UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA E ESTATÍSTICA

JOSE GINALDO DE SOUZA FARIAS

# CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 8$

Campina Grande/PB
2011

JOSE GINALDO DE SOUZA FARIAS

# CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 8$

Trabalho de Conclusão do Curso Licenciatura Plena em Matemática da Universidade Estadual da Paraíba. Em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

Orientador: Dr. Vandemberg Lopes Vieira

Campina Grande/PB
2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

F225c Farias, José Ginaldo de Souza.
Caracterização dos Grupos G com |G|≤8 [manuscrito] / José Ginaldo de Souza Farias. – 2011.
51 f. : il. color

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) – Centro de Ciências Humanas e Exatas, 2011.
"Orientação: Prof. Dr. Vandemberg Lopes Vieira, Departamento de Matemática e Computação".

1. Matemática – Teoria dos Números. 2. Teorema de Lagrange – Aplicação. 3. Álgebra - Teoria dos Grupos. I. Título.

21. ed. CDD 512.7

# CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 8$

Monografia apresentada no Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

**Prof. Dr. Vandenberg Lopes Vieira**
Departamento de Matemática e Computação – CCT/UEPB (10)
Orientador

**Prof. Dr. Juarez Dantas de Souza**
Departamento de Matemática e Computação – CCT/UEPB
Examinador

**Prof. Ms. Ernesto Trajano de Lima Filho**
Departamento de Matemática e Computação – CCT/UEPB
Examinador

Campina Grande, junho de 2011

A toda minha famlia e em especial
aos meus pais por todo o incentivo.
*DEDICO*

# Agradecimentos

A DEUS princípio e razão de tudo e ao meu Senhor e Salvador Jesus Cristo, pois são responsáveis por todas as realizações de minha vida.

Ao meu pai Givaldo, minha mãe Josefa, meu irmão Genaldo e a toda minha família que sempre incentivaram, confiaram em minha capacidade ao enfrentar os desafios.

Ao meu orientador Prof. Vandenberg Lopes Vieira,
pela confiança, orientação, e toda ajuda que me concedeu com o seu conhecimento matemático, sem mencionar a profunda admiração e o respeito que tenho por ele.

Aos professores: Ernesto Trajano e Juarez Dantas que formaram a banca examinadora e me deram ótimas sugestões para o trabalho.

# Resumo

Neste trabalho caracterizamos os grupos finitos de ordem menor ou igual a oito, que são finitamente gerados por dois elementos. Os grupos cíclicos finitos ou infinitos são facilmente classificados por dois grupos clássicos: Os grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$. Para os grupos finitos não-cíclicos, o Teorema de Lagrange surge como ferramenta indispensável para classificá-los. Os grupos $G = \langle a, b \rangle$ considerados apresentam relações importantes entre seus geradores, os quais permitem caracterizá-los por meio de resultados básicos da teoria dos grupos.

**Palavras-chave**: Grupos, Grupos cíclicos, Grupos Finitamente Gerados, Homomorfismo de Grupos.

# Sumário

# Introdução

O conceito de grupo é seguramente uma das idéias centrais da Matemática . A teoria dos grupos tem sua origem no trabalho de Galois (1811-1832). A idéia central da teoria por ele desenvolvida é de considerar as várias maneiras pelas quais é possível permutar as raízes de um polinômio sem alterá-lo. Ao conjunto destas permutações Galois deu nome de *Grupo* da equação. Apesar deste nome ter sido introduzido por Galois, a idéia de grupo já existia em forma latente, tanto no trabalho de Abel quanto no trabalho de Lagrange.A teoria dos grupos logo se difundiu para outros ramos da matemática, entre eles a geometria e a teoria dos números. A enorme gama de aplicações dos grupos levaria os matemáticos a estudá-los por si mesmos, dando lugar à teoria dos grupos.

Neste trabalho pretedemos estudar os grupos finitos gerados por dois elementos, os seja, os grupos da forma $G = \langle a, b\rangle$, em que $ba = a^s b$. Como consequência, estudaremos (classificaremos) os grupos de ordem até oito.

Dados um grupo finito $(G, \cdot)$ e $a \in G$, sabe-se que o subgrupo cíclico $\langle a\rangle$ gerado por $a$ é o menor subgrupo de $G$ que contém o elemento $a$. Agora, para $a, b \in G$, deseja-se determinar o menor subgrupo de $G$ que contenha $a$ e $b$. Ora, qualquer subgrupo contendo $a$ e $b$, deve conter as potências $a^m$ e $b^n$ para todos $n, m \in \mathbb{Z}$,e consequentemente, deve conter todos os produtos finitos dessas potências. O fato é que o conjunto de todos os produtos finitos é um subgrupo de $G$ que, seguramente, é o menor subgrupo $G$ que contém $a$ e $b$. Se este subgrupo for o próprio $G$, então dizemos que o conjunto $\{a, b\}$ gera $G$, que denota-se por $G = \langle a, b\rangle$ . Esse conceito pode ser generalizado da seguinte forma: Sejam $G$ um grupo e $a_i \in G$ para $i \in I$, em que $I$ é um conjunto de índice. O menor subgrupo de $G$ que contém $X = \{a_i : i \in I\}$ é o subgrupo gerado por $X$. Isso de nos conduz naturalmente ao conceito de grupos finitamente gerados.

Os grupos gerados por um elemento, ou seja, os grupos cíclicos, são facilmente classificados através de isomorfismo entre o grupo aditivo dos inteiros $\mathbb{Z}$ ou o grupo aditivo $\mathbb{Z}_n$ das classes de resto módulo $n$. Entretanto, a classificação de grupos gerados por dois elementos pode ser extremamente complicada, isso se deve basicamente as propriedades dos elementos do conjunto gerador $\{a, b\}$. Por outro lado, restringido-se a casos particulares, a saber $G = \langle a, b\rangle$ com $a$ e $b$ satisfazendo uma relação do tipo $ba = a^s b$, os resultados que se obtém são de grande utilidade na classificação de grupos

de ordem pequena.

Nos capítulos 2 e 3 apresenta-se o desenvolvimento deste trabalho. No Capítulo 2 abordaremos os resultados básicos da teoria dos grupos. Dentre os tópicos apresentados, destacaremos neste capítulo,os grupos finitos, grupos abelianos , grupos cíclicos, o Teorema de Lagrange e os isomorfismos de grupos, tópicos fundamentais para uma descrição um pouco mais detalhada sobre a determinação de todos os grupos de ordem $\leq 8$, objetos de estudo no Capítulo 3.

# Capítulo 1

# Grupos

Neste capítulo apresentaremos os resultados básicos da teoria dos grupos que serão usados nos capítulo seguinte. Admitiremos já conhecidos os conceitos e resultados básicos sobre conjuntos, relações de equivalência, funções e operações. Além disso, admitiremos algumas noções preliminares sobre grupo e outros relacionados a este. Para tais tópicos, sugerimos a referência Bega de Domingues e Iezzi (2003) uma vez que este texto traz uma abordagem bastante didática de tais tópicos. Dentre os tópicos apresentados, destacaremos de forma especial os grupos finitos e o Teorema de Lagrange. Para estes indicamos as referências de Garcia e Lequain (2005) e Fraleigh (1988).

**Definição 1.0.1** *Sejam $G$ um conjunto não -vazio e $*$ é uma operação sobre $G$. Diz-se que $G$ munido com esta operação é um* ***grupo*** *quando as seguintes propriedades são satisfeitas:*

*I) A operação $*$ é associativa, ou seja,*

$$a * (b * c) = (a * b) * c \forall a, b, c \in G.$$

*II) Existe elemento neutro para a operação, ou seja,*

$$\exists e \in G, \quad tal\ que \quad e * a = a * e = a, \quad \forall a \in G.$$

*III) Todo elemento em $G$ possui inverso,*

$$\forall a \in G, \ \exists\ a\prime \in G \quad tal\ que \quad a * a\prime = a\prime * a = e.$$

Indica-se o grupo assim definido por $(G, *)$ ou simplesmente por $G$, caso não haja dúvidas quanto à operação em $G$.

Se o grupo $(G, *)$ satisfaz a condição

$$a * b = b * a, \ \forall a, b \in G,$$

então diz-se que $G$ é **comutatitivo** ou **abeliano**.

**Observação 1.0.2** Os elementos $e$ e $a\prime$ das propriedades I e II são únicos e são chamados ***identidade*** *de* $G$ e ***inverso*** de $a$, respectivamente.

Chama-se frequentemente a operação $\star$ de **produto**. Entretanto, isso não tem a princípio relação com os produtos que conhecemos sobre o conjuntos numéricos clássicos. Assim, usa-se $a \cdot b$ ou $ab$ (notação multiplicativa) ao invés de $a \star b$. Neste caso, diz-se que o grupo $G$ é **multiplicativo**. Em geral, isso será considerado no desenvolvimento dos resultados sobre grupos. Isso deve-se apenas à razão de praticidade, pois tais resultados independem da notação usada para indicar a operação considerada em $G$. Especificamente, vamos considerar exemplos de grupos com operações indicadas por $+$, — os **grupos aditivos**.

Quando um grupo $G$ for multiplicativo, então indicaremos o inverso de $a$ por $a^{-1}$. Já para um grupo aditivo, o indicaremos por $-a$.

A seguir exibimos alguns exemplos e contra-exemplos de grupos.

**Exemplo 1.0.3** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ e $(\mathbb{C},+)$ são grupos abelianos, em que as adições saõ as usuais.

**Exemplo 1.0.4** Para cada $n \in \mathbb{Z}$, o conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n}\}$ com a operação de adição dada por

$$\overline{a} + \overline{b} = \overline{a+b},$$

é um grupo aditivo contendo exatamente $n$ elementos.

**Exemplo 1.0.5** O conjunto dos números reais não é um grupo multiplicativo, pois $a = 0 \in \mathbb{R}$ não tem inverso sob a multiplicação. Esse é o único fato que faz com que $\mathbb{R}$ sob a multiplicação não seja um grupo. Por essa razão, $(\mathbb{R}^*, \bullet)$ é um grupo abeliano. Da mesma forma, $(\mathbb{Q}^*, \bullet)$ e $(\mathbb{C}^*, \bullet)$ são grupos abelianos.

***Exemplo 1.0.6*** Seja $\langle V, +, \bullet\rangle$ é um espaço vetorial. Então $\langle V, +\rangle$ é um grupo aditivo abeliano.

**Exemplo 1.0.7** O conjunto $G = M_{n\times m}(\mathbb{R})$ de todas as matrizes reais de ordem $n \times m$ é um grupo abeliano sob a adição usual. De fato, *t*emos que:

1. $X + (Y + Z) = (X + Y) + Z, \quad \forall\ X, Y, Z \in G.$
2. $X + \mathbf{0} = \mathbf{0} + X$, $\forall\ X \in G$, em que

$$\mathbf{0} = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ldots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$

é a matriz nula.

3. Para
$$X = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in G,$$
a matriz
$$Y = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix} \in G$$
é tal que $X+Y = Y+X = \mathbf{0}$. Isso mostra que $G$ é um grupo. A comutatividade da adição em $G$ é imediata.

**Exemplo 1.0.8** Consideremos o conjunto $G = M_n(\mathbb{R})$ de todas as matrizes reais de ordem $n$. Sabe-se que o produto usual de matrizes é associativo, ou seja, dadas as matrizes $X, Y, Z \in G$, então

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z.$$

Além disso, a matriz identidade de ordem $n$,

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \vdots & 0 \\ \vdots & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

é o neutro do produto, pois

$$X \cdot I_n = I_n \cdot X = X, \quad \forall\ X \in G.$$

Agora, certamente existe em $G$ uma matriz tal que $\det X = 0$. Para tal matriz, não existe uma matriz $Y \in G$ tal que $X \cdot Y = I_n$, pois uma matriz $X$ de ordem $n$ é invertível se, e somente se $\det X \neq 0$. Por conseguinte, $G = M_n(\mathbb{R})$ não é um grupo multiplicativo.

**Exemplo 1.0.9** Do exemplo anterior, sabemos que $G = M_n(\mathbb{R})$ não é um grupo sob o produto usual de matrizes, pois a propriedade da existência de inverso para cada elemento não é satisfeita (na verdade, é a única). Consideremos então

$$GL_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}) : \det X \neq 0\}.$$

Vamos mostrar que $GL_n(\mathbb{R})$ é um grupo multiplicativo. Pelo que vimos até agora, é suficiente mostrar que $GL_n(\mathbb{R})$ é fechado sob o produto. Sejam $X, Y \in GL_n(\mathbb{R})$; então $\det X \neq 0$ e $\det Y \neq 0$. Como o determinante do produto de duas matrizes é o produto de seus determinantes, temos

$$\det(X \cdot Y) = \det X \cdot \det Y \neq 0 \Rightarrow X \cdot Y \in GL_n(\mathbb{R}),$$

ou seja, $GL_n(\mathbb{R})$ é sob o produto e, assim, é um grupo. Chama-se $GL_n(\mathbb{R})$ ***grupo linear geral sobre*** $\mathbb{R}$. Em geral, ele é não-abeliano. Similarmente, temos os grupos lineares gerais $GL_n(\mathbb{Q})$ e $GL_n(\mathbb{C})$.

