^r$, segue que $\langle a^k \rangle \subseteq \langle a^d \rangle$. Ademais, sabemos que existem inteiros s, t tais que $d = ns + kt$ e, portanto,

$$a^d = a^{ns} a^{kt} = (a^k)^t \in \langle a^k \rangle.$$

Logo, $\langle a^d \rangle \subseteq \langle a^k \rangle$ e, consequentemente, $\langle a^d \rangle = \langle a^k \rangle$, provando a primeira parte do teorema.

Para a segunda parte, vamos primeiro mostrar que $|a^d| = n/d$ para qualquer divisor d de n. De fato, $(a^d)^{n/d} = a^n = e$, de modo que $|a^d| \leq n/d$. Por outro lado, se i é um inteiro positivo menor que n/d então $(a^d)^i \neq e$ por definição de $|a|$, pois $di < n$. Aplicando esse fato para $d = \text{mdc}(n, k)$, obtemos

$$|a^k| = |\langle a^k \rangle| = |\langle a^{\text{mdc}(n,k)} \rangle| = |a^{\text{mdc}(n,k)}| = \frac{n}{\text{mdc}(n, k)}.$$

■

Corolário 1.1.11.1 Em um grupo cíclico finito, a ordem de um elemento divide a ordem do grupo.

Corolário 1.1.11.2 Sejam G um grupo e $a \in G$ com $|a| = n$. Então $\langle a^i \rangle = \langle a^j \rangle$ se, e somente se, $\text{mdc}(n, i) = \text{mdc}(n, j)$ e $|a^i| = |a^j|$ se, e somente se, $\text{mdc}(n, i) = \text{mdc}(n, j)$.

Demonstração. Pelo Teorema 1.1.11, basta mostrarmos que $\langle a^{\text{mdc}(n,i)} \rangle = \langle a^{\text{mdc}(n,j)} \rangle$ se, e somente se, $\text{mdc}(n, i) = \text{mdc}(n, j)$. Ora, é claro que se $\text{mdc}(n, i) = \text{mdc}(n, j)$ então os subgrupos gerados são iguais. Reciprocamente, se os subgrupos gerados são iguais então $|a^{\text{mdc}(n,i)}| = |a^{\text{mdc}(n,j)}|$ e, pela segunda afirmação do Teorema 1.1.11, temos $n/\text{mdc}(n, i) = n/\text{mdc}(n, j)$ e, consequentemente, $\text{mdc}(n, i) = \text{mdc}(n, j)$. ■

Corolário 1.1.11.3 Sejam G um grupo e $a \in G$ com $|a| = n$. Então $\langle a \rangle = \langle a^j \rangle$ se, e somente se, $\text{mdc}(n, j) = 1$ e $|a| = |\langle a^j \rangle|$ se, e somente se, $\text{mdc}(n, j) = 1$.

Corolário 1.1.11.4 Um inteiro $k \in \mathbb{Z}_n$ é um gerador de $\mathbb{Z}_n$ se, e somente se, $\text{mdc}(n, k) = 1$.

Teorema 1.1.12 — Teorema Fundamental dos Grupos Cíclicos. Todo subgrupo de um grupo cíclico é cíclico. Ademais, se $|\langle a \rangle| = n$, então a ordem de qualquer subgrupo de $\langle a \rangle$ é um divisor de n e, para cada divisor positivo k de n, o grupo $\langle a \rangle$ tem exatamente um subgrupo de ordem k, a saber $\langle a^{n/k} \rangle$.

Demonstração. Sejam $G = \langle a \rangle$ e $H \leq G$. Vamos mostrar que H é cíclico.

Ora, se $H = \{e\}$, então claramente $H = \langle e \rangle$. Então, vamos assumir $H \neq \{e\}$. Afirmamos que H contém um elemento da forma $a^t, t > 0$. De fato, como $G = \langle a \rangle$, todo elemento de H é da forma a^t e, quando $t < 0$, então o inverso dessa potência tem expoente positivo e também pertence a H, verificando nossa afirmação.

Agora, seja m o menor inteiro positivo tal que $a^m \in H$, que existe pois $H \neq \{e\}$. Como H é fechado para a multiplicação, temos $\langle a^m \rangle \subseteq H$. Afirmamos que vale a inclusão $\langle a^m \rangle \supseteq H$, ou seja, que $H = \langle a^m \rangle$. De fato, se b é um elemento qualquer de H, então $b = a^k$ para algum k. Aplicando o algoritmo da divisão para k e m, temos que existem inteiros q, r tais que

$$k = mq + r,\ 0 \leq r < m.$$

Logo,

$$a^k = a^{mq}a^r \iff a^r = a^{-mq}a^k.$$

Como $a^k, a^{-mq} \in H$, segue que $a^r \in H$. Ora, mas m foi tomado como sendo o menor inteiro positivo tal que $a^m \in H$. Portanto, devemos ter $r = 0$ e, daí, $b = a^k \in \langle a^m \rangle$, concluindo a demonstração de que H é cíclico.

Para provar a próxima parte do teorema, suponha que $|\langle a \rangle| = n$ e seja $H \leq \langle a \rangle$. Já mostramos que $H = \langle a^m \rangle$, sendo m o menor inteiro positivo tal que $a^m \in H$. Tomando $a^n = b = e$ no parágrafo anterior, segue que $n = mq$.

Para a parte final do teorema, seja k um divisor positivo de n qualquer. Do Teorema 1.1.11, sabemos que $\langle a^{n/k} \rangle$ tem ordem $n/\operatorname{mdc}(n, n/k) = n/(n/k) = k$. Seja $H \leq \langle a \rangle$ de ordem k. Mostramos acima que $H = \langle a^m \rangle$, onde $m \mid n$. Ora, então $m = \operatorname{mdc}(n, m)$ e

$$k = |a^m| = |a^{\operatorname{mdc}(m,n)}| = n/\operatorname{mdc}(n, m) = n/m.$$

Portanto, $m = n/k$ e $H = \langle a^{n/k} \rangle$. ■

Corolário 1.1.12.1 Para cada divisor positivo k de n, o conjunto $\langle n/k \rangle$ é o único subgrupo de $\mathbb{Z}_n$ de ordem k. Além disso, os subgrupos de $\mathbb{Z}_n$ são todos dessa forma.

Antes de seguir para o próximo teorema, convém definir a seguinte função, que é bastante relevante em Teoria dos Números.

Definição 1.1.8 — Função ϕ de Euler. A função $\phi : \mathbb{N}^* \to \mathbb{N}^*$ tal que

$$\begin{cases} \phi(1) = 1 \\ \phi(n) = \sharp\{d \in \mathbb{N}^* \mid \operatorname{mdc}(d, n) = 1\},\ n > 1 \end{cases}$$

é chamada função phi de Euler. Dito de outro modo, ela associa, a cada $n > 1$, a quantidade de inteiros positivos que são coprimos com n.

Teorema 1.1.13 Se d é um divisor positivo de n, o número de elementos de ordem d em um grupo cíclico de ordem n é $\phi(d)$.

Demonstração. Pelo Teorema 1.1.12, o grupo tem exatamente um subgrupo de ordem d, digamos $\langle a \rangle$. Então todo elemento de ordem d também gera o subgrupo $\langle a \rangle$ e, pelo Corolário 1.1.11.3, um elemento a^k gera $\langle a \rangle$ se, e somente se, $\text{mdc}(k, d) = 1$. A quantidade de tais elementos é precisamente a quantidade de valores de k tais que $\text{mdc}(k, d) = 1$, ou seja, $\phi(d)$. ■

Corolário 1.1.13.1 Em um grupo finito, o número de elementos de ordem d é um múltiplo de $\phi(d)$.

Demonstração. Se o grupo não tiver elementos de ordem d, então o teorema é verdadeiro pois $\phi(d) \mid 0$. Suponhamos então que existe $a \in G$ com $|a| = d$. Pelo Teorema 1.1.13, sabemos que $\langle a \rangle$ tem $\phi(d)$ elementos de ordem d. Se todos os elementos de ordem d em G estiverem em $\langle a \rangle$, terminamos. Do contrário, existe $b \in G$ de ordem d tal que $b \notin \langle a \rangle$. Ora, mas $\langle b \rangle$ também tem $\phi(d)$ elementos de ordem d, ou seja, até o momento temos $2\phi(d)$ elementos de ordem d em G dado que $\langle a \rangle$ e $\langle b \rangle$ não tenham elementos de ordem d em comum.

Caso exista c de ordem d que seja comum a ambos os subgrupos, então $\langle a \rangle = \langle c \rangle = \langle b \rangle$ e $b \in \langle a \rangle$, absurdo.

Procedendo desta forma, vemos que o número de elementos de ordem d em um grupo finito é um múltiplo de $\phi(d)$. ■

1.2 Grupos de permutação

Definição 1.2.1 Um grupo de permutações de um conjunto A é um conjunto de permutações de A que forma um grupo sob a operação de composição.

É comum denotar uma permutação utilizando matrizes. Por exemplo, se α é a permutação em $\{1, 2, 3, 4\}$ que manda 1 em 2, 2 em 3, 3 em 1 e 4 em 4, escrevemos

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Com essa notação, o produto de duas permutações é feito da direita para a esquerda. Por exemplo,

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}.$$

▪ **Exemplo 1.2.1 — Grupo Simétrico S_n.** Seja $A = \{1, 2, \ldots, n\}$. O grupo de todas as permutações de A é chamado grupo simétrico de grau n, denotado por S_n. Os seus elementos têm a forma

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}.$$

Deixamos a cargo do leitor mostrar que $|S_n| = n!$ e que S_n não é abeliano se $n \geq 3$. ∎

A notação de matrizes, apesar de bem visual, pode ser um pouco difícil de trabalhar por vezes. Uma notação alternativa, também muito comum, é a de ciclos. Por exemplo, se α é a permutação que manda 1 em 2, 2 em 1, 3 em 4, 4 em 6, 5 em 5 e 6 em 3, escrevemos

$$\alpha = (1, 2)(3, 4, 6)(5).$$

É comum omitir o ciclo de tamanho um e escrever simplesmente $\alpha = (1, 2)(3, 4, 6)$. Ademais, é comum omitir as vírgulas quando isso não provoca ambiguidade.

Com essa notação, a multiplicação de duas permutações é feita da direita para a esquerda, como no caso de matrizes. Por exemplo,

$$(13)(27)(456) \cdot (1237)(648) = (1732)(48)(56).$$

Propriedades das permutações

Teorema 1.2.1 Toda permutação de um conjunto finito pode ser escrita como um ciclo ou como um produto de ciclos disjuntos.

Demonstração. Seja α uma permutação em $A = \{1, 2, \ldots, n\}$. Para escrever α na forma de ciclos disjuntos, começamos escolhendo qualquer elemento de A, digamos a_1, e definindo

$$a_2 = \alpha(a_1), \qquad a_3 = \alpha^2(a_1), \qquad a_4 = \alpha^3(a_1),$$

e assim por diante, até que encontremos m tal que $a_1 = \alpha^m(a_1)$. Tal m existe pois a sequência

$$a_1, \alpha(a_1), \alpha^2(a_1), \alpha^3(a_1), \ldots$$

é finita, haja vista que A é finito. Então, até o momento temos

$$\alpha = (a_1, a_2, \ldots, a_m) \cdots,$$

onde as reticências indicam a possibilidade de ainda não termos exaurido os elementos de A. Se isso acontecer, basta escolhermos $b_1 \in A$ que não aparece no ciclo dos a_i's e criar um novo ciclo usando o mesmo passo a passo acima. Note que esse novo ciclo não tem elementos em comum com o antigo, uma vez que, se tivesse, então existiriam i, j tais que

$$\alpha^i(a_1) = \alpha^j(b_1) \iff \alpha^{i-j}(a_1) = b_1 \iff b_1 = a_t,$$

para algum t, absurdo.

Procedendo desta forma até exaurirmos os elementos de A, nossa permutação terá a forma

$$\alpha = (a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_k) \cdots (c_1, c_2, \ldots, c_s),$$

demonstrando o resultado desejado. ■

Teorema 1.2.2 Se o par de ciclos $\alpha = (a_1, a_2, \ldots, a_m)$ e $\beta = (b_1, b_2, \ldots, b_n)$ não têm entradas em comum, então $\alpha\beta = \beta\alpha$.

Demonstração. Podemos dizer que α e β são permutações no conjunto

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\},$$

onde os c's são os elementos fixados por α e β (pode ser que não exista nenhum c). Para provar o resultado, vamos mostrar que $(\alpha\beta)(x) = (\beta\alpha)(x)$ para todo $x \in S$.

Se $x = a_i$ para algum i, então

$$(\alpha\beta)(a_i) = \alpha(a_i) = a_{i+1},$$

já que β fixa os a's (se $i = m$, então interpretamos a_{i+1} como a_1). Similarmente,

$$(\beta\alpha)(a_i) = \beta(a_{i+1}) = a_{i+1}.$$

Um argumento inteiramente análogo mostra que $\alpha\beta$ e $\beta\alpha$ concordam nos b's também.

Por fim, se $x = c_i$ para algum i então

$$(\alpha\beta)(c_i) = \alpha(c_i) = c_i = \beta(c_i) = (\beta\alpha)(c_i).$$

■

Teorema 1.2.3 A ordem de uma permutação em um conjunto finito escrita como produto de ciclos disjuntos é o menor múltiplo comum dos comprimentos dos ciclos.

Demonstração. Primeiro, observe que um ciclo de comprimento n tem ordem n (verifique!). Suponha então que α e β são ciclos disjuntos de comprimentos m e n, respectivamente, e seja $k = \text{mmc}(m, n)$. Segue do Teorema 1.2.1 que $\alpha^k = e = \beta^k$ e, como α e β comutam, $(\alpha\beta)^k$ também é a identidade. Portanto, pelo Corolário 1.1.10.2, temos que a ordem t de $\alpha\beta$ divide k.

Ora, mas então $\alpha^t = \beta^{-t}$, e essas duas permutações são disjuntas pois α e β são disjuntos. Logo, ambas devem ser a identidade e, portanto, $m \mid t$ e $n \mid t$. Portanto, $k \mid t$ e segue que $k = t$.

O caso do produto de mais de duas permutações disjuntas é demonstrado de maneira análoga e deixado para o leitor. ■

■ **Exemplo 1.2.2** Esse teorema pode ser usado para mostrar que as únicas ordens possíveis para os elementos de S_7 são 1, 2, 3, 4, 5, 6, 7, 10 e 12. ■

Teorema 1.2.4 Toda permutação de S_n, $n > 1$, é um produto de 2-ciclos.

Demonstração. Primeiro, note que podemos escrever $e = (12)(12)$. Pelo Teorema 1.2.1, toda permutação pode ser escrita como

$$(a_1a_1 \cdots a_k)(b_1b_2 \cdots a_t) \cdots (c_1c_2 \cdots c_s).$$

Ora, mas esse produto é igual a

$$(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)(b_1b_t)(b_1b_{t-1}) \cdots (b_1b_2)(c_1c_s)(c_1c_{s-1}) \cdots (c_1c_2),$$

e segue o resultado. ■

■ **Exemplo 1.2.3** Podemos escrever

$$(12345) = (54)(53)(52)(51)$$

ou também

$$(12345) = (54)(52)(21)(25)(23)(13).$$

■

Lema 1.2.1 Se $e = \beta_1\beta_2 \cdots \beta_r$, sendo os β_i ciclos de tamanho 2, então r é par.

Demonstração. Suponha $r > 2$. Então, $\beta_{r-1}\beta_r$ tem uma das seguintes formas:

$$e = (ab)(ab) \tag{1.1}$$
$$(ab)(bc) = (ac)(ab) \tag{1.2}$$
$$(ac)(cb) = (bc)(ab) \tag{1.3}$$
$$(ab)(cd) = (cd)(ab) \tag{1.4}$$

Se (1.1) ocorre, então $e = \beta_1\beta_2 \cdots \beta_{r-2}$ e, pelo Segundo Princípio da Indução, $r - 2$ é par e, portanto, r é par. Se (1.2), (1.3) ou (1.4) ocorre, podemos substituir o lado direito pelo lado esquerdo em e, levando a última ocorrência de a para o penúltimo ciclo da esquerda para a direita. Prosseguindo dessa maneira para reescrever os pares da forma $\beta_{i-1}\beta_i$, temos de, em algum momento, obter uma sequência com $r - 2$ ciclos de tamanho 2 porque, do contrário, teríamos

$$e = (a\star) \cdots \gamma_r$$

sendo $(a\star)$ a única ocorrência de a. Logo, a seria levado em um elemento distinto de a e teríamos um absurdo, pois e fixa todos os elementos. Portanto, devemos ter uma sequência de $r-2$ ciclos. Pelo Segundo Princípio da Indução Matemática, $r-2$ é par, logo r é par. ■

Ao invés de "ciclos de tamanho 2" ou "2-ciclos", podemos usar o termo *transposições*. De fato, essa nomenclatura é mais intuitiva, pois o que uma permutação de 2 elementos faz é trocar os dois de lugar, ou seja, transpô-los.

Vamos chamar de A_n o conjunto das permutações pares de n elementos, ou seja, as permutações de n elementos que podem ser decompostas em um produto de um número par de transposições. De fato, A_n é subgrupo de S_n, chamado subgrupo alternado, como demonstrado abaixo.

Teorema 1.2.5 $A_n \leq S_n$.

Demonstração. Se $\alpha, \beta \in A_n$, então

$$\alpha\beta^{-1} = \sigma_1\sigma_2\cdots\sigma_r\gamma_1\gamma_2\cdots\gamma_s \in A_n,$$

pois $r+s$ é par já que r e s são pares. ■

Teorema 1.2.6 Para todo $n > 1, |A_n| = \dfrac{n!}{2}$.

Demonstração. Como toda permutação pode ser escrita como produto de ciclos de tamanho 2, sabemos que se $\alpha \in S_n$, α é par ou α é ímpar.

Se α é par, então $(12)\alpha$ é ímpar. Além disso, $(12)\alpha \neq (12)\beta$ para $\alpha \neq \beta$. Logo, a quantidade de permutações pares é maior ou igual à de permutações ímpares, pois multiplicar uma permutação par por (12) gera uma permutação ímpar, mas pode não gerar **todas** as permutações ímpares.

Por outro lado, se α é ímpar, então $(12)\alpha$ é par. Novamente, $(12)\alpha \neq (12)\beta$ para $\alpha \neq \beta$. Logo, a quantidade de permutações ímpares é maior ou igual à de permutações pares, pois multiplicar uma permutação ímpar por (12) gera uma permutação par, mas pode não gerar **todas** as permutações pares.

Portanto, a quantidade de permutações pares é igual à quantidade de permutações ímpares, logo $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$. ■

1.3 Isomorfismos

Definição 1.3.1 — Isomorfismo. Um **isomorfismo** ϕ de um grupo G em um grupo $\overline{G}$ é uma aplicação bijetora ϕ de G em $\overline{G}$ que preserva a operação do grupo, isto é, tal que $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b \in G$. Nesse caso, denotamos $G \cong \overline{G}$.

Na Definição 1.3.1, no lado esquerdo da igualdade a operação é a de G, enquanto que no lado direito a operação é a de $\overline{G}$.

Teorema 1.3.1 — Teorema de Cayley. Todo grupo é isomorfo a um grupo de permutações.

Demonstração. Seja G um grupo. Para qualquer $g \in G$, defina $T_g : G \to G$ por $T_g(x) = gx, \forall x \in G$. Note que T_g é uma permutação no conjunto de elementos de G, pois cada elemento $x \in G$ é levado no elemento gx, também em G.

Agora, seja

$$\overline{G} = \{T_g | g \in G\}.$$

Então $\overline{G}$ é um grupo sob a composição. Para verificar isso, observe que para quaisquer g e h em G temos

$$T_g T_h(x) = T_g(T_h(x)) = T_g(hx) = (gh)x = T_{gh}(x),$$

logo $T_g T_h = T_{gh}$.

Daí, segue que T_e é a identidade e $(T_g)^{-1} = T_{g^{-1}}$. Como a composição é associativa, $\overline{G}$ é grupo.

Agora, podemos definir $\phi : G \to \overline{G}$ dada por $\phi(g) = T_g, \forall g \in G$. Se $T_g = T_h$, então $T_g(e) = T_h(e)$ ou, equivalentemente, $ge = he$. Então, $g = h$ e ϕ é injetora. Pela maneira que construímos $\overline{G}$, vemos que ϕ é sobrejetora. Por fim, sejam $a, b \in G$ quaisquer. Então

$$\phi(ab) = T_{ab} = T_a T_b = \phi(a)\phi(b)$$

e terminamos a demonstração. ■

Os isomorfismos têm algumas propriedades, listadas a seguir nos Teoremas 1.3.2 e 1.3.3.

Teorema 1.3.2 Valem os seguintes itens:

1. ϕ leva a identidade de G na identidade de $\overline{G}$;
2. $\forall n \in \mathbb{N}$ e $\forall a \in G, \phi(a^n) = [\phi(a)]^n$;
3. Dados $a, b \in G$ quaisquer, $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$;
4. $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$;
5. $|a| = |\phi(a)|, \forall a \in G$;
6. Dados $k \in \mathbb{Z}$ e $b \in G$, a equação $x^k = b$ tem a mesma quantidade de soluções em G que a equação $x^k = \phi(b)$ tem em $\overline{G}$;
7. Se G é finito, G e $\overline{G}$ têm o mesmo número de elementos de cada ordem.

Demonstração. **1.** Sejam e, $\overline{e}$ as identidades de G e $\overline{G}$, respectivamente. Logo, temos:

$$e = e \cdot e \Rightarrow \phi(e) = \phi(e)\phi(e)$$

Como $\phi(e) \in \overline{G}$, segue que $\phi(e) = \overline{e}$.

2. Se $n = 0$, temos $\phi(e) = \overline{e} = (\overline{e})^0$. Para $n > 0$, temos $\phi(a^n) = \underbrace{\phi(a)\phi(a)\ldots\phi(a)}_{n} = [\phi(a)]^n$. Agora, se $n < 0$, então $-n > 0$ e temos:

$$\phi(e) = \overline{e} = \phi(a^n a^{-n}) = \phi(a^n)[\phi(a)]^{-n} \Rightarrow [\phi(a)]^n = \phi(a^n)$$

3. Sejam $a, b \in G$. Temos que:

$$(\Rightarrow) \quad ab = ba \Rightarrow \phi(ab) = \phi(ba) \Rightarrow \phi(a)\phi(b) = \phi(b)\phi(a)$$

$$(\Leftarrow) \quad \phi(a)\phi(b) = \phi(b)\phi(a) \Rightarrow \phi(ab) = \phi(ba) \Rightarrow ab = ba$$

em que a volta se deve à injetividade de ϕ.

4. Seja $G = \langle a \rangle$. Como $\overline{G}$ é fechado para a sua operação, $\langle \phi(a) \rangle \subseteq \overline{G}$. Como ϕ é sobrejetora, então para todo $b \in \overline{G}$, existe k inteiro tal que $b = \phi(a^k) = [\phi(a)]^k \in \langle \phi(a) \rangle$, logo $\overline{G} \subseteq \langle \phi(a) \rangle$ e, portanto, $\overline{G} = \langle \phi(a) \rangle$.

Agora, seja $\overline{G} = \langle \phi(a) \rangle$. Como G é fechado para a sua operação, $\langle a \rangle \subseteq G$. Note que $\forall b \in G, \phi(b) \in \langle \phi(a) \rangle$, i.e., existe $k \in \mathbb{Z}$ tal que $\phi(b) = [\phi(a)]^k = \phi(a^k)$. Logo, como ϕ é injetora, $b = a^k \in \langle a \rangle$ e $G \subseteq \langle a \rangle$. Portanto, $G = \langle a \rangle$.

5. Seja $a \in G$ com $|a| = n$ e $|\phi(a)| = k$. Então:

$$\phi(a^n) = \overline{e} = [\phi(a)]^n.$$

logo $k \mid n$. Por outro lado, temos que:

$$[\phi(a)]^k = \overline{e} \Rightarrow a^k = e$$

logo $n \mid k$. Portanto, $n = k$.

6. Seja $a \in G$ tal que $a^k = b$. Então, $\phi(a^k) = [\phi(a)]^k = \phi(b)$, ou seja, se a é solução de $x^k = b$ em G, então $\phi(a)$ é solução de $x^k = b$ em $\overline{G}$. Como ϕ é injetora, $\phi(a) \neq \phi(b)$ quando $a \neq b$, ou seja, soluções diferentes da equação em G levam a soluções diferentes da equação em $\overline{G}$.

7. Como $|a| = |\phi(a)|$ para todo $a \in G$, segue que se G tem k elementos de ordem n_k, então $\overline{G}$ também terá k elementos de ordem n_k devido à injetividade de ϕ. ■

Teorema 1.3.3 Valem os seguintes itens:

1. Se ϕ é um isomorfismo de G em $\overline{G}$, então ϕ^{-1} é um isomorfismo de $\overline{G}$ em G;
2. G é abeliano se, e só se, $\overline{G}$ é abeliano;
3. G é cíclico se, e só se, $\overline{G}$ é cíclico;
4. Se K é um subgrupo de G, então $\phi(K) = \{\phi(k) \mid k \in K\}$ é um subgrupo de $\overline{G}$;
5. Se $\overline{K}$ é subgrupo de $\overline{G}$, então $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\}$ é subgrupo de G;
6. $\phi(Z(G)) = Z(\overline{G})$.

Demonstração. **1.** Como ϕ é bijetiva, ϕ^{-1} também é. Logo, basta verificarmos se ϕ^{-1} preserva a operação.

Para isso, note que

$$\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b) \iff ab = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) \iff ab = ab.$$

Logo, ϕ^{-1} de fato preserva a operação.

2. Pela propriedade 3 do Teorema 1.3.2, sabemos que $ab = ba$ se, e somente se, $\phi(a)\phi(b) = \phi(b)\phi(a)$, ou seja, os elementos de G comutam se, e só se, os elementos de $\overline{G}$ comutam.

3. O resultado segue da propriedade 4 do Teorema 1.3.2, que diz que $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$.

4. Sejam $k_1, k_2 \in K$ quaisquer. Temos que:

$$\phi(k_1)\phi(k_2^{-1}) = \phi(k_1 k_2^{-1}) \in \phi(K)$$

pois $k_1 k_2^{-1} \in K$ já que K é subgrupo.

5. Se $\overline{K}$ é subgrupo de $\overline{G}$, então para quaisquer $\phi(g_1), \phi(g_2^{-1}) \in \overline{K}$, temos:

$$\phi^{-1}(\phi(g_1))\phi^{-1}(\phi(g_2^{-1})) = \phi^{-1}(\underbrace{\phi(g_1)\phi(g_2^{-1})}_{\in \overline{K}}) \in \phi^{-1}(\overline{K}).$$

Portanto, $\phi^{-1}(\overline{K})$ é subgrupo de G.

6. Por definição, sabemos que $Z(G) = \{z \in G \mid gz = zg, \forall g \in G\}$. Daí, $\phi(Z(G)) = \{\phi(z) \in \overline{G} \mid \phi(g)\phi(z) = \phi(z)\phi(g), \forall \phi(g) \in \overline{G}\}$, que é, por definição, $Z(\overline{G})$. ■

Na Definição 1.3.1, nada nos impede de tomar $G = \overline{G}$. De fato, se o fizermos, obtemos um tipo de isomorfismo especial, chamado **automorfismo**.

Definição 1.3.2 — Autormorfismo. Um isomorfismo de um grupo G em si mesmo é chamado automorfismo. O conjunto de todos os automorfismos de um grupo G é denotado por $\mathrm{Aut}(G)$.

Além disso, podemos ainda definir um tipo especial de automorfismo, chamado **automorfismo interno**.

Definição 1.3.3 — Automorfismo Interno. O automorfismo de G definido por $\phi_a(x) = axa^{-1}$ para todo x em G é chamado automorfismo interno de G induzido por a. O conjunto de todos os automorfismos internos de um grupo G é denotado por $\mathrm{Inn}(G)$.

Um fato interessante de $\mathrm{Aut}(G)$ e $\mathrm{Inn}(G)$ é o seguinte.

Teorema 1.3.4 Os conjuntos $\mathrm{Aut}(G)$ e $\mathrm{Inn}(G)$ são grupos sob a operação de composição.

Demonstração. Sejam ϕ_a e ϕ_b elementos quaisquer de $\mathrm{Inn}(G)$. Note que $(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = a(bxb^{-1})a^{-1} = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x) \in \mathrm{Inn}(G)$, logo $\mathrm{Inn}(G)$ é fechado para a composição. Além disso, a composição é associativa, $\phi_e(x) = x$ e $(\phi_a \circ \phi_{a^{-1}})(x) = \phi_e(x)$, ou seja, $\mathrm{Inn}(G)$ tem identidade e contém os inversos. Logo, $\mathrm{Inn}(G)$ é grupo sob composição.

Agora, sejam α e β elementos quaisquer de $\mathrm{Aut}(G)$. Note que

$$\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y) \iff xy = \alpha(\alpha^{-1}(x)\alpha^{-1}(y)) \iff xy = \alpha(\alpha^{-1}(xy)) \iff xy = xy$$

logo α^{-1} preserva a operação de G. Como α^{-1} é bijetiva, então é um isomorfismo, ou seja, temos $\alpha^{-1} \in \mathrm{Aut}(G)$. Além disso, como a composição de funções é associativa, $(\alpha \circ \beta)(x) = \alpha(\underbrace{\beta(x)}_{\in G}) \in \mathrm{Aut}(G)$ e o isomorfismo $\theta(x) = x$ é a identidade, concluímos que $\mathrm{Aut}(G)$ é grupo sob composição. ■

■ **Exemplo 1.3.1** Por exemplo, se tomarmos $(\mathbb{C}^*, \cdot)$, o grupo dos complexos não nulos com a multiplicação, e definirmos a função $\phi : \mathbb{C}^* \to \mathbb{C}^*$ tal que $\phi(a+bi) = a-bi$, com $a, b \in \mathbb{R}$, então ϕ é automorfismo de $\mathbb{C}^*$.

De fato, note que se $\phi(a+bi) = \phi(c+di)$, então:

$$a = bi = c - di \iff \begin{cases} a = b \\ c = d \end{cases}$$

logo ϕ é injetora. Além disso, se $\alpha \in \mathbb{C}^*$, então existe $\beta \in \mathbb{C}^*$ tal que $\phi(\beta) = \alpha$, a saber, $\beta = \overline{\alpha}$, i.e., α e β são conjugados complexos. Logo, ϕ é sobrejetora.

Por fim, temos que

$$\begin{aligned} &\phi[(a+bi)(c+di)] = \phi[(ac-bd)+(ad+bc)i] \\ &= (ac-bd)-(ad+bc)i = (a-bi)(c-di) \\ &= \phi(a+bi)\cdot\phi(c+di). \end{aligned}$$

Logo, ϕ preserva a operação e, portanto, é automorfismo. ■

■ **Exemplo 1.3.2** Outro exemplo é o conjunto de automorfismos internos de D_4, o grupo diedral de ordem 8. Vamos mostrar que

$$\mathrm{Inn}(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\},$$

onde ϕ_{R_θ} denota a rotação de θ graus, ϕ_H denota a reflexão em torno de uma reta horizontal e ϕ_D denota a reflexão em torno da diagonal.

De fato, para tal basta mostrarmos que $\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D$ são todos distintos. Para isso, basta notar que

$$\phi_{R_0}(H) = H \neq V = \phi_{R_{90}}(H)$$
$$\phi_{R_0}(R_{90}) = R_{90} \neq R_{270} = \phi_H(R_{90})$$
$$\phi_{R_0}(R_{270}) = R_{270} \neq R_{90} = \phi_D(R_{270})$$

$$\phi_{R_{90}}(R_{90}) = R_{90} \neq R_{270} = \phi_H(R_{90})$$
$$\phi_{R_{90}}(R_{90}) = R_{90} \neq R_{270} = \phi_D(R_{90})$$
$$\phi_H(V) = V \neq H = \phi_D(V)$$

Logo, $\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D$ são, de fato, todos distintos. ∎

Em geral, dado um grupo G, não é fácil determinar $\mathrm{Aut}(G)$ e $\mathrm{Inn}(G)$. Contudo, para alguns grupos conseguimos fazê-lo com relativa facilidade. Um desses grupos é $\mathbb{Z}_n$.

Teorema 1.3.5 Temos $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$.

Demonstração. Seja $T : \mathrm{Aut}(\mathbb{Z}_n) \to U(n)$ tal que $\alpha \mapsto \alpha(1)$, ou seja, o automorfismo α é levado na imagem de 1 por α. Como $\alpha(k) = k\alpha(1)$, T é injetora, pois se $\alpha(1) = \beta(1)$, então $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$, logo $\alpha = \beta$.

Agora, seja $r \in U(n)$ e tome o automorfismo α de $\mathbb{Z}_n$ dado por $\alpha(s) = sr \pmod n$. Como $T(\alpha) = \alpha(1) = r \pmod n = r$, T é sobrejetora.

Por fim, sejam α e β elementos quaisquer de $\mathrm{Aut}(\mathbb{Z}_n)$. Então, temos:

$$T(\alpha \circ \beta) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)}) = \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)} = \alpha(1) \cdot \beta(1).$$

Logo, T preserva a operação e, portanto, é isomorfismo. ■

Outro exemplo é $\mathrm{Aut}(\mathbb{Z})$. Pela propriedade 4 do Teorema 1.3.2, um isomorfismo deve levar gerador em gerador. Como $\mathbb{Z}$ possui apenas dois geradores, 1 e -1, há apenas dois automorfismos em $\mathrm{Aut}(\mathbb{Z})$: o automorfismo identidade, que leva 1 em 1 e -1 em -1; e o automorfismo que leva 1 em -1 e -1 em 1.

Observação. Pelo Teorema 1.3.5, $|\mathrm{Aut}(\mathbb{Z}_n)| = |U(n)| = \phi(n)$ (sendo $\phi(n)$ a função totiente de Euler). Por outro lado, vemos, a partir do que fizemos acima, que $|\mathrm{Aut}(\mathbb{Z})| = 2$. Logo, em geral, $|\mathrm{Aut}(\mathbb{Z}_n)| > |\mathrm{Aut}(\mathbb{Z})|$, pois em geral $\phi(n) > 2$.

1.4 Classes laterais

Um conceito importante no estudo de grupos é o de **classes laterais**.

Definição 1.4.1 — Classe lateral. Sejam G um grupo e H um subconjunto não vazio de G. Para qualquer $a \in G$, o conjunto $\{ah \mid h \in H\}$ é denotado por aH. Analogamente, $Ha = \{ha \mid h \in H\}$ e $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Quando H é subgrupo de G, o conjunto aH é dito classe lateral à esquerda de H em G contendo a, enquanto que Ha é dito classe lateral à direita de H em G contendo a. Nesse caso, o elemento a é dito o representante da classe lateral aH (ou Ha). Usamos $|aH|$ para denotar o número de elementos no conjunto aH, e $|Ha|$ para denotar o número de elementos em Ha.

Assim como os isomorfismos, as classes laterais têm propriedades, listadas a seguir no Lema 1.4.1.

Lema 1.4.1 Valem os seguintes itens:

1. $a \in aH$ (a classe lateral à esquerda de H contendo a contém a);
2. $aH = H \iff a \in H$ (a classe lateral absorve um elemento se, e só se, esse elemento está em H);
3. $(ab)H = a(bH)$ e $H(ab) = (Ha)b$;
4. $aH = bH \iff a \in bH$ (uma classe lateral é unicamente determinada por um de seus elementos);
5. $aH = bH$ ou $aH \cap bH = \emptyset$ (duas classes laterais ou são iguais ou disjuntas);
6. $aH = bH \iff a^{-1}b \in H$ (uma questão de classe lateral se torna uma questão sobre H);
7. $|aH| = |bH|$ (todas as classes laterais têm mesmo tamanho);
8. $aH = Ha \iff H = aHa^{-1}$;
9. aH é subgrupo de G se, e só se, $a \in H$ (H é a única classe lateral que é subgrupo de G).

Demonstração. **1.** Como $e \in H$, então $a = ae \in H$.

2. Se $aH = H$, então $a \in aH = H$. Por outro lado, se $a \in H$, é claro que $aH \subseteq H$. Além disso, se $h \in H$, então $a^{-1}h \in H$, pois $a^{-1} \in H$ já que H é subgrupo. Logo, $h = (aa^{-1})h = a(a^{-1}h) \in aH$. Portanto, $H \subseteq aH$ e $H = aH$.

3. Como $(ab)h = a(bh)$ e $h(ab) = (ha)b$, o resultado segue.

4. Se $aH = bH$, então $a = ae \in aH = bH$. Por outro lado, se $a \in bH$, então $a = bh$, para algum $h \in H$, logo, $aH = (bh)H = b(hH) \overset{\mathbf{2}}{=} bH$.

5. Note que se $c \in aH \cap bH$, então $c \in aH$ e $c \in bH$, i.e., $cH = aH = bH$. Logo, se

$aH \cap bH \neq \emptyset$, $aH = bH$.

6. Temos que

$$aH = bH \iff H = (a^{-1}b)H \overset{\mathbf{2}}{\iff} a^{-1}b \in H$$

7. Se $aH = bH$, terminamos. Então, seja $f : aH \to bH$ tal que $f(x) = b^{-1}ax$. Tomando x_1 e x_2 em aH, temos que $f(x_1) = f(x_2)$ implica $x_1 = x_2$, logo f é injetiva. Além disso, tomando $a^{-1}by$ em aH, sendo $y \in bH$, temos $f(a^{-1}by) = y$, logo f é sobrejetora. Consequentemente, definimos uma bijeção de aH em bH e, portanto, $|aH| = |bH|$.

8. Note que $aH = Ha \iff (aH)a^{-1} = H(aa^{-1}) = H$, i.e., se, e só se, $aHa^{-1} = H$.

9. Se aH é subgrupo de G, então $e \in aH$. Então, $aH \cap eH \neq \emptyset$, logo $aH = eH = H$ e, por isso, $a \in H$. Por outro lado, se $a \in H, aH = H$, que é subgrupo de G. ■

Com a Definição 1.4.1 e o Lema 1.4.1, podemos enunciar o Teorema 1.4.1.

Teorema 1.4.1 — Teorema de Lagrange. Se $|G| < \infty$ e H é subgrupo de G, então a ordem de H divide a ordem de G. Ademais, a quantidade de classes laterais à esquerda (direita) de H em G é $|G|/|H|$, ou seja, a ordem de um subgrupo divide a ordem do grupo.

Demonstração. Sejam $a_1H, a_2H, \ldots, a_rH$ as classes laterais distintas à esquerda de H em G. Então, temos $aH = a_iH$ para todo a em G e algum $i = 1, 2, \ldots, r$. Pela propriedade **1** do Lema 1.4.1, $a \in aH$. Logo, temos $aH = H = a_iH$ e, daí:

$$G = \bigcup_{1 \leq i \leq r} a_iH \Rightarrow |G| = \sum_{1 \leq i \leq r} |a_iH| = \sum_{1 \leq i \leq r} |H| = r|H|.$$

Portanto, $|G|/|H| = r$. ■

Alguns resultados seguem como consequência imediata do Teorema 1.4.1.

Corolário 1.4.1.1 Em um grupo finito, a ordem de cada elemento divide a ordem do grupo.

Demonstração. Como $|a| = |\langle a \rangle|$ e $\langle a \rangle$ é um subgrupo de G, então $|a|$ divide $|G|$. ■

Observação. Muito cuidado com esse corolário! Ele afirma que, se $g \in G$ com G um grupo finito, então $|g| \mid |G|$. Isso não quer dizer que, para todo n inteiro positivo que divide $|G|$, existe um elemento de ordem n.

Corolário 1.4.1.2 Um grupo de ordem prima é cíclico.

Demonstração. Se $|G| = p$, p primo, e $a \in G$, $a \neq e$, então $|a| = |\langle a \rangle| \neq 1$ divide $|G|$, logo $|a| = p = |G|$. Portanto, $G = \langle a \rangle$. ■

Corolário 1.4.1.3 Seja G um grupo finito, $a \in G$. Então, $a^{|G|} = e$.

Demonstração. Pelo Corolário 1.4.1.1, $|G| = |a|k, k \in \mathbb{Z}_+^*$. Logo, $a^{|G|} = a^{|a|k} = e^k = e$. ■

Corolário 1.4.1.4 — Pequeno Teorema de Fermat. Para todo a inteiro e para todo primo p, $a^p \pmod p = a \pmod p$.

Demonstração. Pelo algoritmo da divisão, podemos escrever $a = pm + r, 0 \leq r < p$. Daí, $a \pmod p = r$ e só precisamos mostrar que $r^p \pmod p = r$.

Se $r = 0$, então $p \mid a$ e é claro que $r^p \pmod p = r \pmod p$.

Suponha $r > 0$. Então, $r \in U(p) = \{1, 2, \ldots, p-1\}$, sendo a operação de $U(p)$ a multiplicação módulo p. Note que $|U(p)| = p - 1$. Daí, pelo Corolário 1.4.1.3, temos que $r^{p-1} \pmod p = 1$ e, consequentemente, $r^p \pmod p = r$. ■

Teorema 1.4.2 Para dois subgrupos finitos H e K de um grupo G, seja

$$HK = \{hk \mid h \in H, k \in K\}.$$

Então, $|HK| = |H||K|/|H \cap K|$.

Demonstração. Apesar do conjunto HK ter $|H||K|$ produtos, nem todos eles são, necessariamente, distintos, isto é, podemos ter $hk = h'k'$ com $h \neq h'$ e $k \neq k'$. Para determinar $|HK|$, devemos descobrir quantas vezes isso ocorre.

Para todo t em $H \cap K$, podemos escrever $hk = (ht)(t^{-1}k)$, então cada elemento de HK pode ser representado por pelo menos $|H \cap K|$ produtos. Mas note que $hk = h'k'$ implica $t = h^{-1}h' = kk'^{-1} \in H \cap K$, logo $h' = ht$ e $k' = t^{-1}k$. Consequentemente, cada elemento em HK pode ser representado por exatamente $|H \cap K|$ produtos. Daí, $|HK| = |H||K|/|H \cap K|$, como afirmado. ■

■ **Exemplo 1.4.1** Um exemplo interessante de isomorfismo é $S_3 \cong GL(2, \mathbb{Z}_2)$. De fato, seja

$\phi : GL(2, \mathbb{Z}_2) \to S_3$, e sejam ainda

$$v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, v_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Todo elemento de $GL(2, \mathbb{Z}_2)$ permuta v_1, v_2 e v_3.

Por exemplo, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ manda v_1 em v_1, v_2 em v_3 e v_3 em v_2, ou seja, nos dá a permutação $(v_2 v_3)$.

Além disso, note que matrizes diferentes em $GL(2, \mathbb{Z}_2)$ nos dão permutações diferentes de $\{v_1, v_2, v_3\}$, logo ϕ é injetiva.

Por fim, como $|GL(2, \mathbb{Z}_2)| = 6 = |S_3|$, ϕ é sobrejetiva e, portanto, é bijetiva. Logo, é isomorfismo.

Outra demonstração possível é notar que para S_3 temos a tabela de multiplicação:

	1	(12)	(13)	(23)	(123)	(132)
1	1	(12)	(13)	(23)	(123)	(132)
(12)	(12)	1	(132)	(123)	(23)	(13)
(13)	(13)	(123)	1	(132)	(12)	(23)
(23)	(23)	(132)	(123)	1	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	1
(132)	(132)	(23)	(12)	(13)	1	(123)

Fazendo

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, j = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, k = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

obtemos a seguinte tabela de multiplicação para $GL(2, \mathbb{Z}_2)$:

	1	i	j	k	a	b
1	1	i	j	k	a	b
i	i	1	b	a	k	j
j	j	a	1	b	i	k
k	k	b	a	1	j	i
a	a	j	k	i	b	1
b	b	k	i	j	1	a

Daí, podemos ver que os dois grupos são isomorfos via $\phi : GL(2, \mathbb{Z}_2) \to S_3$ com

$$1 \mapsto 1, i \mapsto (12), j \mapsto (13), k \mapsto (23), a \mapsto (123), b \mapsto (132).$$

■

Definição 1.4.2 — Estabilizador. Seja G um grupo de permutações de um conjunto S. Para cada $i \in S$, seja $\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. Chamamos $\text{stab}_G(i)$ de estabilizador de i em G. Usamos $|\,\text{stab}_G(i)|$ para denotar o número de elementos em $\text{stab}_G(i)$.

Definição 1.4.3 — Órbita. Seja G um grupo de permutações de um conjunto S. Para cada $s \in S$, seja $\text{orb}_G(s) = \{\phi(s) \mid \phi \in G\}$. O conjunto $\text{orb}_G(s)$ é um subconjunto de S e é chamado de órbita de s sob G. Usamos $|\,\text{orb}_G(s)|$ para denotar o número de elementos em $\text{orb}_G(s)$.

Teorema 1.4.3 — Teorema Órbita-Estabilizador. Seja G um grupo finito de permutações de um conjunto S. Então, para todo i em G, $|G| = |\,\text{orb}_G(s)| \cdot |\,\text{stab}_G(i)|$.

Demonstração. Pelo Teorema 1.4.1, $|G|/|\,\text{stab}_G(i)|$ é o número de classes laterais distintas à esquerda de $\text{stab}_G(i)$ em G. Logo, para provar o teorema, basta estabelecer uma correspondência biunívoca entre as classes laterais à esquerda de $\text{stab}_G(i)$ e os elementos de $\text{orb}_G(s)$.

Para isso, definimos a correspondência T que mapeia a classe lateral $\phi\,\text{stab}_G(i)$ para $\phi(i)$.

Note que T está bem definida, pois se $\alpha\,\text{stab}_G(i) = \beta\,\text{stab}_G(i)$, então, pela propriedade 6 do Lema 1.4.1, $\alpha^{-1}\beta \in \text{stab}_G(i)$, ou seja, $(\alpha^{-1} \circ \beta)(i) = i$ e, portanto, $\alpha(i) = \beta(i)$.

Por outro lado, se $\alpha(i) = \beta(i)$, então $(\alpha^{-1} \circ \beta)(i) = i$. Logo, $\alpha^{-1}\beta \in \text{stab}_G(i)$ e, pela propriedade 6 do Lema 1.4.1, $\alpha\,\text{stab}_G(i) = \beta\,\text{stab}_G(i)$. Logo, T é injetiva.

Por fim, seja $j \in \text{orb}_G(s)$. Então $\alpha(i) = j$ para algum $\alpha \in G$ e é claro que $T(\alpha\,\text{stab}_G(i)) = \alpha(i) = j$, logo T é sobrejetiva e, portanto, é bijetiva.

Mostramos então que $|G|/|\,\text{stab}_G(i)| = |\,\text{orb}_G(i)|$, ou seja, $|G| = |\,\text{orb}_G(i)| \cdot |\,\text{stab}_G(i)|$. ■

Teorema 1.4.4 O conjunto das órbitas dos elementos de S sob um grupo G particionam S.

Demonstração. Sejam $a, b \in S$ quaisquer. É claro que $a \in \text{orb}_G(a)$ e $b \in \text{orb}_G(b)$.

Agora, seja $c \in \text{orb}_G(a) \cap \text{orb}_G(b)$. Então, $c = \alpha(a) = \beta(b)$ para algum α e algum β.

Por um lado, temos que $b = (\beta^{-1} \circ \alpha)(a)$. Logo, se $x \in \text{orb}_G(b)$, então $x = \gamma(b) = (\gamma \circ \beta^{-1} \circ \alpha)(a) \in \text{orb}_G(a)$, para algum γ, ou seja, $\text{orb}_G(b) \subseteq \text{orb}_G(a)$.

Por outro lado, temos que $a = (\alpha^{-1} \circ \beta)(b)$. Daí, se $y \in \text{orb}_G(a)$, então $y = \sigma(a) = (\sigma \circ \alpha^{-1} \circ \beta)(b) \in \text{orb}_G(b)$, para algum σ, ou seja, $\text{orb}_G(b) \supseteq \text{orb}_G(a)$.

Logo, as órbitas de elementos distintos ou são iguais ou são disjuntas. Por isso, as órbitas particionam S, mas não necessariamente particionam igualmente, i.e., não necessariamente têm

a mesma ordem. ■

Teorema 1.4.5 O grupo de rotações de um cubo é isomorfo a S_4.

Demonstração. Como o grupo de rotações de um cubo tem a mesma ordem de S_4, basta mostrar que o grupo de rotações é isomorfo a um subgrupo de S_4 (pela propriedade 5 do Teorema 1.3.3).

Para isso, note que um cubo possui 4 diagonais e o grupo de rotações no cubo induz um grupo de permutações nas diagonais. Contudo, rotações diferentes não provocam, necessariamente, permutações diferentes. Para ver que esse de fato é o caso, vamos mostrar que todas as 24 permutações são obtidas a partir das rotações.

Numerando as diagonais consecutivas com 1, 2, 3 e 4, podemos ver que existe uma rotação de 90 graus que nos dá a permutação $\alpha = (1234)$; outra rotação de 90 graus em torno de um eixo perpendicular ao nosso primeiro eixo nos dá a permutação $\beta = (1423)$.

Logo, o grupo de permutações induzido pelas rotações contém o subgrupo

$$\{e, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}$$

de 8 elementos e também contém $\alpha\beta$, que tem ordem 3.

Portanto, o grupo de permutações induzido pelas rotações tem ordem 24 (já que sua ordem deve ser divisível por 8 e por 3) sendo, por isso, isomorfo a S_4, uma vez que conseguimos obter todas as permutações das diagonais a partir das rotações α e β e suas combinações. ■

1.5 Produto direto externo de grupos

Vamos definir o produto direto externo de grupos, uma maneira de obter novos grupos a partir de grupos já conhecidos.

Definição 1.5.1 — Produto direto. Seja $\{G_1, G_2, \ldots, G_n\}$ uma coleção finita de grupos. O produto direto externo de $G_1, G_2, \ldots, G_n$, denotado por $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, é o conjunto de todas as n-tuplas para as quais o i-ésimo componente é um elemento de G_i e a operação é efetuada componente a componente.

Observação. Ao longo do texto, optamos por utilizar a notação $G \oplus H$ para denotar o produto direto de G e H. Entretanto, é mais comum encontrar a notação $G \times H$.

Teorema 1.5.1 Seja $H = \bigoplus_{i=1}^{n} G_i$, com G_i grupos. Então, H é também um grupo.

Demonstração. Sejam $a_i, b_i \in G_i$. Da Definição 1.5.1, sabemos que:

$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n) \in H$ pois cada um dos G_i é grupo.

Portanto H é fechado. Além disso, temos que:

$$\begin{aligned}(a_1, a_2, \ldots, a_n)[(b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)] &= (a_1, a_2, \ldots, a_n)(b_1c_1, b_2c_2, \ldots, b_nc_n)\\ &= ((a_1b_1)c_1, (a_2b_2)c_2, \ldots, (a_nb_n)c_n)\\ &= (a_1b_1, a_2b_2, \ldots, a_nb_n)(c_1, c_2, \ldots, c_n)\\ &= [(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)](c_1, c_2, \ldots, c_n),\end{aligned}$$

logo a associatividade se mantém em H.

Podemos ver que a identidade de H é $(e_1, e_2, \ldots, e_n)$, sendo e_i a identidade de G_i.

Por fim, basta notar que o inverso de todo elemento $(a_1, a_2, \ldots, a_n)$ em H é dado por $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$. ■

Observação. Segue da Definição 1.5.1 que $(g_1, g_2, \ldots, g_n)^k = (g_1^k, g_2^k, \ldots, g_n^k)$, ou seja, a potência "se distribui" nas entradas.

Teorema 1.5.2 — Classificação dos grupos de ordem 4. Todo grupo de ordem 4 é isomorfo a $\mathbb{Z}_4$ ou $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Demonstração. Seja $G = \{e, a, b, ab\}$. Se G não é cíclico, então $|a| = |b| = |ab| = 2$, pelo Teorema 1.4.1. Logo, podemos definir a correspondência $e \mapsto (0,0)$, $a \mapsto (1,0), b \mapsto (0,1)$, $ab \mapsto (1,1)$, que é um isomorfismo de G em $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Se G é cíclico, então é isomorfo a $\mathbb{Z}_4$, pois todo grupo cíclico de ordem n é isomorfo a $\mathbb{Z}_n$. ■

Teorema 1.5.3 Seja

$$\bigoplus_{i \leq n} G_i = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}.$$

Então, $|(g_1, g_2, \ldots, g_n)| = \text{mmc}(|g_1|, |g_2|, \ldots, |g_n|)$.

Demonstração. Sejam $s = \text{mmc}(|g_1|, |g_2|, \ldots, |g_n|)$ e $t = |(g_1, g_2, \ldots, g_n)|$.

Por um lado, temos que:

$$(g_1, g_2, \ldots, g_n)^s = (g_1^s, g_2^s, \ldots, g_n^s) = (e_1, e_2, \ldots, e_n)$$

pois s é múltiplo de cada $|g_i|$. Logo, $t \leq s$.

Por outro lado, temos que:

$$(g_1^t, g_2^t, \ldots, g_n^t) = (g_1, g_2, \ldots, g_n)^t = (e_1, e_2, \ldots, e_n)$$

logo t é um múltiplo comum de $|g_1|, |g_2|, \ldots, |g_n|$. Portanto, $s \leq t$ e concluímos que $s = t$, pelo Princípio da Tricotomia. ■

Teorema 1.5.4 Sejam G e H grupos cíclicos finitos. Então, $G \oplus H$ é cíclico se, e só se, $\text{mdc}(|G|, |H|) = 1$, isto é, $|G|$ e $|H|$ são primos entre si.

Demonstração. Sejam $|G| = m$ e $|H| = n$. Daí, $|G \oplus H| = mn$ (pelo Princípio Fundamental da Contagem). Suponha que $G \oplus H$ é cíclico e que $\langle (g, h) \rangle = G \oplus H$. Suponha que $\text{mdc}(m, n) = d$. Como $(g, h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e, e)$, temos que $mn = |(g, h)| \leq mn/d$ e, portanto, $d = 1$.

Agora, suponha que $\text{mdc}(m, n) = 1$ e $G = \langle g \rangle$ e $H = \langle h \rangle$. Então, $|(g, h)| = \text{mmc}(|g|, |h|) = \text{mmc}(m, n) \overset{\star}{=} mn = |G \oplus H|$, em que em $\star$ usamos o fato de que $\text{mmc}(a, b)\,\text{mdc}(a, b) = ab$ para quaisquer $a, b \in \mathbb{Z}$. Logo, $G \oplus H = \langle (g, h) \rangle$. ■

Corolário 1.5.4.1 Um produto externo direto $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ de um número finito de grupos cíclicos finitos é cíclico se, e só se, $|G_i|$ e $|G_j|$ são relativamente primos quando $i \neq j$.

Demonstração. Para $n = 2$ temos o Teorema 1.5.4. Suponha que o corolário vale para $n = k > 2$. Então, para $n = k + 1$, temos

$$\underbrace{G_1 \oplus G_2 \oplus \cdots \oplus G_k}_{G} \oplus \underbrace{G_{k+1}}_{H}.$$

Sejam $|G_i| = n_i$ para $i = 1, 2, \ldots, k+1$, $G = \bigoplus_{i=1}^{k} G_i$ de modo que $|G| = \prod_{i=1}^{k} n_i$ e $H = G_{k+1}$. Daí, $|G \oplus H| = \prod_{i=1}^{k+1} n_i$.

Suponha que $G \oplus H = \langle (g_1, g_2, \ldots, g_k, h) \rangle$ e que $\text{mdc}(|G|, |H|) = \text{mdc}\left(\prod_{i=1}^{k} n_i, n_{k+1}\right) = d$. Daí, temos:

$$(g_1, g_2, \ldots, g_k, h)^{\frac{1}{d}\prod_{i=1}^{k+1} n_i} = \left((g_1^{n_1})^{\frac{1}{d}\prod_{i=2}^{k+1} n_i}, \ldots, (h^{n_{k+1}})^{\frac{1}{d}\prod_{i=1}^{k} n_i}\right) = (e, e, \ldots, e).$$

Logo, $\prod_{i=1}^{k+1} n_i = |(g_1, g_2, \ldots, g_k, h)| \leq \frac{1}{d}\prod_{i=1}^{k+1} n_i$, ou seja, $d = 1$.

Como nenhum dos n_i compartilha fator primo para $i = 1, 2, 3, \ldots, k$ e $d = 1$ implica que n_{k+1} não compartilha fator primo com nenhum dos n_i, concluímos que todos os n_i são primos entre si para $i = 1, 2, 3, \ldots, k, k+1$.

Agora, suponha que $\text{mdc}\left(\prod_{i=1}^{k} n_i, n_{k+1}\right) = 1$. Daí, pela hipótese de indução, sabemos que todos os n_i são relativamente primos para $1 \leq i \leq k$. Pela nossa hipótese, n_{k+1} é relativamente primo ao produto dos n_i, que são primos entre si, logo n_{k+1} é relativamente primo a todos os n_i, isto é, $\text{mdc}(n_i, n_j) = 1$ para $i \neq j$.

Tome $G = \langle (g_1, g_2, \ldots, g_k) \rangle$ e $H = \langle h \rangle$. Então, temos:

$$|(g_1, g_2, \ldots, g_k, h)| = \text{mmc}(|g_1|, |g_2|, \ldots, |g_k|, |h|) = \text{mmc}(n_1, n_2, \ldots, n_k, n_{k+1}) \overset{\star}{=} \prod_{i=1}^{k+1} n_i = |G \oplus H|$$

em que $\star$ ressalta o fato de que como nenhum dos n_i compartilha fator primo (já que o mdc de cada par distinto é 1), então o mmc será dado pelo produto dos n_i.

Portanto, $G \oplus H = \langle (g_1, g_2, \ldots, g_k, h) \rangle$. ■

Corolário 1.5.4.2 Seja $m = \prod_{i=1}^{k} n_i$. Então $\mathbb{Z}_m$ é isomorfo a $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ se, e só se, n_i e n_j são relativamente primos quando $i \neq j$.

Demonstração. Do Corolário 1.5.4.1, sabemos que $\bigoplus_{i=n_1}^{n_k} \mathbb{Z}_{n_i}$ é cíclico se, e só se, $|\mathbb{Z}_{n_i}|$ e $|\mathbb{Z}_{n_j}|$ são primos entre si para $n_i \neq n_j$, ou seja, se, e só se, n_i e n_j são primos entre si para $i \neq j$.

Além disso, $\left|\bigoplus_{i=n_1}^{n_k} \mathbb{Z}_{n_i}\right| = \prod_{i=1}^{k} n_i = m = |\mathbb{Z}_m|$.

Logo, como todo grupo cíclico finito de ordem n é isomorfo a $\mathbb{Z}_n$, então $\bigoplus_{i=n_1}^{n_k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 n_2 \cdots n_k} = \mathbb{Z}_m$ se, e só se, $\text{mdc}(n_i, n_j) = 1$ para $i \neq j$. ■

Observação. Em [6], o Teorema 1.5.4 e o Corolário 1.5.4.1 são enunciados (de certo modo) como o seguinte teorema: o grupo $\mathbb{Z}_m \oplus \mathbb{Z}_n$ é cíclico e isomorfo a $\mathbb{Z}_{mn}$ se, e só se, $\text{mdc}(m, n) = 1$.

Lema 1.5.1 Se $\text{mdc}(s, t) = 1$, então $a \pmod{st} = b \pmod{st} \iff \begin{cases} a \pmod{s} = b \pmod{s} \\ a \pmod{t} = b \pmod{t} \end{cases}$

Demonstração. Sejam

$$a - b = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad s = \prod_{i=1}^{n} p_i^{\beta_i}, \quad t = \prod_{i=1}^{n} p_i^{\gamma_i}, \quad p_i \text{ primos }, \alpha_i, \beta_i, \gamma_i \in \mathbb{N}.$$

($\Rightarrow$) Se $a \pmod{st} = b \pmod{st}$, então $st \mid a - b$. Logo:

$$\begin{cases} s \mid a - b \\ t \mid a - b \end{cases} \Rightarrow \begin{cases} a \pmod{s} = b \pmod{s} \\ a \pmod{t} = b \pmod{t} \end{cases}$$

($\Leftarrow$) Se

$$\begin{cases} a \pmod{s} = b \pmod{s} \\ a \pmod{t} = b \pmod{t} \end{cases}$$

então $s \mid a-b$ e $t \mid a-b$. Isso é equivalente a dizer que $\beta_i \leq \alpha_i$ e $\gamma_i \leq \alpha_i$. Como $\text{mdc}(s, t) = 1$, então $\min(\beta_i, \gamma_i) = 0$, logo $\beta_i + \gamma_i \leq \alpha_i$.

