UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

RENNER DA SILVA NASCIMENTO

UM ESTUDO SOBRE GRUPOS FINITOS: DETERMINANDO A QUANTIDADE DE SUBGRUPOS DE ÍNDICE 2.

CAMPINA GRANDE
2021

RENNER DA SILVA NASCIMENTO

UM ESTUDO SOBRE GRUPOS FINITOS: DETERMINANDO A QUANTIDADE DE SUBGRUPOS DE ÍNDICE 2.

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

Área de concentração: Álgebra

Orientador: Profa. Dra. Emanuela Régia de Sousa Coelho

CAMPINA GRANDE
2021

N244e Nascimento, Renner da Silva.

Um estudo sobre grupos finitos [manuscrito] : determinando a quantidade de subgrupos de índice 2 / Renner da Silva Nascimento. - 2021.

56 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2021.

"Orientação : Profa. Dra. Emanuela Régia de Sousa Coelho , Departamento de Matemática - CCT."

1. Grupos finitos. 2. Isomorfismo. 3. Espaços vetoriais. 4. Álgebra. I. Título

21. ed. CDD 512

Elaborada por Lucas H. A. da Silva - CRB - 15/898 BC/UEPB

RENNER DA SILVA NASCIMENTO

UM ESTUDO SOBRE GRUPOS FINITOS: DETERMINANDO A QUANTIDADE DE SUBGRUPOS DE ÍNDICE 2.

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

Área de concentração: Álgebra

Aprovado em: 19/10/2021

BANCA EXAMINADORA

Profa. Dra. Emanuela Régia de Sousa Coelho (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Profa. Dr. Vandenberg Lopes Vieira
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Israel Buriti Galvão
Universidade Estadual da Paraíba (UEPB)

À minha querida família, DEDICO.

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida, por me manter firme e forte durante toda a caminhada acadêmica. Por me manter de cabeça erguida para a realização dos meus sonhos.

Agradeço aos meus pais Ednalva e Linaldo (*in memorian*) e minha irmã, Rennally, por todo o apoio e carinho que precisava e por me incentivar a seguir em frente em busca de meus objetivos.

Agradeço à minha orientadora, Emanuela Régia de Sousa Coelho, por todo o suporte que me deu durante a minha caminhada acadêmica e por ter dedicado o seu tempo para me ajudar na realização deste trabalho de conclusão de curso.

Agradeço ao Professor Doutor Vandenberg Vieira pela oportunidade que me concedeu na participaçao de dois projetos no Programa Institucional de Bolsas de Iniciação Científica - PIBIC(UEPB/CNPq), além da sua disponibilidade e compreensão, orientando e guiando o desenrolar do meu trabalho, manifestando sempre as suas opiniões enriquecedoras para o crescimento do projeto e enriquecimento da minha formação.

Agradeço a todos que conheci durante o curso, em especial, aos meus colegas: Igor Mateus, William, Yalorisa, Hellen, Rozilane e tantos outros que não citarei aqui para não tornar a lista tão cansativa. A vocês, meu muito obrigado!

Por fim, agradeço a todos que de alguma forma contribuíram para a realização desta grande etapa na minha vida.

“Quando algo é importante o suficiente, você realiza, mesmo que as chances não estejam a seu favor.”
Elon Musk

RESUMO

O presente trabalho é um estudo sobre grupos finitos, mais especificamente, apresenta um resultado que determina a quantidade de subgrupos de índice 2 existente entre eles. Para o desenvolvimento do trabalho propomos um abordagem didática do Artigo intitulado "*How Rare Are Subgroups of Index 2?*"de Jean Bernard Nganou e, para isso, utilizamos alguns conceitos e resultados de Álgebra Abstrata e Álgebra Linear, tais como: Grupos, Classes Laterais, Isomorfismos, Espaços Vetoriais, Combinação Linear, Hiperplanos, entre outros.

Palavras-chave: Grupos. Isomorfismos. Espaços Vetoriais.