## 1.1 Propriedades Elementares de Grupos

Destaca-se nesta seção propriedades de um grupo $G$ como consequência da definição de grupo.

**Proposição 1.1.1** *Seja $(G, \star)$ um grupo. Então as leis do cancelamento à esquerda e à direita são válidas em $G$, isto é, dados $a, b, c \in G$,*

$$a \star b = a \star c \Rightarrow b = c \quad e \quad b \star a = c \star a \Rightarrow b = c.$$

**Demonstração:** Suponhamos que $a \star b = a \star c$. Sabemos que existe $a_1 \in G$ tal que $a_1 \star a = e = a \star a_1$. Desse modo;

$$\begin{array}{rcll} a \star b = a \star c & \Rightarrow & a_1 \star (a \star b) = a_1 \star (a \star c) & \text{(operando à esquerda por } a_1) \\ & \Rightarrow & (a_1 \star a) \star b = (a_1 \star a) \star c & \text{(pois } \star \text{ é associativa)} \\ & \Rightarrow & e \star b = e \star c & \text{(pois } a_1 \star a = e) \\ & \Rightarrow & b = c. & \text{(pois } e \text{ é neutro de } \star) \end{array}$$

Da mesma forma, pode-se mostrar que se $b \star a = c \star a$, então $b = c$. ■

**Proposição 1.1.2** *Seja $(G, \star)$ um grupo. Dados $a, b \in G$, então as equações lineares $a \star x = b$ e $x \star a = b$ tem solução em $G$.*

**Demonstração:** Mostra-se a existência e unicidade de solução apenas para equação $a \star x = b$, pois o outro caso é tratado similarmente. Seja $a_1 \in G$ tal que $a_1 \star a = e$; daí, o elemento $x = a_1 \star b$ é tal que

$$a \star (a_1 \star b) = (a \star a_1) \star b = e \star b = b,$$

isto é, $x = a_1 \star b$ é uma solução de $a \star x = b$. agora, suponhamos que $x_1, x_2 \in G$ sejam duas soluções de $a \star x = b$. Por isso, $a \star x_1 = b$ e $a \star x_2 = b$, e pela proposição anterior,

$$a \star x_1 = a \star x_2 \Rightarrow x_1 = x_2,$$

o que mostra a unicidade de solução. ■

**Proposição 1.1.3** *Seja $(G, \star)$ um grupo. Então:*

1. *Existe um único elemento $e \in G$ tal que*

$$e \star a = a \star e = a, \quad \forall\ a \in G.$$

2. *Para cada $a \in G$, existe único $a' \in G$ tal que*

$$a' \star a = a \star a' = e.$$

**Demonstração:** 1) Sejam $e$ e $e'$ elementos neutros da operação $\star$. Assim,

$$\begin{array}{rcll} e & = & e' \star e & \text{(pois } e' \text{ é neutro de } \star) \\ & = & e' & \text{(pois } e \text{ é neutro de } \star). \end{array}$$

2) Seja $b \in G$ tal que $b \star a = e$. Como $a' \star a = e$, então pela Proposição 1.1.1, obtemos

$$b \star a = a' \star a \Rightarrow b = a'.$$

■

Por isso, em um grupo $(G, \star)$, o elemento neutro da operação e o inverso de cada elemento em $G$ são únicos. Chama-se o elemento neutro $e$ de **identidade** de $G$. Quanto ao inverso $a'$ de $a$ em $G$, denotaremos de modo específico por $a^{-1}$ ou $-a$, conforme a operação em $G$ seja multiplicativa ou aditiva, respectivamente. Por exemplo, para o grupo $(\mathbb{Z}, +)$, temos que o inverso de $a = 3$ é $-a = -3$ $(3 + (-3) = 0 = e)$; e para o grupo $(\mathbb{R}^*, \bullet)$ o inverso de $a = 3$ é $a^{-1} = 3^{-1} = \frac{1}{3}$ $(3 \cdot 3^{-1} = 1 = e.)$

**Observação 1.1.4** Em decorrência da Proposição 1.1.2, para mostrar que um elemento $e \in G$ é a identidade do grupo $(G, \star)$, é suficiente mostrar que $e \star a = a$ para algum $a \in G$. Similarmente, dado $a \in G$, para mostrar que $b$ é o inverso de $a$, basta mostrar que $b \star a = e$ ou $a \star b = e$.

**Proposição 1.1.5** *Consideremos um grupo $(G, .)$. Então:*

I) $(a^{-1})^{-1} = a$, $\forall\ a \in G$.

II) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, $\forall\ a, b \in G$.

**Demonstração:** 1) Dado $a \in G$, um elemento $b$ é, por definição, o inverso de $a$ ou vice-versa, quando

$$a \cdot b = b \cdot a = e.$$

Como $a \cdot a^{-1} = a^{-1} \cdot a$, então $a = (a^{-1})^{-1}$.

2) Mostra-se que

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e. \tag{1.1}$$

Usando a propriedade associativa da operação em $G$ e omitindo os parêntesis em (1.1);

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= a \cdot b \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} \\ &= a \cdot a^{-1} = e \end{aligned}$$

e

$$(b^{-1}\cdot a^{-1})\cdot(a\cdot b) = b^{-1}\cdot a^{-1}\cdot a\cdot b = b^{-1}\cdot e\cdot b$$
$$= b^{-1}\cdot b = e.$$

Por conseguinte, $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$. ■

O resultado do item 2 da Proposição 1.1.5 pode ser generalizado dsa seguinte forma: Sejam $a_1, a_2, \ldots, a_n \in G$. Então

$$(a_1\cdot a_2\cdot\cdots\cdot a_n)^{-1} = a_n^{-1}\cdot a_{n-1}^{-1}\cdot\cdots\cdot a_2^{-1}\cdot a_1^{-1}.$$

De fato, por indução, para $n = 1$, o resultado é imediato. Supondo o resultado válido para $n$, temos

$$\begin{aligned}(a_1\cdot a_2\cdot\cdots\cdot a_n\cdot a_{n+1})^{-1} &= ((a_1\cdot a_2\cdot\cdots\cdot a_n)\cdot a_{n+1})^{-1}\\ &= a_{n+1}^{-1}\cdot(a_1\cdot a_2\cdot\cdots\cdot a_n)^{-1}\\ &= a_{n+1}^{-1}\cdot a_n^{-1}\cdot a_{n-1}^{-1}\cdot\cdots\cdot a_2^{-1}\cdot a_1^{-1}.\end{aligned}$$

## 1.2 Grupo de Permutações

Seja $A$ um conjunto não-vazio e $S_A$ o conjunto de todas as permutações de $A$, isto é,

$$S_A = \{f : A\to A :\ f \text{ é bijetora}\}.$$

Mostra-se que $S_A$ com a composição de funções é um grupo. Primeiramente, mostremos que $S_A$ é fechado sob essa operação. Sejam $f, g \in S_A$ e $x_1, x_2 \in A$ tais que $(f\circ g)(x_1) = (f\circ g)(x_2)$. Logo,

Se

$$(f\circ g)(x_1) = (f\circ g)(x_2) \Rightarrow f(g(x_1)) = f(g(x_2)),$$

e desde que $f$ é 1-1, segue que $g(x_1) = g(x_2)$. Mas, como $g$ também é 1-1, temos que $x_1 = x_1$. Desse modo, $f\circ g$ é 1-1. Para mostrar que $f\circ g$ é sobrejetiva, considera-se $y \in A$. Como $f$ é sobrejetiva, existe $x \in A$ tal que $f(x) = y$. Por outro lado, sendo $g$ sobre, existe $z \in A$ de maneira que $x = g(z)$. Desse modo,

$$y = f(x) = f(g(z)) = (f\circ g)(z).$$

Por isso, $f\circ g$ é sobre e, por conseguinte, $f\circ g$ é uma permutação de $A$. Portanto,

$$f\circ g \in S_A, \quad \forall\ f, g \in S_A.$$

Como a composição de funções é associativa. A permutação $id_A : A\to A$ (a identidade sobre $A$) é tal que $id_A\circ f = f\circ id_A = f$ para qualquer $f \in S_A$ . E como um função é bijetora se, e somente se é invertível, cada $f \in S_A$ tem inversa em $S_A$.

Portanto, os três axiomas da definição de um grupo são satisfeitos. Desse modo, $(S_A, \circ)$ é um grupo, não-abeliano em geral (pois a composição de funções não é comutativa). Chama-se $(S_A, \circ)$ **grupo das permutações sobre** $A$.

De modo particular, quando o conjunto $A$ tem um número finito de elementos, digamos, $A = \{1, 2, \ldots, n\}$, então $S_A$ tem uma representação e nomes especiais. Nerte caso, denota-se $S_A$ por $S_n$ e chama-se **grupo simétrico** ou **grupo das permutações de** $n$ **letras**. Observa-se que $S_n$ só é abeliano quando $A = \{1\}$ ou $A = \{1, 2\}$.

É comum representar uma permutação $\alpha \in S_n$ por

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

Pela análise combinatória, verifica-se que o grupo $S_3$ tem $n!$ elementos.

**O Grupo $S_3$**

As permutações de $A = \{1, 2, 3\}$ são:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Desse modo,

$$S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}.$$

Consideremos agora $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Logo,

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha_6,$$

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e,$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id,$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha_4$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha_3$$

$$\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha_4$$

Observamos que qualquer elemento de $S_3$ é obtido de $\alpha$ e $\beta$. Isso significa que esses elementos geram $S_3$, em símbolos $S_3 = \langle \alpha, \beta \rangle$. Além disso, $\alpha^3 = e = \beta$ e $\beta\alpha = \alpha^2\beta \neq \alpha\beta$. Resumindo,

$$\begin{cases} G = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta. \end{cases}$$

### 1.2.1 O grupo das Simetrias de um Quadrado

Consideremos um quadrado com vértices $P_1$, $P_2$, $P_3$ e $P_4$ com centro $O$. Pelo centro $O$, vamos considerar as retas $D_1$, $D_2$, $M$ e $N$, determinadas pelas diagonais e pelas mediatrizes do quadrado.

As transformações espaciais que preservam o quadrado são:

**1.** $id, R_{\frac{\pi}{2}}, R_{\pi,} R_{\frac{3\pi}{2}}$: as rotações planas centradas em $O$, no sentido anti-horário, de ângulos zero, $\frac{\pi}{2}$,$\pi$ e $\frac{3\pi}{2}$, respectivamente.

**2.** $R_{1,}R_2, R_m, R_n$: as rotações espaciais de ângulo $\pi$ com eixos $D_1$,$D_2$,$M$,$N$, respectivamente.

Vamos mostrar que a operação de composição de funções é uma operação sobre

$$D_4 = \left\{ id, R_{\frac{\pi}{2}}, R\pi, R_{\frac{3\pi}{2}}, R_1, R_2, R_m, R_n \right\}$$

e que $(D_4, \circ)$ é um grupo. A tabela $\circ$ para os elementos de $D_4$ é a seguinte:

| $\circ$ | $id$ | $R_{\frac{\pi}{2}}$ | $R_\pi$ | $R_{\frac{3\pi}{2}}$ | $R_1$ | $R_2$ | $R_m$ | $R_n$ |
|---|---|---|---|---|---|---|---|---|
| $id$ | $id$ | $R_{\frac{\pi}{2}}$ | $R_\pi$ | $R_{\frac{3\pi}{2}}$ | $R_1$ | $R_2$ | $R_m$ | $R_n$ |
| $R_{\frac{\pi}{2}}$ | $R_{\frac{\pi}{2}}$ | $R_\pi$ | $R_{\frac{3\pi}{2}}$ | $id$ | $R_m$ | $R_n$ | $R_2$ | $R_1$ |
| $R_\pi$ | $R_\pi$ | $R_{\frac{3\pi}{2}}$ | $id$ | $R_{\frac{\pi}{2}}$ | $R_2$ | $R_1$ | $R_n$ | $R_m$ |
| $R_{\frac{3\pi}{2}}$ | $R_{\frac{3\pi}{2}}$ | $id$ | $R_{\frac{\pi}{2}}$ | $R_\pi$ | $R_n$ | $R_m$ | $R_1$ | $R_2$ |
| $R_1$ | $R_1$ | $R_m$ | $R_2$ | $R_n$ | $id$ | $R_\pi$ | $R_{\frac{\pi}{2}}$ | $R_{\frac{3\pi}{2}}$ |
| $R_2$ | $R_2$ | $R_n$ | $R_1$ | $R_m$ | $R_\pi$ | $id$ | $R_{\frac{3\pi}{2}}$ | $R_{\frac{\pi}{2}}$ |
| $R_m$ | $R_m$ | $R_2$ | $R_n$ | $R_1$ | $R_{\frac{3\pi}{2}}$ | $R_{\frac{\pi}{2}}$ | $id$ | $R_\pi$ |
| $R_n$ | $R_n$ | $R_1$ | $R_m$ | $R_2$ | $R_{\frac{\pi}{2}}$ | $R_{\frac{3\pi}{2}}$ | $R_\pi$ | $id$ |

Tábua da composição sobre $D_4$

Está tábua mostra que a composição de simetrias é uma operação em $D_4$. A associatividade da operação é válida, pois a coposição de funções é associativa. Temos também que $id$ é o elemento neutro da operação. Por fim, temos que :

$$R_{\frac{\pi}{2}}^{-1} = R_{\frac{3\pi}{2}}, \quad R_\pi^{-1} = R_{\pi,} \quad R_1^{-1} = R_1$$

$$R_2^{-1} = R_{2,} \quad R_m^{-1} = R_m, \quad , R_n^{-1} = R_n.$$

Portanto, $(D_4, \circ)$ é um grupo, chamado **grupo das simetrias espaciais de um quadrado**. Observe que $D_4$ não é abeliano.