Mas isso implica que $st \mid a - b$, ou seja, $a \pmod{st} = b \pmod{st}$. ■

Lema 1.5.2 $\text{mdc}(a, bc) = 1 \iff \text{mdc}(a, b) = 1 = \text{mdc}(a, c)$.

Demonstração. Sejam

$$a = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{n} p_i^{\beta_i}, \quad c = \prod_{i=1}^{n} p_i^{\psi_i}, \quad \alpha_i, \beta_i, \psi_i \in \mathbb{N}.$$

Note que mostrar que $\text{mdc}(a, bc) = 1 \iff \text{mdc}(a, b) = 1 = \text{mdc}(a, c)$ é equivalente a mostrar que $\min(\alpha_i, \beta_i + \psi_i) = 0 \iff \min(\alpha_i, \beta_i) = 0 = \min(\alpha_i, \psi_i)$.

Note que $\min(\alpha_i, \beta_i + \psi_i) = 0$ se, e só se, $\alpha_i = 0$ ou $\beta_i = \psi_i = 0$. Em ambos os casos, temos $\min(\alpha_i, \beta_i) = 0 = \min(\alpha_i, \psi_i)$. ■

Antes de prosseguir para o próximo teorema, uma definição é necessária.

Definição 1.5.2 $U_k(n) = \{x \in U(n) \mid x \pmod{k} = 1\}$.

Teorema 1.5.5 Suponha que s e t são primos entre si. Então, $U(st) \cong U(s) \oplus U(t)$. Além disso, $U_s(st) \cong U(t)$ e $U_t(st) \cong U(s)$.

Demonstração. Um isomorfismo (ϕ_1) de $U(st)$ em $U(s) \oplus U(t)$ é $x \mapsto (x \pmod{s}, x \pmod{t})$.

Um isomorfismo (ϕ_2) de $U_s(st)$ em $U(t)$ é $x \mapsto x \pmod{t}$.

Um isomorfismo (ϕ_3) de $U_t(st)$ em $U(s)$ é $x \mapsto x \pmod{s}$.

Vamos mostrar que ϕ_1 de fato é isomorfismo.

Note que se $x, y \in U(st)$, então:

$$\phi_1(xy) = (xy \ (\mathrm{mod} s), xy \ (\mathrm{mod} t)) = [(x \ \mathrm{mod} s)(y \ \mathrm{mod} s), (x \ \mathrm{mod} t)(y \ \mathrm{mod} t)] = \phi_1(x)\phi_1(y)$$

logo ϕ_1 preserva a operação.

Agora, se $(x \pmod{s}, x \pmod{t}) = (y \pmod{s}, y \pmod{t})$, então

$$\begin{cases} x \pmod{s} = y \pmod{s} \\ x \pmod{t} = y \pmod{t} \end{cases} \overset{\text{Lema 1.5.1}}{\iff} x \pmod{st} = y \pmod{st}$$

logo ϕ_1 é injetora.

Agora vamos mostrar que ϕ_1 é sobrejetora.

Seja $(a, b) \in U(s) \oplus U(t)$. Então, $\mathrm{mdc}(a, s) = 1 = \mathrm{mdc}(b, t)$. Como $\mathrm{mdc}(s, t) = 1, \exists q_1, q_2 \in \mathbb{Z} : sq_1 + tq_2 = 1$. Logo, $\mathrm{mdc}(t, q_1) = 1 = \mathrm{mdc}(s, q_2)$.

Tome $z = bsq_1 + atq_2$. Suponha que um primo p divide st. Então $p \mid s$ ou $p \mid t$. Se $p \mid s$, então $p \mid bsq_1$ mas $p \nmid atq_2$ pois $\mathrm{mdc}(s, a) = 1 = \mathrm{mdc}(s, q_2)$, o que implica que $\mathrm{mdc}(s, aq_2) = 1$ pelo Lema 1.5.2. Além disso, $\mathrm{mdc}(s, t) = 1$, logo $\mathrm{mdc}(s, atq_2) = 1$ pelo Lema 1.5.2 novamente.

Então, se $p \mid s$, $p \nmid z$.

Se $p \mid t$, então $p \mid atq_2$ mas $p \nmid bsq_1$ pois $\text{mdc}(b,t) = 1 = \text{mdc}(q_1,t)$ logo $\text{mdc}(t, bq_1) = 1$ pelo Lema 1.5.2 e, como $\text{mdc}(t,s) = 1$, então $\text{mdc}(t, bsq_1) = 1$ pelo Lema 1.5.2 novamente.

Então, se $p \mid t$, $p \nmid z$.

Logo, nenhum primo p que divide st divide z. Daí, $\text{mdc}(z, st) = 1$, ou seja, $z \in U(st)$.

Finalmente, tendo em mente que $sq_1 + tq_2 = 1$, obtemos:

$$\begin{aligned}
\phi_1(z) &= \Big((bsq_1 + atq_2) \bmod s, (bsq_1 + atq_2) \bmod t\Big) \\
&= (atq_2 \pmod s, bsq_1 \pmod t) \\
&= \Big((a - asq_1) \bmod s, (b - btq_2) \bmod t\Big) \\
&= (a \pmod s, b \pmod t)
\end{aligned}$$

logo ϕ_1 é sobrejetora.

Vamos mostrar que ϕ_2 de fato é isomorfismo.

Sejam $x, y \in U_s(st)$ quaisquer. Então, temos:

$$\phi_2(xy) = (xy) \ (\bmod t) = (x \bmod t)(y \bmod t) = \phi_2(x)\phi_2(y)$$

logo ϕ_2 preserva a operação.

Agora, suponha $x, y \in U_s(st)$ com $\phi_2(x) = \phi_2(y)$. Sabemos que $x \bmod s = 1 = y \bmod s$. Logo, temos

$$\begin{cases} \phi_2(x) = \phi_2(y) \\ x \pmod s = y \pmod s \end{cases} \iff \begin{cases} x \pmod t = y \pmod t \\ y \pmod s = y \pmod s \end{cases}$$
$$\overset{\text{Lema 1.5.1}}{\iff} x \pmod{st} = y \pmod{st},$$

logo ϕ_2 é injetora.

Agora, vamos mostrar que ϕ_2 é sobrejetora.

Seja $b \in U(t)$. Então, $\text{mdc}(b,t) = 1$. Além disso, sabemos que $\exists q_1, q_2 \in \mathbb{Z} : sq_1 + tq_2 = 1$, pois $\text{mdc}(s,t) = 1$ e também sabemos que $\text{mdc}(t, q_1) = 1 = \text{mdc}(s, q_2)$.

Tome $z = bsq_1 + tq_2$ e suponha que um primo p divide st. Então, $p \mid s$ ou $p \mid t$. Se $p \mid s$, então $p \mid bsq_1$ mas $p \nmid tq_2$, pois $\text{mdc}(s,t) = 1 = \text{mdc}(s, q_2)$, logo $\text{mdc}(s, tq_2) = 1$ pelo Lema 1.5.2.

Logo, se $p \mid s$, $p \nmid z$.

Se $p \mid t$, então $p \mid tq_2$ mas $p \nmid bsq_1$, pois $\text{mdc}(b,t) = 1 = \text{mdc}(q_1,t) = \text{mdc}(s,t)$, logo $\text{mdc}(t, bsq_1) = 1$ pelo Lema 1.5.2.

Logo, se $p \mid t$, $p \nmid z$.

Portanto, $\text{mdc}(z, st) = 1$, pois nenhum primo que divida st divide z. Além disso, note que

$$z \pmod{s} = tq_2 \pmod{s} = 1 - sq_1 \pmod{s} = 1.$$

Logo, $z \in U_s(st)$.

Finalmente, tendo em mente que $sq_1 + tq_2 = 1$, temos

$$\begin{aligned}\phi_2(z) &= (bsq_1 + tq_2) \bmod t \\ &= bsq_1 \bmod t \\ &= (b - btq_2) \bmod t \\ &= b \bmod t\end{aligned}$$

logo ϕ_2 é sobrejetora.

Vamos mostrar que ϕ_3 de fato é isomorfismo.

Sejam $x, y \in U_t(st)$ quaisquer. Então, temos:

$$\phi_3(xy) = (xy) \pmod{s} = (x \pmod{s})(y \pmod{s}) = \phi_3(x)\phi_3(y)$$

logo ϕ_3 preserva a operação.

Agora, suponha $x, y \in U_t(st)$ com $\phi_3(x) = \phi_3(y)$. Sabemos que $x \pmod{t} = 1 = y \pmod{t}$. Logo, temos:

$$\begin{cases}\phi_3(x) = \phi_3(y) \\ x \pmod{t} = y \pmod{t}\end{cases} \iff \begin{cases}x \pmod{s} = y \pmod{s} \\ y \pmod{t} = y \pmod{t}\end{cases}$$
$$\overset{\text{Lema 1.5.1}}{\iff} x \pmod{st} = y \pmod{st},$$

logo ϕ_3 é injetora.

Agora, vamos mostrar que ϕ_3 é sobrejetora.

Seja $b \in U(s)$. Então, $\text{mdc}(b, s) = 1$. Além disso, sabemos que $\exists q_1, q_2 \in \mathbb{Z} : sq_1 + tq_2 = 1$, pois $\text{mdc}(s, t) = 1$ e também sabemos que $\text{mdc}(t, q_1) = 1 = \text{mdc}(s, q_2)$.

Tome $z = sq_1 + btq_2$ e suponha que um primo p divide st. Então, $p \mid s$ ou $p \mid t$. Se $p \mid s$, então $p \mid sq_1$ mas $p \nmid btq_2$, pois $\text{mdc}(s, t) = 1 = \text{mdc}(s, q_2) = \text{mdc}(s, b)$, logo $\text{mdc}(s, btq_2) = 1$ pelo Lema 1.5.2.

Logo, se $p \mid s$, $p \nmid z$.

Se $p \mid t$, então $p \mid btq_2$ mas $p \nmid sq_1$, pois $\text{mdc}(q_1, t) = 1 = \text{mdc}(s, t)$, logo $\text{mdc}(t, sq_1) = 1$ pelo Lema 1.5.2.

Logo, se $p \mid t$, $p \nmid z$.

Portanto, $\text{mdc}(z, st) = 1$, pois nenhum primo que divida st divide z. Além disso, note que

$$z \pmod t = sq_1 \pmod t = 1 - tq_2 \pmod t = 1.$$

Logo, $z \in U_t(st)$.

Finalmente, tendo em mente que $sq_1 + tq_2 = 1$, temos

$$\begin{aligned} \phi_3(z) &= (sq_1 + btq_2) \pmod s \\ &= btq_2 \pmod s \\ &= (b - bsq_1) \pmod s \\ &= b \pmod s \end{aligned}$$

logo ϕ_3 é sobrejetora. ■

Corolário 1.5.5.1 Seja $m = \prod_{i=1}^{k} n_i$ com $\text{mdc}(n_i, n_j) = 1$ quando $i \neq j$. Então,

$$U(m) \cong \bigoplus_{i=1}^{k} U(n_i).$$

Demonstração. Para o caso $k = 2$ temos o Teorema 1.5.5. Suponha então que o corolário vale para $i = k - 1$, sendo k um inteiro maior que 3. Vamos mostrar, por indução, que o corolário vale para $i = k$. Por hipótese, sabemos que $U(n_1 n_2 \cdots n_{k-1}) \cong \bigoplus_{i=1}^{k-1} U(n_i)$. Como

$\text{mdc}\left(\prod_{i=1}^{k-1} n_i, n_k\right) = 1$, devido às condições do enunciado, temos:

$$U(m) \cong U\left(\prod_{i=1}^{k-1} n_i\right) \oplus U(n_k) \cong \bigoplus_{i=1}^{k-1} U(n_i) \oplus U(n_k) \cong \bigoplus_{i=1}^{k} U(n_i),$$

como afirmado. ■

1.6 Subgrupos normais e grupo quociente

Definição 1.6.1 — Subgrupo normal. Um subgrupo H de um grupo G é dito subgrupo **normal** de G se $aH = Ha$ para todo a em G. Denotamos isso por $H \lhd G$.

Teorema 1.6.1 Um subgrupo H de G é normal em G se, e somente se, $xHx^{-1} \subseteq H, \forall x \in G$.

Demonstração. Se H é normal em G, então para todo $x \in G$ e $h \in H$ existe $h' \in H$ tal que $xh = h'x$, ou seja, $xhx^{-1} = h'$ e, portanto, $xHx^{-1} \subseteq H$.

Agora, suponha que $xHx^{-1} \subseteq H$. Tomando $x = a$, obtemos $aH \subseteq Ha$ e, tomando $x = a^{-1}$, obtemos $Ha \subseteq aH$, logo $aH = Ha$ e, portanto, H é normal em G. ■

Note que o Teorema 1.6.1 é uma versão mais fraca da propriedade 8 do Lema 1.4.1. Por exemplo, a partir do Teorema 1.6.1, temos que todo subgrupo de um grupo abeliano é normal. Nesse caso, $ah = ha$ para a no grupo e h no subgrupo.

A partir dos grupos normais, podemos definir o quociente de dois grupos.

Teorema 1.6.2 — Grupo quociente. Seja G um grupo e H um subgrupo normal de G. O conjunto $G/H = \{aH \mid a \in G\}$ é um grupo sob a operação $(aH)(bH) = abH$. Ademais, o grupo G/H é chamado grupo fator ou grupo quociente de G por H.

Demonstração. Primeiro, vamos mostrar que a operação é bem definida. Para isso, suponha que para alguns elementos a, a', b, b' em G, $aH = a'H$ e $bH = b'H$. Daí, sabemos que $a' = ah_1$ e $b' = bh_2$, para alguns h_1, h_2 em H. Logo, $a'b'H = ah_1bh_2H = ah_1bH = ah_1Hb = aHb = abH$.

Por fim, basta notar que $a^{-1}H$ é o inverso, $eH = H$ é a identidade e $(aHbH)cH = (ab)HcH = (ab)cH = a(bc)H = aH(bcH) = aH(bHcH)$. Logo, G/H é grupo. ■

Observação. O grupo quociente de G por H é o grupo formado pelo conjunto das classes laterais à esquerda (ou direita) de H. Eles são úteis pois estudando um grupo quociente podemos obter informações acerca do grupo em si.

Teorema 1.6.3 Sejam G um grupo e $Z(G)$ o centro de G. Se $G/Z(G)$ é cíclico, então G é abeliano.

Demonstração. Note que G ser abeliano é equivalente a $Z(G) = G$, logo basta mostrar que o único elemento de $G/Z(G)$ é a classe lateral identidade $Z(G)$.

Para isso, tome $G/Z(G) = \langle gZ(G)\rangle$ e seja $a \in G$ qualquer. Daí, existe $i \in \mathbb{Z}$ tal que $aZ(G) = (gZ(G))^i = g^iZ(G)$. Logo, $a = g^iz$, para algum z em $Z(G)$. Como g^i e z comutam com g, então a comuta com g. Mas a é um elemento qualquer de G, logo todo elemento de G comuta com g, ou seja, $g \in Z(G)$.

Portanto, $gZ(G) = Z(G)$ e $G/Z(G) = \langle Z(G)\rangle$. ■

Observação. Note que essa demonstração revela que se $G/Z(G)$ é cíclico, então ele tem de ser trivial.

Observação. Essa demonstração também revela que se G/H é cíclico, sendo H um subgrupo de $Z(G)$, então G é abeliano.

Observação. Por fim, a contra-positiva do Teorema 1.6.3 é mais usada, isto é, se G não é abeliano, $G/Z(G)$ não é cíclico. Por exemplo, segue dessa sentença e do Teorema 1.4.1 que um grupo não abeliano de ordem pq, com p, q primos, deve ter um centro trivial, pois como todo grupo de ordem prima é cíclico, então $|G/Z(G)| \overset{!}{=} pq$ (pois $G/Z(G)$ não pode ser cíclico), o que implica $|Z(G)| = 1$.

Teorema 1.6.4 Para todo grupo G, $G/Z(G)$ é isomorfo a $\mathrm{Inn}(G)$.

Demonstração. Tome a correspondência $T : gZ(G) \to \phi_g$. Primeiro, vamos mostar que T é bem definida.

Para isso, suponha que $gZ(G) = hZ(G)$; daí, $h^{-1}g \in Z(G)$. Portanto, para todo x em G, $h^{-1}gx = xh^{-1}g$, logo $gxg^{-1} = hxh^{-1}$ para todo x em G e, portanto, $\phi_g = \phi_h$.

Agora, suponha que $\phi_g = \phi_h$. Então, $gxg^{-1} = hxh^{-1}$, para todo x em G, ou seja, $h^{-1}gx = xh^{-1}g$. Daí, $h^{-1}g \in Z(G)$, ou seja, $gZ(G) = hZ(G)$. Logo, T é injetora.

Pela maneira que definimos T, ela é naturalmente sobrejetora.

Por fim,

$$T[(gZ(G))(hZ(G))] = T(ghZ(G)) = \phi_{gh} = \phi_g \circ \phi_h = T(gZ(G))T(hZ(G)),$$

logo T preserva a operação. ■

Teorema 1.6.5 — Teorema de Cauchy. Seja G um grupo e p um primo que divide a ordem de G. Então, G tem um elemento de ordem p.

Demonstração. Vamos provar o teorema usando o Segundo Princípio da Indução.

Note que se G tem ordem 2, nosso teorema é satisfeito. Suponha que G tem ordem maior que 2 e que para todo grupo com ordem menor que $|G|$, o teorema é satisfeito.

Certamente G tem elementos de ordem prima, pois se $|x| = m$ e $m = qn$, com q primo, então $(x^n)^q = e$, ou seja, $|x^n| = q$, ou seja, x^n tem ordem prima q.

Então, seja x um elemento de G de ordem prima q. Se $q = p$, acabamos. Então, suponha $q \neq p$ e seja $\overline{G} = G/\langle x \rangle$.

Daí, p divide $|\overline{G}|$, pois $|\overline{G}| = |G|/q$. Por indução, pois $|\overline{G}| < |G|$, $\overline{G}$ tem um elemento de ordem p, digamos $y \cdot \langle x \rangle$.

Logo, $(y\langle x \rangle)^p = y^p\langle x \rangle = \langle x \rangle$, ou seja, $y^p \in \langle x \rangle$. Como $|\langle x \rangle| = q$, então y^p ou é a identidade ou tem ordem q, pelo Teorema 1.4.1.

Se $y^p = e$, terminamos, pois $y \in G$ e $|y| = p$. Se $(y^p)^q = e$, então $(y^q)^p = e$ e terminamos, pois $y^q \in G$ e $|y^q| = p$. ■

Definição 1.6.1. *Dizemos que G é o produto direto interno de H e K e escrevemos $G = H \times K$ se H e K são subgrupos normais de G com $G = HK$ e $H \cap K = \{e\}$.*

Mais geralmente, se $H_1, H_2, \ldots, H_n$ é uma coleção finita de subgrupos normais de G, então dizemos que G é o produto direto interno de $H_1, H_2, \ldots, H_n$ e escrevemos $G = H_1 \times H_2 \times \cdots \times H_n$ se

1. $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i\}$;
2. $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$, *para* $i = 1, 2, \ldots, n-1$.

Teorema 1.6.6 Se um grupo G é o produto direto interno de um número finito de subgrupos $H_1, H_2, \ldots, H_n$, então G é isomorfo ao produto direto externo de $H_1, H_2, \ldots, H_n$.

Demonstração. Primeiro vamos mostrar que a normalidade dos $H's$, junto com a segunda condição da Definição 1.6.1, implica na comutatividade dos $h's$. Tome $h_i \in H_i$ e $h_j \in H_j$ com $i \neq j$. Então, temos

$$(h_i h_j h_i^{-1}) h_j^{-1} \in H_j h_j^{-1} = H_j,$$
$$h_i (h_j h_i^{-1} h_j^{-1}) \in h_i H_i = H_i.$$

Então, $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j = \{e\}$, logo $h_i h_j = h_j h_i$. Além disso, vamos provar que cada elemento de G pode ser expresso unicamente na forma $h_1 \cdots h_n$, com $h_i \in H_i$. Pela condição 1 da Definição 1.6.1, sabemos que existe pelo menos uma representação. Então, suponha que $g = h_1 \cdots h_n$ e $g = h'_1 \cdots h'_n$. Daí, usando a comutatividade dos $h's$, podemos resolver a seguinte equação

$$h_1 \cdots h_n = h'_1 \cdots h'_n$$

para $h'_n h_n^{-1}$ para obter

$$h'_n h_n^{-1} = (h'_1)^{-1} h_1 \cdots (h'_{n-1})^{-1} h_{n-1}.$$

Mas então $h'_n h_n^{-1} \in H_1 \cdots H_{n-1} \cap H_n = \{e\}$, ou seja, $h'_n = h_n$. Com isso, podemos cancelar h'_n e h_n na equação acima e resolver de modo análogo para $h'_{n-1} h_{n-1}^{-1}$. Procedendo dessa maneira, concluímos que $h'_i = h_i$ para $i = 1, 2, \ldots, n$.

Com isso, podemos definir uma função ϕ de G em $\bigoplus_{i=1}^{n} H_i$ por $\phi(h_1 \cdots h_n) = (h_1, \ldots, h_n)$. Vamos mostrar que ϕ é um isomorfismo.

Note que se $\phi(h_1 \cdots h_n) = \phi(h'_1 \cdots h'_n)$, então $(h_1, \ldots, h_n) = (h'_1, \ldots, h'_n)$, ou seja, $h_i = h'_i$ para $i = 1, 2, \ldots, n$. Logo, ϕ é injetiva.

Pelo modo que definirmos ϕ, vemos que ela é naturalmente sobrejetora.

Por fim, sejam $(h_1 \cdots h_n), (h'_1 \cdots h'_n) \in G$. Daí, temos

$$\begin{aligned} \phi[(h_1 \cdots h_n)(h'_1 \cdots h'_n)] &= \phi(h_1 h'_1 \cdots h_n h'_n) \\ &= (h_1 h'_1, \ldots, h_n h'_n) \\ &= (h_1, \ldots, h_n)(h'_1, \ldots, h'_n) \end{aligned}$$

$$= \phi(h_1 \cdots h_n)\phi(h'_1 \cdots h'_n).$$

Portanto, ϕ é, de fato, isomorfismo. ■

Teorema 1.6.7 — Classificação dos grupos de ordem p^2. Todo grupo de ordem p^2, p primo, é isomorfo a $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Demonstração. Seja G um grupo de ordem p^2. Se G tem um elemento de ordem p^2, então G é cíclico e, portanto, isomorfo a $\mathbb{Z}_{p^2}$. Então, suponha que todo elemento não identidade de G tem ordem p. Vamos, primeiro, mostrar que para todo a em G, $\langle a \rangle \lhd G$.

Suponha o contrário. Então, existe $b \in G$ tal que $bab^{-1} \notin \langle a \rangle$. Logo, $\langle a \rangle$ e $\langle bab^{-1} \rangle$ são subgrupos distintos de ordem p. Note que $\langle a \rangle \cap \langle bab^{-1} \rangle = \{e\}$. Daí, as classes laterais à esquerda de $\langle bab^{-1} \rangle$ são $\langle bab^{-1} \rangle$, $a\langle bab^{-1} \rangle$, $\ldots$, $a^{p-1}\langle bab^{-1} \rangle$. Como b^{-1} deve estar em uma dessas classes, podemos escrever

$$b^{-1} = a^i(bab^{-1})^j$$

para alguns $i, j \in \mathbb{Z}$. Daí,

$$b^{-1} = a^i b a^j b^{-1} \iff e = a^i b a^j \iff b = a^{-i-j} \in \langle a \rangle$$

o que é absurdo. Portanto, para todo a em G, o subgrupo $\langle a \rangle$ é normal.

Por fim, seja x um elemento não identidade de G e y um elemento de G fora de $\langle x \rangle$. Tanto $\langle x \rangle$ quanto $\langle y \rangle$ são normais de ordem p, e sua interseção é trivial. Logo, $G = \langle x \rangle \times \langle y \rangle \cong \langle x \rangle \oplus \langle y \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$. ■

Corolário 1.6.7.1 Se G é um grupo de ordem p^2, p primo, então G é abeliano.

Demonstração. Do Teorema 1.6.7, segue que G é isomorfo a $\mathbb{Z}_{p^2}$ ou a $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Como ambos são abelianos, segue que G também é abeliano, pois isomorfismos levam grupos abelianos em grupos abelianos. ■

1.7 Homomorfismos

Definição 1.7.1 — Homomorfismo. Um **homomorfismo** ϕ de um grupo G para um grupo $\overline{G}$ é uma função de G em $\overline{G}$ que preserva a operação do grupo, isto é, $\phi(ab) = \phi(a)\phi(b), \forall a, b \in G$.

Definição 1.7.2 — Núcleo. O **núcleo** de um homomorfismo ϕ de um grupo G para um grupo com identidade e é o conjunto $\{x \in G \mid \phi(x) = e\}$, ou seja, o conjunto dos elementos que são levados na identidade. O núcleo de ϕ é denotado por $\operatorname{Ker}\phi$.

Observação. Note que, das Definições 1.3.1 e 1.7.1, temos que um isomorfismo nada mais é que um homomorfismo bijetor.

Assim como foi para isomorfismos, os homomorfismos também têm propriedades, que naturalmente são parecidas com as dos isomorfismos.

Teorema 1.7.1 Sejam ϕ um homomorfismo de G em $\overline{G}$ e $g \in G$ um elemento qualquer. Então,

1. ϕ leva a identidade de G na identidade de $\overline{G}$;
2. $\phi(g^n) = (\phi(g))^n, \forall n \in \mathbb{Z}$;
3. se $|g|$ é finita, então $|\phi(g)|$ divide $|g|$;
4. $\operatorname{Ker}\phi$ é subgrupo de G;
5. $\phi(a) = \phi(b) \iff a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$;
6. Se $\phi(g) = g'$, então $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\operatorname{Ker}\phi$.

Demonstração. **1.** Note que

$$e = ee \Rightarrow \phi(e) = \phi(e)\phi(e) \Rightarrow \phi(e) = \overline{e} \text{ sendo } \overline{e} \text{ a identidade de } \overline{G}$$

2. Para $n = 0$ a propriedade é imediata. Suponha, então, $n > 0$. Daí, temos

$$\phi(g^n) = \underbrace{\phi(g)\phi(g)\cdots\phi(g)}_{n} = (\phi(g))^n.$$

Agora, suponha $n < 0$. Daí, podemos escrever

$$\phi(e) = \phi(g^n g^{-n}) = \phi(g^n)(\phi(g))^{-n} = \overline{e} \Rightarrow \phi(g^n) = (\phi(g))^n.$$

3. Sejam $|g| = n$ e $|\phi(g)| = m$. Sabemos, então, que $\phi(e) = \phi(g^n) = (\phi(g))^n = \overline{e}$. Portanto, a ordem de $\phi(g)$ divide a ordem de g, ou seja, $m|n$. Note que a volta nem sempre é válida, pois ϕ não precisa ser injetora.

4. Sabemos que $e \in \operatorname{Ker}\phi$. Sejam $a, b \in \operatorname{Ker}\phi$. Então, sabemos que

$\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1} = \overline{e}\,\overline{e} = \overline{e} \therefore ab^{-1} \in \operatorname{Ker}\phi$ e, pelo teste do subgrupo, Ker ϕ é subgrupo de G.

5. Note que

$$\phi(a) = \phi(b) \iff (\phi(b))^{-1}\phi(a) = \overline{e} \iff b^{-1}a \in \operatorname{Ker}\phi \overset{\text{Lema } 1.4.1}{\iff} a\operatorname{Ker}\phi = b\operatorname{Ker}\phi.$$

6. Seja $x \in \phi^{-1}(g')$. Então, sabemos que

$$\phi(x) = \phi(g) \overset{5}{\iff} x\operatorname{Ker}\phi = g\operatorname{Ker}\phi \overset{\text{Lema } 1.4.1}{\iff} x \in g\operatorname{Ker}\phi \therefore \phi^{-1}(g') \subseteq g\operatorname{Ker}\phi,$$

em que foi usada a propriedade anterior na primeira equivalência. Agora, seja $k \in \operatorname{Ker}\phi$. Daí, sabemos que

$$\begin{cases} \phi(k) = \overline{e} \\ \phi(gk) = \phi(g) = g' \end{cases} \text{, ou seja, } gk \in \phi^{-1}(g') \therefore g\operatorname{Ker}\phi \subseteq \phi^{-1}(g')$$

Logo, $g\operatorname{Ker}\phi = \phi^{-1}(g')$. ■

Teorema 1.7.2 Sejam ϕ um homomorfismo de G em $\overline{G}$ e H um subgrupo de G. Então,

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ é subgrupo de $\overline{G}$
2. Se H é cíclico, então $\phi(H)$ é cíclico
3. Se H é abeliano, então $\phi(H)$ é abeliano
4. Se H é normal em G, então $\phi(H)$ é normal em $\phi(G)$
5. Se $|\operatorname{Ker}\phi| = n$, então ϕ é um mapeamento n para 1 de G em $\phi(G)$
6. Se $|H| = n$, então $|\phi(H)|$ divide n
7. Se $\overline{K}$ é um subgrupo de $\overline{G}$, então $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ é subgrupo de G
8. Se $\overline{K}$ é um subgrupo normal de $\overline{G}$, então $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ é subgrupo normal de G
9. Se ϕ é sobrejetora e $\operatorname{Ker}\phi = \{e\}$, então ϕ é um isomorfismo de G em $\overline{G}$

Demonstração. **1.** Sejam $\phi(h_1), \phi(h_2) \in \phi(H)$ quaisquer. Então, temos

$$\phi(h_1)(\phi(h_2))^{-1} = \phi(\underbrace{h_1h_2^{-1}}_{\in H}) \in \phi(H).$$

Portanto, pelo teste do subgrupo, $\phi(H)$ é subgrupo.

2. Sejam $H = \langle h_1 \rangle$, $|\phi(h_1)| = k$ e $|h_1| = n$. Por um lado, sabemos que

$$\phi(h_1^n) = (\phi(h_1))^n = \overline{e} \therefore k \mid n.$$

Por outro lado, sabemos que

$$(\phi(h_1))^k = \phi(h_1^k) = \overline{e} \Rightarrow h_1^k = e \therefore n \mid k.$$

Logo, $n = k$. Agora, basta notar que, como todo elemento de H é uma potência de h_1, então todo elemento de $\phi(H)$ é uma potência de $\phi(h_1)$, logo $\phi(H) = \langle \phi(h_1) \rangle$.

3. Sejam $h_1, h_2 \in H$. Se H é abeliano, então

$$h_1 h_2 = h_2 h_1 \Rightarrow \phi(h_1)\phi(h_2) = \phi(h_2)\phi(h_1).$$

Logo, $\phi(H)$ é abeliano. Note que a volta nem sempre é verdadeira, pois ϕ não é injetora, necessariamente.

4. Se H é normal em G, então existem $h_1, h_2 \in H$ tais que, para todo $g \in G$, $gh_1 = h_2 g$. Daí, sendo $\phi(g) = g'$, temos

$$\phi(g)\phi(h_1) = \phi(h_2)\phi(g) \Rightarrow g'\phi(h_1) = \phi(h_2)g' \Rightarrow g'\phi(H) = \phi(H)g' \therefore \phi(H) \lhd \phi(G).$$

5. Sejam $e = x_1, x_2, \ldots, x_n$ os elementos de $\operatorname{Ker}\phi$. Seja ainda $g \in G$ qualquer. Note que para todo $i = 1, 2, \ldots, n$, $\phi(x_i g) = \phi(g)$, ou seja, há n elementos que são enviados para $\phi(g)$, a saber $g, x_2 g, \ldots, x_n g$.

6. Seja ϕ_H a restrição de ϕ aos elementos de H. Então, ϕ_H é um homomorfismo de H em $\phi(H)$. Suponha que $|\operatorname{Ker}\phi_H| = t$. Então, pela propriedade 5, ϕ_H é um mapeamento t para 1, logo $|\phi(H)|t = |H| = n$, ou seja, $|\phi(H)|$ divide n.

7. Note que e pertence a $\phi^{-1}(\overline{K})$. Agora, sejam $k_1, k_2 \in \phi^{-1}(\overline{K})$. Então, por definição, sabemos que $\phi(k_1), \phi(k_2) \in \overline{K}$. Note que $\phi(k_1 k_2^{-1}) = \phi(k_1)(\phi(k_2))^{-1} \in \overline{K}$, pois $k_1 k_2^{-1} \in G$ e $\phi(k_1), (\phi(k_2))^{-1} \in \overline{K}$. Logo, por definição, $k_1 k_2^{-1} \in \phi^{-1}(\overline{K})$.

8. Vamos usar o Teorema 1.6.1. Basta mostrar que $x\phi^{-1}(\overline{K})x^{-1} \subseteq \phi^{-1}(\overline{K})$, para todo x em G. Note que todo elemento em $x\phi^{-1}(\overline{K})x^{-1}$ tem a forma xkx^{-1}, sendo $\phi(k) \in \overline{K}$. Como $\overline{K} \lhd \overline{G}$, então $\phi(xkx^{-1}) = \phi(x)\phi(k)(\phi(x))^{-1}$ deve pertencer a $\overline{K}$. Como $xkx^{-1} \in G$, então de fato $xkx^{-1} \in \phi^{-1}(\overline{K})$

9. Como $|\operatorname{Ker}\phi| = 1$, sabemos, pela propriedade 5, que ϕ é injetora. Como, por hipótese, ϕ é sobrejetora e, por definição ϕ preserva a operação, concluímos que ϕ é isomorfismo. ■

A propriedade 8 do Teorema 1.7.2 tem um caso especial interessante, a saber quando $\overline{K} = \{\overline{e}\}$.

Corolário 1.7.2.1 Seja ϕ um homomorfismo de G em $\overline{G}$. Então, $\operatorname{Ker}\phi \lhd G$.

Demonstração. Tomando $\overline{K}$ trivial na propriedade 8, obtemos o fato de que $\phi^{-1}(\overline{e}) = \operatorname{Ker}\phi$ é normal em G. ■

■ **Exemplo 1.7.1** Usando as propriedades dos homomorfismos, vamos determinar todos os homomorfismos de $\mathbb{Z}_{12}$ em $\mathbb{Z}_{30}$. Pela propriedade 2 do Teorema 1.7.1, sabemos que os homomorfismos são completamente definidos pela imagem de 1, ou seja, se 1 é mapeado em a, então x é mapeado em xa. Pelo Teorema 1.4.1, $|a|$ divide 30 e, pela propriedade 3 do Teorema 1.7.1, $|a|$ divide 12. Daí, $|a| = 1, 2, 3$ ou 6. Agora, temos de ver quais elementos de $\mathbb{Z}_{30}$ têm tais ordens. Podemos ver que $a = 0, 15, 10, 20, 5$ ou 25. Cada uma dessas seis correspondências nos dá uma aplicação bem definida e que preserva a operação. ■

■ **Exemplo 1.7.2** Outro exemplo é entre S_n e $\mathbb{Z}_2$. A função de S_n em $\mathbb{Z}_2$ que leva uma permutação par para 0 e uma permutação ímpar para 1 é um homomorfismo. Para mostrar isso, basta notar que se a, b são duas permutações quaisquer de S_n, então ab ou é par ou é ímpar. Se ab é par, então a e b ou são ambos pares ou ambos ímpares. Se ambos são pares, $\phi(ab) = 0 = 0 + 0 = \phi(a) + \phi(b)$. Se ambos são ímpares, $\phi(ab) = 0 = 1 + 1 = \phi(a) + \phi(b)$. Por fim, se ab é ímpar, podemos assumir, sem perda de generalidade, que a é ímpar e b é par. Daí, $\phi(ab) = 1 = 1 + 0 = \phi(a) + \phi(b)$. ■

Teorema 1.7.3 — Primeiro Teorema dos Isomorfismos. Seja ϕ um homomorfismo de G em $\overline{G}$. Então, a correspondência de $G/\operatorname{Ker}\phi$ para $\phi(G)$ dada por $g\operatorname{Ker}\phi \to \phi(g)$, é um isomorfismo. Em símbolos, $G/\operatorname{Ker}\phi \cong \phi(G)$.

Demonstração. Seja ψ tal correspondência. Pela propriedade 5 do Teorema 1.7.1, ψ é bem definida e injetora. Para mostrar que ψ preserva a operação, basta notar que para quaisquer $x, y \in G$, temos

$$\psi(x\operatorname{Ker}\phi y\operatorname{Ker}\phi) = \psi(xy\operatorname{Ker}\phi) = \phi(xy) = \phi(x)\phi(y) = \psi(x\operatorname{Ker}\phi)\psi(y\operatorname{Ker}\phi).$$

Como todo $\phi(g)$ em $\phi(G)$ é atingido por algum elemento de $G/\operatorname{Ker}\phi$, a saber $g\operatorname{Ker}\phi$, então ψ é sobrejetora e, portanto, isomorfismo. ■

Usando o Teorema 1.4.1, a propriedade 1 do Teorema 1.7.2 e o Teorema 1.7.3, podemos provar o seguinte corolário.

Corolário 1.7.3.1 Se ϕ é um homomorfismo de um grupo finito G em outro grupo finito $\overline{G}$, então $|\phi(G)|$ divide $|G|$ e $|\overline{G}|$.

Demonstração. Do Teorema 1.7.3, sabemos que $G/\operatorname{Ker}\phi \cong \phi(G)$, ou seja, $|G/\operatorname{Ker}\phi| = |\phi(G)|$. Daí, sabemos que $|G| = |\phi(G)| \cdot |\operatorname{Ker}\phi|$, portanto $|\phi(G)|$ divide $|G|$. Agora, usando a propriedade 1 do Teorema 1.7.2, sabemos que $\phi(G)$ é subgrupo de $\overline{G}$. Consequentemente, pelo Teorema 1.4.1, $|\phi(G)|$ divide $|\overline{G}|$. ■

Com o Teorema 1.7.3 podemos mostrar que $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$. Para isso, considere a função ϕ definida por $\phi(m) = m \pmod n$. Podemos ver que todos os múltiplos de n são levados na identidade, ou seja, $\operatorname{Ker}\phi = \langle n\rangle$. Então, do Teorema 1.7.3, $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$, uma vez que $\phi(\mathbb{Z}/\langle n\rangle) = \mathbb{Z}_n$.

Teorema 1.7.4 $N(H)/C(H)$ é isomorfo a um subgrupo de $\operatorname{Aut}(H)$.

Demonstração. Seja H um subgrupo de G e lembre-se que o normalizador de H em G é $N(H) = \{x \in G \mid xHx^{-1} = H\}$ e que o centralizador de H em G é $C(H) = \{x \in G \mid xhx^{-1} = h, \forall h \in H\}$. Considere o mapeamento de $N(H)$ em $\operatorname{Aut}(H)$ dado por $g \mapsto \phi_g$, em que ϕ_g é o automorfismo interno de H induzido por g (ou seja, $\phi_g(h) = ghg^{-1}, \forall h \in H$). Esse mapeamento é um homomorfismo (pois se γ é tal aplicação, então $\gamma(g_1g_2) = \phi_{g_1g_2} = \phi_{g_1} \circ \phi_{g_2} = \gamma(g_1)\gamma(g_2)$) com núcleo $C(H)$ (pois o núcleo é o conjunto dos g tais que $ghg^{-1} = h, \forall h \in H$, que é $C(H)$, por definição). Daí, do Teorema 1.7.3, temos $N(H)/C(H)$ isomorfo a um subgrupo de $\operatorname{Aut}(H)$. ■

Teorema 1.7.5 Todo subgrupo normal de um grupo G é o núcleo de um homomorfismo de G. Em particular, um subgrupo normal N é núcleo do homomorfismo $g \mapsto gN$ de $G \to G/N$. Tal homomorfismo é chamado **homomorfismo natural** de G em G/N.

Demonstração. Seja $\gamma : G \underset{g \mapsto gN}{\to} G/N$. Note que $\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y)$, logo γ é homomorfismo. Além disso, note que se g é um elemento qualquer de $\operatorname{Ker}\gamma$, então $gN = \gamma(g) = N$ que, pela propriedade 2 do Lema 1.4.1, é verdade se, e só se, $g \in N$. Logo, todo elemento do núcleo é, na verdade, elemento de N e vice-versa. Portanto, $N = \operatorname{Ker}\gamma$. ■

Assim como foi o caso com grupos quocientes, as imagens homomórficas de um grupo nos dizem

algumas propriedades do grupo original. Uma medida da similaridade entre um grupo e sua imagem homomórfica é o tamanho do núcleo. Se o núcleo é a identidade, então a imagem de G nos diz tudo sobre G (uma vez que ambos são isomorfos). Por outro lado, se o núcleo é o próprio grupo, então a imagem não nos diz nada sobre G. Entre esses dois extremos, alguma parte da informação sobre G é preservada e outra é perdida. A utilidade de um homomorfismo particular é preservar propriedades que queremos e descartar propriedades desnecessárias. Desse modo, substituímos G por um grupo mais simples de estudar, mas que possui as características essenciais de G em que estamos interessados.

■ **Exemplo 1.7.3** Por exemplo, se G tem ordem 60 e uma imagem homomórfica cíclica de ordem 12, então sabemos (pelas propriedades 5, 7 e 8 do Teorema 1.7.2) que G tem subgrupos normais de ordens 5, 10, 15, 20, 30 e 60. Para ilustrar melhor, suponha que quiséssemos encontrar um grupo infinito que é dado pela união de três subgrupos próprios. Podemos tornar o problema mais simples encontrando, primeiro, um grupo finito que é a união de três subgrupos próprios. Notando que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ é a união de $H_1 = \langle 1, 0\rangle$, $H_2 = \langle 0, 1\rangle$ e $H_3 = \langle 1, 1\rangle$, encontramos nosso grupo finito. Agora, precisamos encontrar um grupo infinito cuja imagem homomórfica é $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ e pegar as imagens inversas de H_1, H_2 e H_3. Podemos ver que o mapeamento de $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}$ em $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ dado por $\phi(a, b, c) = (a, b)$ satisfaz nossas condições e, portanto, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}$ é a união de $\phi^{-1}(H_1) = \{(a, 0, c) \mid a \in \mathbb{Z}_2, c \in \mathbb{Z}\}$, $\phi^{-1}(H_2) = \{(0, b, c) \mid b \in \mathbb{Z}_2, c \in \mathbb{Z}\}$ e $\phi^{-1}(H_3) = \{(a, a, c) \mid a \in \mathbb{Z}_2, c \in \mathbb{Z}\}$. ■

Apesar de serem parecidos, homomorfismos e isomorfismos desempenham papeis diferentes. Enquanto isomorfismos nos permitem olhar de um modo diferente para um grupo, homomorfismos agem como ferramentas investigativas. Em certas áreas de Teoria dos Grupos (especialmente nas aplicações à Física e à Química), geralmente queremos saber todas as imagens homomórficas de um grupo, mas sendo essas imagens grupos de matrizes sobre os complexos (chamadas representações de grupos).

Antes de definir produto semidireto, seja N um subgrupo normal de G. Cada elemento g de G define um automorfismo $n \mapsto gng^{-1}$ de N e isso define um homomorfismo

$$\theta : G \to \mathrm{Aut}(N),\ g \mapsto i_g|_N.$$

Se existe um subgrupo Q de G tal que $G \to G/N$ mapeia Q isomorficamente em G/N, então podemos reconstruir G a partir de N, Q e a restrição de θ a Q. De fato, um elemento g de G pode ser escrito de forma única na forma

$$g = nq,\ n \in N,\ q \in Q,$$

onde q deve ser o único elemento de Q sendo mapeado em $gN \in G/N$, e n deve ser gq^{-1}. Logo, temos uma correspondência injetiva entre os conjuntos G e $N \oplus Q$.

Se $g = nq$ e $g' = n'q'$, então

$$gg' = (nq)(n'q') = n(qn'q^{-1})qq' = n \cdot \theta_q(n') \cdot qq'.$$

Definição 1.7.3 — Produto semidireto. Um grupo G é o produto semidireto de seus subgrupos N e Q se N é normal e o homomorfismo $G \to G/N$ induz um isomorfismo $Q \to G/N$. Equivalentemente, G é o produto semidireto de N e Q se

$$N \lhd Q,\ NQ = G,\ N \cap Q = \{1\}\,.$$

Note que Q não precisa ser normal em G. Quando G é o produto semidireto de N e Q, escrevemos $G = N \rtimes Q$ ou ainda $G = N \rtimes_\theta Q$.

Se um grupo G é produto semidireto de dois grupos cíclicos, então G é dito **metacíclico**. Em outras palavras, um grupo G é **metacíclico** se existe um subgrupo normal N de G tal que N e G/N são grupos cíclicos.

■ **Exemplo 1.7.4** Por exemplo, em D_n, $n \geq 2$, sejam $C_n = \langle r \rangle$ e $C_2 = \langle s \rangle$, sendo r uma rotação de $2\pi/n$ em torno do centro do polígono e s uma reflexão em torno da reta que liga o vértice 1 ao centro do polígono. Nesse caso, temos

$$D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes_\theta C_2,$$

com $\theta_s(r^i) = r^{-i}$. ■

■ **Exemplo 1.7.5** O grupo alternado A_n é normal em S_n (pois tem índice 2) e $C_2 = \{(12)\}$ é isomorfo a S_n/A_n. Portanto, $S_n = A_n \rtimes C_2$. ■

■ **Exemplo 1.7.6** Um grupo cíclico de ordem p^2, p primo, não pode ser escrito como produto semidireto, uma vez que tem apenas um subgrupo de ordem p e seriam necessários 2. ■

■ **Exemplo 1.7.7** Seja $G = GL(n, \mathbb{F})$. Seja B o subgrupo de matrizes triangulares superiores em G, T o subgrupo de matrizes diagonais em G e U o subgrupo de matrizes triangulares superiores com coeficientes diagonais unitários. Então, para $n = 2$,

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},\ T = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\},\ U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$$

Então, $U \lhd B$, $UT = B$ e $U \cap T = \{1\}$. Logo,

$$B = U \rtimes T.$$

Note que para $n \geq 2$, T não é normal em B e, portanto

$$B \neq T \rtimes U.$$

■

Vimos que, a partir de um produto semidireto $G = N \rtimes Q$, obtemos a terna

$$(N, Q, \theta : Q \to \mathrm{Aut}(N))$$

e que essa terna determina G. Agora, vamos mostrar que toda terna (N, Q, θ) consistindo de dois grupos N e Q e um homomorfismo $\theta : Q \to \mathrm{Aut}(N)$ surge de um produto semidireto. Então, seja $G = N \times Q$ e defina

$$(n, q)(n', q') = (n \cdot \theta_q(n'), qq').$$

Proposição 1.7.1 A lei de composição acima torna G em um grupo, de fato, o produto semidireto de N e Q. ■

Demonstração. A partir da lei de composição, temos

$$((n, q)(n', q'))(n'', q'') = (n\theta_q(n'), qq')(n'', q'') = (n \cdot \theta_q(n') \cdot \theta_{qq'}(n''), qq'q'') = (n, q)((n', q')(n'', q''))$$

e, portanto, a associatividade vale. Como $\theta_1(1) = 1$ e $\theta_q(1) = 1$,

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1)$$

e, portanto, $(1, 1)$ é a identidade. Por fim,

$$(n, q)(\theta_{q^{-1}}(n^{-1}), q^{-1}) = (1, 1) = (\theta_{q^{-1}}(n^{-1}), q^{-1})(n, q)$$

e, portanto, $(\theta_{q^{-1}}(n^{-1}), q^{-1})$ é o inverso de (n, q). Portanto, G é um grupo e, como $N \lhd G$, $NQ = G$ e $N \cap Q = \{1\}$, segue que $G = N \rtimes Q$. Além disso, quando N e Q são pensados como subgrupos de G, a ação de Q em N é dada por θ. ■

O produto direto pode ser pensado como um produto semidireto. De fato, a bijeção

$$(n, q) \mapsto (n, q) : N \times Q \to N \rtimes_\theta Q$$

é um isomorfismo de grupos se, e só se, θ é o homomorfismo trivial $Q \to \mathrm{Aut}(N)$, i.e., $\theta_q(n) = n$ para todo $q \in Q, n \in N$.

Podemos usar o produto semidireto para construir grupos de ordem p^3. De fato, seja $N = \langle a \rangle$ cíclico de ordem p^2 e seja $Q = \langle b \rangle$ cíclico de ordem p, sendo p um primo ímpar. Então $\mathrm{Aut}(N) \cong C_{p-1} \times C_p$ e C_p é gerado por $\alpha : a \mapsto a^{1+p}$ (note que $\alpha^2(a) = a^{1+2p}$). Defina $Q \to \mathrm{Aut}(N)$ por $b \mapsto \alpha$. O grupo $G = N \rtimes_\theta Q$ tem geradores a, b e relações

$$a^{p^2} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p}. \tag{1.5}$$

G é um grupo não comutativo de ordem p^3, e possui um elemento de ordem p^2.

Por outro lado, sejam $N = \langle a, b \rangle$ o produto de dois grupos cíclicos $\langle a \rangle$ e $\langle b \rangle$ de ordem p e $Q = \langle c \rangle$ um grupo cíclico de ordem p. Defina $\theta : Q \to \mathrm{Aut}(N)$ como o homomorfismo tal que

$$\theta_{c^i}(a) = ab^i,\ \theta_{c^i}(b) = b.$$

O grupo $G = N \rtimes_\theta Q$ é um grupo de ordem p^3 com geradores a, b, c e relações

$$a^p = b^p = c^p = 1,\ ab = cac^{-1},\ ab = ba,\ bc = cb. \tag{1.6}$$

Como $b \neq 1$, a relação $ab = cac^{-1}$ mostra que G não é comutativo. Quando p é ímpar, todo elemento não trivial tem ordem p. Quando $p = 2$, $G \cong D_4$, que tem um elemento de ordem 2^2. Note que isso mostra que um grupo pode ter representações bem diferentes como produto semidireto:

$$D_4 \cong C_4 \rtimes C_2 \cong (C_2 \times C_2) \rtimes C_2.$$

Para um primo ímpar p, um grupo não comutativo (ou não abeliano) de ordem p^3 é isomorfo ao grupo em (1.5) se possui elemento de ordem p^2 e isomorfo ao grupo em (1.6) se não possui elemento de ordem p^2. Em particular, há exatamente dois grupos não abelianos de ordem p^3, a menos de isomorfismo.

Capítulo 2

Grupos livres

"Mathematics is not about numbers, equations, computations, or algorithms: it is about understanding."

— William Paul Thurston

2.1 Introdução

Primeiramente, vamos introduzir algumas definições e notações. Para qualquer conjunto $S = \{a, b, c, \dots\}$ de símbolos distintos, criamos o novo conjunto $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, \dots\}$ substituindo cada x em S por x^{-1}. Defina o conjunto $W(S)$ como a coleção de todas as sequências finitas da forma $x_1 x_2 \cdots x_k$, sendo $x_i \in S \cup S^{-1}$. Os elementos de $W(S)$ são chamados *palavras* de S. A sequência com nenhum símbolo está em $W(S)$ e é chamada *palavra vazia*, denotada por e.

Podemos definir uma operação binária em $W(S)$ por justaposição, isto é, se $x_1 x_2 \cdots x_k$ e $y_1 y_2 \cdots y_t$ pertencem a $W(S)$, então $x_1 x_2 \cdots x_k y_1 y_2 \cdots y_t$ também pertence. Observe que a operação é associativa e que a palavra vazia é a identidade. Além disso, note que uma palavra como aa^{-1} não é, a priori, a identidade, porque estamos tratando os elementos de $W(S)$ como símbolos formais sem nenhum significado implícito.

Agora, temos tudo para definir um grupo com $W(S)$, exceto inversos. Aqui encontramos uma dificuldade, pois $abb^{-1}a^{-1}$ não é a palavra vazia a priori, apenas uma sequência de símbolos sem nenhum significado particular. Por isso, utilizamos classes de equivalências.

Definição 2.1.1 — Classes de equivalências de palavras. Para quaisquer pares u e v de $W(S)$, dizemos que u está relacionado a v se v pode ser obtido a partir de u através de uma sequência finita de inserções ou exclusões de palavras da forma xx^{-1} ou $x^{-1}x$, $x \in S$.

Vamos mostrar que essa relação é uma relação de equivalência em $W(S)$.

Demonstração. Seja u uma palavra de S. Sabemos que u está relacionado a u, pois podemos obter u de u sem fazer nenhuma inserção nem exclusão (ou seja, $u \sim u$). Agora, se u está relacionado a v, então podemos obter u a partir de v inserindo ou excluindo elementos da forma xx^{-1} ou $x^{-1}x$. Portanto, basta realizar o processo inverso para obter v a partir de u (ou seja, $u \sim v$ implica $v \sim u$). Por fim, se u pode ser obtido de v e v pode ser obtido de w, então, para obter u de w basta primeiro obter v de w e, em seguida, obter u de v (ou seja, $u \sim v$ e $v \sim w$ implica $u \sim w$). ■

Por exemplo, podemos ter $S = \{a, b, c\}$. Então, $acc^{-1}b$ é equivalente a ab; $aab^{-1}bbaccc^{-1}$ é equivalente a $aabac$; $a^{-1}aabb^{-1}a^{-1}$ é equivalente à palavra vazia e a palavra $ca^{-1}b$ é equivalente a $cc^{-1}caa^{-1}a^{-1}bbca^{-1}ac^{-1}b^{-1}$.

Teorema 2.1.1 — Grupo livre. Seja S um conjunto de símbolos distintos. Para qualquer palavra u em $W(S)$, seja $\overline{u}$ o conjunto de todas as palavras de $W(S)$ que são equivalentes a u (ou seja, $\overline{u}$ é a classe de equivalência contendo u). Então, o conjunto de todas as classes de equivalência de elementos de $W(S)$ é um grupo sob a operação $\overline{u} \cdot \overline{v} = \overline{uv}$.

Demonstração. Se u e v são duas palavras de S, então uv também é. Daí, é claro que $\overline{u} \cdot \overline{v} = \overline{uv}$, logo nosso conjunto é fechado para essa operação. Podemos ver que a identidade é a classe $\overline{e}$ (ou seja, o conjunto de palavras equivalentes à palavra vazia). Agora, sejam u, v e w palavras distintas de S. Então, note que

$$(\overline{u} \cdot \overline{v}) \cdot \overline{w} = \overline{uv} \cdot \overline{w} = \overline{uvw} = \overline{u} \cdot (\overline{vw}) = \overline{u} \cdot (\overline{v} \cdot \overline{w}).$$

Logo, a operação é associativa. Por fim, o inverso de $\overline{u}$ é a classe de equivalência da palavra v que, justaposta com u, nos dá uma palavra equivalente à palavra vazia. Em símbolos, se $uv \sim e$, então $\overline{u} \cdot \overline{v} = \overline{e}$ e $\overline{v}$ é o inverso de $\overline{u}$. ■

Teorema 2.1.2 — Propriedade do mapeamento universal. Todo grupo é imagem homomórfica de um grupo livre.

Demonstração. Sejam G um grupo, S o conjunto dos geradores de G (tal conjunto existe pois podemos tomar $S = G$) e F o grupo livre em S. Para maior claridade, vamos denotar a palavra $x_1x_2 \cdots x_n$ em $W(S)$ por $(x_1x_2 \cdots x_n)_F$ e o produto em G por $(x_1x_2 \cdots x_n)_G$. Além disso, assim como antes, $\overline{x_1x_2 \cdots x_n}$ é a classe de equivalência em F contendo $(x_1x_2 \cdots x_n)_F$.

Agora, considere a correspondência $\phi : F \to G$ dada por:

$$\phi(\overline{x_1x_2 \cdots x_n}) = (x_1x_2 \cdots x_n)_G.$$

Podemos ver que ϕ está bem definida, uma vez que inserir ou deletar expressões da forma xx^{-1} ou $x^{-1}x$ na palavra equivale a inserir ou deletar identidades no produto em G. Agora, para verificar que ϕ preserva a operação, basta notar que

$$\begin{aligned}\phi[(\overline{x_1x_2\cdots x_n})(\overline{y_1y_2\cdots y_m})] = \phi(\overline{x_1x_2\cdots x_ny_1y_2\cdots y_m}) = \\ =(x_1\cdots x_ny_1\cdots y_m)_G = (x_1\cdots x_n)_G(y_1\cdots y_m)_G,\end{aligned}$$

e finalizamos a demonstração. ■

Corolário 2.1.2.1 Todo grupo é isomorfo a um grupo quociente de um grupo livre.

Demonstração. Do Teorema 1.7.3, sabemos que $F/\operatorname{Ker}\phi \cong \phi(F)$, sendo $\phi(F)$ um subgrupo de G. Como S gera G, então a nossa aplicação ϕ é sobrejetora. Portanto, $\phi(F) = G$ e, consequentemente, $F/\operatorname{Ker}\phi \cong G$. ■

Definição 2.1.2 — Geradores e relações. Seja G um grupo gerado por um subconjunto $A = \{a_1, a_2, \ldots, a_n\}$ e seja F o grupo livre em A. Seja $W = \{w_1, w_2, \ldots, w_t\}$ um subconjunto de F e seja N o menor subgrupo normal de F contendo W. Dizemos que G é dado pelos geradores $a_1, a_2, \ldots, a_n$ e pelas relações $w_1 = w_2 = \cdots = w_t = e$ se existe um isomorfismo de F/N em G que leva a_iN para a_i. A notação para essa situação é

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e\rangle.$$

Note que restringimos o número de geradores e relações a um número finito, mas isso não é necessário. Além disso, geralmente é mais conveniente escrever as relações na forma implícita. Por exemplo, a relação $a^{-1}b^{-3}ab = e$ é usualmente escrita como $ab = b^3a$. Na prática, não escrevemos o subgrupo normal N que contém as relações. Em vez disso, manipulamos os geradores e tratamos qualquer coisa em N como a identidade. Ao invés de dizer que G é dado por

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e\rangle,$$

muitos autores preferem dizer que G tem a apresentação

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e\rangle.$$

Note que um grupo livre é "livre" de relações, isto é, a classe de equivalência contendo a palavra vazia é a única relação. Um fato interessante é que todo subgrupo de um grupo livre também é livre: esse é o chamado **Teorema de Nielsen-Schreier**. Além disso, grupos livres são fundamentais para a Teoria Combinatória dos Grupos, um dos ramos da Álgebra.

■ **Exemplo 2.1.1** Por exemplo, podemos escrever

$$D_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = e \rangle \tag{2.1}$$

sendo D_4 o grupo diedral de ordem 8. ■

■ **Exemplo 2.1.2** Outro exemplo é o grupo dos quatérnios, aqui denotado por Q_8, que tem apresentação

$$Q_8 = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle. \tag{2.2}$$

■

■ **Exemplo 2.1.3** Vamos chamar de $\mathcal{Q}(+)$ o grupo dos racionais com a adição. Observe que os elementos da forma

$$x_n = \frac{1}{n!},\ n \in \mathbb{N}$$

geram $\mathcal{Q}(+)$. De fato, se $\frac{a}{b} \in \mathcal{Q}(+)$, sendo $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, temos que

$$\frac{a}{b} = \frac{a(b-1)!}{b(b-1)!} = a(b-1)! \cdot x_b.$$

Como x_n satisfaz a seguinte igualdade

$$nx_n = x_{n-1},$$

então é razoável assumir que $\mathcal{Q}(+)$ tem apresentação, escrita na forma multiplicativa, dada por

$$P = \langle x_n, n \geq 1 \mid x_n^n = x_{n-1}, n \geq 2 \rangle.$$

Como quaisquer dois pares de geradores de P comutam, já que um é potência do outro, então P é abeliano. Por conveniência, podemos usar a notação aditiva:

$$\mathcal{Q}(+) = \langle x_n, n \geq 1 \mid nx_n = x_{n-1}, n \geq 2 \rangle. \tag{2.3}$$

De fato, a apresentação em (2.3) é uma apresentação de $\mathcal{Q}(+)$. Note que ela é o nosso primeiro exemplo de apresentação com infinitos geradores. ■

■ **Exemplo 2.1.4** Por fim, o grupo dos inteiros com a adição é um grupo livre em uma letra, isto é, $\mathbb{Z} = \langle a \mid - \rangle$. Esse é o único grupo livre abeliano não trivial. ■

Teorema 2.1.3 — Segundo Teorema dos Isomorfismos. Sejam K um subgrupo de G e N um subgrupo normal de G. Então, $K/(K \cap N) \cong KN/N$.

