UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII - GOVERNADOR ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA EM MATEMÁTICA

LÍVIA PEDRO DA SILVA

CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 11$

PATOS - PB
2017

Lívia Pedro da Silva

CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 11$

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciada em Matemática.

Área de Concentração: Matemática

Orientador: Prof. Me. José Ginaldo de Souza Farias

PATOS - PB
2017

S586c Silva, Livia Pedro da.
Caracterização dos grupos G com |G| ≤ 11 [manuscrito] : / Livia Pedro da Silva. - 2017. 75 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2017.

"Orientação: Prof. Me. José Ginaldo de Souza Farias, Coordenação do Curso de Matemática - CCEA."

1. Grupos Cíclicos. 2. Teorema de Lagrange.
3. Homomorfismos de Grupos. 4. Grupos Finitamente Gerados.

21. ed. CDD 510

Lívia Pedro da Silva

CARACTERIZAÇÃO DOS GRUPOS G COM $|G| \leq 11$.

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura Plena emMatemática da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Matemática.

Aprovado em 07 de dezembro de 2017

Prof. Me. José Ginaldo de Souza Farias (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. Me. Arlandson Matheus Silva Oliveira (Examinador)
Universidade Estadual da Paraíba (UEPB)

Prof. Francisco Anderson Mariano da Silva (Examinador)
Universidade Estadual da Paraíba (UEPB)

Aos meus pais Joselita e Francisco, dedico.

AGRADECIMENTOS

Em primeiro lugar à DEUS, o Alfa e Ômega, o Princípio e o Fim de tudo; por todas as maravilhas em minha vida.

À minha mãe Joselita Francisco da Silva, ao meu pai Francisco Pedro da Silva por todo o esforço feito para que eu pudesse estudar na UEPB, por apoiarem e acreditarem sempre em mim, vocês são o motivo das minhas conquistas; aos meus irmãos Islla Pedro e Pedro Antônio por todo o incentivo e carinho, a minha sobrinha Luna Lorena luz da minha vida e à minha família.

Ao meu namorado Jair Damascena pelo apoio, incentivo, companheirismo e a contribuição na formatação do trabalho.

Ao professor orientador Me. José Ginaldo de Souza Farias pela sua dedicação a orientação, aos professores Arlandson Matheus (obrigada por tudo, todas as considerações e aprendizado), Francisco Anderson e Francisco Sibério pelas contribuições.

Ao professor Me. Vilmar Vaz da Silva pelas disciplinas ministradas, por todo incentivo e amizade.

Aos meus amigos, em especial Marcos Thadeu, Creuzenira, Luciclaudia, Rubea e Aline Marques pelo apoio, incentivo e amizade.

Aos professores da UEPB Campus VII que contribuiram com a minha formação acadêmica, aos colegas de classe. Por fim, a todos que contribuiram de alguma maneira para o desenvolvimento deste trabalho e da minha graduação.

“ Toda a educação científica que não se inicia com a Matemática é, naturalmente, imperfeita na sua base.”
(Auguste Comte).

RESUMO

Nesta monografia caracterizaremos os grupos finitos gerados por dois elementos de ordem menor ou igual que 11. Exibiremos conceitos elementares da Teoria dos Grupos, tais como o de grupo cíclico, com o propósito de estudar grupos que constituem uma classe mais abrangente, grupos finitos gerados por dois elementos. Nessa perspectiva, objetiva-se a utilização dessa classe de grupo, juntamente com o Teorema de Lagrange, este que possibilita a classificação dos grupos finitos não cíclicos para caracterização e estudo de tais grupos.

Palavras Chave: Grupos; Grupos Cíclicos; Teorema de Lagrange; Homomorfismos de Grupos; Grupos Finitamente Gerados.

ABSTRACT

In this monograph we will characterize the finite groups generated by two elements of order smaller or same that 11. Being exhibited elementary concepts of the Theory of the Groups, such as the one of cyclic group, with the purpose of studying groups that constitute an including class, finite groups generated by two elements. In that perspective, the use of that group class is aimed at, together with the Theorem of Lagrange, this that makes possible the classification of the finite groups no cyclic for characterization and study of such groups.

Keywords: Groups; Cyclic Groups; Theorem of Lagrange; Homomorphisms of Groups; Finitely Generated Groups.

Sumário

Introdução

A Álgebra é um dos principais ramos da Matemática Pura. O estudo de Grupos é o ponto inicial da Álgebra Abstrata, seu conceito é de suma importância para a Matemática. O processo que levou à introdução de um aspecto genuinamente abstrato em álgebra teve início no ano de 1815, quando matemáticos da Universidade de Cambridge, tais como Charles Babbage (1792-1871), George Peacock (1791-1858) e John Herschel (1792-1878) fundaram a Analytical Society, cuja contribuição fundamental foi repensar e discutir os fundamentos da álgebra.

O estudo das permutações se iniciou com os trabalhos de Joseph Louis Lagrange (1736 - 1813) sobre equações algébricas em 1770, seguido das contribuições de Paolo Ruffini (1765 - 1822) e Niels Henrik Abel (1802 - 1829). Mas primeiro a considerar explicitamente grupos de permutações foi Evariste Galois (1811 - 1832), que usou em 1830 o termo "grupo" em seu sentido técnico em matemática, hoje clássico. Ademais, Agustin Cauchy notou a importância inerente dos grupos de permutações, escreveu vários artigos a respeito, dentre 1844 a 1846, os quais influenciou Arthur Cayley, o primeiro a formular o conceito abstrato de grupo em 1954.

Um grupo é uma estrutura algébrica relativamente simples, com relação ao número de operações binárias, seu conceito é uma das ideias centrais da matemática, a teoria dedicada ao seu estudo - Teoria dos Grupos-, envolve tópicos de complexidade considerável, com vários problemas em aberto.

Nesta monografia pretende-se estudar os grupos finitos gerados por dois elementos, tendo em vista que nosso interesse maior será a caracterização destes grupos de ordem até 11. Dividido em quatro capítulos, o capítulo 1 é voltado a conceitos preliminares essenciais para o desenvolvimento do nosso estudo, tais como os de Grupo,

Subgrupos e Grupos Cíclicos. No que segue, o capítulo 2 nos dá a noção de isomorfismo, que nos fornece uma forma de verificar quando dois grupos são possuem as mesmas propriedades algébricas e o contato com o Teorema de Lagrange, cruciais para o estudo e classificação desses grupos finitos. No capítulo 3 aborda-se grupos finitos gerados por dois elementos , a saber $G = \langle a, b \rangle$ com a e b satisfazendo a relação $ba = a^s b$, de grande utilidade para o capítulo 4 com o desfecho do tema central do presente trabalho.

Capítulo 1

Grupos

Neste Capítulo daremos uma breve introdução à Teoria dos Grupos. Supõe-se já conhecidos conceitos preliminares tais como os de conjuntos, relações e funções, encontrados na referência [8]. Um grupo é uma estrutura algébrica relativamente simples, no que diz respeito ao número de operações binárias (possui somente uma operação), daremos foco aos grupos finitos, seu comportamento. O estudo será feito em torno dessas estruturas com suas devidas operações, as quais analizaremos se possuem mesmas propriedades.

1.1 Operação Binária

Definição 1.1 *Seja A um conjunto não vazio. Diz-se* ***operação binária*** *sobre A uma função $f : A \times A \to A$.*

Definição 1.2 *Sejam $\star$ uma operação sobre A e H um subconjunto de A. Quando*

$$a \star b \in H, \ \forall a, b \in H,$$

H é dito ***fechado sob*** *$\star$ e chama-se* ***operação induzida*** *de $\star$ sobre H a restrição de $\star$ ao conjunto H.*

Definição 1.3 *Diz-se uma* ***estrutura algébrica*** *um conjunto não vazio munido com uma ou mais operações.*

Notação: $(A, \star, \triangle, *, \blacktriangle, \blacksquare, \clubsuit ...)$

1.2 Grupos

Definição 1.4 *Um conjunto G não vazio munido de uma operação $\star$, definida entre pares de G, denotada por,*

$$\begin{array}{rccc} \star: & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x \star y \end{array}$$

diz-se ***grupo*** *quando as seguintes propriedades são satisfeitas:*

(G1) $a \star (b \star c) = (a \star b) \star c, \quad \forall a, b, c \in G$; *(Associatividade);*

(G2) $\exists\ e \in G$ *tal que* $a \star e = e \star a, \quad \forall a \in G$; *(Existência de elemento neutro);*

(G3) $\forall a \in G, \exists\ b \in G$ *tal que* $a \star b = b \star a = e$, *onde* $b = a^{-1}$; *(Existência de inverso para todo elemento).*

Onde o elemento neutro, identidade de (G, $\star$), denotado por e e o inverso de a denotado por a^{-1} são únicos.

Definição 1.5 *Um grupo $(G, \star)$ é* ***abeliano*** *ou* ***comutativo*** *se satisfeita a condição*

$$a \star b = b \star a, \ \forall\ a, b \in G.$$

Observação 1.1 Quando não se há dúvida quanto a operação considerada sobre G, bem definida, simplificamos a notação por G simplesmente.

Observação 1.2 Por questão de praticidade frequentemente chamamos a operação $\star$ de **produto**, com notação $a \cdot b$ ou ab, ao invés de $a \star b$, G com esta operação é um grupo **multiplicativo**, de maneira análoga os grupos **aditivos**, com operações indicadas por $+$.

Observação 1.3 Para grupos aditivos o inverso será denotado por $-a$, para grupos multiplicativos permanece a notação a^{-1}.

Vejamos alguns exemplos e contra exemplos de grupos:

Exemplo 1.1 $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ com adições usuais são exemplos de grupos abelianos.

Exemplo 1.2 $(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$ são grupos multiplicativos abelianos.

Exemplo 1.3 Todo espaço vetorial é um grupo abeliano.

Exemplo 1.4 Para cada $n \in \mathbb{N}$, o conjunto $\mathbb{Z}_n$, dos inteiros módulo n, com adição dada por,

$$\begin{array}{rccc} + : & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\overline{a}+\overline{b}) & \longmapsto & \overline{a}+\overline{b}=\overline{a+b} \end{array}$$

é um grupo aditivo abeliano.

Exemplo 1.5 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. Com efeito,

1) $X + (Y + Z) = (X + Y) + Z, \quad \forall X, Y, Z \in G.$

2)$X + 0 = 0 + X, \quad \forall X \in G$, onde

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

é a matriz nula.

3) $X + Y = Y + X = 0$, tal que

$$X = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$$

e a matriz

$$Y = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix},$$

sua inversa. Logo G é grupo. A comutatividade da adição em G é imediata.

Exemplo 1.6 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,

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

é o neutro do produto, pois

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

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 1.7 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

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

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 fechado 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-beliano. Similarmente, tem-se grupos lineares gerais $GL_n(\mathbb{Q})$ e $GL_n(\mathbb{C})$.

Exemplo 1.8 Seja $G = \mathbb{R}^{\mathbb{R}}$ [1] munido de sua adição usual, isto é, para $f, g \in G$ e $x \in \mathbb{R}$,

$$(f + g)(x) = f(x) + g(x).$$

Esta operação é claramente comutativa. Considerando $f, g, h \in G$ e a adição usual sobre $\mathbb{R}$ ser associativa, temos para $x \in \mathbb{R}$,

$$\begin{aligned} [f + (g + h)](x) = f(x) + (g + h)(x) &= f(x) + g(x) + h(x) \\ &= (f(x) + g(x)) + h(x) \\ &= (f + g)(x) + h(x) \\ &= [(f + g) + h](x), \end{aligned}$$

de maneira que $f + (g + h) = (f + g) + h)$ e, assim a adição em G é associativa. A função nula $0 \in G$ satisfaz

$$(f + 0) = f(x) + 0(x) = f(x) + 0 = f(x),$$

portanto, $f + 0 = f$, então 0 é o elemento neutro da adição. Por fim, a função $-f \in G$ dada por $(-f)(x) = -f(x), \ \ \forall x \in \mathbb{R}$, é um inverso aditivo de f, pois

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0$$

[1] $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \longrightarrow \mathbb{R}\}$.

assim, $f + (-f) = 0$. Logo, $(\mathbb{R}^{\mathbb{R}}, +)$ é um grupo abeliano.