Vamos mostrar agora que os elementos $R_{\frac{\pi}{2}}$e $R_1$ geram o grupo $D_4$, isto é, qualquer elemento de $D_4$ é um produto de potências desses elementos. Temos que:

1. $\left(R_{\frac{\pi}{2}}\right)^2 = R_{\frac{\pi}{2}} \circ R_{\frac{\pi}{2}} = R_\pi$.
2. $\left(R_{\frac{\pi}{2}}\right)^3 = R_\pi \circ R_{\frac{\pi}{2}} = R_{\frac{3\pi}{2}}$.
3. $\left(R_{\frac{\pi}{2}}\right)^4 = id = e$.
4. $R_1^2 = id = e$.
5. $R_{\frac{\pi}{2}} \circ R_1 = R_m$.
6. $R_1 \circ \left(R_{\frac{\pi}{2}}\right)^2 = R_1 \circ R_\pi = R_2$.
7. $\left(R_1 \circ \left(R_{\frac{\pi}{2}}\right)^3\right) = \left(R_1 \circ R\frac{3\pi}{2}\right) = R_n$.

Portanto,

$$\begin{cases} D_4 = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^3\beta, \end{cases}$$

em que $\alpha = R_{\frac{\pi}{2}}$ e $\beta = R_1$.

## 1.3 Subgrupos

Ao estudar uma determinada estrutura algébrica é importante ir em busca de subconjuntos que herdam da estrutura original as mesmas propriedades . No caso em que essa estrutura é um grupo, esses subconjuntos recebem o nome de *subgrupo*.

**Definição 1.3.1** *Se $G$ é um grupo e $H$ é um subconjunto não-vazio de $G$, então se diz que $H$ é um subgrupo de $G$ quando a operação de $G$ restringida a $H$ faz deste um grupo, isto é, quando as condições seguintes são satisfeitas:*

1. $h_1h_2 \in H$, $\forall h_1, h_2 \in H$
2. $h_1(h_2h_3) = (h_1h_2)\, h_3$, $\forall h_1, h_2, h_3 \in H$
3. $\exists\ e_H \in H$ tal que $e_Hh = he_H = h$, $\forall h \in H$
4. Para cada $h \in H$,existe $k \in H$ tal que $hk = kh = e_H$.

Para indicar que $H$ é um subgrupo de $G$, usaremos a notação $H < G$.
Quanto ao subgrupo $H$ temos que:

1. O elemento neutro de $H$, $e_H \in H$, é igual ao elemento neutro $e$ do grupo $G$. De fato, para $a \in H \subseteq G$, temos $e_H \cdot a = a$; desse modo,

$$e_H \cdot a = a \Rightarrow (e_H \cdot a)\, a^{-1} = a \cdot a^{-1} = e$$
$$\Rightarrow e_H \cdot (a \cdot a^{-1}) = e \Rightarrow e_H = e.$$

2. Dado $h \in H$, o inverso de $h$ em $H$ é igual ao inverso de $h$ em $G$. De fato, seja $k$ o inverso de $h$ em $H$. Então

$$h \cdot k = k \cdot h = e_H = e.$$

Não é necessário verificar os três axiomas da definição de grupo para decidir se um dado subconjunto $H$ de um grupo $G$ é ou não um grupo. Isso se deve a seguinte proposição, o qual caracteriza os subgrupos de um grupo.

**Proposição 1.3.2** *Seja $H$ um subconjunto não vazio de um do grupo $G$. Então $H$ é um subgrupo de $G$ se, e somente se as duas condições seguintes são satisfeitas:*

*1.* $h_1.h_2 \in H$, $\forall\ h_{1,}h_2 \in H$.

*2.* $h^{-1} \in H$, $\forall\ h \in H$.

No que segue apresenta-se alguns exemplo e contra-exemplos de subgrupos.

**Exemplo 1.3.3** Para um grupo qualquer $G$, $\{e\}$ e $G$ são claramente subgrupos de $G$, chamados ***subgrupos triviais*** de $G$.

**Exemplo 1.3.4** Com a adição usual, temos que $\mathbb{Z} < \mathbb{Q}$. Aliás, temos os subgrupos

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$

**Exemplo 1.3.5** Sob a multiplicação usual, obtemos

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

**Exemplo 1.3.6** O conjunto $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ é um subgrupo de $\mathbb{Z}$. Mais geralmente, se $n \in \mathbb{Z}$, então $n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$. Reciprocamente, se $H$ é um subgrupo de $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que

$$H = nZ = \{nk : k \in \mathbb{Z}\}.$$

**Exemplo 1.3.7** O conjunto $H$ dos números ímpares não é um subgrupo de $(\mathbb{Z}, +)$, pois a soma de dois números ímpares é um número par, ou seja, se $a, b \in H$, então $a + b \notin H$.

**Exemplo 1.3.8** Seja $U_n = \{1, e^{\frac{2\pi}{n}i}, e^{\frac{4\pi}{n}i}, ..., e^{\frac{2(n-1)\pi}{n}i}\}$ o grupo multiplicativo das raizes $n-$ésimas da unidade. Temos a seguinte cadeia de subgrupos de $\mathbb{C} - \{0\}$ :

$$U_n < S^1 < \mathbb{C} - \{0\},$$

*em que $S^1$ é o grupo dos números complexos de norma 1, ou seja, $S^1$ é o circulo unitário.*

**Exemplo 1.3.9** Considerando o conjunto $H = \{x \in \mathbb{R}^* : x > 0\}$. Então $H$ é um subgrupo do grupo multiplicativo $G = (\mathbb{R}^*, \cdot)$. De fato, para $a, b \in H$, temos $a > 0, b > 0$. Logo $a \cdot b > 0 \in H$. Por outro lado, $a^{-1} \in H$ e é tal que $a \cdot a^{-1} = 1 = e$. Por isso,

$$H < G.$$

**Proposição 1.3.10** *Sejam $H_1$ e $H_2$ dois subgrupos de um grupo $G$. Então a interseção $H = H_1 \cap H_2$ também é um subgrupo de $G$.*

**Demonstração:** Primeiramente, notamos que $e \in H \neq \emptyset$, pois $e \in H_1$ e $e \in H_2$. Agora, para $a$, $b \in H$,

$$\left\{ \begin{array}{lll} a \in H_1 & \text{e} & a \in H_2 \\ b \in H_1 & \text{e} & b \in H_2 \end{array} \right. \Rightarrow ab \in H_1 \quad \text{e} \quad ab \in H_2,$$

pois $H_1 < G$ e $H_2 < G$. Desse modo, $ab \in H_1 \cap H_2$. Da mesma forma, $a^{-1} \in H_1$ e $a^{-1} \in H_2$. Portanto, $a^{-1} \in H_1 \cap H_2$. Por isso, $H_1 \cap H_2 < G$. ■

Mais geralmente, se $H_1, ..., H_n, \ldots$ são subgrupos de um grupo $G$, então prova-se que

$$\bigcap_{i \in \mathbb{N}} H_i = H_1 \cap H_2 \cap \cdots \cap H_n \cap \cdots$$

é um subgrupo de $G$.

Ao contrário da interseção de subgrupos, a união de dois subgrupos de $G$ não é necessariamente um subgrupo de $G$. Por exemplo, $H_1 = \{(x, 0) : x \in \mathbb{R}\}$ e $H_2 = \{(0, x) : x \in \mathbb{R}\}$ são subgrupos do grupo aditivo $(\mathbb{R}^2, +)$. Entretanto, a união de $H_1 \cup H_2$ não o é. De fato, $(2, 0), (0, 3) \in H_1 \cup H_1$, mas $(2, 0) + (0, 3) = (2, 3) \notin H_1 \cup H_2$. Na verdade,

**Proposição 1.3.11** *Sejam $H_1$ e $H_2$ subgrupos de um grupo $G$. Então*

$$H_1 \cup H_2 < G \Leftrightarrow H_1 \subset H_2 \quad ou \quad H_2 \subset H_1.$$

## 1.4 Grupos Cíclicos

Destaca-se nesta seção uma classe importante de grupo, a saber, a classe de grupos cíclicos.

**Definição 1.4.1** *Sejam $(G,\cdot)$ um grupo e $a \in G$. Se $n \in \mathbb{Z}$, definimos $a^n$ da seguinte forma:*

$$a^n = \begin{cases} e & \text{se} \quad n = 0, \\ a^{n-1} \cdot a & \text{se} \quad n > 0, \\ (a^{-n})^{-1} & \text{se} \quad n < 0. \end{cases}$$

Se a opreação de um grupo $G$ for aditiva, então tem-se os múltiplos de $a$, ao invés de potências.

Prova-se por indução que:

1. $a^n \cdot a^m = a^{n+m}$, $\forall\ n, m \in \mathbb{Z}$.
2. $(a^n)^m = a^{nm}$.

Considerando que $a \in G$ e $H$ o subconjunto de $G$, dado por

$$H = \{a^n : n \in \mathbb{Z}\}.$$

Vamos provar que $H < G$. Seja $\alpha, \beta \in H$, digamos $\alpha = a^n$ e $\beta = a^m$, temos $\alpha \cdot \beta = a^n \cdot a^m = a^{n+m} \in H$, isto é, $H$ é fechado sob a operação de $G$. Por outro lado, $\alpha^{-1} = (a^n)^{-1} = a^{-n} \in H$. Portanto, $H$ é um subgrupo de $G$, o qual é chamado **subgrupo cíclico gerado por** $a$ e é indicado por $H = \langle a \rangle$. Neste caso, o elemento $a$ é um **gerador** de $H$.

De um modo mais geral, um grupo $G$ é dito **cíclico** se existe $x \in G$ tal que

$$G = \langle x \rangle.$$

**Exemplo 1.4.2** O grupo aditivo $(\mathbb{Z}, +)$ é cíclico, pois $\mathbb{Z} = \langle 1 \rangle$. Aliás, $a = -1$ também é um gerador de $\mathbb{Z}$.

**Exemplo 1.4.3** O grupo $(\mathbb{Z}_3, +)$ é cíclico gerado por $a = \overline{1}$, pois

$$\begin{aligned} \overline{0} &= 3 \cdot \overline{1} = \overline{1} + \overline{1} + \overline{1}, \\ 1 &= 1 \cdot \overline{1}, \\ 2 &= 2 \cdot \overline{1} = \overline{1} + \overline{1}. \end{aligned}$$

Por isso, $\mathbb{Z}_3 = \langle \overline{1} \rangle$. Verifica-se também que $\mathbb{Z}_3 = \langle \overline{2} \rangle$. Mais geralmente, para cada $n \in \mathbb{Z}$, o grupo $(\mathbb{Z}_n, +)$ é cíclico e que $\overline{a} \in \mathbb{Z}_n$ é um gerador de $\mathbb{Z}_n$ se e somente se, $mdc(a, n) = 1$, de acordo com o Teorema 1.4.8.

É claro que todo grupo cíclico $G = \langle a \rangle$ é abeliano, pois dados $\alpha = a^n$ e $\beta = a^m$ em $G$, temos que

$$\alpha \cdot \beta = a^n \cdot a^m = a^{n+m} = a^{m+n} =$$
$$= a^m \cdot a^n = \beta \cdot \alpha.$$

A recíproca desta resultado não é válida. Por exemplo, o produto direto $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ é abeliano, pois $\mathbb{Z}_2$ o é, mas não é cíclico, pois para cada $x \in G$, temos qu $x + x = (\overline{0}, \overline{0})$, ou seja, não há como obter todos os elementos de $G$ a partir de um dado elemento em $G$.

**Definição 1.4.4** *A **ordem** de um grupo $G$ é o número de elementos em $G$, em símbolos $|G|$.*

Por exemplo, $|\mathbb{Z}_n| = n$, $|D_4| = 8$ e $|S_n| = n!$.

**Definição 1.4.5** *Seja $G$ um grupo e $\alpha \in G$. Se exise $k \in \mathbb{N}$ tal que $\alpha^k = e$, então a **ordem** de $\alpha$, em símbolos $\mathcal{O}(\alpha)$, é o menor elemento satisfazendo esta condição, ou seja,*

$$\mathcal{O}(\alpha) = \min\{n \in \mathbb{N} : \alpha^n = e\}.$$

*Se não existe nenhum natural $k$ tal que $\alpha^k = e$, então dis-ze que $\alpha$ é de ordem infinita.*

No grupo $S_3$ o elemento

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{1.2}$$

tem ordem dois, pois $\alpha \neq e$ e $\alpha^2 = e$. No grupo aditivo $(\mathbb{Z}, +)$ todo elemento $\alpha \neq 0$ é de ordem infinita, pois $\alpha \cdot n = 0$ só é possível quando $n = 0$.