Demonstração. Seja $\phi : K \to KN/N$, $k \mapsto kN$. Vamos mostrar que ϕ é um homomorfismo cujo núcleo é $K \cap N$.

Note que ϕ está bem definida, pois se k_1 e k_2 são dois elementos de K tais que $k_1 = k_2$, então $k_1 k_2^{-1} = e \in N$. Logo, $k_1 N = k_2 N$, ou seja, $\phi(k_1) = \phi(k_2)$.

Além disso, se kN é um elemento qualquer de KN/N, então basta tomar $x = k$ para obtermos $\phi(x) = kN$. Logo, ϕ é sobrejetora.

Note também que se $k_1, k_2 \in K$, então $\phi(k_1 k_2) = k_1 k_2 N = k_1 N k_2 N = \phi(k_1)\phi(k_2)$, logo ϕ preserva a operação.

Por fim, $\operatorname{Ker}\phi = \{k \in K \mid \phi(k) = N\} = \{k \in K \mid kN = N\} = \{k \in K \mid k \in N\} = K \cap N$. Consequentemente, pelo Teorema 1.7.3, $K/(K \cap N) \cong KN/N$. ■

Teorema 2.1.4 — Terceiro Teorema de Isomorfismos. Sejam M e N subgrupos normais de G, com $N \leq M$. Então, $(G/N)/(M/N) \cong G/M$.

Demonstração. Seja $\phi : G/N \to G/M$, $gN \mapsto gM$. Vamos mostrar que ϕ é um homomorfismo de núcleo M/N.

Primeiro, note que ϕ está bem definida pois se g_1 e g_2 são dois elementos quaisquer de G e $g_1 N = g_2 N$, então $g_1 g_2^{-1} \in N$. Como $N \subseteq M$, então $g_1 g_2^{-1} \in M$ e, por isso, $g_1 M = g_2 M$, ou seja $\phi(g_1 N) = \phi(g_2 N)$.

Além disso, note que se $g_1, g_2 \in G$, então $\phi(g_1 N g_2 N) = \phi(g_1 g_2 N) = g_1 g_2 M = g_1 M g_2 M = \phi(g_1 N)\phi(g_2 N)$, logo ϕ preserva a operação.

Note também que se gM é um elemento qualquer de G/M, então basta tomarmos $x = gN$ para obter $\phi(x) = gM$, logo ϕ é sobrejetora.

Por fim,

$$\begin{aligned}\operatorname{Ker}\phi &= \{gN \in G/N \mid \phi(gN) = M\} \\ &= \{gN \in G/N \mid gM = M\} \\ &= \{gN \in G/N \mid g \in M\}\end{aligned}$$

$$= MN/N$$
$$= M/(M \cap N)$$
$$= M/N,$$

em que na penúltima igualdade usamos o Teorema 2.1.3. Portanto, pelo Teorema 1.7.3, $(G/N)/(M/N) \cong G/M$. ■

Teorema 2.1.5 — Teorema de Dyck. Sejam

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e \rangle,$$
$$\overline{G} = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = w_{t+1} = \cdots = w_{t+k} = e \rangle.$$

Então, $\overline{G}$ é uma imagem homomórfica de G.

Demonstração. Sejam F o grupo livre em $\{a_1, a_2, \ldots, a_n\}$, N o menor subgrupo normal contendo $\{w_1, w_2, \ldots, w_t\}$ e M o menor subgrupo normal contendo $\{w_1, w_2, \ldots, w_t, w_{t+1}, \ldots, w_{t+k}\}$. Então, $F/N \cong G$ e $F/M \cong \overline{G}$.

A correspondência $\phi : F/N \to F/M$ define um homomorfismo de F/N em F/M. Para ver isso, note que ϕ está bem definida, pois se a_1 e a_2 são elementos quaisquer de F e $a_1N = a_2N$, então $a_1a_2^{-1} \in N \subseteq M$. Logo, $a_1a_2^{-1} \in M$, portanto $a_1M = a_2M$, ou seja, $\phi(a_1N) = \phi(a_2N)$. $\overset{aN \mapsto aM}{}$

Além disso, se aM é um elemento qualquer de F/M, então basta tomarmos $x = aN$ para obter $\phi(x) = aM$, logo ϕ é sobrejetora.

Por fim, sejam $a_1N, a_2N \in F/N$. Então, $\phi(a_1Na_2N) = \phi(a_1a_2N) = a_1a_2M = a_1Ma_2M = \phi(a_1N)\phi(a_2N)$, logo ϕ preserva a operação.

Como $F/N \cong G$ e $F/M \cong \overline{G}$, então ϕ induz um homomorfismo de G em $\overline{G}$. ■

Corolário 2.1.5.1 Se K é um grupo que satisfaz as relações de um grupo finito G e $|K| \geq |G|$, então K é isomorfo a G.

Demonstração. Do Teorema 2.1.5 anterior, sabemos que K é imagem homomórfica de G, portanto $|K| \leq |G|$. Por hipótese, $|K| \geq |G|$, logo $|K| = |G|$. ■

Teorema 2.1.6 — Classificação dos grupos de ordem 8. A menos de isomorfismo, há apenas 5 grupos de ordem 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_4 e Q_8.

Demonstração. O caso dos grupos abelianos já foi visto anteriormente na Seção 1.5. Então, seja G um grupo não abeliano de ordem 8. Além disso, sejam $G_1 = \langle a, b | a^4 = b^2 = (ab)^2 = e \rangle$ e $G_2 = \langle a, b | a^2 = b^2 = (ab)^2 \rangle$. Sabemos, das equações (2.1) e (2.2), que G_1 é isomorfo a D_4 e G_2 é isomorfo a Q_8. Portanto, basta mostrarmos que todo grupo não abeliano de ordem 8 satisfaz as relações de G_1 ou de G_2.

Como todo grupo que tem apenas elementos de ordem 2 é abeliano, então sabemos, pelo Teorema 1.4.1, que G tem pelo menos um elemento de ordem 4. Seja a tal elemento. Então, se b é um elemento de G que não está em $\langle a \rangle$, sabemos que

$$G = \langle a \rangle \cup \langle a \rangle b = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Considere o elemento b^2 de G. Note que b^2 não pode ser b, ab, a^2b nem a^3b, pois todos esses casos implicam em absurdos. Também não pode ser a, pois b^2 comuta com b e a não comuta com b. Também não pode ser a^3, pelo mesmo motivo. Logo, $b^2 = e$ ou $b^2 = a^2$.

Como $\langle a \rangle$ é um subgrupo normal de G, sabemos que $bab^{-1} \in \langle a \rangle$. Disso e do fato que $|bab^{-1}| = |a|$, sabemos que $bab^{-1} = a$ ou $bab^{-1} = a^{-1}$. A primeira hipótese implica G abeliano, o que não queremos, logo $bab^{-1} = a^{-1}$.

Agora, suponha $b^2 = e$. Então, $(ab)^2 = a(ba)b = a(a^{-1}b)b = b^2 = e$, ou seja, G satisfaz as relações de G_1. Por outro lado, se $b^2 = a^2$, então $(ab)^2 = a(ba)b = a(a^{-1}b)b = b^2 = a^2$, ou seja, G satisfaz as relações de G_2. ■

Lema 2.1.1 Para qualquer grupo G, $\langle a, b \rangle = \langle a, ab \rangle$.

Demonstração. Note que $a, ab \in \langle a, b \rangle$, logo $\langle a, ab \rangle \subseteq \langle a, b \rangle$. Por outro lado, $a = a^1(ab)^0$ e $b = a^{-1}(ab)^1$, ou seja, $a, b \in \langle a, ab \rangle$, logo $\langle a, b \rangle \subseteq \langle a, ab \rangle$. Portanto, $\langle a, b \rangle = \langle a, ab \rangle$. ■

Lema 2.1.2 A apresentação $\langle x, y \mid x^2 = y^n = (xy)^2 = e \rangle$ de D_n é equivalente à apresentação $\langle x, y \mid x^2 = y^n = e, xyx = y^{-1} \rangle$.

Demonstração. Partindo da segunda apresentação, note que $xyx = y^{-1}$ implica $xyxy = (xy)^2 = e$. Por outro lado, partindo da primeira apresentação, note que $(xy)^2 = xyxy = e$ implica $xyx = y^{-1}$. Logo, ambas as apresentações são equivalentes. ■

Teorema 2.1.7 — Classificação dos grupos diedrais. Qualquer grupo gerado por um par de elementos de ordem 2 é diedral.

Demonstração. Seja G um grupo gerado por um par de elementos distintos de ordem 2, a e b. Se a ordem de ab é infinita, então G é infinito e satisfaz as relações de D_∞. Vamos mostrar que $G \cong D_\infty$.

Pelo Teorema 2.1.5, sabemos que G é isomorfo a um grupo quociente de D_∞, digamos D_∞/H. Suponha que h é um elemento não identidade de H. Como todo elemento de D_∞ tem uma das formas $(ab)^i$, $(ba)^i$, $(ab)^i a$ ou $(ba)^i b$, por simetria, podemos assumir que $h = (ab)^i$ ou $h = (ab)^i a$.

Se $h = (ab)^i$, então $(ab)^i$ está em H e, portanto, temos

$$H = (ab)^i H = (abH)^i$$

de modo que $(abH)^{-1} = (abH)^{i-1}$. Mas

$$(ab)^{-1}H = b^{-1}a^{-1}H = baH$$

e segue que

$$aHabHaH = a^2HbHaH = baH = (abH)^{-1}.$$

Pelo Lema 2.1.1, $D_\infty/H = \langle aH, bH\rangle = \langle aH, abH\rangle$ e note que D_∞/H satisfaz as relações de D_i (basta substituir x e y no lema 8.6 por aH e abH, respectivamente). Em particular, G é finito, o que é impossível.

Agora, se $h = (ab)^i a$, então

$$H = (ab)^i aH = (ab)^i HaH$$

e, consequentemente,

$$(abH)^i = (ab)^i H = (aH)^{-1} = a^{-1}H = aH.$$

Segue então que

$$\langle aH, bH\rangle = \langle aH, abH\rangle \subseteq \langle abH\rangle.$$

Contudo,

$$(abH)^{2i} = (aH)^2 = H$$

então D_∞/H é finito novamente. Essa contradição força $H = \{e\}$ e G isomorfo a D_∞.

Finalmente, suponha que $|ab| = n$. Como $G = \langle a, b\rangle = \langle a, ab\rangle$, podemos mostrar (devido ao Lema 2.1.2) que G é isomorfo a D_n provando que $b(ab)b = (ab)^{-1}$, o que é equivalente a provar que $ba = (ab)^{-1}$ o que, por sua vez, é imediato, uma vez que a e b têm ordem 2. ■

Definição 2.1.3 — Matrizes de permutação. Uma **matriz de permutação** é uma matriz quadrada de ordem n formada apenas por zeros e uns (ou seja, binária). Em cada linha e coluna, há apenas uma entrada não nula. Tais matrizes têm como efeito permutar as linhas ou colunas de outras matrizes (ou, dependendo do contexto, as entradas de um vetor).

Lema 2.1.3 O grupo formado pelas matrizes de permutação (denotado por $\mathbb{P}_{n\times n}$) é isomorfo a S_n.

Demonstração. Seja $\phi : S_n \underset{\alpha\mapsto P_\alpha}{\to} \mathbb{P}_{n\times n}$, sendo $P_\alpha = \begin{bmatrix} e_{\alpha(1)} \\ \vdots \\ e_{\alpha(n)} \end{bmatrix}$ e sendo e_i os vetores da base canônica de $\mathbb{R}^n$.

Note que ψ está bem definida, pois permutações iguais são levadas em matrizes iguais.

Além disso, note que $P_\alpha P_\beta = \begin{bmatrix} e_{\alpha(1)} \\ \vdots \\ e_{\alpha(n)} \end{bmatrix} \begin{bmatrix} e_{\beta(1)} \\ \vdots \\ e_{\beta(n)} \end{bmatrix} = \begin{bmatrix} e_{\alpha(\beta(1))} \\ \vdots \\ e_{\alpha(\beta(n))} \end{bmatrix} = P_{\alpha\circ\beta}$. Isso se justifica pois multiplicando P_β por P_α, estamos permutando as linhas de P_β com a permutação α. Mas as linhas de P_β são as linhas da matriz identidade permutadas por β. Então, $P_\alpha P_\beta$ tem o mesmo efeito de permutar as linhas da matriz identidade por β e depois por α, ou seja, permutar por $\alpha \circ \beta$.

Note também que ψ preserva a operação, pois se α, β são permutações quaisquer de S_n, então $\psi(\alpha \circ \beta) = P_{\alpha\circ\beta} = P_\alpha P_\beta = \psi(\alpha)\psi(\beta)$.

Ademais, ψ é sobrejetora, pois basta tomarmos, em $\mathbb{P}_{n\times n}$, a matriz cujas linhas estão permutadas do mesmo modo que a permutação α em S_n; em símbolos, para toda matriz $P_\alpha \in \mathbb{P}_{n\times n}$, devemos tomar $\alpha \in S_n$ de modo a obter $\psi(\alpha) = P_\alpha$.

Por fim, temos que $\operatorname{Ker}\psi = \{\alpha \in S_n \mid \psi(\alpha) = I_n\} = \{\alpha \in S_n \mid P_\alpha = I_n\} = \{\alpha \in S_n \mid \alpha(i) = i, i = 1, 2, \ldots, n\} = \{e\}$, sendo I_n a matriz identidade de ordem n.

Consequentemente, como ψ é um homomorfismo sobrejetor, então pelo Teorema 1.7.3 concluímos que $S_n \cong \mathbb{P}_{n\times n}$. ■

Observação. Pelo Teorema 1.3.1, sabemos que todo grupo finito G é isomorfo a um subgrupo de S_n, digamos, H. Como S_n é isomorfo a $\mathbb{P}_{n\times n}$, e este é um subgrupo de $GL(n,K)$ (sendo K um corpo), então podemos mergulhar G em $GL(n,K)$. Em símbolos, $G \cong H \leq S_n \cong \mathbb{P}_{n\times n} \leq GL(n,K)$.

Teorema 2.1.8 — Classificação dos grupos de ordem $2p$. Seja p primo. Todo grupo de ordem $2p$ é cíclico ou isomorfo a D_p.

Demonstração. Primeiro, note que ser cíclico de ordem $2p$ é equivalente a ser isomorfo a $\mathbb{Z}_{2p}$.

Pelo Teorema 1.6.5, sabemos que G tem um elemento de ordem p, digamos a. Agora, suponha que G não possui elemento de ordem $2p$, ou seja, não é cíclico, e seja $b \in G$ não trivial tal que $b \notin \langle a\rangle$. Então, pelo Teorema 1.4.1, $|b| = 2$ ou $|b| = p$.

Como $|\langle a\rangle \cap \langle b\rangle|$ divide $|\langle a\rangle| = p$ e $\langle a\rangle \neq \langle b\rangle$, então $|\langle a\rangle \cap \langle b\rangle| = 1$.

Então, suponha $|b| = p$. Daí, pelo Teorema 1.4.2, $|\langle a\rangle\langle b\rangle| = |\langle a\rangle||\langle b\rangle|/|\langle a\rangle \cap \langle b\rangle| = p^2 > 2p$, o que é absurdo. Portanto, $|b| = 2$, ou seja, $b^2 = e$.

Usando o mesmo argumento que acima, mostramos que $|ab| = 2$, ou seja, $(ab)^2 = e$.

Como $D_p = \langle a, b | a^p = b^2 = (ab)^2 = e\rangle$ e G tem ordem $2p$ e satisfaz as relações de D_p, então $G \cong D_p$.

Finalmente, se G tem um elemento de ordem $2p$, então G é cíclico e, portanto, isomorfo a $\mathbb{Z}_{2p}$. ■

Sendo $Q_6 = \langle a, b \mid a^6 = 1, a^3 = b^2 = (ab)^2\rangle$ o grupo dicíclico de ordem 12 e A_4 o grupo alternante de ordem 12, as considerações feitas até aqui nos permitem construir a seguinte tabela:

Ordem	Abeliano	Não abeliano
1	$\mathbb{Z}$	–
2	$\mathbb{Z}_2$	–
3	$\mathbb{Z}_3$	–
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4$	–
5	$\mathbb{Z}_5$	–
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$	$S_3 \cong D_3 \cong GL(2, \mathbb{Z}_2)$
7	$\mathbb{Z}_7$	–
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_8$	D_4, Q_8
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_9$	–
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_2$	D_5
11	$\mathbb{Z}_{11}$	–
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$, $\mathbb{Z}_{12}$	D_6, A_4, Q_6
13	$\mathbb{Z}_{13}$	–
14	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_7 \oplus \mathbb{Z}_2$	D_7
15	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_3$	–

2.2 Apresentações de produtos diretos

Podemos, em termos das apresentações de dois grupos, escrever uma apresentação do produto direto desses grupos, da seguinte forma.

Proposição 2.2.1 Sejam G e H grupos com apresentações $\langle X|R\rangle$ e $\langle Y|S\rangle$, respectivamente. Então, o produto direto $G \oplus H$ (ou $G \times H$) tem apresentação

$$\langle X, Y \mid R, S, [X, Y] \rangle$$

onde $[X, Y]$ denota o comutador de X e Y, ou seja, o conjunto que contém todos os comutadores de um elemento de x com um elemento de y. ∎

Por exemplo, os grupos $\mathbb{Z}_2 = \langle a \mid a^2 = 1\rangle$ e $\mathbb{Z}_3 = \langle b \mid b^3 = 1\rangle$ têm produto direto dado pela apresentação

$$\mathbb{Z}_3 \oplus \mathbb{Z}_2 = \langle a, b \mid b^3 = a^2 = 1, ab = ba\rangle \cong \mathbb{Z}_6$$

e obtemos outra apresentação para o grupo cíclico de ordem 6, $\mathbb{Z}_6$.

2.3 Grupos abelianos finitamente gerados

Grande parte dos grupos que surgem na topologia como grupos fundamentais de superfícies e também em outras áreas da Matemática são grupos abelianos, ou seja, são grupos G tais que

$$xy = yx \ , \forall x, y \in G.$$

No caso de grupos abelianos, é comum adotar a notação aditiva para a operação do grupo, e esse será o nosso caso. Nessa seção, apresentaremos o **Teorema Fundamental dos Grupos Abelianos Finitamente Gerados** (Teorema 2.3.3), que caracteriza os grupos abelianos finitamente gerados como soma direta de grupos cíclicos (finitos e infinitos), e essa soma é unicamente determinada a menos da ordem dos fatores cíclicos. Com isso, vemos que a estrutura de um grupo abeliano finitamente gerado é naturalmente simples.

A primeira demonstração desse Teorema foi obtida por Leopold Kronecker em 1858. Mais precisamente, Kronecker demonstrou esse resultado para grupos abelianos finitos, i.e., ele provou que todo grupo abeliano finito é soma direta de grupos cíclicos de ordens iguais a potências de primos, e que a fatoração é única a menos da ordem dos fatores na decomposição.

É interessante nos determos um pouco no estudo dos grupos abelianos finitamente gerados, pois podemos enxergar suas apresentações de uma maneira interessante: através de matrizes. Antes de começar, vale a pena introduzir o conceito de comutador:

Definição 2.3.1 — Comutador. Sejam G um grupo e $g, h \in G$. O comutador de g e h em G é o elemento $[g, h] = g^{-1}h^{-1}gh$. Note que se $[g, h] = 1$, então g comuta com h.

Definição 2.3.2 — Grupo finitamente gerado. Dada uma apresentação $G = \langle X \mid R\rangle$ de um grupo G, se o conjunto de geradores, X, é finito, dizemos que G é finitamente gerado.

Agora podemos começar.

Grupos abelianos finitamente apresentados

Definição 2.3.3 — Grupo finitamente apresentado. Dada uma apresentação $G = \langle X \mid R\rangle$ de um grupo G, se o conjunto de geradores, X, e o conjunto de relatores, R, são finitos, dizemos que G é finitamente apresentado.

■ **Exemplo 2.3.1** O grupo $\langle a, b, c \mid a^4 = b^2 = 1, ab = ba, ac = ca, bc = cb\rangle$ é um exemplo de grupo abeliano finitamente apresentado (e, consequentemente, finitamente gerado) [1] escrito na forma multiplicativa. Aditivamente, escreveríamos $\langle a, b, c \mid 4a = 2b = 0, a + b = b + a, a + c = c + a, b + c = c + b\rangle$. ■

Contudo, como estamos trabalhando com grupos abelianos, sabemos que os geradores comutam. Por isso, é comum, quando estamos trabalhando apenas com grupos abelianos, omitir as relações de comutação e usar $[\cdot]$ ao invés de $\langle\cdot\rangle$. Daí, escrevemos simplesmente $[a, b, c \mid 4a = 2b = 0]$ ou de forma ainda mais simples $[a, b, c \mid 4a, 2b]$.

[1] Todo grupo finitamente apresentado é também finitamente gerado, mas a recíproca é falsa.

Denotamos o grupo abeliano gerado por $X_1, X_2, \ldots, X_n$ com relatores $R_1, R_2, \ldots, R_m$ por

$$[X_1, X_2, \ldots, X_n \mid R_1, R_2, \ldots, R_m],$$

onde os relatores R_i são escritos na forma $a_{i1}X_1 + \cdots + a_{in}X_n$ e os a_{ij} formam uma matriz A $m \times n$ de inteiros. Como o nome dos geradores não é importante, sua quantidade é a mesma que a quantidade de colunas de A, podemos recuperar a apresentação a partir da matriz A.

Para qualquer matriz inteira $A = (a_{ij})$ $m \times n$, $[A]$ denota o grupo abeliano em n geradores $X_1, \ldots, X_n$, sujeitos às m relações

$$\begin{array}{rcl} a_{11}X_1 + \cdots + a_{1n}X_n & = & 0 \\ a_{21}X_1 + \cdots + a_{2n}X_n & = & 0 \\ & \vdots & \\ a_{m1}X_1 + \cdots + a_{mn}X_n & = & 0. \end{array}$$

■ **Exemplo 2.3.2** Por exemplo, a matriz

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 2 & 2 & 2 \end{bmatrix}$$

denota o grupo abeliano $[a, b, c \mid 8a = 8b = 8c = 2a + 2b + 2c = 0]$. ■

Em essência, um grupo abeliano finitamente apresentado é um sistema linear homogêneo, mas com coeficientes inteiros. A maior diferença entre os sistemas aqui e os sistemas que aparecem na Álgebra Linear é que aqui a divisão não é permitida. Por exemplo, um elemento x de ordem 8 satisfaz $8x = 0$, o que, em Álgebra Linear, implicaria $x = 0$ [2]. Aqui, isso não acontece porque só podemos dividir pelos inteiros que têm inversos multiplicativos, i.e., ± 1.

■ **Exemplo 2.3.3** Por exemplo, a matriz

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix}$$

denota o grupo abeliano $[x, y, z \mid 8x = 8y = 8z = 0]$ que é claramente a soma direta de 3 grupos cíclicos de ordem 8, ou seja, isomorfo a $\mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$. ■

Se a matriz $[A]$ é diagonal, como foi o caso do exemplo acima, podemos escrever o grupo abeliano como soma direta a partir das entradas da diagonal principal.

[2] Isso se deve ao fato de que na Álgebra Linear os coeficientes formam um corpo.

■ **Exemplo 2.3.4** Por exemplo, a matriz

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

denota o grupo abeliano $[x, y, z \mid 8x = 8y = 0]$. A rigor, deveríamos ter escrito a relação $0z = 0$, mas ela é claramente redundante. O último gerador, z, tem ordem infinita, então o grupo é isomorfo a $\mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}$, ou seja, as entradas nulas da diagonal principal correspondem (se a matriz é diagonal) a $\mathbb{Z}$. ■

No exemplo acima, a terceira linha é supérflua, e podemos escrever

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cong \begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \end{bmatrix} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}.$$

Operações elementares de linha

Aqui, estamos em uma situação parecida com a de resolver sistemas lineares na Álgebra Linear. Lá, as operações elementares de linha eram fundamentais tanto para a solução dos sistemas quanto para a eliminação de Gauss. Vamos revisar as operações elementares de linha, e observar as diferenças para os grupos abelianos.

$R_i \leftrightarrow R_j$: trocar as linhas i e j. Esse movimento é equivalente a trocar a ordem de um par de equações do nosso sistema e, assim como em Álgebra Linear, é permitido. O novo sistema é equivalente ao original e, portanto, os grupos são isomorfos. Por exemplo

$$\begin{bmatrix} 8 & 6 & 5 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix} \cong \begin{bmatrix} 3 & 8 & -2 \\ 8 & 6 & 5 \\ 1 & 0 & -3 \end{bmatrix},$$

pois apenas trocamos as linhas 1 e 2.

$R_i \div k$: dividir a linha i por k ($k = \pm 1$ apenas). Aqui a nossa situação de grupos abelianos difere da Álgebra Linear, pois nossos "escalares" são inteiros e a divisão, em geral, não é permitida. De fato, os únicos valores de k para os quais essa operação é permitida são $k = \pm 1$, como mencionado anteriormente.

$R_i - kR_j$: subtrair k vezes a linha j da linha i (k qualquer inteiro). Essa é a operação de linha mais útil na Álgebra Linear, e aqui a situação não é diferente. Note que aqui só

podemos usar valores inteiros de k. Por exemplo, temos

$$G = \begin{bmatrix} 8 & 6 & 5 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix} \overset{R_1-2R_2}{\cong} \begin{bmatrix} 2 & -10 & 9 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix} \overset{R_1 \leftrightarrow R_3}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 3 & 8 & -2 \\ 2 & -10 & 9 \end{bmatrix}.$$

Imitando a eliminação de Gauss, podemos efetuar as seguintes operações

$$\begin{aligned} G &\cong \begin{bmatrix} 1 & 0 & -3 \\ 3 & 8 & -2 \\ 2 & -10 & 9 \end{bmatrix} \\ &\overset{R_2-3R_1}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 0 & 8 & 7 \\ 2 & -10 & 9 \end{bmatrix} \\ &\overset{R_3-2R_1}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 0 & 8 & 7 \\ 0 & -10 & 15 \end{bmatrix} \\ &\overset{R_2+R_3}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 0 & 8 & 7 \\ 0 & -2 & 22 \end{bmatrix} \\ &\overset{R_2+4R_3}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 0 & 0 & 95 \\ 0 & -2 & 22 \end{bmatrix} \\ &\overset{R_2 \leftrightarrow R_3}{\cong} \begin{bmatrix} 1 & 0 & -3 \\ 0 & -2 & 22 \\ 0 & 0 & 95 \end{bmatrix}. \end{aligned}$$

Se pudéssemos obter uma matriz diagonal, teríamos identificado nosso grupo G como uma soma direta de grupos cíclicos. Mas aqui parece ser o máximo que podemos atingir: qualquer outra operação elementar de linha tornaria a matriz mais complicada, mais longe de uma matriz diagonal. Precisamos de operações adicionais.

Operações elementares de coluna

Enquanto que as operações elementares de linhas convertem um conjunto de equações homogêneas em outro conjunto, equivalente, nas mesmas variáveis, as operações elementares de colunas também convertem um conjunto de equações homogêneas em outro conjunto, equivalente, mas muda as variáveis.

Contudo, como estamos interessados na estrutura de grupo a menos de isomorfismo, essa mudança pode ser feita e podemos usar tais operações para obter equações mais simples em um conjunto gerador diferente mas equivalente.

O caso mais simples é a troca de duas colunas.

$C_i \leftrightarrow C_j$**: trocar as colunas** i **e** j**.** O efeito, na apresentação do grupo, é trocar os geradores correspondentes, sendo que os grupos descritos pelas duas apresentações são isomorfos. Por exemplo

$$\begin{aligned}\begin{bmatrix}3 & 3 & 6\\ 8 & 4 & 0\\ 0 & 12 & 12\end{bmatrix} &\cong [a,b,c|3a+3b+6c=8a+4b=12b+12c=0]\\ &\cong [a,b,c|3a+3c+6b=8a+4b=12c+12b=0]\\ &\cong [a,b,c|3a+6b+3c=8a+4b=12b+12c=0] \cong \begin{bmatrix}3 & 6 & 3\\ 8 & 0 & 4\\ 0 & 12 & 12\end{bmatrix}.\end{aligned}$$

No exemplo acima, fizemos $C_2 \leftrightarrow C_3$.

$C_i \times k$**: multiplicar uma coluna por** k **(**$k = \pm 1$ **apenas).** Para $k = 1$ não há nenhuma alteração. Para $k = -1$, contudo, o efeito é trocar o sinal de cada entrada da coluna. Se X_i é o gerador correspondente, essa operação equivale a substituir X_i por $-X_i$.

$C_i - kC_j$**: subtrair** k **vezes a coluna** j **da coluna** i **(**k **qualquer inteiro).** Para essa operação, o efeito é menos óbvio. Considere o exemplo

$$\begin{bmatrix}3 & 6 & 3\\ 8 & 17 & 4\\ 0 & 5 & 2\end{bmatrix} = [X_1, X_2, X_3 \mid 3X_1+6X_2+3X_3 = 8X_1+17X_2+4X_3 = 5X_2+2X_3 = 0]$$

e defina $X_1' = X_1 + 2X_2$. Claramente, o grupo é gerado por $\{X_1', X_2, X_3\}$ pois $X_1 = X_1' - 2X_2$. Escrevendo as relações em termos do novo conjunto de geradores, temos

$$3(X_1' - 2X_2) + 6X_2 + 3X_3 = 8(X_1' - 2X_2) + 17X_2 + 4X_3 = 5X_2 + 2X_3 = 0.$$

Logo, o grupo tem a apresentação equivalente

$$[X_1', X_2, X_3 \mid 3X_1' + 3X_3 = 8X_1' + X_2 + 4X_3 = 5X_2 + 2X_3 = 0] \cong \begin{bmatrix}3 & 0 & 3\\ 8 & 1 & 4\\ 0 & 5 & 2\end{bmatrix}.$$

O efeito da mudança de variáveis $X_1 \to X_1' = X_1 + 2X_2$ é a operação elementar de coluna $C_2 - 2C_1$. Note que o sinal muda e os índices também.

Então, se os geradores são $X_1, \ldots, X_n$, temos que

- $C_i \leftrightarrow C_j$ corresponde a $X_i \leftrightarrow X_j$;
- $C_i \times -1$ corresponde a $X_i \to -X_i$;

- $C_i - kC_j$ corresponde a $X_j \to X_j + kX_i$.

Com essas observações, provamos o seguinte teorema:

Teorema 2.3.1 Se a matriz inteira (i.e., com entradas inteiras) B é obtida da matriz inteira A por uma sequência de operações elementares de linhas e colunas, então $[B] \cong [A]$.

Por exemplo,

$$\begin{bmatrix} 10 & 14 & 4 \\ 12 & 16 & 8 \\ 14 & 18 & 8 \end{bmatrix} \overset{C_1 \leftrightarrow C_3}{\cong} \begin{bmatrix} 4 & 14 & 10 \\ 8 & 16 & 12 \\ 8 & 18 & 14 \end{bmatrix}$$
$$\overset{C_2-3C_1, C_3-2C_1}{\cong} \begin{bmatrix} 4 & 2 & 2 \\ 8 & -8 & -4 \\ 8 & -6 & -2 \end{bmatrix}$$
$$\overset{R_2-2R_1, R_3-2R_1}{\cong} \begin{bmatrix} 4 & 2 & 2 \\ 0 & -12 & -8 \\ 0 & -10 & -6 \end{bmatrix}$$
$$\overset{C_1 \leftrightarrow C_2}{\cong} \begin{bmatrix} 2 & 4 & 2 \\ -12 & 0 & -8 \\ -10 & 0 & 6 \end{bmatrix}$$
$$\overset{C_2-2C_1, C_3-C_1}{\cong} \begin{bmatrix} 2 & 0 & 0 \\ -12 & 24 & 4 \\ -10 & 20 & 4 \end{bmatrix}$$
$$\overset{R_2+6R_1, R_3+5R_1}{\cong} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 24 & 4 \\ 0 & 20 & 4 \end{bmatrix}$$
$$\overset{R_2-R_3, R_3-5R_2}{\cong} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 4 & -4 \end{bmatrix}$$
$$\overset{R_3-R_2}{\cong} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -4 \end{bmatrix}$$
$$\overset{R_3 \div -1}{\cong} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4.$$

Usando as operações elementares de linhas e colunas, podemos colocar todas as matrizes inteiras na forma diagonal, e temos o seguinte teorema:

Teorema 2.3.2 — Teorema Fundamental dos Grupos Abelianos Finitamente Apresentados. Todo grupo abeliano finitamente apresentado é uma soma direta de grupos cíclicos.

Demonstração. Seja A a matriz da apresentação finita de um grupo abeliano.

1° caso: A é 1×1. Seja $A = (m)$. Podemos multiplicar por -1, se necessário, então

podemos assumir $m \geq 0$. Então, $[A] \cong \mathbb{Z}$ se $m = 0$ e $[A] \cong \mathbb{Z}_m$ se $m > 0$ ($\mathbb{Z}_1$ é o grupo trivial e pode ser desconsiderado caso apareça).

2° caso: $A = (m, 0, \ldots, 0)$ **para algum** m**.** Nesse caso, podemos ver que $[A]$ é isomorfo à soma direta $\mathbb{Z}_m \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-1}$.

3° caso: $A = \begin{pmatrix} m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ **para algum** m**.** Podemos ver que $[A] \cong \mathbb{Z}_m$.

4° caso: A **é a matriz nula** $m \times n$**.** Podemos ver que $[A]$ é isomorfo à soma direta de n cópias de $\mathbb{Z}$.

5° caso: caso geral. Suponha que $A \neq 0$ e possui pelo menos 2 linhas e 2 colunas. Escolha um elemento não nulo de menor valor absoluto e permute linhas e colunas para trazer esse elemento para a posição a_{11} multiplicando, se necessário, por -1 para torná-lo positivo. Agora, subtraia múltiplos adequados da primeira linha e da primeira coluna das outras linhas e colunas de modo que todas as entradas da primeira linha e da primeira coluna fiquem entre 0 (incluso) e a_{11}. Esse processo pode continuar, reduzindo o menor valor absoluto não nulo, até que a matriz tome a forma $(m, 0, \ldots, 0)$, $\begin{pmatrix} m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ ou $\begin{pmatrix} m & 0 \\ 0 & B \end{pmatrix}$, sendo m um inteiro não negativo e B uma matriz inteira com uma linha e uma coluna a menos que A. O teorema segue, então, por indução: já tratamos os dois primeiros casos e, para o último, aplicamos o processo para a matriz B. ■

Por exemplo,

$$\begin{bmatrix} 9 & 6 & 7 & 5 \\ 30 & 21 & 17 & 13 \\ 18 & 15 & 7 & 5 \end{bmatrix} \overset{\text{permutar colunas}}{\cong} \begin{bmatrix} 5 & 9 & 6 & 7 \\ 13 & 30 & 21 & 17 \\ 5 & 18 & 15 & 7 \end{bmatrix}$$

$$\overset{C_3 - C_1}{\cong} \begin{bmatrix} 5 & 9 & 1 & 7 \\ 13 & 30 & 8 & 17 \\ 5 & 18 & 10 & 7 \end{bmatrix}$$

$$\overset{\text{permutar colunas}}{\cong} \begin{bmatrix} 1 & 5 & 9 & 7 \\ 8 & 13 & 30 & 17 \\ 10 & 5 & 18 & 7 \end{bmatrix}$$

$$\overset{R_2 - 8R_1, R_3 - 10R_1}{\cong} \begin{bmatrix} 1 & 5 & 9 & 7 \\ 0 & -27 & -42 & -39 \\ 0 & -45 & -72 & -63 \end{bmatrix}$$

$$\overset{C_2 - 5C_1, C_3 - 9C_1, C_4 - 7C_1}{\cong} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 27 & 42 & 39 \\ 0 & 45 & 72 & 63 \end{bmatrix}$$

$$
\begin{aligned}
&\overset{\text{omitir } \mathbb{Z}_1}{\cong} \begin{bmatrix} 27 & 42 & 39 \\ 45 & 72 & 63 \end{bmatrix} \\
&\overset{C_3 - C_1}{\cong} \begin{bmatrix} 27 & 42 & 12 \\ 45 & 72 & 18 \end{bmatrix} \\
&\overset{\text{permutar colunas}}{\cong} \begin{bmatrix} 12 & 27 & 42 \\ 18 & 45 & 72 \end{bmatrix} \\
&\overset{C_2 - 2C_1}{\cong} \begin{bmatrix} 12 & 3 & 42 \\ 18 & 9 & 72 \end{bmatrix} \\
&\overset{\text{permutar colunas}}{\cong} \begin{bmatrix} 3 & 12 & 42 \\ 9 & 18 & 72 \end{bmatrix} \\
&\overset{R_2 - 3R_1}{\cong} \begin{bmatrix} 3 & 12 & 42 \\ 0 & -18 & -54 \end{bmatrix} \\
&\overset{C_2 - 4C_1, C_3 - 14C_1}{\cong} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 18 & 54 \end{bmatrix} \\
&\cong \mathbb{Z}_3 \oplus \begin{bmatrix} 18 & 54 \end{bmatrix} \\
&\overset{C_2 - 3C_1}{\cong} \mathbb{Z}_3 \oplus \begin{bmatrix} 18 & 0 \end{bmatrix} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}.
\end{aligned}
$$

Note que o Teorema 2.3.2 lida com grupos abelianos *finitamente apresentados*, i.e., os grupos em que há não só um conjunto finito de geradores, mas também em que as relações formam um conjunto finito de relações.

Não obstante, podemos adaptar a demonstração acima para mostrar que grupos abelianos *finitamente gerados* também são somas diretas de grupos cíclicos. Além disso, como somas diretas de um número finito de grupos cíclicos é também finitamente apresentada, segue que todo grupo abeliano finitamente gerado é também finitamente apresentado, ou seja, para grupos abelianos, ser finitamente apresentado e finitamente gerado são características equivalentes.

Teorema 2.3.3 — Teorema Fundamental dos Grupos Abelianos Finitamente Gerados. Todo grupo abeliano finitamente gerado é soma direta de grupos cíclicos.

Demonstração. Suponha que temos um grupo abeliano G finitamente gerado. Considere o conjunto de todas as relações entre seus geradores e sejam os coeficientes organizados em uma matriz inteira. De fato, essa matriz terá tantas colunas quanto houver geradores mas, possivelmente, infinitas linhas. O mesmo algoritmo da demonstração do Teorema 2.3.2 pode ser usado; claro que, havendo infinitas linhas, teríamos dificuldades práticas em implementar o algoritmo, mas como todas as colunas podem ser operadas em paralelo (i.e., simultaneamente), não há problemas na teoria. A finitude do número de colunas implica que o algoritmo terminará eventualmente. ■

2.4 Alguns subgrupos importantes de um grupo abeliano

Dados um inteiro n e um grupo abeliano G, definimos $nG = \{ng \mid g \in G\}$. Note que sendo $x, y^{-1} \in G$, temos que $(nx)(ny^{-1}) = \underbrace{x + \cdots + x}_{n} + \underbrace{(-y - \cdots - y)}_{n} = n(xy^{-1}) \in nG$. Logo, nG é subgrupo de G.

Em notação multiplicativa, escreveríamos $G^n = \{g^n | g \in G\}$. Uma vez que G^n pode não ser subgrupo de G caso G não seja abeliano, não definiremos tal grupo se G não for abeliano.

Por exemplo, se $G = \mathbb{Z}_4 \oplus \mathbb{Z}_8$, então $2G = \{(0,0), (0,2), (0,4), (0,6), (2,0), (2,2), (2,4), (2,6)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$ e também $3G = G$.

Outro exemplo é $G = \mathbb{Z}_4 \oplus \mathbb{Z}_6$. Nesse caso, $2G = \{(0,0), (0,2), (0,4), (2,0), (2,2), (2,4)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ e $3G = \{(0,0), (0,3), (3,0), (3,3), (2,0), (2,3), (1,0), (1,3)\} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Em ambos os exemplos acima, constatamos os isomorfismos calculando todos os elementos do grupo, ou seja, de modo braçal. Contudo, não é preciso fazer isso toda vez devido às duas proposições a seguir.

Proposição 2.4.1 Sejam G e H dois grupos abelianos. Então, $n(G \oplus H) \cong nG \oplus nH$. ∎

Demonstração. Vamos mostrar que a correspondência $n(x, y) \mapsto (nx, ny)$ é de fato um isomorfismo. Para isso, seja $f : n(G \oplus H) \to nG \oplus nH$ que leva $n(x, y)$ em (nx, ny). Primeiro, note que se $n(x_1, y_1) = n(x_2, y_2)$, então é claro que $f(n(x_1, y_1)) = f(n(x_2, y_2))$, logo f está bem definida.

Além disso, note que $\operatorname{Ker} f = \{n(x, y) \in n(G \oplus H) | f(n(x, y)) = (0, 0)\} = \{(0, 0)\}$, logo f tem núcleo trivial, ou seja, é injetiva.

Note também que dado $(g, h) \in nG \oplus nH$, basta tomarmos $n(x, y) \in n(G \oplus H)$ tal que $nx = g$ e $ny = h$ para obtermos $f(n(x, y)) = (g, h)$, logo f é sobrejetora.

Por fim, sejam $n(x, y)$ e $n(x', y')$ em $n(G \oplus H)$. Daí, temos

$$\begin{aligned} f(n(x,y) + n(x',y')) &= f(n(x + x', y + y')) \\ &= (n(x + x'), n(y + y')) \\ &= (nx + nx', ny + ny') \\ &= (nx, ny) + (nx', ny') \end{aligned}$$

$$= f(n(x,y)) + f(n(x',y')),$$

logo f preserva a operação. Portanto, f é isomorfismo. ■

Proposição 2.4.2 Temos $m\mathbb{Z}_n \cong \mathbb{Z}_d$, sendo $d = \dfrac{n}{\text{mdc}(m,n)}$. ■

Demonstração. Note que $m\mathbb{Z}_n$ é cíclico gerado por m. Além disso, note que $km = 0$ em $\mathbb{Z}_n$ se, e somente se, $\dfrac{n}{\text{mdc}(m,n)}$ divide k. Isso porque $km = 0 \implies n|km \implies \dfrac{n}{\text{mdc}(m,n)} \left| \dfrac{m}{\text{mdc}(m,n)}k \implies \dfrac{n}{\text{mdc}(m,n)} \right| k$, pois $\dfrac{m}{\text{mdc}(m,n)}$ e $\dfrac{n}{\text{mdc}(m,n)}$ são relativamente primos. Logo, m tem ordem $\dfrac{n}{\text{mdc}(m,n)}$ e gera um grupo cíclico isomorfo a $\mathbb{Z}_{n/\,\text{mdc}(m,n)}$. ■

■ **Exemplo 2.4.1** Por exemplo, se $G = \mathbb{Z}_{30} \oplus \mathbb{Z}_{100}$, então $2G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{50}$, $3G \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{100}$, $6G \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{50}$ e $28G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{25}$. ■

Outro subgrupo muito útil é $G[n] = \{g \in G \mid ng = 0\}$, $n \in \mathbb{Z}_+^*$. Note que $G[n]$ consiste nos elementos de G cujas ordens dividem n. De maneira quase idêntica ao que fizemos para nG, podemos mostrar que $G[n]$ é subgrupo de G.

Na forma multiplicativa, escrevemos $G[n] = \{g \in G \mid g^n = 1\}$. Novamente, não definimos $G[n]$ a não ser que G seja abeliano.

■ **Exemplo 2.4.2** Por exemplo, se $G = \mathbb{Z}_4 \oplus \mathbb{Z}_8$, então $G[2] = \{(0,0),(0,4),(2,0),(2,4)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ e $G[3] = 0$. ■

■ **Exemplo 2.4.3** Se $G = \mathbb{Z}_4 \oplus \mathbb{Z}_6$, temos $G[2] = \{(0,0),(0,3),(2,0),(2,3)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ e $G[3] = \{(0,0),(0,2),(0,4)\} \cong \mathbb{Z}_3$. ■

■ **Exemplo 2.4.4** Se $G = U(20)$, então $G^2 = \{1, 3^2, 7^2, 9^2, 11^2, 13^2, 17^2, 19^2\} = \{1, 3^2, 7^2, 9^2\} = \{1, 9\} \cong \mathbb{Z}_2$ e $G[2] = \{1, 9, 11, 19\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ■

Assim como foi para o subgrupo nG, não precisamos calcular todos os elementos à mão para determinar a soma direta. Para isso, usamos as seguintes proposições.

Proposição 2.4.3 Sejam G e H grupos abelianos. Então, $(G \oplus H)[n] \cong G[n] \oplus H[n]$. ■

Demonstração. Vamos usar a notação multiplicativa. Basta notar que como $(x,y)^n = (x^n, y^n)$, então $(x,y)^n = 1$ se, e somente se, $x^n = 1$ em G e $y^n = 1$ em H. ■

Proposição 2.4.4 $\mathbb{Z}_m[n] \cong \mathbb{Z}_{\text{mdc}(m,n)}$. ■

Demonstração. Suponha $k \in \mathbb{Z}_m[n]$. Então, $nk = 0$ em $\mathbb{Z}_m$, ou seja, $m|nk$. Consequentemente, $\dfrac{m}{\text{mdc}(m,n)}$ divide k, uma vez que $m|nk$ implica que $\dfrac{m}{\text{mdc}(m,n)}\Big|\dfrac{n}{\text{mdc}(m,n)}k$ que, por sua vez, implica que $\dfrac{m}{\text{mdc}(m,n)}\Big|k$, pois $\dfrac{m}{\text{mdc}(m,n)}$ e $\dfrac{n}{\text{mdc}(m,n)}$ são relativamente primos.

Então, $\mathbb{Z}_m[n]$ é um grupo cíclico gerado por $\dfrac{m}{\text{mdc}(m,n)}$, sendo isomorfo a $\mathbb{Z}_{\text{mdc}(m,n)}$. ■

■ **Exemplo 2.4.5** Por exemplo, se $G = \mathbb{Z}_{30} \oplus \mathbb{Z}_{100}$, temos $G[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $G[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{100}$, $G[6] \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$ e $G[28] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$. ■

O perfil das ordens de um grupo abeliano finito

Uma vez que todo grupo abeliano finito G pode ser escrito como uma soma direta de grupos cíclicos, podemos facilmente determinar o número de elementos de cada ordem em G. Essa facilidade se deve ao fato de que podemos facilmente identificar os subgrupos $G[n]$ para cada n e, portanto, recuperar informações acerca da ordem. A tabela que lista a quantidade de elementos de cada ordem é chamada de *perfil das ordens* de G.

Como a ordem de $G[n]$ é a quantidade de elementos cujas ordens dividem n, podemos contar a quantidade de elementos de ordem n da seguinte forma:

$$\sharp\text{elementos de ordem } n \text{ em } G = |G[n]| - \sum_{d|n, d<n} \sharp\text{elementos de ordem d.}$$

Por exemplo, podemos encontrar o perfil das ordens de $G = \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_9$. Note que como $36G = 0$, a ordem de cada elemento divide 36. Vamos listar os subgrupos $G[n]$ e suas ordens:

n	$G[n]$	$\lvert G[n]\rvert$
1	1	1
2	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	4
3	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	9
4	$\mathbb{Z}_4 \oplus \mathbb{Z}_2$	8
6	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	36
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_9$	27
12	$\mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_3$	72
18	$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_9$	108
36	G	216

Então, o perfil das ordens é

Ordem	Quantidade	
1	1	
2	3	$= 4 - 1$
3	8	$= 9 - 1$
4	4	$= 8 - 3 - 1$
6	24	$= 36 - 8 - 3 - 1$
9	18	$= 27 - 8 - 1$
12	32	$= 72 - 24 - 4 - 8 - 3 - 1$
18	54	$= 108 - 18 - 24 - 8 - 3 - 1$
36	72	$= 216 - 54 - 32 - 18 - 24 - 4 - 8 - 3 - 1$
Total	216	

O processo acima pode ser revertido para grupos abelianos finitos, i.e., sabendo a quantidade de elementos de cada ordem podemos determinar o grupo, a menos de isomorfismos. Contudo, essa reversão não é possível para grupos não abelianos.

2.5 Subgrupos de Sylow

Um terceiro subgrupo interessante é o chamado *subgrupo de Sylow*.

Definição 2.5.1 — Subgrupo de Sylow. Sejam p um primo e G um grupo finito. O p-subgrupo de Sylow de G é o conjunto de todos os elementos cujas ordens são potências de p. Denotamos o p-subgrupo de Sylow de G por $\mathrm{Syl}_p(G)$.

O nome é uma homenagem ao matemático norueguês Peter Ludwig Sylow (1832 – 1918). Por exemplo, o 2-subgrupo de Sylow de $\mathbb{Z}_{100}$ é $\{0, 25, 50, 75\} = \langle 25 \rangle$, que é isomorfo a $\mathbb{Z}_4$.

Uma das grandes utilidades dos p-subgrupos de Sylow é mostrada no seguinte teorema.

Teorema 2.5.1 Todo grupo abeliano finito é a soma direta de seus subgrupos de Sylow.

Demonstração. Pelo Teorema 2.3.3, podemos escrever todo grupo abeliano finito como soma direta de grupos cíclicos. Além disso, pelo Corolário 1.5.4.2, sabemos que todo grupo cíclico pode ser escrito como soma direta de p-grupos, para vários primos p. Juntando todos os grupos para um primo p particular, obtemos o p-subgrupo de Sylow correspondente, logo podemos escrever nosso grupo como soma direta de seus subgrupos de Sylow. ■

Similarmente aos subgrupos nG e $G[n]$, temos a seguinte proposição para subgrupos de Sylow, que não será demonstrada.

Proposição 2.5.1 Sejam G e H dois grupos abelianos finitos. Então, segue que $\mathrm{Syl}_p(G \oplus H) \cong \mathrm{Syl}_p(G) \oplus \mathrm{Syl}_p(H)$. ▪

Demonstração. Suponha $|G| = p^k m$ e $|H| = p^l n$, com $p \nmid m, n$. Dados $P_G \in \mathrm{Syl}_p(G)$ e $P_H \in \mathrm{Syl}_p(H)$, temos que $P_G \oplus P_H \leq G \oplus H$ e $|P_G \oplus P_H| = p^{k+l}$, ou seja, $P_G \oplus P_H \in \mathrm{Syl}_p(G \oplus H)$. Por outro lado, dado $P \oplus Q \in \mathrm{Syl}_p(G \oplus H)$, temos que $P \leq G$ e $Q \leq H$ com $|P \oplus Q| = p^{k+l}$. Então $|P| = p^k$ e $|Q| = p^l$, pois $|P| \mid |G|$ e $|Q| \mid |H|$. Portanto, $P \in \mathrm{Syl}_p(G), Q \in \mathrm{Syl}_p(H)$. ■

Por exemplo, $\mathrm{Syl}_2(\mathbb{Z}_{100} \oplus \mathbb{Z}_{50}) \cong \mathrm{Syl}_2(\mathbb{Z}_{100}) \oplus \mathrm{Syl}_2(\mathbb{Z}_{50}) \cong \langle 25 \rangle \oplus \langle 25 \rangle$. É importante frisar que as duas parcelas da última soma direta não são iguais, pois apesar de ambas serem geradas aditivamente, elas estão em grupos diferentes. A primeira parcela é isomorfa a $\mathbb{Z}_4$, enquanto que a segunda é isomorfa a $\mathbb{Z}_2$. Logo, $\mathrm{Syl}_2(\mathbb{Z}_{100} \oplus \mathbb{Z}_{50}) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Como dissemos anteriormente, é possível, dado o perfil das ordens de um grupo abeliano finito, determinar que grupo é esse, identificando-o como soma direta de grupos cíclicos. Por exemplo, suponha que um grupo abeliano G tem ordem $216 = 8 \times 27$. Há 9 possibilidades para G:

$\mathbb{Z}_8 \oplus \mathbb{Z}_{27}$	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$
$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$
$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

Suponha também que temos o seguinte perfil das ordens:

Ordem	Quantidade
1	1
2	3
3	8
4	4
6	24
9	18
12	32
18	54
36	72
Total	216

Como G tem elementos de ordem 4 mas não de ordem 8, temos $\mathrm{Syl}_2(G) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Similarmente, $G[3]$ tem ordem 9 e então $\mathrm{Syl}_3(G)$ tem de ser a soma direta de dois grupos cíclicos, ou seja, $\mathbb{Z}_3 \oplus \mathbb{Z}_9$. Logo, $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_9$, que de fato tem o perfil mostrado, como vimos anteriormente.

2.6 Abelianização de um grupo

Dado um grupo G, o **subgrupo derivado** de G (ou subgrupo comutador de G) é definido como o subgrupo de G gerado por todos os comutadores $\{g^{-1}h^{-1}gh \mid g, h \in G\}$ de elementos de G. Esse grupo é geralmente denotado por G'. Podemos ver que $G' \trianglelefteq G$ (a igualdade vale se

G é abeliano) e que G/G' é um grupo abeliano. Além disso, G' é o menor subgrupo de G tal que

$$\forall N \trianglelefteq G,\ G/N \text{ é abeliano} \iff N \supseteq G'$$

ou seja, G' é o menor subgrupo normal de G tal que G/G' é abeliano, e que qualquer outro subgrupo normal N tal que G/N é abeliano contém G'. Desse modo, temos que G/G' é o maior quociente abeliano de G, e definimos $G_{ab} = G/G'$ como a **abelianização** de G. De fato, a abelianização de um grupo G é um invariante de G.

Sejam $X = \{x_1, x_2, \ldots, x_r\}$ e $C = \{[x_i, x_j] \mid 1 \leq i < j \leq r\}, r \in \mathbb{N}$.

Proposição 2.6.1 Se $G = \langle X \mid R\rangle$, então $G_{ab} = \langle X \mid R, C\rangle$. ∎

Demonstração. Pelo Teorema 2.1.5, é suficiente mostrar que G' coincide com o fecho normal $\overline{C}$ de C em G. Como os geradores de $\langle X|R, C\rangle = G/C$ todos comutam, temos que esse grupo é abeliano e, daí, temos que $G' \subseteq \overline{C}$ pela caracterização de subgrupo derivado. Por outro lado, G' é um subgrupo normal de G que contém C, portanto $\overline{C} \subseteq G'$. ■

Por exemplo, seja G um grupo dado pela apresentação

$$\langle x, y, z, t \mid (xyz)^6 = 1,\ t^2 = (xz)^2,\ (xy^3zt^2)^2 = 1,\ (yt^2)^2 = x^2z^3,\ (xyz)^4(yt)^2 = 1\rangle.$$

Então, G_{ab} tem apresentação

$$\begin{aligned}\langle x, y, z, t \mid (xyz)^6 = 1,\ t^2 = (xz)^2,\ (xy^3zt^2)^2 = 1,\\ (yt^2)^2 = x^2z^3,\ (xyz)^4(yt)^2 = 1\\ [x, y] = [x, z] = [x, t] = [y, z] = [y, t] = [z, t] = 1\rangle.\end{aligned}$$

Usando as relações de comutadores da apresentação acima, chegamos à apresentação

$$\begin{aligned}\langle x, y, z, t \mid x^6y^6z^6 = x^2z^2t^{-2} = x^2y^6z^2t^4 = x^{-2}y^2z^{-3}t^4 = x^4y^6z^4t^2 = 1,\\ [x, y] = [x, z] = [x, t] = [y, z] = [y, t] = [z, t] = 1.\rangle\end{aligned}$$

A potência de cada gerador em cada uma das cinco primeiras relações é chamada de seu expoente soma.

Agora, suponha que temos uma apresentação $P = \langle X \mid R\rangle$ para um grupo G. Daí, naturalmente surgem as seguintes perguntas:

(i) Como obter informações de G_{ab} a partir da apresentação P de G?

(ii) O que as informações obtidas nos dizem?

Para X finito, ambas as questões podem ser respondidas satisfatoriamente. A resposta da segunda questão é um teorema de classificação: podemos listar todos os grupos abelianos finitamente gerados em um conjunto L tais que todos os outros grupos abelianos finitamente gerados são isomorfos a algum grupo de L: esse é o chamado Teorema de Base para grupos abelianos finitamente gerados, cuja demonstração é um algoritmo numérico simples que responde a questão (i). Vamos agora falar de alguns fatos sobre grupos abelianos.

Um *grupo de torção* é um grupo em que todos os elementos têm ordem finita, e.g., os grupos cíclicos $\mathbb{Z}/n\mathbb{Z}$. Já sabemos o que é um *grupo livre de torção*.

Então, seja G um grupo abeliano. O conjunto de elementos de ordem finita de G é denotado por $\mathrm{Tor}(G)$. Para G abeliano, esse conjunto é na verdade um subgrupo de G, chamado de *subgrupo de torção* de G. Logo, dizemos que G é um grupo de torção se $\mathrm{Tor}(G) = G$ e livre de torção se $\mathrm{Tor}(G) = \{1\}$, o grupo trivial.

Lema 2.6.1 Seja G um grupo abeliano. Então, $\mathrm{Tor}(G)$ é um grupo de torção e $G/\mathrm{Tor}(G)$ é um grupo livre de torção.

Demonstração. Para a primeira afirmação, basta notar que $\mathrm{Tor}(\mathrm{Tor}(G)) = \mathrm{Tor}(G)$, logo $\mathrm{Tor}(G)$ é um grupo de torção. Seja $x \in G$ e considere a classe $x + \mathrm{Tor}(G)$ no quociente $G/\mathrm{Tor}(G)$. Vamos mostrar que $x+\mathrm{Tor}(G)$ não é elemento de torção, i.e., não tem ordem finita. Para isso, suponha o contrário. Então, existe $m \in \mathbb{Z}$ tal que $m(x + \mathrm{Tor}(G)) = mx + \mathrm{Tor}(G) = \mathrm{Tor}(G)$, que implica $mx \in \mathrm{Tor}(G)$ e, consequentemente, $n(mx) = 0$ para algum $n \in \mathbb{Z}$. Mas isso significa que $x \in \mathrm{Tor}(G)$, logo $x+\mathrm{Tor}(G) = \{0\}$. Portanto, apenas a identidade tem ordem finita em $G/\mathrm{Tor}(G)$. ■

A proposição a seguir assegura quando que G/nG é um espaço vetorial.

Proposição 2.6.2 Sejam G um grupo abeliano e p um número primo, então G/pG é um espaço vetorial sobre $\mathbb{F}_p$, o corpo em p elementos. ■

Demonstração. Como pG é claramente normal em G, então o quociente G/pG está bem definido e então basta munirmos G/pG de uma multiplicação por escalar. Definamos então

$$k(g + pG) = kg + pG$$

sendo $k \in \mathbb{Z}$. Logo, se $k' \equiv k \mod p$, então $k' = k + pm$, para algum $m \in \mathbb{Z}$. Portanto, $k'a + pG = (k + pm)a + pG = ka + pma + pG = ka + pG$, pois $pma \in pG$. Resta mostrar as

demais propriedades de um espaço vetorial, que fica a cargo do leitor. ■

2.7 Algumas propriedades de grupos livres

Vamos apresentar algumas outras propriedades interessantes dos grupos livres. Então, seja $F = F(X)$ o grupo livre em um conjunto fixo X e considere a seguinte definição.