ABSTRACT

The present work aims to carry out a study on finite groups, more specifically, to present a result that determines the amount of 2 index subgroups existing among them. For the development of the work, we propose a didactic approach of the article entitled "*How Rare Are Subgroups of Index 2?*"by Jean Bernard Nganou and, for that, we will use some concepts and results of Abstract Algebra and Linear Algebra, such as: Groups, Classes Laterals, Isomorphisms, Vector Spaces, Linear Combination, Hyperplanes, among others.

Keywords: Groups. Isomorphisms. Vector Spaces.

SUMÁRIO

Página

1 INTRODUÇÃO

Este trabalho consite em apresentar um resultado que determina a quantidade de subgrupos de índice 2 de grupos finitos e, para isto, é necessário abordar alguns conceitos e resultados preliminares de Álgebra Abstrata e Álgebra Linear. Este resultado é apresentado no artigo "How Rare Are Subgroups of Index 2?"de Nganou (2012). Assim, este trabalho consiste em uma apresntação didática do artigo de Nganou, fazendo com que o texto se torne o mais autossuficiente possível.

Segundo Souza (2012), a concepção de Grupo é uma das formas mais utilizadas na Matemática Moderna. Dentre as diversas áreas das Ciências, onde os conceitos da Teoria dos Grupos são fundamentais, estão incluídas a Cristalografia, a Teoria Quântica de Campos, a Estrutura Atômica e Molecular, entre outros. Além disso, no próprio estudo da Álgebra Abstrata, é utilizada para a construção de outras Estruturas Algébricas como: Espaços Vetoriais, Anéis e Corpos, uma vez que estes podem ser vistos como grupos munidos de operações e axiomas complementares.

O estudo da Teoria de Grupos teve início com o trabalho do matemático francês Évariste Galois (1811-1832), tratando da solubilidade por radicais de equações polinomiais, para isso, Galois contou com a valiosa contribuição de outros grandes matemáticos como o italiano Paolo Ruffini (1765-1822), o francês Joseph Louis Lagrange (1736-1813), o suíço Leonard Euler (1707-1783), o alemão Carl Friedrich Gauss (1777-1855) e o norueguês Niels Henrik Abel (1802-1829), que colaboraram através de estudos voltados para a teoria dos números, a geometria e a teoria das equações algébricas.

O britânico Arthur Cayley (1821-1895) foi o primeiro a definir o conceito moderno de Grupo, o qual disse: "Um grupo é definido por meio de leis que combinam seus elementos". Ademais, tal conceito não ganhou real aceitação até as apresentações do alemão Walther Franz Anton von Dyck (1856-1934), em 1882. O incentivo para estudar grupos de dimensão infinita veio da geometria e topologia por causa do norueguês Marius Sophus Lie (1842-1899), do francês Henri Poincaré (1854-1912), do alemão Felix Klein (1840-1925), do alemão Max Dehn (1878-1952) e do também norueguês Peter Ludwig Mejdell Sylow (1832-1918). Nessa época, o estudo dos grupos apresentou sua forma abstrata independente e se desenvolveu muito rapidamente.

A primeira grande etapa da teoria dos grupos finitos obteve o seu ápice no período imediatamente antes da Primeira Guerra Mundial, com os trabalhos do inglês William Burnside (1852-1927), do alemão Ferdinand Georg Frobenius (1849-1917) e do bielorrusso Issai Schur (1875-1936).

Após 1928, grandes contribuições para o desenvolvimento da Teoria de Grupos Finitos foram feitas pelo alemão Helmut Wielandt (1910-2001) e pelo inglês Philip Hall (1904-1982),e no campo de representações de grupos, as contribuições vieram do alemão

Richard Dagobert Brauer (1901-1977). Em 1982, com a participação de centenas de matemáticos, coordenados pelo norte-americano Daniel Gorenstein (1923-1992) completou-se a classificação dos grupos finitos.

Hoje, a teoria dos grupos está separada em diversas subáreas e os interesses são muitos, espacialmente, por matemáticos e físicos.