Em um grupo $G$ valem:

**1.** $\mathcal{O}(\alpha) = 1 \Leftrightarrow \alpha = e$.

**2.** Se $\alpha \in G - \{e\}$, então $\mathcal{O}(\alpha) = 2 \Leftrightarrow \alpha = \alpha^{-1}$.

**Proposição 1.4.6** *Sejam $\alpha$ um elemento do grupo $G$ e $< \alpha >$ o subgrupo gerado por $\alpha$. Então as seguintes condições são equivalentes:*

**1.** *A ordem $|< \alpha >|$ é finita.*

**2.** *Existe $t \geq 1$ tal que $\alpha^t = e$.*

*Neste caso, denotando por $n$ a ordem de $\alpha$, temos*

$$\langle \alpha \rangle = \left\{e, \alpha, ...\alpha^{n-1}\right\},$$

*ou seja, a ordem de $\alpha$ é igual a ordem do grupo por ele gerado.*

Voltemos ao grupo $S_3$ e $\alpha$ como em (1.2). Temos que

$$\begin{aligned}\alpha^2 = e \Rightarrow \left(\alpha^2\right)^2 = e \Rightarrow \alpha^4 = e \\ \Rightarrow \alpha^8 = e.\end{aligned}$$

Em geral, para qualquer $k \in \mathbb{Z}$, obtemos que $\alpha^{2k} = e$. Isso não é um caso isolado, de fato:

**Proposição 1.4.7** *Sejam $G$ um grupo e $\alpha \in G$ tal que $\mathcal{O}(\alpha) = n$ (ordem finita). Se $\alpha^m = e$ e $m \neq 0$, então $n$ divide $m$.*

**Demonstração:** Pelo Algoritmo da divisão, tem-se

$$m = n \cdot q + r \quad \text{com} \quad 0 \leq r < n.$$

Desse modo,

$$\alpha^m = \alpha^{n \cdot q + r} = \alpha^{n \cdot q} \cdot \alpha^r = (\alpha^n)^q \cdot \alpha^r.$$

Portanto, $\alpha^r = e$. Por isso, $r = 0$ e $n$ divide $m$. ■

O resultado final do Exemplo 1.4.3 é parte de um resultado bem mais geral.

**Teorema 1.4.8** *Seja $G = \langle a \rangle$ um grupo cíclico de ordem $n$. Então $a^t$ é um gerador de $G$ se, e somente se $mdc(n, t) = 1$.*

**Demonstração:** Suponha que $a^t$ é um gerador de $G$. Desse modo, como $a \in G$, existe $r \in \mathbb{Z}$ tal que $a^{tr} = a$. Daí,

$$a^{tr-1} = e.$$

Pela Proposição 1.4.7, $n$ divide $tr - 1$, isto é, $tr - 1 = nk$ para algum $k \in \mathbb{Z}$. Por isso, $tr - nk = 1$, de onde obtemos que $mdc(n, t) = 1$. Reciprocamente, se $mdc(n, t) = 1$, então pela identidade de Bézout, existem $x, y \in \mathbb{Z}$ tais que $n \cdot x + t \cdot y = 1$. Assim,

$$a^{ty} = a$$

Agora, dado $x \in G$, temos que existe $r \in \mathbb{Z}$ tal que $x = a^r$. Logo,

$$x = a^r = (a^{ty})^r = (a^t)^{yr},$$

isto é, $x \in \langle a^t \rangle$ e, por isso, $\langle a^t \rangle = G$. ■

**Exemplo 1.4.9** Determinar os geradores dos grupo aditivo $\mathbb{Z}_{14}$.

**Solução:** Para determinar os geradores de $\mathbb{Z}_{14}$, vamos em busca de todos os $t \in \mathbb{N}$ tais que $mdc(14, t) = 1$. Assim, $t$ assume os seguintes valores:

$$t = 1, 3, 5, 9, 11, 13$$

Daí, pelo Teorema 1.4.8 temos que os geradores de $\mathbb{Z}_{14}$ são os seguites elementos: $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{9}$, $\overline{11}$ e $\overline{13}$. ■

**Teorema 1.4.10** *Todo subgrupo de um grupo cíclico é também cíclico.*

## 1.5 Classes Laterais e o Teorema de Lagrange

Sejam $G$ um grupo e $H$ um subgrupo de $G$. Considere a relação $\equiv_E \pmod H$ sobre $G$ dada por

$$x \equiv_E y \pmod H \Leftrightarrow x^{-1}y \in H.$$

Essa relação é de equivalência. De fato, sejam $x, y, z \in G$. Temos

**1.** $x^{-1}x = e \in H \Rightarrow x \equiv_E x \pmod H$. ($\equiv_E \pmod H$ é reflexiva)

**2.** Se $x \equiv_E y \pmod H$, então $x^{-1}y \in H \Rightarrow y^{-1}x \in H \Rightarrow y \equiv_E x \pmod H$. ($\equiv_E \pmod H$ é simétrica)

**3.** Se $x \equiv_E y \pmod H$ e $y \equiv_E z \pmod H$, então $x^{-1}y \in H$ e $y^{-1}z \in H$. Portanto,

$$\left(x^{-1}y\right)\left(y^{-1}z\right) \in H \Rightarrow x^{-1}z \in H \Rightarrow x \equiv_E z \pmod H,$$

o que mostra que $x \equiv_E y \pmod H$ é transitiva e, por conseguinte, é de equivalência.

Sob a relação $\equiv_E y \pmod H$, para cada $x \in G$, a classe de equivalência de $x$ é o conjunto

$$\{y \in G : y \equiv_E x \pmod H\}.$$

Verifica-se que $\{y \in G : y \equiv_E x \pmod H\} = \{xh : h \in H\}$ e por isso, vamos denotá-la por $xH$, ou seja,

$$xH = \{xh : h \in H\},$$

e chamá-la **classe lateral à esquerda de $H$ determinada por $x$**, ou simplesmente **classe lateral de $x$ à esquerda**.

De maneira similar, a relação $\equiv_E \pmod H$ sobre $G$ dada por

$$x \equiv_D y \pmod H \Leftrightarrow xy^{-1} \in H$$

e que a classe de equivalência de $x \in G$, simbolizada por $Hx$ é

$$Hx = \{hx : h \in H\}$$

e chamada **classe lateral de $x$ à direita.**

Observe que $eH = H = He$, ou seja, $H$ é tanto uma classe à esquerda quanto à direira. Além disso, quando $G$ é comutativo [Nal], então $xH = Hx$ para todo $x \in H$.

**Exemplo 1.5.1** Seja $G = \mathbb{Z}_6$ e $H = \{\overline{0}, \overline{3}\}$. As classes laterais à esquerda de $H$ são as seguintes*:*

$$\begin{aligned}
\overline{0} + H &= \{\overline{0}, \overline{3}\} = H \\
\overline{1} + H &= \{\overline{1}, \overline{4}\} \\
\overline{2} + H &= \{\overline{2}, \overline{5}\} \\
\overline{3} + H &= \{\overline{3}, \overline{0}\} = H \\
\overline{4} + H &= \{\overline{4}, \overline{1}\} = \overline{1} + H \\
\overline{5} + H &= \{\overline{5}, \overline{2}\} = \overline{2} + H
\end{aligned}$$

Observe como $\mathbb{Z}_6$ é um grupo aditivo abeliano as classes laterais à esquerda de $H$ coincidem com suas classes laterais à direita.

Para um grupo $G$ e $H < G$, vamos denotar por $G_E$ e $G_D$ os conjuntos de todas as classes laterais à esquerde e á direita de $H$, respectivamente, ou seja,

$$G_E = \{xH : x \in G\} \quad \text{e} \quad G_D = \{Hx : x \in G\}.$$

Como os elementos de $G_E$ e $G_D$ são classes de equivalência, então ambos constituem partições de $G$. Em geral, tem-se que $G_E \neq G_D$; entretanto, eles têm a mesma cardinalidade, pois a função

$$\begin{array}{rccc}
\varphi : & G_E & \to & G_D \\
 & xH & \mapsto & Hx^{-1}
\end{array}$$

é uma bijeção.

Sob certas condições, verifica-se que os conjuntos $G_E$ e $G_D$ coincidem.

**Definição 1.5.2** *A cardinalidade do conjunto $G_E$ chama-se **índice** de $H$ em $G$, e simboliza-se por $(G : H)$.*

**Exemplo 1.5.3** No exemplo 2.4.1, temos $G_E = \{\overline{0}+H, \overline{1}+H, \overline{2}+H\}$. Logo, $(G : H).= 3$.

Para cada $x \in G$, a função $f : H \to xH$ dada por $f(x) = xH$ é uma bijeção. Por isso, toda classe lateral à esquerda tem a mesma cardinalidade de $H$. Da mesma forma, tem-se que quaisquer duas classes laterais à direita têm a mesma cardinalidade, igual a cardinalidade de $H$.

O Teorema de Lagrange dado a seguir é o principal resultados sobre grupos finitos.

**Teorema 1.5.4** (Teorema de Lagrange) *Sejam $G$ um grupo finito e $H$ um subgrupo de $G$. Então*

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

*Ou seja, a ordem e o índice de $H$ em $G$ dividem a ordem de $G$.*

**Demonstração:** Suponha que $(G : H) = r$ e seja $G_E = \{x_1H, x_2H, \ldots, x_rH\}$. Como $G_E$ é uma partição de $G$, segue que

$$G = x_1H \cup x_2H \cup \ldots \cup x_rH.$$

Como $x_iH$ tem a mesma cardinalidade de $H$ para $i \in \{1, \ldots, r\}$ e $x_iH \cap x_jH = \emptyset$ com $i \neq j$,

$$|G| = |H| + |H| + \cdots + |H|\,. \quad \text{(r vezes)}$$

De onde concluí-se que

$$|G| = r \cdot |H| \Rightarrow |G| = |H|\,(G : H)\,.$$

■

A seguir destacam-se algumas consequências do teorema de Lagrange.

**Corolário 1.5.5** *Sejam $G$ um grupo finito e $\alpha \in G$. Então a ordem de $\alpha$ divide a ordem de $G$. Em particular,*

$$\alpha^{|G|} = e.$$

**Demonstração:** Por definição, $\mathcal{O}(\alpha) = |\langle\alpha\rangle|$ e pelo Teorema de Lagrange, temos que $\mathcal{O}(\alpha)$ divide $|G|$. Façamos então $|G| = n$ e $\mathcal{O}(\alpha) = r$. Dai, $n = r \cdot k$ para algum $k \in \mathbb{Z}$ e

$$\alpha^{|G|} = \alpha^{r\cdot k} = \alpha^{r\cdot k} = (\alpha^r)^k = e^k = e \Rightarrow \alpha^{|G|} == e.$$

**Corolário 1.5.6** *Todo grupo $G$ de ordem prima é cíclico. Em particular, $G$ é abeliano.*

**Demonstração:** Seja $G$ um grupo tal que $|G| = p$, em que $p$ é um número primo. Desse modo, existe $x \in G - \{e\}$. Pelo Teorema de Lagrange, $|\langle\alpha\rangle|$ divide $p$. Mas, sendo $p$ primo, temos $|\langle x\rangle| = p$, pois $|\langle x\rangle| \neq 1$. Por isso, $|\langle x\rangle| = G$ e, por conseguinte, $G$ é cíclico. ■

**Corolário 1.5.7** *Se $G$ é um grupo finito tal que $|G| \leq 5$, então $G$ é abeliano.*

**Demonstração:** Se $|G| = 1 \Rightarrow G = \{e\}$ e, desse modo, $G$ é cíclico. Se $|G| = 2, 3$ ou $5$, então $G$ tem ordem prima e pelo Corolário 1.5.6, $G$ é abeliano. Só nos resta considerar o caso em que $|G| = 4$.

Suponha que $|G| = 4$. Se existe $x \in G - \{e\}$ tal que $\langle x \rangle = G$, então $G$ é cíclico e, portanto, abeliano. Suponham que

$$\langle x \rangle \neq G, \quad \forall\, x \in G.$$

Assim, pelo Teorema de Lagrange, temos $|\langle x \rangle| = 2$ para todo $x \in G - \{e\}$. Assim, para todo $x \in G$,

$$x^2 = e \Leftrightarrow x = x^{-1}.$$

Daí, para $x, y \in G$,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

Portanto, $G$ é abeliano. ■

## 1.6 Subgrupos Normais e Grupos Quocientes

O objetivo desta seção é mostrar que o conjunto das classes laterais à esquerda de $H < G$ com uma operação induzida da operação em $G$ é um grupo, chamado Grupo Quociente. Há muitos resultados a serem explorados sobre esses tópicos, mas vamos destacar os que de fato serão usados no próximo capítulo.

Inicialmente define-se o conceito de subgrupo normal.