Definição 2.7.1 — Palavra ciclicamente reduzida. Uma palavra reduzida $a = x_1x_2\cdots x_l$, $x_i \in X^{\pm}$ (sendo $X^{\pm}$ o conjunto das letras de X com seus respectivos inversos), $1 \leq i \leq l$, é dita ciclicamente reduzida se $x_l \neq x_1^{-1}$.

Com essa noção, podemos mostrar a seguinte proposição.

Proposição 2.7.1 $F(X)$ é livre de torção. ■

Demonstração. Então, seja $a = x_1x_2\cdots x_l$ uma palavra reduzida qualquer em $X^{\pm}$, e seja $a^2 = x_1x_2\cdots x_{l-r}x_{r+l}\cdots x_l$ reduzida, de modo que $l(a^2) = l(a) - 2r$. O quão grande r pode ser? Claramente, $r = 0$ se, e somente se a é ciclicamente reduzida. Para responder essa questão de forma geral, façamos primeiro $l = 2k + 1$, i.e., ímpar. Então, é claro que $r \leq k$, pois do contrário $x_{k+1} = x_{k+1}^{-1}$, isto é, $x_{k+1}^2 = e$. Mas isso é impossível, pois nenhuma palavra reduzida de comprimento positivo em $X^{\pm}$ é trivial. Por outro lado, se fizermos $l = 2k$, i.e., par, devemos ter $r < k$, pois do contrário $x_k = x_{k+1}^{-1}$, o que contraria o fato de que a é reduzida.

Portanto, segue que $r < l/2$ e, portanto, $a = u^{-1}\breve{a}u$, sendo

$$u^{-1} = x_1\cdots x_r = x_l^{-1}\cdots x_{l-r+1}^{-1},\ \breve{a} = x_{r+1}\cdots x_{l-r},$$

com $\breve{a} \neq e$ e $x_{r+1} \neq x_{l-r}^{-1}$, de modo que $\breve{a}$ é ciclicamente reduzida. Note que

$$l(a^2) = 2l - 2r \overset{r<l/2}{>} 2l - l = l = l(a).$$

De modo mais geral, dado $n \in \mathbb{N}$, $a^n = u^{-1}\breve{a}^n u$, e como é claro que $\breve{a}^n$ é ciclicamente reduzida também segue que

$$l(a^n) = nl(\breve{a}) + 2r > (n-1)l(\breve{a}) + 2r = l(a^{n-1}). \tag{2.4}$$

Logo, $F(X)$ não possui elementos não triviais de ordem finita, uma vez que tomar potências de uma palavra qualquer sempre aumenta seu comprimento. Concluímos, então, que $F(X)$ de fato é livre de torção. ■

O próximo ponto é que grupos livres são o mais não comutativos possível. Em qualquer grupo, se dois elementos são potências de um mesmo elemento, então eles comutam. O seguinte lema assegura que a recíproca é verdadeira para grupos livres.

Lema 2.7.1 Sejam $a, b \in F(X)$ tais que $ab = ba$. Então, existe $c \in F(X)$ tal que $a = c^k$ e $b = c^h$, $k, h \in \mathbb{Z}$.

Demonstração. Vamos proceder por indução em $l(a) + l(b)$. Como o resultado é claro quando a ou b são triviais, já temos a base de indução e podemos assumir $a \neq e \neq b$. Tomando $a = x_1 \cdots x_l$ e $b = y_1 \cdots y_m$, assuma, por simetria, que $l = l(a) \leq l(b) = m$. Agora, considere a equação $ab = ba$ na forma reduzida:

$$x_1 \cdots x_{l-r} y_{r+1} \cdots y_m = y_1 \cdots y_{m-r} x_{r+1} \cdots x_l \tag{2.5}$$

sendo $0 \leq r \leq \min(l, m) = l$, por hipótese. Vamos dividir nossa análise em três casos.

Caso (i): $r = 0$. Daí, segue de (2.5) que $x_i = y_i$, $1 \leq i \leq l$ por comparação dos segmentos iniciais. Então, $b = au$, com $l(u) = m - l < m$, de modo que $l(a) + l(u) < l(a) + l(b)$. Então, $au = b = a^{-1}ba = a^{-1}aua = ua$ e a hipótese de indução nos dá que a e u são potências de um $c \in F(X)$, logo $b = au$ também é.

Caso (ii): $r = l$. Aqui, $y_i = x_{l-i+1}^{-1}$ e $b = a^{-1}u$, com $l(u) = m - l < m$. Segue como no Caso (i) que a^{-1} e u comutam e, portanto, são novamente potências de um elemento $c \in F(X)$, logo $b = a^{-1}u$ também é.

Caso (iii): $0 < r < l$. Nesse caso,

$$x_1 = y_1, \ x_l = y_m, \ x_l = y_1^{-1}, \ y_m = x_1^{-1}$$

de onde segue que

$$a = x_1 a' x_1^{-1}, \ b = x_1 b' x_1^{-1}$$

sendo $l(a') = l - 2$ e $l(b') = m - 2$. Pela hipótese de indução, a' e b' são potências de um mesmo elemento c'. Como a conjugação de $ab = ba$ por x_1 nos dá $a'b' = b'a'$, segue que a e b são potência de $c = x_1 c' x_1^{-1}$, concluindo nossa demonstração. ■

Proposição 2.7.2 Valem os seguintes itens:

1. em um grupo livre F, raízes n-ésimas, quando existem, são únicas, ou seja, se $a, b \in F$ satisfazem $a^n = b^n$, $n \in \mathbb{N}$, então $a = b$;

2. Qualquer elemento $w \in F$ tem um número finito de raízes, isto é, o conjunto

$$\sharp \{a \in F \mid a^n = w, n \in \mathbb{N}\} < +\infty.$$

■

Demonstração. Vamos começar com o item 1. Primeiro, escreva $a = u^{-1}\check{a}u$ e $b = v^{-1}\check{b}v$, com $\check{a}$ e $\check{b}$ ciclicamente reduzidas e $l(u) = r, l(v) = s$, digamos. Agora, aplique (2.4) nas equações $a^n = b^n$ e $a^{2n} = b^{2n}$ para obter

$$nl(\check{a}) + 2r = nl(\check{b}) + 2s,$$
$$2nl(\check{a}) + 2r = 2nl(\check{b}) + 2s.$$

Então, $l(\check{a}) = l(\check{b})$ e $r = s$, e como a equação

$$u^{-1}\check{a}^n = v^{-1}\check{b}^n v$$

não tem cancelamentos, segue que $u = v$ e $\check{a} = \check{b}$, logo $a = b$.

Para a demonstração do item 2, seja a uma raiz de w, digamos $a^n = w, n \in \mathbb{N}$. Se $w = e$, o resultado segue da Proposição 2.7.1. Se $w \neq e$, então nem a nem $\check{a}$ são triviais, e segue de 2.4 que $n \leq l(w)$. Então, w é uma potência n-ésima para no máximo uma quantidade finita de n e, para cada n, w é a n-ésima potência de no máximo um elemento devido ao item 1. Logo, o número total de raízes é finito. ■

O item 1 da Proposição 2.7.2 pode ser usado para fortalecer o Lema 2.7.1 da seguinte forma.

Lema 2.7.2 Se $a^h b^k = b^k a^h$ para $a, b \in F$ e $h, k \in \mathbb{Z}^*$, então a e b são potências de um elemento comum.

Demonstração. Devido a uma manipulação simples, podemos assumir $h, k \in \mathbb{N}$. Então,

$$a^h = b^k a^h b^{-k} = (b^k a b^{-k})^h$$

de onde segue que $a = b^k a b^{-k}$ pelo item 1 da Proposição 2.7.2. Logo,

$$b^k = a b^k a^{-1} = (aba^{-1})^k$$

de onde segue, novamente pelo item 1 da Proposição 2.7.2, que $b = aba^{-1}$, ou seja, $ab = ba$. Daí, o resultado segue do Lema 2.7.1. ■

Proposição 2.7.3 A comutatividade é uma relação de equivalência em $F - \{e\}$, isto é, o centralizador $C(a) = \{w \in F \mid aw = wa\}$ de qualquer $a \in F - \{e\}$ é abeliano. ■

Demonstração. Devemos mostrar que se $u, v \in F$ comutam com algum $a \in F - \{e\}$, então eles comutam um com o outro. Suponha que $ua = au$ e $va = av$, e que $u \neq e \neq v$ para evitar trivialidade. Então, pelo Lema 2.7.1, existem $b, d \in F$ e $p, q, r, s \in \mathbb{Z} - \{0\}$ tais que

$$u = b^p, \ a = b^q, \ a = d^r, \ v = d^s.$$

Mas então b^q e d^r comutam, pois são iguais, e segue do Lema 2.7.2 que existe um $c \in F$ e $h, k \in \mathbb{Z}$ tais que

$$b = c^h, \ d = c^k.$$

Logo, $u = c^{hp}$ e $v = c^{ks}$ também comutam. ■

Por fim, a Proposição 2.7.3 pode ser fortalecida da seguinte forma.

Teorema 2.7.1 Para qualquer $w \in F - \{e\}$, $C(w)$ é um grupo cíclico infinito.

Demonstração. Como $e \neq w \in C(w)$, $C(w)$ não pode ser finito pela Proposição 2.7.1.

Agora, seja d um elemento de comprimento minimal em $C(w) - \{e\}$, e seja $v \in C(w)$ arbitrário. Então, v deve ser uma potência de d. Como v e d comutam (pela Proposição 2.7.3), eles são potência de um elemento comum (pelo Lema 2.7.1):

$$d = a^h, \ v = a^k.$$

Da segunda equação, a^k comuta com w, de onde temos que $a \in C(w)$ pelo Lema 2.7.2. Aplicando (2.4) na primeira equação, temos

$$l(d) = l(a^h) = |h| l(\check{a}) + 2r \overset{2r=l(a)-l(\check{a})}{=} (|h| - 1) l(\check{a}) + l(a)$$

sendo $|h| \neq 0$ e $d \neq e$. Como $a \in C(w)$, segue da minimalidade de $l(d)$ que $|h| = 1$ e então $v = d^{\pm k}$, como desejado. ■

2.8 Grupos, isometrias e polinômios

Vamos mostrar duas aplicações interessantes de apresentações de grupos: para isometrias de $\mathbb{R}^2$ e para polinômios.

Primeiro, considere o reticulado dos pontos inteiros em $\mathbb{R}^2$, isto é,

$$L = \left\{(k, l) \in \mathbb{R}^2 \mid k, l \in \mathbb{Z}\right\}$$

e o grupo $G = \mathrm{Sim}(L)$ das isometrias de $\mathbb{R}^2$ que levam L em L, isto é, que deixam o reticulado fixo. Um exemplo de isometria é a translação t. Se t leva a origem de $\mathbb{R}^2$ para o ponto (m, n), então um ponto qualquer $(k, l) \in \mathbb{R}^2$ é levado em $(k + m, l + n)$.

Então, vemos que a translação t é determinada pelo par (m, n). Além disso, denotando por a e b as translações $(0, 0) \mapsto (1, 0)$ e $(0, 0) \mapsto (0, 1)$, respectivamente, temos $t = a^m b^n$. Note também que se t' é a translação $(0, 0) \mapsto (k, l)$, então

$$tt'(0, 0) = t(k, l) = (k + m, l + n).$$

Em outras palavras, temos que $a^k b^l a^m b^n = a^{k+m} b^{l+n}$. Portanto, o conjunto de todas as translações T de G formam um subgrupo de G. Sabendo disso, temos

$$T = \langle a \rangle \times \langle b \rangle \overset{\text{Proposição 2.2.1}}{=} \langle a, b \mid [a, b] = 1 \rangle$$

e, consequentemente, vemos que T é um grupo abeliano livre com dois geradores (posto 2).

Agora, considere as isometrias S que fixam a origem: a rotação y no sentido anti-horário de um ângulo θ, $0 \leq \theta \leq \pi/2$, e a reflexão x sobre a direção $(1, 0)$, ou seja, sobre o eixo das abscissas. Em termos de matrizes sobre o sistema de coordenadas usual (pela direita), temos

$$x = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \; y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Note que todo elemento de S induz uma única simetria do quadrado de vértices $(\pm 1, 0), (0, \pm 1)$. Logo, não podem haver mais de 8 simetrias. Desse modo, como valem as relações $y^4 = x^2 = 1$, $x^{-1} y x = y^{-1}$, então S define o grupo

$$S = \langle x, y \mid y^4 = x^2 = 1, xyx^{-1} = y^{-1} \rangle,$$

que é o grupo diedral de ordem 8, D_4.

Agora, seja $g \in G$ um elemento qualquer. Se $g(0) = (m, n)$ e $t = a^m b^n \in T$, então gt^{-1} fixa a origem e, portanto, pertence a S. Fazendo $gt^{-1} = s \in S$, temos $g = st$, logo $G = ST$, pois g é um elemento qualquer. Como uma translação que fixa qualquer ponto deve ser a identidade, temos $S \cap T = 1$ e, consequentemente, podemos ver G como produto semidireto.

Para mostrar que esse de fato é o caso, seja $P = (m, n)$ um ponto qualquer e note que, a partir das matrizes x e y, temos

$$\begin{aligned} xax^{-1}(P) &= xa(-m, n) = x(-m + 1, n) = (m - 1, n) = a^{-1}(P), \\ xbx^{-1}(P) &= xb(-m, n) = x(-m, n + 1) = (m, n + 1) = b(P), \end{aligned}$$

$$yay^{-1}(P) = ya(n,-m) = y(n+1,-m) = (m,n+1) = b(P),$$
$$yby^{-1}(P) = yb(n,-m) = y(n,-m+1) = (m-1,n) = a^{-1}(P).$$

Portanto,

$$xax^{-1} = a^{-1},\ xbx^{-1} = b,\ yay^{-1} = b,\ yby^{-1} = a^{-1} \tag{2.6}$$

Então, T é normalizado por S. Sendo $G = ST$ e T abeliano, segue que $T \trianglelefteq G$. As equações em (2.6) mostram que as matrizes x e y definem um homomorfismo

$$\alpha : S \to GL_2(\mathbb{Z}) = \mathrm{Aut}(T).$$

Portanto, $G = T \rtimes_\alpha S$. Também é possível mostrar que usando

$$T = \langle a \rangle \times \langle b \rangle = \langle a, b \mid [a,b] = 1 \rangle,\ S = \langle x, y \mid y^4 = x^2 = 1, xyx^{-1} = y^{-1} \rangle$$

e (2.6), G tem apresentação

$$G = \langle x, y, a, b \mid [a,b] = x^2 = y^4 = 1, xyx^{-1} = y^{-1}, xax^{-1} = a^{-1},\ xbx^{-1} = b,\ yay^{-1} = b,\ yby^{-1} = a^{-1} \rangle$$

e obtemos uma apresentação para $\mathrm{Sim}(L)$.

Agora, sejam p primo e $n \in \mathbb{N}$. Considere

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_1 x + a_2 x^2 + \cdots + x^n,$$

ou seja, os monômios de grau menor ou igual a n, sobre o corpo $\mathbb{Z}_p$, com coeficiente independente nulo. Vamos chamar de $G_n(p)$ o conjunto de todos esses polinômios, isto é

$$G_n(p) = \{ f(x) \mid gr(f) \leq n, a_i \in \mathbb{Z}_p, a_0 = 0, a_n = 1 \}.$$

De fato, $(G_n(p), \circ)$ é grupo, sendo $\circ$ a operação de composição de funções $\pmod{x^{n+1}}$. Além disso, $|G_n(p)| = p^{n-1}$.

Esse grupo tem muitas propriedades interessantes; vamos, no momento, obter uma apresentação para o grupo $G = G_5(2)$, de ordem $2^{5-1} = 16$. Note que os coeficientes são obtidos módulo 2 e que a maior potência é 5.

Seja $a = x + x^2$. Daí, temos o seguinte:

$$a^2 = a(x + x^2) = x + x^2 + (x + x^2)^2 = x + x^4,$$
$$a^3 = a(x + x^4) = x + x^4 + (x + x^4)^2 = x + x^2 + x^4,$$

$$a^4 = a^2(x + x^4) = x + x^4 + (x + x^4)^4 = x.$$

Logo, a tem ordem 4 em G e, portanto, $A = \langle a \rangle$ é um subgrupo de ordem 4. Seja agora $b = x + x^3$. Semelhantemente:

$$\begin{aligned} b^2 &= b(x + x^3) = x + x^3 + (x + x^3)^3 = x + x^3 + x^3 + x^5 = x + x^5, \\ b^3 &= b(x + x^5) = x + x^5 + (x + x^5)^3 = x + x^3 + x^5, \\ b^4 &= b(x + x^3 + x^5) = x + x^3 + x^5 + (x + x^3 + x^5)^3 = x. \end{aligned}$$

Logo, o subgrupo $B = \langle b \rangle$ tem ordem 4. Como $A \cap B = 1$ e AB tem 16 elementos, temos $AB = G$. Contudo, nesse caso nem A nem B são normais em G e, portanto, não temos um produto semidireto.

Também temos que

$$\begin{aligned} ab &= a(x + x^3) = x + x^3 + (x + x^3)^2 = x + x^2 + x^3, \\ b^{-1} &= x + x^3 + x^5. \end{aligned}$$

Desse modo,

$$ab^{-1} = a(x + x^3 + x^5) = x + x^3 + x^5 + (x + x^3 + x^5)^2 = x + x^2 + x^3 + x^5$$

e temos

$$\begin{aligned} (ab)^2 &= ab(x + x^2 + x^3) = x + x^2 + x^3 + (x + x^2 + x^3)^2 + (x + x^2 + x^3)^3 = x, \\ (ab^{-1}) &= (ab^{-1})(x + x^2 + x^3 + x^5) = x. \end{aligned}$$

Portanto, $(ab)^2 = (ab^{-1})^2$.

Parte II

Começando a viagem — Tranças e Nós

Capítulo 3

A Teoria das Tranças

"Nature is written in mathematical language."
— Galileu Galilei

3.1 Introdução

Definição 3.1.1 — Trança (informal). Uma **trança** de n cordas nada mais é que um conjunto de n cordas (que podem se cruzar ou não). Contudo, em uma trança cada corda deve "se mover" monotonicamente da esquerda para a direita, isto é, se seguirmos qualquer corda da esquerda para a direita, ela não pode "voltar" (ir para a esquerda), apenas "ir" (ir para a direita) e, também, duas cordas não podem passar uma por dentro da outra.

A Definição 3.1.1, apesar de informal, ajuda a ter um entendimento intuitivo do conceito de trança. Essa definição será formalizada no Teorema 3.1.1.

O conjunto das tranças de n cordas (mais precisamente, o conjunto das classes de equivalência das tranças de n cordas) forma um grupo sob a operação de concatenação (que será aqui tratada como produto), grupo esse denotado por B_n.

Podemos ainda imaginar as tranças como cordas que tiveram suas extremidades coladas em duas paredes opostas no espaço tridimensional. Nesse sentido, é fácil pensar em vários exemplos de tranças que surgem no cotidiano: a trança francesa no cabelo, os pães artesanais feitos com a massa trançada (nas extremidades do pão as "cordas" da trança são "coladas" juntas, então o pão não é, em si, uma trança, mas o padrão contido nele é). Veja os exemplos abaixo.


Figura 3.1: Trança francesa (à esquerda) e pão trançado (à direita)

Podemos ainda representar as tranças através de diagramas, como mostram os exemplos abaixo.

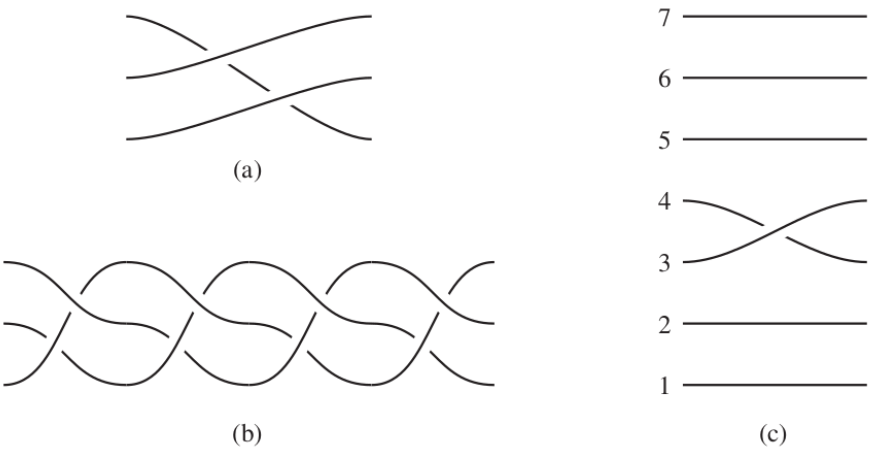


Figura 3.2: (a) Uma trança de 3 cordas com 2 cruzamentos
(b) A trança "comum" de 3 cordas (trança francesa)
(c) Corda 3 passa sobre a corda 4

Note que cada corda recebe um número (a numeração pode ser feita de cima para baixo ou de baixo para cima). Como dito anteriormente, podemos definir o produto de duas tranças como sendo a concatenação dessas tranças. Além disso, também definimos a trança identidade de maneira bastante intuitiva: ela é apenas o conjunto de n cordas, sem nenhum cruzamento. Veja exemplos abaixo.

Figura 3.3: O produto de duas tranças de 3 cordas

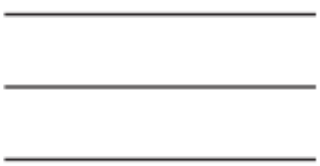


Figura 3.4: A identidade em B_3

Figura 3.5: Duas representações para a identidade em B_2. Apesar de parecerem diferentes à primeira vista, elas pertencem à mesma classe de equivalência, ou seja, são a mesma trança em B_n

Definido o produto da forma acima, o que significa ter o inverso de uma trança? Por exemplo, qual seria o inverso da trança α na Figura 3.2(b)?. Bom, para saber isso devemos, primeiro, conhecer a identidade em B_3, que é mostrada acima.

Bom, como poderíamos estender α para fazê-la parecer a identidade? É impossível: α tem cruzamentos, e desenhar mais coisas não vai mudar isso. Precisamos de uma maneira de cancelar cruzamentos, de modo que as duas tranças na Figura 3.5 sejam equivalentes.

Para isso, a ideia é que devemos ser capazes de mover as tranças do mesmo modo que fazemos no espaço (ou seja, sem passar nenhuma corda por dentro de outra) e obter uma trança equivalente. Para definir equivalência, é necessário dizer que quando movemos as tranças, as extremidades devem ficar fixas (do contrário, qualquer trança seria equivalente à identidade).

Podemos ainda imaginar que as extremidades da esquerda de cada trança estão presas à parede vertical $x = 0$ no espaço tridimensional e as extremidades da direita estão presas à

parede $x = 1$. Nessa configuração, duas tranças são ditas *equivalentes* se podemos mover uma delas, mantendo-a entre as paredes e com as extremidades fixas, e fazê-la parecer a outra.

Com essa definição, as duas últimas tranças da Figura 3.5 são equivalentes, assim como as tranças abaixo.

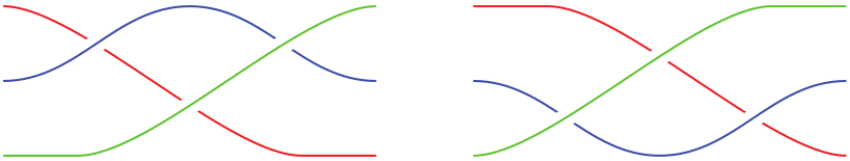


Figura 3.6: Duas tranças equivalentes

Apenas um aspecto técnico: se fixarmos as paredes que limitam as tranças como sendo $x = 0$ e $x = 1$, devemos tomar mais cuidado com o que significa multiplicar duas tranças. Especificamente, para formar β vezes β', devemos transladar β' uma unidade no eixo x, tomar a união de β com a versão transladada de β' e redimensionar tudo por um fator de $1/2$. Isso faz com que o produto de duas tranças seja também uma trança.

Desse modo, note que se fizermos o produto de uma trança γ qualquer pela segunda trança da Figura 3.5, seja à esquerda ou à direita, não alteraremos o número de cruzamentos nem sua configuração, ou seja, não alteraremos a trança γ. Portanto, de fato, a segunda trança da Figura 3.5 é a identidade em B_2.

Note também que para obter o inverso de uma trança α, basta espelharmos α, ou seja, o inverso de uma trança qualquer α, denotado por α^{-1}, nada mais é que a imagem espelhada de α.

Observação. Nesse sentido, encontrar o inverso de uma trança é parecido com encontrar o inverso de uma matriz: devemos ir "desfazendo" a trança, de trás para frente (da direita para a esquerda), assim como o inverso de um produto ABC de matrizes é dado por $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$.

Lema 3.1.1 — Grupo de Tranças. Para n fixo, as (classes de equivalência de) tranças de n cordas formam um grupo.

Demonstração. A identidade é evidente: ela é apenas o conjunto de n cordas, sem nenhum cruzamento. Anteriormente, enunciamos um procedimento para construir o inverso de uma trança (inverso esse que também é uma trança), logo toda trança possui inverso. A concatenação

(que nada mais é que o produto) de duas tranças de n cordas nos dá outra trança também de n cordas (como vimos anteriormente), logo o conjunto é fechado para o produto. Por fim, a associatividade pode ser verificada através de um diagrama, como o da Figura 3.7.

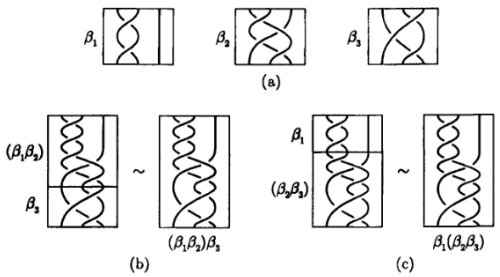


Figura 3.7: Associatividade do produto de tranças

■

Quando estamos desenhando uma trança, podemos sempre usar a equivalência para evitar que três ou mais cordas se cruzem no mesmo ponto do desenho. Também podemos fazer com que nenhum cruzamento ocorra diretamente acima de outro, como mostra a figura abaixo.

Figura 3.8: Podemos evitar fazer desenhos como esses

Por conta disso, podemos sempre "cortar" qualquer trança, usando linhas verticais, de modo que cada pedaço seja uma trança que contenha somente um cruzamento, como abaixo.

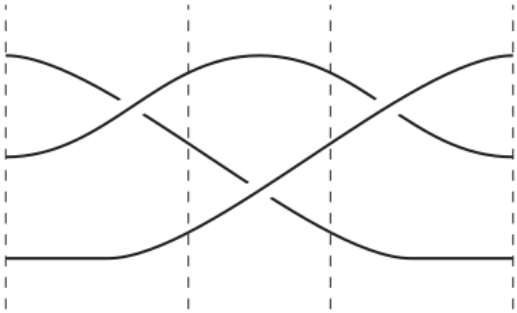


Figura 3.9: Uma trança como produto de cruzamentos

Em outras palavras, B_n é gerado pelo conjunto de todas as tranças de n cordas que têm exatamente um cruzamento. A trança em que a corda i passa por cima da corda $i+1$ é usualmente denotada por σ_i. Por exemplo, a Figura 3.2(c) mostra a trança σ_3 em B_7. O seu inverso seria σ_3^{-1}, a corda 3 passando por baixo da corda 4. Em geral, a trança em que a corda i passa por baixo da corda $i+1$ (ou, equivalentemente, a corda $i+1$ passa por cima da corda i) é denotada por σ_i^{-1}.

Agora, podemos ver que B_n é gerado pelo conjunto $\{\sigma_1, \ldots, \sigma_{n-1}\}$. Note, porém, que a notação σ_i não diz em que grupo de trança estamos, exceto que deve ser pelo menos B_{i+1}. Por exemplo, o cruzamento σ_2 é um gerador de B_3, mas também de B_4, B_5 e assim por diante. O contexto geralmente deixa claro em qual grupo de tranças estamos.

Tendo isso em mente, podemos escrever algumas das tranças vistas anteriormente em termos dos geradores σ_i. Por exemplo, as tranças (a), (b) e (c) da Figura 3.2 podem ser escritas, respectivamente, como $\sigma_2\sigma_1$, $(\sigma_1\sigma_2^{-1})^4$ e σ_3; a trança da Figura 3.3 pode ser escrita como $\sigma_2\sigma_1^{-1}$; tanto a trança da Figura 3.4 quanto a trança da Figura 3.5 são a identidade em seus respectivos grupos (B_3 e B_2), podendo ser denotadas por e ou, para evitar confusões, 1_3 e 1_2, respectivamente (de modo geral, podemos denotar a identidade em B_n por 1_n); a trança da Figura 3.6 pode ser escrita como $\sigma_1\sigma_2\sigma_1$ ou também como $\sigma_2\sigma_1\sigma_2$. Mais à frente veremos que esse fato não é coincidência, mas uma relação muito importante para o grupo de trança.

Queremos agora pensar sobre como os diferentes σ_i se relacionam. Note que se σ_i e σ_j envolvem cordas completamente distintas, então eles comutam, como ilustrado abaixo.

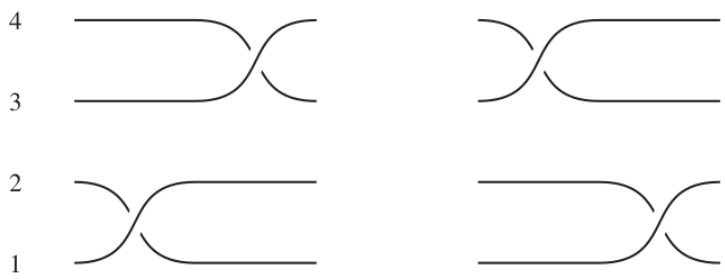


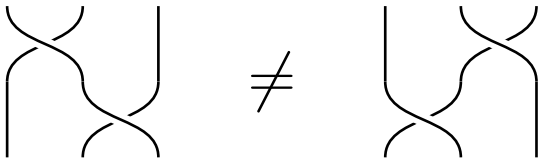
Figura 3.10: $\sigma_1\sigma_3$ e $\sigma_3\sigma_1$ são equivalentes.

Observação. Intuitivamente, se dois cruzamentos envolvem cordas completamente distintas, então podemos "deslizá-los" livremente. Daí vem a comutatividade.

É natural pensar, então, que se dois cruzamentos têm uma corda em comum, então a comutatividade não deve valer. De fato, isso é demonstrado pelo seguinte lema.

Lema 3.1.2 Dado B_n e σ_i um gerador de B_n, com $1 \leq i \leq n-1$, os cruzamentos vizinhos não comutam, isto é, $\sigma_i\sigma_{i+1} \neq \sigma_{i+1}\sigma_i$.

Demonstração. Basta fazer o desenho, como o do diagrama abaixo.



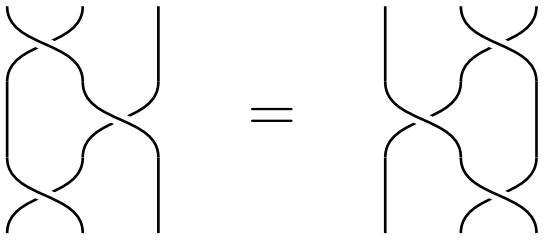
Note que não é possível deslizar os cruzamentos de uma das tranças para obter a outra e, consequentemente, cruzamentos vizinhos não comutam. ■

Contudo, os σ_i's vizinhos satisfazem a seguinte relação, chamada *relação de trança*:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

Lema 3.1.3 Em B_n, $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, para todo $1 \leq i \leq n-1$.

Demonstração. Basta olhar o diagrama abaixo.



Note que podemos obter o diagrama da direita a partir do diagrama da esquerda da seguinte forma: a corda i (à esquerda) é puxada um pouco para baixo; a corda $i+1$ (centro) é puxada para a direita; e a corda $i+2$ (à direita) é puxada um pouco para cima.

Então, de fato $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ para todo $1 \leq i \leq n-1$, como queríamos demonstrar. ■

Essas duas relações, a comutatividade e a relação de trança, implicam todas as outras relações entre os σ_i. Em outras palavras:

Teorema 3.1.1 O grupo de trança tem a apresentação

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ para } |i-j| > 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \text{ para } 1 \leq i \leq n-2 \rangle.$$

Aceitaremos o Teorema 3.1.1 sem demonstração.

As duas relações do Teorema 3.1.1 nos ajudam a simplificar e manipular palavras em B_n. Por exemplo, sabendo que $[a,b] = a^{-1}b^{-1}ab$, podemos manipular $(\sigma_i\sigma_{i+1})^{-1}[\sigma_{i+2}\sigma_i^{-1}, \sigma_i\sigma_{i+1}^{-1}]\sigma_i\sigma_{i+1}$ para obter $\sigma_{i+2}\sigma_i^{-1}$ da seguinte forma:

$$\begin{aligned}
&(\sigma_i\sigma_{i+1})^{-1}[\sigma_{i+2}\sigma_i^{-1}, \sigma_i\sigma_{i+1}^{-1}]\sigma_i\sigma_{i+1} \\
&= \sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_i\sigma_{i+2}^{-1}\sigma_{i+1}\sigma_i^{-1}\sigma_{i+2}\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1} \\
&= (\sigma_{i+1}^{-1}\sigma_{i+2}^{-1}\sigma_{i+1})\sigma_i^{-1}\sigma_{i+2}(\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}).
\end{aligned}$$

Usando a relação de trança, deduzimos a seguinte relação:

$$\begin{aligned}
\sigma_i^{-1}\sigma_{i+1}^{-1}\sigma_i &= \sigma_{i+1}\sigma_i^{-1}\sigma_{i+1}^{-1} \\
\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1} &= \sigma_i\sigma_{i+1}\sigma_i^{-1}
\end{aligned}$$

Usando essa igualdade, temos

$$\begin{aligned}
&(\sigma_{i+1}^{-1}\sigma_{i+2}^{-1}\sigma_{i+1})\sigma_i^{-1}\sigma_{i+2}(\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}) \\
&= (\sigma_{i+2}\sigma_{i+1}^{-1}\sigma_{i+2}^{-1})\sigma_i^{-1}\sigma_{i+2}(\sigma_i\sigma_{i+1}\sigma_i^{-1}) \\
&= \sigma_{i+2}\sigma_{i+1}^{-1}\sigma_{i+2}^{-1}\sigma_i^{-1}\sigma_i\sigma_{i+2}\sigma_{i+1}\sigma_i^{-1} \\
&= \sigma_{i+2}\sigma_i^{-1}.
\end{aligned}$$

Outra aplicação do Teorema 3.1.1 é o fato de que $B_2 \cong \mathbb{Z}$. Para perceber isso, basta notar que pelo Teorema 3.1.1, $B_2 = \langle \sigma_1 | - \rangle$ e $\mathbb{Z}$ tem essa mesma apresentação.

Também com o Teorema 3.1.1, podemos escrever $B_3 = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$ e, com isso, mostrar que $B_3 \cong \langle x, y \mid x^3 = y^2 \rangle$ da seguinte maneira.

Da apresentação $B_3 = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$, podemos obter a relação equivalente $(\sigma_1\sigma_2)^3 = (\sigma_2\sigma_1\sigma_2)^2 = (\sigma_1\sigma_2\sigma_1)^2$. Daí, usando o Lema 2.1.1, sabemos que $\langle \sigma_1, \sigma_2 \rangle = \langle \sigma_1\sigma_2, \sigma_2 \rangle = \langle \sigma_1\sigma_2, \sigma_2\sigma_1 \rangle = \langle \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_1 \rangle$. Portanto, fazendo $x = \sigma_1\sigma_2$ e $y = \sigma_1\sigma_2\sigma_1$, concluímos que $B_3 \cong \langle x, y \mid x^3 = y^2 \rangle$.

Observação. Um fato interessante é que como $SL(2,\mathbb{Z}) = \langle s, t \mid s^3 = t^2, t^4 = 1 \rangle$ (não será demonstrado), e $B_3 = \langle x, y \mid x^3 = y^2 \rangle$, podemos ver que o conjunto de relações de B_3 está contido no conjunto de relações de $SL(2,\mathbb{Z})$. Consequentemente, pelo Teorema 2.1.5, $SL(2,\mathbb{Z})$ é imagem homomórfica de B_3, i.e., B_3 é homomorfo a $SL(2,\mathbb{Z})$.

Lema 3.1.4 — Homomorfismo de comprimento. Seja $l : B_n \to \mathbb{Z}$ tal que se w é uma palavra nos geradores σ_i e seus inversos, então $l(w)$ é a soma dos expoentes dos σ_i em w. Então l é um homomorfismo, chamado **homomorfismo de comprimento** .

Demonstração. Sejam w_1, w_2 duas palavras em B_n tais que $w_1 = w_2$. Então, por definição, podemos, após uma quantidade finita de inserções e remoções de elementos da forma $\sigma_i\sigma_i^{-1}$, sair de w_1 e chegar em w_2. Como cada inserção/remoção desse tipo não altera a soma dos expoentes, pois estamos somando 0, então $l(w_1) = l(w_2)$, i.e., l está bem definida.

Agora, sejam w_1, w_2 duas palavras quaisquer em B_n. Note que $l(w_1w_2)$ é, por definição, a soma dos expoentes de w_1w_2. Mas essa soma nada mais é do que a soma dos expoentes de w_1 acrescida à soma dos expoentes de w_2, i.e., nada mais é do que $l(w_1) + l(w_2)$. Note que essa igualdade vale ainda que o final de w_1 seja o inverso do início de w_2 (por exemplo, $w_1 = \cdots\sigma_1\sigma_2^{-1}$ e $w_2 = \sigma_2\sigma_3\cdots$. Nesse caso, $l(w_1w_2)$ continua sendo igual a $l(w_1) + l(w_2)$). Logo, $l(w_1w_2) = l(w_1) + l(w_2)$ e l preserva a operação, sendo portanto, homomorfismo.

Por fim, note também que l é sobrejetora, uma vez que dado $n \in \mathbb{Z}$, podemos tomar a palavra $w = \underbrace{\sigma_1\sigma_1\cdots\sigma_1}_{n}$ de forma a obter $l(w) = n$. ■

Observação. A função l do Lema 3.1.4 é bem útil na verificação de equivalência entre duas tranças. Isso porque a função l é um invariante no grupo de tranças, i.e, se duas tranças são equivalentes, suas imagens por l (expoentes) devem ser iguais (segue da boa definição de l). Daí, podemos usar a contra-positiva: se duas tranças têm expoentes diferentes, então elas não podem ser equivalentes.

Da definição de l, é imediato que dada uma palavra w qualquer, $l(w^{-1}) = -l(w)$.

Uma aplicação interessante de l é a seguinte: se γ é uma trança qualquer conjugada ao seu inverso, i.e., se existe um trança δ tal que $\delta\gamma\delta^{-1} = \gamma^{-1}$, então $l(\gamma) = 0$.

De fato, se γ é conjugada ao seu inverso, sabemos que $l(\delta\gamma\delta^{-1}) = l(\gamma^{-1})$. Pela definição de

l, temos que $l(\delta\gamma\delta^{-1}) = l(\gamma)$. Daí, $l(\gamma) = l(\gamma^{-1}) = -l(\gamma)$ e, consequentemente, $l(\gamma) = 0$.

Podemos, ainda, pensar em tranças em termos de permutações, no sentido de que existe uma correspondência $\pi : B_n \to S_n$ em que tomamos uma trança, ignorando se os cruzamentos são por cima ou por baixo, e, numerando as posições inicial e final de cada corda, apenas lemos a permutação correspondente (lembre que S_n se refere ao grupo simétrico).

Lema 3.1.5 A função $\pi : B_n \to S_n$ definida anteriormente é um homomorfismo.

Demonstração. Seja $\psi : \underset{\sigma_i \mapsto (i\ i+1)}{B_n \to S_n}$. Note que ψ está bem definida, uma vez que $\sigma_i = \sigma_j \Rightarrow \psi(\sigma_i) = \psi(\sigma_j)$. Sejam $\sigma_i, \sigma_j \in B_n$ quaisquer. Suponha $|i-j| > 1$. Então, $\psi(\sigma_i\sigma_j) = (i\ i+1)(j\ j+1) = \psi(\sigma_i)\psi(\sigma_j)$. Se $|i-j| = 1$, podemos supor, sem perda de generalidade, que $j = i+1$. Então, temos $\psi(\sigma_i\sigma_{i+1}) = (i\ i+2\ i+1) = (i\ i+1)(i+1\ i+2) = \psi(\sigma_i)\psi(\sigma_{i+1})$. Portanto, ψ preserva a operação.

Por fim, note também que ψ é sobrejetora, uma vez que dada uma permutação qualquer, sempre podemos construir uma trança cuja imagem por ψ é tal permutação. Esse argumento será formalizado mais adiante. ■

Lema 3.1.6 Seja

$$\begin{aligned} G = \langle \tau_1, \ldots, \tau_{n-1} | & \tau_i\tau_j = \tau_j\tau_i, \text{ para } |i-j| > 1, \\ & \tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}, \text{ para } 1 \leq i \leq n-2, \\ & \tau_i^2 = 1, \text{ para } 1 \leq i \leq n-1 \rangle. \end{aligned}$$

Temos $S_n \cong G$, ou seja,

$$\begin{aligned} S_n = \langle \tau_1, \ldots, \tau_{n-1} | & \tau_i\tau_j = \tau_j\tau_i, \text{ para } |i-j| > 1, \\ & \tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}, \text{ para } 1 \leq i \leq n-2, \\ & \tau_i^2 = 1, \text{ para } 1 \leq i \leq n-1 \rangle. \end{aligned}$$

Demonstração. Primeiro, note que as transposições τ_i em S_n satisfazem todas as relações de G. Seja $\gamma : \underset{\tau_i \mapsto (i\ i+1)}{G \to S_n}$. A boa definição de γ e a propriedade de preservar a operação são demonstradas de maneira análoga ao que foi feito no Lema 3.1.5.

Então, seja $(i\ i+1) \in S_n$ qualquer e tome $\tau_i \in G$. Daí, $\gamma(\tau_i) = (i\ i+1)$ e, portanto, γ é sobrejetora.

Por fim, suponha $\gamma(\tau_i) = \gamma(\tau_j)$. Então, $(i\ i+1) = (j\ j+1)$, ou seja, $i = j$, o que é equivalente a $\tau_i = \tau_j$. Portanto, γ é injetora e, consequentemente, γ é um isomorfismo de G em

S_n, como queríamos demonstrar. ■

Podemos, ainda, definir uma trança geometricamente, como a seguir.

Definição 3.1.2 — Trança (geométrica). Seja $I = [0, 1]$. Uma trança geométrica em $n \geq 1$ cordas é um conjunto $b \subset \mathbb{R}^2 \times I$ formado por n intervalos topológicos disjuntos chamados cordas de b tal que a projeção $\mathbb{R}^2 \times I \to I$ mapeia cada corda homeomorficamente em I e

$$b \cap (\mathbb{R}^2 \times \{0\}) = \{(1, 0, 0), (2, 0, 0), \ldots, (n, 0, 0)\},$$
$$b \cap (\mathbb{R}^2 \times \{1\}) = \{(1, 0, 1), (2, 0, 1), \ldots, (n, 0, 1)\}.$$

Da Definição 3.1.2, podemos ver que cada corda de b intercepta cada plano $\mathbb{R}^2 \times \{t\}$, com $t \in I$, em exatamente um ponto. Também vemos que cada corda de b conecta um ponto $(i, 0, 0)$ a um ponto $(s(i), 0, 1)$, com $i, s(i) \in \{1, 2, \ldots, n\}$. A sequência $(s(1), s(2), \ldots, s(n))$ é uma permutação do conjunto $\{1, 2, \ldots, n\}$ chamada permutação subjacente de b.

Observação. Apesar de ser técnica, note que a Definição 3.1.2 nos diz algo simples; o que ela está falando é que uma trança é um subconjunto b da região $0 \leq z \leq 1$ de $\mathbb{R}^3$. Além disso, as interseções entre b e os planos $z = 0$ e $z = 1$ são, respectivamente, o conjunto de pontos $\{(1, 0, 0), \ldots, (n, 0, 0)\}$ e o conjunto de pontos $\{(1, 0, 1), \ldots, (n, 0, 1)\}$. Esses dois conjuntos são as extremidades de cada corda da trança.

Note também que, da Definição 3.1.1, sabemos que as cordas de uma trança não podem passar uma por dentro da outra, ou seja, não podem se interceptar e também sabemos que cada corda deve ir monotonicamente da esquerda para a direita, ou seja, não pode haver loops. A Definição 3.1.2 respeita essas condições, uma vez que cada plano $\mathbb{R}^2 \times \{t\}$, com $t \in [0, 1]$, intercepta cada corda de b em exatamente um ponto, logo cada corda vai monotonicamente de cima para baixo, e as cordas de b são disjuntas, isto é, não se interceptam. Essa última propriedade significa que entre os planos $\mathbb{R}^2 \times \{0\}$ e $\mathbb{R}^2 \times \{1\}$, o valor da coordenada y varia: começa em 0, aumenta (em módulo), e retorna a 0.

Podemos, ainda, reescrever a Definição 3.1.2 da seguinte forma:

Definição 3.1.3 Seja $n \in \mathbb{N}$ fixo. Sejam ainda n pontos distintos $p_1, \ldots, p_n$ em $\mathbb{R}^2$. Seja $(f_1, \ldots, f_n)$ uma n-upla de funções $f_i : [0, 1] \to \mathbb{R}^2$ tais que $f_i(0) = p_i$, $f_i(1) = p_j$ para algum $j = 1, \ldots, n$ e tais que os n caminhos

$$[0, 1] \to \mathbb{R}^2 \times [0, 1]$$
$$t \mapsto (f_i(t), t)$$

chamados cordas, tenham imagens disjuntas. Essas n cordas são chamadas de trança. O grupo de trança B_n em n cordas é o grupo de classes de isotopia de tranças. O produto de uma trança $(f_1(t), \ldots, f_n(t))$ por uma trança $(g_1(t), \ldots, g_n(t))$ é definido por

$$(f \bullet g)_i(t) = \begin{cases} f_i(2t), 0 \leq t \leq \frac{1}{2} \\ g_j(2t - 1), \frac{1}{2} \leq t \leq 1 \end{cases} \quad \text{sendo } j \text{ tal que } f_i(1) = p_j. \tag{3.1}$$

O interessante de se observar na Definição 3.1.3 é o modo como o produto de tranças foi apresentado na Definição 3.1.3. O que a equação 3.1 nos diz é que para multiplicar a trança $\alpha = (f_1(t), \ldots, f_n(t))$ pela trança $\beta = (g_1(t), \ldots, g_n(t))$, devemos diminuir o "tamanho" de ambas as tranças pela metade e, em seguida, conectá-las, colocando α "em cima" de β. Outra maneira equivalente de pensar é que apenas "encurtamos" α por um fator de $1/2$, sem transladá-la, e "encurtamos" β também por um fator de $1/2$, mas transladamos $1/2$ na direção negativa do eixo $\mathcal{O}z$. Essa definição é a mesma que a Definição 3.1.1, apenas formalizada!

"The essence of math is not to make simple things complicated, but to make complicated things simple."
— Stan Gudder

3.2 Propriedades de B_n e o grupo de tranças puras

Vamos demonstrar algumas propriedades das tranças. Para evitar confusões, por vezes será usada a notação 1_n para indicar a identidade de B_n.

Proposição 3.2.1 Para $1 \leq m \leq n$, a função $\psi : B_m \underset{\sigma_i \mapsto \sigma_i}{\to} B_n$ para $1 \leq i \leq m-1$ é um homomorfismo injetor de B_m em B_n e então podemos considerar B_m como um subgrupo de B_n. ∎

Demonstração. Pelo Teorema 3.1.1, temos

$$\begin{aligned} B_m = \langle \sigma_1, \sigma_2, \ldots, \sigma_{m-1} | \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ para } |i-j| > 1 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, 1 \leq i \leq m-2 \rangle, \\ B_n = \langle \sigma_1, \sigma_2, \ldots, \sigma_{m-1}, \ldots, \sigma_{n-1} | \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ para } |i-j| > 1 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, 1 \leq i \leq n-2 \rangle. \end{aligned}$$

Daí, como B_n satisfaz as relações de B_m, então pelo Teorema 2.1.5, ψ é homomorfismo.

Agora, suponha que existe $\beta \in B_n$ tal que $\psi(\beta) = 1_n$, ou seja, existe uma trança β de m cordas que, quando adicionamos $n-m$ cordas retas, se torna a trança trivial em B_n. Mas então devemos ter $\beta = 1_m$, logo ψ é injetora. ■

Observação. Como consequência da Proposição 3.2.1, se $\beta \in B_m$ é não trivial, então $\beta \in B_n$, $n \geq m$, também é não trivial (sendo $\beta \in B_n$ a trança β de m cordas adicionada de $n-m$ cordas retas);

Observação. Em particular, $B_m \cong B_n$ se, e só se, $m = n$.

Proposição 3.2.2 B_n é **livre de torção**, i.e., todo gerador de B_n tem ordem infinita. Equivalentemente, $\sigma_i^k \neq 1, \forall k \in \mathbb{Z}^*$. ∎

Demonstração. Vamos demonstrar a Proposição 3.2.2 por indução em i, o índice dos geradores. Como $B_2 = \langle \sigma_1 | - \rangle$, então $|\sigma_1| = \infty$. Logo, em B_n, $|\sigma_1| = \infty$. Suponha, então, que $\sigma_2 \in B_n$ tem ordem finita. Logo, por definição, $\exists l \in \mathbb{Z}$ tal que $\sigma_2^l = 1_n$. Daí,

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

Note que como $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, então $\sigma_i\sigma_{i+1}\sigma_i^{-1} = \sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}$ e, consequentemente, $\sigma_i\sigma_{i+1}^l\sigma_i^{-1} = \sigma_{i+1}^{-1}\sigma_i^l\sigma_{i+1}$. Substituindo na equação acima, temos

$$\begin{aligned} 1_n &= \sigma_1\sigma_2\sigma_1\sigma_2^l\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1} \\ &= \sigma_1\sigma_2\sigma_2^{-1}\sigma_1^l\sigma_2\sigma_2^{-1}\sigma_1^{-1} \\ &= \sigma_1^l \end{aligned}$$

o que é absurdo, logo $|\sigma_2| = \infty$.

Então, suponha indutivamente que $|\sigma_j| = \infty, 1 \leq j \leq i-1$. Suponha que $|\sigma_i| = l, l \in \mathbb{Z}$. Então,

$$\begin{aligned} 1_n &= \sigma_{i-1}\sigma_i\sigma_{i-1}\sigma_i^l\sigma_{i-1}^{-1}\sigma_i^{-1}\sigma_{i-1}^{-1} \\ &= \sigma_{i-1}\sigma_i\sigma_i^{-1}\sigma_{i-1}^l\sigma_i\sigma_i^{-1}\sigma_{i-1}^{-1} \\ &= \sigma_{i-1}^l \end{aligned}$$

o que é absurdo também. Então, por indução, $|\sigma_i| = \infty, i \geq 1$. ■

Observação. Como todo elemento não trivial de B_n tem ordem infinita, é possível mostrar que para toda trança β não trivial de B_n, $\beta^k \neq 1_n$ se $k \neq 0$.

Proposição 3.2.3 O grupo B_n, $n \geq 1$, é gerado pelos elementos σ_1 e $\alpha = \sigma_1\sigma_2\cdots\sigma_{n-1}$. ■

Demonstração. Queremos obter os σ_i, $i \geq 2$, em termos de σ_1 e α. Primeiro, vamos mostrar que

$$\sigma_{i+1} = \alpha\sigma_i\alpha^{-1}. \tag{3.2}$$

Para isso, note que

$$\begin{aligned} \alpha\sigma_i &= \sigma_1\sigma_2\cdots\sigma_{i-1}\sigma_i\sigma_{i+1}\sigma_{i+2}\cdots\sigma_{n-1}\sigma_i \\ &= \sigma_1\sigma_2\cdots\sigma_{i-1}(\sigma_i\sigma_{i+1}\sigma_i)\sigma_{i+2}\cdots\sigma_{n-1} \\ &= \sigma_1\sigma_2\cdots\sigma_{i-1}(\sigma_{i+1}\sigma_i\sigma_{i+1})\sigma_{i+2}\cdots\sigma_{n-1} \\ &= \sigma_{i+1}\sigma_1\sigma_2\cdots\sigma_{i-1}\sigma_i\sigma_{i+1}\cdots\sigma_{n-1} \\ &= \sigma_{i+1}\alpha, \end{aligned}$$

em que usamos as duas relações do Teorema 3.1.1. Mas $\alpha\sigma_i = \sigma_{i+1}\alpha$ é equivalente à equação (3.2), como queríamos demonstrar.

Agora, vamos mostrar, por indução, que $\sigma_i = \alpha^{i-1}\sigma_1\alpha^{1-i}$.

Para $i = 1$, temos $\sigma_1 = \alpha^0\sigma_1\alpha^0 = \sigma_1$. Suponha que $\sigma_{i-1} = \alpha^{(i-1)-1}\sigma_1\alpha^{1-(i-1)}$. Daí, temos

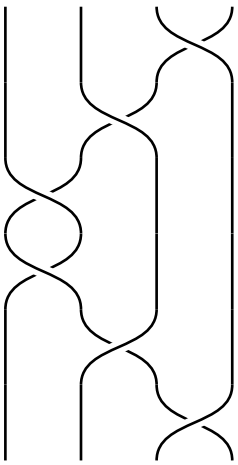
$$\begin{aligned}\alpha^{i-1}\sigma_1\alpha^{1-i} &= \alpha\Big(\alpha^{(i-1)-1}\sigma_1\alpha^{1-(i-1)}\Big)\alpha^{-1}\\ &= \alpha\sigma_{i-1}\alpha^{-1}\\ &= \sigma_i,\end{aligned}$$

em que usamos a equação (3.2) na última igualdade.

Ora! Então, como $\sigma_i = \alpha^{i-1}\sigma_1\alpha^{1-i}$, podemos representar todo gerador de B_n em termos de σ_1 e α. Consequentemente, σ_1 e α geram B_n. ■

Definição 3.2.1 — Grupo de Tranças puras. O núcleo do homomorfismo π definido no Lema 3.1.5 é chamado grupo de tranças puras e denotado por P_n. Uma trança geométrica de n cordas representa um elemento de P_n se, e só se, para todo $i = 1, 2 \ldots, n$, a corda dessa trança ligada ao ponto $(i, 0, 0)$ tem o segundo ponto fixo em $(i, 0, 1)$. Em símbolos, $P_n = \mathrm{Ker}(\pi : B_n \to S_n)$.

Em outras palavras, o grupo de tranças puras P_n nada mais é que o grupo formado pelas tranças cujas cordas chegam na posição original, correspondendo à permutação identidade. Abaixo segue um exemplo de trança pura.



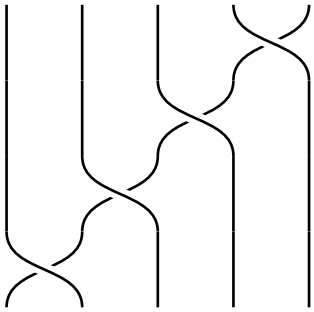
Note que todas as cordas saem e chegam à posição original.

Proposição 3.2.4 Temos que $P_n \lhd B_n$. Além disso, $B_n/P_n \cong S_n$ e $[B_n : P_n] = |B_n/P_n| = |S_n| = n!$. ■

Demonstração. Suponha $\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$ uma permutação de S_n. Queremos construir uma trança de n cordas baseados em α. Para isso, tome n pontos $A_1, A_2, \ldots, A_n$ na reta l_1 e n pontos $B_1, B_2, \ldots, B_n$ na reta l_2 paralela e "abaixo" de l_1. Tome os segmentos d_j que ligam o ponto A_j ao ponto B_{i_j} e escolha para todo cruzamento dos d_j, escolha arbitrariamente se ele

é por cima ou por baixo. Desse modo, formamos uma trança, γ que, por construção, é tal que $\pi(\gamma) = \alpha$. Portanto, o homomorfismo π do Lema 3.1.5 é sobrejetor.

Por exemplo, para a permutação (1 2 3 4 5) em S_5, podemos construir a seguinte trança:



Pela Definição 1.7.2, $\operatorname{Ker}\pi = \{\gamma \in B_n | \pi(\gamma) = (1)\} = P_n$. Daí, pelo Teorema 1.7.5, temos $P_n \triangleleft B_n$ e, pelo Teorema 1.7.3, temos $B_n/P_n \cong S_n$. Consequentemente, $[B_n : P_n] = |B_n/P_n| = |S_n| = n!$.
■

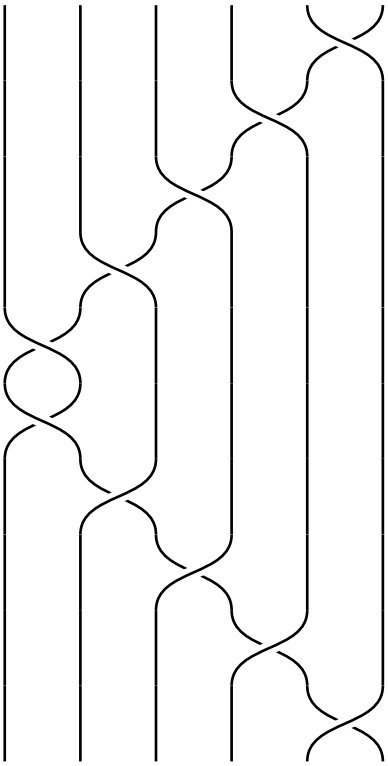
Para P_n, encontrar um conjunto de geradores não é tão simples quanto foi com B_n, pois nem sempre podemos "fatiar" uma trança pura em pedações óbvios que também são puros. Michael Artin mostrou que, para $1 \leq i < j \leq n$, se definirmos

$$A_{i,j} = \sigma_{j-1}\sigma_{j-2}\cdots\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}\cdots\sigma_{j-2}^{-1}\sigma_{j-1}^{-1}, \qquad \text{(Geradores de Artin)}$$

então o conjunto $\{A_{i,j}\}_{i,j}$ gera P_n. Em particular note que, usando um argumento combinatório, a cardinalidade desse conjunto é

$$(n-1) + (n-2) + \cdots + 2 + 1 = \frac{n(n-1)}{2} = \binom{n}{2}.$$

Abaixo está o diagrama de $A_{i,j}$, sendo i a corda mais à esquerda e j a corda mais à direita.



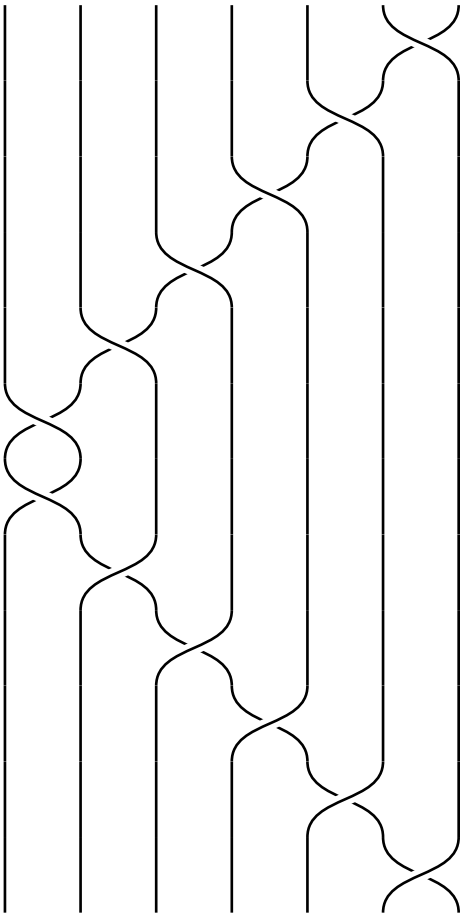
Algo interessante de se notar é que as tranças do conjunto $\{A_{i,j}\}_{i,j}$ são conjugadas umas às outras em B_n. De fato, seja

$$\alpha_{i,j} = \sigma_{j-1}\sigma_{j-2}\cdots\sigma_i$$

para $1 \leq i < j \leq n$. Através de diagramas, podemos verificar que valem as relações abaixo, dados quaisquer $1 \leq i < j < k \leq n$.

$$\alpha_{j,k}A_{i,j}\alpha_{j,k}^{-1} = A_{i,k} \quad \text{e} \quad \alpha_{i,k}A_{i,j}\alpha_{i,k}^{-1} = A_{j,k}.$$

Abaixo mostramos a primeira relação para $i = 1, j = 5, k = 7 = n$.