1.3 Propriedades Elementares de um Grupo

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

Proposição 1.1 *Seja $(G, \star)$ um grupo Então dados $a, b, c \in G$,*

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

ou seja, são válidas as leis do cancelamento à esquerda e a direita em G.

Demonstração: Como G é um grupo, existe $a_1 \in G$ tal que $a_1 \star a = e = a \star a_1$, assim para $a, b, c \in G$, temos:

$$\begin{array}{rcccl}
a \star b = a \star c & \Rightarrow & a_1 \star (a \star b) & = & a_1 \star (a \star c) \quad (operando\ com\ a_1\ \ esquerda) \\
& \Rightarrow & (a_1 \star a) \star b & = & (a_1 \star a) \star c \quad (G_1) \\
& \Rightarrow & e \star b & = & e \star c \quad (G_3) \\
& \Rightarrow & b & = & c \quad (G_2)
\end{array}$$

$$\begin{array}{rcccl}
b \star a = c \star a & \Rightarrow & (b \star a) \star a_1 & = & (c \star a) \star a_1 \quad (operando\ com\ a_1\ \ direita) \\
& \Rightarrow & b \star (a \star a_1) & = & c \star (a \star a_1) \quad (G_1) \\
& \Rightarrow & b \star e & = & c \star e \quad (G_3) \\
& \Rightarrow & b & = & c \quad (G_2)
\end{array}$$

Logo, são válidas as leis do cancelamento à esquerda e à direita em G.

Proposição 1.2 *Seja $(G, \star)$, um grupo e $a, b \in G$ Então as equações lineares $a \star x = b$ e $x \star a = b$ tem única solução em G.*

Demonstração: Seja $a_1 \in G$ tal que $a_1 \star a = e$, temos:

$$\begin{aligned} a \star x_0 &= b \\ a_1 \star (a \star x_0) &= a_1 \star b \\ (a_1 \star a) \star x_0 &= a_1 \star b \\ e \star x_0 &= a_1 \star b \end{aligned}$$

o elemento $x_0 = a_1 \star b \in G$ é tal que,

$$\begin{aligned} a \star (a_1 \star b) &= (a \star a_1) \star b \\ &= e \star b \\ &= b \end{aligned}$$

assim, x_0 é uma solução da equação linear $a \star x = b$ Suponhamos que $x_1 \in G$ seja também solução, como $a \star x_0 = b$ e $a \star x_1 = b$, temos que $a \star x_0 = a \star x_1$ Pela proposição anterior $x_0 = x_1$, logo a solução é única. De modo análogo mostra-se a existência e unicidade de solução para $x \star a = b$.

Proposição 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 $a^{-1} \in G$ tal que,

$$a^{-1} \star a = a \star a^{'} = e.$$

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

$$\begin{aligned} e &= e^{'} \star e \quad \text{(pois } e^{'} \text{ o elemento neutro de } \star) \\ &= e^{'} \qquad \text{(pois } e \text{ o elemento neutro de } \star .) \end{aligned}$$

2) Seja $b \in G$ tal que $b \star a = e$. Como $a^{'} \star a = e$, então pela Proposição 1.1, obtemos

$$b \star a = a^{'} \star a \Rightarrow b = a^{'}.$$

Por isso, em grupo $(G, \star)$, o elemento neutro da operação e o inverso de cada elemento do conjunto 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 $(\mathbb{Z}, \star)$, temos que o inverso de $a = 5$ é $-a = -5$, onde $5+(-5) = 0 = e$; e para o grupo $(\mathbb{R}^*, \cdot)$ o inverso de $a = 5$ é $a^{-1} = 5^{-1} = \frac{1}{5}$, onde $5 \cdot 5^{-1} = 1 = e$.

Observação 1.4 Em decorrência da Proposição 1.2, para mostrar que um elemento de $e \in G$ 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 qeu b é o inverso de a, basta mostrar que $b \star a = e$ ou $a \star b = e$.

Proposição 1.4 *Considere um grupo* $(G, \cdot)$. *Então:*
1) $(a^{-1})^{-1} = a, \forall a \in G$.
2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}, \forall a, b \in G$.

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

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

Usando a propriedade associativa da operação em G e omitindo os parênteses 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

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

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

O resultado do item 2) da Proposição 1.4 pode ser generalizado da seguinte forma: Sejam $a_1, a_2, \ldots, a_n \in G$. Então,

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

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

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

1.4 Grupos de Permutações

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

$$S_A = \{f : A \longrightarrow A \ / f \text{ é } Bijetora\}.$$

Mostra-se que S_A com a composição de funções é um grupo. Primeiramente, mostra-se 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,

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

e desde que f é 1-1 [2], segue que $g(x_1) = g(x_2)$. Mas, como g também é 1-1, temos que $x_1 = x_2$. Desse modo, $f \circ g$ é 1-1. Para mostrar que $f \circ g$ é sobrejetora, considera-se $y \in A$. Como f é sobrejetora, existe $x \in A$ tal que $f(x) = y$. Por outro lado, sendo g sobrejetora, existe $z \in A$ de maneira que $x = g(z)$. Desse modo,

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

[2] Às vezes, chama-se uma função bijetora uma **correspondência** 1-1.

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

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

Conhecemos que composição de funções é associativa, a permutação $id_A : A \longrightarrow A$ (a identidade sobre A) é tal que $id_A \circ f = f \circ id_A = f$ para qualquer $f \in S_A$. E como uma função é bijetora se, e somente se, é invertível, cada $f \in S_A$ tem inversa em S_A. Portanto, as propriedades são satisfeitas. Desse modo, $(S_A, \circ)$ é um grupo, nâo-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. Neste caso, denota-se S_A por S_n e chama-se **grupo simétrico de grau** n 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_n tem $n!$ elementos.

Exemplo 1.9 O Grupo S_3

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

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

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

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,

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

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

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

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

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

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

Observando que qualquer elemento de S_3 é obtido dos elementos α e β, 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,

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

1.5 Grupo Diedral

O grupo Diedral D_n é o grupo das simetrias espaciais do polígono regular de n lados, de ordem $2n$ gerado por dois elementos α e β, satisfazendo

$$\begin{cases} |D_n| &= 2n \\ D_n &= \langle \alpha, \beta \rangle \\ \alpha^n &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha^{n-1}\beta, \end{cases}$$

em que,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}.$$

Observa-se que o grupo D_n contém ele próprio um subgrupo de ordem n,

$$R_n = \{e, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$$

é o **grupo das rotações do polígono** P_n.

Exemplo 1.10 Grupo Das Simetrias De Um Quadrado

Considere um quadrado com vértices P_1, P_2, P_3, P_4 com centro em O. Por O, considere 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. Obtêm-se as simetrias

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

e

$$\alpha_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \alpha_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

2. R_1, R_2, R_m, R_n : as rotações espaciais de ângulo π com eixos D_1, D_2, M, N, respectivamente. Desse modo,

$$\beta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \beta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

e

$$\beta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \beta_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

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

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

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_π	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_m	R_n
id	id	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_m	R_n
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_π	$R_{\frac{3\pi}{2}}$	id	R_m	R_n	R_2	R_1
R_π	R_π	$R_{\frac{3\pi}{2}}$	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_π	R_n	R_m	R_1	R_2
R_1	R_1	R_m	R_2	R_n	id	R_π	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_2	R_2	R_n	R_1	R_m	R_π	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_π
R_n	R_n	R_1	R_m	R_2	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_π	id

Tabela 1.1: Tábua da composição sobre D_4

A tábua mostra que operação é a composição de simetrias. A associatividade é válida, pois a composição de funções é associativa, Tem-se também que id é o elemento neutro da operação. O D_4 não é abeliano;

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

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

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

Mostra-se 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. Onde,

$$R_{\frac{\pi}{2}} = \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{e} \quad R_1 = \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Tem-se:

1. $\alpha^2 = \alpha \circ \alpha = \alpha_3$.
2. $\alpha^3 = \alpha_3 \circ \alpha = \alpha_4$.
3. $\alpha^4 = \alpha_3 \circ \alpha_3 = id = e$.
4. $\beta^2 = \beta \circ \beta = id = e$.
5. $\alpha \circ \beta = \beta_3$.
6. $\beta \circ \alpha^2 = \beta \circ \alpha_3 = \beta_2$.
7. $\beta \circ \alpha^3 = \beta \circ \alpha_4 = \beta_4$.

Portanto,

$$\begin{cases} D_4 = \langle \alpha, \beta \rangle \\ \alpha_4 = e \\ \beta_2 = e \\ \beta\alpha = \alpha^3\beta, \end{cases}$$

Exemplo 1.11 Grupo Das Simetrias De Um Pentágono

De forma análoga descrevemos o grupo D_5, como

$$\begin{cases} D_5 &= \langle \alpha, \beta \rangle \\ \alpha_5 &= e \\ \beta_2 &= e \\ \beta\alpha &= \alpha^4\beta, \end{cases}$$

onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

1.6 Subgrupos

Tomando o exemplo $\mathbb{Z} \subset \mathbb{Q}$, sendo $G_1 = (\mathbb{Z}, +)$ e $G_2 = (\mathbb{Q}, +)$ grupos, em que a operação em G_1 é induzida da operação em G_2. É vantajoso estudar um subconjunto H de um grupo G, sobre o qual o estudo desse grupo se torna mais factível, de modo a obter informações importantes de G.

Definição 1.6 *Consideremos um grupo G e H é um subconjunto não-vazio de G, então diz-se que H é um subgrupo de G quando a operação induzida de G, também é 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 $h \in H$, exixte $k \in H$ tal que $hk = kh = e_H$.*

Usaremos a notação $H < G$ para indicar que H é um subgrupo de 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 $e_H.a = a$; 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,

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

A caracterização dos subgrupos de um grupo é feita a seguir:

Proposição 1.5 *Seja H um subconjunto não-vazio de um grupo G. Então H é um subgrupo de G se, e somente se, uma das seguintes condições é satisfeita:*

1. $h_1 \cdot h_2 \in H$ e ${h_1}^{-1} \in H, \quad \forall h_1, h_2 \in H$;
2. $h_1 \cdot {h_2}^{-1} \in H, \quad \forall h_1, h_2 \in H$.

Vejamos alguns exemplos e contra-exemplos de subgrupos.

Exemplo 1.12 Para um grupo qualquer $G, \{e\}$ e G são claramente subgrupos de G, chamados **subgrupos triviais** de G. Se $H < G$ não é trivial, então H é dito **subgrupo próprio**.

Exemplo 1.13 Com a adição usual, temos que $\mathbb{Z} < \mathbb{Q}$. Aliás, temos os subgrupos

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

E sob a multiplicação usual, obtemos

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

Exemplo 1.14 O conjunto $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ é um subgrupo de $\mathbb{Z}$.
De fato, sejam $h_1, h_2 \in 2\mathbb{Z}$, digamos $h_1 = 2k_1$ e $h_2 = 2k_2$. Como o inverso aditivo de h_2 é $-h_2 = -2k_2$, segue que

$$h_1 + (-h_2) = 2(k_1 - k_2) = 2k_3 \in 2\mathbb{Z},$$

com $k_3 = k_1 + k_2 \in \mathbb{Z}$. Isso mostra que $2\mathbb{Z} < \mathbb{Z}$.

Mais geralmente, consideremos subconjuntos H de $\mathbb{Z}$ constituídos por múltiplos de outros inteiros e, ainda assim, obtemos $H < \mathbb{Z}$, ou seja, se $n \in \mathbb{Z}$ então $n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$. Reciprocamente [3], se H é um subgrupo de $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que

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

Exemplo 1.15 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 1.16 Seja $n \in \mathbb{Z}^*$ fixado e $H = \{r \in \mathbb{Q} : nr = 2\}$. Então H não é um subgrupo do grupo multiplicativo dos números racionais $\mathbb{Q}$, pois $0 \notin H$.