A proposta deste trabalho se trata em determinar a quantidade de subgrupos de índices 2 de grupos finitos, utilizando resultados da Álgebra Abstrata e da Álgebra Linear. Para alcançar a nossa finalidade precisamos estudar conceitos e resultados necessários para o bom entendimento da prova do resultado principal.

O trabalho está organizado da seguinte forma: o Primeiro Capítulo possui resultados imprecindíveis da Álgebra Abstrata e da Álgebra Linear para o bom entendimento do Capítulo seguinte.

O Segundo Capítulo se trata da prova do Teorema principal do trabalho que se trata da quantidade de subgrupos de índice 2 de grupos finitos, a partir de uma abordagem didática da referência Nganou (2012).

2 PRELIMINARES

Nesta seção apresentamos conceitos e resultados para o entendimento do Capítulo Principal desta monografia a fim de tornar o texto autossuficiente. Mostraremos inicialmente resultados de Álgebra Abstrata - foco principal do nosso trabalho- e, em seguida, resultados de Álgebra Linear.

2.1 Tópicos em Álgebra Abstrata

Para esta seção nos baseamos em Alencar Filho (1981), Garcia e Lequain (2001), Domingues (2003), e Vieira (2015). Todos os resultados serão provados, a menos dos que fogem do escopo do nosso trabalho, sendo encontrados nas referências devidamente mencionadas.

Definição 2.1 (Operações Binárias)**.** Seja A um conjunto não vazio. Uma aplicação $f : A \times A \to A$ chama-se **operação binária** sobre A.

Exemplo 2.1. As funções $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dadas por $f(a,b) = a + b$ e $h(a,b) = a \cdot b$ são operações binárias sobre $\mathbb{N}$, chamadas de adição e multiplicação, respectivamente. Por exemplo, $f(4,5) = 4 + 5 = 9$ e $h(4,5) = 4 \cdot 5 = 20$. Podemos estender estas operações aos conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Observação 2.1. Vamos omitir o nome operações binárias e, a partir de agora, chamaremos apenas de operação.

2.1.1 Grupos

Definição 2.2 (Grupos)**.** Seja G um conjunto não vazio munido da operação $\cdot$. G é intitulado de grupo quando atende as seguintes propriedades:

i) Associatividade da operação, ou seja,

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

ii) Existência do elemento neutro para $\cdot$, ou seja,

$$\exists\ e \in G \text{ tal que } a \cdot e = e \cdot a = a, \forall\ a \in G.$$

iii) Existência do inverso para todo elemento em G segundo à operação $\cdot$, ou seja,

$$\forall\ a \in G, \exists\ a' \in G \text{ tal que } a \cdot a' = a' \cdot a = e.$$

Nesse caso, o elemento a' é dito inverso de a e é denotado por a^{-1}.

O grupo assim determinado será denotado por $(G, \cdot)$.

Definição 2.3. Um grupo $(G, \cdot)$ é dito **abeliano** ou **comutativo** quando

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

ou seja, quando a operação em G for comutativa.

Observação 2.2. Quando não houver confusão, identificaremos o par $(G, \cdot)$ apenas por G e escreveremos ab no lugar de $a \cdot b$.

Observação 2.3. Se G é um grupo, então

1. O elemento neutro é único;

   Sejam e_1 e e_2 elementos neutros em G, da definição de elemento neutro, tem-se

   $$e_1 = e_1 e_2 = e_2.$$

2. Se $a \in G$, então a^{-1} é único

   De fato, sejam a' e a'' inversos de a, em G. Temos

   $$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

3. $(a^{-1})^{-1} = a$ para todo $a \in G$. Segue imediatamente da definição de inverso.

4. $(ab)^{-1} = b^{-1}a^{-1}$ para todo $a, b \in G$.

   Temos, para $a, b \in G$,

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

   e, analogamente, $(b^{-1}a^{-1})(ab) = e.$, Logo, temos $(ab)^{-1} = b^{-1}a^{-1}$.