**Definição 1.6.1** *Sejam $G$ um grupo e $N$ um subgrupo de $G$. Diz-se que $N$ é um* ***subgrupo normal*** *de $G$, em símbolos $N \trianglelefteq G$, quando*

$$gNg^{-1} \subset N, \quad \forall g \in G,$$

*em que $gNg^{-1} = \{gng^{-1} : g \in G \text{ e } n \in N\}$. Equivalentemente, $N$ é normal quando*

$$gng^{-1} \in N, \quad \forall g \in G \quad e \quad \forall n \in N.$$

**Exemplo 1.6.2** $\{e\}$ e $G$ são subgrupos normais de $G$.

**Exemplo 1.6.3** Se $G$ é abeliano, então todo subgrupo de $G$ é normal. Portanto, para cada $n \in \mathbb{Z}$, $n \cdot \mathbb{Z}$ é normal em $\mathbb{Z}$..

**Exemplo 1.6.4** O centro $Z(G)$ de $G$ é normal em $G$

**Solução:** De fato, mostremos primeiro $Z(G) < G$. Sejam $n_1 n_2 \in Z(G)$. Desse modo, para $g \in G$,

$$\begin{array}{rcccl} (n_1n_2)g & = & n_1(n_2g) & = & n_1(gn_2) \quad (\text{pois } n_2 \in Z(G)) \\ & = & (n_1g)n_2 & = & g(n_1n_2) \quad (\text{pois } n_1 \in Z(G)). \end{array}$$

ou seja, $n_1 n_2 \in Z(G)$. Por outro lado, para $n \in Z(G)$ e $g \in G$,

$$\begin{aligned} n^{-1}g &= n^{-1}gnn^{-1} = n^{-1}ngn^{-1} \quad (\text{pois } n_2 \in Z(G)) \\ &= gn^{-1}. \end{aligned}$$

Por isso, $n^{-1} \in Z(G)$, o que mostra que $Z(G) < G$. Por fim, como

$$ng = gn, \quad \forall g \in G \quad e \quad \forall n \in Z(G),$$

então

$$ng = gn \Rightarrow g^{-1}ng = n \in Z(G) \Rightarrow Z(G) \trianglelefteq G.$$

♣

**Exemplo 1.6.5** Em $S_3$, o subgrupo gerado por $H = \{e, \alpha\}$, em que

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

não é normal, pois

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

e

$$\beta\alpha\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin H.$$

O próximo teoremanos ajuda a caracterizar os subgrupos normais de um grupo $G$. Sua demonstração não será apresentada aqui, mas está em qualquer uma das referências de Garcia e Lequain (2005, p.135) e Gonçalves (2009, p.140).

**Teorema 1.6.6** *Seja $G$ um grupo e $N$ um subgrupo de $G$. As afirmações seguintes são equivalentes:*

1. $N \trianglelefteq G$.
2. $gNg^{-1} \subseteq N, \quad \forall\ g \in G$.
3. $gNg^{-1} = N, \quad \forall g \in G$.
4. $gN = Ng, \quad \forall g \in G$.

5. $(g_1N)(g_2N) = g_1g_2N, \quad \forall g_1, g_2 \in G.$

O Teorema acima mostra que quando $N$ é normal em $G$, então qualquer classe lateral à esquerda de $g$ é igual a sua classe à direita e virce versa; daí, $G_E = G_D$. Quando $N$ for um subgrupo normal de $G$, vamos denotar o conjunto $G_E$ por $G/N$ ou $\frac{G}{N}$. Ainda de acordo com o Teorema 1.6.6, o conjunto $G/N$ munido da operação

$$\begin{array}{rccc} \cdot : & G/N \times G/N & \to & G/N \\ & (g_1N, g_2N) & \mapsto & g_1g_2N \end{array}$$

é um grupo, chamado **grupo quociente** de $G$ por $N$. O elemento neutro de $G/N$ é a classe lateral $N$; o inverso de $gN$ é a classe $g^{-1}N$.

**Exemplo 1.6.7** Como para cada $n \in \mathbb{Z}$, $n \cdot \mathbb{Z}$ é normal em $G$. Desse modo, $\frac{\mathbb{Z}}{n\cdot\mathbb{Z}}$ é um grupo que, como veremos, é idêntico ao grupo $(\mathbb{Z}_n, +)$. *P*or isso, vamos escrever $\frac{\mathbb{Z}}{n\cdot\mathbb{Z}} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

**Exemplo 1.6.8** Para o grupo multiplicativo $G = \{1, -1, i, -i\} \subset C$, $N = \{1, -1\}$ é normal. O grupo quociente é

$$G/N = \{N, \{i, -i\}\}.$$

## 1.7 Homomorfismos de grupos

Dentre as aplicações entre grupos, as de maior interesse são aquelas que preservam as estrururas entre eles, no sentido da seguinte definição:

**Definição 1.7.1** *Sejam $(G, \cdot)$ e $(K, \times)$ dois grupos. Uma aplicação $f : G \longrightarrow K$ é dita um **homomorfismo** quando*

$$f(a \cdot b) = f(a) \times f(b), \quad \forall a, b \in G.$$

Um homomorfimo $f : G \longrightarrow K$ bijetivo chama-se **isomorfismo**. Em particular, um isomorfismo $f : G \longrightarrow G$ é dito um **automorfismo** de $G$.

Prova-se que se $f : G \longrightarrow K$ é um isomorfismo, então $f^{-1} : K \longrightarrow G$ também o é. Neste caso, diz-se que dois grupos $G$ e $K$ são **isomorfos**, em símbolos $G \simeq K$, quando existir um isomorfismo entre eles. Dois grupos isomorfos são idênticos, isto com relação às suas propriedades. Assim, se $f : G \longrightarrow K$ é um isomorfismo, identificamos um elemento $x \in G$ com sua imagem $f(x)$, em símbolos

$$x \mapsto f(x).$$

**Exemplo 1.7.2** Para um grupo qualquer $G$, a função $id : G \longrightarrow G$ dada por $id(g) = g$ para todo $g \in G$, é um homomorfismo. Chama-se $id$ ***homomorfismo idêntico.***

**Exemplo 1.7.3** A função $f : G \longrightarrow K$ dada por $f(x) = e_2$, em que $e_2$ é a identidade de $K$, é um homomorfismo trivial e chama-se ***homomorfismo trivial.***

**Exemplo 1.7.4** Seja $H \lhd G$,então $\varphi : G \to G/H$ dada por $\varphi(g) = gH$ , é um homomorfismo chamado de ***projeção canônica.***

**Exemplo 1.7.5** Sejam $G$ um um grupo e $g \in G$ fixo. Então, $\mathcal{I}_g : G \longrightarrow G$ dada por $\mathcal{I}_g(x) = gxg^{-1}$ para todo $x \in G$, é um automorfismo chamado ***automorfismo interno associado a*** $g \in G$..

### 1.7.1 Propriedades Elementares do Homomorfismos

Destaca-se a seguir algumas propriedades dos homomorfismo de grupos. No que segue, $e_1$ e $e_2$ representam as identidades dos grupos $G$ e $K$, respectivamente.

Dois conceitos relacionados ao de homomorfismo e que são imprescindíveis em teoria dos grupos são os de núcleo e imagem de um homomorfismo.

**Definição 1.7.6** *Seja $f : G \longrightarrow K$ um homomorfismo de grupos. O* ***núcleo*** *e* imagem *de $f$, denotados por* $\ker f$ *e* $\operatorname{Im} f$*, respectivamente, como sendo os seguintes conjuntos:*

$$\ker f = \{x \in A : f(x) = e_2\},$$
$$\operatorname{Im} f = \{f(x) : x \in A\}.$$

**Exemplo 1.7.7** Para o homomorfismo idêntico $f = id : G \longrightarrow G$, tem-se que $\ker f = \{e\}$ e $\operatorname{Im} f = G$.

**Exemplo 1.7.8** Consideremos a aplicação $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ definida por $f(m) = i^m$. Assim, para $n, m \in \mathbb{Z}$,

$$f(m+n) = i^{m+n} = i^m \cdot i^n = f(m) \cdot f(n),$$

isto é, $f$ é um homomorfismo. Além disso,

$$\ker(f) = \{m \in \mathbb{Z} : f(m) = e\} \Rightarrow \ker(f) = \{0, \pm 4, \pm 8, ...\}$$

e

$$\operatorname{Im} f = \{f(m) \in \mathbb{C}^* : m \in \mathbb{Z}\} \Rightarrow \operatorname{Im} f = \{1, i, -1, -i\}.$$

**Proposição 1.7.9** *Seja $f : G \longrightarrow K$ um homomorfismo. Então*

1. $f(e_1) = e_2$.

*2.* $f(x^{-1}) = f(x)^{-1}, \quad \forall\, x \in G.$

**Demonstração:** 1) Como, $f(e_1) = \varphi(e_1 \cdot e_1) = \varphi(e_1) \cdot \varphi(e_1)$. Portanto, $f(e_1) = e_2$. 2) Para $x \in G$, $e_2 = f(e_1) = f(xx^{-1}) = f(x)f(x^{-1})$; por isso, $f(e_1) = e_2$. ■

**Teorema 1.7.10** *Seja $f : G \longrightarrow K$ um homomorfismo. Então*

*1.* $\ker f \trianglelefteq G$.

*2.* $\operatorname{Im} f < K$.

**Demonstração:** Provaremos apenas o item 1. Primeiramente, mostremos que $\ker f < G$. Dados, $x, y \in \ker f$, temos:

$$f(xy) = f(x)\, f(y) = e_2 e_2 = e_2 \Rightarrow xy \in \ker f.$$

Temos também,

$$f\left(x^{-1}\right) = f(x)^{-1} = e_2^{-1} = e_2 \Rightarrow x^{-1} \in \ker f.$$

Portanto, $\ker f < G$. Agora, para $g \in G$,

$$\begin{aligned} f\left(gxg^{-1}\right) &= f(g)\, f(x)\, \varphi\left(g^{-1}\right) = f(g)\, e_2 \varphi\left(g^{-1}\right) \\ &= f(g)\, f(g)^{-1} = e_2. \end{aligned}$$

Logo, $gxg^{-1} \in \ker f$, o que mostra que $\ker f \trianglelefteq G$. ■

O teorema seguinte caracteriza[1] os grupos cíclicos finitos. O mesmo será bastante usado no capítulo seguinte.

**Teorema 1.7.11** *Seja $G = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ um grupo cíclico de ordem $n$. Então*

$$\begin{array}{rccc} f: & (\mathbb{Z}_n, +) & \to & (G, \cdot) \\ & \overline{m} & \mapsto & a^m \end{array}$$

*é um isomorfismo.*

**Demonstração:** Temos claramente que $f$ é bijetora. Por outro lado, para $\overline{m_1}, \overline{m_2} \in \mathbb{Z}_n$,

$$\begin{aligned} f(\overline{m_1} + \overline{m_2}) &= f(\overline{m_1 + m_2}) = a^{m_1 + m_2} \\ &= a^{m_1} \cdot a^{m_2} = f(\overline{m_1}) \cdot f(\overline{m_2}). \end{aligned}$$

Portanto, $f$ é um isomorfismo. ■

[1] Há também um teorema que caracteriza os grupos cíclicos infinitos. Entretanto, ele não será apresentado aqui devido ao objetivo do trabalho.

Em outras palavras, resume-se o Teorema 1.7.11 com a seguinte afirmação: A menos de isomorfismo, existe único grupo cíclico finito de ordem $n$, ou melhor, se $G$ é um grupo cíclico de ordem $n$, então ele é isomorfo a $\mathbb{Z}_n$ e, por isso, é identico a $\mathbb{Z}_n$.

Esta seção se encerrará com o principal teorema dos homomorfismos. O mesmo é base para muitos resultados importantes em álgebra abstrata, nos dando outra forma de mostrar que dois grupos são isomorfos, no caso em que um deles é um grupo quociente.

**Teorema 1.7.12** (Fundamental dos Homomorfismos) *Seja $f : G \longrightarrow K$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker f} \simeq \operatorname{Im} f.$$

**Demonstração:** Seja $F$ a aplicação definida por

$$\begin{array}{rccc} F: & \frac{G}{Ker\ f} & \longrightarrow & \operatorname{Im} f \\ & x(Ker) & \longmapsto & f(x) \end{array}$$

Observe que $F$ está bem definida, pois se $x(Ker\ f) = y(Ker\ f)$ então $xy^{-1} \in Ker\ f$ e portanto $f(xy^{-1}) = e_{G_2}$, o que implica em $f(x) = f(y)$.Além disso, $F$ é um homomorfismo pois,

$$F(x(Kerf).y(Kerf)) = F(xy(Kerf)) = f(xy) = f(x) \circ f(y) = F(x(Kerf)) \circ F(y(Kerf)).$$

Claramente $F$ é sobrejetora pois,

$$\operatorname{Im} F = \{F(xKerf) : x(Kerf) \in \frac{G}{Kerf}\} = \{f(x) : x \in G\} = \operatorname{Im} F.$$

e ainda,

$$KerF = \{x(Kerf) | f(x) = e\} = \{x(Kerf) : x \in Kerf\} = (Kerf)$$

assim $Ker\ F = \{\ e_{\frac{G}{Ker\ f}}\}$, ou seja, $F$ é injetiva. Logo, $\frac{G}{Ker\ f} \backsimeq \operatorname{Im}\ f$. ■

Os dois exemplos seguintes são aplicações do Teorema Fundamental.