Exemplo 1.17 Seja S_1 o grupo de todos os números complexos de norma 1, ou seja, **o círculo trigonométrico unitário** em $\mathbb{R}^2$ e $U_n = \{1, e^{\frac{2\pi}{n}i}, e^{\frac{4\pi}{n}i}, \ldots, e^{\frac{2(n-1)\pi}{n}i}\}$ o grupo multiplicativo das raízes n -ésimas da unidade. Temos

$$U_n < S^1 < \mathbb{C}^*.$$

Exemplo 1.18 O conjunto $H = \mathcal{L}[0,1] = \{f : [0,1] \longrightarrow \mathbb{R}$ tal que f é contínua$\}$ é um subgrupo de $G = (\mathbb{R}^{\mathbb{R}}, +)$.
De fato, como a função nula $0 : [0,1] \longrightarrow \mathbb{R}$ é contínua, então $0 \in H$. Por outro lado, dados $f, g \in H$, sabe-se do Cálculo Diferencial que $f - g$ é contínua. Logo, H é um subgrupo de G.

Proposição 1.6 *Se h_1 e h_2 subgrupos de um grupo G. Então a interseção $H = H_1 \cap H_2$ também é um subgrupo de G.*

Demonstração: É claro que $e \in H \neq \varnothing$, pois $e \in H_1$ e $e \in H_2$. Agora, para $a, b \in H$,

$$\begin{cases} a \in H_1 \quad \text{e} \quad a \in H_2 \\ b \in H_1 \quad \text{e} \quad b \in H_2 \end{cases} \Rightarrow \quad ab \in H_1 \quad \text{e} \quad ab \in H_2,$$

[3] A demonstração encontra-se na referência [8], pág. 194.

pois $H_1 < G$ e $H_2 < G$. Desse modo, $ab \in H_1 \cap H_2$. Pelo mesmo motivo, $a^{-1} \in H_1$ e $a_{-1} \in H_2$. Portanto, $a_{-1} \in H_1 \cap H_2$. Por isso, $H_1 \cap H_2 < G$.

De forma mais geral, se $H_1, \ldots, H_n, \ldots$ 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.

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

Proposição 1.7 *Sejam H_1 e H_2 subgrupos de um grupo G. Então*

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

1.7 Grupos Cíclicos

Destaca-se nesta seção os grupos cíclicos, os quais são essenciais na Teoria dos Grupos, pois fornecem importantes resultados. Os exemplos mais importante de grupo cíclicos são $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$.

Definição 1.7 *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 operação 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. $(a^n)^m = a^{nm}$.

Sejam G um grupo e $a \in G$, considerando H subconjunto de G, dado por

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

Vamos mostrar que $H < G$. Seja $\alpha, \beta \in H$, digamos $\alpha = a^n$ e $\beta = a^m$, temos $\alpha \cdot \beta = a^n \cdot a^m = an + m \in H$, isot 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 $H = \langle a \rangle$. Nestde 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 1.19 O grupo aditivo $(\mathbb{Z}, +)$ é cíclico, pois $\mathbb{Z} = \langle 1 \rangle$. Aliás, $a = -1$ também é um gerador de $\mathbb{Z}$.

Exemplo 1.20 O grupo $(\mathbb{Z}_3, +)$ é cíclico gerado por $a = \overline{1}$, pois

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

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 $\overline{a} \in \mathbb{Z}^n$ é um gerador de $\mathbb{Z}^n$ se, e somente se, $mdc(a, n) = 1$, de acordo com o Teorema 2.4.

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

$$\begin{aligned} \alpha \cdot \beta &= a^n \cdot a^m \\ &= a^{n+m} \\ &= a^{m+n} \\ &= a^m \cdot a^n \\ &= \beta \cdot \alpha. \end{aligned}$$

A recíproca deste resultado não é verdadeira. 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 que $x + x = (\overline{0}, \overline{0})$, ou seja, não há como obter todos os elementos de G a partir de um dado elemento em G.

Definição 1.8 *A **ordem** de um grupo G é o número de elementos que compõem G.*
Notação: $|G|$.

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

Definição 1.9 *Seja G um grupo e $\alpha \in G$. Se existe $k \in \mathbb{N}$ tal que $\alpha^k = e$. então a **ordem** de α, 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 diz-se que α é de ordem infinita.

No grupo S_3 o elemento

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

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 $\mathcal{O}(\alpha) = 2 \Leftrightarrow \alpha = \alpha^{-1}$.

Teorema 1.1 *Todo subgrupo de um grupo cíclico é também cíclico.*

Demonstração: Sejam $G = \langle a \rangle$ um grupo cíclcico e H um subgrupo de G. Para $H = \{e\}$, temos $H = \langle e \rangle$. Se $H \neq \{e\}$, então existe $b \in H$, com $b \neq e$. Como $b \in G, b = a^k$ para algum $k \in \mathbb{Z}^*$. Mas, sendo $H < G, a^{-k} \in H$. Por isso,

$$X = \{n \in \mathbb{N} : a^n \in H\} \neq \varnothing.$$

Pelo PBO [4], existe $m \in X$, com $m = \min X$. Vamos mostrar que $H = \langle a^m \rangle$. Como $a^m \in H$, então $\langle a^m \rangle \subset H$. Consideremos, pois $h \in H$. Desde que $H < G$, então $h = a^n$ para algum $n \in \mathbb{Z}$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que

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

Logo, $a^n = a^{mq+r} = a^{mq} \cdot a^r$, isto é,

$$a^r = a^n \cdot (a^m)^{-q}.$$

Como $a^m \in H$, segue que $(a^m)^{-q} \in H$. Além disso, sendo a^n e $(a^m)^{-q}$ elementos de H, temos que $a^n \cdot (a^m)^{-q}) \in H$, isto é, $a^r \in H$. Mas, desde que $m = \min X$, devemos necessariamente ter $r = 0$. Por conseguinte, $n = mq$ e

$$h = a^n = (a^m)^q \in \langle a^m \rangle,$$

isto é, $H \subset \langle a^m \rangle$ e, portanto, $H = \langle a^m \rangle$..

Teorema 1.2 *Sejam $G_1 = \langle a \rangle$ e $G_2 = \langle b \rangle$ grupos cíclicos finitos de ordem n e m respectivamente. Se $mdc(n, m) = 1$, então $G_1 \times G_2$ é cíclico de ordem nm.*

Demonstração: Vamos mostrar que $G_1 \times G_2 = \langle (a, b) \rangle$. Claramente, a ordem de $G_1 \times G_2$ é nm. Consideremos $\mathcal{O}(a, b) = d$. Como temos $\mathcal{O}(a) = n$ e $\mathcal{O}(b) = m$,

$$(a, b)^{nm} = \underbrace{(a, b) \cdot (a, b) \cdots (a, b)}_{nm \text{ vezes}} = (a^{nm}, b^{nm}) = (e_1, e_2).$$

[4] Princípio da Boa Ordenação

Por isso, pela Proposição 2.3 $d|nm$. Por outro lado,

$$(a,b)^d = (a^d, b^d) = (e_1, e_2),$$

ou seja, $a^d = e_1$ e $b^d = e_2$, usando novamente a proposição, $n|d$ e $m|d$. Portanto, de $mdc(n,m) = 1$ segue $nm|d$ e, assim, $nm = d$. Logo, $\mathcal{O}(a,b) = nm$ e $G_1 \times G_2 = \langle (a,b) \rangle$.

Capítulo 2

Teorema de Lagrange, Subgrupos Normais, Grupos Quocientes e Homomorfismos de Grupos

2.1 Classes Laterais

Antes de apresentar o Teorema de Lagrange se faz necessário uma breve explanação sobre classe lateral. Sejam G um grupo e H um subgrupo de G. A relação $\equiv_E (mod\ H)$ sobre G, dada por,

$$x \equiv_E y\ (mod\ H) \Leftrightarrow x^{-1}y \in H.$$

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

1. $x^{-1}x = e \in H \Rightarrow x \equiv_E x\ (mod\ H)$; **(Reflexividade)**
2. Se $x \equiv_E y\ (mod\ H)$, então $x^{-1}y \in H \Rightarrow y^{-1}x \in H \Rightarrow y \equiv_E x\ (mod\ H)$; **(Simetria)**
3. Se $x \equiv_E y\ (mod\ H)$ e $y \equiv_E z\ (mod\ H)$, então $x^{-1}y \in H$ e $y^{-1}z \in H$. Portanto, $(x^{-1}y)(y^{-1}z) \in H \Rightarrow x^{-1}z \in H \Rightarrow x \equiv_E z\ (mod\ H)$. **(Transitividade)**

Portanto, é de equivalência.

Com a relação $\equiv_E\ y\ (mod\ H)$, para cada $x \in G$, por definição a classe de equivalência de x é o conjunto

$$\{y \in G : x \equiv_E y\ (mod\ H)\}.$$

Nota-se que $y \in G : x \equiv_E y\ (mod\ H) = xh : h \in H$ e por isso, denotamos por xH, ou seja,

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

e chamamos de **classe lateral à esqueda de H determinada por** x, ou simplesmente **classe lateral de x à esquerda.**

Analogamente, a relação $\equiv_D\ (mod\ H)$ sobre G dada por

$$x \equiv_D y\ (mod\ H) \Leftrightarrow xy^{-1} \in H$$

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

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

e chamamos **classe lateral de x à direita.**

Observação 2.1 Se $eH = H = He$, significa que, H é tanto uma classe à esquerda quanto à direita. E quando G é comutativo, então $xH = Hx$ para todo $x \in H$.

Exemplo 2.1 Seja $G = \mathbb{Z}_6$ e $H = \{\overline{0}, \overline{2}, \overline{4}\}$. Temos

$$\overline{0} + H = \overline{2} + H = \overline{4} + H,$$

pois $\overline{0}, \overline{2}, \overline{4} \in H$. e

$$\overline{1} + H = \{\overline{1}, \overline{3}, \overline{5}\} = \overline{3} + H = \overline{5} + H.$$

Logo, existem duas classes laterais à esquerda (à direita) de H, que são H e $\{\overline{1}, \overline{3}, \overline{5}\}$ por $\mathbb{Z}_6$ ser um grupo aditivo abeliano.

Seja G um grupo e $H < G$, vamos denotar por G_E e G_D os conjuntos de todas

as classes laterais à esquerda e à direita de H, respectivamente, ou seja,

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

Os elementos de G_E e G_D constituem partições de G. Em geral, tem-se que $G_E \neq G_D$; entretanto, eles têm a mesma cardinalidade, pois a função

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

é uma bijeção.

Definição 2.1 *Chama-se de* ***índice*** *de H em G, a cardinalidade do conjunto G_E e simboliza-se por $(G : H)$.*

A função $f : H \longrightarrow xH$ dada por $f(x) = xH, \quad \forall x \in G$ é uma bijeção. Por isso, toda classe lateral à esquerda (à direita) tem a mesma cardinalidade de H.

2.2 Teorema de Lagrange

Base para a Teoria dos grupos finitos, este Teorema iniciou-se dos estudos das permutações de Joseph Louis Lagrange sobre equações algébricas, de onde se extraiu certas propriedades as quais outros matemáticos lapidaram resultando no atual Teorema de Lagrange, principal resultado sobre grupos finitos. Este será uma das ferramentas utilizadas mais adiante para a exposição do tema central abordado, visto que, através dele entenderemos o comportamento dos grupos finitos.

Teorema 2.1 *(**Teorema de Lagrange**) Sejam G um grupo finito e H um subgrupo de G. Então a ordem e o índice de H em G dividem a ordem de G. Especificamente,*

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

Demonstração: Sendo G finito, então $(G : H)$ também o é. Suponha que $(G : H) = r$ e seja $G_E = \{a_1H, a_2H, \ldots, a_rH\}$.