Exemplo 2.2. O conjunto $M_{m\times n}(\mathbb{R})$, das matrizes sobre $\mathbb{R}$ com m linhas e n colunas, é um grupo sob a adição usual de matrizes. De fato, sejam A, B e $C \in M_{m\times n}(\mathbb{R})$ com

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \dots & \vdots \\ b_{n1} & \dots & b_{nm} \end{pmatrix} \text{ e } C = \begin{pmatrix} c_{11} & \dots & c_{1m} \\ \vdots & \dots & \vdots \\ c_{n1} & \dots & c_{nm} \end{pmatrix}.$$

Temos

i) $A+(B+C) = (A+B)+C$, pois para cada $a_{i,j} \in A, b_{i,j} \in B$ e $c_{i,j} \in C$ pelas propriedades sobre $\mathbb{R}$ temos $a_{i,j} + (b_{i,j} + c_{i,j}) = (a_{i,j} + b_{i,j}) + c_{i,j}$.

ii) Seja

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in M_{m\times n}(\mathbb{R})$$

e considere

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in M_{m\times n}(\mathbb{R})$$

temos

$A+0 = A = 0+A$, pois para cada $a_{i,j} \in A$ e $0_{i,j} \in 0$, pelas propriedades sobre $\mathbb{R}$ temos, $a_{i,j} + 0_{i,j} = a_{i,j} = 0_{i,j} + a_{i,j}$.

iii) Para

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in M_{m\times n}(\mathbb{R}),$$

seja

$$-A = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix} \in M_{m\times n}(\mathbb{R}),$$

temos

$A + (-A) = 0 = -A + A$, pois dado $a_{i,j} \in A$ e $-a_{i,j} \in -A$, pelas propriedades sobre $\mathbb{R}$, temos $a_{i,j} - a_{i,j} = 0 = -a_{i,j} + a_{i,j}$.

iv) Sejam $A, B \in M_{m\times n}(\mathbb{R})$, com

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \dots & \vdots \\ b_{n1} & \dots & b_{nm} \end{pmatrix}$$

temos

$A + B = B + A$, pois dado $a_{i,j} \in A$ e $b_{i,j} \in B$, pelas propriedades vistas sobre $\mathbb{R}$ temos, $a_{i,j} + b_{i,j} = b_{i,j} + a_{i,j}$.

Isso mostra que $(M_{m\times n}(\mathbb{R}), +)$ é um grupo. Além disso, o mesmo é abeliano.

Exemplo 2.3. O conjunto dos números inteiros $\mathbb{Z}$, munido da soma usual, é um grupo abeliano, cujo elemento neutro é o 0 (zero) e se $a \in \mathbb{Z}$, $-a$ é o inverso de a. Este resultado se estende para os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Antes de mostrarmos o próximo exemplo, chamado de grupo das **classes residuais**, devemos atentar algumas considerações importantes.

Definição 2.4. Seja $n \in \mathbb{N}$ um número fixo. Dois núemros $a, b \in \mathbb{Z}$ chamam-se **congruentes** módulo n, se $a - b$ é múltiplo de n. Em símbolos, $a \equiv b \pmod{n}$. Assim,

$$a \equiv b \pmod{n} \Leftrightarrow n|(a-b).$$

Dado um inteiro positivo $n > 1$, particionamos o conjunto $\mathbb{Z}$ em subconjuntos, cada um formado pelos números inteiros que deixam o mesmo resto quando divididos por n. Desta maneira, temos os seguintes subconjuntos:

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z};\ x \equiv 0 \pmod{n}\},\\
\overline{1} &= \{x \in \mathbb{Z};\ x \equiv 1 \pmod{n}\},\\
&\vdots\\
\overline{n-1} &= \{x \in \mathbb{Z};\ x \equiv n-1 \pmod{n}\},
\end{aligned}$$

Observação 2.4. Paramos em $\overline{n-1}$, pois teremos repetições, ou seja, $\overline{n} = \overline{0}, \overline{n+1} = \overline{1}, \ldots$

É importante notar que, dados dois números inteiros a e b, $\overline{a} = \overline{b}$, se e somente se, o resto da divisão módulo n de a e b são iguais.