**Exemplo 1.7.13** Consideremos os grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$. Mostrar que

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n.$$

**Solução:** Exibindo um homomorfismo sobrejetivo $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ tal que $\ker f = n\mathbb{Z}$. Consideremos então

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ & m & \mapsto & \overline{m}. \end{array}$$

É claro que $f$ é sobrejetiva. Agora, para $m_1, m_2 \in \mathbb{Z}$, segue que

$$f(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m_1} + \overline{m_2} = f(m_1) + f(m_2),$$

ou seja, $f$ é um homomorfismo. Por fim,

$$\begin{array}{rcl} m \in \ker f & \Leftrightarrow & f(m) = \overline{0} \\ & \Leftrightarrow & \overline{m} = \overline{0} \\ & \Leftrightarrow & m \in n\mathbb{Z}. \end{array}$$

Logo, $\ker f = n\mathbb{Z}$ e, pelo Teorema Fundamental, concluímos que $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n$. ♣

**Exemplo 1.7.14** Sejam $GL(n,\mathbb{R})$ e $SL_n(\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : \det(A) = 1\}$. Mostrar que $\frac{GL(n;\mathbb{R})}{SL_n(\mathbb{R})} \backsimeq \mathbb{R}^*$.

**Solução:** Sejam $GL(n,\mathbb{R})$ e $SL_n(\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : \det(A) = 1\}$.Observemos primeiro que, $SL_n(\mathbb{R}) < GL(n;\mathbb{R})$. De fato, sejam $A, B \in SL_n(\mathbb{R})$,

$$|AB| = |A|\,|B| = 1.1 = 1$$

isto é, $A.B \in SL_n(\mathbb{R})$. Além disso,dado $A \in SL_n(\mathbb{R})$,

$$\left|A^{-1}\right| = |A|^{-1} = 1$$

isto é, $A^{-1} \in SL_n(\mathbb{R})$. Logo, $SL_n(\mathbb{R}) < GL(n,\mathbb{R})$.Observemos ainda que $SL_n(\mathbb{R}) \lhd GL(n,\mathbb{R})$. Com efeito, dados $A \in SL_n(\mathbb{R})$ e $B \in GL(n,\mathbb{R})$,

$$\left|BAB^{-1}\right| = |B|\,|A|\left|B^{-1}\right| = |B|\left|B^{-1}\right| = 1,$$

ou seja, $BAB^{-1} \in SL_n(\mathbb{R})$. Donde concluímos que $SL_n(\mathbb{R}) \lhd GL(n,\mathbb{R})$. Agora, consideremos a aplicação $f$ definida da seguinte forma:

$$\begin{array}{rccc} f: & GL(n,\mathbb{R}) & \to & \mathbb{R}^* \\ & A & \mapsto & |A| \end{array}$$

Para $A, B \in GL(n,\mathbb{R})$,

$$f(AB) = |AB| = |A|\,|B| = f(A)f(B),$$

ou seja, $f$ é um homomorfismo. Também, Im $f = \{f(A) : A \in GL(n;\mathbb{R})\} = \{|A| : A \in GL(n;\mathbb{R})\} = \mathbb{R}^*$, ou seja, $f$ é sobrejetora. Por fim,

$$\begin{aligned} \ker f &= \{A \in GL(n;\mathbb{R}) : f(A) = 1\} \\ &= \{A \in GL(n;\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R}). \end{aligned}$$

Dai, pelo Teorema do Homomorfismo,

$$\frac{GL(n;\mathbb{R})}{SL_n(\mathbb{R})} \backsimeq \mathbb{R}^*$$

. ♣

# Capítulo 2

# Grupos Finitos Gerados por Dois Elementos

Os grupos gerados por um elemento, os grupos cíclicos,foram facilmente classificados mediante os isomorfismos existentes entre $\mathbb{Z}$ e $\mathbb{Z}_n$. No entanto a classificação dos grupos gerados por dois elementos pode ser extremamente complicada. Nosso foco então é classificar grupos finitos gerados por dois elementos, isto é, $G = \langle a, b\rangle$ com $a, b$ satisfazendo a seguinte condição

$$ba = a^s b.$$

Considere o grupo das permutações de $\{1, 2, 3\}$, a saber,

$$S_3 = \left\{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\},$$

em que

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Considerando

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Tem-se

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Além disso,

$$\alpha^3 = \beta^2 = Id.$$

Portanto,

$$\begin{cases} S_3 = \langle \alpha, \beta\rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \alpha\beta = \alpha^2\beta. \end{cases} \tag{2.1}$$

Mostraremos que se $G$ é um grupo de ordem seis no qual existem $a$ e $b$ satisfazendo

$$\begin{cases} G = \langle a, b\rangle \\ a^3 = e \\ b^2 = e \\ ab = a^2b, \end{cases}$$

então existem um isomorfismo entre $S_3$ e $G$. Portanto, a menos de isomorfismo, o grupo $S_3$ é único satisfazendo as condições como em (2.1). Resultado análogo será realizado para o grupo das simetrias espaciais de um quadrado. O Teorema 2.0.15 fundamental para estudarmos grupos isomorfos sob condições análogas às de $S_3$.

**Teorema 2.0.15** *Sejam $s \geq 1$ um inteiro e $G_1$ um grupo finito e $a$,$b \in G_1$ tais que $ba = a^sb$. Consideremos $G_2$ um grupo e $\alpha$,$\beta \in G$. Sejam $n, m \geq 1$ tais que*

$$a^n = e, \quad b^m \in \langle a\rangle . \tag{2.2}$$

1. *$b^ta^r = a^{rs^t}b^t, \quad \forall r$,$t \in \mathbb{N}$, e*

$$\langle a, b\rangle = \left\{a^ib^j : 0 \leq i \leq n-1 \quad e \quad 0 \leq j \leq m-1\right\}.$$

2. *Se os inteiros $n, m$ são escolhidos minimalmente satisfazendo as condições em (2.2), então o grupo $\langle a, b\rangle$ tem ordem igual a $n \cdot m$.*

3. *Se os inteiros $n, m$ são escolhidos minimalmente, e se $u$ é um inteiro tal que $b^m = a^u$, então exite um homomorfismo*

$$f : \langle a, b\rangle \to G_2$$

com $f(a) = \alpha$ e $f(b) = \beta$ se, e somente se,

$$\beta\alpha = \alpha^s\beta, \quad \beta^m = \alpha^u \quad \text{e} \quad \alpha^n = e.$$

**Demonstração:** Sendo $G$ um grupo finito, então a existência dos inteiros $n, m$ é garantida. Sendo $G$ um grupo finto, então existem $h, k \in Z$ para os quais $a^h = a^k$ com $h > k$. Desse modo, $a^ha^{-k} = a^{h-k} = e$ e $h - k > 0$; assim, basta considerar $n = h - k$.

1) Mostra-se que $b^ta^r = a^{rs^t}b^t$, ou equivalentemente, $\mathcal{I}_{b^t}(a^r) = a^{rs^t}$, em que, para cada $g \in G_1$, $\mathcal{I}_g : G_1 \to G_1$ é o automorfismo dado por $\mathcal{I}_g(x) = gxg^{-1}$. Vamos usar indução finita sobre $t$. Se $t = 1$, então

$$\mathcal{I}_b(a^r) = (\mathcal{I}_b(a))^r = (a^s)^r = a^{rs},$$

ou seja, o resultado é válido para $t = 1$. Suponha, por hipótese de indução, que o resultado válido para $t - 1$. Desse modo,

$$b^{t-1}a^r = a^{rs^{t-1}}b^{t-1}.$$

Daí,

$$\mathcal{I}_{b^t}(a^r) = \mathcal{I}_b \circ \mathcal{I}_{b^{t-1}}(a^r) = \mathcal{I}_b(a^{rs^{t-1}}) = (\mathcal{I}_b(a))^{rs^{t-1}} = (a^s)^{rs^{t-1}} = a^{rs^t}.$$

Portanto, $b^t a^r = a^{rs^t} b^t$, $\forall r,t \in \mathbb{N}$. Por por outro lado, sejam $a^{l_1} \cdot b^{l_2} \in \langle a, b\rangle$. Pelo algoritmo da divisão, podemos escrever $l_1$ e $l_2$ da forma

$$l_1 = n \cdot q_1 + r_1 \quad \text{com} \quad 0 \leq r_1 \leq n-1$$

e

$$l_1 = m \cdot q_2 + r_2 \quad \text{com} \quad 0 \leq r_2 \leq m-1$$

Por conseguinte, $a^{l_1} = a^{r_1}$ e $b^{l_2} = b^{mq_2} \cdot b^{r_2}$. Como $b^m \in \langle a\rangle$, então $b^m = a^\lambda$ com $\lambda \in \mathbb{Z}$. Portanto,

$$\begin{aligned} a^{l_1} \cdot b^{l_2} &= a^{r_1} \cdot (b^m)^{q_2} \cdot b^{r_2} = a^{r_1} \cdot a^{\lambda q_2} \cdot b^{r_2} \\ &= a^{r_1 + \lambda q_2} \cdot b^{r_2} \end{aligned}$$

Façamos $a^{r_1+\lambda q_2} = a^{\lambda_1}$ com $\lambda \in \{1, 2, \ldots, n-1\}$. Assim,

$$\langle a, b\rangle = \left\{a^i b^j : 0 \leq i \leq n-1 \quad \text{e} \quad 0 \leq j \leq m-1\right\}.$$

Suponha agora que $n$ e $m$ são mínimos satisfazendo as condições em (2.2). Sejam $0 \leq i, k \leq n-1$ e $0 \leq j, l \leq m-1$ tais que $a^i b^j = a^k b^l$. Mostra-se que $i = k, j = l$, implicando em $|G| = n \cdot m$. Suponhamos que $l \leq j$; multiplicando ambos os lado da igualdade $a^i b^j = a^k b^l$ por $a^{-i}$ à esquerda e por $b^{-l}$ à direita, obtemos

$$b^{j-l} = a^{k-i} \in \langle a\rangle$$

com $0 \leq j - l \leq j \leq m-1$. Pela minimalidade de $m$, temos $j - l = 0$. Assim, $j = l$. Consequentemente $a^{k-i} = e$, o pela minimalidade de $n$ implica em $k - i = 0$, isto é, $k = i$.

b) Suponha que exista um homomorfismo $f : \langle a, b\rangle \to G_2$ tal que $f(a) = \alpha$ e $f(b) = \beta$. Como $ba = a^s b$, temos

$$\beta\alpha = f(b)\, f(a) = f(ba) = f(a^s b) = (f(a))^s\, f(b) = \alpha^s \beta,$$

ou seja, $\beta\alpha = \alpha^s\beta$. Da mesma forma, como $a^n = e$ e $b^m = a^u$, temos $\alpha^n = e$ e $\beta^m = \alpha^u$. Reciprocamente, suponha que $\beta\alpha = \alpha^s\beta$, $\alpha^n = e$ e $\beta^m = \alpha^u$. Pela parte a) aplicada a $G_2$ e $\alpha, \beta$ temos que $\beta^t\alpha^r = \alpha^{rs^t}b^t$ para todos $r, t \in \mathbb{N}$. Considere a aplicação

$$\begin{array}{rccc} f: & \langle a, b\rangle & \to & G_2 \\ & a^i b^j & \mapsto & \alpha^i\beta^j \end{array},$$

para $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$, é um homomorfismo. Devido as escolhas mínimas de $n$ e $m$, a aplicação $f$ está bem definida. Para $i, j, k, l \in \mathbb{N}$, escrevendo $j+l = pm+v$ com $0 \leq v \leq m-1$ e $i + ks^j + pu = qn + w$ com $0 \leq w \leq n-1$. Temos

$$\begin{aligned} f\left(\left(a^i b^j\right) \cdot \left(a^k b^l\right)\right) &= f(a^i \cdot (b^j a^k) \cdot b^l) = f\left(a^i \cdot \left(a^{sk^j} b^j\right) \cdot b^l\right) = f(a^{i+sk^j} \cdot b^{j+l}) \\ &= f(a^{i+ks^j} \cdot b^{pm} b^v) = f(a^{i+ks^j} \cdot b^{pm+v}) = f(a^{i+ks^j} \cdot a^{pu} b^v) \\ &= f(a^w b^v) = \alpha^w \beta^v = \alpha^{i+ks^j+pu} \beta^v = \alpha^{i+ks^j} \alpha^{pu} \beta^v \\ &= \alpha^{i+ks^j} \beta^{pm} \beta^v = \alpha^{i+sk^j} \beta^{j+l} = \alpha^i \alpha^{sk^j} \beta^j \beta^l \\ &= \alpha^i \beta^j \alpha^k \beta^l = g = f\left(a^i b^j\right) f\left(a^k b^l\right). \end{aligned}$$

Portanto, $f$ é um homomorfismo. Observe que $f(a) = \alpha$ e $f(b) = \beta$. ■

Considerando a condição de minimalidade de $n$ com em (2.2), temos que $\mathcal{O}(a) = n$. Considera-se esse fato no próximo teorema, o qual é fundamental na classificação dos grupos $G = \langle a, b \rangle$.