Como G_E é uma partição de G,

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH.$$

e mais, $a_iH \cap a_jH = \varnothing$ com $i \neq j$, como a cardinalidade de cada classe em G_E ser igual a ordem de G

$$|G| = \underbrace{|H| + |H| + \ldots + |H|}_{n \text{ vezes}}.$$

Logo,

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

Algumas consequências do Teorema de Lagrange:

Corolário 2.1 *Sejam G um grupo finito e $\alpha \in G$ Então a ordem de α divide a ordem de G. Em particular,*

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

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

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

Corolário 2.2 *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, $|\langle x\rangle|$ divide p. Mas, sendo p primo, temos que $|\langle x\rangle| = p$, pois $|\langle x\rangle| \neq 1$. Por isso, $|\langle x\rangle| = |G|$ e, por conseguinte, G é cíclico.

Corolário 2.3 *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 2.2, G é abeliano. Só nos resta considerar o caso em que $|G| = 4$.

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

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

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.

2.3 Subgrupos Normais e Grupos Quocientes

Estabeleceremos condições para que ocorra a igualdade $G_E = G_D$ sobre um subgrupo H e G_E com a devida operação G_E torne-se um grupo.

Definição 2.2 *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 $gNg^{-1} = \{gng^{-1} : g \in Gen \in N\}$. Equivalentemente, N é normal quando

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

Exemplo 2.2 Para um grupo G qualquer, $\{e\}$ e G são subgrupos normais de G.

Exemplo 2.3 Se G é abeliano, então todo subgrupo H de G é normal. Portanto, para cada $n \in \mathbb{Z}$, $n\mathbb{Z}$ é normal em $\mathbb{Z}$.

Exemplo 2.4 O centro $Z(G) = \{a \in G : xa = ax, \quad \forall x \in G\}$ de G é normal.

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

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

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

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

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

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

então

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

Exemplo 2.5 Consideremos em S_3, o subgrupo gerado por $H = \{e, \alpha\}$, em que

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

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

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

Quando N for um subgrupo normal de G, denotamos G_E por G/N ou $\frac{G}{N}$.

Sejam $(G, \cdot)$ um grupo e N um subgrupo normal de G. Então o conjunto G/N

munido da operação

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

é um grupo e chama-se **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 2.6 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 isomorfo ao grupo $(\mathbb{Z}_n, +)$. Por isso, escreve-se $\frac{\mathbb{Z}}{n\cdot\mathbb{Z}} = \mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Exemplo 2.7 Para o grupo multiplicativo $G = \{1, -1, i, -i\} \subset C, N = \{1, -1\}$ é normal. O grupo quociente é

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

2.4 Homomorfismos de Grupos

As aplicações $f : G_1 \longrightarrow G_2$ essenciais para o estudo de grupos são aquelas que preservam as operações de G_1 e G_2, no sentido da seguinte definição:

Definição 2.3 *Sejam $(G_1, \cdot)$ e $(G_2, \times)$ dois grupos. Uma aplicação $f : G_1 \longrightarrow G_2$ é dita um* ***homomorfismo*** *quando*

$$f(a \cdot b) = f(a) \times f(b), \quad \forall a, b \in G_1.$$

Exemplo 2.8 A função $f : G_1 \longrightarrow G_2$ dada por $f(x) = e_2$, em que e_2 é a identidade de G_2, é um homomorfismo e chama-se **homomorfismo trivial.**

Exemplo 2.9 Para um grupo qualquer G, a função $id_G : G \longrightarrow G$ dada por $id_G(g) = g$ para todo $g \in G$, é um homomorfismo. Chama-se id **homomorfismo identidade.**

Exemplo 2.10 Se H é subgrupo normal de G, então $\varphi : G \longrightarrow G/H$ dada por $\varphi(g) = gH$, é um homomorfismo sobrejetor, chamado de **homomorfismo canônico.** de G sobre G/H.

Vejamos algumas propriedades dos homomorfismos de grupos. Onde, e_1 e e_2 representam as identidades dos grupos G_1 e G_2, respectivamente.

Definição 2.4 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. O núcleo e a imagem de f, denotados por $\ker f$ e $\mathrm{Im}f$, respectivamente, como sendo os seguintes conjuntos:*

$$\ker f = \{x \in G_1 : f(x) = e_2\},$$

$$\mathrm{Im}f = \{f(x) : x \in G_1\}.$$

Exemplo 2.11 Para o homomorfismo identidade $f = id : G \longrightarrow G$, tem-se que $\ker f = \{e\}$ e $\mathrm{Im}f = G$.

Exemplo 2.12 Considere a aplicação $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ definida por $f(m) = i^m$. Assim, para $n, m \in \mathbb{Z}$,

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

isto é , f é um homomorfismo. Além disso,

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

e

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

Proposição 2.1 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo. Então*

1. $f(e_1) = e_2$;
2. $f(x^{-1}) = f(x)^{-1}, \quad \forall x \in G_1$.

Demonstração: 1. Como $f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1)$. Portanto, $f(e_1) = e_2$.
2. Para $x \in G_1, e_2 = f(e_1) = f(xx^{-1}) = f(x)f(x^{-1})$. Por isso, $f(e_1) = e_2$.

Teorema 2.2 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo. Então*

1. $\ker f \trianglelefteq G_1$.

2. $\mathrm{Im} f < G_2$.

Demonstração: 1. Primeiramente, mostra-se 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,

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

Portanto, $\ker f < G_1$. Agora, para $g \in G_1$,

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

Logo, $gxg^{-1} \in \ker f$, o que mostra que $\ker f \trianglelefteq G_1$.

2. Tome $Im(f) = \{f(a) : a \in G_1\}$, sendo $f(e_1) = e_2$, então $Im(f) \neq \varnothing$. Agora, dados $x, y \in Im(f)$, existem $a, b \in G_1$ tais que $f(a) = x$ e $f(b) = y$. Por isso,

$$x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b)^{-1} = f(a \cdot b^{-1}),$$

de maneira que $x \cdot y^{-1} \in Im(f)$ e $Im(f) < G_2$.

2.5 Isomorfismos de Grupos

O isomorfismo de grupos nos oferece um método capaz de aferir quando dois grupos possuem as mesmas propriedades algébricas.

Definição 2.5 *Um homomorfismo $f : G_1 \longrightarrow G_2$ bijetivo chama-se* ***isomorfismo.*** *Em particular, um isomorfismo $f : G \longrightarrow G$ é dito um* ***automorfismo*** *de G.*

Exemplo 2.13 Sejam G 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** $g \in G$.

Proposição 2.2 *Se $f : G_1 \longrightarrow G_2$ é um isomorfismo, então $f^{-1} : G_2 \longrightarrow G_1$ também é um isomorfismo.*

Definição 2.6 *Dois grupos G_1 e G_2 são **isomorfos**, quando existir um isomorfismo entre eles. Denotamos por $G_1 \simeq G_2$.*

Dois grupos isomorfos, são idênticos, isto com relação às suas propriedades, independente da natureza de seus elementos. Assim, se $f : G_1 \longrightarrow G_2$ é um isomorfismo, identificamos um elemento $x \in G_1$ com sua imagem $f(x)$, em símbolos

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

Teorema 2.3 *Se G e K são dois grupos cíclicos, então $G \simeq K$ se, e somente se, $|G| = |K|$.*

Demonstração: Sejam G e K grupos cíclicos e $G \simeq K$, pela definição de isomorfismo temos que é imediato $|G| = |K|$, visto que $f : G \longrightarrow K$ é uma bijeção de G em K. Reciprocamente, sejam $G = \langle g \rangle$ e $K = \langle k \rangle$. Definindo a aplicação f por:

$$\begin{array}{rccc} f: & G & \longrightarrow & K \\ & g^i & \longmapsto & k^i. \end{array}$$

De tal forma que verifica-se que f é um homomorfismo. De fato,

$$\begin{aligned} f(g^i \cdot g^j) &= f(g^{i+j}) \\ &= k^{i+j} \\ &= k^i k^j \\ &= f(g^i) f(g^j). \end{aligned}$$

Agora, verifica-se que f é um homomorfismo injetor. Ora, $f(g^i) = f(g^j)$ então $k^i = k^j$. Se $\mathcal{O}(g) = \infty$ então $i = j$; por outro lado, $\mathcal{O}(k) < \infty$ então da equação $k^i = k^j$ obtem-se $\mathcal{O}(k)|(i-j)$ e como $0 \leq i, j < \mathcal{O}(g) = \mathcal{O}(k)$, conclui-se que $i - j = 0$, ou seja, $i = j$.. Por outro lado, a verificação de que f é um homomorfismo sobrejetor é imediata, uma vez que para qualquer $h^i \in G'$, tomamos $g^i \in G$ de tal forma que $f(g^i) = k^i$.

Corolário 2.4 *Qualquer grupo cíclico infinito é isomorfo aos inteiros.*

Demonstração: Se G é um grupo cíclico infinito então $|G| = \infty = |\mathbb{Z}|$. Daí pelo teorema anterior concluímos que $G \simeq \mathbb{Z}$.

Corolário 2.5 *Se n é um número natural, então existe um único grupo cíclico de ordem m, a menos de isomorfismo.*

Demonstração: Se G é um grupo cíclico de ordem n então $|G| = |\mathbb{Z}/n\mathbb{Z}|$. Desta forma, pelo Teorema 2.3 concluímos que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Corolário 2.6 *Sejam α um elemento do grupo G e $\langle\alpha\rangle$ o subgrupo gerado por α. Então as seguintes condições são equivalentes:*

1. *A ordem $|\langle\alpha\rangle|$ é finita;*
2. *Existe $t \geq 1$ tal que $\alpha^t = e$.*

   Neste caso, denotando por n a ordem de α, temos

$$\langle\alpha\rangle = \{e, \alpha, \ldots, \epsilon^{n-1}\},$$

ou seja, a ordem do grupo por ele gerado.

Voltemos ao grupo S_3 e α como em (1.2). Temos que

$$\alpha^2 = e \Rightarrow (\alpha^2)^2 = e \Rightarrow \alpha^4 = e \Rightarrow a^8 = e.$$

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

Proposição 2.3 *Sejam G um grupo e $\alpha \in G$ tal que $\mathcal{O} = n$ (ordem finita). Se $\alpha^m = e$ e $m \neq 0$ então n divide m.*

Demonstração: Pelo Algoritmo da divisão, tem-se

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

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

O resultado final do Exemplo 1.20 é a parte de um resultado bem mais geral. De fato,

Teorema 2.4 *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 2.3, 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 2.14 Determinar os geradores do grupo aditivo $\mathbb{Z}_{10}$.

Solução: Para determinar os geradores de $\mathbb{Z}_{10}$, vamos em busca de todos os $t \in \mathbb{N}$ tais que $madc(10,t) = 1$. Assim t, assume os seguintes valores:

$$t = 1, 3, 7, 9.$$

Daí, pelo Teorema 1.9.2 temos que os geradores de $\mathbb{Z}_{10}$ são os seguintes elementos:
$\overline{1}^1 = 1$;
$\overline{1}^3 = \overline{1} + \overline{1} + \overline{1} = \overline{3}$;
$\overline{1}^7 = \overline{5}$;
$\overline{1}^9 = \overline{9}$.

Teorema 2.5 ***(Caracterização dos Grupos Cíclicos).*** *Todo grupo cíclico é isomorfo a* $(\mathbb{Z}, +)$ *ou a* $(\mathbb{Z}_n, +)$ *para algum* n.