Observação 2.5. Se $n > 0$, $a, b \in \mathbb{Z}$ escritos da seguinte forma

$$a = nq_1 + r_1 \quad \text{e} \quad b = nq_2 + r_2$$

com $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ $(0 \leq r_1, r_2 < n)$. Então,

$$a \equiv b \pmod{n} \Leftrightarrow r_1 = r_2.$$

Prova. Se $r_1 = r_2$ temos $a - b = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2)$, logo $n|(a-b)$. Isto significa $a \equiv b \pmod{n}$.

Se $a \equiv b \pmod{n}$, temos $n|(a-b) = n(q_1 - q_2) + (r_1 - r_2)$ e daí, $n|(r_1 - r_2)$. Mas de $0 \leq |r_1 - r_2| < n$ concluímos então $r_1 - r_2 = 0$, logo $r_1 = r_2$.

■

Definição 2.5. Definimos a **classe residual módulo** n do elemento $a \in \mathbb{Z}$, representado por $\overline{a}$, como sendo o subconjunto

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a \pmod{n}\}.$$

O conjunto de todas as classes residuais módulo n será indicada por $\mathbb{Z}_n$, ou seja,

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

A partir das operações de adição e multiplicação em $\mathbb{Z}$, podemos definir operações de adição e multiplicação sobre $\mathbb{Z}_n$ da seguinte forma: dados $\overline{a}, \overline{b} \in \mathbb{Z}_n$, defininimos as operações de adição e multiplicação de $\overline{a}$ e $\overline{b}$ respectivamente, por

$$\overline{a} + \overline{b} = \overline{a + b} \text{ e } \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

A seguinte proposição nos diz que estas operações estão bem definidas.

Proposição 2.1. *Seja $n > 1$ um número natural. Então,*

$$\begin{array}{rccc} + : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b} = \overline{a + b} \end{array} \quad e \quad \begin{array}{rccc} \cdot : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array}$$

determinam, respectivamente, as operações de adição e multiplicação sobre $\mathbb{Z}_n$.

Prova. Sejam $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tais que

$$\overline{a_1} = \overline{a_2} \quad \text{e} \quad \overline{b_1} = \overline{b_2} \text{ em } \mathbb{Z}_n.$$

Precisamos provar que

$$\overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2} \quad \text{e} \quad \overline{a_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{b_2},$$

isto é, que os resultados destas operações não dependem da escolha dos representantes das classes $\overline{a_1}$ e $\overline{b_1}$. Por hipótese, $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$ e, por definição, $a_1 \equiv a_2 \pmod{n}$ e $b_1 \equiv b_2 \pmod{n}$. Desse modo,

$$a_1 = a_2 + n \cdot k_1 \quad \text{e} \quad b_1 = b_2 + n \cdot k_2, \tag{2.1}$$

com $k_1, k_2 \in \mathbb{Z}$. Somando a_1 com b_1, temos

$$a_1 + b_1 = a_2 + b_2 + n \cdot k_3, \text{ com } k_3 = k_1 + k_2 \in \mathbb{Z},$$

isto é,

$$(a_1 + b_1) - (a_2 + b_2) = n \cdot k_3$$

ou seja,

$$n \mid [(a_1 + b_1) - (a_2 + b_2)]$$

daí,

$$(a_1 + b_1) \equiv (a_2 + b_2) \pmod{n}$$

ou, equivalentemente,

$$\overline{a_1 + b_1} = \overline{a_2 + b_2}.$$

Dessa forma,

$$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} + \overline{b_2}.$$

Consideremos agora a multiplicação. Das igualdades em 2.1, temos

$$\begin{aligned} a_1 \cdot b_1 = (a_2 + n \cdot k_1)(b_2 + n \cdot k_2) &= a_2 \cdot b_2 + a_2 k_2 n + b_2 k_1 n + k_1 k_2 n^2 \\ &= a_2 \cdot b_2 + n \cdot (a_2 k_2 + b_2 k_1 + k_1 k_2 n) \\ &= a_2 \cdot b_2 + n \cdot k_4 \end{aligned}$$

em que $k_4 = a_2 k_2 + b_2 k_1 + k_1 k_2 n \in \mathbb{Z}$. Dessa forma,

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 (\mathrm{mod} n)$$

ou, equivalentemente,

$$\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}.$$

Assim,

$$\overline{a_1} \cdot \overline{b_1} = \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2} = \overline{a_2} \cdot \overline{b_2}.$$