3.3 Centro de B_n

Para estudar o centro de B_n (e também de P_n), a trança abaixo é muito útil, chamada *volta completa* e denotada por Δ_n^2.

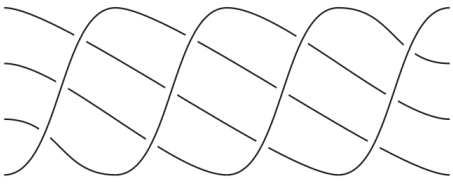


Figura 3.11: A volta completa, Δ_n^2.

Da Figura 3.11, podemos ver que $\Delta_n^2 = (\sigma_1\sigma_2\cdots\sigma_{n-1})^n$. Além disso, podemos também denotar por Δ_n a meia volta, e podemos escrevê-la em termos dos geradores σ_i de B_n da seguinte forma: $\Delta_n = (\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2})\cdots(\sigma_2\sigma_1)\sigma_1$. Daí, como a notação sugere, Δ_n^2 realmente é o quadrado de uma trança (e também a raiz n-ésima de uma trança, como podemos ver da Figura 3.11).

Em particular, note que a meia volta não comuta, em geral, com os geradores de B_n, uma vez que $\Delta_n\sigma_2 \neq \sigma_2\Delta_n$, por exemplo. De fato, o que ocorre é que $\sigma_i\Delta_n = \Delta_n\sigma_{n-i}$, ou seja, o cruzamento σ_i "desliza" (é claro que se n é par e $i = n/2$, então Δ_n comuta com σ_i).

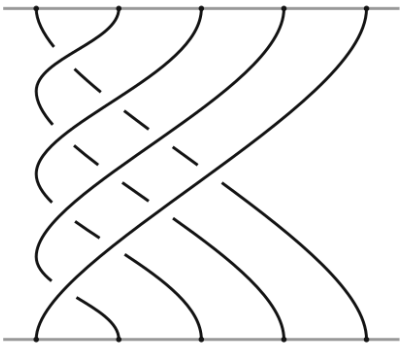


Figura 3.12: Diagrama de Δ_5. Podemos ver que o cruzamento σ_i "desliza", se tornando σ_{n-i}.

Contudo, Δ_n^2 comuta com toda trança de B_n, como é mostrado abaixo.

Demonstração. Primeiro, note que $\sigma_i\Delta_n = \Delta_n\sigma_{n-i}$, como ilustram os diagramas acima. Daí, temos

$$\sigma_i\Delta_n^2 = \sigma_i\Delta_n\Delta_n = \Delta_n\sigma_{n-i}\Delta_n = \Delta_n^2\sigma_i,$$

ou seja, Δ_n^2 comuta com todo gerador de B_n e, consequentemente, com toda trança de B_n. ■

Ora! Então Δ_n^2 pertence ao centro de B_n. Na verdade, é possível mostrar que Δ_n^2 gera o centro de B_n para $n \geq 3$, i.e.

Teorema 3.3.1 Se $n \geq 3$, então $Z(B_n) = Z(P_n) = \langle\Delta_n^2\rangle = \langle(\sigma_1\sigma_2\cdots\sigma_{n-1})^n\rangle$.

Em outras palavras, toda trança do centro de B_n é uma potência de Δ_n^2. Demonstramos o Teorema 3.3.1 para $n = 3$.

Proposição 3.3.1 $Z(B_3) = \langle(\sigma_1\sigma_2)^3\rangle$. ■

Demonstração. Primeiro, note que $(\sigma_1\sigma_2)^3\sigma_1 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1 = \sigma_1(\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2) = \sigma_1(\sigma_1\sigma_2)^3$ e também que $(\sigma_1\sigma_2)^3\sigma_2 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_2 = \sigma_2(\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2) = \sigma_2(\sigma_1\sigma_2)^3$. Portanto, $\langle(\sigma_1\sigma_2)^3\rangle \subseteq Z(B_3)$.

Agora, seja $g \in Z(B_3)$. Então, devemos ter, necessariamente, $g\sigma_1 = \sigma_1 g$ e $g\sigma_2 = \sigma_2 g$. Suponha, então, $g = \sigma_1^i\sigma_2^j$. Daí, temos

$$\begin{cases} \sigma_1^i\sigma_2^j\sigma_1 = \sigma_1^{i+1}\sigma_2^j \\ \sigma_1^i\sigma_2^{j+1} = \sigma_2\sigma_1^i\sigma_2^j \end{cases} \Rightarrow \begin{cases} \sigma_2^j\sigma_1 = \sigma_1\sigma_2^j \\ \sigma_1^i\sigma_2 = \sigma_2\sigma_1^i \end{cases} \Rightarrow i = j = 0.$$

Suponha, agora, $g = (\sigma_1\sigma_2)^i$, $i \neq 0$. Então, temos

$$\begin{cases} (\sigma_1\sigma_2)^i\sigma_1 = \sigma_1(\sigma_1\sigma_2)^i \\ (\sigma_1\sigma_2)^i\sigma_2 = \sigma_2(\sigma_1\sigma_2)^i \end{cases} \Rightarrow i = 3k, k \in \mathbb{Z}.$$

A última implicação se deve ao seguinte raciocínio. A quantidade de termos no produto $(\sigma_1\sigma_2)^i\sigma_1$ é $2i+1$. Para transformar $(\sigma_1\sigma_2)^i\sigma_1$ em $\sigma_1(\sigma_1\sigma_2)^i$, devemos manipular os $2i$ termos de $\sigma_2(\sigma_1\sigma_2)^{i-1}\sigma_1$ usando a relação $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ para chegar em $(\sigma_1\sigma_2)^i$. Ora! Mas para utilizar a relação, precisamos de blocos de 3 geradores, ou seja, devemos ter $i \in \mathbb{Z}$ tal que $\frac{2i}{3} \in \mathbb{Z}$. Como 2 e 3 são relativamente primos, devemos ter i múltiplo de 3. Por exemplo,

$$\sigma_2(\sigma_1\sigma_2)^{4-1}\sigma_1 = \sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1 = (\sigma_1\sigma_2)^3\sigma_2\sigma_1 \neq (\sigma_1\sigma_2)^4.$$

Daí, concluímos que todo elemento do centro de B_3 é uma potência de $(\sigma_1\sigma_2)^3$, ou seja, $Z(B_3) \subseteq \langle(\sigma_1\sigma_2)^3\rangle$. Portanto, $Z(B_3) = \langle(\sigma_1\sigma_2)^3\rangle$. ■

Proposição 3.3.2 Temos $l(\Delta_n^2) = n(n-1)$, sendo l a função homomorfismo de comprimento definida no Lema 3.1.4 e Δ_n^2 a volta completa em B_n. ▪

Demonstração. Escrevendo $\Delta_n^2 = (\sigma_1\sigma_2\cdots\sigma_{n-1})^n$, segue da definição de l que $l(\Delta_n^2) = n(n-1)$.

Também podemos escrever $l(\Delta_n^2) = 2l(\Delta_n)$ e, como

$$\Delta_n = (\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2})\cdots(\sigma_1\sigma_2)\sigma_1,$$

então

$$l(\Delta_n^2) = 2\Big((n-1) + (n-2) + \cdots + 2 + 1\Big) = 2\Big(\frac{n(n-1)}{2}\Big) = n(n-1).$$

■

Podemos ainda definir $f_n : P_n \to P_{n-1}$ como sendo a função que pega uma trança em P_n, retira a n-ésima corda e a mapeia à trança resultante em P_{n-1}. Essa função é um homomorfismo sobrejetor, chamada *homomorfismo esquecido*.

Para $n \geq 2$, definimos $U_n := \mathrm{Ker}(f_n : P_n \to P_{n-1})$. Do diagrama do gerador de Artin, $A_{i,j}$, fica claro que $A_{i,n} \in U_n$, com $1 \leq i \leq n-1$.

Teorema 3.3.2 Para todo $n \geq 2$, U_n é livre nos $n-1$ geradores $\{A_{i,n}\}_{i=1,2,\ldots,n-1}$.

Aceitaremos o Teorema 3.3.2 sem demonstração. Contudo, um corolário interessante é o seguinte.

Corolário 3.3.2.1 B_n e seus subgrupos são residualmente finitos.

Demonstração. Um grupo G é dito residualmente finito se para todo $\beta \in G - \{1\}$ existe um homomorfismo f de G em um grupo finito tal que $f(\beta) \neq 1$.

Sabemos que grupos livres são residualmente finitos e que o produto semidireto de dois grupos finitamente gerados e residualmente finitos é também residualmente finito.

Também sabemos, do Teorema 1.7.5, que $U_n \lhd P_n$. Da Definição 1.7.3, temos $P_n \cong U_n \rtimes P_{n-1}$. Tanto U_n quanto P_{n-1} são finitamente gerados e do Teorema 3.3.2, U_n é residualmente finito. Daí, por indução em n, o Teorema 3.3.2 implica P_n residualmente finito.

Note que qualquer extensão de um grupo residualmente finito P por um grupo finito é residualmente finita. Como B_n é uma extensão de P_n por S_n e P_n é residualmente finito, concluímos que B_n também é.

Por fim, observe que todos os subgrupos de um grupo residualmente finito são também residualmente finitos. ■

3.4 Tranças como espaços de configuração

Há varias conexões entre grupos de tranças e topologia, e uma delas envolve *espaços de configuração*, que nada mais são do que espaços que contêm todos os estados possíveis de um sistema. Por vezes, espaços de configuração são chamados de *espaços de estado* ou *espaços de parâmetros* .

Por exemplo, podemos usar um espaço de configuração para modelar o movimento coletivo de vários objetos, como carros nas ruas de uma cidade ou moléculas em uma solução ou ainda robôs em uma fábrica.

Para um exemplo mais concreto, considere o seu braço. Nele, há três juntas: uma no ombro, uma no cotovelo e uma no pulso. Tanto o seu ombro quanto o seu pulso têm dois graus de liberdade (i.e., podem girar em dois sentidos diferentes), enquanto que o seu cotovelo tem apenas um grau de liberdade, totalizando cinco dimensões de configuração.

Um braço robótico modelado a partir do seu braço tem de navegar por um espaço de configuração cinco-dimensional para poder aproveitar toda a flexibilidade existente nesse sistema de juntas. Para ilustrar, imagine que ao invés de uma mão, você tem uma plataforma rígida

conectada ao seu pulso e suponha que você queira levantar um copo d'água de abaixo da sua cintura até acima do seu ombro. Isso não será possível de fazer com a plataforma rígida no lugar da mão, porque apenas a rotação do ombro não é suficiente para fazer o movimento desejado (isso é o que os bebês fazem, e eles sempre derramam a água).

Mas qual a conexão entre espaços de configuração e grupos de trança? Bom, até agora, falamos de tranças individuais como objetos topológicos, como indicam as Definições 3.1.2 e 3.1.3. Contudo, os grupos de trança em si também são objetos topológicos, no sentido de que cada grupo de trança descreve, de forma natural, os diferentes tipos de *loops* que existem em um certo espaço de configuração. O espaço em questão modela o movimento coletivo de n partículas distintas no plano que não podem colidir.

Então, imagine n partículas no plano e estenda esse plano para formar a parede esquerda de uma trança. Agora, deslize o plano da esquerda para a direita, e imagine que cada partícula deixa um rastro à medida que o plano se move. O que acontece?

Bom, se as partículas ficam paradas (no plano), então quando o plano parar, você terá n trilhas paralelas: a trança identidade!

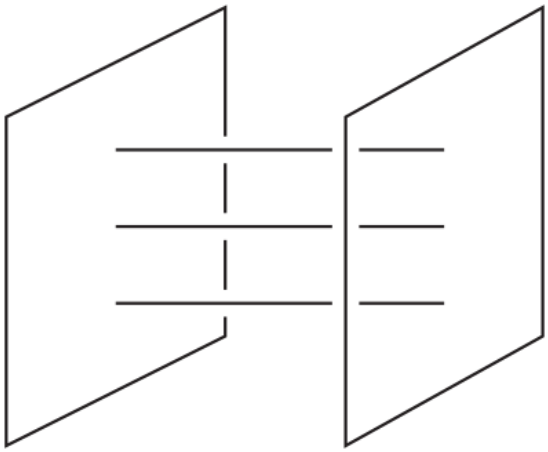


Figura 3.13: A trança identidade em um espaço de configuração

Entretanto, se as partículas se movem no plano à medida que eles desliza, o que ocorre? Bom, desde que nenhum par de partículas colida, veremos uma trança! E claramente toda trança pode ser feita desse modo. Veja a figura abaixo. Note que estamos visualizando a direção x como o eixo temporal.

Para um exemplo mais visual, podemos observar o movimento dos planetas do Sistema Solar, como nesse vídeo.

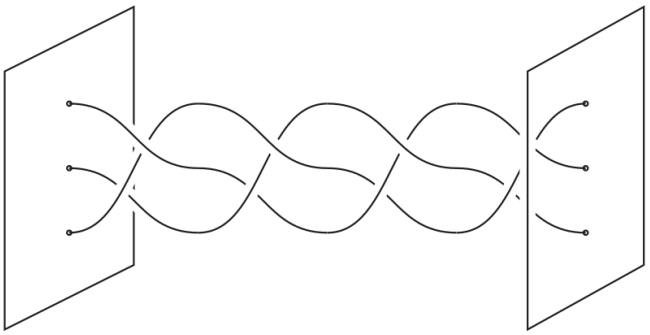


Figura 3.14: Uma trança não trivial em um espaço de configuração.

Para fazermos o produto de duas tranças usando essa ideia, precisamos ter certeza de que o conjunto de partículas no final da trança está no mesmo lugar que no começo da trança, pois assim podemos concatenar duas tranças sem haver nenhuma descontinuidade no meio.

A posição inicial é uma **configuração** de n partículas. O conjunto de todas as configurações possíveis é o espaço de configuração

$$C_n(\mathbb{R}^2) = \{(p_1, \ldots, p_n) \in (\mathbb{R}^2)^n \mid p_i \neq p_j \text{ para } i \neq j\}, \tag{3.3}$$

em que a condição $p_i \neq p_j$ indica a necessidade de um par partículas não colidirem.

O que definimos em (3.3) foi o conjunto de configurações **ordenadas**. Como o nosso propósito é descrever tranças, gostaríamos de ignorar a ordem e apenas focar no conjunto de partículas, e.g., queremos considerar (p_1, p_2) como o mesmo que (p_2, p_1) e pensar em ambos apenas como $\{p_1, p_2\}$. Para isso, definimos a versão não ordenada:

$$UC_n(\mathbb{R}^2) = \{\{p_1, \ldots, p_n\} \subset \mathbb{R}^2 \mid p_i \neq p_j \text{ para } i \neq j\} \tag{3.4}$$

ou, em palavras, o conjunto de subconjuntos de n pontos do plano.

Podemos também denotar $C_n(\mathbb{R}^2)$ por $\mathbb{F}_n(\mathbb{R}^2)$ e $UC_n(\mathbb{R}^2)$ por $\widetilde{\mathbb{F}}_n(\mathbb{R}^2)$, sendo $\sim$ a relação de equivalência cujas classes são os conjuntos de permutações de um dado ponto em $(\mathbb{R}^2)^n$.

De forma geral, se $\mathbb{M}$ é uma variedade de dimensão maior ou igual a 2, então $\mathbb{F}_n(\mathbb{M})$ denota o subespaço de $\mathbb{M}^{(n)}$ definido por

$$\mathbb{F}_n(\mathbb{M}) = \{(x_1, \ldots, x_n) \in \mathbb{M}^{(n)} \mid x_i \neq x_j \text{ para } i \neq j\}. \tag{3.5}$$

Esse subespaço é chamado *espaço de configuração* de $\mathbb{M}$. Sendo $\sim$ a mesma relação de equivalência definida acima, o espaço quociente ${}^{\mathbb{F}_n(\mathbb{M})}/_{\sim}$, que também pode ser denotado por $\widetilde{\mathbb{F}}_n(\mathbb{M})$, é definido por

$$\widetilde{\mathbb{F}}_n(\mathbb{M}) = \{\{x_1, \ldots, x_n\} \subset \mathbb{M} \mid x_i \neq x_j \text{ para } i \neq j\}. \tag{3.6}$$

Pelo modo como definimos $\sim$ acima, podemos ver que $UC_n(\mathbb{R}^2) = C_n(\mathbb{R}^2)/S_n$. Agora, voltando na Figura 3.14, tanto a parede da esquerda quando a parede da direita representam pontos de $UC_3(\mathbb{R}^2)$. Na verdade, as duas paredes representam o mesmo ponto (mas não o mesmo ponto de $C_3(\mathbb{R}^2)$, pois a configuração final é (p_2, p_3, p_1), sendo p_1 o ponto inferior e p_3 o ponto superior).

Além disso, quando deslizamos a parede da esquerda para a direita de forma a criar a trança, em cada instante de tempo temos um ponto de $UC_3(\mathbb{R}^2)$. Isso se deve ao fato de que cada corda é monotônica. Em outras palavras, podemos ver a trança como um *loop* em $UC_3(\mathbb{R}^2)$.

Para fixar, podemos pensar em esquerda-direita como o eixo temporal, e então a trança tridimensional toda é como um filme de três partículas dançando no plano bidimensional (sem colidir) e retornando ao lugar onde começaram.

Equivalentemente, a trança é o gráfico de uma função $[0, 1] \to UC_3(\mathbb{R}^2)$, cujos pontos inicial e final concordam, ou seja, podemos pensar em tranças como *loops* de configurações. De fato, essa é, essencialmente, uma correspondência injetiva.

Antes de prosseguirmos, vamos definir de maneira informal o que vem a ser um grupo fundamental.

Definição 3.4.1 — Grupo Fundamental. Dado um espaço topológico X e um ponto qualquer $x_0 \in X$, o conjunto de loops que começam e terminam em x_0 e que são caminhos fechados em X é chamado grupo fundamental de X com ponto base x_0 e denotado por $\pi_1(X, x_0)$.

Um detalhe importante é que se X é conexo por caminhos (i.e., dado um par de pontos em X, existe um caminho totalmente contido em X que liga esses dois pontos), então a escolha do ponto base não faz diferença. Esse é o nosso caso, e então denotaremos o grupo fundamental de X por $\pi_1(X)$ apenas.

Com a Definição 3.4.1, podemos enunciar o seguinte teorema.

Teorema 3.4.1 O grupo fundamental $\pi_1(UC_n(\mathbb{R}^2))$ é isomorfo ao grupo de trança B_n, e o grupo fundamental $\pi_1(C_n(\mathbb{R}^2))$ é isomorfo ao grupo de tranças puras P_n.

Da Definição 3.4.1, podemos ver que o grupo fundamental trata sobre os diferentes *loops* em

um espaço topológico. A noção de equivalência de *loops* (i.e., homotopia, que nada mais é que uma deformação contínua de um caminho para outro) se traduz diretamente para nossa noção de equivalência de tranças.

Portanto, o Teorema 3.4.1 nos diz não só que tranças podem ser vistas como *loops* em um espaço de configuração, mas também que podemos construir todos os *loops* nesse espaço de configuração dessa maneira.

Além de nos proporcionar um outro modo de pensar em tranças, essa perspectiva topológica é útil tanto para provar coisas sobre tranças quanto para realizar generalizações interessantes. Por exemplo, é possível demonstrar o Teorema 3.1.1 usando essas ideias.

Para outro exemplo, observe que a própria notação, $C_n(\mathbb{R}^2)$ sugere uma generalização óbvia, de substituir $\mathbb{R}^2$ por outros espaços topológicos, como superfícies, grafos ou variedades. Da mesma forma, o conjunto de (classes de equivalência de) *loops* em um espaço de configuração de n partículas em um espaço topológico X é chamado de *grupo de trança associado a* X.

Em símbolos, escrevemos $\pi_1(UC_n(X)) = B_n(X)$ e $\pi_1(C_n(X)) = P_n(X)$. Desse modo, os grupos usuais B_n e P_n são, na verdade, $B_n(\mathbb{R}^2)$ e $P_n(\mathbb{R}^2)$.

Por exemplo, sendo $X = \mathbb{R}$ e tomando $n = 2$, temos que

$$UC_2(\mathbb{R}) = \big\{\{p_1, p_2\} \subset \mathbb{R} \mid p_1 \neq p_2\big\},$$
$$C_2(\mathbb{R}) = \big\{(p_1, p_2) \in \mathbb{R}^2 \mid p_1 \neq p_2\big\},$$

ou seja, os espaços de configuração não ordenado e ordenado, respectivamente, de dois pontos em uma reta. Não é difícil perceber que tanto $C_2(\mathbb{R})$ quanto $UC_2(\mathbb{R})$ possuem 3 componentes conexos e, em geral, $C_n(\mathbb{R})$ e $UC_n(\mathbb{R})$ possuem $n+1$ componentes conexos. Também podemos tomar $X = \mathbb{S}^1$, ou seja, uma circunferência. Nesse caso, $C_n(\mathbb{S}^1)$ e $UC_n(\mathbb{S}^1)$ têm n componentes conexos.

Agora, vamos considerar $X = \mathbb{S}^2$, a esfera em $\mathbb{R}^3$. Nesse caso, $B_n(X) = B_n(\mathbb{S}^2)$ é chamado de *grupo de tranças esféricas*. Uma primeira pergunta natural seria: qual a diferença entre tranças esféricas e "tranças planares"? Bom, podemos imaginar as paredes dos diagramas das tranças planares como sendo pequenos pedaços de esferas enormes, por exemplo, como mostra a Figura 3.15 abaixo (na verdade, essa ideia pode ser aplicada a tranças em qualquer superfície, não apenas na esfera).

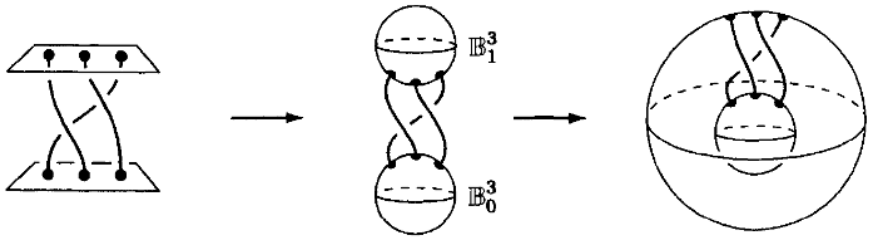


Figura 3.15: Diagrama de uma trança esférica

Logo, temos de modo natural a função $f : B_n(\mathbb{R}^2) \to B_n(\mathbb{S}^2)$. Não é muito difícil perceber que podemos obter toda trança esférica a partir de uma trança planar, i.e., que f é sobrejetora. Contudo, f não é injetora.

Isso se deve ao fato de que, para tranças esféricas, as cordas podem ser deformadas de modo a "darem a volta", como mostra a figura a seguir. Podemos pensar em $B_n(\mathbb{R}^2)$ como tranças dentro de um cubo, ficando "presas" lá dentro e, portanto, impossibilitadas de realizar movimentos como os que estão abaixo.

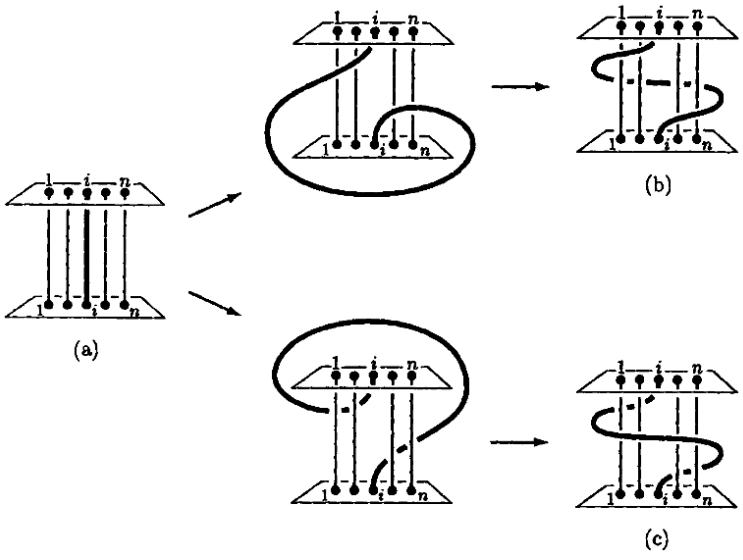


Figura 3.16: Movimentos possíveis para tranças esféricas, mas impossíveis para tranças planares

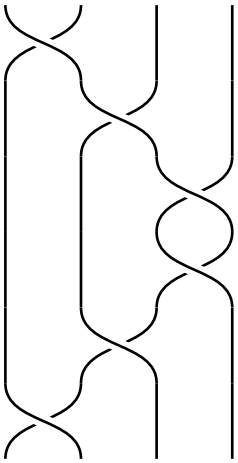
Como os geradores σ_i de $B_n(\mathbb{R}^2)$ também são geradores de $B_n(\mathbb{S}^2)$, as relações das tranças planares continuam válidas para as tranças esféricas. Contudo, os novos movimentos mostrados na Figura 3.16 nos dão uma nova relação em $B_n(\mathbb{S}^2)$, a saber

$$\sigma_{i-1}\sigma_{i-2}\cdots\sigma_2\sigma_1^2\sigma_2\sigma_3\cdots\sigma_{n-2}\sigma_{n-1}^2\sigma_{n-2}\sigma_{n-3}\cdots\sigma_i = 1. \tag{3.7}$$

Contudo, toda relação, para $i = 1, 2 \ldots, n-1$, em (3.7) é consequência da única relação

$$(\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_{n-1}\sigma_{n-2}\cdots\sigma_1) = 1. \tag{3.8}$$

De fato, essa relação é dada pelo mesmo movimento que o diagrama (b) da Figura 3.16, mas com a corda 1 indo para a direita, como o diagrama abaixo.



Portanto, uma apresentação de $B_n(\mathbb{S}^2)$ tem os mesmos geradores e relações que $B_n(\mathbb{R}^2)$, mas com a última relação em (3.8). De fato, essa é a apresentação completa de $B_n(\mathbb{S}^2)$, conforme o teorema abaixo, que não será demonstrado.

Teorema 3.4.2 O grupo de tranças esféricas $B_n(\mathbb{S}^2)$ tem apresentação

$$\begin{aligned} B_n(\mathbb{S}^2) = \langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} | & \sigma_i\sigma_j = \sigma_j\sigma_i, \text{ para } |i-j| > 1, \\ & \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \text{ para } 1 \le i \le n-2, \\ & \sigma_1\sigma_2\cdots\sigma_{n-2}\sigma_{n-1}^2\sigma_{n-2}\cdots\sigma_2\sigma_1 = 1 \rangle. \end{aligned}$$

Então, voltando à nossa função f: ela não é injetora, pois a trança em (3.8) pertence ao núcleo de f, ou seja, Ker f não é trivial. Outra trança que pertence ao núcleo de f é $(\Delta_n^2)^2$, o quadrado da volta completa, que tem ordem 2 em $B_n(\mathbb{S}^2)$.

Na verdade, esse fato pode ser generalizado no seguinte lema.

Lema 3.4.1 Para todo $n > 2$, a trança de Dirac $\delta = (\sigma_1\sigma_2\cdots\sigma_{n-1})^{kn} = (\Delta_n^2)^k$ é trivial em $B_n(\mathbb{S}^2)$ se, e só se, k é par.

Demonstração. Já sabemos que $(\Delta_n^2)^2 = 1$ em $B_n(\mathbb{S}^2)$. Então, se k é par, podemos escrever $k = 2j$ e segue que $(\Delta_n^2)^k = [(\Delta_n^2)^2]^j = 1^j = 1$. Por outro lado, como $|\Delta_n^2| = 2$ em $B_n(\mathbb{S}^2)$, então $(\Delta_n^2)^k = 1$ implica que $2 \mid k$, i.e, k par. ■

Do Teorema 3.4.2, podemos obter alguns fatos interessantes sobre o grupo de tranças esféricas.

Por exemplo, $B_2(\mathbb{S}^2) = \langle \sigma_1 \mid \sigma_1^2 = 1 \rangle$, ou seja, $B_2(\mathbb{S}^2)$ é um grupo finito de ordem 2 com um gerador: $\mathbb{Z}_2$. Além disso, também podemos definir o homomorfismo de comprimento que definimos para as tranças planares, mas com uma pequena alteração.

Proposição 3.4.1 Seja $\beta \in B_n(\mathbb{S}^2)$. Tomando $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$, sendo $\varepsilon_i = \pm 1$ para $i = 1, 2, \ldots, k$, então podemos definir a função l, chamada *homomorfismo de comprimento*, de $B_n(\mathbb{S}^2)$ em $\mathbb{Z}$ como

$$l(\beta) = \sum_{i=1}^{k} \varepsilon_i \bmod(2(n-1)),$$

ou seja, a soma dos expoentes módulo $2(n-1)$. Então, l é invariante em $B_n(\mathbb{S}^2)$, i.e., se $\beta = \beta'$ em $B_n(\mathbb{S}^2)$, então $l(\beta) = l(\beta') \bmod(2(n-1))$. ∎

Demonstração. Do Teorema 3.4.2, sabemos todas as relações de $B_n(\mathbb{S}^2)$. Para as duas primeiras, $l(\beta)$ é constante para cada uma dessas relações. Contudo, para a terceira relação, $l(\beta)$ difere por um fator de $\pm 2(n-1)$ para os dois lados da relação. Como $l(1) = 0$ e l está bem definida (demonstração análoga à do Lema 3.1.4), devemos ter a igualdade módulo $2(n-1)$. ■

∎ **Exemplo 3.4.1** Como $l((\sigma_1\sigma_2)^3) = 6 \neq 0 \bmod 4$ e $l(1) = 0$, então, em $B_3(\mathbb{S}^2)$, $(\sigma_1\sigma_2)^3 \neq 1$. ∎

∎ **Exemplo 3.4.2** Temos $\sigma_1^4 = 1$ em $B_3(\mathbb{S}^2)$, mas $\sigma_1^4 \neq 1$ em $B_4(\mathbb{S}^2)$. Esse exemplo nos mostra uma diferença notável entre $B_n(\mathbb{R}^2)$ e $B_n(\mathbb{S}^2)$, pois se β é trivial em $B_m(\mathbb{R}^2)$ e $m \leq n$, então β também é trivial em $B_n(\mathbb{R}^2)$, enquanto que para $B_m(\mathbb{S}^2)$ e $B_n(\mathbb{S}^2)$ isso, em geral, não é verdade. ∎

Note também que a recíproca da Proposição 3.4.1 é falsa. Por exemplo, $\sigma_1^6 \neq 1$ em $B_4(\mathbb{S}^2)$ mas $l((\sigma_1)^6) = 0 \bmod 6 = l(1)$.

A apresentação no Teorema 3.4.2 tem também uma interessante consequência, enunciada no Lema 3.4.2. Antes, contudo, introduziremos um pequeno conceito, as *transformações de Tietze*.

Transformações de Tietze

Dada uma apresentação de um grupo G, temos os seguintes movimentos:

1. se uma relação pode ser deduzida a partir das relações existentes, então podemos adicionar essa nova relação à apresentação. Por exemplo, se $G = \langle x \mid x^3 = 1 \rangle$, obtemos a relação $x^6 = 1$ a partir de $x^3 = 1$. Logo, podemos escrever $G = \langle x \mid x^3 = 1, x^6 = 1 \rangle$.

2. Reciprocamente, se uma relação da apresentação pode ser deduzida a partir das outras, então podemos removê-la. Em $G = \langle x \mid x^3 = 1, x^6 = 1\rangle$, a relação $x^6 = 1$ pode ser deduzida de $x^3 = 1$ e, portanto, pode ser removida da apresentação. Contudo, note que não podemos remover $x^3 = 1$, pois teríamos outro grupo.

3. Podemos adicionar um gerador escrito como uma palavra nos geradores originais. Começando com $G = \langle x \mid x^3 = 1\rangle$ e fazendo $y = x^2$, a nova apresentação $G = \langle x, y \mid x^3 = 1, y = x^2\rangle$ define o mesmo grupo.

4. De modo semelhante, se podemos formar uma relação em que um dos geradores é uma palavra nos outros geradores, então esse gerador pode ser removido. Por exemplo, a apresentação do grupo abeliano de ordem 4, $G = \langle x, y, z \mid x = yz, y^2 = 1, z^2 = 1, x = x^{-1}\rangle$ pode ser substituído por $G = \langle y, z \mid y^2 = 1, z^2 = 1, (yz) = (yz)^{-1}\rangle$.

Usaremos essas transformações para demonstrar o seguinte lema.

Lema 3.4.2 $B_3(\mathbb{S}^2)$ tem apresentação $\langle a, b \mid b^6 = 1, a^2 = b^3 = (ab)^2\rangle$, sendo, portanto, isomorfo a Q_6, o grupo dicíclico de ordem 12.

Demonstração. Sabemos, do Teorema 3.4.2, que

$$B_3(\mathbb{S}^2) = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2,\ \sigma_1\sigma_2^2\sigma_1 = 1\rangle.$$

Fazendo $a = \sigma_1\sigma_2\sigma_1$ e $b = \sigma_1\sigma_2$, temos:

$$\begin{aligned} a^2 &= \sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2 = (\sigma_1\sigma_2)^3 = b^3, \\ (ab)^2 &= \sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1\sigma_2 \underbrace{\sigma_1\sigma_2\sigma_2\sigma_1}_{1} \sigma_1\sigma_2 = (\sigma_1\sigma_2)^3 = b^3, \\ b^6 &= \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2 = \underbrace{\sigma_1\sigma_2\sigma_2\sigma_1}_{1}\sigma_2\sigma_2\underbrace{\sigma_1\sigma_2\sigma_2\sigma_1}_{1}\sigma_2\sigma_2 = \sigma_2^4. \end{aligned}$$

Vamos mostrar que tanto σ_1 quanto σ_2 têm ordem 4. Então, seja N o fecho normal de a^2, i.e., $N = \{1, a\}$. Daí, $N \lhd B_3(\mathbb{S}^2)$ e, portanto, o grupo quociente $B_3(\mathbb{S}^2)/N$ tem apresentação $\langle a, b | a^2 = b^3 = (ab)^2 = 1\rangle$, que é a apresentação de S_3, o grupo simétrico em 3 elementos. Logo, $|B_3(\mathbb{S}^2)| = |N| \cdot |S_3| = 12$.

Por fim, note que $(ab)^2 = a^2$ implica $a = b^{-1}ab^{-1}$, logo

$$\sigma_1^4 = (b^{-1}a)^4 = (b^{-1}ab^{-1})a(b^{-1}ab^{-1})a = a^4 = 1.$$

Observe o diagrama abaixo.

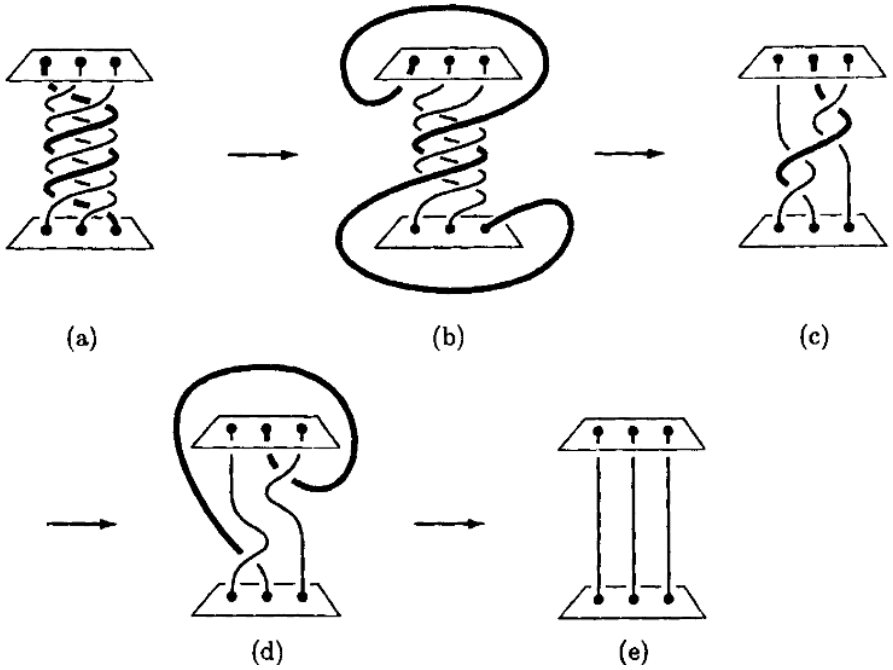


Figura 3.17: $a^4 = 1$ em $B_3(\mathbb{S}^2)$

Como $\sigma_1 \neq 1$ e $\sigma_1^2 \neq 1$, então, pela Proposição 3.4.1, $|\sigma_1| = 4$.

Similarmente, $(ab)^2 = a^2$ implica $bab = a$ e também $ba = a^{-1}b^2$, logo

$$\sigma_2^4 = (a^{-1}b^2)^4 = (ba)^4 = (bab)a(bab)a = a^4 = 1.$$

Como $\sigma_2 \neq 1$ e $\sigma_2^2 \neq 1$ então, da Proposição 3.4.1, temos $|\sigma_2| = 4$. Além disso, como $a^4 = 1$, temos $b^6 = 1$. Por fim, da Tabela 2.1, vemos que $B_3(\mathbb{S}^2) \cong Q_6$, o grupo dicíclico de ordem 12. ■

Do Lema 3.4.2, podemos listar os elementos de $B_3(\mathbb{S}^2)$:

$$B_3(\mathbb{S}^2) = \left\{1, a, a^2, a^3, b, b^2, b^4, b^5, ab, ab^2, ab^4, ab^5\right\}.$$

Podemos ainda escrever esse elementos em termos dos geradores σ_1 e σ_2. Com algumas simplificações, obtemos:

$$B_3(\mathbb{S}^2) = \left\{1, \sigma_1\sigma_2\sigma_1, (\sigma_1\sigma_2\sigma_1)^2, (\sigma_1\sigma_2\sigma_1)^3, \sigma_1\sigma_2, (\sigma_1\sigma_2)^2, \sigma_1^3\sigma_2, \sigma_2\sigma_1, \sigma_1, \sigma_2^3, \sigma_2\sigma_1^3\sigma_2, \sigma_1^3\right\}.$$

Fazendo os diagramas, vemos que apenas 1 e $(\sigma_1\sigma_2\sigma_1)^2 = a^2 = b^3$ são tranças puras. Além disso, como $a^4 = 1 = b^6$, concluímos que $P_3(\mathbb{S}^2) = \langle a^2 \rangle = \langle b^3 \rangle$.

Agora, vamos considerar $B_4(\mathbb{S}^2)$, que tem apresentação

$$B_4(\mathbb{S}^2) = \langle \sigma_1, \sigma_2, \sigma_3 | \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$$

$$\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$$
$$\sigma_1\sigma_3 = \sigma_3\sigma_1$$
$$\sigma_1\sigma_2\sigma_3^2\sigma_2\sigma_1 = 1\rangle.$$

Seja N o fecho normal de $\sigma_1\sigma_3^{-1}$. Então, a apresentação do grupo quociente $G = B_4(\mathbb{S}^2)/N$, é obtida de $B_4(\mathbb{S}^2)$ adicionando a relação $\sigma_1\sigma_3^{-1} = 1$ ou, equivalentemente, $\sigma_1 = \sigma_3$. O efeito dessa relação extra é reduzir o número de relações para duas, a saber

$$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \quad \text{e} \quad \sigma_1\sigma_2\sigma_1^2\sigma_2\sigma_1 = 1.$$

A última relação pode ser manipulada como segue:

$$\begin{aligned} 1 &= \sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1 \\ &= \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2 \\ &= (\sigma_1\sigma_2)^3 \end{aligned}$$

Portanto, $G = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, (\sigma_1\sigma_2)^3 = 1\rangle$. Como antes, tome $a = \sigma_1\sigma_2\sigma_1$ e $b = \sigma_1\sigma_2$. Como $\sigma_1 = b^{-1}a$ e $\sigma_2 = a^{-1}b^2$, as relações de G se tornam $a^2 = b^3$ e $b^3 = 1$, logo $G = \langle a, b \mid a^2 = b^3 = 1\rangle$. Vamos mostrar que G é infinito, usando o seguinte lema, que será aceito sem demonstração.

Lema 3.4.3 O grupo triangular, ou grupo de Dyck, $T(l, m, n) = \langle a, b \mid a^l = b^m = (ab)^n = 1\rangle$ é finito se, e só se, $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1 > 0$.

Proposição 3.4.2 $G = \langle a, b \mid a^2 = b^3 = 1\rangle$ é infinito e, consequentemente, $B_4(\mathbb{S}^2)$ é infinito. ∎

Demonstração. Seja $\widehat{G} = \langle a, b | a^2 = b^3 = (ab)^7 = 1\rangle$. Note que $\widehat{G}$ é um grupo quociente de G e, além disso, $\widehat{G} = T(2, 3, 7)$. Do Lema 3.4.3, temos $\widehat{G}$ infinito, pois $\frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 < 0$. Logo, como $\widehat{G}$ é um grupo quociente de G, então G também é infinito, pois se todo grupo finito com apresentação finita tem, no máximo, tantos geradores quanto relações. Por fim, como G é um grupo quociente de $B_4(\mathbb{S}^2)$, temos $B_4(\mathbb{S}^2)$ infinito, também pelo mesmo fato citado acima sobre grupos finitos e finitamente apresentados. Observe que o número 7 não tem nada de especial: poderíamos tomar qualquer $k \geq 7$. ■

Podemos, ainda, generalizar esse fato no seguinte lema, que não será demonstrado.

Lema 3.4.4 $|B_n(\mathbb{S}^2)| = \infty$ para todo $n \geq 4$.

Observando o Lema 3.4.4, a distinção mais simples que podemos fazer entre $B_n(\mathbb{R}^2)$ e $B_n(\mathbb{S}^2)$ é que $B_n(\mathbb{R}^2)$ é finito apenas para $n = 1$, enquanto que $B_n(\mathbb{S}^2)$ é finito para $n = 1, 2$ e 3.

Contudo, a maior diferença entre esses dois grupos (ou famílias de grupos) é o fato de que $B_n(\mathbb{R}^2) < B_{n+1}(\mathbb{R}^2)$, como mostrado na Proposição 3.2.1, enquanto que $B_n(\mathbb{S}^2) \not< B_{n+1}(\mathbb{S}^2)$.

De fato, a relação $(\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_{n-1}\cdots\sigma_2\sigma_1) = 1$ em $B_n(\mathbb{S}^2)$ pode não ser válida em $B_{n+1}(\mathbb{S}^2)$. Por exemplo, do Teorema 3.4.2, sabemos que $\sigma_1^2 = 1$ em $B_2(\mathbb{S}^2)$, mas não em $B_3(\mathbb{S}^2)$, devido à Proposição 3.4.1.

Além disso, também do Teorema 3.4.2, $\sigma_1\sigma_2^2\sigma_1 = 1$ em $B_3(\mathbb{S}^2)$, mas não em $B_4(\mathbb{S}^2)$, de novo devido à Proposição 3.4.1.

Consequentemente, a função identidade $\psi : B_n(\mathbb{S}^2) \underset{\sigma_i \mapsto \sigma_i}{\to} B_{n+1}(\mathbb{S}^2)$, para $1 \leq i \leq n-1$, não é um homomorfismo e não podemos considerar $B_n(\mathbb{S}^2)$ como um subgrupo natural de $B_{n+1}(\mathbb{S}^2)$.

É interessante notar também que algumas tranças não identidades são triviais em $B_n(\mathbb{S}^2)$, i.e., $B_n(\mathbb{S}^2)$ **não é** livre de torção, como mostrado no seguinte lema.

Lema 3.4.5 Para todo $n \geq 2$, $\gamma = \sigma_1\sigma_2\cdots\sigma_{n-1}$ (a raiz n-ésima da volta completa) tem ordem finita maior que 1 e, portanto, $B_n(\mathbb{S}^2)$ tem elementos de torção.

Demonstração. Primeiro, note que como $l(\gamma) = (n-1) \neq 0 \bmod(2(n-1))$, então, para todo $n \geq 2$, $\gamma \neq 1$. Por outro lado, sabemos que o quadrado da volta completa é trivial, i.e., $(\Delta_n^2)^2 = 1$, logo, como $\Delta_n^2 = \gamma^n$, temos $\gamma^{2n} = 1$.

Portanto, γ tem ordem finita k com $2 \leq k \leq 2n$, para todo $n \geq 2$. Consequentemente, $B_n(\mathbb{S}^2)$ tem elemento não trivial de ordem finita, não sendo, portanto, livre de torção. ■

3.5 Diagrama de van Kampen

Vamos nos deter brevemente para descrever o **diagrama de van Kampen**. Inicialmente, podemos descrever o diagrama de van Kampen de modo visual: ele ilustra o fato de que uma palavra $w \in F(X)$ no grupo livre sobre X é uma relação em um grupo G, i.e., w é um produto de palavras em $R \cup R^{-1}$. Em um nível mais rigoroso, os diagrama de van Kampen são a base de uma das técnicas mais poderosas da Teoria Combinatória dos Grupos.

Informalmente, o diagrama de van Kampen para uma apresentação $G = \langle X \mid R \rangle$ é um grafo conexo finito planar $\Gamma \subseteq \mathbb{R}^2$, cujas arestas são direcionadas e marcadas por elementos de X em um caminho tal que toda face de Γ é um disco cuja fronteira é marcada e pertence a R (ou seja, é uma relação). Daí, é quase imediato que a palavra marcada sobre o bordo de Γ é ela

própria uma relação em G. Assim, o diagrama de van Kampen pode ser utilizado para ilustrar a dedução de novas relações a partir das antigas relações.

Antes dos exemplos, vejamos como que cada relator de G é uma palavra limitando algum diagrama de van Kampen Γ de G. Podemos, ainda, assumir que Γ está reduzido, no sentido de que nenhum circuito não trivial carrega a palavra vazia. Agora, o fato de que Γ está imerso no plano impõe várias restrições sobre sua estrutura, e.g., sobre a característica de Euler. Essas restrições podem ser usadas para argumentar sobre propriedades locais de Γ (correspondendo a condições combinatoriais no conjunto R) e sobre propriedades do bordo (correspondendo a propriedades grupo-teóricas de G).

Um modo de construir o diagrama de van Kampen para uma apresentação $G = \langle X \mid R \rangle$ é o seguinte. Pensemos em cada relator como o bordo de uma célula bidimensional. Podemos, então, colar coleções dessas células ao longo de arestas com a mesma palavra e orientação.

Por exemplo, o grupo dos quatérnios, Q_8, tem ordem 8 e apresentação:

$$\langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$

Vamos fazer $r = x^4$, $s = x^2y^{-2}$ e $t = y^{-1}xyx$. Daí, o diagrama de van Kampen é o seguinte.

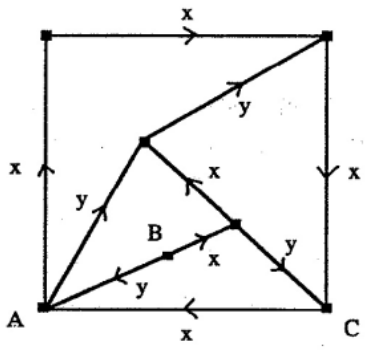


Figura 3.18: Diagrama de van Kampen para o grupo dos quatérnios, Q_8

Na parte superior da face esquerda, a fronteira, lida no sentido horário a partir de A é $s = x^2y^{-2}$. De modo análogo, a face contendo B, lida no sentido anti-horário a partir de B também nos dá $s = x^2y^{-2}$. Na face inferior contendo B, a delimitação do bordo lida no sentido horário a partir de A nos dá $t = y^{-1}xyx$. Do mesmo modo, a face mais à direita, lida no sentido horário a partir de C também nos dá $t = y^{-1}xyx$. Por fim, como a marca sobre a fronteira, lida no sentido horário a partir de A, é $x^4 = 1$, isso nos mostra que essa primeira relação na apresentação de Q_8 é supérflua.

Outro exemplo é o grupo

$$G = \langle a, b, c, d \mid ab = c, bc = d, cd = a, da = b \rangle.$$

Ele é claramente gerado por a e b, uma vez que $c = ab$ e $d = bc = bab$. Contudo, esse fato pode ser verificado a partir do diagrama de van Kampen para essa apresentação. Nele, as faces estão marcadas pelas seguintes relações definidoras:

$$r_1 = abc^{-1},\ r_2 = bcd^{-1},\ r_3 = cda^{-1},\ r_4 = dab^{-1}.$$

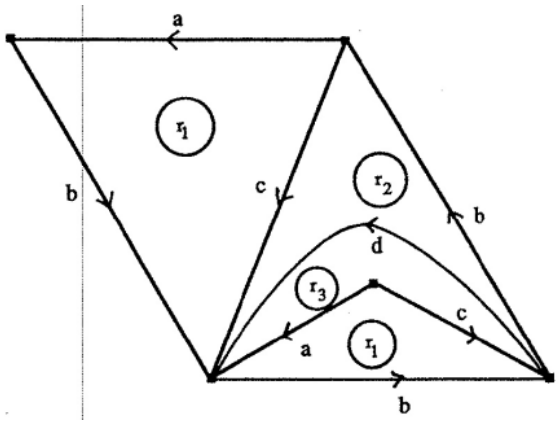


Figura 3.19: Diagrama de van Kampen de G

A partir do diagrama, vemos que lendo a fronteira, no sentido anti-horário, a partir do vértice superior direito, temos $ab^3 = 1$, ou seja, $a = b^{-3}$ e, portanto, G é gerado apenas por b, sendo cíclico. De fato, podemos fazer uma manipulação desse diagrama para obter o seguinte diagrama:

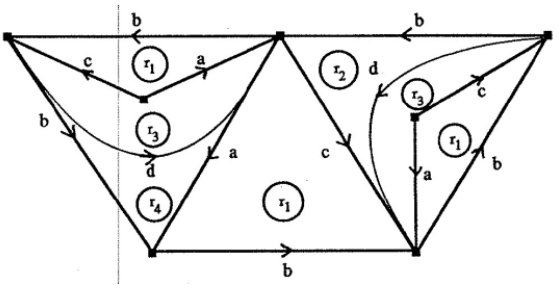


Figura 3.20: Diagrama de van Kampen manipulado de G

A partir desse diagrama, vemos, a partir da leitura do bordo, que $b^5 = 1$. Logo, G é o grupo cíclico de ordem 5 (b não trivial) ou 1 (b trivial).

É interessante notar que se a, b, c e d são geradores de um grupo tais que a e b comutam com c e d, então o fato de que ab comuta com cd pode ser deduzido pelo seguinte diagrama:

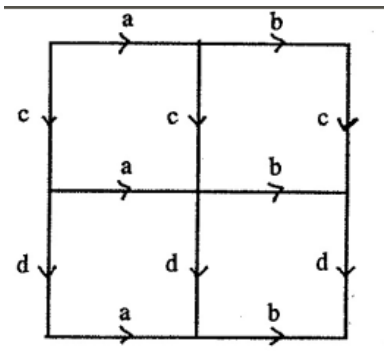
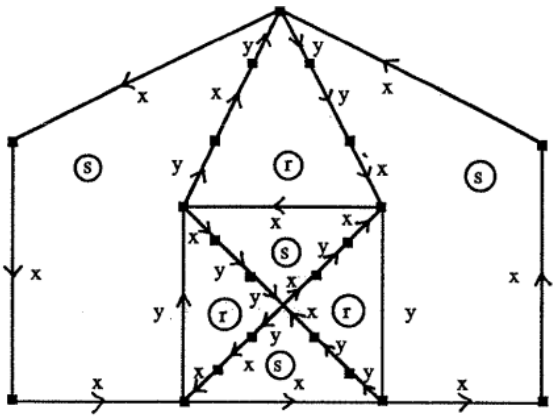


Figura 3.21: Diagrama de van Kampen em que a e b comutam com c e d

Do diagrama, é imediato que $abcd(ab)^{-1}(cd)^{-1} = 1$, ou seja, $[ab, cd] = 1$.

Um último exemplo é o seguinte: fazendo $r = x^2yxy^3 = 1 = y^2xyx^3 = s$, obtemos o seguinte diagrama:



Da leitura do bordo no sentido anti-horário, obtemos $x^7 = 1$.

Dos exemplos acima, podemos ver que os diagramas de van Kampen nos ajudam a deduzir relações que não são tão imediatas tendo apenas a apresentação do grupo.

3.6 Tranças como discos perfurados

Podemos, ainda, pensar em tranças de uma terceira maneira. Voltando na trança da Figura 3.14, vamos imaginar o seguinte: suponha que a trança é feita de fios rígidos, e que o plano é, na verdade, uma seção quadrada do plano (como está desenhado), ou seja, um disco topológico, exceto que esse disco tem buracos.

Agora, imagine que o interior do disco é feito de um material muito flexível e que a fronteira (bordo) quadrada é uma armação rígida (parecida com aqueles *frisbees* de tecido, mas agora quadrados). Imagine o processo de empurrar esse disco perfurado ao longo da trança de fios rígidos até chegar na parede da direita. A trança não se moveu, mas o disco em si foi todo torcido, ou seja, a trança provocou uma mudança na superfície.

Mais especificamente, o que aconteceu ao disco perfurado foi que a trança implementou um homeomorfismo da superfície nela mesma. O bordo fica fixo, porque é rígido, e as perfurações são permutadas conforme a permutação associada à trança. Funções como essa, a menos de homotopia, formam o *grupo de classes* de D_n, um disco com n perfurações com bordo ∂D_n (e não o grupo diedral):

$$\text{Mod}(D_n) = \{f : D_n \to D_n | f \text{ é homeomorfismo}, \\ f|_{\partial D_n} = 1\}/\text{Homotopia}.$$

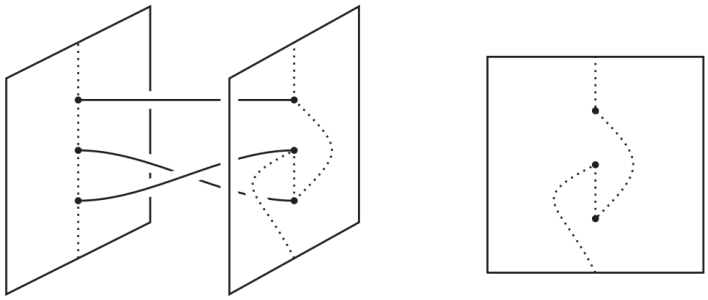


Figura 3.22: Diagrama de curva associado a σ_1.

A operação do grupo é a composição de funções: dois homeomorfismos f e g podem ser compostos para formar um homeomorfismo $g \circ f$ (ou $f \circ g$, que geralmente é diferente). Acima, descrevemos uma função $\psi : B_n \to \text{Mod}(D_n)$, a saber, dada uma trança, deslize o disco pela trança e considere o homeomorfismo resultante. De fato, ψ é, na verdade, um isomorfismo.

Teorema 3.6.1 $B_n \cong \text{Mod}(D_n)$

Demonstração. Não demonstraremos a sobrejetividade de ψ, pois exige conhecimentos além do escopo deste texto.

Primeiro, note que ψ está bem definida, pois se $\alpha, \beta \in B_n$ são tais que $\alpha = \beta$, então elas induzem a mesma deformação no disco, i.e., o mesmo homeomorfismo e, portanto, temos $\psi(\alpha) = \psi(\beta)$.

Além disso, o núcleo de ψ é, por definição, formado pelas tranças que induzem o homeomorfismo identidade, ou seja, as tranças que não fazem nada com o interior do disco (o bordo fica fixo sempre). Ora, mas a única trança que não deforma o interior do disco é a identidade e, portanto, $\operatorname{Ker}\psi = \{1\}$.

Agora, sejam $\alpha, \beta \in B_n$ duas tranças quaisquer tais que $\psi(\alpha) = f$ e $\psi(\beta) = g$. Daí, temos

$$\psi(\alpha\beta) = g \circ f = \psi(\alpha) \circ \psi(\beta).$$

Essa última igualdade nos diz simplesmente que, fazendo o produto de duas tranças α e β, a deformação resultante é equivalente a aplicar a deformação da segunda trança (β) na deformação da primeira trança (α), ou seja, compor as duas deformações.

Portanto, como ψ é um homomorfismo sobrejetor de núcleo trivial, então $B_n \cong \operatorname{Mod}(D_n)$. ■

Diagramas de curvas

Vamos nos aprofundar um pouco nessa nova perspectiva dos grupos de tranças. Olhe novamente a Figura 3.14, mas foque agora nos discos quadrados perfurados nas extremidades da imagem. Imagine que há uma linha vertical pontilhada no disco da esquerda passando por todas as perfurações. A pergunta é: para onde irá a linha pontilhada após deslizarmos o disco pela trança?

A Figura 3.22 mostra um exemplo mais simples. Nela, a trança é simplesmente σ_1, e tanto a linha pontilhada original quanto o resultado torcido estão desenhados. A linha pontilhada na parede da direita é dita *diagrama de curva* induzido pela trança (σ_1, nesse caso).

Vamos chamar a linha pontilhada original de **eixo** do disco. Ele consiste de $n+1$ segmentos pontilhados $a_0, \ldots, a_n$, numerados em ordem de baixo para cima. Então, em geral, o diagrama de curva associado a uma trança β é a união dos arcos $\psi_\beta(a_i)$ (os arcos que são as imagens dos a_i's), i.e., você pensa em β como um homeomorfismo do disco e o diagrama de curva é para onde o eixo vai (a imagem do eixo).

Denotaremos os arcos do diagrama de curva por c_i, e o diagrama todo por c. Note que, como β fixa ∂D_n (o bordo), os c_i's (isto é, o diagrama de curva) se encaixam ponta a ponta, em ordem, para formar o único arco c que começa no centro inferior, nunca se cruza, passa por cada perfuração uma única vez e termina no centro superior. Veja novamente a Figura 3.22.

Diagramas de curva podem ser extremamente complicados, como poderíamos esperar se

tivermos uma trança longa. Por exemplo, o diagrama de curva da trança da Figura 3.14 é bem complicado de desenhar.

Uma maneira preliminar de simplificar um diagrama de curva é ter certeza de que ele está *reduzido*, no seguinte sentido: dado um diagrama de curva em um disco perfurado, desenhe o eixo no mesmo disco. O diagrama é dito *reduzido* se não existem *biágonos* na figura, i.e., regiões cujas fronteiras consistem de um sub-arco de um único a_i e um sub-arco de um único c_i.

Podemos resumir o que foi dito no parágrafo anterior nas seguintes definições:

Definição 3.6.1 — Biágono. Um biágono é um região cuja fronteira consiste de um sub-arco de um único a_i e um sub-arco de um único c_i.

Definição 3.6.2 — Diagrama reduzido. Um diagrama de curva é dito reduzido quando não possui biágonos.

Os biágonos podem ser facilmente eliminados, de modo que todo diagrama de curva pode ser reduzido.

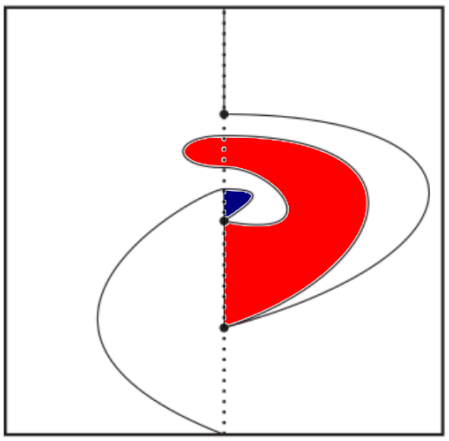


Figura 3.23: Esse diagrama possui 2 biágonos (em vermelho e em azul), e pode ser reduzido ao diagrama da Figura 3.22.