Demonstração: Primeiramente, suponhamos que $G = \langle a \rangle$ seja um grupo cíclico infinito, e consideremos a função

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & G \\ & m & \longmapsto & a^m. \end{array}$$

Dados, $m_1, m_2 \in \mathbb{Z}$,

$$f(m_1 + m_2) = a^{m_1+m_2} = a^{m_1} \cdot a^{m_2} = f(m_1) \cdot f(m_2),$$

portanto, F é um homomorfismo. Nota-se que se $a^k \in G$, então $f(k) = a^k$, de maneira que f é sobrejetora. Assim, dado $m \in \mathbb{Z}$,

$$m \in \ker(f) \Leftrightarrow f(m) = e \Leftrightarrow a^m = e \Leftrightarrow m = 0.$$

pois a tem ordem infinita. Temos, $\ker(f) = \{0\}$ tornando f injetora. Logo, f é um homomorfismo e $\mathbb{Z} \simeq G$.

Agora, seja $G = \langle a \rangle$ um grupo cíclico de ordem n, digamos $G = \{e, a, \ldots, a^{n-1}\}$. Então vamos mostrar que a aplicação

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

é um isomorfismo.

Como existem $m_1, m_2 \in \mathbb{Z}$ com $m_1 \neq m_2$ tais que $\overline{m_1} = \overline{m_2}$ vamos verificar que f está bem definida. Temos,

$$\overline{m_1} = \overline{m_2} \Leftrightarrow m_1 \equiv m_2 (\mod n) \Leftrightarrow m_1 - m_2 = kn$$

para algum $k \in \mathbb{Z}$.

Assim,

$$a^{m_1-m_2} = (a^n)^k = e \Rightarrow a^{m_1} = a^{m_2} \Rightarrow f(\overline{m_1}) = f(\overline{m_2}),$$

f está bem definida.

Para $\overline{m_1}, \overline{m_2} \in \mathbb{Z}_n$,

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

f é um homomorfismo. Claramente, f é um homomorfismo sobrjetivo. Além disso, dado $\overline{m} \in \mathbb{Z}_n$,

$$\overline{m} \in \ker(f) \Leftrightarrow f(\overline{m}) = e \Leftrightarrow a^m = e \Rightarrow n|m,$$

ou seja $m = 0$. Por isso, $\ker(f) = \{\overline{0}\}$, f é assim bijetora. Concluímos que $\mathbb{Z}_n \simeq G$.

O Teorema que segue, nos dá outra forma de mostrar que dois grupos são isomorfos, no caso em que um deles é um grupo quociente.

Teorema 2.6 ***(Fundamental dos Homomorfismos)*** *Seja $f : G \longrightarrow K$ um homomorfismo de grupos. Então*

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

Demonstração: Seja F a aplicação definida por

$$\begin{aligned} F : \quad \frac{G}{\ker f} &\longrightarrow \mathrm{Im} f \\ x(\ker) &\longmapsto f(x) \end{aligned}$$

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,

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

Claramente F é sobrejetora pois,

$$\mathrm{Im}F = \{F(x \ker f) : x(\ker f) \in \frac{G}{\ker f}\} = \{f(x) : x \in G\} = \mathrm{Im}F.$$

e ainda,

$$\ker F = \{x(\ker f)|f(x) = e\} = \{x(\ker f) : x \in \ker f\} = (\ker f)$$

assim $\ker f = \{e_{\frac{G}{\ker f}}\}$, ou seja, F é injetiva. Logo, $\frac{G}{\ker f} \simeq \mathrm{Im} f$.

Duas aplicações do Teorema Fundamental:

Exemplo 2.15 Considere os grupos aditivos $(\mathbb{Z}, +)$ e $\mathbb{Z}_{\ltimes}, +)$. Mostrar que

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

Solução: Exibindo um homomorfismo sobrejetivo $f : \mathbb{Z} \longrightarrow \mathbb{Z}_{\ltimes}$ tal que $\ker f = n\mathbb{Z}$. Considere então

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{\ltimes} \\ & m & \longmapsto & \overline{m}. \end{array}$$

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 $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_{\ltimes}$. Sejam $GL(n;\mathbb{R})$ e $SL_n(\mathbb{R}) = \{A \in GL(n;\mathbb{R}) : \det(A) = 1\}$. Mostrar que $\frac{GL(n;\mathbb{R})}{SL_n(\mathbb{R})} \simeq \mathbb{R}^*$.

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

$$|AB| = |A||B| = 1 \cdot 1 = 1$$

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

$$|A^{-1}| = |A|^{-1} = 1,$$

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

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

ou seja,

$$BAB^{-1} \in SL_n(\mathbb{R}).$$

Donde conclui-se que $SL_n(\mathbb{Z}) \lhd GL(n;\mathbb{R})$.

Agora considere a aplicação definida da seguinte forma:

$$\begin{array}{rccc} f: & GL(n;\mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ & A & \longmapsto & |A| \end{array}$$

f é um homomorfismo. De fato, $f(A \cdot B) = |A \cdot B| = |A||B| = f(A) \cdot f(B) \ \ \forall A, B \in GL(n;\mathbb{R})$. Observe ainda que $\mathrm{Im}f = \{f(A)A \in GL(n;\mathbb{R})\} = \{|A| : A \in GL(n;\mathbb{R})\} = \mathbb{R}^*$, ou seja, f é sobrejetora. Agora, $Kerf = \{A \in GL(n;\mathbb{R}) : f(A) = 1\} = \{a \in GL(n;\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R})$. Daí, pelo Teorema do Homomorfismo,

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

Capítulo 3

Grupos Finitos Gerados por Dois Elementos

No capítulo 1 definimos os grupos cíclicos, grupos gerados por um elemento, os classificamos segundo os isomorfismos existentes entre $\mathbb{Z}$ e $\mathbb{Z}_n$. Também pode-se classificar os grupos gerados por dois elementos, porém sua classificação dá-se de forma mais complexa. Neste capítulo focaremos na classificação dos grupos **finitos** gerados por dois elementos $\langle a, b\rangle = G$, onde $a, b \in G$, $s \geq 1$ um inteiro, satisfazem

$$ba = a^s b,$$

visto que ajudarão na classificação dos grupos de ordem ≤ 11.

Considere o grupo $(S_3, \circ)$ como exemplo de grupo com essa propriedade:

$$S_3 = \left\{ e = id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$

$$\left. \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Temos,

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

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

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

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

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

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

assim,

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

Se G é um grupo qualquer de ordem 6 mostraremos que possui elementos a e b tais que satisfazem

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

então existe um isomorfismo entre S_3 e G.

Logo, a menos de isomorfismo, o grupo S_3 é o único que satisfaz

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

Proposição 3.1 *A relação $ba = a^s b$ é equivalente a $\mathcal{I}_b(a) = a^s$.*

Demonstração: $ba = a^s b \Leftrightarrow bab^{-1} = a^s bb^{-1} = a^s e \Leftrightarrow bab^{-1} = a^s \Leftrightarrow \mathcal{I}_b(a) = a^s$.

Para estudarmos grupos isomorfos sob condições análogas às de S_3, vejamos o teorema,

Teorema 3.1 *Sejam G um grupo finito com $a, b \in G$, $s \geq 1$ um inteiro tais que $ba = a^s b$ e G_1 um grupo arbitrário com $\alpha, \beta \in G_1$. Sejam $m, n \geq 1$ inteiros tais que*

$$a^n = e, \quad b^m \in \langle a \rangle. \tag{3.1}$$

Então,

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

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

2. *Se os inteiros n, m são escolhidos minimalmente satisfazendo* (3.1)*, então o grupo $\langle a, b \rangle$ tem ordem igual a nm.*

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

$$f : \ \langle a, b \rangle \ \longrightarrow \ G_1$$

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

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

Demonstração: Sendo G um grupo finito, temos que a existência de n, m está garantida e existe $h, k \in \mathbb{Z}$ para os quais $a^h = a^k$ com $h > k$, onde $a^h a^k = a^{h-k} = e$ e $h - k > 0$, bastando considerar $n = h - k$.

1) Mostra-se que que $b^t a^r = a^{rs^t} b^t$, equivalente a $\mathcal{I}_{b^t}(a) = a^{rs^t}$, em que , para cada $g \in G$, $I_g : G \longrightarrow G$ é um automorfismo dado por $I_g(x) = gxg^{-1}$. Faremos uso da indução finita sobre t.

Se $t = 1$, então tem-se

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

Se $t \geq 2$, suponha por hipótese que a relação é válida para $t - 1$, assim:

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

Então, para t, temos:

$$\begin{array}{rcrcl} \mathcal{I}_{b^t}(a^r) & = & \mathcal{I}_b \circ \mathcal{I}_{b^{t-1}}(a^r) & = & \mathcal{I}_b(\mathcal{I}_{b^{t-1}}(a^r)) \\ & = & \mathcal{I}_b(a^{rs^{t-1}}) & = & (\mathcal{I}_b(a))^{rs^{t-1}} \\ & = & (a^s)^{rs^{t-1}} & = & a^{srs^{t-1}} \\ & = & a^{rss^{t-1}} & = & a^{rs^t}. \end{array}$$

Logo, $b^t a^r = a^{rs^t} b^t, \quad \forall r, s \in \mathbb{N}$.

Agora sejam $a^{l_1} \cdot b^{l_2} \in \langle a, b \rangle$. Pelo algoritmo da divisão, l_1 e l_2 podem ser escritos como

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

$$l_2 = m.q_2 + r_2, \quad \text{com} \quad 0 \leq r_1 \leq m - 1$$

como $a^n = e, b^m \in \langle a \rangle, a^{l_1} = a^{r_1}$ e $b^{l_2} = b^{mq_2} \cdot b^{r_2}$, onde $b^m = a^\lambda$ com $\lambda \in \mathbb{Z}$. Portanto,

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

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

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

2) Suponha que n e m sejam mínimos e que satisfaçam (3.1). Vamos mortrar que dados $0 \leq i, k \leq n-1$ e $0 \leq j, l \leq m-1$ tais que $a^i b^j = a^k b^l, \forall i, j, k, l \in \mathbb{N}$, então $i = k, j = l$, implicando assim em $|G| = mn$.

Supondo sem perda de gemeralidade que $l \leq j$ e multiplicando ambos os ledos da igualdade $a^i b^j = a^k b^l$ por a^{-i} à esquerda e por b^{-l} à direita, temos

$$\begin{aligned} a^i b^j = a^k b^l &\Rightarrow a^{-i} a^i b^j b^{-l} = a^{-i} a^k b^l b^{-l} \\ &\Rightarrow e b^{j-l} = a^{-i+k} e \\ &\Rightarrow b^{j-l} = a^{k-i} \quad \in \langle a\rangle. \end{aligned}$$

Pela minimalidade de m, temos $j - l = 0$, assim, $j = l$, já que $0 \leq j - l \leq j \leq m = 1$. Por consequência

$$a^{k-i} = e,$$

analogamente, pela minimalidade de n, conclui-se $k - i = 0$, já que temos $0 \leq i - k \leq i \leq n-1$, assim $k = i$.