**Teorema 2.0.16** *Considere $n, m, s, u \in \mathbb{N}$.*

1. *Sejam $G$ um grupo de ordem $nm$ e $a, b \in G$ tais que*

$$\begin{cases} G = \langle a, b \rangle \\ a^n = e \\ b^m = a^u \\ ba = a^s b. \end{cases} \tag{2.3}$$

   *Então*

$$s^m \equiv (1 \bmod n) \quad e \quad u(s-1) \equiv (0 \bmod n).$$

   *Reciprocamente, se $s^m \equiv (1 \bmod n)$ e $u(s-1) \equiv (0 \bmod n)$, então existe um grupo $G$ de ordem $nm$ que possui dois elementos $a, b$ satisfazendo as condições em (2.3).*

2. *Quando existir um grupo $G$ de ordem $nm$ satisfazendo as condições em (2.3), tal grupo é único a menos de isomorfismos.*

**Demonstração:** 1) Será demonstrado apenas o item 1). Para o item 2) sugere-se a referência de Garcia e Laquain (p.168).

Pelo Teorema 2.0.15, sabemos que $b^m a = a^{s^m} b^m$. Como $b^m \in \langle a \rangle$ e $\langle a \rangle$ é cíclico, portanto abeliano, temos que $b^m$ comuta com $a$ e $ab^m = a^{s^m} b^m$; multiplicando por $a^{-1}$ à esquerda e por $b^{-1}$ à direita de $ab^m = a^{s^m} b^m$,

$$a^{s^m - 1} = e.$$

Portanto, $s^m - 1$ é um múltiplo da ordem de $a$, isto é, $s^m \equiv 1 \bmod n$. Analogamente, temos $ba^u = a^{su}b$. Como $a^u = b^m$, então $a^u \in \langle b \rangle$ ; desse modo, então $a^u b = ba^u = a^{su}b$. Logo,

$$a^{u(s-1)} = e.$$

Portanto, $u\,(s-1)$ é um múltiplo da ordem de $a$, isto é, $u\,(s-1) \equiv 0 \bmod n$.

A próxima proposição é uma consequência do Teorema 2.0.15.

**Proposição 2.0.17** *Sejam $n, m, s, u$ inteiros não negativos. Seja $G$ um grupo de ordem $nm$ que possui dois elementos $a, b$ tais que:*

$$\begin{cases} G = \langle a, b \rangle \\ a^n = e \\ b^m = a^u \\ ba = a^s b. \end{cases}$$

*Consideremos $G_1 = \{(\alpha, \beta) \in G \times G : \beta\alpha = \alpha^s\beta,\ \alpha^n = e,\ \beta^m = \alpha^u\}$, em que $G = \langle \alpha, \beta \rangle$ . Então,*

$$\begin{array}{rccc} \varphi: & Aut\,(G) & \to & G_1 \\ & f & \mapsto & (f(a), f(b)) \end{array}$$

*é uma bijeção.*

**Exemplo 2.0.18** Mostrar que $Aut\,(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \backsimeq S_3$.

**Solução:** Sabemos que $S_3$ é um grupo não cíclico tal que

$$\begin{cases} S_3 = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \alpha\beta = \alpha^2\beta, \end{cases}$$

em que

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Vamos mostrar que $|Aut\,(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})| = 6 = 2{\cdot}3$, com elementos $\varphi_i$,$\varphi_j \in Aut\,(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ satisfazendo

$$\begin{cases} Aut\,(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \langle \varphi_i, \varphi_j \rangle \\ \varphi_i^3 = e \\ \varphi_j^2 = e \\ \varphi_i\varphi_j = \varphi_j^2\varphi_i. \end{cases}$$

Os automorfismos de

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{\alpha_1 = (0,0)\,, \alpha_2 = (0,1)\,, \alpha_3 = (1,0)\,, \alpha_4 = (1,1)\}$$

são dados por:

$$\begin{array}{rccc} \varphi_1: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_2 \\ & \alpha_3 & \mapsto & \alpha_3 \\ & \alpha_4 & \mapsto & \alpha_4 \end{array}, \quad \begin{array}{rccc} \varphi_2: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_4 \\ & \alpha_3 & \mapsto & \alpha_2 \\ & \alpha_4 & \mapsto & \alpha_3 \end{array}, \quad \begin{array}{rccc} \varphi_3: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_2 \\ & \alpha_3 & \mapsto & \alpha_4 \\ & \alpha_4 & \mapsto & \alpha_3 \end{array},$$

e

$$\begin{array}{rccc} \varphi_4: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_3 \\ & \alpha_3 & \mapsto & \alpha_2 \\ & \alpha_4 & \mapsto & \alpha_4 \end{array}, \quad \begin{array}{rccc} \varphi_5: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_3 \\ & \alpha_3 & \mapsto & \alpha_4 \\ & \alpha_4 & \mapsto & \alpha_2 \end{array}, \quad \begin{array}{rccc} \varphi_6: & G & \to & G \\ & \alpha_1 & \mapsto & \alpha_1 \\ & \alpha_2 & \mapsto & \alpha_4 \\ & \alpha_3 & \mapsto & \alpha_3 \\ & \alpha_4 & \mapsto & \alpha_2 \end{array},$$

ou seja, $Aut\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\right)=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6\}$. Agora, temos que

$$\varphi_4^2(\alpha_1)=\alpha_1,\quad \varphi_4^2(\alpha_2)=\alpha_2,\quad \varphi_4^2(\alpha_3)=\alpha_3,\quad \varphi_4^2(\alpha_4)=\alpha_4$$

e

$$\varphi_2^3(\alpha_1)=\alpha_1,\quad \varphi_2^3(\alpha_2)=\alpha_2,\quad \varphi_2^3(\alpha_3)=\alpha_3,\quad \varphi_2^3(\alpha_4)=\alpha_4,$$

ou seja, $\varphi_2^3=\varphi_4^2=\varphi_1$, isto é, $\mathcal{O}\left(\varphi_2\right)=3$ e $\mathcal{O}\left(\varphi_4\right)=2$. Além disso,

$$\varphi_6=\varphi_4\cdot\varphi_2,\quad \varphi_5=\varphi_2\cdot\varphi_2,\quad \varphi_3=\varphi_4\cdot\varphi_2^2$$

Como $\varphi_2,\varphi_4\in\langle\varphi_2,\varphi_4\rangle$, segue que $Aut\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\right)=\langle\varphi_2,\varphi_4\rangle$. Temos também que $\varphi_2\varphi_4=\varphi_2^2\varphi_4$. Portanto,

$$\begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}=\langle\varphi_2,\varphi_4\rangle \\ \varphi_4^3=e \\ \varphi_4^2=e \\ \varphi_2\varphi_4=\varphi_2^2\varphi_4. \end{cases}$$

Pelo Teorema 2.0.16 parte 2, concluímos que

$$Aut\left(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\right)\backsimeq S_3.$$

## 2.1 Caracterização de Todos os Grupos $G$ com $|G|\leq 8$

Nesta seção, faremos uso dos resultados obtidos de modo a abordar o problema central do trabalho, ou seja, a caracterização dos grupos $G$ tais que $|G|\leq 11$.

Se $|G|=1$, então $G=\{e\}$ é o único grupo com um elemento. Vamos por isso supor que $2\leq|G|\leq 11$.

### 2.1.1 Grupos de ordem $p$ com $p$ primo

Consideremos $|G|=p$ com $p=2,3,5$, ou 7. Pelo Corolário 1.5.6, sabemos que $G$ é cíclico e, pelo Teorema 1.7.11, $G$ é isomorfo a $\mathbb{Z}_p$. Portanto,

$$G\simeq\mathbb{Z}_p.$$

### 2.1.2 Grupos de ordem 4

Realizaremos o estudo dos grupos de ordem quatro por meio dos grupos aditivos $G_1 = \mathbb{Z}_4$ e $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, os seja,

$$G_1 = \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \quad \text{e} \quad G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}.$$

Esses não são isomorfos, pois $\mathbb{Z}_4$ é cíclico ($\mathbb{Z}_4 = \langle\overline{1}\rangle$), enquanto $\mathbb{Z}_2 \times \mathbb{Z}_2$ não o é, uma vez que todo elemento $x \in G_2 - \{(\overline{0}, \overline{0})\}$ tem ordem dois. Vamos mostrar que, a menos de isomorfismos, $G_1$ e $G_2$ são os únicos grupos de ordem 4.

Consideremos $G$ um grupo de ordem quatro, digamos, $G = \{e, a, b, c\}$. Se $G$ possui um elemento de ordem 4, então ele é cíclico e, desse modo,

$$G \simeq \mathbb{Z}_4.$$

Caso contrário, pelo teorema de Lagrange, cada elemento $x$ em $G$, $x \neq e$, tem ordem 2, pois a ordem de $x$ divide quatro.

Vamos construir a tábua de $G$. Pelo Corolário 1.5.7, todo grupo de ordem quatro é abeliano. Desse modo, a questão principal é determinar o valor de $ab$. Temos que $ab \in \{e, a, b, c\}$ . Consideremos as seguintes condições:

**a)** Se $ab = e$, então $a = b^{-1}$. Mas, sendo $b$ de ordem 2,então $b = b^{-1}$, ou seja, $a = b$, o que não é verdade.

**b)** Se $ab = a$, então $b = e$, o que é um absurdo. Da mesma forma, tem-se que $ab \neq b$.

Portanto, $ab = c = ba$, pois $G$ é abeliano. Da mesma forma, $ac = b = ca$ e $bc = a = cb$. A tábua de $G$ é então dada por

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

(2.4)

Observe que $|G| = 4 = 2{\cdot}2$. Considerando $n = 2$ e $m = 2$, e levando em consideração a Tábua em (2.4), obtemos

$$\begin{cases} G = \langle a, b\rangle \\ a^2 = e \\ b^2 = a^2 \\ ba = ab. \end{cases}$$

Da mesma forma, para o grupo $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$, com $\alpha = (\overline{0}, \overline{1})$ e $\beta = (\overline{1}, \overline{0})$,temos que

$$\begin{cases} G_2 = \langle\alpha, \beta\rangle \\ \alpha^2 = \alpha + \alpha = e = (\overline{0}, \overline{0}) \\ \beta^2 = \beta + \beta = \alpha^2 \\ \beta + \alpha = \alpha + \beta. \end{cases}$$

Portanto, pelo item 2 do Teorema 2.0.16, concluímos que

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Isso pode ser verificado observando que a função

$$\begin{array}{rccc} \varphi: & G & \to & G \\ & (\overline{0},\overline{0}) & \mapsto & e \\ & (\overline{1},\overline{0}) & \mapsto & a \\ & (\overline{0},\overline{1}) & \mapsto & b \\ & (\overline{1},\overline{1}) & \mapsto & c, \end{array}$$

é um isomorfismo. Portanto, a menos de isomorfismos, $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ são os únicos grupos de ordem 4.

### 2.1.3 Grupos de ordem 6

Sabemos que $\mathbb{Z}_6$ e $S_3$ são ambos de ordem seis e não isomorfos, pois $\mathbb{Z}_6$ é cíclico $S_3$ não o é. grupos de ordem 6. Vamos mostrar que, a menos de isomorfismos, eles são os únicos grupos de ordem 6. Para tanto, seja $G$ um grupo qualquer de ordem 6. Mostremos que $G \simeq \mathbb{Z}_6$ ou $G \simeq S_3$. Isso consiste em demonstrar as duas seguintes proposições:

**Proposição 2.1.1** *O grupo $G$ possui um elemento $\alpha$ de ordem 3 .*

**Demonstração:** Vamos considerar os seguintes casos:

**Caso 1** O grupo $G$ é cíclico.

Neste caso, temos que $G = \langle\alpha\rangle$ para algum $\alpha \in G$ com $\mathcal{O}(\alpha) = 6$. Assim, basta considerarmos o elemento $\beta = \alpha^2$, e então $\mathcal{O}(\beta) = 3$.

**Caso 2** O grupo $G$ não é cíclico.

Por absurdo, suponhamos que $\mathcal{O}(\beta) \neq 3$ para todo $\beta \in G$. Assim, pelo Teorema de Lagrange, todo elemento $x \in G - \{e\}$ tem ordem 2. Por isso, $x = x^{-1}$ e, de acordo com a demostração do Corolário 1.5.7, o grupo $G$ é abeliano. Considerando dois elementos $a, b \in G - \{e\}$, temos que o conjunto $H = \{e, a, b, ab\}$ é um subgrupo de ordem 4 de $G$. Isto contraria o Teorema de Lagrange. Assim, existe $\alpha \in G$ tal que $\mathcal{O}(\alpha) = 3$. ■

**Proposição 2.1.2** *O grupo $G$ possui pelo menos um elemento $\beta$ de ordem 2 e $G = \langle\alpha, \beta\rangle$.*

**Demonstração:** Análogo ao que foi feito na demonstração da Proposição 2.1.1, vamos estudar os seguintes casos:

**Caso 1** O grupo $G$ é cíclico

Assim, temos que $G = \langle\gamma\rangle$ e $\beta = \gamma^3$ é tal que $\gamma^3 \notin \langle\gamma^2\rangle$, pois $\langle\gamma^2\rangle = \{e, \gamma^2, \gamma^4\}$; daí $|\langle\gamma^2, \gamma^3\rangle| > 3$ e, pelo Teorema de Lagrange, $|\langle\gamma^2, \gamma^3\rangle|$ divide 6. Isso implica que portanto $G = \langle\gamma^2, \gamma^3\rangle = \langle\alpha, \beta\rangle$, em que $\alpha = \gamma^2$.