É, então, natural considerar os diagramas das Figuras 3.22 e 3.23 como equivalentes. Esse fato nos leva à seguinte definição.

Definição 3.6.3 — Diagramas equivalentes. Dois diagramas de curva são ditos equivalentes se têm a mesma forma reduzida.

Vamos, agora, mostrar uma aplicação interessante dos diagramas de curva, a saber, na demonstração da Proposição 3.2.2.

Dada uma trança β, vamos olhar para o seu diagrama de curva c. Comece na parte de baixo e observe o primeiro arco c_i que não é igual ao arco correspondente a_i no eixo. Se c_i está à direita de a_i, dizemos que β é *desviada à direita* e, se c_i está à esquerda de a_i, dizemos que β é *desviada à esquerda*. Se $c_i = a_i$ para todo i, então β é a trança identidade (tecnicamente, estamos usando o Teorema 3.6.1). A trança da Figura 3.22 é desviada à esquerda, pois começando na parte inferior, o arco c_0 desvia para a esquerda.

Proposição 3.6.1 Se β é desviada à esquerda, então β^{-1} é desviada à direita. ∎

Demonstração. O efeito, no diagrama de curva, de inverter uma trança é simplesmente realizar uma reflexão em torno de uma das arestas do disco paralelas ao eixo. Observe a Figura 3.24.

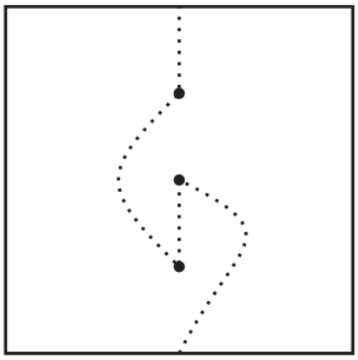


Figura 3.24: Diagrama de curva de σ_1^{-1}

Portanto, como inverter uma trança equivale a refletir o seu diagrama de curva, segue que se a trança original era desviada à esquerda, o seu inverso será desviado à direita e vice-versa. ■

Queremos mostrar que B_n é livre de torção. Esse fato segue do seguinte lema.

Lema 3.6.1 Se β é desviada à direita, então β^n é desviada à direita para todo $n > 0$.

Demonstração. Suponha que β é desviada à direita, e observe o diagrama de curva reduzido c de β. Encontre o primeiro c_i que difere do a_i correspondente, e chame esse arco de c_k. Denotando por c^2 o diagrama de curva de β^2, e por c_i^2 os arcos de c^2, imagine dois discos separados: um em que a_i e c_i estão desenhados e um em que c_i e c_i^2 estão desenhados. Observe que a segunda figura é obtida da primeira aplicando a trança β (pensada como um homeomorfismo). Então, como c_k está à direita de a_k, segue que c_k^2 está à direita de c_k. Além disso, como não há biágonos na primeira figura, também não há biágonos na segunda figura.

Queremos mostrar que β^2 é desviada à direita, i.e, que c_k^2 está à direita de a_k. Sabemos que β não afeta os arcos a_i para $i < k$, e então β^2 também não. Também sabemos que, nas figuras, c_k está à direita de a_k e c_k^2 está à direita de c_k.

O que falta observar é que o diagrama de β^2 pode não estar reduzido. Sabemos que não há biágonos entre o eixo e c, e também que não há biágonos entre c e c^2, mas se c^2 e o eixo formarem um biágono, então c^2 precisa ser reduzido e pode acabar não sendo desviado à direita.

Felizmente, isso não ocorre. Para ver que esse é o caso, seja d o segmento inicial de c_k que vai até a primeira vez que c_k intercepta o eixo, de forma que d está contido em uma metade (a metade da direita) do disco (é possível que d seja c_k inteiro, mas em geral c_k pode "passear" bastante antes de atingir uma perfuração). Agora, a única maneira de c_k^2 estar à esquerda (ou ser igual) do arco a_k do eixo é formando um biágono com a_k. Mas isso forçaria c_k^2 a cruzar d, criando um biágono entre c e c^2, o que sabemos que não existe. Veja a figura abaixo.

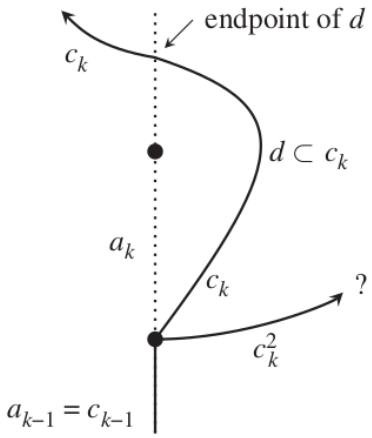


Figura 3.25: Ilustração da demonstração

Portanto, β^2 é, de fato, desviada à direita. Repetindo o argumento, mostramos que β^n é desviada à direita para todo $n > 0$. ■

Corolário 3.6.1.1 B_n é livre de torção.

Demonstração. Do Lema 3.6.1, sabemos que se β é desviada à direita, β^n também o é para todo n positivo. Da Proposição 3.6.1, sabemos que β^{-1} é desviada à esquerda e então, novamente do Lema 3.6.1, $(\beta^{-1})^n$ também o é para todo n positivo. Portanto, toda trança que é desviada (seja à direita ou à esquerda) tem ordem infinita. Como, do Teorema 3.6.1, a trança

trivial é a única trança que não é desviada, temos que B_n é livre de torção. ■

Observação. Na demonstração do Lema 3.6.1, alguns detalhes foram omitidos. Por exemplo, homeomorfismos podem ser complicados: poderia ser o caso de que o arco c_0 interceptasse a_0 infinitas vezes. Então, como reduzi-lo? Esse e outros detalhes podem ser tratados de maneira rigorosa, mas isso está além do escopo desse texto.

Uma última aplicação interessante dessa nova visualização dos grupos de trança é na identificação de tranças (palavras) que são equivalentes à identidade, ou seja, o problema da palavra (veja Seção 5.1). Usando o Teorema 3.6.1, sabemos que uma trança β é trivial se, e só se, $\psi(\beta) = \mathrm{Id}$, ou seja, se, e só se, β induz o homeomorfismo identidade (não faz nada com o disco). Portanto, dada uma trança β qualquer, basta observarmos o efeito de β no disco perfurado: se provoca torção, não é trivial; se não provoca torção, é trivial. Esse procedimento é complicado de computar para tranças longas, mas continua sendo uma solução igualmente válida.

Capítulo 4

A Teoria dos Nós

"As far as the laws of mathematics refer to reality,
they are not certain, and as far as they are certain,
they do not refer to reality."
— Albert Einstein

4.1 Conexões entre tranças e nós

Vamos agora discutir algumas conexões entre tranças e a teoria dos nós.

Resumidamente, um nó é uma curva poligonal simples fechada em $\mathbb{R}^3$, mas para os propósitos deste texto poderemos pensar em um nó como sendo uma curva suave simples, como os diagramas da Figura 4.1.

Os nós (ou, de modo mais geral, *links*) e as tranças possuem semelhanças. Por exemplo, ambos são definidos em termos de figuras de cordas no espaço tridimensional, e ambos têm uma noção de equivalência, geralmente chamada de isotopia, que descreve quando duas figuras são equivalentes, ou seja, quando duas figuras representam o mesmo nó ou a mesma trança.

Figura 4.1: Exemplos de nós

É claro que há algumas diferenças, a principal delas sendo o fato de que as tranças têm extremidades que não podem se mover durante isotopias, i.e., as extremidades ficam fixas conforme deformamos a trança, como vimos nas seções anteriores. Outra diferença é que cada corda de uma trança vai monotonicamente da esquerda para a direita, enquanto que não há

essa restrição em relação aos *links*.

Na verdade, uma das primeiras motivações para o estudo das tranças era ajudar a entender a teoria dos nós e *links*. A conexão é que toda trança pode ser "fechada" para formar um *link*. Era esperado que a estrutura de grupo nas tranças levasse a algum tipo de estrutura de grupo no conjunto de *links*, mas isso não acontece. Não obstante, há outras maneiras de usar tranças para ajudar com o estudo de *links*.

Mas como formamos um *link* a partir de uma trança? Fácil: basta ligar as extremidades sem introduzir novos cruzamentos.

Assim como fizemos para as tranças, também é possível alterar diagramas de nós através de deformações (ou movimentos) elementares (e seus respectivos inversos). Esses movimentos são chamados de *movimentos de Reidemeister* , classificados em 3 tipos.

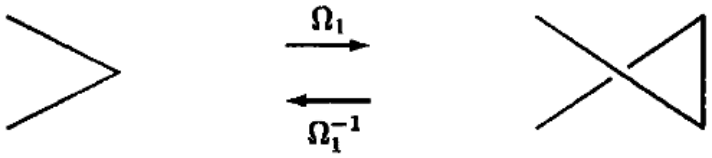


Figura 4.2: Movimento de Reidemeister do tipo I

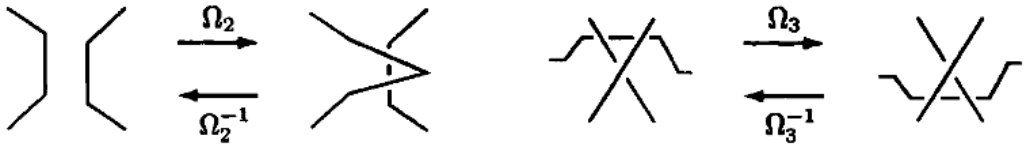


Figura 4.3: Movimentos de Reidemeister dos tipos II e III

O teorema a seguir, que não será demonstrado, nos dá os análogos, para nós e *links*, das relações de trança.

Teorema 4.1.1 Seja K um nó (ou *link*) e suponha que D e D' são dois diagramas de nó de K. Então, D pode ser deformado em D' através de uma sequência finita de movimentos de Reidemeister, ou seja, através de uma sequência finita das deformações $\Omega_1^{\pm 1}, \Omega_2^{\pm 1}$ e $\Omega_3^{\pm 1}$.

O Teorema 4.1.1 nos dá um algoritmo conceitualmente muito simples para verificar se dois diagramas são, de fato, equivalentes, i.e., representam o mesmo nó: basta tentar todas as sequências possíveis de movimentos em um dos diagramas e ver se o outro diagrama é produzido em alguma dessas sequências. Esse método de tentativa é válido pois recentemente foi

provado que, dados dois diagramas, se um deles pode ser deformado no outro, ou seja, se eles representam o mesmo nó, então a quantidade de movimentos é limitada superiormente por uma função do número de cruzamentos no diagrama. Contudo, como esse limite superior é extremamente grande [4, 9, 14], esse algoritmo ainda não é prático. Ainda assim, os movimentos de Reidemeister são úteis para vários propósitos teóricos, como estabelecer vários invariantes de nós.

Os movimentos de Reidemeister, definidos para nós e *links*, possuem análogos para as tranças. Esses análogos são os próprios movimentos de Reidemeister, com exceção do tipo I, uma vez que cada corda da trança deve ser monotônica. Isso significa que nunca podemos fazer um movimento do tipo I, pois não podemos ter *loops*.

Mas e os movimentos tipo II? Se, na trança, há uma parte que parece com o diagrama à esquerda da Figura 3.5, então podemos endireitar ambas as cordas: esse é um movimento tipo II. Algebricamente, ele corresponde a cancelar $\sigma_i\sigma_i^{-1}$ (ou $\sigma_i^{-1}\sigma_i$) em uma palavra, o que é claro que podemos fazer. Também podemos sempre inserir tais pares sempre que quisermos, sem alterar a trança.

E os movimentos tipo III? Observe a Figura 3.6: ela é um movimento de Reidemeister tipo III!

De forma análoga ao Teorema 4.1.1, por meio de uma sequência de movimentos de Reidemeister dos tipos II e III, podemos partir de um diagrama de uma trança e chegar em qualquer outro diagrama de uma trança equivalente. Note, em particular, que esses movimentos (tipo II e tipo III) não alteram a paridade do número de cruzamentos.

Voltando às conexões entre tranças e *links* (e nós), lembre-se do que foi dito no início da seção: que fechando uma trança, obtemos um *link*. De fato, não só podemos obter *links* (e nós) a partir de tranças, como também podemos obter **todos** os *links* a partir de tranças, como diz o seguinte teorema, que não será demonstrado aqui.

Teorema 4.1.2 — Teorema de Alexander. Qualquer nó ou link K pode ser representado como uma trança fechada.

Uma consequência boa do Teorema 4.1.2 é que temos uma maneira direta de descrever qualquer nó (e *link*) sem precisar fazer um desenho. Em vez de dizer "é o nó que vai por cima, depois por baixo, e volta por trás para onde estava antes só que do outro lado e...", o que tem desvantagens óbvias, podemos simplesmente dizer "é o nó que obtemos fechando a trança de 3 cordas $\sigma_1\sigma_2^{-1}\sigma_1\sigma_2^2\sigma_1^2\sigma_2^3$". Muito mais simples.

Contudo, o Teorema 4.1.2 não nos dá uma correspondência única entre tranças e *links*. Várias tranças diferentes podem ser fechadas no mesmo *link* e pode até ser o caso de que tranças com quantidades de cordas diferentes fechem no mesmo *link*, como mostra a figura a seguir.

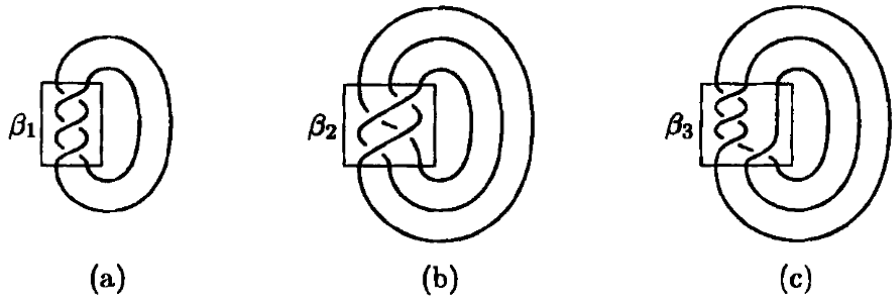


Figura 4.4: Tranças não equivalentes que fecham em nós equivalentes.

Quando dois nós (ou *links*) podem ser deformados um no outro, dizemos que eles são *equivalentes* ou *isotópicos*. Por exemplo, todas as tranças de $B_2(\mathbb{R}^2)$ (ou seja, todas as tranças de duas cordas) são fechadas no mesmo nó: o trivial.

Logo, se queremos estudar teoria dos nós via teoria das tranças, precisamos de um método para determinar se duas tranças fechadas são equivalentes, ou seja, se dois *links* são isotópicos. De fato, a resposta para essa pergunta está no chamado *teorema de Markov*, que será enunciado mais à frente.

Outro fato importante é que invariantes de trança podem não ser invariantes na trança fechada associada. Por exemplo, sabemos que dada uma trança β, l (o homomorfismo de comprimento) é um invariante de β. Contudo, l não precisa ser um invariante de $\widetilde{\beta}$, a trança fechada associada a β. Por exemplo, na Figura 4.4 $l(\beta_1) = 3 \neq 4 = l(\beta_2)$, mas $\widetilde{\beta_1} \sim \widetilde{\beta_2}$, i.e., os seus fechamentos são nós equivalentes.

Isso suscita a seguinte questão: existe um invariante de nó da trança fechada $\widetilde{\beta}$ que é definido a partir de um invariante da trança β?

A resposta é sim. Consideremos a permutação $\pi(\beta)$ associada à trança β. Sabemos que $\pi(\beta)$ pode ser expressa como produto de transposições, a saber

$$\pi(\beta) = C_1 \cdots C_k.$$

Então k, que denotaremos por $\mu(\beta)$, é o número de componentes de $\widetilde{\beta}$ e um invariante do link

$\widetilde{\beta}$, uma vez que o seguinte é válido:

$$\beta \sim \beta' \Rightarrow \pi(\beta) = \pi(\beta') \Rightarrow \mu(\beta) = \mu(\beta').$$

Portanto, $\widetilde{\beta}$ é um nó se, e somente se, $\pi(\beta)$ é um ciclo de ordem n, isto é, $\pi(\beta)$ não deixa pontos fixos. Nesse caso, dizemos que β é uma trança fechada de um componente. Como um ciclo de ordem n é escrito por um produto de $n-1$ transposições, então $\widetilde{\beta}$ é um nó se, e só se, $k = n-1$.

Note também que da maneira que definimos $\mu(\beta)$, é claro que, escrevendo $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$, sendo $\varepsilon_i = \pm 1$, temos como consequência imediata o fato de que $\mu(\beta) = \sum_{i}^{k} |\varepsilon_i|$.

Até agora, vimos que a toda trança podemos associar um *link*, mas que essa correspondência não é única (veja a Figura 4.4). Esse fato levanta a questão: é possível dizer quando que o fechamento de duas tranças não equivalentes nos dá o mesmo *link*?

A resposta (em parte) é sim, contida no *teorema de Markov* (ainda que não tenha sido o próprio Markov quem demonstrou). Mas o quê exatamente é o teorema de Markov?

Primeiro, vamos observar alguns fatos, como o lema a seguir.

Lema 4.1.1 Sejam β e γ duas tranças de n cordas. Então, o fechamento de β e o fechamento de $\gamma\beta\gamma^{-1}$ nos dão o mesmo *link*.

Demonstração. A demonstração segue a ideia da Figura 4.5. Basicamente, fechando a trança $\gamma\beta\gamma^{-1}$, podemos mover a trança γ^{-1} pelo *link* de modo que tenhamos a trança $\beta\gamma^{-1}\gamma$, ou seja, a trança β. Observe a figura.

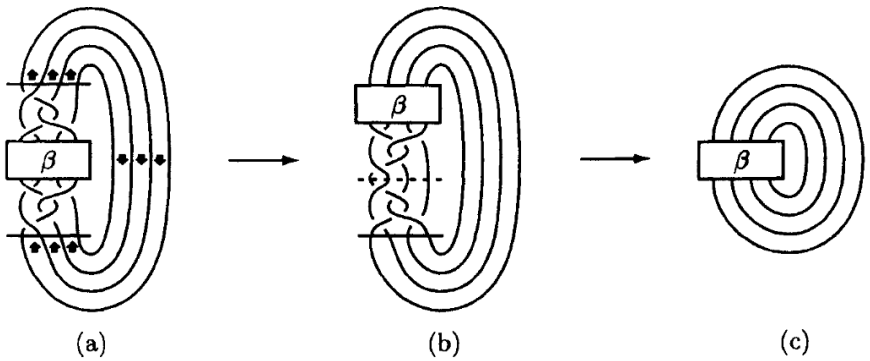


Figura 4.5: Conjugações não alteram o *link*.

■

Por fim, antes de enunciarmos o teorema de Markov, suponha que β é um trança de n cordas

e considere σ_n um gerador de $B_{n+1}(\mathbb{R}^2)$. De maneira natural, se considerarmos β como um elemento de $B_{n+1}(\mathbb{R}^2)$ em vez de $B_n(\mathbb{R}^2)$, podemos definir outras duas tranças de $n+1$ cordas,

$$\beta' = \beta\sigma_n \quad \text{e} \quad \beta'' = \beta\sigma_n^{-1}.$$

Nesse caso, β, β' e β'' fecham no mesmo *link*, como ilustra a figura abaixo. A figura (a) mostra o fecho de β, a figura (b), o fecho de $\beta\sigma_n$ e a (c), o fecho de $\beta\sigma_n^{-1}$.

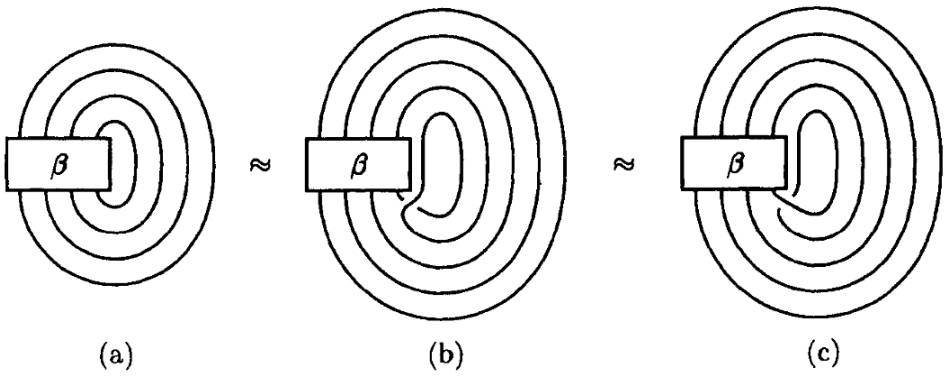


Figura 4.6: Movimentos de Markov

É claro que há outras maneiras de obter tranças cujos fechos representam o mesmo *link*, mas, como veremos adiante, as duas transformações acima mostradas nas Figuras 4.5 e 4.6 são especiais. Como foi Markov quem primeiro as introduziu, elas são usualmente chamadas de *movimento de Markov tipo I* e *movimentos de Markov tipo II*. Vamos defini-los formalmente.

Definição 4.1.1 — Movimento de Markov Tipo 1. Um movimento de Markov tipo I, denotado M_1, substitui uma trança β de n cordas pelo seu conjugado $\gamma\beta\gamma^{-1}$, sendo γ uma trança de n cordas arbitrária.

Definição 4.1.2 — Movimento de Markov Tipo 2. Um movimento de Markov do tipo II, denotado M_2, substitui a trança β de n cordas pela trança $\beta\sigma_n$ ou $\beta\sigma_n^{-1}$ de $n+1$ cordas, sendo β visualizada com uma trança de $B_{n+1}(\mathbb{R}^2)$ e σ_n um gerador de $B_{n+1}(\mathbb{R}^2)$.

É claro que podemos definir também os inversos de M_1 e M_2, que denotaremos por M_1^{-1} e M_2^{-1}, respectivamente. Agora, estamos prontos para enunciar o teorema (que não será demonstrado).

Teorema 4.1.3 — Teorema de Markov. Suponha β e β' duas tranças (orientadas) não necessariamente com o mesmo número de cordas. Então, os fechos de β e β' representam o mesmo *link* ou nó K (orientado) se, e somente se, β pode ser deformada em β' por uma sequência finita dos movimentos $M_1^{\pm 1}, M_2^{\pm 1}$. Em símbolos, existe a seguinte sequência finita,

$$\beta = \beta_0 \to \beta_1 \to \cdots \to \beta_m = \beta'$$

tal que, para $i = 0, 1, \ldots, m-1$, β_{i+1} é obtida a partir de β_i pela aplicação de um dos movimentos $M_1^{\pm 1}$ e $M_2^{\pm 1}$.

Podemos, ainda, pensar nos movimentos de Markov para as tranças como paralelos diretos dos movimentos de Reidemeister para *links*. Por conveniência, diremos que duas tranças β e β' são *Markov equivalentes*, denotado por $\beta \underset{M}{\sim} \beta'$, se uma pode ser deformada na outra por meio de uma sequência finita de movimentos de Markov. De fato,

Proposição 4.1.1 Markov equivalência é uma relação de equivalência. ∎

Demonstração. Sejam α, β e γ tranças quaisquer, não necessariamente com o mesmo número de cordas. Note que

$$\alpha = \alpha_0 \overset{M_1}{\to} \alpha_1 \overset{M_1^{-1}}{\to} \alpha_2 = \alpha,$$

logo $\alpha \underset{M}{\sim} \alpha$ e, portanto, a relação $\underset{M}{\sim}$ é reflexiva.

Agora, suponha que $\alpha \underset{M}{\sim} \beta$. Então, por definição, existe uma sequência finita

$$\alpha \to \cdots \to \beta$$

de movimentos de Markov que nos permite deformar α em β. Consequentemente, podemos partir de β e, usando a mesma sequência, só que de trás para frente, chegar em α. Portanto, $\alpha \underset{M}{\sim} \beta$ implica $\beta \underset{M}{\sim} \alpha$ e a relação $\underset{M}{\sim}$ é simétrica.

Por fim, suponha $\alpha \underset{M}{\sim} \beta$ e $\beta \underset{M}{\sim} \gamma$. Por definição, existem duas sequências finitas, S_1 e S_2, digamos,

$$\alpha \overset{S_1}{\to} \beta, \qquad \beta \overset{S_2}{\to} \gamma$$

e, consequentemente, existe uma sequência finita S_3 de α em γ

$$\alpha \overset{S_1}{\to} \beta \overset{S_2}{\to} \gamma$$

sendo S_3 a sequência S_1 seguida de S_2. Portanto, $\underset{M}{\sim}$ é transitiva e configura uma relação de equivalência. ■

Com a noção de Markov equivalência, podemos reescrever o Teorema 4.1.3 da seguinte forma.

Teorema 4.1.4 — Teorema de Markov simplificado. Sejam $\widetilde{\beta}$ e $\widetilde{\beta}'$ dois *links* (ou nós). Então, $\widetilde{\beta}$ é equivalente a $\widetilde{\beta}'$ se, e somente se, $\beta \underset{M}{\sim} \beta'$.

Algumas observações são necessárias.

Observação. Primeiro, note que o Teorema 4.1.3, em si, não é suficiente para classificarmos todos os *links* e nós. O obstáculo é que, atualmente, não existe nenhum algoritmo conhecido para determinar se duas tranças β e β' são Markov equivalentes ou não. Dito isso, nos casos relativamente simples de tranças de 2 ou 3 cordas, se os fechos de β e β' são equivalentes, então (a menos de uma família de tranças de 3 cordas que já foi completamente classificada, vide [2]) β e β' são conjugadas.

Segundo, tenha em mente que nos restringimos a *links* e nós **orientados**. Se ignorarmos a orientação, o teorema de Markov pode não valer. Por exemplo, considere a figura abaixo.

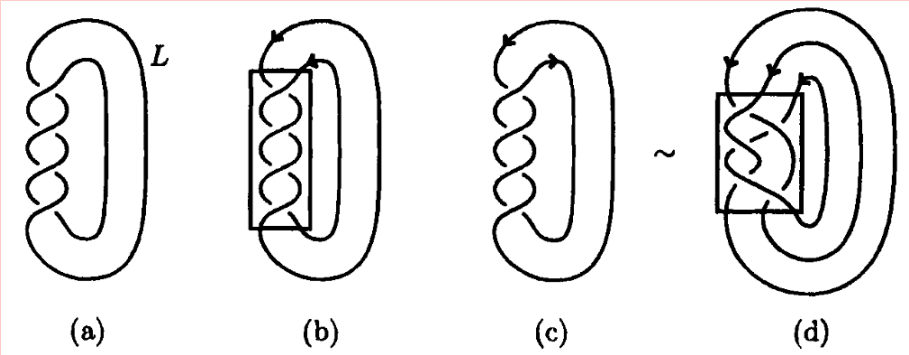


Figura 4.7: O *link* L e duas orientações possíveis.

Se orientarmos L como na Figura 4.7(b), então (o *link* orientado) L é o fecho da trança de 2 cordas σ_1^4. Por outro lado, se orientarmos L como na Figura 4.7(c), então o mesmo *link* L não pode ser o fecho de nenhuma trança de 2 cordas. Mas, de fato, é possível mostrar que com essa orientação, L na verdade é o fecho da trança de 3 cordas $\sigma_1^{-1}\sigma_2\sigma_1^2\sigma_2^1$, Figura 4.7(d).

Portanto, o *link* (não orientado) L da Figura 4.7(a) pode ser representado por duas tranças distintas, σ_1^4 e $\sigma_1^{-1}\sigma_2\sigma_1^2\sigma_2^1$. Contudo, essas duas tranças **não** são Markov equivalentes.

Outro exemplo é o da Figura 4.8.

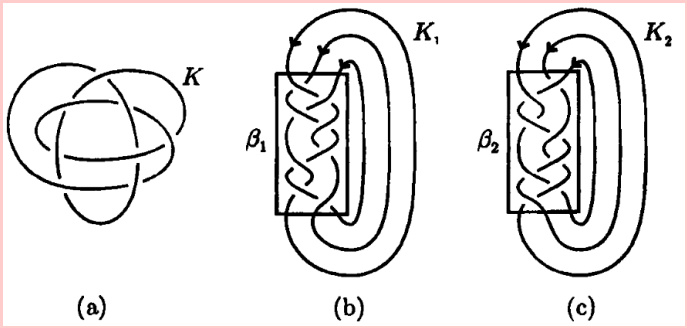


Figura 4.8: O nó K e duas orientações possíveis.

É sabido, mas não é fácil mostrar, que os nós (orientados) K_1 e K_2 da Figura 4.8, apesar de obtidos a partir do mesmo nó não orientado K, não são equivalentes, justamente por serem

dados por orientações diferentes. Pela figura, K_1 e K_2 são representados pelas tranças β_1 e β_2, respectivamente. Como K_1 e K_2 não são equivalentes, então β_1 e β_2 não são Markov equivalentes.

4.2 Algumas aplicações do Teorema de Markov

Seja K um nó (ou *link*) orientado em $\mathbb{R}^3$. Se considerarmos o plano xy como um espelho, então a imagem de K nesse espelho também é um nó em $\mathbb{R}^3$, veja a figura abaixo.

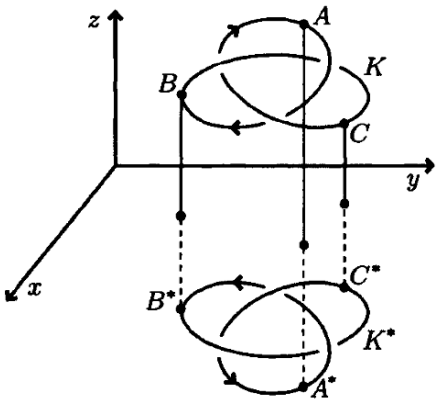


Figura 4.9: O nó K refletido em torno do plano xy.

O nó K^* é chamado de imagem espelhada de K. Como K é orientado, K^* herda uma orientação de K.

Proposição 4.2.1 Seja D um diagrama (orientado) de um nó K. Então, o diagrama D^* do nó K^* é obtido de D substituindo cruzamentos superiores por cruzamentos inferiores. ∎

Demonstração. Como a imagem espelhada de K é obtida a partir de uma rotação de K, então os cruzamentos superiores passam a ser inferiores e vice-versa. ■

Na Figura 4.10 abaixo estão representados os diagramas D e D^* de um nó K. Esse nó K é chamado de *nó de trevo*.

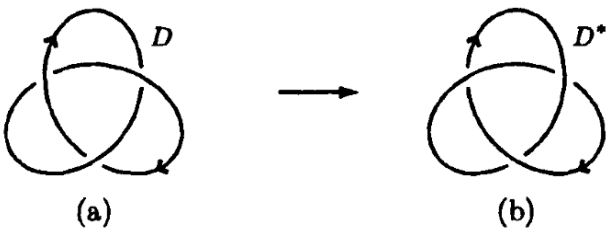


Figura 4.10: O nó de trevo orientado.

Apesar de que, em geral, um nó e sua imagem espelhada não são equivalentes, há casos em que isso acontece. Um nó que é equivalente à sua imagem espelhada é chamado de *aquiral*. Um exemplo de nó aquiral é o nó da figura abaixo.

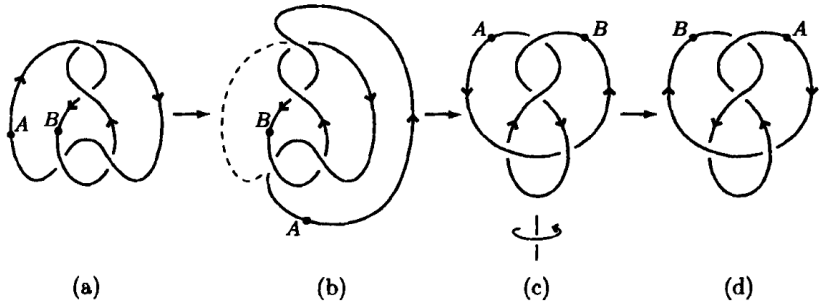


Figura 4.11: O nó figura oito, um exemplo de nó aquiral.

O nó da Figura 4.11(a), representado pelo diagrama D, pode ser representado pelo fecho da trança de 3 cordas $\beta = \sigma_1\sigma_2^{-1}\sigma_1\sigma_2^{-1} = (\sigma_1\sigma_2^{-1})^2$. Na sua forma de trança, a imagem espelhada K^* de K é exatamente o fecho da trança β^{-1} (com a orientação inversa), como mostra a figura abaixo.

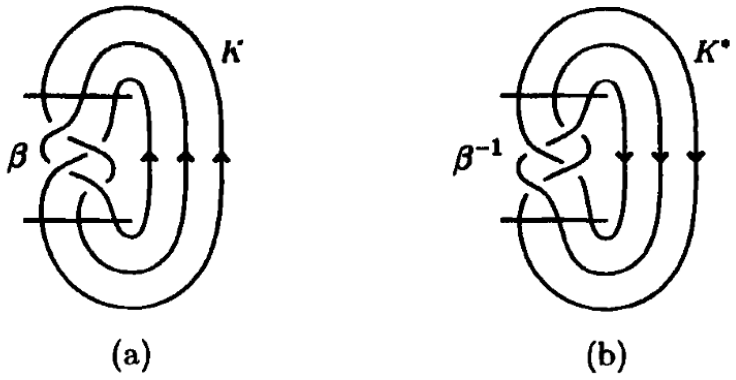


Figura 4.12: Trança do nó figura oito.

Esse exemplo suscita a pergunta: dado um nó (ou *link*) orientado e uma trança que representa esse nó, como podemos expressar K^* baseados em β? A resposta está na proposição a seguir.

Proposição 4.2.2 Seja K um nó (ou *link*) orientado e suponha que K é o fecho de uma trança de n cordas $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$, sendo $1 \leq i_1, i_2, \ldots, i_k \leq n-1$ e $\varepsilon_i = \pm 1$. Então,

1. a imagem espelhada K^* de K, com a orientação invertida, pode ser representada como o fecho de $\beta^{-1} = \sigma_{i_k}^{-\varepsilon_k} \cdots \sigma_{i_1}^{-\varepsilon_1}$

2. o nó $\overline{K}$ obtido de K revertendo a orientação de K pode ser representado por

$$\overline{\beta} = \sigma_{i_k}^{\varepsilon_k} \cdots \sigma_{i_i}^{\varepsilon_1}$$

ou

$$\overline{\overline{\beta}} = \sigma_{n-i_k}^{\varepsilon_k} \cdots \sigma_{n-i_1}^{\varepsilon_1}$$

e, portanto, $\overline{\beta} \underset{M}{\sim} \overline{\overline{\beta}}$.

■

Demonstração. A demonstração do item 1 segue diretamente dos diagramas da Figura 4.12. De fato, inverter a orientação de K equivale a espelhar a trança β, ou seja, invertê-la. Para o item 2, observe a Figura 4.13, que ilustra o processo aqui descrito. Primeiro, mude a orientação da Figura 4.13(a) para obter a Figura 4.13(b). Então, vire a Figura 4.13(b) de cabeça para baixo, obtendo a Figura 4.13(c). Em seguida, rotacione a Figura 4.13(c) em torno do eixo vertical por um ângulo de π radianos, Figura 4.13(d). Podemos ver que a Figura 4.13(c) é $\overline{\overline{\beta}}$ e que a Figura 4.13(d) é $\overline{\beta}$. Como não alteramos o nosso nó $\overline{K}$, então os fechos de $\overline{\beta}$ e $\overline{\overline{\beta}}$ são equivalentes e representam o mesmo nó, $\overline{K}$. Por fim, pelo Teorema 4.1.4, temos $\overline{\beta} \underset{M}{\sim} \overline{\overline{\beta}}$.

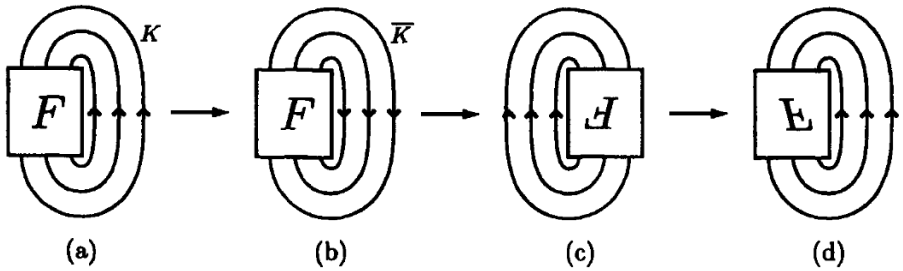


Figura 4.13: Inversão da orientação de um nó.

■

Se os nós K e $\overline{K}$ são equivalentes, então K é dito *inversível*. O nó da Figura 4.11(a) é inversível, uma vez que os dois nós das Figuras 4.11(c) e (d) são equivalentes. Apesar de muitos nós serem inversíveis, isso não quer dizer que todos os nós o são. De fato, um contraexemplo é o nó K da Figura 4.8.

4.3 Grupos de nó

Até agora, tratamos de nós de maneira um tanto quanto informal. Contudo, assim como fizemos para a trança, podemos tomar uma abordagem mais topológica. De fato, podemos utilizar,

assim como foi com as tranças, grupos fundamentais. Para isso, recorde que definimos nó como uma curva poligonal simples fechada em $\mathbb{R}^3$. Contudo, por conveniência, é comum substituir $\mathbb{R}^3$ por $\mathbb{S}^2$ (a esfera tridimensional unitária), pois $\mathbb{S}^2$ pode ser obtida de $\mathbb{R}^3$ adicionando um único ponto (de fato, isso é verdade para $\mathbb{S}^{n-1}$ e $\mathbb{R}^n$, realizando-se um análogo da projeção estereográfica para dimensões superiores. Como exercício, imagine o caso $n = 1$. Informalmente, estamos adicionando a $\mathbb{R}$ o "ponto infinito", ∞.)

Nesse contexto, podemos definir o *complemento de um nó* como abaixo.

Definição 4.3.1 — Complemento de nó. Dado um nó K, o complemento de K é o subconjunto $\mathbb{S}^2 - K$ de $\mathbb{S}^2$.

Com essa definição, podemos então definir o **grupo fundamental do complemento de nó**, muitas vezes chamado simplesmente de **grupo fundamental de nó**.

Definição 4.3.2 — Grupo fundamental de nó. O grupo fundamental de um nó K com ponto base $b \in \mathbb{S}^2 - \mathrm{Im}(K)$ é o grupo fundamental do complemento de K, com b como ponto base.

Como $\mathbb{S}^2$ é conexo por caminhos, podemos omitir o ponto base, pois a escolha dele não afeta a estrutura de grupo. Em símbolos, denotamos o grupo fundamental do nó K por $\pi_1(\mathbb{S}^2 \setminus K)$.

Um primeiro exemplo é o grupo fundamental do nó trivial. Apesar do nó ser trivial, seu grupo não o é; de fato, o grupo fundamental do nó trivial é o grupo cíclico infinito, $\mathbb{Z}$. Outro exemplo é o nó de trevo, mostrado na Figura 4.10; o seu grupo fundamental tem apresentação

$$\langle x, y | x^3 = y^2 \rangle,$$

ou seja, o grupo do nó de trevo é (isomorfo a) $B_3(\mathbb{R}^2)$! Um último exemplo é o nó figura oito, mostrado na Figura 4.11; seu grupo fundamental tem apresentação

$$\langle x, y | yxy^{-1}xy = xyx^{-1}yx \rangle.$$

O grupo fundamental de nó também é um invariante: se dois nós são equivalentes, então seus grupos fundamentais são isomorfos. Contudo, o contrário não é verdadeiro. Por exemplo, os dois nós de trevo abaixo têm o mesmo grupo fundamental, mas não são equivalentes (pois o nó de trevo é quiral, como vimos).

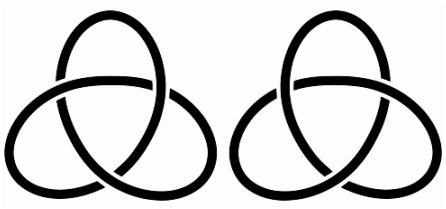


Figura 4.14: Os nós de trevo destro (à esquerda) e canhoto (à direita).

Uma das maiores questões quando estudamos nós é determinar se dois nós são ou não equivalentes, ou seja, como podemos distinguir dois nós. Uma das ferramentas que nos ajuda nessa tarefa são os chamados *invariantes de nós*. Demos um exemplo de invariante de nó acima, a saber, o número de componentes $\mu(\beta)$. Esse invariante era, de certo modo, esperado, uma vez que não podemos "cortar" nosso nó, ou seja, é impossível alterar o número de componentes por meio de movimentos de Reidemeister ($\Omega_1^{\pm 1}$, $\Omega_2^{\pm 1}$ e $\Omega_3^{\pm 1}$). Outros exemplos de invariantes são o polinômio de Alexander e o polinômio de Jones, que serão abordados a seguir. Antes, porém, uma curiosidade.

Um tipo particular de nó são os chamados *nós de toro* (ou *nós torais*). Como o nome sugere, são nós que pertencem à superfície de um toro (que, por sua vez, é um subconjunto de $\mathbb{R}^3$). Podemos definir um nó de toro usando coordenadas da seguinte forma [15].

Definição 4.3.3 — Nó de toro. Para todo par de inteiros a e b coprimos, o nó de toro padrão $K_{a,b} : \mathbb{S}^1 \to \mathbb{S}^2$ correspondente ao par (a, b) é dado, em coordenadas euclidianas, por

$$\theta \mapsto \begin{pmatrix} (2 + \cos(b\theta)) \cos(a\theta) \\ (2 + \cos(b\theta)) \sin(a\theta) \\ -\sin(a\theta) \end{pmatrix}.$$

Essa função é uma imersão do círculo ($\mathbb{S}^1$) no toro T parametrizado por

$$(\theta, \varphi) \mapsto \begin{pmatrix} (2 + \cos(\theta)) \cos(\varphi) \\ (2 + \cos(\theta)) \sin(\varphi) \\ \sin(\theta) \end{pmatrix}.$$

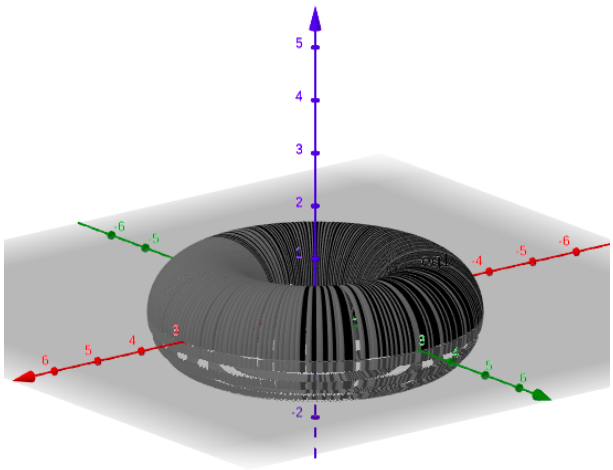
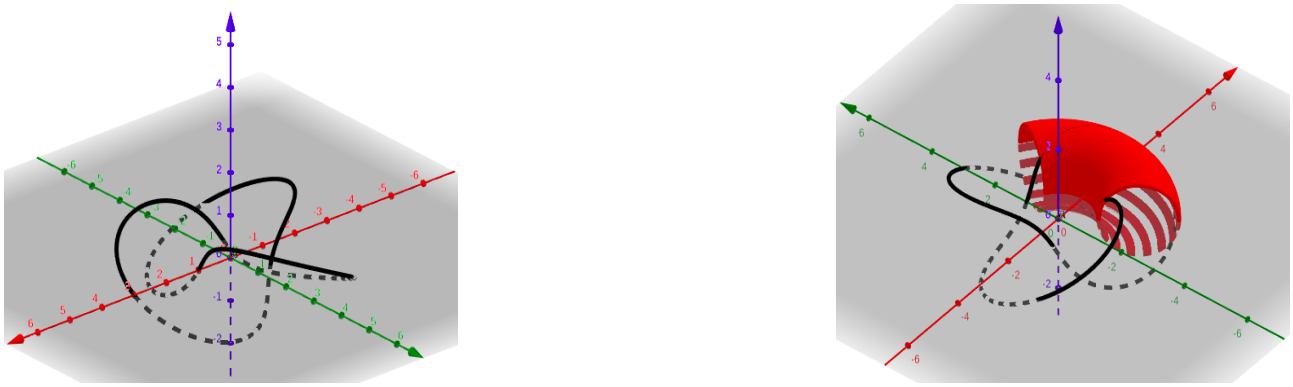


Figura 4.15: O toro T em $\mathbb{R}^3$.

Os exemplos mais simples de nós torais são os nós de toro $K_{2,3}$ e $K_{2,-3}$, que são os nós de trevo destro e canhoto, respectivamente. Note que os nós de trevo ficam completamente

contidos na superfície do toro T, assim como todos os nós torais. Em particular, se $a = \pm 1$ ou se $b = \pm 1$, então o nó $K_{a,b}$ resultante é trivial.



(a) (b)

Figura 4.16: O nó toral $K_{2,3}$ (nó de trevo destro), figura (a) e parte do toro, envolvendo $K_{2,3}$, figura (b)

É interessante observar que, sem a restrição de (a, b) coprimos, a função de $K_{a,b} : \mathbb{S}^1 \to \mathbb{S}^3$ descreve um *link*. Logo, podemos generalizar a Definição 4.3.3 para *links*, da seguinte forma.

Definição 4.3.4 — Link de toro. Para todo par de inteiros a e b (não necessariamente coprimos), o *link* de toro (ou link toral) padrão $K_{a,b} : \mathbb{S}^1 \to \mathbb{S}^2$ correspondente ao par (a, b) é dado, em coordenadas euclidianas, por

$$\theta \mapsto \begin{pmatrix} (2 + \cos(b\theta)) \cos(a\theta) \\ (2 + \cos(b\theta)) \sin(a\theta) \\ -\sin(a\theta) \end{pmatrix}.$$

O número de componentes do link correspondente ao par (a, b) é dado por $d = \text{mdc}(a, b)$, e cada componente é uma cópia do nó $K_{a/d,b/d}$ rotacionado em torno do eixo z.

Uma propriedade interessante é que todo nó toral não trivial é quiral, i.e., não é igual à sua imagem espelhada (daí a nomenclatura "destro" e "canhoto"). Por fim, vale mencionar que todo nó toral $K_{a,b}$ pode ser representado pela trança fechada $(\sigma_1\sigma_2 \cdots \sigma_{a-1})^b$.

Cálculo do grupo de nó

Como dito antes, dados dois nós equivalentes K_1 e K_2, então $\pi_1(\mathbb{R}^3 \setminus K_1) \cong \pi_1(\mathbb{R}^3 \setminus K_2)$. Contudo, novamente, a recíproca não é verdadeira: $\pi_1(\mathbb{R}^3 \setminus K_1) \cong \pi_1(\mathbb{R}^3 \setminus K_2)$ não implica K_1 e K_2 equivalentes.

Se queremos usar os grupos de nó para obter informações acerca dos nós, devemos ser capazes de efetivamente determinar esses grupos. Felizmente, existe um algoritmo simples,

introduzido por Wirtinger por volta de 1904 em suas aulas em Viena e publicado em 1908 por Tietze. Vamos descrever o **método de Wirtinger**.

Algoritmo de Wirtinger

Suponha que temos uma projeção de nó.

1. Fixe uma direção ao longo de K e denote os arcos sucessivos entre dois cruzamentos inferiores por $\alpha_1, \ldots, \alpha_n$.

2. Para $1 \leq i \leq n$, desenhe um seta curta x_i passando por baixo de α_i, em que a direção de x_i é dada pela regra da mão direita, com o dedão apontando na direção escolhida sobre K. Tal seta representa um *loop* em $\mathbb{R}^3 \setminus K$ do seguinte modo: tome um ponto base acima do plano de desenho; então o *loop* consiste do triângulo orientado a partir do ponto base para a cauda de x_i, ao longo de x_i até a ponta e de volta para o ponto base.

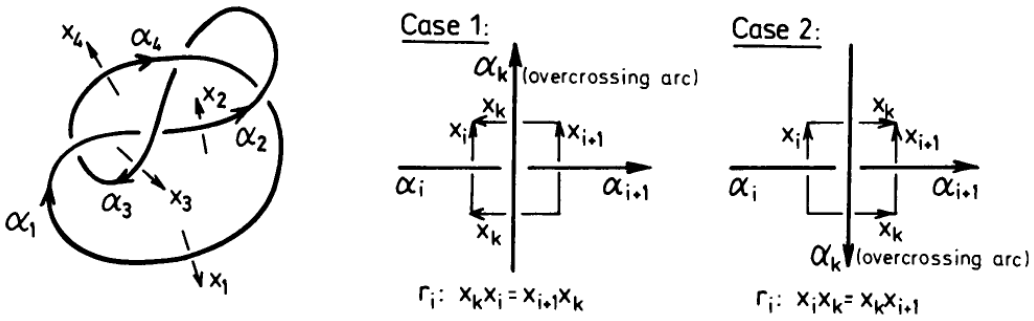


Figura 4.17: Desenhos possíveis

3. Em cada cruzamento, indique o quadrado formado pelas setas sob os arcos envolvidos no cruzamento, e escreva a relação r_i indicada por esse quadrado; há duas possibilidades dadas pelos desenhos na Figura 4.17 (note que $k = i$ ou $k = i + 1$ é possível)

   Então o grupo do nó K é gerado por (classes de homotopia de) *loops* x_i e tem apresentação

$$\pi_1(\mathbb{R}^3 \setminus K) = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_n \rangle. \qquad \text{(Apresentação de Wirtinger)}$$

   Ademais, qualquer das relações r_i é consequência das $n - 1$ relações restantes e pode, portanto, ser omitida.

Não vamos, aqui, demonstrar precisamente o teorema, mas vamos dar algumas observações. É razoavelmente claro, geometricamente, que $\pi_1(\mathbb{R}^3 \setminus K)$ é gerado pelos *loops* x_i; para qualquer *loop* em $\mathbb{R}^3 \setminus K$, basta checar quantas voltas ele dá em cada um dos arcos α_i e deformá-lo

de acordo. Também é claro que as relações r_i devem valer, i.e., que $x_k x_i x_k^{-1} x_{i+1}^{-1}$ (caso 1) ou $x_i x_k x_{i+1}^{-1} x_k^{-1}$ (caso 2) podem ser reduzidas a um ponto em $\mathbb{R}^3 \setminus K$. Isso é mostrado nas seguintes figuras.

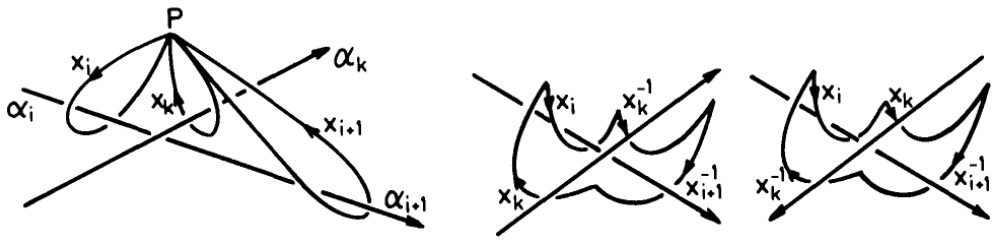


Figura 4.18: Redução em cada caso

O que não é tão óbvio é que nenhuma relação adicional vale e que qualquer uma das n relações pode ser omitida. Vamos olhar os dois exemplos dados acima, do nó de trevo e do nó figura oito, mais de perto.

■ **Exemplo 4.3.1 — Nó de trevo.** Seja K o nó de trevo dado abaixo.

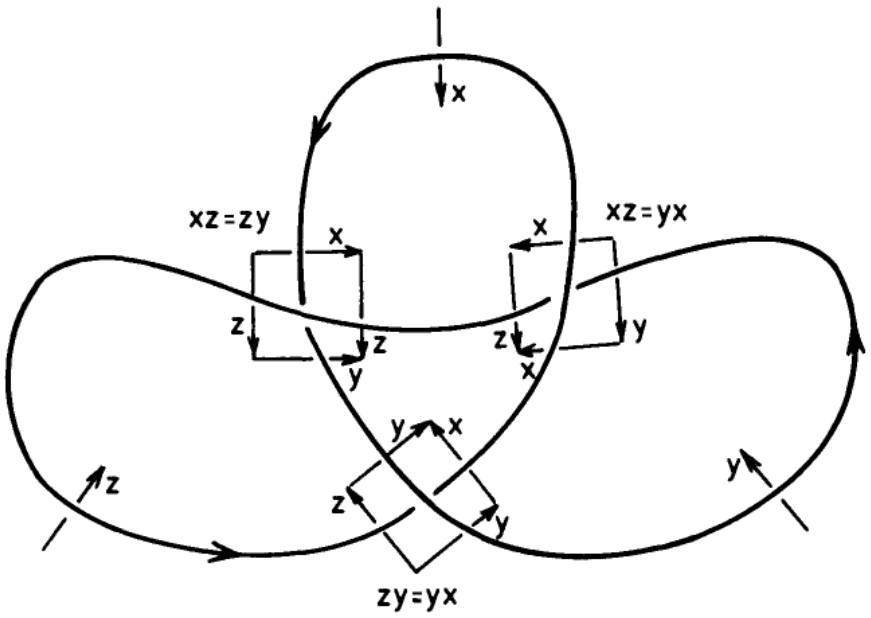


Figura 4.19: Cálculo do grupo de nó do nó de trevo.

Usando a terminologia da figura, vemos que $\pi_1(\mathbb{R}^3 \setminus K)$ é gerado por 3 elementos x, y, z, sujeitos às relações $xz = zy, xz = yx$ e $zy = yx$. De acordo com o teorema de Wirtinger, qualquer uma dessas relações, digamos a terceira, pode ser omitida; isso pode ser verificado algebricamente: eliminando $z = x^{-1}yx$ da segunda relação, a primeira relação se torna $xyx =$

yxy. Logo, obtemos uma apresentação para $\pi_1(\mathbb{R}^3 \setminus K)$ do nó de trevo:

$$\pi_1(\mathbb{R}^3 \setminus K) = \langle x, y \mid xyx = yxy \rangle.$$

Fazendo $a = xyx$ e $b = xy$, temos $x = b^{-1}a, y = a^{-1}b^2$ e $a^2 = (xyx)^2 = (xyx)(xyx) = (xyx)(yxy) = (xy)^3 = b^3$. Assim, podemos escrever o grupo do nó de trevo como

$$\pi_1(\mathbb{R}^3 \setminus K) = \langle a, b \mid a^2 = b^3 \rangle.$$

Note que $\alpha = (12)$ e $\beta = (123)$ em S_3 também satisfazem $\alpha^2 = \beta^3 = e$. Logo, S_3 é imagem homomórfica de $\pi_1(\mathbb{R}^3 \setminus K)$, o que implica que $\pi_1(\mathbb{R}^3 \setminus K)$ não é abeliano. Em particular, o grupo de K não é isomorfo ao grupo do nó trivial ($\mathbb{Z}$), logo K não pode ser desatado sem cortes e colagens (como esperado). ∎

∎ **Exemplo 4.3.2 — Nó figura oito.** O nó figura oito é mostrado abaixo.

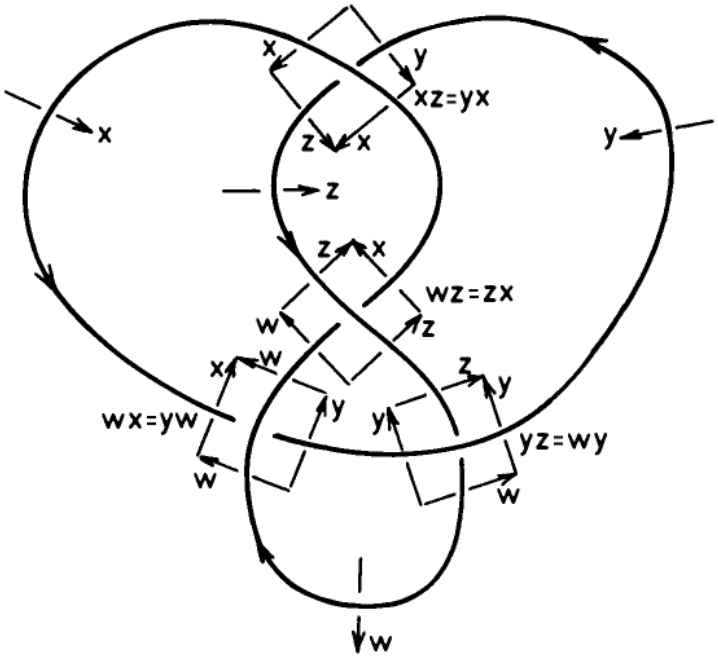


Figura 4.20: Cálculo do grupo de nó do nó figura oito

O algoritmo de Wirtinger nos dá quatro geradores x, y, z, w e quatro relações $xz = yx, wz = zx, yz = wy$ e $wx = yw$. Novamente, a última dessas relações pode ser omitida. Escrevemos a primeira relação na forma $z = x^{-1}yx$ e então a segunda relação na forma $w = zxz^{-1} = (x^{-1}yx)x(x^{-1}y^{-1}x) = x^{-1}yxy^{-1}x$; e a última relação, a terceira, torna-se $yx^{-1}yx = x^{-1}yxy^{-1}xy$. Logo, o grupo $\pi_1(\mathbb{R}^3 \setminus K)$ do nó de trevo pode ser apresentado como

$$\pi_1(\mathbb{R}^3 \setminus K) = \langle x, y \mid yx^{-1}yx = x^{-1}yxy^{-1}xy \rangle.$$

■

Se dois nós têm grupos não isomorfos, então não é possível deformar um dos nós no outro; em particular, se o grupo de um nó não é isomorfo a $\mathbb{Z}$, então esse nó não é trivial. Portanto, podemos utilizar a teoria dos grupos para distinguir tipos diferentes de nós. Contudo, vale pontuar que se dois nós são dados por uma apresentação (como a apresentação de Wirtinger), em geral é um problema algébrico difícil decidir se esses grupos são isomorfos ou não.

Por outro lado, pode-se pensar no problema puramente algébrico de decidir se dois grupos dados por apresentações são isomorfos ou não. Se soubermos que esses grupos ocorrem como grupos de nó, e também soubermos, por considerações topológicas, que esses nós não são equivalentes, então podemos concluir que esses dois grupos não são isomorfos. Portanto, não apenas a teoria dos grupos ajuda a topologia, mas reciprocamente!

4.4 Representação de Burau e os polinômios de Alexander e Jones

Como consequência do Teorema 4.1.3, podemos usar tranças e a teoria das tranças para determinar invariantes de nós. Um dos exemplos mais elegantes desse método é o chamado *polinômio de Alexander*, nomeado em homenagem ao matemático norte-americano J.W. Alexander, e denotado por $\Delta_K(t)$, sendo K um nó (ou *link*).

Mesmo com a descoberta do polinômio de Jones (outro invariante que também será tratado mais à frente) e seus híbridos em 1980, o polinômio de Alexander ainda permanece, mesmo após mais de 50 anos de pesquisa, um dos mais importantes e úteis invariantes de nós (e *links*).

Para definir o polinômio de Alexander, devemos primeiro definir o que é um módulo. Para os nossos propósitos, vamos definir módulo como um grupo abeliano munido de uma operação $\cdot$, chamada de multiplicação por escalar. [1]

Agora, podemos introduzir a chamada *representação de Burau* de $B_n(\mathbb{R}^2)$. Então, seja $\beta \in B_n(\mathbb{R}^2)$. Podemos representar essa trança como

$$\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k},$$

com $1 \leq i_1, \ldots, i_k \leq n-1$ e $\varepsilon_i = \pm 1$. Agora, vamos definir a função

$$\varphi_n : B_n \to M(n, \mathbb{Z}[t, t^{-1}])$$

[1] Essa definição é bastante incompleta, mas o meu foco não é sobre as definições algébricas em si, e sim nas ideias envolvendo as tranças.

sendo $M(n, \mathbb{Z}[t, t^{-1}])$ as matrizes de ordem n sobre o módulo $\mathbb{Z}[t, t^{-1}]$, tal que

$$\varphi_n(\sigma_i) = \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 1-t & t & \\ & 1 & 0 & \\ \hline & & & I_{n-i-1} \end{array}\right], \tag{4.1}$$

sendo I_m a matriz identidade de ordem m e os espaços vazios correspondem a matrizes nulas. A representação de B_n dada em (4.1) é chamada *representação de Burau*. De fato, φ_n é homomorfismo, como mostraremos a seguir.