3) Suponha a existência de um homomorfismo

$$f : \langle a, b\rangle \longrightarrow G_1$$

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,

$$f(a)^{\mathcal{O}(a)} = e.$$

Segue que

$$a^n = e \Rightarrow \alpha^n = f(a)^n = e.$$

e $b^m \in \langle a \rangle$, ou seja, $b^m = a^u$, com $u \in \mathbb{N}$, então:

$$b^m = a^u \Rightarrow \beta^m = \alpha^u.$$

Reciprocamente, suponha $\beta\alpha = \alpha^s\beta, \alpha^n = e$ e $\beta^m = \alpha^u$. Aplicando a parte 1) a G_1 e α, β, obtemos

$$\beta^t\alpha^r = \alpha^{rs^t}\beta^t, \quad \forall r, t \in \mathbb{N}.$$

Basta então, verificarmos a aplicação

$$\begin{array}{rccc} f: & \langle a, b\rangle & \longrightarrow & G_1 \\ & a^ib^j & \longmapsto & \alpha^i\beta^j \end{array}$$

para $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$, é um homomorfismo. Devido as escolhas minimais de n e m, f está bem definida. Escrevendo para $i, j, k, l \in \mathbb{N}$,

$$\begin{array}{lll} j + l = pm + v & , com & 0 \leq v \leq m-1 \\ i + ks^j + pu = qn + w & , com & 0 \leq w \leq n-1. \end{array}$$

Fazendo a aplicação da função f em $a^ib^j \cdot a^kb^l$,

$$\begin{array}{rclclcl} f(a^ib^j)\cdot(a^kb^l)) & = & f(a^i\cdot(b^ja^k)\cdot b^l) & = & f(a^i\cdot(a^{sk^j}b^j)\cdot b^l) & = & f(a^{i+sk^j}\cdot b^{j+l}) \\ & = & f(a^{i+sk^j}\cdot b^{pm}\cdot b^v) & = & f(a^{i+sk^j}\cdot b^{pm+v}) & = & f(a^{i+sk^j}\cdot a^{pu}b^v) \\ & = & f(a^wb^v) & = & \alpha^w\beta^v & = & \alpha^{i+ks^j+pu}\beta^{j+l} \\ & = & \alpha^{i+sk^j}\cdot\alpha^{pu}\cdot\beta^v & = & \alpha^{i+sk^j}\beta^{pm}\beta^v & = & \alpha^{i+sk^j}\beta^{j+l} \\ & = & \alpha^i\alpha^{sk^j}\beta^j\beta^l & = & \alpha^i\beta^j\alpha^k\beta^l & = & f(a^ib^j)f(a^kb^l). \end{array}$$

Logo, f é um homomorfismo, onde $f(a) = \alpha$ e $f(b) = \beta$.

Teorema 3.2 *Considere* $n, m, s, u \in \mathbb{Z}$.

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

$$\begin{cases} G &= \langle a, b \rangle \\ a^n &= e \\ b^m &= a^u \\ ba &= a^s b \end{cases} \tag{3.2}$$

Se e somente se

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

2. *Quando existir um grupo G de ordem nm satisfazendo as condições em (3.2), tal grupo é único a menos de isomorfismos.*

Demonstração: 1. Vamos demonstrar somente a ida, pois a volta necessita de conhecimentos prévios de produto semidireto de dois grupos, sua demonstração encontra-se na referência [5]. Pelo Teorema 3.1 , temos que $b^m a = a^{s^m} b^m$. Como $b^m \in \langle a \rangle$ e $\langle a \rangle$ é cíclico, ou seja, abeliano, sabemos que b^m comuta com a assim $ab^m = a^{s^m} b^m$, multiplicando por a^{-1} à esquerda e por b^{-m} à direita, temos

$$\begin{aligned} ab^m &= a^{s^m} b^m \\ a^{-1} ab^m b^{-m} &= a^{-1} a^{s^m} b^m b^{-m} \\ e &= a^{s^m - 1}. \end{aligned}$$

Portanto $s^m - 1$ é um múltiplo da ordem de a, isto é, $s^m \equiv (1 \mod n)$. Analogamente, temos que $b^m a = a^{s^m} b^m$. Como $a^u = b^m$, então $a^u \in \langle b \rangle$, a^u comuta com b assim $a^u b = ba^u = a^{su} b$. Logo, multiplicando ambos os lados por a^{-u} à esquerda e por b^{-1} à direita

$$\begin{aligned} a^u b &= a^{su} b \\ a^{-u} a^u b b^{-1} &= a^{-u} a^{su} b b^{-1} \\ e &= a^{us-u} \\ e &= a^{u(s-1)}. \end{aligned}$$

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

2. Suponha G_1 um grupo de ordem nm que possui dois elementos α, β, tais que

$$\begin{cases} G_1 &= \langle \alpha, \beta \rangle \\ \alpha^n &= e \\ \beta^m &= \alpha^u \\ \beta\alpha &= \alpha^s\beta \end{cases}$$

Como $|G| = |G_1| = nm$ então a aplicação

$$\begin{array}{rccc} f: & G & \longrightarrow & G_1 \\ & a^ibj & \longmapsto & \alpha^i\beta^j, \end{array}$$

para $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$ é uma bijeção. E pelo item 3 do Teorema 3.1, conclui-se que f é um isomorfismo.

Proposição 3.2 *Sejam n, m, s, u inteiros não negativos. Seja G um grupo de ordem nm que possui dois elementos a, b tais que:*

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

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

$$\begin{array}{rccc} \varphi: & Aut(G) & \longrightarrow & G_1 \\ & f & \longmapsto & (f(a)f(b)) \end{array}$$

é uma bijeção.

Exemplo 3.1 Mostrar que $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq S_3$.

Solução: Sabemos que S_3, é o grupo das permutações de grau 3, não cíclico tal que

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

onde,

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

Vamos mostrar que $|Aut(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})| = 6 = 2\cdot 3$, com elementos $\varphi_1, \varphi_2 \in Aut(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$ satisfazendo

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

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:

$$\begin{array}{rccc|rccc|rccc} \varphi_1: & G & \longrightarrow & G & \varphi_2: & G & \longrightarrow & G & \varphi_3: & G & \longrightarrow & G \\ & \alpha_1 & \longmapsto & \alpha_1 & & \alpha_1 & \longmapsto & \alpha_1 & & \alpha_1 & \longmapsto & \alpha_1 \\ & \alpha_2 & \longmapsto & \alpha_2 \ , & & \alpha_2 & \longmapsto & \alpha_4 \ , & & \alpha_2 & \longmapsto & \alpha_2 \ , \\ & \alpha_3 & \longmapsto & \alpha_3 & & \alpha_3 & \longmapsto & \alpha_2 & & \alpha_3 & \longmapsto & \alpha_4 \\ & \alpha_4 & \longmapsto & \alpha_4 & & \alpha_4 & \longmapsto & \alpha_3 & & \alpha_4 & \longmapsto & \alpha_3 \end{array}$$

e

$$\begin{array}{rccc|rccc|rccc} \varphi_4: & G & \longrightarrow & G & \varphi_5: & G & \longrightarrow & G & \varphi_6: & G & \longrightarrow & G \\ & \alpha_1 & \longmapsto & \alpha_1 & & \alpha_1 & \longmapsto & \alpha_1 & & \alpha_1 & \longmapsto & \alpha_1 \\ & \alpha_2 & \longmapsto & \alpha_3 \ , & & \alpha_2 & \longmapsto & \alpha_3 \ , & & \alpha_2 & \longmapsto & \alpha_4 \ , \\ & \alpha_3 & \longmapsto & \alpha_2 & & \alpha_3 & \longmapsto & \alpha_4 & & \alpha_3 & \longmapsto & \alpha_3 \\ & \alpha_4 & \longmapsto & \alpha_4 & & \alpha_4 & \longmapsto & \alpha_2 & & \alpha_4 & \longmapsto & \alpha_2 \end{array}$$

ou seja, $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$. 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, $\mathcal{O}(\varphi_2) = 3$ e $\mathcal{O}(\varphi_4) = 2$. 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 $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \langle \varphi_2, \varphi_4 \rangle$. Temos também que $\varphi_4\varphi_2 = \varphi_2^2\varphi_4$. Portanto,

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

Pelo Teorema 3.2 item 2, concluímos que

$$Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq S_3.$$

Capítulo 4

Caracterização dos Grupos G de ordem ≤ 11

Veremos neste capítulo a abordagem do problema central do presente trabalho, a caracterização dos grupos G de ordem ≤ 11, onde os classificaremos e os entenderemos melhor, a partir da aplicação dos resultados obtidos até aqui.

4.1 Grupo de ordem 1

Sendo $|G| = 1$, então $G = \{e\}$ é o único com um elemento.

4.2 Grupos de ordem p, com p primo ($p = 2, 3, 5, 7$ e 11)

Se $|G| = p$ com $p = 2, 3, 5, 7,$ e 11, temos que pelo Corolário 2.2, G é cíclico e de ordem p, portanto pelo Teorema 2.5, G é isomorfo a $\mathbb{Z}_p$. Logo,

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

4.3 Grupos de ordem 4

O estudo destes grupos de ordem 4 será realizado a partir dos grupos aditivos

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

Os grupos apresentados acima não são isomorfos, pois $\mathbb{Z}_4 = \langle\overline{1}\rangle$, é cíclico, possui elementos de ordem 4, já $\mathbb{Z}_2 \times \mathbb{Z}_2$ não é cíclico, uma vez que todo elemento $g \in G - \{(\overline{0}, \overline{0})\}$ tem ordem 2. Mostra-se que, a menos de isomorfismos G_1 e G_2 são os únicos grupos de ordem 4.

Seja G um grupo de ordem 4, $|G| = 4$, consideremos $G = \{e, a, b, c\}$,

1. Se G possui um elemento de ordem 4, G é cíclico, então temos pelo Teorema 2.5 que

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

2. Se G não possui um elemento de ordem 4, pelo Teorema de Lagrange, todo $g \in G$ com $g \neq e$, tem ordem 2, uma vez que a ordem de g tem que dividir $|G| = 4$ e assim pelo Corolário 2.3 G é abeliano.

Vamos construir a tábua de G, com os resultados das possíveis multiplicações, para isto, precisa-se determinar o valor de ab. Temos que $ab \in G = \{e, a, b, c\}$, com $\mathcal{O}(a) = \mathcal{O}(b) = \mathcal{O}(c) = 2$, onde $|G| = 4$, ou seja, obviamente todos os elementos são distintos. Estudaremos as seguintes condições:

1. Se $ab = e$, então $a = b^{-1}$. Como $\mathcal{O}(b) = 2$ implica $b = b^{-1}$, temos $a = b$, o que é um absurdo;
2. Se $ab = a$, então $b = e$, o que é um absurdo;
3. Se $ab = b$, então $a = e$, o que não é verdade;

Portanto sendo G abeliano, $ab = ba = c$. Analogamente, tem-se $ac = ca = b$ e $bc = cb = a$, resultando assim a tábua de G, 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

Tabela 4.1: Tábua de G

Observe que $|G| = 4 = 2 \cdot 2$. Considerando $n = 2$ e $m = 2$, e a Tábua de G, temos

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

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 $\beta = (\overline{1}, \overline{0})$, obtemos que

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

Tomemos a aplicação

$$\begin{aligned} \Pi : \ \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow G \\ (\overline{0}, \overline{0}) &\longmapsto e \\ (\overline{1}, \overline{0}) &\longmapsto a \\ (\overline{0}, \overline{1}) &\longmapsto b \\ (\overline{1}, \overline{1}) &\longmapsto c \end{aligned}$$

Temos que Π é uma bijeção, pois todos os elementos de ambos os grupos, G_2 e G são distintos entre si, onde:

$$
\begin{array}{rcccl}
\Pi[(\overline{0},\overline{0})+(\overline{1},\overline{0})] & = & \Pi(\overline{1},\overline{0}) = a = e\cdot a & = & \Pi(\overline{0},\overline{0})\cdot\Pi(\overline{1},\overline{0}) \\
\Pi[(\overline{0},\overline{0})+(\overline{0},\overline{1})] & = & \Pi(\overline{0},\overline{1}) = b = e\cdot b & = & \Pi(\overline{0},\overline{0})\cdot\Pi(\overline{0},\overline{1}) \\
\Pi[(\overline{0},\overline{0})+(\overline{1},\overline{1})] & = & \Pi(\overline{1},\overline{1}) = c = e\cdot c & = & \Pi(\overline{0},\overline{0})\cdot\Pi(\overline{1},\overline{1}) \\
\Pi[(\overline{1},\overline{0})+(\overline{0},\overline{1})] & = & \Pi(\overline{1},\overline{1}) = c = a\cdot b & = & \Pi(\overline{1},\overline{0})\cdot\Pi(\overline{0},\overline{1}) \\
\Pi[(\overline{1},\overline{0})+(\overline{1},\overline{1})] & = & \Pi(\overline{0},\overline{1}) = b = a\cdot c & = & \Pi(\overline{1},\overline{0})\cdot\Pi(\overline{1},\overline{1}) \\
\Pi[(\overline{1},\overline{0})+(\overline{1},\overline{0})] & = & \Pi(\overline{0},\overline{0}) = e = a\cdot a & = & \Pi(\overline{1},\overline{0})\cdot\Pi(\overline{1},\overline{0}) \\
\Pi[(\overline{0},\overline{1})+(\overline{0},\overline{1})] & = & \Pi(\overline{0},\overline{0}) = e = b\cdot b & = & \Pi(\overline{0},\overline{1})\cdot\Pi(\overline{0},\overline{1}) \\
\Pi[(\overline{0},\overline{1})+(\overline{1},\overline{0})] & = & \Pi(\overline{1},\overline{1}) = c = b\cdot a & = & \Pi(\overline{0},\overline{1})\cdot\Pi(\overline{1},\overline{0}) \\
\Pi[(\overline{0},\overline{1})+(\overline{1},\overline{1})] & = & \Pi(\overline{1},\overline{0}) = a = b\cdot c & = & \Pi(\overline{0},\overline{1})\cdot\Pi(\overline{1},\overline{1}) \\
\Pi[(\overline{1},\overline{1})+(\overline{1},\overline{1})] & = & \Pi(\overline{0},\overline{0}) = e = c\cdot c & = & \Pi(\overline{1},\overline{1})\cdot\Pi(\overline{1},\overline{1})
\end{array}
$$