■

Exemplo 2.4. Sejam $n > 1$ um inteiro e $\overline{a} = \{x \in \mathbb{Z}; x \equiv a \pmod{n}\}$. Considerando o conjunto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\},$$

munido da operação de adição sobre $\mathbb{Z}_n$ dada pela Proposição 2.1, $(\mathbb{Z}_n, +)$, é um grupo abeliano. De fato,

i) Dados $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$ temos:

$$\begin{aligned} \overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + \overline{(y+z)} &&= \overline{x + (y+z)} \\ &= \overline{(x+y) + z} &&= \overline{x+y} + \overline{z} \\ &= (\overline{x} + \overline{y}) + \overline{z}. \end{aligned}$$

ii) Considerando $\overline{0} \in \mathbb{Z}_n$, temos

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x} = \overline{0+x} = \overline{0} + \overline{x}, \forall\ \overline{x} \in \mathbb{Z}_n.$$

Logo, $\overline{0}$ é neutro em $\mathbb{Z}_n$.

iii) Para $\overline{x} \in \mathbb{Z}_n$, considere $\overline{n-x} \in \mathbb{Z}_n$, temos

$$\overline{x} + \overline{n-x} = \overline{x + (n-x)} = \overline{n} = \overline{0}.$$

Da mesma forma, temos

$$\overline{n-x}+\overline{x}=\overline{(n-x)+x}=\overline{n}=\overline{0}.$$

Logo, $\overline{n-x}$ é inverso de $\overline{x}\in\mathbb{Z}_n$.

iv) Dados $\overline{x},\overline{y}\in\mathbb{Z}_n$,

$$\overline{x}+\overline{y}=\overline{x+y}=\overline{y+x}=\overline{y}+\overline{x}.$$

Portanto, $(\mathbb{Z}_n,+)$ é um grupo abeliano.

Exemplo 2.5. Considerando o conjunto $\mathbb{Z}_n$ e a operação de produto da Proposição 2.1 acima, $(\mathbb{Z}_n,\cdot)$ não é um grupo. De fato,

i) Para todo $\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_n$, temos:

$$\begin{aligned}\overline{x}\cdot(\overline{y}\cdot\overline{z}) &= \overline{x}\cdot\overline{(y\cdot z)} &&= \overline{x\cdot(y\cdot z)}\\ &= \overline{(x\cdot y)\cdot z} &&= \overline{(x\cdot y)}\cdot\overline{z}\\ &= (\overline{x}\cdot\overline{y})\cdot\overline{z}.\end{aligned}$$

ii) Considerando $\overline{1}\in\mathbb{Z}_n$, temos

$$\overline{x}\cdot\overline{1}=\overline{x\cdot 1}=\overline{x}=\overline{1\cdot x}=\overline{1}\cdot\overline{x},\ \forall\ \overline{x}\in\mathbb{Z}_n$$

logo, $\overline{1}$ é o neutro em $\mathbb{Z}_n$.

iii) Para $\overline{0}\in\mathbb{Z}_n$, não existe $\overline{a}\in\mathbb{Z}_n$, tal que

$$\overline{0}\cdot\overline{a}=\overline{1}=\overline{a}\cdot\overline{0}.$$

De fato, se existisse $\overline{a}\in\mathbb{Z}_n$ como nas condições acima, teríamos

$$\overline{0}=\overline{0}\cdot\overline{a}=\overline{1}$$

logo, $1\equiv 0(\mathrm{mod}\ n)$, o que é um absurdo, uma vez que $n>1$.

iv) Para $\overline{x},\overline{y}\in\mathbb{Z}_n$, temos

$$\overline{x}\cdot\overline{y}=\overline{x\cdot y}=\overline{y\cdot x}=\overline{y}\cdot\overline{x}.$$

Como o $\overline{0}$ não possui inverso com respeito a operação ' $\cdot$ ', então $(\mathbb{Z}_n,\cdot)$ não é um grupo, embora as outras propriedades sejam satisfeitas, inclusive a comutatividade.