Proposição 4.4.1 A função φ_n definida em (4.1) é um homomorfismo. ∎

Demonstração. Basta mostrarmos que toda relação de B_n é mapeada na matriz identidade ou, equivalentemente, que as relações de B_n se mantêm para φ_n.

Primeiro, vamos mostrar que se $|i-j| \geq 2$, então $\varphi_n(\sigma_i)\varphi_n(\sigma_j) = \varphi_n(\sigma_j)\varphi_n(\sigma_i)$. Sem perda de generalidade, podemos tomar $j > i+1$ e, portanto,

$$\begin{aligned}
\varphi_n(\sigma_i)\varphi_n(\sigma_j) &= \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 1-t & t & \\ & 1 & 0 & \\ \hline & & & I_{n-i-1} \end{array}\right] \cdot \left[\begin{array}{c|cc|c} I_{j-1} & & & \\ \hline & 1-t & t & \\ & 1 & 0 & \\ \hline & & & I_{n-j-1} \end{array}\right] \\
&= \left[\begin{array}{c|cc|c|c} I_{i-1} & & & & \\ \hline & 1-t & t & & \\ & 1 & 0 & & \\ \hline & & & I_{j-i-2} & \\ \hline & & & & \begin{array}{cc} 1-t & t \\ 1 & 0 \end{array} \\ \hline & & & & I_{n-j-1} \end{array}\right] \\
&= \left[\begin{array}{c|cc|c} I_{j-1} & & & \\ \hline & 1-t & t & \\ & 1 & 0 & \\ \hline & & & I_{n-j-1} \end{array}\right] \cdot \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 1-t & t & \\ & 1 & 0 & \\ \hline & & & I_{n-i-1} \end{array}\right] \\
&= \varphi_n(\sigma_j)\varphi_n(\sigma_i)
\end{aligned}$$

sendo os espaços vazios preenchidos por matrizes nulas.

Agora, para a segunda e última relação, $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, basta considerarmos o caso $n = 3$, uma vez que na representação de Burau as entradas não nulas correspondem a matrizes identidade, ou seja, aumentando n a partir de 3, estaremos apenas acrescentando uma nova linha e uma nova coluna que serão ambas nulas com exceção da entrada diagonal, que será 1; portanto, a multiplicação das matrizes não é afetada.

Então, tomando $n = 3$, temos

$$\begin{aligned}
\varphi_3(\sigma_1\sigma_2\sigma_1) &= \varphi_3(\sigma_1)\varphi_3(\sigma_2)\varphi_3(\sigma_1) \\
&= \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} (1-t)^2 + t(1-t) & t(1-t) & t^2 \\ 1-t & t & 0 \\ 1 & 0 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{bmatrix} \\
&= \varphi_3(\sigma_2)\varphi_3(\sigma_1)\varphi_3(\sigma_2) \\
&= \varphi_3(\sigma_2\sigma_1\sigma_2).
\end{aligned}$$

■

Observação. Em geral, a função φ_n não é fiel, i.e., injetiva. Para $n = 2$ e $n = 3$, é sabido que φ_n é fiel; para $n = 4$, contudo, não sabemos.

Note também que como $\det(\varphi_n(\sigma_i)) = -t$ (basta expandir o determinante pelas primeiras $i-1$ linhas e, em seguida, pelas últimas $n-i-1$ linhas, restando apenas a matriz $\left[\begin{smallmatrix} 1-t & t \\ 1 & 0 \end{smallmatrix}\right]$), então existe o inverso de $\varphi_n(\sigma_i)$. Para computá-lo, note que

$$\varphi_n(1) = I_n = \varphi_n(\sigma_i\sigma_i^{-1}) = \varphi_n(\sigma_i)\varphi_n(\sigma_i^{-1}) \Leftrightarrow \varphi_n(\sigma_i^{-1}) = (\varphi_n(\sigma_i))^{-1}.$$

Calculando o inverso de $\varphi_n(\sigma_i)$ (que se resume basicamente a encontrar o inverso de $\left[\begin{smallmatrix} 1-t & t \\ 1 & 0 \end{smallmatrix}\right]$), obtemos

$$\varphi_n(\sigma_i^{-1}) = \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 0 & 1 & \\ & t^{-1} & 1-t^{-1} & \\ \hline & & & I_{n-i-1} \end{array}\right].$$

Por exemplo, tomando $\beta = \sigma_1\sigma_2^{-1}$, temos

$$\varphi_3(\beta) = \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix} = \begin{bmatrix} 1-t & 0 & t \\ 1 & 0 & 0 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix}.$$

Vamos, agora, tratar do polinômio de Alexander em si.

Então, suponha que percebemos que uma quantidade $\lambda(\beta)$, derivada de uma trança β de n cordas, é um invariante de nó (ou *link*). Devido ao Teorema 4.1.3, para mostrar que $\lambda(\beta)$ é realmente um invariante, é suficiente mostrar que para uma trança β de n cordas valem as seguintes propriedades:

1. $\lambda(\beta) = \lambda(\gamma\beta\gamma^{-1})$ para $\gamma \in B_n$ arbitrária;

2. $\lambda(\beta\sigma_n) = \lambda(\beta) = \lambda(\beta\sigma_n^{-1})$ para tranças de $n+1$ cordas $\beta\sigma_n$ e $\beta\sigma_n^{-1}$.

Voltando à representação de Burau apresentada anteriormente, uma quantidade que satisfaz as propriedades 1 e 2 é o determinante da matriz, pois como $\det(\varphi_n(\sigma_i)) = -t$, e sabendo que podemos escrever $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$, temos

$$\begin{aligned}
\det(\varphi_n(\beta)) &= \det\left(\prod_{i=1}^{k} \varphi_n^{\varepsilon_i}(\sigma_i)\right) \\
&= \prod_{i=1}^{k} (\det(\varphi_n(\sigma_i)))^{\varepsilon_i} \\
&= (-t)^{\sum_{i=1}^{k} \varepsilon_i} \\
&= (-t)^{l(\beta)} \\
&= (-t)^{l(\gamma\beta\gamma^{-1})} \\
&= \det(\varphi_n(\gamma\beta\gamma^{-1})),
\end{aligned}$$

sendo l a função homomorfismo de comprimento definida no Lema 3.1.4. Em particular, note que

$$\det(\varphi_n(\beta)) = (-t)^{l(\beta)}. \tag{4.2}$$

Portanto, se fizermos $\lambda(\beta) = \det(\varphi_n(\beta))(-t)^{-\epsilon}$, sendo $\epsilon = l(\beta)$, então $\lambda(\beta)$ se torna um invariante.

Contudo, esse invariante não é muito interessante, uma vez que $\lambda(\beta) = 1$ para toda trança β. Então, ao invés do determinante de $\varphi_n(\beta)$, vamos considerar o "polinômio característico" de $\varphi_n(\beta)$, a saber

$$\det(\varphi_n(\beta) - I_n).$$

Como veremos a seguir, isso leva a um invariante (não trivial) de nós, mas antes precisamos do seguinte lema técnico.

Lema 4.4.1 Escrevendo a representação de Burau de uma trança de n cordas β como $\varphi_n(\beta) = ||a_{ij}||$, $i, j = 1, 2, \ldots, n$, então as seguintes propriedades valem:

$$\sum_{j=1}^{n} a_{ij} = 1, \tag{4.3}$$

$$\sum_{i=1}^{n} t^i a_{ij} = t^j, \tag{4.4}$$

ou seja, a soma de todos os elementos da linha i é igual a 1 (4.3) e somando os elementos da coluna j (com o primeiro elemento multiplicado por t, o segundo por t^2 e assim por diante) obtemos t^j, como em (4.4).

Demonstração. Primeiro, note que (4.3) e (4.4) valem se $\beta = \sigma_i^{\pm 1}$, para i qualquer, basta usar (4.1). Agora, vamos mostrar que se A e B são duas matrizes que satisfazem (4.3) e (4.4), então o seu produto AB também satisfaz as mesmas equações. Mostrando isso, o resultado segue por indução.

Então, suponha $A = ||a_{ij}||$ e $B = ||b_{kl}||$ duas matrizes de ordem n para as quais (4.3) e (4.4) valem. Além disso, seja $AB = ||c_{pq}||$, com $c_{pq} = \sum_{j=1}^{n} a_{pj} b_{jq}$. Daí,

$$\sum_{q=1}^{n} c_{pq} = \sum_{q=1}^{n} \sum_{j=1}^{n} a_{pj} b_{jq} = \sum_{j=1}^{n} a_{pj} \underbrace{\left\{ \sum_{q=1}^{n} b_{jq} \right\}}_{=1} = \sum_{j=1}^{n} a_{pj} = 1$$

$$\sum_{p=1}^{n} t^p c_{pq} = \sum_{p=1}^{n} \sum_{j=1}^{n} t^p a_{pj} b_{jq} = \sum_{j=1}^{n} \underbrace{\left\{ \sum_{p=1}^{n} t^p a_{pj} \right\}}_{=t^j} b_{jq} = \sum_{j=1}^{n} t^j b_{jq} = t^q.$$

■

Segue imediatamente do Lema 4.4.1 que

$$\sum_{j=1}^{n} (a_{ij} - \delta_{ij}) = \sum_{j=1}^{n} a_{ij} - 1 = 0, \tag{4.5}$$

$$\sum_{i=1}^{n} (t^i a_{ij} - t^i \delta_{ij}) = \sum_{i=1}^{n} t^i a_{ij} - t^j = 0, \tag{4.6}$$

sendo δ_{ij} o delta de Kronecker.

O significado da equação (4.5) é que, na matriz $\varphi_n(\beta) - I_n$, excluindo a primeira coluna e adicionando todas as colunas restantes à primeira, obtemos uma coluna nula. Similarmente, na equação (4.6) adicionamos a i-ésima linha multiplicada por t^i, $i = 1, 2, \ldots, n$, à primeira linha, obtendo a linha nula. Consequentemente, obtemos

$$\det(\varphi_n(\beta) - I_n) = 0.$$

Antes de seguir para o polinômio de Alexander em si, precisaremos dos dois lemas a seguir, o primeiro dos quais será aceito sem demonstração.

Lema 4.4.2 Seja $M = \varphi_n(\beta)$ para uma trança β de n cordas. Denote por $M_{p,q}$ a matriz de ordem $(n-1)$ obtida de M deletando a p-ésima linha e a q-ésima coluna, e denote o seu determinante por $\det[M]_{p,q}$. Então, valem as seguintes igualdades:

1. $\det[M - I_n]_{p,p} = t^{p-1} \det[M - I_n]_{1,1}$ para $p = 1, 2, \ldots, n$
2. $\det[M - I_n]_{p,q} = (-1)^{p+q} t^{p-1} \det[M - I_n]_{1,1}$ para quaisquer $1 \leq p, q \leq n$.

Antes do próximo lema, convém fazer algumas definições. Então, seja S uma matriz de ordem n tal que

$$S = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

$$S^{-1} = \begin{bmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Então, sendo $M = \varphi_n(\beta)$, temos

$$S^{-1}MS = \left[\begin{array}{c|c} \Lambda(t) & \\ \hline * \cdots * & 1 \end{array}\right],$$

em que $\Lambda(t)$ é uma matriz não singular $(n-1) \times (n-1)$. Portanto, temos

$$\det[S^{-1}MS - I_n]_{n,n} = \det[S^{-1}(M - I_n)S]_{n,n} = \det(\Lambda(t) - I_{n-1}),$$

uma vez que

$$\det[S^{-1}(M-I_n)S]_{n,n} = \det[S^{-1}MS-I_n]_{n,n} = \det\left[\left[\begin{array}{c|c} \Lambda(t) - I_{n-1} & \\ \hline * \cdots * & 0 \end{array}\right]\right]_{n,n} = \det(\Lambda(t)-I_{n-1}).$$

Lema 4.4.3 Temos

$$\det(\Lambda(t) - I_{n-1}) \doteq (1 + t + \cdots + t^{n-1}) \det[M - I_n]_{1,1}$$

ou, equivalentemente,

$$\det[S^{-1}(M - I_n)S]_{n,n} \doteq (1 + t + \cdots + t^{n-1}) \det[M - I_n]_{1,1},$$

em que $f \doteq g$ denota que $f = \pm t^k g$ para algum $k \in \mathbb{Z}$.

Demonstração. Seja $M = ||a_{ij}||_{1\leq i,j\leq n}$. Por simplicidade, denote por $[M - I_n]_{0,n}$ a matriz $n \times (n-1)$ obtida deletando a n-ésima coluna. Então, as linhas de $[M - I_n]_{0,n}$ têm a seguinte forma:

$$\begin{aligned} A_1 &= (a_{11} - 1, a_{12}, \ldots, a_{1\,n-1}), \\ A_2 &= (a_{21}, a_{22} - 1, \ldots, a_{2\,n-1}), \\ &\vdots \\ A_n &= (a_{n1}, a_{n2}, \ldots, a_{n\,n-1}). \end{aligned}$$

Uma computação direta e cuidadosa nos dá

$$U(\Lambda(t) - I_{n-1})V = \begin{bmatrix} A_1 - A_2 \\ A_1 - A_3 \\ \vdots \\ A_1 - A_n \end{bmatrix},$$

sendo $U = [S^T]_{n,n}$ e $V = [S^{-1}]_{n,n}$. Daí, usando a multilinearidade do determinante, obtemos:

$$\begin{aligned} \det(\Lambda(t) - I_{n-1}) &= \det[U(\Lambda(t) - I_{n-1})V] \\ &= \det \begin{bmatrix} A_1 - A_2 \\ A_1 - A_3 \\ \vdots \\ A_1 - A_n \end{bmatrix} \\ &= \det \begin{bmatrix} A_1 \\ -A_3 \\ -A_4 \\ \vdots \\ -A_n \end{bmatrix} + \det \begin{bmatrix} -A_2 \\ A_1 \\ -A_4 \\ \vdots \\ -A_n \end{bmatrix} + \cdots \\ &\cdots + \det \begin{bmatrix} -A_2 \\ \vdots \\ -A_k \\ A_1 \\ -A_{k+2} \\ \vdots \\ -A_n \end{bmatrix} + \cdots \\ &\cdots + \det \begin{bmatrix} -A_2 \\ -A_3 \\ \vdots \\ -A_{n-1} \\ A_1 \end{bmatrix} + \det \begin{bmatrix} -A_2 \\ -A_3 \\ \vdots \\ -A_n \end{bmatrix}. \end{aligned}$$

Daí, temos

$$\det\begin{bmatrix} -A_2 \\ -A_3 \\ \vdots \\ -A_n \end{bmatrix} = (-1)^{n-1}\det[M-I_n]_{1,n} = (-1)^{n-1+n+1}t^0\det[M-I_n]_{1,1} = \det[M-I_n]_{1,1},$$

em que na primeira igualdade retiramos todos os fatores -1 do determinante e, na segunda igualdade, utilizamos o Lema 4.4.2. Analogamente, temos

$$\det\begin{bmatrix} A_1 \\ -A_3 \\ \vdots \\ -A_n \end{bmatrix} = (-1)^{n-2}\det[M-I_n]_{2,n} = (-1)^{n-2+n+2}t^1\det[M-I_n]_{1,1} = t\det[M-I_n]_{1,1}.$$

Por fim, de modo análogo para todo $2 \leq k \leq n-1$, obtemos

$$\det\begin{bmatrix} -A_2 \\ \vdots \\ -A_k \\ A_1 \\ -A_{k+2} \\ \vdots \\ -A_n \end{bmatrix} = (-1)^{n-2+k-1}\det\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_k \\ A_{k+2} \\ \vdots \\ A_n \end{bmatrix} = (-1)^{n+k-3}\det[M-I_n]_{k+1,n} = t^k\det[M-I_n]_{1,1}.$$

Consequentemente, $\det(\Lambda(t)-I_{n-1}) = (1+t+\cdots+t^{n-1})\det[M-I_n]_{1,1}$. ■

Agora estamos prontos para enunciar e demonstrar o teorema desejado.

Teorema 4.4.1 Seja K um nó (ou link) orientado e suponha β uma trança de n cordas cujo fecho é K. Se fizermos $M = \varphi_n(\beta)$, então $\det[M-I_n]_{1,1}$ é um invariante de K, a menos de um fator $\pm t^k$, para algum $k \in \mathbb{Z}$.

A essência do Teorema 4.4.1 é que se $\beta_1 \in B_n$ e $\beta_2 \in B_m$ são duas tranças cujos fechos são equivalentes, i.e., tais que $\widetilde{\beta_1} \approx \widetilde{\beta_2}$, então existe $k \in \mathbb{Z}$ tal que

$$\det[\varphi_n(\beta_1)-I_n]_{1,1} = \pm t^k\det[\varphi_m(\beta_2)-I_m]_{1,1}.$$

Esse invariante é chamado *polinômio de Alexander* (reduzido) de K e denotado por $\Delta_K(t)$. Multiplicando por um fator adequado, $\Delta_K(t)$ (se não for nulo) pode ser escrito como

$$\Delta_K(t) = c_0 + c_1t + \cdots + c_mt^m, c_0 > 0.$$

Agora, para a demonstração.

Demonstração. Pelo Teorema 4.1.3, basta mostrarmos que para duas tranças quaisquer β e γ de n cordas, valem

1. $\det[\varphi_n(\gamma\beta\gamma^{-1}) - I_n]_{1,1} \doteq \det[\varphi_n(\beta) - I_n]_{1,1}$;
2. $\det[\varphi_n(\beta\sigma_n) - I_{n+1}]_{1,1} \doteq \det[\varphi_n(\beta) - I_n]_{1,1} \doteq \det[\varphi_n(\beta\sigma_n^{-1}) - I_{n+1}]_{1,1}$.

Note que em 2, o centro é o determinante de uma matriz de ordem $n-1$, enquanto que nos lados esquerdo e direito temos o determinante de uma matriz de ordem n. Vamos começar com a demonstração de 1.

Suponha β e γ duas tranças de n cordas. Então, podemos escrever

$$S^{-1}\varphi_n(\beta)S = \left[\begin{array}{c|c} \Lambda(\beta) & \\ \hline a_1 \cdots a_{n-1} & 1 \end{array}\right] \text{ e } S^{-1}\varphi_n(\gamma)S = \left[\begin{array}{c|c} \Lambda(\gamma) & \\ \hline b_1 \cdots b_{n-1} & 1 \end{array}\right].$$

Similarmente, podemos escrever

$$S^{-1}\varphi_n(\gamma^{-1})S = \left[\begin{array}{c|c} \Lambda^{-1}(\gamma) & \\ \hline c_1 \cdots c_{n-1} & 1 \end{array}\right].$$

Logo, multiplicando essas matrizes e usando o fato de que φ_n é homomorfismo, temos

$$S^{-1}\varphi_n(\gamma\beta\gamma^{-1})S = \left[\begin{array}{c|c} \Lambda(\gamma)\Lambda(\beta)\Lambda^{-1}(\gamma) & \\ \hline d_1 \cdots d_{n-1} & 1 \end{array}\right]$$

e, portanto,

$$\begin{aligned} \det[S^{-1}\varphi_n(\gamma\beta\gamma^{-1})S - I_n]_{n,n} &= \det(\Lambda(\gamma)\Lambda(\beta)\Lambda^{-1}(\gamma) - I_{n-1}) \\ &= \det[\Lambda(\gamma)(\Lambda(\beta) - I_{n-1})\Lambda^{-1}(\gamma)] \\ &= \det(\Lambda(\gamma))\det(\Lambda^{-1}(\gamma))\det(\Lambda(\beta) - I_{n-1}) \\ &= \det(\Lambda(\beta) - I_{n-1}). \end{aligned}$$

Aplicando o Lema 4.4.3 a ambos os lados da igualdade, temos

$$(1 + t + \cdots + t^{n-1})\det[\varphi_n(\gamma\beta\gamma^{-1}) - I_n]_{1,1} \doteq (1 + t + \cdots + t^{n-1})\det[\varphi_n(\beta) - I_n]_{1,1}$$

e, portanto,

$$\det[\varphi_n(\gamma\beta\gamma^{-1}) - I_n]_{1,1} \doteq \det[\varphi_n(\beta) - I_n]_{1,1},$$

finalizando a demonstração de 1. Agora, para a demonstração de 2.

Suponha β uma trança de n cordas e seja $\varphi_n(\beta)(= M) = ||a_{ij}||$. Se considerarmos $\beta \in B_{n+1}$, então

$$\varphi_{n+1}(\beta) = \left[\begin{array}{c|c} M & \\ \hline & 1 \end{array}\right]$$

e, como da definição da representação de Burau em (4.1), temos

$$\varphi_{n+1}(\sigma_n) = \left[\begin{array}{c|cc} I_{n-1} & & \\ \hline & 1-t & t \\ & 1 & 0 \end{array}\right].$$

Multiplicando as duas matrizes acima e usando o fato de que φ_n é homomorfismo, segue que

$$\varphi_{n+1}(\beta\sigma_n) = \left[\begin{array}{c|cc} & a_{1n}(1-t) & a_{1n}t \\ M_{n,n} & \vdots & \vdots \\ & a_{n-1\,n}(1-t) & a_{n-1\,n}t \\ a_{n1}\cdots a_{n\,n-1} & a_{n\,n}(1-t) & a_{n\,n}t \\ \hline & 1 & 0 \end{array}\right].$$

Logo,

$$\begin{aligned} \det[\varphi_{n+1}(\beta\sigma_n) - I_{n+1}]_{n,n} &= \det\left[\begin{array}{c|c} M_{n,n} - I_{n-1} & \begin{array}{c} a_{1n}t \\ \vdots \\ a_{n-1\,n}t \end{array} \\ \hline & -1 \end{array}\right] \\ &= -\det[M_{n,n} - I_{n-1}] \\ &= -\det[\varphi_n(\beta) - I_n]_{n,n} \\ &\doteq \det[\varphi_n(\beta) - I_n]_{n,n}. \end{aligned}$$

Pelo Lema 4.4.2, sabemos que $\det[M - I_n]_{1,1} \doteq \det[M - I_n]_{n,n}$. Daí, aplicando esse fato a ambos os lados da igualdade, obtemos

$$\det[\varphi_{n+1}(\beta\sigma_n) - I_{n+1}]_{1,1} \doteq \det[\varphi_{n+1}(\beta\sigma_n) - I_{n+1}]_{n,n} \doteq \det[\varphi_n(\beta) - I_n]_{1,1}.$$

De modo similar, podemos escrever

$$\varphi_{n+1}(\sigma_n^{-1}) = \left[\begin{array}{c|cc} I_{n-1} & & \\ \hline & 0 & 1 \\ & t^{-1} & 1-t^{-1} \end{array}\right].$$

Daí, novamente usando a definição da representação de Burau em (4.1), temos

$$\varphi_{n+1}(\beta\sigma_n^{-1}) = \left[\begin{array}{c|c|c} & & a_{1n} \\ M_{n,n} & & \vdots \\ & & a_{n-1\,n} \\ a_{n1}\cdots a_{n\,n-1} & & a_{n\,n} \\ \hline & t^{-1} & 1-t^{-1} \end{array}\right].$$

Logo, multiplicando as matrizes acima e usando o fato de que φ_n é homomorfismo, segue que

$$\det[\varphi_{n+1}(\beta\sigma_n^{-1}) - I_{n+1}]_{n,n} = \det\left[\begin{array}{c|c} M_{n,n} - I_{n-1} & \begin{array}{c} a_{1n} \\ \vdots \\ a_{n-1\,n} \end{array} \\ \hline & -t^{-1} \end{array}\right]$$

$$\begin{aligned} &= -t^{-1}\det[M_{n,n} - I_{n-1}] \\ &= -t^{-1}\det[\varphi_n(\beta) - I_n]_{n,n} \\ &\doteq \det[\varphi_n(\beta) - I_n]_{n,n}. \end{aligned}$$

Pelo Lema 4.4.2, sabemos que $\det[M - I_n]_{1,1} \doteq \det[M - I_n]_{n,n}$. Daí, aplicando esse fato a ambos os lados da igualdade, obtemos

$$\det[\varphi_{n+1}(\beta\sigma_n^{-1}) - I_{n+1}]_{1,1} \doteq \det[\varphi_{n+1}(\beta\sigma_n^{-1}) - I_{n+1}]_{n,n} \doteq \det[\varphi_n(\beta) - I_n]_{1,1}$$

e concluímos a demonstração. ■

Por exemplo, o nó trivial em B_1 é $\beta = 1$. Logo, $\varphi_1(1) = [1]$ e então $\varphi_1(1) - 1 = [0]$ e $[\varphi_1(1) - 1]_{1,1}$ é a matriz vazia, $\varnothing$. Vamos definir $\det(\varnothing) = 1$, e então $\Delta_{\widetilde{1}}(t) = 1$.

O nó trivial também é representado por σ_1 em B_2. Nesse caso,

$$N = \varphi_2(\sigma_1) - I_2 = \begin{bmatrix} -t & t \\ 1 & -1 \end{bmatrix},$$

logo $\det[N]_{1,1} = -1$ e $\det[N]_{2,2} = -t$ e temos, novamente, $\Delta_{\widetilde{\sigma_1}}(t) = 1$.

Por outro lado, em B_3 a trança σ_1 representa o fecho de um *link* trivial de 2 componentes. Nesse caso,

$$N = \varphi_3(\sigma_1) - I_3 = \begin{bmatrix} -t & t & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

e, portanto, $\det[N]_{1,1} = 0$. Logo, para $\sigma_1 \in B_3$, $\Delta_{\widetilde{\sigma_1}}(t) = 0$. Note que acabamos de mostrar que o polinômio de Alexander pode ser 0 para um *link*.

Tomando $\beta = \sigma_1\sigma_2$ em B_3, temos que $\widetilde{\beta}$, i.e, o fecho de β, é o nó trivial. Nesse caso, temos

$$\varphi_3(\beta) - I_3 = \begin{bmatrix} -t & t(1-t) & t^2 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

logo, $\det[\varphi_3(\beta) - I_3]_{1,1} = 1 = \Delta_{\widetilde{\beta}}(t)$, como esperado.

Da Figura 4.21, pode-se mostrar que $\beta_1 \underset{M}{\sim} \beta_2$. Vamos ver o que acontece quando calculamos $\varphi_3(\beta_1)$ e $\varphi_2(\beta_2)$ (esperamos que sejam iguais).

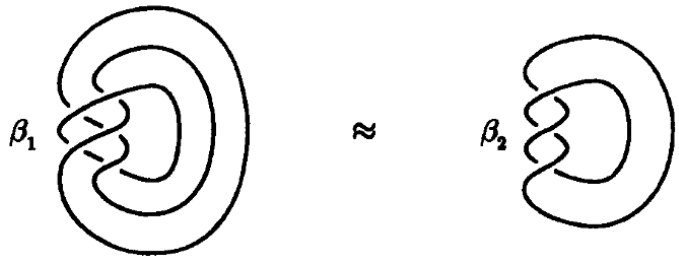


Figura 4.21: Dois nós Markov equivalentes.

Como $\beta_1 = (\sigma_1\sigma_2)^2$ e $\beta_2 = \sigma_1^3$ e, por definição,

$$\varphi_3(\sigma_1) = \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ e } \varphi_3(\sigma_2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-t & t \\ 0 & 1 & 0 \end{bmatrix}$$

segue que

$$\varphi_3(\sigma_1\sigma_2)^2 = \begin{bmatrix} 1-t & t-t^2+t^3 & t^2-t^3 \\ 1-t & t-t^2 & t^2 \\ 1 & 0 & 0 \end{bmatrix}.$$

Logo,

$$\Delta_{\widetilde{\beta}_1}(t) = \det[\varphi_3(\beta_1) - I_3]_{1,1} = \det \begin{bmatrix} -1+t-t^2 & t^2 \\ 0 & -1 \end{bmatrix} = 1 - t + t^2.$$

Por outro lado,

$$\varphi_2(\sigma_1) = \begin{bmatrix} 1-t & t \\ 1 & 0 \end{bmatrix} \text{ e } \varphi_2(\sigma_1)^3 = \begin{bmatrix} 1-t+t^2-t^3 & t(1-t+t^2) \\ 1-t+t^2 & t-t^2 \end{bmatrix}.$$

Logo,

$$\Delta_{\widetilde{\beta}_2}(t) = \det[\varphi_2(\beta_2) - I_2]_{1,1} = -1 + t - t^2$$

e, consequentemente, $\Delta_{\widetilde{\beta}_1}(t) = -\Delta_{\widetilde{\beta}_2}(t)$, ou seja,

$$\Delta_{\widetilde{\beta}_1}(t) \doteq \Delta_{\widetilde{\beta}_2}(t),$$

como esperado.

Observe os nós da Figura 4.22. O nó (a) é o nó K_a, fecho de $(\sigma_1\sigma_2^{-1})^2$ em B_3 e o nó (b) é o nó K_b, fecho de σ_1^n em B_2.

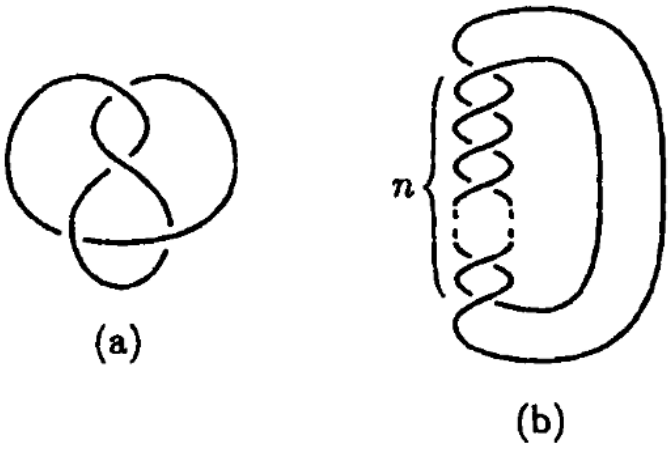


Figura 4.22: O nó figura oito (a) e um nó com n cruzamentos (b).

Por definição, temos

$$\varphi_3(\sigma_1\sigma_2^{-1}) = \begin{bmatrix} 1-t & t & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix} = \begin{bmatrix} 1-t & 0 & t \\ 1 & 0 & 0 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix}.$$

Logo,

$$\varphi_3(\sigma_1\sigma_2^{-1})^2 = \begin{bmatrix} 1-t & 0 & t \\ 1 & 0 & 0 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix} \begin{bmatrix} 1-t & 0 & t \\ 1 & 0 & 0 \\ 0 & t^{-1} & 1-t^{-1} \end{bmatrix} = \begin{bmatrix} (1-t)^2 & 1 & -1+2t-t^2 \\ 1-t & 0 & t \\ t^{-1} & t^{-1}-t^{-2} & (1-t^{-1})^2 \end{bmatrix}.$$

Daí, obtemos

$$\Delta_{K_a}(t) = \det[\varphi_3(\sigma_1\sigma_2^{-1})^2 - I_3]_{1,1} = \det \begin{bmatrix} -1 & t \\ t^{-1}-t^{-2} & -1+(1-t^{-1})^2 \end{bmatrix} = -1+3t^{-1}-t^{-2} \underset{\times(-t^2)}{\doteq} 1-3t+t^2.$$

Para o nó K_b, temos que

$$\varphi_2(\sigma_1)^n = \begin{bmatrix} 1-t & t \\ 1 & 0 \end{bmatrix}^n.$$

Como $\varphi_2(\sigma_1)$ tem autovalores $\lambda_{1,2} = 1, -t$ e autovetores $v_{1,2} = (1,1), (-t,1)$, obtemos

$$\begin{aligned} \varphi_2(\sigma_1)^n &= \frac{1}{1+t} \begin{bmatrix} 1 & -t \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -t \end{bmatrix}^n \begin{bmatrix} 1 & t \\ -1 & 1 \end{bmatrix} \\ &= \frac{1}{1+t} \begin{bmatrix} 1 & -t \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (-t)^n \end{bmatrix} \begin{bmatrix} 1 & t \\ -1 & 1 \end{bmatrix} \\ &= \frac{1}{1+t} \begin{bmatrix} 1 & (-t)^{n+1} \\ 1 & (-t)^n \end{bmatrix} \begin{bmatrix} 1 & t \\ -1 & 1 \end{bmatrix} \\ &= \frac{1}{1+t} \begin{bmatrix} 1-(-t)^{n+1} & t+(-t)^{n+1} \\ 1-(-t)^n & t+(-t)^n \end{bmatrix}. \end{aligned}$$

Daí, temos que

$$\Delta_{K_b}(t) = \det[\varphi_2(\sigma_1)^n - I_2]_{1,1} = \frac{1}{1+t}[t+(-t)^n] - 1$$

$$
\begin{aligned}
&= \frac{-1+(-t)^n}{1+t} \\
&= -\frac{1-(-t)^n}{1+t} \\
&= -\sum_{i=1}^{n}(-t)^{i-1} \\
&= -(1-t+t^2-\cdots+(-1)^{n-1}t^{n-1}) \\
&\doteq 1-t+t^2-\cdots+(-1)^{n-1}t^{n-1}.
\end{aligned}
$$

Em particular, para $n=3$ temos o nó de trevo (veja Figura 4.10) e o polinômio de Alexander $\Delta_{K_b} = 1-t+t^2 \underset{\times(t^{-1})}{\doteq} t-1+t^{-1}$.

Outro exemplo interessante é o nó toral $K_{a,b}$, cujo polinômio de Alexander é

$$\Delta_{K_{a,b}} = \frac{(1-t^{ab})(1-t)}{(1-t^a)(1-t^b)}.$$

Usando a representação de Burau $\varphi_n : B_n \to M(n, \mathbb{Z}[t,t^{-1}])$, podemos definir outras funções. Por exemplo, podemos definir $\overline{\varphi}_n : B_n \to M(n-1, \mathbb{Z}[t,t^{-1}])$ dada por

$$\overline{\varphi}_n(\beta) = \Lambda(t),$$

sendo $\Lambda(t)$ a matriz definida logo antes do Lema 4.4.3. Daí, afirmamos o seguinte.

Proposição 4.4.2 A função $\overline{\varphi}_n$ é um homomorfismo. ∎

Demonstração. Primeiro, note que se $|i-j| \geq 2$, temos

$$
\begin{aligned}
(S^{-1}\varphi_n(\sigma_i)S)(S^{-1}\varphi_n(\sigma_j)S) &= S^{-1}\varphi_n(\sigma_i)\varphi_n(\sigma_j)S \\
&= S^{-1}\varphi_n(\sigma_j)\varphi_n(\sigma_i)S \\
&= (S^{-1}\varphi_n(\sigma_j)S)(S^{-1}\varphi_n(\sigma_i)S)
\end{aligned}
$$

Isso implica que

$$
\begin{aligned}
\left[\begin{array}{c|c} \Lambda(\sigma_i)\Lambda(\sigma_j) & \\ \hline *\cdots* & 1 \end{array}\right] &= \left[\begin{array}{c|c} \Lambda(\sigma_i) & \\ \hline *\cdots* & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_j) & \\ \hline *\cdots* & 1 \end{array}\right] \\
&= \left[\begin{array}{c|c} \Lambda(\sigma_j) & \\ \hline *\cdots* & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_i) & \\ \hline *\cdots* & 1 \end{array}\right] \\
&= \left[\begin{array}{c|c} \Lambda(\sigma_j)\Lambda(\sigma_i) & \\ \hline *\cdots* & 1 \end{array}\right],
\end{aligned}
$$

ou seja, $\overline{\varphi}_n(\sigma_i)\overline{\varphi}_n(\sigma_j) = \overline{\varphi}_n(\sigma_j)\overline{\varphi}_n(\sigma_i)$ para $|i-j| \geq 2$.

De modo similar, vamos mostrar que $\overline{\varphi}_n(\sigma_i)\overline{\varphi}_n(\sigma_{i+1})\overline{\varphi}_n(\sigma_i) = \overline{\varphi}_n(\sigma_{i+1})\overline{\varphi}_n(\sigma_i)\overline{\varphi}_n(\sigma_{i+1})$, ou seja, que $\Lambda(\sigma_i)\Lambda(\sigma_{i+1})\Lambda(\sigma_i) = \Lambda(\sigma_{i+1})\Lambda(\sigma_i)\Lambda(\sigma_{i+1})$. Para isso, basta considerar o caso para $n = 3$ pelo mesmo motivo que o fizemos na demonstração da Proposição 4.4.1. Note que

$$(S^{-1}\varphi_3(\sigma_1)S)(S^{-1}\varphi_3(\sigma_2)S)(S^{-1}\varphi_3(\sigma_1)S) = (S^{-1}\varphi_3(\sigma_2)S)(S^{-1}\varphi_3(\sigma_1)S)(S^{-1}\varphi_3(\sigma_2)S).$$

Isso implica que

$$\begin{aligned}\left[\begin{array}{c|c} \Lambda(\sigma_1)\Lambda(\sigma_2)\Lambda(\sigma_1) & \\ \hline * \cdots * & 1 \end{array}\right] &= \left[\begin{array}{c|c} \Lambda(\sigma_1) & \\ \hline * \cdots * & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_2) & \\ \hline * \cdots * & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_1) & \\ \hline * \cdots * & 1 \end{array}\right] \\ &= \left[\begin{array}{c|c} \Lambda(\sigma_2) & \\ \hline * \cdots * & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_1) & \\ \hline * \cdots * & 1 \end{array}\right]\left[\begin{array}{c|c} \Lambda(\sigma_2) & \\ \hline * \cdots * & 1 \end{array}\right] \\ &= \left[\begin{array}{c|c} \Lambda(\sigma_2)\Lambda(\sigma_1)\Lambda(\sigma_2) & \\ \hline * \cdots * & 1 \end{array}\right],\end{aligned}$$

como queríamos mostrar. Portanto, $\overline{\varphi}_n$ de fato é homomorfismo. ■

Também é possível mostrar que para quaisquer $\beta, \gamma \in B_n$, valem as igualdades:

1. $\overline{\varphi}_n(\gamma\beta\gamma^{-1}) = \overline{\varphi}_n(\beta)$
2. $\overline{\varphi}_{n+1}(\beta\sigma_n)(1 + t + \cdots + t^{n-1}) = \overline{\varphi}_n(\beta)(1 + t + \cdots + t^n)$

Desse modo, vamos definir, para uma trança $\beta \in B_n$ arbitrária,

$$\lambda(\beta) = \frac{\overline{\varphi}_n(\beta)}{1 + t + \cdots + t^{n-1}}.$$

Então, $\lambda(\beta)$ é um invariante do fecho de β, ou seja, se os fechos de $\beta_1 \in B_n$ e $\beta_2 \in B_m$ representam o mesmo nó K, então

$$\frac{\overline{\varphi}_n(\beta_1)}{1 + t + \cdots + t^{n-1}} = \frac{\overline{\varphi}_m(\beta_2)}{1 + t + \cdots + t^{m-1}}$$

Pode ser mostrado que, na verdade, $\overline{\varphi}_n(\beta)$ é o polinômio de Alexander de $\widetilde{\beta}$.

Podemos definir também $\varphi_n^* : B_n \to M(n, \mathbb{Z}[t, t^{-1}])$ por

$$\varphi_n^*(\sigma_{i_1}^{\varepsilon_1}\sigma_{i_2}^{\varepsilon_2}\cdots\sigma_{i_k}^{\varepsilon_k}) = \varphi_n(\sigma_{i_1}^{\varepsilon_1})^T\varphi_n(\sigma_{i_2}^{\varepsilon_2})^T\cdots\varphi_n(\sigma_{i_k}^{\varepsilon_k})^T.$$

De fato, φ_n^* também é homomorfismo: a demonstração é praticamente idêntica à demonstração da Proposição 4.4.1, com a pequena diferença de que

$$\varphi_n^*(\sigma_i) = \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 1-t & 1 & \\ & t & 0 & \\ \hline & & & I_{n-i-1} \end{array}\right] \tag{4.7}$$

é a matriz com a qual devemos nos preocupar. Visto que a demonstração é virtualmente idêntica, não a faremos aqui. Ao leitor interessado, basta aplicar os mesmo passos da demonstração da Proposição 4.4.1 à matriz em (4.7).

Além disso, é possível mostrar que

$$\det[\varphi_n^*(\beta) - I_n]_{1,1} \doteq \det[\varphi_n(\beta) - I_n]_{1,1},$$

logo

$$\Delta_{\widetilde{\beta}}(t) \doteq \det[\varphi_n^*(\beta) - I_n]_{1,1},$$

isto é, usar $\varphi_n^*(\beta)$ ao invés de $\varphi_n(\beta)$ preserva o polinômio de Alexander a menos de um fator de $\pm t^k$.

Por fim, antes de passarmos ao polinômio de Jones, seja $\beta \in B_n$ e defina um novo polinômio $\nabla_{\widetilde{\beta}}(t)$ na incógnita $\sqrt{t}$ da seguinte forma

$$\nabla_{\widetilde{\beta}}(t) = (-1)^{n-1} t^{-\frac{1}{2}(l(\beta)-n+1)} \det[\varphi_n(\beta) - I_n]_{1,1}.$$

É possível mostrar que $\nabla_{\widetilde{\beta}}(t)$ é um invariante de nó. Além disso, se tomarmos $\sigma_p \in B_n$ e, por convenção, fizermos $(\sqrt{t})^2 = t$, então ∇ satisfaz

$$\nabla_{\widetilde{\beta\sigma_p}}(t) - \nabla_{\widetilde{\beta\sigma_p^{-1}}}(t) = \left(\frac{1}{\sqrt{t}} - \sqrt{t}\right) \nabla_{\widetilde{\beta}}(t). \tag{4.8}$$

O invariante $\nabla_{\widetilde{\beta}}(t)$ é chamado *polinômio de Alexander-Conway* de $\widetilde{\beta}$, uma vez que foi J.H. Conway quem, por meio de sua (re)descoberta de (4.8) em 1969, evidenciou essa maneira eficiente de determinar um invariante de um nó (ou *link*). O próprio J.W. Alexander vários anos antes já havia mencionado uma fórmula similar. Como $\Delta_{\widetilde{\beta}}(t) \doteq \nabla_{\widetilde{\beta}}(t)$ (claramente por um fator de $(-1)^{n-1}t^{-\frac{1}{2}(l(\beta)-n+1)}$), podemos pensar em $\nabla_{\widetilde{\beta}}(t)$ como uma reinterpretação do polinômio de Alexander.

Agora, vamos tratar do polinômio de Jones.

Em 1984, Vaughan Frederick Randal Jones definiu um novo invariante, hoje nomeado em sua homenagem, o *polinômio de Jones*, denotado por $V_{\widetilde{\beta}}(t)$, para o fecho da trança β. Assim como o polinômio de Alexander, $V_{\widetilde{\beta}}(t)$ é independente da escolha de β no sentido de que se $\widetilde{\beta}_1 = \widetilde{\beta}_2$, temos $V_{\widetilde{\beta}_1}(t) = V_{\widetilde{\beta}_2}(t)$. Antes de definir o invariante de Jones, precisamos de alguns fatos e definições preliminares.

Definição 4.4.1 — Produto tensorial. Sejam $A = (a_{ij})$ e $B = (a_{kl})$ duas matrizes $p \times q$ e $r \times s$, respectivamente. Então, o produto tensorial de A e B, denotado por $A \otimes B$, é a matriz $pr \times qs$ definida por

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1q}B \\ a_{21}B & a_{22}B & \cdots & a_{2q}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1}B & a_{p2}B & \cdots & a_{pq}B \end{bmatrix}.$$

■ **Exemplo 4.4.1** Se

$$A = \begin{bmatrix} a_{11} & a_{12} \end{bmatrix} \text{ e } B = \begin{bmatrix} b_{11} \\ b_{21} \end{bmatrix}$$

então

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{12}b_{11} \\ a_{11}b_{21} & a_{12}b_{21} \end{bmatrix}.$$

■

Da definição de produto tensorial, segue que

$$(A \otimes B) \otimes C = A \otimes (B \otimes C). \tag{4.9}$$

Além disso, note também que se A e C são duas matrizes de ordem k e B e D são duas matrizes de ordem l, então

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD). \tag{4.10}$$

De fato, da definição de produto de matrizes, temos que as entradas de $(A \otimes B)(C \otimes D)$ são da forma

$$(A \otimes B)(C \otimes D) = \left(\sum_{j=1}^{k} a_{ij}Bc_{js}D \right) = \left(\sum_{j=1}^{k} a_{ij}c_{js}BD \right) = AC \otimes BD$$

Agora, dada uma matriz quadrada $M = (a_{ij})$ de ordem n, definimos o *traço* de M, denotado por $\operatorname{tr}(M)$, como

$$\operatorname{tr}(M) = \sum_{i=1}^{n} a_{ii},$$

ou seja, a soma dos elementos da diagonal principal. O traço de M também pode ser definido em termos do polinômio característico de M. Se $\mu_M(\lambda) = \det(M - \lambda I_n)$ é o polinômio característico de M, então $(-1)^{n-1} \operatorname{tr}(M)$ é igual ao coeficiente de λ^{n-1} em $\mu_M(\lambda)$.

Essa reinterpretação pode ser usada como base para a demonstração do seguinte teorema:

Teorema 4.4.2 Sejam P uma matriz não singular de ordem n e M uma matriz de ordem n. Então,

$$\operatorname{tr}(M) = \operatorname{tr}(PMP^{-1})$$

e, consequentemente,

$$\operatorname{tr}(MP) = \operatorname{tr}(PM).$$

Demonstração. Para o primeiro item, usaremos o fato mencionado anteriormente sobre o coeficiente de λ^{n-1} em $\mu_M(\lambda)$. Note que

$$\begin{aligned}
\det(PMP^{-1} - \lambda I_n) &= \det[PMP^{-1} - \lambda PP^{-1}] \\
&= \det[(PM - \lambda P)P^{-1}] \\
&= \det[(PM - P\lambda)P^{-1}] \\
&= \det[P(M - I_n\lambda)P^{-1}] \\
&= \det[P(M - \lambda I_n)P^{-1}] \\
&= \det(M - \lambda I_n).
\end{aligned}$$

Portanto, M e PMP^{-1} têm o mesmo polinômio característico e, consequentemente, segue que $(-1)^{n-1}\operatorname{tr}(M) = (-1)^{n-1}\operatorname{tr}(PMP^{-1})$, ou seja, $\operatorname{tr}(M) = \operatorname{tr}(PMP^{-1})$.

Para o segundo item, faremos uma demonstração mais simples e direta. Sejam $P = (a_{ij})$ e $M = (b_{kl})$ duas matrizes de ordem n, com P não singular. Então, temos que

$$\operatorname{tr}(PM) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji} = \sum_{j=1}^{n}\sum_{i=1}^{n} b_{ji}a_{ij} = \operatorname{tr}(MP).$$

Uma demonstração alternativa seria notar que

$$\begin{aligned}
\det(MP - \lambda I_n) &= \det(MP - \lambda P^{-1}P) \\
&= \det[(M - \lambda P^{-1})P] \\
&= \det[(P^{-1}PM - P{-}1\lambda)P] \\
&= \det[P^{-1}(PM - \lambda I_n)P] \\
&= \det(PM - \lambda I_n).
\end{aligned}$$

Portanto, MP e PM têm o mesmo polinômio característico e, consequentemente, segue que $(-1)^{n-1}\operatorname{tr}(MP) = (-1)^{n-1}\operatorname{tr}(PM)$, ou seja, $\operatorname{tr}(MP) = \operatorname{tr}(PM)$. ■

■ **Exemplo 4.4.2** Por exemplo, seja

$$\mu = \begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix}. \tag{4.11}$$

Denotando $\underbrace{\mu \otimes \mu \otimes \cdots \otimes \mu}_{n}$ por $\mu^{\otimes n}$, então $\mu^{\otimes n}$ é uma matriz $2^n \times 2^n$ e

$$\operatorname{tr}(\mu^{\otimes n}) = (1+t)^n. \tag{4.12}$$

Para perceber esse fato podemos desenvolver $\mu^{\otimes n}$ para alguns valores de n ou então usar o fato de que $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$, que pode ser verificado diretamente da definição de produto tensorial. De fato, tomando A e B matrizes de ordem n, temos

$$\operatorname{tr}(A \otimes B) = a_{11}\operatorname{tr}(B) + a_{22}\operatorname{tr}(B) + \cdots + a_{nn}\operatorname{tr}(B) = \operatorname{tr}(A)\operatorname{tr}(B)$$

pois, devido à definição de produto tensorial, cada entrada da diagonal de $A \otimes B$ tem a forma $a_{ii}B$, $1 \leq i \leq n$. Consequentemente, o traço de $A \otimes B$ tem a forma

$$\sum_{i=1}^{n} a_{ii}(b_{11} + b_{22} + \cdots + b_{nn}) = \operatorname{tr}(B)\sum_{i=1}^{n} a_{ii} = \operatorname{tr}(A)\operatorname{tr}(B).$$

∎

Para que possamos definir o invariante de Jones, precisamos primeiro definir uma nova função $\Phi_n : B_n \to M(2^n, \mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}])$, baseada na matriz R dada abaixo e em seu inverso. Note que Φ_n associa uma trança a uma matriz de ordem 2^n sobre o módulo $\mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}]$.

Note também que Φ_n é similar à representação de Burau: ela também é uma função que associa uma trança a uma matriz de ordem 2^n. Contudo, aqui o módulo é $\mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}]$ ao invés de $\mathbb{Z}[t, t^{-1}]$. Além disso, como veremos a seguir, Φ_n também é definida, em um certo sentido, sobre os geradores σ_i do grupo de tranças.

Então, sejam

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{t} & 0 \\ 0 & -\sqrt{t} & 1-t & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ e } R^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-\frac{1}{t} & -\frac{1}{\sqrt{t}} & 0 \\ 0 & -\frac{1}{\sqrt{t}} & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Como antes, usamos a convenção de que $(\sqrt{t})^2 = t$.

Para um i arbitrário, definimos $\Phi_n(\sigma_i^{\varepsilon})$ como a seguinte matriz de ordem 2^n:

$$\Phi_n(\sigma_i^{\varepsilon}) = \underbrace{I_2 \otimes \cdots \otimes I_2}_{i-1} \otimes R^{\varepsilon} \otimes \underbrace{I_2 \otimes \cdots \otimes I_2}_{n-i-1} = I_2^{\otimes i-1} \otimes R^{\varepsilon} \otimes I_2^{n-i-1}, \tag{4.13}$$

sendo $\varepsilon = \pm 1$ e I_2 a matriz identidade de ordem 2. Note que de fato $\Phi_n(\sigma_i^{\varepsilon})$ tem ordem $2^{i-1} \cdot 4 \cdot 2^{n-i-1} = 2^n$.

De (4.13) podemos definir

$$\Phi_n(\beta) = \Phi_n(\sigma_{i_1}^{\varepsilon_1}) \cdots \Phi_n(\sigma_{i_k}^{\varepsilon_k}) \in M(2^n, \mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}]) \tag{4.14}$$

para $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$, com $1 \leq i_1, \ldots, i_k \leq n-1$ e $\varepsilon_j = \pm 1$.

A função

$$\xi(\beta) = \frac{t^{\nu}\,\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t},$$

sendo $\nu = \frac{1}{2}\big(l(\beta) - n + 1\big)$, é o invariante de Jones. Essa afirmação será propriamente demonstrada no Teorema 4.4.3, a partir dos dois lemas a seguir.

Lema 4.4.4 A função Φ_n é um homomorfismo de B_n em $M(2^n, \mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}])$.

Demonstração. Precisamos mostrar que

1. $\Phi_n(\sigma_i\sigma_j) = \Phi_n(\sigma_j\sigma_i)$ se $|i-j| \geq 2$;
2. $\Phi_n(\sigma_i\sigma_{i+1}\sigma_i) = \Phi_n(\sigma_{i+1}\sigma_i\sigma_{i+1})$ para $i = 1, 2, \ldots, n-2$.

Vamos começar com 1. Sem perda de generalidade, podemos supor $j > i+1$. Então, de (4.9) e (4.10) tomando $I = I_2$, temos

$$\begin{aligned}
\Phi_n(\sigma_i\sigma_j) &= \Phi_n(\sigma_i)\Phi_n(\sigma_j) \\
&= (I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1})(I^{\otimes j-1} \otimes R \otimes I^{\otimes n-j-1}) \\
&= (I^{\otimes i-1} \otimes R \otimes I^{\otimes j-i-2} \otimes I^{\otimes 2} \otimes I^{\otimes n-j-1}) \times (I^{\otimes i-1} \otimes I^{\otimes 2} \otimes I^{\otimes j-i-2} \otimes R \otimes I^{\otimes n-j-1}) \\
&= [(I^{\otimes i-1} \otimes R \otimes I^{\otimes j-i-2}) \underbrace{\times (I^{\otimes i-1} \otimes I^{\otimes 2} \otimes I^{\otimes j-i-2})}_{I^{\otimes j-1} = I_{2j-1}}] \otimes [\underbrace{(I^{\otimes 2} \otimes I^{\otimes n-j-1})}_{I^{\otimes n-j+1} = I_{2n-j+1}} \times (R \otimes I^{\otimes n-j-1})] \\
&= I^{\otimes i-1} \otimes R \otimes I^{\otimes j-i-2} \otimes R \otimes I^{\otimes n-j-1}.
\end{aligned}$$

De modo similar, obtemos

$$\Phi_n(\sigma_j\sigma_i) = I^{\otimes i-1} \otimes R \otimes I^{\otimes j-i-2} \otimes R \otimes I^{\otimes n-j-1}.$$

Vamos demonstrar 2 agora. Primeiro, note que de (4.9) e (4.10) temos

$$\begin{aligned}
\Phi_n(\sigma_i\sigma_{i+1}\sigma_i) &= (I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1})(I^{\otimes i} \otimes R \otimes I^{\otimes n-i-2})(I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1}) \\
&= (I^{\otimes i-1} \otimes (R \otimes I) \otimes I^{\otimes n-i-2})(I^{\otimes i-1} \otimes (I \otimes R) \otimes I^{\otimes n-i-2})(I^{\otimes i-1} \otimes (R \otimes I) \otimes I^{\otimes n-i-2}) \\
&= I^{\otimes i-1}[(R \otimes I)(I \otimes R)(R \otimes I)]I^{\otimes n-i-2},
\end{aligned}$$

enquanto que

$$\Phi_n(\sigma_{i+1}\sigma_i\sigma_{i+1}) = I^{\otimes i-1}[(I \otimes R)(R \otimes I)(I \otimes R)]I^{\otimes n-i-2}.$$

Portanto, basta mostrar que

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R),$$

o que pode ser verificado por uma computação direta (mas entediante). ■

Lema 4.4.5 Seja $\xi(\beta)$ a função definida acima (e também no Teorema 4.4.3). Então, ela satisfaz as seguintes condições:

1. para quaisquer tranças $\beta, \gamma \in B_n$, $\xi(\gamma\beta\gamma^{-1}) = \xi(\beta)$;
2. para uma trança $\beta \in B_n$ qualquer e para as tranças $\beta\sigma_n^{\pm 1}$, $\xi(\beta) = \xi(\beta\sigma_n) = \xi(\beta\sigma_n^{-1})$.

Demonstração. Vamos mostrar o item 1. Podemos escrever $\beta \in B_n$ como $\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k}$. Então,

$$\Phi_n(\beta) = R_{i_1}^{\varepsilon_1} \cdots R_{i_k}^{\varepsilon_k},$$

sendo

$$R_{i_j}^{\varepsilon_j} = \underbrace{I \otimes \cdots \otimes I}_{i_j - 1} \otimes R^{\varepsilon_j} \otimes \underbrace{I \otimes \cdots \otimes I}_{n - i_j - 1}.$$

Para qualquer trança $\beta \in B_n$, temos

$$\Phi_n(\beta)\mu^{\otimes n} = \mu^{\otimes n}\Phi_n(\beta).$$

Para ver isso, note que basta mostrarmos que

$$R^{\varepsilon}\mu^{\otimes 2} = \mu^{\otimes 2}R^{\varepsilon}, \tag{4.15}$$

sendo $\varepsilon = \pm 1$, devido ao fato de que se R^{ε} comuta com $\mu^{\otimes 2}$, então ele também comuta com $\mu^{\otimes n}$, pois $\mu^{\otimes n}$ é formada por blocos de $\mu^{\otimes 2}$ multiplicados por fatores t^k. Calculando, temos

$$\begin{aligned} R\mu^{\otimes 2} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{t} & 0 \\ 0 & -\sqrt{t} & 1-t & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & t & & \\ & & t & \\ & & & t^2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -t\sqrt{t} & 0 \\ 0 & -t\sqrt{t} & (1-t)t & 0 \\ 0 & 0 & 0 & t^2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & & & \\ & t & & \\ & & t & \\ & & & t^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{t} & 0 \\ 0 & -\sqrt{t} & 1-t & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mu^{\otimes 2}R \end{aligned}$$

e também

$$R^{-1}\mu^{\otimes 2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-\frac{1}{t} & -\frac{1}{\sqrt{t}} & 0 \\ 0 & -\frac{1}{\sqrt{t}} & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & t & & \\ & & t & \\ & & & t^2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & t-1 & -\frac{t}{\sqrt{t}} & 0 \\ 0 & -\frac{t}{\sqrt{t}} & 0 & 0 \\ 0 & 0 & 0 & t^2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & & & \\ & t & & \\ & & t & \\ & & & t^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-\frac{1}{t} & -\frac{1}{\sqrt{t}} & 0 \\ 0 & -\frac{1}{\sqrt{t}} & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mu^{\otimes 2} R^{-1}.$$

Daí, sendo $\beta, \gamma \in B_n$ arbitrárias, temos

$$\begin{aligned} \Phi_n(\gamma\beta\gamma^{-1})\mu^{\otimes n} &= \Phi_n(\gamma)\Phi_n(\beta)\Phi_n(\gamma^{-1})\mu^{\otimes n} \\ &= \Phi_n(\gamma)(\Phi_n(\beta)\mu^{\otimes n})\Phi_n(\gamma^{-1}). \end{aligned}$$

Logo, como Φ_n é homomorfismo e pelo Teorema 4.4.2, obtemos

$$\begin{aligned} \mathrm{tr}(\Phi_n(\gamma\beta\gamma^{-1})\mu^{\otimes n}) &= \mathrm{tr}(\Phi_n(\gamma)(\Phi_n(\beta)\mu^{\otimes n})\Phi_n^{-1}(\gamma)) \\ &= \mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n}). \end{aligned}$$

Como $l(\gamma\beta\gamma^{-1}) = l(\beta)$, segue que

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

e concluímos a demonstração de 1. Agora, 2.

Suponha $\beta \in B_n$. Então, $\Phi_n(\beta) = M \in M(2^n, \mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}])$. Precisamos computar a matriz $\Phi_{n+1}(\beta\sigma_n)$, de ordem 2^{n+1}. De (4.14), temos

$$\Phi_{n+1}(\beta\sigma_n) = \Phi_{n+1}(\beta)\Phi_{n+1}(\sigma_n).$$

Além disso, de (4.13), temos

$$\Phi_{n+1}(\beta) = \Phi_n(\beta) \otimes I \text{ e } \Phi_{n+1}(\sigma_n) = I^{\otimes n-1} \otimes R.$$

Se fizermos $\Phi_n(\beta) = M = ||a_{ij}||$, então

$$\Phi_{n+1}(\beta\sigma_n)\mu^{\otimes n+1} = (M \otimes I)(I^{\otimes n-1} \otimes R)(\underbrace{\mu \otimes \cdots \otimes \mu}_{n+1}),$$

enquanto que

$$\Phi_n(\beta)\mu^{\otimes n} = M(\underbrace{\mu \otimes \cdots \otimes \mu}_{n}).$$

Agora, se escrevermos

$$\mu^{\otimes n} = \begin{bmatrix} b_1 & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_{2^n} \end{bmatrix},$$

então

$$\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n}) = \sum_{i=1}^{2^n} a_{ii}b_i,$$

sendo os b_i da forma

$$b_1 = 1, b_2 = t$$

$$\text{para } p \geq 1, b_i = tb_p \text{ se } i = 2p \text{ e } b_i = b_p \text{ se } i = 2p-1.$$

Isso pode ser verificado por indução em n. De fato, devido à definição de μ é imediato que $b_1 = 1$ e $b_2 = t$. Suponha, então, que essa forma é válida para $p = 2^{n-1}$, ou seja, para $\mu^{\otimes n-1}$. Assim, segue da definição de produto tensorial que para $\mu^{\otimes n}$ a mesma forma se manterá.