Sendo $(G_2,+)$ um grupo abeliano observamos que:

$$\Pi[(\overline{a},\overline{b})+(\overline{c},\overline{d})] = \Pi[(\overline{c},\overline{d})+(\overline{a},\overline{b})], \quad \forall(\overline{a},\overline{b}),(\overline{c},\overline{d}) \in G_2.$$

Logo, Π é um homomorfismo, como é bijetivo, portanto é um isomorfismo. Pelo item 2 do Teorema 3.2,

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

Conclui-se que a menos de isomorfismos, $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ são os únicos grupos de ordem 4.

4.4 Grupos de ordem 6

Entendemos que os grupos $\mathbb{Z}_6$ e S_3 possuem ambos ordem seis. Eles não são isomorfos, pois $\mathbb{Z}_6$ é cíclico enquanto que S_3 não o é. Vamos mostrar que, a menos de isomorfismos, eles são os únicos grupos de ordem 6.

Conderemos G um grupo qualquer com $|G| = 6$.

Proposição 4.1 *O grupo G possui um elemento α de ordem 3.*

Demonstração Consideramos dois casos:

1. G é um grupo cíclico gerado por um elemento α. Neste caso, temos que $G = \langle\alpha\rangle$ para algum $\alpha \in G$, assim $\mathcal{O}(\alpha) = 6$. Tomemos então $\beta = \alpha^2$, $\mathcal{O}(\beta) = 3$.

2. O grupo G não é cíclico. Suponhamos por absurdo que nenhum elemento de G tem ordem 3, $\mathcal{O}(\beta) \neq 3, \quad \forall\beta \in G$. Neste caso, pelo Teorema de Lagrange, todo elemento $x \in G - \{e\}$ tem que ter ordem 2, portanto $x = x^{-1}$ e pelo Corolário 2.3 G é abeliano. Tomando dois elementos $a, b \in G - \{e\}$, o conjunto $H = \{e, a, b, ab\}$ é um subgrupo de G, tal que $|H| = 4$, o que contraria o Teorema de Lagrange, já que 4 não divide 6. Logo, existe $\alpha \in G$ onde $\mathcal{O}(\alpha) = 3$.

Proposição 4.2 *O grupo G possui pelo menos um elemento β de ordem 2 e $G = \langle\alpha, \beta\rangle$.*

Demonstração: Análogo a proposição anterior, consideramos dois casos:

1. G é um grupo cíclico, onde $G = \langle\gamma\rangle$, tome $\beta = \gamma^3$ tal que $\gamma^3 \neq \langle\gamma^2\rangle$, pois $\langle\gamma^2\rangle = \{e, \gamma^2, \gamma^4\}$, logo $|\langle\gamma^2, \gamma^3\rangle| > 3$ e, pelo Teorema de Lagrange, $|\langle\gamma^2, \gamma^3\rangle$ divide 6, a ordem do grupo. Portanto $G = \langle\gamma^2, \gamma^3\rangle = \langle\alpha, \beta\rangle$, onde $\alpha = \gamma^2$.

2. G não é um grupo cíclico. Pela proposição 4.2 , $\ni \alpha \in G$ tal que $\mathcal{O}(\alpha) = 3$, tome $\beta \in G$ com $\beta \notin \langle\alpha\rangle$ e $\langle\alpha\rangle = \{e, \alpha, \alpha^2\}$.

Afirmação: Os 6 elementos $e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta$ são distintos. De fato, se $\alpha\beta = \alpha^2\beta$, então $\alpha = \alpha^2$, ou seja, $\alpha = e$, o que não é verdade. Os demais casos são analisados analogamente.

Assim temos,

$$G = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\} \quad \text{e} \quad G = \langle\alpha, \beta\rangle.$$

A ordem do elemento β pode ser igual a dois ou três; vamos verificar que $\mathcal{O}(\beta) = 2$. Primeiro observe que $\beta^2 \in \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$, pois caso contrário teríamos $\beta^2 \in \{\beta, \alpha\beta, \alpha^2\beta\}$ e então $\beta \in \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$, absurdo, pois $\beta \notin \langle\alpha\rangle$.

Suponhamos agora que $\mathcal{O}(\beta) = 3$, temos

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

o que não é verdade. Logo, $\mathcal{O}(\beta) = 2$.

Conclui-se que

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

Precisamos analisar as possibilidades para o produto
betaα. Notamos que $\beta\alpha \notin \langle\alpha\rangle$, pois senão, teríamos $\beta = \alpha^{-1}, \beta = e, \beta = \alpha$ ou $\alpha = e$, contradição. Logo, $\beta\alpha = \alpha\beta$ ou $\beta\alpha = \alpha^2\beta$. Assim temos duas possibilidades para G:

$$\begin{cases} |G| &= 6 = 3 \cdot 2 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^3 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha\beta \end{cases} \quad \text{e} \quad \begin{cases} |G| &= 6 = 3 \cdot 2 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^3 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha^2\beta. \end{cases} \tag{4.1}$$

Pelo item 2 do Teorema 3.2, em cada caso, temos no máximo um grupo, a menos de isomorfismos, satisfazendo as condições em (4.1). Observamos que $G = \mathbb{Z}_6$ satisfaz as condições do primeiro caso e $G = S_3$ satisfaz as condições do segundo caso.

Note que o grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ também satisfaz as condições do primeiro caso, observe que o elemento $(\overline{\overline{1}}, \overline{1}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ tem ordem 6, e que portanto, pela unicidade, concluímos que $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

4.5 Grupos de ordem 8

O grupos

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{e} \quad D_4$$

possuem ordem 8. Não são isomorfos entre si, os estudaremos.

O grupo $\mathbb{Z}_8$ é cíclico; isto significa que existe $\alpha \in \mathbb{Z}_8$ tal que $\mathcal{O}(\alpha) = 8$, especificamente este possui quatro elementos de ordem 8, α assume os valores $\overline{1}, \overline{3}, \overline{5}$ e $\overline{7}$, enquanto os demais grupos não pois tais elementos, portanto $\mathbb{Z}_8$ não é isomorfo a nenhum dos grupos acima citados.

O grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$ não é cíclico, mas é abeliano possuindo elementos cuja ordem é 4 ou 2, os elementos de ordem 4 são estes $(\overline{1},\overline{0})$; $(\overline{1},\overline{1})$; $(\overline{3},\overline{0})$ e $(\overline{3},\overline{1})$.

O grupo $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ não é cíclico, mas é abeliano, pois todos os seus elementos diferentes da identidade tem ordem 2.

O grupo D_4 das simetrias espaciais de um quadrado, não é abeliano, possui 5 elementos de ordem 2, impossibilitando seu isomorfismo com $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, e dois elementos de ordem 4, logo não é isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Mostremos então que os quatro grupos acima mencionados juntamente com o grupo dos Quatérnios Q_3, grupo multiplicativo com a operação de matrizes, dado por

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

com $i \in \mathbb{C}$ tal que $i^2 = -1$ e :

$$id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$D = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, F = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, G = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

são, a menos de isomorfismo, os únicos grupos de ordem 8.

Tomando dois elementos de Q_3 e realizando a operação, temos:

$$AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = F$$

$$BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = G.$$

Observa-se que o grupo Q_3 não é isomorfo a nenhum dos grupos $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, visto que estes são abelianos. Para mostrar que Q_3 e D_4 não são isomorfos,

bastar notar que Q_3 possui apenas um elemento de ordem 2, sendo este

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

enquanto D_4 como já visto possui cinco elementos de ordem 2.

O grupo Q_3 é caracterizado pela relação

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

e o grupo D_4 por

$$\begin{cases} D_4 &= \langle \alpha, \beta \rangle \\ \alpha_4 &= e \\ \beta_2 &= e \\ \beta\alpha &= \alpha^3\beta, \end{cases}$$

Logo grupo Q_3 não é isomorfo a D_4. De fato,

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

e

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

ou seja, α e β são dois elementos de D_4 que têm ordem 2; enquanto apenas um elemento de Q_3,

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = id$$

possui essa mesma ordem.

Seja agora G um grupo qualquer de ordem 8. Dado $\alpha \in G - \{e\}$, temos pelo Teorema Lagrange, que as possíveis ordens de α são 2, 4 e 8. Analisaremos os casos.

caso 1: G possui um elemento de ordem 8.

Neste caso, temos que G é cíclico e seja $\gamma \in G$ tal que $\mathcal{O}(\gamma) = 8$, portanto $G \simeq \mathbb{Z}_8$.

Caso 2: G não possui nenhum elemento de ordem 8.

Assim, dado $\alpha \in G = \{e\}$, as possíveis ordens de α são $\mathbb{O}(\alpha) = 2$ ou $\mathcal{O}(\alpha) = 4$. Consideremos os dois subcasos separadamente:

Caso 2.1: G não possui nenhum elemento de ordem 4.

Então, todos os elementos em $G - \{e\}$ são de ordem 2, por conseguinte G é a abeliano. Seja $\alpha \in G = \{e\}$ com $\mathbb{O}(\alpha) = 2$; temos que $H = \{e, \alpha\}$ é um subgrupo de G. Tome agora $\beta \in G - H$, logo $K = \{e, \alpha, \beta, \alpha\beta\}$ é um subgrupo de G. Considere $\gamma \in G - K$, temos então,

$$G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\} = \{\alpha^i\beta^j\gamma^k : i, j, k \in \{0, 1\}\}.$$

Logo a aplicação dada por

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \longrightarrow & G \\ & (\overline{i}, \overline{j}, \overline{k}) & \longmapsto & \alpha^i\beta^j\gamma^k. \end{array}$$

é um isomorfismo de grupos. A função está bem definida, analisamos um caso de compatibilidade entre as estruturas dos grupos, fazendo $\alpha = (1, 0, 0)$ e $\beta = (0, 1, 0)$, temos $\varphi(\alpha + \beta) = \varphi(1, 1, 0) = \alpha\beta = \varphi(1, 0, 0) \cdot \varphi(0, 1, 0)$., os outros casos são análogos.

A função φ é sobrejetora, pois $G = \{e, \alpha, \beta, \alpha\beta, \gamma, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\}$ e injetora com

$$\begin{array}{llll} \varphi(0,0,0) = e, & \varphi(1,0,0) = \alpha, & \varphi(0,1,0) = \beta, & \varphi(0,1,1) = \beta\gamma, \\ \varphi(0,0,1) = \gamma, & \varphi(1,1,0) = \alpha\beta, & \varphi(1,0,1) = \alpha\gamma, & \varphi(1,1,1) = \alpha\beta\gamma. \end{array}$$

Logo, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq G$

Caso 2.2: G possui um elemento de ordem 4.