**Caso 2** O grupo $G$ não é cíclico.

Pela Proposição 2.1.1, existe $\alpha \in G$ tal que $\mathcal{O}(\alpha) = 3$. Consideremos $\beta \in G$ tal que $\beta \notin \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$. Agora, é fácil verificar que os seis elementos $e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta$ são todos distintos. Por exemplo, se $\alpha\beta = \alpha^2\beta$, então $\alpha = \alpha^2$, isto é, $\alpha = e$, o que não é possível. Os outros casos são analisados da mesma forma.

O elemento $\beta$ pode ter ordem dois ou três; mostremos que $\mathcal{O}(\beta) = 2$. Observe que $\beta^2 \in \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$, pois caso contrário, $\beta^2 \in \{\beta, \alpha\beta, \alpha^2\beta\}$ e, portanto, $\beta \in \{e, \alpha, \alpha^2\}$ o que é absurdo, pois $\beta \notin \langle\alpha\rangle$. Suponhamos que $\mathcal{O}(\beta) = 3$. Daí,

$$e = \beta^3 \Rightarrow \beta = \beta^4 = \left(\beta^2\right)^2 \in \left\{e, \alpha, \alpha^2\right\},$$

o que não é possível. Portanto, a ordem $\beta$ de é igual a 2.

Dessa forma, concluímos que

$$\begin{cases} |G| = 6 \\ G = \langle\alpha, \beta\rangle \\ \alpha^3 = e \\ \beta^2 = e. \end{cases}$$

Vamos agora considerar as possibilidades para o produto $\beta\alpha$. Observamos que $\beta\alpha \notin \{e, \alpha, \alpha^2, \beta\}$, pois caso contrário, teríamos $\beta = \alpha^{-1}$, $\beta = e$, $\beta = \alpha$ ou $\alpha = e$. Isso conduz a uma contradição. Por conseguinte, $\beta\alpha = \alpha\beta$ ou $\beta\alpha = \alpha^2\beta$. . Temos as duas possibilidades:

$$\begin{cases} |G| = 6 = 3.2 \\ G = \langle\alpha, \beta\rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases} \quad \text{e} \quad \begin{cases} |G| = 6 = 3.2 \\ G = \langle\alpha, \beta\rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta. \end{cases} \tag{2.5}$$

Portanto, pelo item 2 do Teorema 2.0.16, em cada caso, temos no máximo um grupo, amenos de isomorfismos, satisfazendo as condições em (2.5). Observamos que o grupo $G = \mathbb{Z}_6$ satisfaz as condições do Caso 1; e o grupo $G = S_3$ satisfaz as condições do Caso 2. Notamos também que o grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ também satisfaz as condições do caso 1) e, pela unicidade, concluímos que $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$. ■

### 2.1.4 Grupos de ordem 8

Vamos agora estudar os grupos $G$ tais que $|G| = 8$. Inicialmente, observamos que os grupos $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e $D_4$ são todos de ordem oito.possuem 8 elementos. Eles não são isomorfos entre si. De fato, temos que o grupo $\mathbb{Z}_8$ é cíclico; isto significa que existe $\alpha \in \mathbb{Z}_8$ tal que $\mathcal{O}(\alpha) = 8$. O grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$ não é cíclico, porém abeliano e possui elementos cuja ordem é 4 ou 2. O grupo $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{a}, \overline{b}, \overline{c}) : \overline{a}, \overline{b}, \overline{a} \in \mathbb{Z}_2\}$ não é cíclico, pois todos seus elementos diferentes da identidade têm ordem. Por fim o grupo $D_4$ das simetrias espaciais de um quadrado, não é abeliano. Portanto, esses grupos não são isomorfos entre si. Não é difícil mostrat que o conjunto $Q_3$, dado por

$$Q_3 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \ \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \ \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\},$$

em que $i \in \mathbb{C}$ é tal que $i^2 = -1$, é um grupo multiplicativo, chamado **grupo dos quatérnios** $Q_3$.

Vamos mostrar que esses grupos são, a menos de isomorfismo, os únicos grupos de ordem oito — totalizando cinco grupos de ordem oito. O grupo $Q_3$ não é isomorfo a nenhum dos grupos $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, pois esses são abelianos. Para mostar que $Q_3$ não é isomorfo a $D_4$, basta notar que $D_4$ possui cinco elemento de ordem 2, enquanto $Q_3$ possui apenas um elemento de ordem 2, a saber

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

O grupo $Q_3$ é caracterizado pela relação´

$$\begin{cases} |Q_3| = 8 \\ Q_3 = \langle A, B \rangle \\ A^4 = id \\ B^2 = A^2 \\ BA = A^3 B, \end{cases}$$

em que

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{e} \quad id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

O grupo $D_4$ e $Q_3$ não são isomorfos. De fato, notemos

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \Rightarrow \alpha^2 = id$$

e

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \Rightarrow \beta^2 = id,$$

ou seja, $\alpha$ e $\beta$ têm ordem dois. Por outro lado,

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in Q_3$$

é o único elemento de $Q_3$ que tem ordem 2. Isso é suficiente para mostrar que os grupos $D_4$ e $Q_3$ não são isomorfos.

Consideremos $G$ um grupo qualquer de ordem 8. Dado $\alpha \in G = \{e\}$, temos pelo teorema de Lagrange as possíbilidades:

$$\mathcal{O}\alpha) = 2, \quad \mathcal{O}\alpha) = 4 \quad \text{ou} \quad \mathcal{O}\alpha) = 8.$$

Vamos estudar esses casos.

**Caso 1** $G$ possui um elemento de ordem 8.

Neste caso, temos que $G$ é cíclico e, por isso, $G \simeq \mathbb{Z}_8$.

**Caso 2** $G$ não possui elemento de ordem 8.

Desse modo, dado $\alpha \in G = \{e\}$, segue que $\mathcal{O}\alpha) = 2$ ou $\mathcal{O}\alpha) = 4$. Vamos considerar dois casos separadamente.

**Caso 2.1** $G$ não possui nenhum elemento de ordem 4

Neste caso, todos os elementos $\neq e \in G$ são de ordem 2, e o grupo $G$ é abeliano. Seja $\alpha \neq e$ com $O(a) = 2$; assim $H = \{e, a\}$ é um subgrupo de $G$. Consideremos agora $\beta \in G - H$. Logo, $K = \{e, a, b, ab\}$ é um subgrupo de $G$. Para $\gamma \in G - K$, temos $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\} = \left\{a^i b^j c^k : i, j, k \in \{0, 1\}\right\}$.

A aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_2^3 & \to & G \\ & \left(\overline{i}, \overline{j}, \overline{k}\right) & \mapsto & \alpha^i \beta^j \gamma^k \end{array}$$

é um isomorfismo de grupo, em que $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Verifiquemos um caso de compatibilidade entre as estruturas dos grupos. Façamos $a = (1, 0, 0)$ e $b = (0, 1, 0)$; logo,

$$\varphi(a + b) = \varphi(1, 1, 0) = \alpha\beta = \varphi(1, 0, 0) . \varphi(0, 1, 0).$$

Os outros casos são tratados da mesma forma. A função $\varphi$ é sobrejetora, uma vez que $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\}$, e injetora, pois

$$\begin{aligned} &\varphi(0, 0, 0) = e, \quad \varphi(1, 0, 0) = a, \quad \varphi(0, 1, 0) = b, \quad \varphi(0, 1, 1) = bc, \\ &\varphi(0, 0, 1) = c, \quad \varphi(1, 1, 0) = ab, \quad \varphi(1, 0, 1) = ac, \quad \varphi(1, 1, 1) = abc. \end{aligned}$$

Portanto, $\mathbb{Z}_2^3 \simeq G$.

**Caso 2.2** $G$ possui um elemento de ordem 4.

Sejam $\alpha \in G$ tal que $\mathcal{O}(\alpha) = 4$ e o subgrupo $H = \langle \alpha \rangle$. Consideremos $\beta \in G - H$ e o subgrupo $K$ de $G$ gerado por $\alpha$ e $\beta$, isto é, $K = \langle \alpha, \beta \rangle$. Como $\beta \notin H$, temos que $|K| > 4$ e, pelo teorema de Lagrange, $|K|$ divide 8; logo $K = G = \langle a, b \rangle = \{e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, a^3\beta\}$. Por isso, $\beta^2 \in H$, uma vez que $\beta^2 \notin \{\beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$. Também temos que $\beta\alpha \notin \{e, \alpha, \alpha^2, \alpha^3\}$, pois $\beta \notin H$. Dessa forma,

$$\begin{cases} |G| = 8 \\ G = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = \alpha^u, \quad \text{para algum } u \in \{0, 1, 2, 3\} \\ \beta\alpha = \alpha^s\beta, \quad \text{para algum } s \in \{1, 2, 3\}. \end{cases}$$

Vamos analisar agora as possibilidades para $u \in \{0, 1, 2, 3\}$ e $s \in \{1, 2, 3\}$. Inicialmente, temos $\mathcal{O}(\beta\alpha\beta^{-1}) = \mathcal{O}(\alpha) = 4$, de modo que $s = 1$ ou $s = 3$. Por outro lado, $\beta^2 \notin \{\alpha, \alpha^3\}$, pois caso contrário, $\beta^2$ teria ordem 4 e $\beta$ teria ordem 8, o que não é possível, ou $\beta$ teria ordem 4, o que implicaria em $O(\beta^2) = 2$, o que é um absurdo, pois $\beta^2 = \alpha^u$ com $u \in \{0, 1, 2, 3\}$. Concluímos que $u = 0$ ou $u = 2$ e $s = 1$ ou $s = 3$.

Se $u = 0$, temos dois casos correspondentes a $s = 1$ e $s = 3$. Portanto,

$$(1) \quad \begin{cases} |G| = 8 \\ G = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases} \quad \text{e} \quad (2) \quad \begin{cases} |G| = 8 \\ G = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^3\beta. \end{cases} \tag{2.6}$$

Pela item 2 do Teorema 2.0.16, segue que em cada caso em (2.6), existe no máximo um grupo, a menos de isomorfismo, satisfazendo as condições. Como exemplo, para o caso (1), temos o grupo $G = \mathbb{Z}_4 \times \mathbb{Z}_2$; e para o caso (2), temos $G = D_4$.

Se $u = 2$, então

$$(3) \quad \begin{cases} |G| = 8 \\ G = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = \alpha^2 \\ \beta\alpha = \alpha\beta \end{cases} \quad \text{e} \quad (4) \quad \begin{cases} |G| = 8 \\ G = \langle \alpha, \beta \rangle \\ \alpha^4 = e \\ \beta^2 = \alpha^2 \\ \beta\alpha = \alpha^3\beta. \end{cases} \tag{2.7}$$

Da mesma forma, concluímos pelo item 2 do Teorema 2.0.16 que, para cada caso em (2.7), existe no máximo um grupo, a menos de isomorfismo. Para o caso (3), considere $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, e no caso (4), $G = Q_3$.

Portanto , obtemos que, a menos de isomorfismo existem 5 grupos de ordem 8, que são: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2^3$, $D_4$ e $Q_3$.

**Observação 2.1.3** Os casos (1) e (3) afirmam que um mesmo grupo pode ser apresentado,por meio de geradores e relações diferentes. Isto é, mudando os geradores podemos alterar as relações entre eles.

## 2.2 Conclusão

Este trabalho proporcionou a apresentação de uma parte importante da teoria dos grupos, como os conceitos de grupos finitos e do Teorema de Lagrange, resultados importantes na apresentação um pouco mais detalhada da classificação de Grupos de Ordem $\leq 8$. Este estudo possibilitou o contato com alguns conceitos mais avançados da Teoria dos grupos, tendo como foco principal a classificação de todos os grupos de ordem $\leq 8$.

# Bibliografia


[1] Baumgart, J. K. *Tópicos de História da Matemática*; trad. Hygino H. Domingues — Atual Editora, 1992.

[2] Boyer, C. B. *História da Matemática*. $2^a$.ed. São Paulo. Edgard Blücher, 2003.

[3] Garcia, A. e Lequain, Y. *Elementos de Álgebra*. Projeto Euclides, IMPA, $3^{\underline{nd}}$. ed., 2005.

[4] Gonçalves, A. *Introdução à Álgebra*. Projeto Euclides, $5^{\underline{nd}}$. ed., 2009.

[5] Fraleigh, J. B. *A First Course In Abstract Algebra*. 7th ed. Pearson Education, Inc, 2003.

[6] Domingues, H. H. *Álgebra Moderna*. $4^a$.ed. — São Paulo: Atual Editora, 2003.