Exemplo 2.6. Considere os grupos $(G_1, \star)$ e $(G_2, \triangle)$. O produto cartesiano $G_1 \times G_2$ munido da operação ' $\cdot$ ' dada por

$$(a, b) \cdot (c, d) = (a \star c, b \triangle d),$$

para quaisquer (a, b) e (c, d) em $G_1 \times G_2$, é um grupo.

Solução. As operações em G_1 e G_2 são associativas, logo a operação em $G_1 \times G_2$ também o é. Agora, sejam $e_1 \in G_1$ e $e_2 \in G_2$ os elementos neutros das operações $\star$ e $\triangle$, respectivamente, então $e = (e_1, e_2) \in G_1 \times G_2$ satisfaz

$$(a, b) \cdot (e_1, e_2) = (a \star e_1, b \triangle e_2) = (a, b) = (e_1 \star a, e_2 \triangle b) = (e_1, e_2) \cdot (a, b), \ \forall \ (a, b) \in G_1 \times G_2,$$

ou seja, $e = (e_1, e_2)$ é o elemento neutro da operação em $G_1 \times G_2$. Ademais, se $(a, b) \in G_1 \times G_2$, existem $a_1 \in G_1$ e $b_1 \in G_2$, tais que

$$a \star a_1 = e_1 = a_1 \star a \text{ e } b \triangle b_1 = e_2 = b_1 \triangle b.$$

Dessa forma,

$$(a, b) \cdot (a_1, b_1) = (a \star a_1, b \triangle b_1) = (e_1, e_2) = (a_1 \star a, b_1 \triangle b) = (a_1, b_1) \cdot (a, b),$$

isto é, (a_1, b_1) é o inverso de (a, b) em $G_1 \times G_2$. Portanto, $(G_1 \times G_2, \cdot)$ é um grupo.

Observação 2.6. O grupo $(G_1 \times G_2, \cdot)$ é chamado produto direto (externo) de G_1 e G_2. De modo análogo, se $G_1, G_2, \cdots, G_n$ são grupos, então o produto cartesiano

$$G_1 \times G_2 \times \cdots \times G_n = \{(x_1, x_2, ..., x_n) : x_i \in G_i, \ i = 1, 2, ..., n\}$$

por meio da operação

$$(x_1, x_2, ..., x_n) \cdot (y_1, y_2, ..., y_n) = (x_1 \cdot y_1, x_2 \cdot y_2, ..., x_n \cdot y_n).$$

é um grupo, chamado de produto direto (externo) dos grupos $G_1, G_2, ..., G_n$.

Vale ressaltar que, como as operações são efetuadas entrada a entrada, então o produto direto $G_1 \times G_2 \times ... \times G_n$ é abeliano se, e somente se, G_i é, abeliano para cada $i = 1, 2, ..., n$.

Na sequência, introduzimos um importante grupo, chamando de Grupo de Permutações.

Exemplo 2.7 (Grupo de Permutações)**.** Sejam A um conjunto não vazio e $\text{Bij}(A)$ o conjunto de todas as bijeções de A em A, ou seja,

$$\text{Bij}(A) = \{f : A \to A; f \text{ é bijetora}\}.$$

O conjunto $\mathrm{Bij}(A)$, munido da composição de funções, é um grupo, chamado de Grupo de Permutações de A e denotado por S_A.

Para provar que S_A é efetivamente um grupo, inicialmente, mostramos que S_A é fechado sobre a composição de funções. Para isso, sejam $f, g \in S_A$ e $a, b \in A$ temos,

$$(f \circ g)(a) = (f \circ g)(b) \Leftrightarrow f(g(a)) = f(g(b))$$

como f é injetora, visto $f \in S_A$ temos,

$$g(a) = g(b),$$

mas como g também é injetora, então $a = b$. Desse modo, $f \circ g$ é injetora.