Sejam $\alpha \in G$ um elemento de ordem 4 e $H = \langle \alpha \rangle$ um subgrupo de G. Considere $\beta \in G - H$ e K subgrupo de G tal que $K = \langle \alpha, \beta \rangle$. Como $\beta \notin H$, temos $|K| > 4$, pelo Teorema de Lagrange, $|K|$ divide $|G| = 8$; o que implica em

$$K = G = \langle \alpha, \beta \rangle = \{e, \alpha, \beta, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\},$$

temos $\beta \in H$, pois $\beta^2 \notin \{\beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$, como também $\beta\alpha \notin \beta^2 \notin \{e, \alpha, \alpha^2, \alpha^3, \beta\}$.

Provamos então que:

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

Vejamos agora as possibilidades para $u, s \in \{0,1,2,3\}$. A princípio, temos $\mathcal{O}(\beta\alpha\beta^{-1}) = \mathcal{O}(\alpha) = 4$, dessa forma $s = 1$ ou $s = 3$. Agora, $\beta \notin \{\alpha, \alpha^3\}$, caso contrário $\mathcal{O}(\beta^2)$ seria 4 e β teria ordem 8, absurdo, pois por hipótese G não possui elementos de ordem 8, ou ordem de β seria 4, implicando em $\mathcal{O}(\beta^2) = 2$, absurdo, pois $\beta^2 = \alpha^u$ com $u \in \{0,1,2,3\}$. Temos portanto, $u = 0$ ou $u = 2$ e $s = 1$ ou $s = 3$. Analisemos:

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

$$(1) \begin{cases} |G| &= 8 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^4 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha\beta \end{cases} \quad \text{e} \quad (2) \begin{cases} |G| &= 8 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^4 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha^3\beta \end{cases} \tag{4.2}$$

Pelo item 2, do Teorema 3.2, em cada um dos casos em 4.2, temos que existe no máximo um grupo, a menos de isomorfismo, satisfazendo as condições. Tais grupos existem, para o caso (1) tomamos o grupo $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ e para o caso (2) temos $G = D_4$.

Agora se $u = 2$, temos analogamente os dois casos correspondentes a $s = 1$ e $s = 3$:

$$(3)\ \begin{cases} |G| &= 8 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^4 &= e \\ \beta^2 &= \alpha^2 \\ \beta\alpha &= \alpha\beta \end{cases} \quad \text{e} \quad (4)\ \begin{cases} |G| &= 8 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^4 &= e \\ \beta^2 &= \alpha^2 \\ \beta\alpha &= \alpha^3\beta \end{cases} \tag{4.3}$$

Pelo item 2, do Teorema 3.2, em cada um dos casos em 4.3, temos que existe no máximo um grupo, a menos de isomorfismo, satisfazendo as condições. É fácil ver que tais grupos existem, para o caso (3) tomamos o grupo $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ e para o caso (2) temos $G = Q_3$.

Concluímops que, a menos de isomorfismos

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4 \ \text{ e } \ Q_3$$

são os únicos 5 grupos de ordem 8.

Observação 4.1 Os casos (1) e (3) evidenciam que um mesmo grupo pode ser apresentado, por meio de geradores e relações, de forma distintas. Ou seja, mudando os geradores podemos alterar as relações entre eles.

4.6 Grupos de ordem 9

Estudaremos os grupos $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$, estes de ordem 9. Não são isomorfos, visto que $\mathbb{Z}_9$ possui elementos de ordem 9, o que não ocorre com $\mathbb{Z}_3 \times \mathbb{Z}_3$ que não possui tais elementos. Vamos mostrar que, a menos de isomorfismos, estes dois grupos são os únicos de ordem 9.

Seja G um grupo não cíclico de ordem 9. Pelo Teorema de Lagrange, todos os seus elementos são tais que $x \in G - \{e\}$ onde $\mathcal{O}(x) = 3$. Tome $e \neq \alpha \in G$ e

$\beta \in G - \langle\alpha\rangle$. Então, $\langle\alpha\rangle = \{\alpha, \alpha^2, \alpha^3 = e\} \in G$, $\langle\beta\rangle = \{\beta, \beta^2, \beta^3 = e\} \in G$ onde $\alpha^i \neq \beta^j \quad \forall i, j \in \{1, 2\}$. Portanto, elementarmente

$$G = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta, \beta^2, \alpha\beta^2, \alpha^2\beta^2\}$$

por conseguinte,

$$\begin{cases} |G| &= 9 \\ G &= \langle\alpha, \beta\rangle \\ \alpha^3 &= e \\ \beta^3 &= e. \end{cases}$$

Precisa-se determinar o valor de $\beta\alpha$, para tanto, temos $\beta\alpha \notin \{e, \alpha, \alpha^2, \beta, \beta^2\}$. Analisaremos agora os casos para os demais elementos do grupo, sempre fazendo uso do item 2 do Teorema 3.2, logo em cada caso temos no máximo um grupo, a menos de isomorfismo.

Caso 1: $\beta\alpha = \alpha\beta$.

Tal grupo existe, basta tomar $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

Caso 2: $\beta\alpha = \alpha^2\beta$.

Tal grupo não existe, pois $2^3 = 8 \not\equiv (1 \mod 3)$.

Caso 3: $\beta\alpha = \alpha\beta^2$.

Tal grupo não existe, caso contrário, tomando $A = \beta^2$ e $B = \alpha$, terímos $G = \langle A, B\rangle$, com $A^3 = e, B^3 = e, BA = \alpha\beta^2 = \beta\alpha = A^2B$, o que não é verdade, pois $2^3 = 8 \not\equiv (1 \mod 3)$.

Caso 4: $\beta\alpha = \alpha^2\beta^2$.

Tal grupo não existe, pois senão teríamos que

$$(\alpha\beta)^2 = \alpha\beta\alpha\beta = \alpha(\beta\alpha)\beta = \alpha(\alpha^2\beta^2)\beta = e,$$

absurdo, pois sabemos que $\mathcal{O}(\alpha\beta) = 3$.

Conclui-se que, a menos de isomorfismos, os grupos $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$ são os únicos de ordem 9.

4.7 Grupos de ordem 10

Sabemos que os grupos $\mathbb{Z}_{10}$ e D_5 possuem ordem 10. não são isomorfos entre si. O grupo $\mathbb{Z}_{10}$ é cíclico; isto significa que existe $\alpha \in \mathbb{Z}_{10}$ tal que $\mathcal{O}(\alpha) = 10$, especificamente este possui quatro elementos de ordem 8, α assume os valores $\overline{1}, \overline{3}, \overline{7}$ e $\overline{9}$, Já D_5 não o é.

Seja G um grupo arbritário tal que $|G| = 10$, vamos mostrar que, $G \simeq \mathbb{Z}_{10}$ ou $G \simeq D_5$. Isso consiste em demonstrar as seguintes proposições:

Proposição 4.3 *O grupo G possui um elemento α de ordem 5*

Demonstração: Consideramos dois casos:

1. G é um grupo cíclico gerado por um elemento α. Neste caso, temos que $G = \langle\alpha\rangle$ para algum $\alpha \in G$, assim $\mathcal{O}(\alpha) = 10$. Assim, basta considerarmos o elemento $\beta = \alpha^2$, e então $\mathcal{O}(\beta) = 5$.

2. O grupo G não é cíclico. Suponhamos por absurdo que nenhum elemento de G tem ordem 5, $\mathcal{O}(\beta) \neq 5, \quad \forall \beta \in G$. Assim pelo Teorema de Lagrange, todo elemento $x \in G - \{e\}$ tem que ter ordem 2, por isso $x = x^{-1}$, pelo Corolário 2.3 G é abeliano. Tomando dois elementos $a, b \in G - \{e\}$, o conjunto $H = \{e, a, b, ab\}$ é um subgrupo de G, tal que $|H| = 4$, o que contraria o Teorema de Lagrange, já que 4 não divide 10. Logo, existe $\alpha \in G$ onde $\mathcal{O}(\alpha) = 5$.

Proposição 4.4 *O grupo G possui um elemento β de ordem 2 e $G = \langle\alpha, \beta\rangle$.*

Demonstração: Se G é cíclico tal que $G = \langle\gamma\rangle$, tome $\beta = \gamma^5$.

Se G não é cíclico, tome $\beta \in G - \langle\alpha\rangle$; temos pelo Teorema de Lagrange que $\mathcal{O}(\beta) = 2$ ou $\mathcal{O}(\beta) = 5$. Suponhamos que $\mathcal{O}(\beta) = 5$, mas sendo subgrupo de $G = \langle\alpha\rangle$, a interseção $\langle\alpha\rangle \cap \langle\beta\rangle$ tem ordem igual a um divisor de 5, portanto igual a 1(Teorema de Lagrange). Assim, $e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \beta^2, \beta^3, \beta^4$ representam em G nove elementos distintos, mas como temos $\alpha\beta$ e $\alpha^2\beta$ são outros dois elementos de G claramente distintos dos demais. Conclusão, obtivemos que o grupo G possui pelo menos onze elementos , absurdo. Logo, $\mathcal{O}(\beta) = 2$.

Fica então claro que

$$G = \langle \alpha, \beta \rangle = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta, \alpha^4\beta\}.$$

Precisa-se determinar o valor de $\beta\alpha$, para tanto, temos $\beta\alpha \notin \{e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta\}$ e pelo Teorema 3.2 $\beta\alpha \neq \alpha^2\beta$ já que $2^2 = 4 \not\equiv (1 \mod 5)$ e $3^2 = 9 \not\equiv (1 \mod 5)$. Desta forma, temos duas possibilidades:

$$(1) \begin{cases} |G| = 10 = 5 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^5 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases} \qquad (2) \begin{cases} |G| = 10 = 5 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^5 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^4\beta \end{cases}$$

Logo, pelo item 2 do Teorema 3.2, em cada um dos casos, temos no máximo um grupo, a menos de isomorfismos, que satisfaz as condições. Tais grupos existem, no caso (1) tome $G = \mathbb{Z}_{10}$ e no caso (2) $G = D_5$. Note que o grupo $\mathbb{Z}_2 \times \mathbb{Z}_5$ também satisfaz as condições em (1) e pela unicidade estabelecida no item 2 do Teorema 3.2, temos que $\mathbb{Z}_2 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{10}$.

Conclui-se que $\mathbb{Z}_{10}$ e D_5 são os dois únicos grupos de ordem 10, a menos de isomorfismos.

Considerações Finais

O presente trabalho propiciou a exposição de uma importante parte da Teoria dos Grupos, visto que esta abrange tópicos de complexidade considerável. O estudo da caracterização dos grupos G com $|G| \leq 11$ possibilitou revisitar conceitos elementares da Teoria dos Grupos, tais como os de grupos cíclicos, Teorema de Lagrange e grupos finitamente gerados por dois elementos; e ter contato com conceitos mais avançados desta.

Referências Bibliográficas

[1] Boyer.C.B., Merzbach.U.C. *História da Matemática.* 3 ed. Blucher, São Paulo, 2015.

[2] Domingues, H. H. *Álgebra Moderna.* 4 ed. - São Paulo: Atual Editora, 2003.

[3] Farias, J. G. S. *Caracterização dos Grupos G com* $|G| \leq 8$. Campina Grande, 2011.

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

[5] Garcia, A. E Lequain, Y *Elementos de Álgebra.* Projeto Euclides, IMPA, 2001.

[6] Gonçalves, A. *Introdução à Álgebra.* IMPA, 5. ed.,Rio de Janeiro, 2009.

[7] Milies, C. P. *Breve História da Álgebra Abstrata.* II Bienal da Sociedade Brasileira de Matemática (www.bienasbm.ufba.br/M18.pdf), 2004.

[8] Vieira, V.L. *Álgebra Abstrata para Licenciatura.* 2 ed. Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.