Como consequência imediata segue o fato de que se $i = 2^k q$, com $q = 2r-1$, então $b_i = t^k b_q$. Em particular, $b_{2^k} = t^k$.

Como $\mu^{\otimes n+1}$ é uma matriz diagonal, para calcularmos $\mathrm{tr}((\Phi_{n+1}(\beta\sigma_n))\mu^{\otimes n+1})$ basta conhecer as entradas da diagonal de $\Phi_{n+1}(\beta\sigma_n)$, ou seja, as entradas da diagonal de $(M \otimes I)(I^{\otimes n-1} \otimes R)$.

Sabemos que $I^{\otimes n-1} \otimes R$ é uma matriz diagonal de ordem 2^{n+1} da forma

$$I^{\otimes n-1} \otimes R = \left.\begin{bmatrix} R & & & \\ & R & & \\ & & \ddots & \\ & & & R \end{bmatrix}\right\} 2^{n-1} \text{ blocos.}$$

Portanto, cada uma das entradas da diagonal de $\Phi_{n+1}(\beta\sigma_n)$ vêm do produto

$$\left(\begin{bmatrix} a_{2i-1,2i-1} & a_{2i-1,2i} \\ a_{2i,2i-1} & a_{2i,2i} \end{bmatrix} \otimes I\right) R$$

que, ignorando todas as entradas fora da diagonal, pode ser expandido como

$$\begin{bmatrix} a_{2i-1,2i-1} & & & \\ & 0 & & \\ & & a_{2i,2i}(1-t) & \\ & & & a_{2i,2i} \end{bmatrix}.$$

Usando a forma dos b_i encontrada anteriormente, encontramos

$$\begin{aligned}
\mathrm{tr}((\Phi_{n+1}(\beta\sigma_n))\mu^{\otimes n+1}) &= \sum_{i=1}^{2^{n-1}} \{a_{2i-1,2i-1}b_{4i-3} + a_{2i,2i}(1-t)b_{4i-1} + a_{2i,2i}b_{4i}\} \\
&= \sum_{i=1}^{2^{n-1}} \left\{a_{2i-1,2i-1}b_{2(2i-1)-1} + a_{2i,2i}(1-t)b_{2(2i)-1} + a_{2i,2i}b_{2(2i)}\right\} \\
&= \sum_{i=1}^{2^{n-1}} \{a_{2i-1,2i-1}b_{2i-1} + a_{2i,2i}[(1-t)b_{2i} + tb_{2i}]\}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{2^{n-1}} \{a_{2i-1,2i-1}b_{2i-1} + a_{2i,2i}b_{2i}\} \\
&= \sum_{j=1}^{2^n} a_{jj}b_j \\
&= \mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n}).
\end{aligned}
$$

Uma vez que $l(\beta\sigma_n) = l(\beta) + 1$, segue que

$$\xi(\beta\sigma_n) = \xi(\beta),$$

pois os traços são iguais e o expoente de t em $\xi(\beta\sigma_n)$ é $\frac{1}{2}(l(\beta) + 1 - (n+1) + 1) = \frac{1}{2}(l(\beta) - n + 1)$, que é igual ao expoente de t em $\xi(\beta)$.

De modo similar, para σ_n^{-1} no lugar de σ_n, basta substituirmos R por R^{-1}. Desse modo,

$$\Phi_{n+1}(\beta\sigma_n^{-1})\mu^{\otimes n+1} = (M \otimes I)(I^{\otimes n-1} \otimes R^{-1})\mu^{\otimes n+1}.$$

Como antes, para calcular $\mathrm{tr}((\Phi_{n+1}(\beta\sigma_n^{-1}))\mu^{\otimes n+1})$ é suficiente saber as entradas da diagonal de $\Phi_{n+1}(\beta\sigma_n^{-1})$, ou seja, as entradas da diagonal de $(M \otimes I)(I^{\otimes n-1} \otimes R^{-1})$.

Sabemos que $I^{\otimes n-1} \otimes R^{-1}$ é uma matriz diagonal de ordem 2^{n+1}, podendo ser escrita como

$$I^{\otimes n-1} \otimes R^{-1} = \left.\begin{bmatrix} R^{-1} & & & \\ & R^{-1} & & \\ & & \ddots & \\ & & & R^{-1} \end{bmatrix}\right\} 2^{n-1} \text{ blocos.}$$

Consequentemente, as entradas diagonais de $\Phi_{n+1}(\beta\sigma_n^{-1})$ vêm do produto

$$\left(\begin{bmatrix} a_{2i-1,2i-1} & a_{2i-1,2i} \\ a_{2i,2i-1} & a_{2i,2i} \end{bmatrix} \otimes I\right) R^{-1},$$

que, ignorando as entradas não diagonais, pode ser expandida como

$$\begin{bmatrix} a_{2i-1,2i-1} & & & \\ & a_{2i-1,2i-1}(1-\frac{1}{t}) & & \\ & & 0 & \\ & & & a_{2i,2i} \end{bmatrix}.$$

Daí, usando a forma dos b_i encontrada anteriormente, temos

$$
\begin{aligned}
\mathrm{tr}((\Phi_{n+1}(\beta\sigma_n^{-1}))\mu^{\otimes n+1}) &= \sum_{i=1}^{2^{n-1}} \left\{ a_{2i-1,2i-1}b_{4i-3} + a_{2i-1,2i-1}\left(1 - \frac{1}{t}\right) b_{4i-2} + a_{2i,2i}b_{4i} \right\} \\
&= \sum_{i=1}^{2^{n-1}} \left\{ a_{2i-1,2i-1}b_{2(2i-1)-1} + a_{2i-1,2i-1}\left(1 - \frac{1}{t}\right) b_{2(2i-1)} + a_{2i,2i}b_{2(2i)} \right\}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=1}^{2^{n-1}} \{a_{2i-1,2i-1}[b_{2i-1} + tb_{2i-1} - b_{2i-1}] + a_{2i,2i}tb_{2i}\} \\
&= t\sum_{i=1}^{2^{n-1}} \{a_{2i-1,2i-1}b_{2i-1} + a_{2i,2i}b_{2i}\} \\
&= t\sum_{j=1}^{2^n} a_{jj}b_j \\
&= t\,\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n}).
\end{aligned}
$$

Como $l(\beta\sigma_n^{-1}) = l(\beta) - 1$, temos

$$
\begin{aligned}
\xi(\beta\sigma_n^{-1}) &= \frac{\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t} t \cdot t^{\frac{1}{2}(l(\beta)-1-(n+1)+1)} \\
&= \frac{\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t} t^{\frac{1}{2}(l(\beta)-n+1)} \\
&= \xi(\beta)
\end{aligned}
$$

e finalizamos a demonstração. ■

Agora podemos demonstrar o teorema desejado.

Teorema 4.4.3 — Polinômio de Jones. Com a função Φ_n definida em (4.13) e (4.14) e a matriz μ definida em (4.11), temos que

$$
\xi(\beta) = \frac{t^{\nu}\,\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t}, \tag{4.16}
$$

com $\nu = \frac{1}{2}(l(\beta) - n + 1)$, é um invariante de $\widetilde{\beta}$, independente da escolha de β. Em outras palavras, se $\widetilde{\beta_1} \approx \widetilde{\beta_2}$, para $\beta_1 \in B_n$ e $\beta_2 \in B_m$, então $\xi(\beta_1) = \xi(\beta_2)$. Esse invariante de nó é chamado polinômio de Jones de um nó (ou link) e denotado por $V_{\widetilde{\beta}}(t)$.

Demonstração. Suponha que os fechos de β e β', $\widetilde{\beta}$ e $\widetilde{\beta'}$ respectivamente, são equivalentes. Então, pelo Teorema 4.1.3, $\beta \underset{M}{\sim} \beta'$, i.e., existe uma sequência finita

$$
\beta = \beta_0 \to \beta_1 \to \cdots \to \beta_m = \beta'
$$

tal que β_{i+1} é obtida de β_i, para $i = 0, 1, \ldots, m-1$, aplicando um dos movimentos de Markov $M_1^{\pm 1}$ e $M_2^{\pm 1}$.

Note que se β e β' são tranças equivalentes, então $\beta = \beta'$ como tranças de n cordas e, portanto, $\Phi_n(\beta) = \Phi_n(\beta')$. Como $l(\beta) = l(\beta')$ (pois $l(\beta)$ é um invariante de tranças), segue que $\xi(\beta) = \xi(\beta')$.

Se β_{i+1} é conjugada de β_i, ou seja, se $\beta_i \xrightarrow{M_1} \beta_{i+1}$ ou $\beta_i \xrightarrow{M_1^{-1}} \beta_{i+1}$, então pelo item 1 do Lema 4.4.5 temos $\xi(\beta_i) = \xi(\beta_{i+1})$.

Por outro lado, se $\beta_i \xrightarrow{M_2} \beta_{i+1}$ ou $\beta_i \xrightarrow{M_2^{-1}} \beta_{i+1}$, então pelo item 2 do Lema 4.4.5, temos $\xi(\beta_i) = \xi(\beta_{i+1})$.

Portanto, $\xi(\beta) = \xi(\beta')$, como queríamos mostrar. ■

Para $n = 2$, por exemplo, temos $\Phi_2(\sigma_1) = R$ e $\mathrm{tr}(\Phi_2(\sigma_1)\mu^{\otimes 2}) = \mathrm{tr}(R\mu^{\otimes 2}) = 1+t$ (veja o cálculo de (4.15)). Daí, como $l(\sigma_1) = 1$, temos $V_{\widetilde{\sigma_1}}(t) = \xi(\sigma_1) = \dfrac{t^{\frac{1}{2}(1-2+1)}(1+t)}{1+t} = 1$.

Para $n = 3$ e $\beta = \sigma_1\sigma_2$ em B_3, é trabalhoso, mas não muito difícil, mostrar que

$$\mathrm{tr}(\Phi_3(\sigma_1\sigma_2)\mu^{\otimes 3}) = \mathrm{tr}((R\otimes I)(I\otimes R)\mu^{\otimes 3}) = 1+t.$$

De fato, temos

$$\begin{aligned}
\Phi_3(\sigma_1\sigma_2) &= (R\otimes I)(I\otimes R)\\
&= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&-\sqrt{t}&0&0&0\\ 0&0&0&0&0&-\sqrt{t}&0&0\\ 0&0&-\sqrt{t}&0&1-t&0&0&0\\ 0&0&0&-\sqrt{t}&0&1-t&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&-\sqrt{t}&0&0&0&0&0\\ 0&-\sqrt{t}&1-t&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&-\sqrt{t}&0\\ 0&0&0&0&0&-\sqrt{t}&1-t&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}\\
&= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&-\sqrt{t}&0&0&0&0&0\\ 0&0&0&0&-\sqrt{t}&0&0&0\\ 0&0&0&0&0&-\sqrt{t}&0&0\\ 0&t&0&0&1-t&0&0&0\\ 0&0&0&-\sqrt{t}&0&0&-\sqrt{t}(1-t)&0\\ 0&0&0&0&0&-\sqrt{t}&1-t&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}.
\end{aligned}$$

Daí, como

$$\mu^{\otimes 3} = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&t&0&0&0&0&0&0\\ 0&0&t&0&0&0&0&0\\ 0&0&0&t^2&0&0&0&0\\ 0&0&0&0&t&0&0&0\\ 0&0&0&0&0&t^2&0&0\\ 0&0&0&0&0&0&t^2&0\\ 0&0&0&0&0&0&0&t^3 \end{bmatrix},$$

segue que

$$\mathrm{tr}((R\otimes I)(I\otimes R)\mu^{\otimes 3}) = 1+0+0+0+t(1-t)+t^2(1-t)+t^3 = 1+t.$$

Como $l(\beta) = 2$, temos

$$V_{\widetilde{\beta}}(t) = \frac{t^{\frac{1}{2}(2-3+1)}(1+t)}{1+t} = 1,$$

o que era esperado, pois σ_1 em B_2 e $\sigma_1\sigma_2$ em B_3 representam o nó trivial.

Se considerarmos a trança trivial $\beta = 1_n \in B_n$, então $\Phi_n(\beta) = I^{\otimes n}$ e, daí, usando (4.12), temos

$$\mathrm{tr}(\Phi_n(\beta)\mu^{\otimes n}) = \mathrm{tr}(\mu^{\otimes n}) = (1+t)^n.$$

Uma vez que $l(\beta) = 0$, segue que

$$V_{\widetilde{\beta}}(t) = \frac{t^{-\frac{n-1}{2}}(1+t)^n}{1+t} = \left(\frac{1}{\sqrt{t}} + \sqrt{t}\right)^{n-1}.$$

Se fizermos $t = 1$, então, como $\sqrt{1}$ é a raiz primitiva da unidade (i.e., $e^{i\pi} = -1$), temos $\sqrt{t} = -1$ e, portanto

$$V_{\widetilde{\beta}}(1) = V_{\widetilde{1_n}}(1) = (-2)^{n-1}. \tag{4.17}$$

Em geral, computar $V_{\widetilde{\beta}}(t)$ para uma trança β arbitrária é algo trabalhoso devido ao fato de que o produto tensorial faz com que a ordem das matrizes cresça muito rapidamente.

■ **Exemplo 4.4.3** Outros exemplos são os polinômios de Jones para o nó figura oito

$$V_{\widetilde{\beta}}(t) = t^2 - t + 1 - t^{-1} + t^{-2}$$

e para os nós torais

$$V_{K_{p,q}}(t) = \frac{1 - t^{p+1} - t^{q+1} + t^{p+q}}{1 - t^2} t^{(p-1)(q-1)/2}.$$

■

Alexander vs Jones

Agora, vamos falar um pouco das diferenças entre os dois invariantes de nós definidos anteriormente, os polinômios de Alexander e Jones.

Uma primeira diferença notável entre os dois polinômios é que, por exemplo, para o *link* $K = \widetilde{\sigma_1\sigma_3}$ em B_4, temos $\Delta_K(t) = 0$ (não é muito trabalhoso calcular). Contudo, vamos provar que $V_K(t) \neq 0$ qualquer que seja o *link* ou nó K. Portanto, devido a essa observação, podemos dizer que nesse aspecto $V_K(t)$ é um invariante "mais forte" que $\Delta_K(t)$.

Começamos com um fato acerca do polinômio de Alexander.

Proposição 4.4.3 Se K é um nó, então $|\Delta_K(1)| = 1$. ■

Demonstração. Seja σ_i um gerador de B_n e defina $\widehat{\varphi}_n$ por

$$\widehat{\varphi}_n(\sigma_i) = \varphi_n(\sigma_i)|_{t=1} = \left[\begin{array}{c|cc|c} I_{i-1} & & & \\ \hline & 0 & 1 & \\ & 1 & 0 & \\ \hline & & & I_{n-i-1} \end{array}\right].$$

Daí, temos $\widehat{\varphi}_n(\sigma_i^2) = I_n$. Portanto, $\widehat{\varphi}_n$ define um homomorfismo de $B_n/\langle\sigma_i^2\rangle$ em $M(n,\mathbb{Z})$. Como $B_n/\langle\sigma_i^2\rangle \cong S_n$, $\widehat{\varphi}_n$ é um homomorfismo de S_n em $M(n,\mathbb{Z})$. Contudo, o isomorfismo $B_n/\langle\sigma_i^2\rangle \cong S_n$ é dado pela permutação $\pi(\beta)$ associada à trança $\beta \in B_n$. Logo, se $\pi(\beta) = \pi(\beta')$ então $\widehat{\varphi}_n(\beta) = \widehat{\varphi}_n(\beta')$, ou seja

$$|\Delta_{\widetilde{\beta}}(1)| = |\Delta_{\widetilde{\beta'}}(1)|. \tag{4.18}$$

Como $\widetilde{\beta}$ é um nó, $\pi(\beta)$ é uma permutação de ordem n. Daí, segue que tomando uma conjugação apropriada de β, temos

$$\pi(\gamma\beta\gamma^{-1}) = (123\cdots n).$$

Então, seja $\beta' = \sigma_{n-1}\sigma_{n-2}\cdots\sigma_2\sigma_1$. Consequentemente, $\pi(\beta') = (123\ldots n)$ e, por (4.18)

$$|\Delta_{\widetilde{\gamma\beta\gamma^{-1}}}(1)| = |\Delta_{\widetilde{\beta'}}(1)|.$$

Mas $\widetilde{\gamma\beta\gamma^{-1}}$ é o mesmo nó que $\widetilde{\beta}$, devido ao movimento de Markov tipo 1, M_1. Fazendo $K = \widetilde{\beta}$ e $K' = \widetilde{\beta'}$, temos

$$|\Delta_K(1)| = |\Delta_{K'}(1)|.$$

Como K' é o nó trivial, segue que $\Delta_{K'}(t) = 1$ e, em particular, que $\Delta_{K'}(1) = 1$. Portanto, para qualquer nó K,

$$|\Delta_K(1)| = |\Delta_{K'}(1)| = 1.$$

■

Note que na Proposição 4.4.3 não escrevemos "ou *link*". De fato, como veremos mais à frente, essa proposição não vale para *links*. Na verdade, o módulo é zero para *links*.

Por outro lado, para o polinômio de Jones temos a seguinte proposição.

Proposição 4.4.4 Se K é um link com r componentes, $r \geq 1$, então $V_K(1) = (-2)^{r-1}$. ■

Demonstração. Primeiro, lembre que tomamos $\sqrt{t}|_{t=1} = -1$, i.e., a raiz primitiva da unidade. Daí, como

$$R|_{t=1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

temos que

$$\begin{aligned}\widehat{\Phi}_n(\sigma_i^2) = \Phi_n(\sigma_i^2)|_{t=1} &= (I^{\otimes i-1} \otimes R|_{t=1} \otimes I^{\otimes n-i-1})(I^{\otimes i-1} \otimes R|_{t=1} \otimes I^{\otimes n-i-1}) \\ &= (I^{\otimes i-1} \cdot I^{\otimes i-1}) \otimes (R|_{t=1} \cdot R|_{t=1}) \otimes (I^{\otimes n-i-1} \cdot I^{\otimes n-i-1}) \\ &= I^{\otimes i-1} \otimes I^{\otimes 2} \otimes I^{\otimes n-i-1} \\ &= I^{\otimes n} = I_{2^n}.\end{aligned}$$

Portanto, $\widehat{\Phi}_n$ induz um homomorfismo de $S_n(\cong B_n/\langle\sigma_i^2\rangle)$ em $M(2^n, \mathbb{Z})$, as matrizes de ordem 2^n sobre $\mathbb{Z}$. Além disso, como

$$\mu|_{t=1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

segue que $(\mu|_{t=1})^{\otimes n} = I_{2^n}$.

Como antes, se $\pi(\beta) = \pi(\beta')$, então $V_{\widetilde{\beta}}(1) = V_{\widetilde{\beta'}}(1)$. Agora, suponha $K = \widetilde{\beta}$ um *link* de r componentes. Daí, $\pi(\beta)$ é um produto de r ciclos mutuamente disjuntos $C_1C_2\cdots C_r$. Tomando uma conjugação apropriada, podemos assumir que

$$\pi(\gamma\beta\gamma^{-1}) = (12\cdots p_1)(p_1+1\cdots p_2)\cdots(p_{r-1}+1\cdots n).$$

Seja $\beta' \in B_n$ dada por

$$\beta' = (\sigma_{p_1-1}\sigma_{p_1-2}\cdots\sigma_1)(\sigma_{p_2-1}\cdots\sigma_{p_1+1})\cdots(\sigma_{n-1}\cdots\sigma_{p_{r-1}+1}).$$

Então $\pi(\gamma\beta\gamma^{-1}) = \pi(\beta')$ e, portanto,

$$V_{\widetilde{\gamma\beta\gamma^{-1}}}(1) = V_{\widetilde{\beta'}}(1).$$

Contudo, $\widetilde{\beta'}$ é o *link* trivial de r componentes. Consequentemente, $\widetilde{\beta'}$ é equivalente a $\widetilde{1_r}$ e obtemos

$$V_K(1) = V_{\widetilde{\beta'}}(1) = V_{\widetilde{1_r}}(1).$$

Usando o resultado encontrado em (4.17), temos

$$V_{\widetilde{1_r}}(1) = (-2)^{r-1}.$$

■

Usando um argumento similar, podemos demonstrar a seguinte proposição.

Proposição 4.4.5 Se K é um link com r componentes, $r \geq 2$, então $\Delta_K(1) = 0$. ■

Demonstração. A demonstração segue as mesmas linhas da demonstração da Proposição 4.4.3, com a mudança de que como agora $\widetilde{\beta}$ é um *link*, então $\pi(\beta)$ é um produto de r ciclos mutuamente disjuntos. Daí, podemos tomar uma conjugação adequada e assumir que

$$\pi(\gamma\beta\gamma^{-1}) = (12\cdots p_1)(p_1+1\cdots p_2)\cdots(p_{r-1}+1\cdots n)$$

e, tomando $\beta' \in B_n$ dada por

$$\beta' = (\sigma_{p_1-1}\sigma_{p_1-2}\cdots\sigma_1)(\sigma_{p_2-1}\cdots\sigma_{p_1+1})\cdots(\sigma_{n-1}\cdots\sigma_{p_{r-1}+1}),$$

obtemos $\pi(\gamma\beta\gamma^{-1}) = \pi(\beta')$ e, daí,

$$|\Delta_{\widetilde{\gamma\beta\gamma^{-1}}}(1)| = |\Delta_{\widetilde{\beta'}}(1)|.$$

Como $\widetilde{\gamma\beta\gamma^{-1}}$ é equivalente a $\widetilde{\beta}$, segue que

$$|\Delta_{\widetilde{\beta}}(1)| = |\Delta_{\widetilde{\beta'}}(1)|.$$

Por fim, como $\Delta_{\widetilde{\beta'}}(t) = 0$, segue que

$$\Delta_K(1) = \Delta_{\widetilde{\beta'}}(1) = 0.$$

■

É sabido que se K é o nó trivial, então $V_K(t) = 1$, mas ainda é uma questão em aberto se $V_K(t) = 1$ **apenas** para o nó trivial. Essa conjectura, em inglês chamada de *Jones unknot conjecture*, ainda está em aberto. Resultados mais recentes (veja [19, 20]) verificaram que para todo nó não trivial com até 24 cruzamentos, o polinômio de Jones não é 1, ou seja, para nós não triviais de até 24 cruzamentos, o polinômio de Jones detecta o nó trivial. Caso a conjectura se mostre verdadeira, será mais uma diferença entre os polinômios de Jones e Alexander.

Por outro lado, existe nó não trivial cujo polinômio de Alexander é igual a 1. Um exemplo é o fecho da trança de 4 cordas $\beta = \sigma_1^3\sigma_3^2\sigma_2\sigma_3^{-1}\sigma_1^{-2}\sigma_2\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}$, usualmente chamado *nó de Kinoshita-Terasaka*.

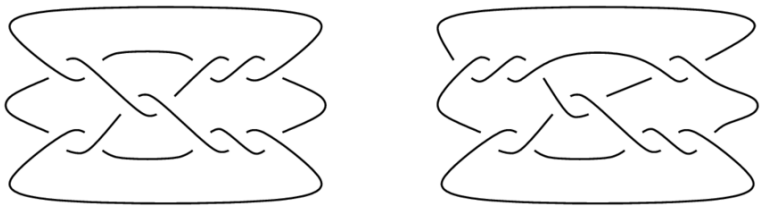


Figura 4.23: O nó de Kinoshita-Terasaka (à esquerda) e o nó de Conway (à direita)

Recentemente, foi mostrado ([18]) que o nó de Conway (um nó descoberto por J.H. Conway meio século atrás), não é *slice*. Essa propriedade, ser *slice*, basicamente significa que esse nó é uma fatia de um nó em dimensão maior. Saber se um dado nó é *slice* é uma das primeiras perguntas feitas a respeito de nós em espaços de dimensões maiores, e para todos os milhares de nós com 12 cruzamentos ou menos essa pergunta já havia sido respondida, com exceção de um nó: o de Conway, com 11 cruzamentos.

A dificuldade de responder se o nó de Conway era *slice* ou não se devia ao fato de que ele é muito parecido com outro nó: o de Kinoshita-Terasaka. De fato, esses nós são ditos **mutantes**, pois é possível obter um do outro a partir de uma **mutação** (uma operação em um nó). Por ser muito parecido com o nó de Kinoshita-Terasaka, o nó de Conway conseguia escapar e evitar todos os invariantes utilizados para detectar nós que não fossem *slice*.

Antes de continuar com as propriedades dos polinômios de Alexander e Jones, seja K um nó (ou *link*) orientado. Se invertermos a orientação de K, obtemos um novo nó $\overline{K}$. Podemos supor que K é o fecho da trança $\beta = \sigma_{i_1}^{\varepsilon_1}\sigma_{i_2}^{\varepsilon_2}\cdots\sigma_{i_k}^{\varepsilon_k}$. Daí, pelo item 2 da Proposição 4.2.2, $\overline{K}$ é o fecho da trança $\overline{\beta} = \sigma_{i_k}^{\varepsilon_k}\sigma_{i_{k-1}}^{\varepsilon_{k-1}}\cdots\sigma_{i_1}^{\varepsilon_1}$.

Proposição 4.4.6 Com os nós K e $\overline{K}$ definidos acima, temos

$$\Delta_{\overline{K}}(t) \doteq \Delta_K(t).$$

■

Demonstração. Considere o homomorfismo $\varphi_n^* : B_n \to M(n, \mathbb{Z}[t, t^{-1}])$ definido anteriormente. Se $\beta = \sigma_{i_1}^{\varepsilon_1}\sigma_{i_2}^{\varepsilon_2}\cdots\sigma_{i_k}^{\varepsilon_k}$, então

$$\varphi_n^*(\overline{\beta}) = \varphi_n(\sigma_{i_k}^{\varepsilon_k})^T\cdots\varphi_n(\sigma_{i_1}^{\varepsilon_1})^T = (\varphi_n(\sigma_{i_1}^{\varepsilon_1})\cdots\varphi_n(\sigma_{i_k}^{\varepsilon_k}))^T = \varphi_n(\beta)^T.$$

Logo,

$$\det[\varphi_n^*(\overline{\beta}) - I_n]_{1,1} = \det[\varphi_n(\beta)^T - I_n]_{1,1} = \det[\varphi_n(\beta) - I_n]_{1,1}.$$

Portanto,

$$\Delta_{\overline{K}}(t) \doteq \Delta_K(t).$$

■

Com isso, concluímos que o polinômio de Alexander não é forte o bastante para detectar se um nó é invertível ou não (i.e., se é igual ao seu inverso), pois mostramos que o polinômio de Alexander é o mesmo para um nó K e seu inverso $\overline{K}$. Além disso, como mostraremos a seguir, o polinômio de Alexander também falha em determinar se um nó é aquiral (i.e., se é igual a sua imagem espelhada) ou não.

Proposição 4.4.7 Sejam K um nó (ou link) orientado e K^* a imagem espelhada de K. Então,

$$\Delta_K(t) \doteq \Delta_{K^*}(t).$$

■

Demonstração. Suponha que K é representado como o fecho de uma trança β de n cordas. Então, o fecho de β^{-1} representa o nó $\overline{K}^*$, que é a imagem espelhada de K com orientação invertida (isso se deve ao item 1 da Proposição 4.2.2). Contudo, pelo Lema 4.4.3, temos

$$\Delta_K(t) \doteq \det[\varphi_n(\beta) - I_n]_{1,1} = \frac{1}{(1+t+\cdots+t^{n-1})}\det(\Lambda(t) - I_{n-1})$$

e

$$\Delta_{\overline{K}^*}(t) \doteq \det[\varphi_n(\beta^{-1}) - I_n]_{1,1} = \frac{1}{(1+t+\cdots+t^{n-1})}\det(\Lambda(t)^{-1} - I_{n-1}).$$

Note que

$$\begin{aligned}\det(\Lambda(t)^{-1} - I_{n-1}) &= \det(\Lambda(t)^{-1})\det(I_{n-1} - \Lambda(t)) \\ &= -\det(\Lambda(t)^{-1})\det(\Lambda(t) - I_{n-1}) \\ &\doteq \det(\Lambda(t)^{-1})(1+t+\cdots+t^{n-1})\Delta_K(t)\end{aligned}$$

e

$$\det(\Lambda(t)^{-1}) = \det(S^{-1}\varphi_n(\beta)^{-1}S) = \det(\varphi_n(\beta)^{-1}) = (-t)^{\alpha},$$

em que a última igualdade segue de (4.2) e sendo $\alpha = l(\beta^{-1})$. Portanto,

$$(1+t+\cdots+t^{n-1})\Delta_{\overline{K}^*}(t) \doteq t^{\alpha}(1+t+\cdots+t^n-1)\Delta_K(t)$$

e, daí,

$$\Delta_{\overline{K}^*}(t) \doteq \Delta_K(t).$$

Como $\overline{K}^*$ é o inverso de K^*, então pela Proposição 4.4.6, temos, finalmente

$$\Delta_{K^*}(t) \doteq \Delta_K(t).$$

■

A implicação das Proposições 4.4.6 e 4.4.7 é que o polinômio de Alexander não é forte o suficiente para detectar ou não se um dado nó é aquiral nem invertível. Por outro lado, para o polinômio de Jones valem resultados similares, mas mais fortes.

Teorema 4.4.4 Seja K um nó (ou link) orientado e sejam $\overline{K}$ e K^* os nós definidos a partir de K nas Proposições 4.4.6 e 4.4.7, respectivamente. Então, valem os itens abaixo.

1. $V_{\overline{K}}(t) = V_K(t)$;
2. $V_{K^*}(t) = V_K(t^{-1})$.

Demonstração.

1. Sabemos, pela Proposição 4.2.2, que se K é o fecho da trança

$$\beta = \sigma_{i_1}^{\varepsilon_1} \cdots \sigma_{i_k}^{\varepsilon_k},$$

então $\overline{K}$ é o fecho da trança

$$\overline{\beta} = \sigma_{i_k}^{\varepsilon_k} \cdots \sigma_{i_1}^{\varepsilon_1}.$$

Ora, então por definição temos $l(\beta) = l(\overline{\beta})$ e, como Φ_n é homomorfismo, $\Phi_n(\overline{\beta}) = \Phi_n(\beta)$. Portanto,

$$V_{\overline{K}}(t) = \frac{t^{\frac{1}{2}(l(\overline{\beta})-n+1)} \operatorname{tr}(\Phi_n(\overline{\beta})\mu^{\otimes n})}{1+t} = \frac{t^{\frac{1}{2}(l(\beta)-n+1)} \operatorname{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t} = V_K(t).$$

2. Também pela Proposição 4.2.2, sabemos que K^* é o fecho da trança

$$\beta^{-1} = \sigma_{i_k}^{-\varepsilon_k} \cdots \sigma_{i_1}^{-\varepsilon_1}.$$

Também sabemos que $l(\beta^{-1}) = -l(\beta)$ e que $\Phi_n(\beta^{-1}) = \Phi_n(\beta)^{-1}$. Portanto,

$$\begin{aligned} V_{K^*}(t) &= \frac{t^{\frac{1}{2}(l(\beta^{-1})-n+1)} \operatorname{tr}(\Phi_n(\beta^{-1})\mu^{\otimes n})}{1+t} \\ &= \frac{t^{\frac{1}{2}(-l(\beta)-n+1)} \operatorname{tr}(\Phi_n(\beta)^{-1}\mu^{\otimes n})}{1+t}. \end{aligned}$$

Neste ponto, eu não consegui prosseguir com as computações. Entretanto, me parece que, argumentando como na prova do Lema 4.4.5, deve ser possível mostrar que

$$\operatorname{tr}(\Phi_n(\beta)^{-1}\mu^{\otimes n}) = t^n \operatorname{tr}(\Phi_n(\beta)\mu^{\otimes n}).$$

Daí, segue que

$$\begin{aligned} V_{K^*}(t) &= \frac{t^{-\frac{1}{2}(l(\beta)-n-1)} \operatorname{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t} \\ &= \frac{(t^{-1})^{\frac{1}{2}(l(\beta)-n+1)} \operatorname{tr}(\Phi_n(\beta)\mu^{\otimes n})}{1+t^{-1}} \\ &= V_K(t^{-1}). \end{aligned}$$

■

Um corolário imediato do Teorema 4.4.4 é o seguinte.

Corolário 4.4.4.1 Todo nó K cujo polinômio de Jones $V_K(t)$ não é *palindrômico* (i.e., simétrico sob a mudança de t por t^{-1}) é *quiral*, ou seja, distinto de sua imagem espelhada.

Portanto, podemos usar o polinômio de Jones para detectar quando um nó (ou *link*) **não** é aquiral. Contudo, o polinômio de Jones não é suficientemente forte para determinar o contrário. De fato, nós quirais para os quais $V_{K^*}(t) = V_K(t)$ foram encontrados. Por exemplo, o fecho da trança de 4 cordas $\beta = \sigma_1^3\sigma_3\sigma_2^{-1}\sigma_3\sigma_1^{-2}\sigma_2^{-1}$ é quiral, mas

$$V_{\widetilde{\beta^{-1}}}(t) = t^{-3} - t^{-2} + t^{-1} - 1 + t - t^2 + t^3 = V_{\widetilde{\beta}}(t).$$

De modo similar ao polinômio de Alexander, se tomarmos um gerador σ_p de B_n e uma trança $\beta \in B_n$, temos

$$\frac{1}{t}V_{\widetilde{\beta\sigma_p}}(t) - tV_{\widetilde{\beta\sigma_p^{-1}}}(t) = \left(\frac{1}{\sqrt{t}} - \sqrt{t}\right) V_{\widetilde{\beta}}(t).$$

4.5 O grupo de Alexander

Um outro invariante de nós é o chamado *grupo de Alexander*, denotado por $A(K)$, K um nó. O grupo de Alexander de um nó é um grupo abeliano definido em termos das regiões de um nó.

Suponha que a projeção de um nó tenha n cruzamentos. Daí, essa projeção tem $n+2$ regiões (contando o "lado de fora" como uma região). Os geradores de $A(K)$ são exatamente essas $n+2$ regiões. Há também n relações, uma para cada cruzamento.

Se as regiões em volta de um cruzamento são a, b, c, d, com a, b de um lado do cruzamento e c, d do outro, a relação correspondente é $a + b = c + d$.

■ **Exemplo 4.5.1** Por exemplo, o nó figura oito abaixo tem grupo de Alexander dado por

$$A(K) = [a, b, c, d, e, f \mid a + b = c + f,\ a + d = b + c,\ a + f = d + e,\ c + d = e + f]$$

que, escrito em forma matricial, se torna

$$\begin{bmatrix} 1 & 1 & -1 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{bmatrix} \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_5.$$

Figura 4.24: Nó figura oito e suas regiões

■

Outro invariante também relacionado às regiões de um nó é o *número de Alexander*. Ele é análogo ao grupo de Alexander, mas agora vamos numerar as regiões ao invés de nomeá-las. Antes de tudo, a notação usada é a seguinte:

$$\begin{array}{c|c} a & b \\ \hline c & d \end{array}$$

As duas linhas representam as duas cordas de um cruzamento e as letras a, b, c, d representam as regiões em volta de tal cruzamento. Assim como antes, devemos ter $a + b = c + d$. Por exemplo, se tivermos

$$\begin{array}{c|c} 3 & 5 \\ \hline 1 & ? \end{array}$$

então devemos ter $? = 7$, uma vez que $5 + 3 = 1 + 7$.

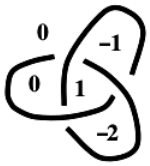
Para começar, começamos colocando 0, 0 e 1 em três regiões em volta de um cruzamento. A região restante será numerada com 1 ou -1, o que for necessário para satisfazer a igualdade.

$$\begin{array}{c|c} 0 & 0 \\ \hline 1 & -1 \end{array} \text{ ou } \begin{array}{c|c} 0 & 1 \\ \hline 0 & 1 \end{array}$$

Na prática, é uma boa ideia começar a numeração com a região de fora e ir preenchendo todas as regiões. Por exemplo, para o nó de trevo

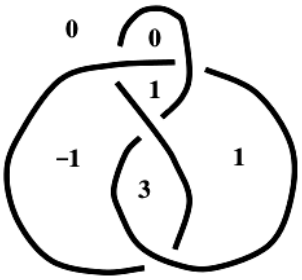
começamos com a região de fora

e balanceamos o cruzamento à direita, da seguinte forma: lembre que toda a região de fora é 0, então de um lado temos $-1+0=-1$. Logo, a última região deve ser -2, uma vez que $-1+0=1+(-2)$. Daí, obtemos a figura abaixo.



Note, contudo, que no cruzamento inferior à esquerda, temos $0+1=-2+0$, i.e., $3=0$. Isso não seria verdade em aritmética ordinária, mas em aritmética modular essa igualdade é verdade para módulo 3. De fato, o número de Alexander é o maior módulo que faz com que o último cruzamento fique balanceado. Nesse caso, é 3. Então, note que se o último cruzamento tem equação $n=0$ para algum n positivo, então n é o nosso número de Alexander.

Para o nó figura oito, temos a figura a seguir.



O último cruzamento (inferior) nos dá $3+1=-1+0$, ou seja, $5=0$. Logo, o número de Alexander para o nó figura oito é 5.

O número de Alexander para o nó de trevo é 3. Logo, o nó de trevo não é equivalente ao nó figura oito, como esperado.

Para ganhar um pouco mais de intuição e certeza de que o número de Alexander é um invariante (não demonstraremos aqui), observe as seguintes figuras.

(a) Ω_1 (b) Ω_2

Figura 4.25: O nó figura oito submetido aos movimentos de Reidemeister 1 e 2

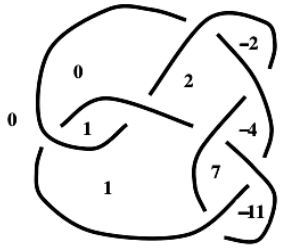
Note que em ambos os diagramas acima o número de Alexander não mudou: tanto para a Figura 4.25a quanto para a Figura 4.25b o último cruzamento continua tendo equação $3+1 = -1+0$, i.e., $5 = 0$, e o número de Alexander continua sendo 5.

O exemplo acima esboça a ideia para se demonstrar que o número de Alexander de fato é um invariante: basta mostrarmos que os movimentos de Reidemeister dos tipos I e II não alteram o número de Alexander.

Um último exemplo que vale a pena mencionar é o preenchimento do seguinte nó

Considere que começamos o preenchimento da seguinte forma

Começando no cruzamento superior, chegamos em um impasse: não há como seguir preenchendo, pois todo cruzamento tem pelo menos duas regiões não preenchidas. Contudo, se começarmos o preenchimento da seguinte forma.



conseguimos finalizá-lo, obtendo, no último cruzamento, $1+7=-11+0$, i.e., $19=0$. Logo, o número de Alexander para esse nó é 19.

Como pudemos perceber, às vezes podemos contornar um impasse sendo um pouco mais espertos. Contudo, esse nem sempre é o caso. Existem nós mais complicados para os quais, independentemente do que façamos, é impossível proceder. Ainda assim, é possível encontrar o número de Alexander, mas são necessárias técnicas mais avançadas.

Capítulo 5

Curiosidades finais

"What is mathematics? It is only a systematic effort of solving puzzles posed by nature."
— Shakuntala Devi

5.1 O problema da palavra em $B_n(\mathbb{R}^2)$ – uma breve introdução

Vamos agora falar mais um pouco sobre o problema da palavra em B_n. Mas o que é o problema da palavra?

De modo geral, suponha que nos seja dado um grupo G com apresentação

$$G = \langle x_1, x_2, \ldots, x_n \mid w_1 = w_2 = \cdots = w_m = 1 \rangle,$$

sendo m e/ou n não necessariamente finitos. Como vimos anteriormente no Capítulo 2, a partir dessa apresentação qualquer elemento g de G pode ser expresso como uma palavra nos geradores x_i de G e seus inversos.

O problema da palavra consiste em encontrar um método (razoavelmente prático) que nos permita decidir se duas palavras arbitrárias g_1 e g_2 em G são iguais ou, equivalentemente, dado um elemento $g(= g_1 g_2^{-1})$, nos permita decidir se $g = 1$, ou seja, trivial.

O problema da palavra é um dos problemas fundamentais em Teoria dos Grupos. Infelizmente, não é garantido que tal método sempre exista. Contudo, se existir, dizemos que o problema da palavra é *solúvel* para G; do contrário, dizemos que o problema da palavra é *insolúvel* para G.

Dissemos que o método deve ser "razoavelmente prático". Bom, isso é algo bem vago e não exatamente uma afirmação matemática. Na verdade, para ser mais preciso, o problema da palavra pertence ao reino da Lógica Matemática ao invés da Teoria dos Grupos. Então, uma

primeira investida na direção de uma solução do problema da palavra é tentar deixar claro, matematicamente, o que é possível quando dizemos "razoavelmente prático". Uma boa maneira de fazer isso é olhar para alguns grupos nos quais o problema da palavra é solúvel.

Teorema 5.1.1 O problema da palavra para um grupo livre é solúvel.

Demonstração. Seja F um grupo livre em n geradores, $x_1, \ldots, x_n$. Um elemento

$$g = x_{i_1}^{\varepsilon_1} \cdots x_{i_m}^{\varepsilon_m}$$

de F é igual à palavra vazia, 1, se e somente se podemos eliminar cada $x_{i_j}^{\varepsilon_j}$ cancelando produtos em g da forma $x_i x_i^{-1}$ ou $x_i^{-1} x_i$. Se não encontrarmos tais cancelamentos, então g nunca é igual à palavra vazia.

Portanto, para resolver o problema da palavra para uma palavra g arbitrária de um grupo livre F, precisamos apenas checar se $x_i x_i^{-1}$ ou $x_i^{-1} x_i$ existe dentro da palavra g. Tal método é bem direto e podemos considerá-lo "razoavelmente prático", e então o problema da palavra é solúvel para um grupo livre. ■

■ **Exemplo 5.1.1** Se tomarmos $F = \langle a, b, c \mid - \rangle$, então as palavras

$$g_1 = aba^{-1}b \qquad \text{e} \qquad g_2 = b^{-1}a^2a^{-1}baa^{-1}b^{-2}a^{-1}$$

não são iguais à identidade, mas $g_1 = g_2^{-1}$, ou seja, $g_1 g_2 = 1$. ■

Para o grupo de tranças, B_n, o problema da palavra consiste em perguntar se, dadas duas tranças β_1 e β_2, existe um método para determinar se $\beta_1 = \beta_2$? Note que podemos modificar essa pergunta e perguntar se existe um método que nos permita dizer se dada uma trança β $(= \beta_1 \beta_2^{-1})$, temos $\beta = 1$. Felizmente, para B_n, tal método existe (e não é único). Um exemplo é a solução que demos ao final da Seção 3.6.

Outro problema interessante é o problema da conjugação: dados dois elementos g_1 e g_2 em G, encontrar um método razoavelmente prático para determinar se g_1 é conjugado de g_2 em G, ou, equivalentemente, determinar se existe um elemento h em G tal que $g_1 = hg_2h^{-1}$. Note que se tomarmos $g_2 = 1$, o problema da conjugação se reduz ao problema da palavra. Claro que o problema da conjugação é mais difícil de se resolver do que o problema da palavra. Para $B_n(\mathbb{R}^2)$, o grupo de tranças usual, o problema da conjugação também é solúvel.

Como vimos anteriormente na Seção 3.4, podemos pensar em tranças em um espaço topológico qualquer X, definindo o grupo $B_n(X)$. Também podemos falar tanto do problema da

palavra quanto do problema da conjugação para $B_n(X)$. Em particular, para $X = \mathbb{S}^2$, i.e., o grupo de tranças esféricas, o problema da palavra também é solúvel, assim como o problema da conjugação.

Apesar disso, sabemos que para muitas classes de grupos o problema da conjugação (e, consequentemente, o problema da palavra) é indecidível, i.e., não é possível construir um algoritmo que sempre responda corretamente sim ou não. Algumas classes de grupos para as quais é sabido que o problema da conjugação (e também o problema da palavra) é solúvel são:

- Grupos livres
- Grupos com uma relação e com torção
- Grupos de tranças
- Grupos de nós
- Grupos abelianos finitamente gerados

entre outras classes. O problema da conjugação também é conhecido como problema da transformação; foi identificado em 1911 por Max Dehn como um dos problemas de decisão fundamentais em Teoria dos Grupos, junto com o problema da palavra e o problema do isomorfismo: dados dois grupos G e H com apresentações finitas, como determinar se $G \cong H$ ou não?

5.2 O *linking number*

Antes de introduzir uma aplicação interessante dos nós e tranças, convém definir o *linking number*, ou número de enlaçamento, de um *link* K, que também é outro invariante de *link*, assim como os polinômios de Jones e Alexander, a função l definida no Lema 3.1.4, o grupo e o número de Alexander.

Então, sejam M e N dois componentes de um *link*, e escolha uma orientação para cada um deles. Então, em cada cruzamento entre os dois componentes, uma das seguintes configurações ocorre.

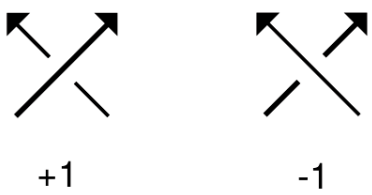


Figura 5.1: Computando o *linking number*

Contamos $+1$ se a seta "por cima" está à direita da seta "por baixo" e -1 se o contrário ocorre. Podemos ainda chamar $+1$ e -1 de cruzamentos destro e canhoto, respectivamente. Às vezes, pode ser um pouco difícil determinar qual o tipo de cruzamento a partir do diagrama. Uma dica é notar que para cruzamentos destros, podemos girar a seta inferior no sentido horário de forma que as duas setas coincidam; analogamente, para cruzamentos canhotos podemos girar a seta inferior no sentido anti-horário de forma que as duas seta coincidam.

Agora, vamos somar os $+1$ e -1 de todos os cruzamentos entre M e N e dividir essa soma por 2. Esse é o *linking number*. Note que nós não levamos em consideração para o cálculo do *linking number* os autocruzamentos dos componentes M e N.

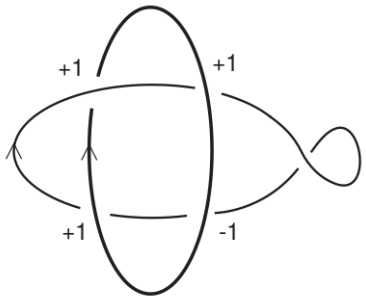


Figura 5.2: *Linking number*$= (1+1+1-1)/2 = 1$

Note, na Figura 5.2, que se revertermos a orientação de apenas um dos dois componentes, o *linking number* será multiplicado por -1. Contudo, se pensarmos no valor absoluto do *linking number* então ele independe da orientação dada aos componentes.

Note que usamos uma projeção particular do *link* para computar o *linking number*. De fato, vamos mostrar que o *linking number* independe da projeção escolhida. Para tal, vamos mostrar que os movimentos de Reidemeister não alteram o *linking number*. Uma vez que podemos sair de uma projeção de um *link* para qualquer outra projeção desse mesmo *link* via uma sequência de movimentos de Reidemeister, então duas projeções do mesmo *link* devem, necessariamente, nos dar o mesmo *linking number*.

Vamos primeiro analisar o efeito de um movimento de Reidemeister tipo I, Ω_1. Da Figura 4.2, vemos que esse movimento apenas introduz autocruzamentos, não afetando, portanto, o *linking number*. Agora os movimentos tipo II e III, Ω_2 e Ω_3. Observe a figura a seguir.

(a) (b)

Figura 5.3: Os movimentos de Reidemeister tipo II e tipo III não alteram o *linking number*

Portanto, os movimentos de Reidemeister de fato não alteram o *linking number*. Daí, podemos dizer que o *linking number* é um invariante de *link* (orientado). Com isso, podemos usá-lo para distinguir *links* (se quisermos distinguir *links* não orientados, basta tomar o módulo do *linking number*).

5.3 Tranças, nós e protetores solares de para-brisa

Você já deve estar familiarizado com aqueles protetores solares de para-brisa, meio arredondados como na Figura 5.4, que lembram um disco e que se dobram de maneira um tanto quanto estranha.

Figura 5.4: O protetor de para-brisa aberto e fechado

Vamos analisar mais de perto a estrutura desse protetor de para-brisa. A parte fundamental do protetor é um arame metálico que percorre todo o perímetro do protetor, formando um loop contínuo. Esse arame é torcionalmente rígido, i.e., podemos dobrá-lo ao longo de seu comprimento sem problemas, mas não podemos torcê-lo. Esse fato servirá de base para a nossa análise.

Esse arame do protetor, quando aberto, tem a forma aproximada de um círculo, sem torções no arame. Quando fechado, esse arame deve ser enrolado em vários círculo/*loops* menores, mas sem que haja torção do arame. Para ser mais preciso, perguntamos o seguinte:

1. Com o protetor na sua posição fechada "normal", quantos *loops* o arame faz, e por quê?

2. De modo mais geral, quais são todas as possíveis posições fechadas para o protetor, em termos de quantos *loops* o arame faz?

Note que a parte de "quantos" da pergunta 1 pode ser respondida através de observações experimentais, dobrando o protetor de fato, mas isso não nos ajuda a responder a parte do "por quê".

Antes de prosseguir, um pouco de terminologia: vamos dizer que o arame é uma fita. Essa fita tem duas arestas, que chamaremos de círculos de fronteira. Vamos também chamar de centro o círculo no meio do caminho entre os círculos de fronteira.

Agora, vamos esclarecer o que significa dizer que quando o protetor está fechado a fita é "enrolada" em vários *loops*.

Informalmente, isso seria como enrolar um pedaço de linha em um carretel e depois juntar as pontas da linha (de forma que o pedaço de linha é ele próprio um *loop*). De fato, isso é exatamente o que temos em mente; contudo, para sermos mais gerais, devemos permitir que essa linha passe por baixo dos *loops* que já estão no carretel, e é aqui que entram as tranças!

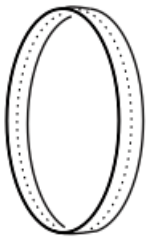


Figura 5.5: O centro da fita (pontilhado) e os círculos de fronteira (curvas sólidas) com o protetor aberto.

A partir da maneira que estamos considerando o protetor e do que dissemos acima, podemos ver que o seguinte é verdade:

Afirmação 1. Com o protetor fechado, o centro da fita é uma trança fechada de um componente, ou seja, um nó.

Então, suponha que nossa trança fechada de um componente foi construída a partir de uma trança de m cordas e com n cruzamentos. Como nossa trança fechada tem apenas um componente, temos que m e n têm paridades diferentes.

Isso se deve ao fato de que a permutação associada à nossa trança fechada deve ter a forma

$$(i_1 i_2 \cdots i_m) = \underbrace{(i_1 i_m)(i_1 i_{m-1}) \cdots (i_1 i_2)}_{m-1 \text{ transposições}},$$

sendo que cada i_j é um elemento distinto do conjunto $\{1, 2, \ldots, m\}$. Consequentemente, como $m - 1 = n$, segue que m e n têm paridades distintas. Daí, sabemos também que o seguinte é verdade:

Afirmação 2. Com o protetor fechado, se a fita é enrolada em m *loops* e o centro da fita tem n cruzamentos, então m e n têm paridades opostas.

Agora vamos considerar os dois círculos de fronteira da fita. Aqui entram os *links* e o *linking number*!

Nessa análise, o que nos interessa é o fato de que o valor absoluto do *linking number* é um invariante topológico.

Com o protetor aberto, o *linking number* dos círculos de fronteira é, claramente, 0. Como esse valor não muda quando dobramos o protetor, o seguinte também é verdade:

Afirmação 3. Com o protetor fechado, o *linking number* dos círculos de fronteira é 0.

Agora, pense no protetor fechado. Como a fita não tem torções, os únicos cruzamentos entre os círculos de fronteira ocorrem próximo dos n autocruzamentos do centro, como na Figura 5.6. O centro da fita já serviu seu próposito; podemos ignorá-lo agora. Agora, no lugar dos n autocruzamentos do centro, vemos 4 novos cruzamentos envolvendo os círculos de fronteira: dois autocruzamentos e dois cruzamentos. Como estamos interessados no *linking number* dos círculos de fronteira, vamos ignorar os autocruzamentos. Então, temos um total de $2n$ cruzamentos, arranjados em n pares, entre os círculos de fronteira.

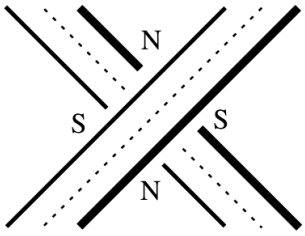


Figura 5.6: A letra S indica os autocruzamentos dos círculos de fronteira e N indica os outros cruzamentos. A linha contínua mais grossa indica um dos círculos de fronteira, enquanto que a linha contínua mais fina indica o outro. A linha pontilhada representa o centro da fita.

Para computar o *linking number*, olhe novamente para a Figura 5.6 e note que para cada círculo de fronteira, seus dois pedaços na figura estarão orientados ambos para cima ou para baixo. Daí, segue que em cada um dos n pares de cruzamentos temos ou dois $+1$ (círculos orientados para cima) ou dois -1 (círculos orientados para baixo). Portanto, cada um desses n pares de cruzamentos contribui com exatamente 1 ou -1 para o *linking number*.

Note que 1 e -1 são ambos ímpares, e se somarmos n números ímpares o resultado tem a mesma paridade de n. Mas, pela Afirmação 3, o *linking number* é 0; logo, n deve ser par. Portanto, pela Afirmação 2, m deve ser ímpar e demonstramos o teorema:

Teorema 5.3.1 Quando fechado, o arame do protetor deve ser enrolado em um número ímpar de *loops*.

De fato, o arame do protetor se enrola em 3 *loops* (respondendo à pergunta 1) não havendo torsões no arame. Para responder à pergunta 2, você pode verificar experimentalmente que mesmo sendo possível forçar o protetor em 2 ou 4 *loops*, isso causará torsões no arame. Contudo, 3 *loops* não é a única configuração possível, como demonstramos: em tese, qualquer número ímpar de *loops* pode ser alcançado.

Referências Bibliográficas

[1] Adams, C. *The Knot Book: An Elementary Introduction to the Mathematical Theory of Knots.* W.H. Freeman and Company, 1994.

[2] Birman, J. S., and Menasco, W. W. Studying links via closed braids. iii. classifying links which are closed 3-braids. *Pacific J. Math. 161*, 1 (1993), 25–113.

[3] Clay, M., and Margalit, D. *Office Hours With a Geometric Group Theorist.* Princeton University Press, 2017.

[4] Coward, A., and Lackenby, M. An upper bound on reidemeister moves. *Amer. J. Math. 136*, 4 (2014), 1023–1066.

[5] Feist, C., and Naimi, R. Topology explains why automobile sunshades fold oddly. *College Math. J. 40*, 2 (2009), 93–98.

[6] Fraleigh, J. *A First Course in Abstract Algebra, 7th edition.* Pearson, 2003.

[7] Gallian, J. *Contemporary Abstract Algebra, 8th edition.* Brooks/Cole, 2013.

[8] González-Meneses, J. Basic results on braid groups. *Ann. Math. Blaise Pascal 18*, 1 (2011), 15–59.

[9] J., H., and Lagarias, J. C. The number of reidemeister moves needed for unknotting. *Amer. Math. Soc. 14*, 1 (2001), 399–428.

[10] Johnson, D. *Presentations of groups, 2nd edition.* Cambridge University Press, 1997.

[11] Joyner, D. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine and Other Mathematical Toys, 2nd edition.* The Johns Hopkins University Press, 2008.

[12] Kassel, C., and Turaev, V. *Braid Groups.* Springer, 2008.

[13] Kurpita, B.; Murasugi, K. *A Study of Braids.* Kluwer Academic Publisher, 1999.

[14] Lackenby, M. A polynomial upper bound on reidemeister moves. *Ann. of Math. (2) 182*, 2 (2015), 491–564.

[15] Linov, L. *An introduction to knot theory an the knot group.* University of Chicago REU, 2014.

[16] Milne, J. S. Group theory (v4.00), 2021. Available at www.jmilne.org/math/.

[17] Moran, S. *The Mathematical Theory of Knots and Braids: An Introduction.* Elsevier Science Publishers B.V., 1983.

[18] Piccirillo, L. The conway knot is not slice. *Annals of Mathematics 18*, 2 (2020), 581–591.

[19] Tuzun, R. E., and Sikora, A. S. Verification of the Jones unknot conjecture up to 22 crossings. *J. Knot Theory Ramifications 27*, 3 (2018), 1840009, 18.

[20] Tuzun, R. E., and Sikora, A. S. Verification of the Jones unknot conjecture up to 24 crossings. *J. Knot Theory Ramifications 30*, 3 (2021), Paper No. 2150020, 6.

[21] Wilson, J. *The geometry and topology of braid groups.* University of Chicago, 2018.

Índice Remissivo

Abelianização, 76
Apresentação, 54
Automorfismo, 21
Automorfismo Interno, 21

Centralizador, 9
Centro, 9
Classe lateral, 24
Complemento de nó, 138
Comutador, 63

Diagrama de van Kampen, 117

Espaços de configuração, 106
Estabilizador, 28

Função ϕ de Euler, 12

Geradores de Artin, 101
Grupo, 5
Grupo de Alexander, 177
Grupo de Dyck, 116
Grupo de permutação, 13
Grupo de Tranças, 89
Grupo de Tranças Puras, 100
Grupo finitamente apresentado, 63
Grupo finitamente gerado, 63
Grupo Fundamental, 109
Grupo fundamental de nó, 138
Grupo livre, 53
Grupo metacíclico, 49
Grupo quociente, 38
Grupo Simétrico, 13

Homomorfismo, 43
Homomorfismo de comprimento, 94
Homomorfismo natural, 47

Isomorfismo, 18

Matrizes de permutação, 60
Movimentos de Markov, 132
Movimentos de Reidemeister, 128

Nó, 127
Núcleo, 43
Número de enlaçamento, 184

Operação binária, 5
Operações elementares de coluna, 66
Operações elementares de linha, 65

Pequeno Teorema de Fermat, 26
Polinômio
    de Alexander, 151
    de Alexander-Conway, 159
    de Jones, 168
Primeiro Teorema dos Isomorfismos, 46
Problema da Conjugação, 184
Problema da Palavra, 182
Problema do Isomorfismo, 184

Produto direto, 29
Produto semidireto, 49
Produto tensorial, 160

Relações, 54
Representação de Burau, 144

Segundo Teorema dos Isomorfismos, 56
Subgrupo, 7
Subgrupo de Sylow, 74
Subgrupo de torção, 77
Subgrupo derivado, 75
Subgrupo normal, 38

Teorema
    de Alexander, 129
    de Cauchy, 40
    de Cayley, 18
    de Classificação dos Grupos de Ordem $2p$, 61
    de Classificação dos Grupos de Ordem p^2, 42
    de Classificação dos Grupos de Ordem 4, 30
    de Classificação dos Grupos de Ordem 8, 57
    de Classificação dos Grupos Diedrais, 59
    de Dyck, 57
    de Lagrange, 25
    de Markov, 132
    de Markov Simplificado, 133
    do Mapeamento Universal, 53
    Fundamental dos Grupos Abelianos Finitamente Apresentados, 68
    Fundamental dos Grupos Abelianos Finitamente Gerados, 70
    Fundamental dos Grupos Cíclicos, 11
    Órbita-Estabilizador, 28
Terceiro Teorema dos Isomorfismos, 56
Transformações de Tietze, 113
Trança, 86
Tranças esféricas, 110

Órbita, 28