Para mostrar a sobrejetividade, seja $y \in A$. Como f é sobrejetora, existe $x \in A$ tal que $f(x) = y$, mas como g também é sobrejetora, então existe $z \in A$ de forma que $x = g(z)$. Desta forma,

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

Ou seja, $f \circ g$ é sobrejetora, portanto é bijetora. Então,

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

Para provar que S_A é um grupo, devemos mostrar que o mesmo satisfaz as três propriedades da Definição 2.2.

i) **Associatividade:** Sejam as funções $f, g, h \in S_A$. Então,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

De fato, inicialmente, observa-se que as funções $h \circ (g \circ f)$ e $(h \circ g) \circ f$ têm o mesmo domínio e mesmo contradomínio. Assim, basta mostrar que $[h \circ (g \circ f)](x) = [(h \circ g) \circ f](x)$, para todo $x \in A$. Dado $x \in A$, por definição, temos

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

e

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

ou seja, $h \circ (g \circ f) = (h \circ g) \circ f$. Desta forma, mostramos que a composição de funções é associativa.

ii) **Existência do elemento neutro:** Sejam $f \in S_A$ qualquer e $id_A : A \to A$ com $Id_A(x) = x, \ \forall \ x \in A$. Se $x \in A$ temos

$$(id_A \circ f)(x) = id_A(f(x)) = f(x)$$

e

$$(f \circ id_A)(x) = f(id_A(x)) = f(x),$$

ou seja, $f \circ Id_A = f = Id_A \circ f$ e desse modo id_A é neutro em S_A.
iii) **Existência do inverso:** Dada uma função $f \in S_A$, por definição uma função $g \in S_A$ é uma inversa de f quando

$$f \circ g = id_A = g \circ f.$$

Se $f \in S_A$, então f é bijetora. Desta forma, dado $y \in A$, existe único $x \in A$ tal que $y = f(x)$. Ademais, sendo f sobrejetora, segue que $Im(f) = A$. Por essas condições, consideramos a função $g : A \to A$ dada por $g(y) = x$, em que $y = f(x)$. Portanto, para $y \in A$,

$$(f \circ g)(y) = f(g(y)) = f(x) = y,$$

isto é, $f \circ g = id_A$. Para $x \in A$,

$$(g \circ f)(x) = g(f(x)) = g(y) = x,$$

ou seja, $g \circ f = id_A$. Resta provar que $g \in S_A$.

Sejam $x_1, x_2 \in A$ tais que $g(x_1) = g(x_2)$. Deste modo,

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

pois $f \circ g = id_A$, logo, g é injetora. Agora, dado $y \in A$, como $g \circ f = id_A$,

$$(g \circ f)(y) = y \Rightarrow g(f(y)) = y,$$

isto é, y é imagem de $f(y)$ por g. Por isso, g é sobrejetora e, desse modo, g é bijetora.

Desta forma, mostramos que toda a permutação $f \in S_A$ possui inversa em S_A.

Assim, as três propriedades foram satisfeitas, logo $(S_A, \circ)$ é um grupo. O mesmo é chamado **grupo das permutações sobre** A.

De maneira particular, quando um conjunto A possui uma quantidade finita de elementos, suponhamos $A = \{1, 2, ..., n\}$, então S_A tem uma representação e nomes especiais. Nesse caso, indica-se S_A por S_n e chama-se **grupo simétrico de grau** n ou **grupo das permutações de** n **letras.**

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

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

Pela análise combinatória, constata-se que o grupo S_n possui $n!$ elementos.

Ordem de um Grupo

Definição 2.6. Um grupo $(G, \cdot)$ é dito finito quando o conjunto G é finito, nesse caso, chamamos o número de elementos de G por **ordem** de G ao qual denotaremos por $|G|$. Caso contrário dizemos que G é infinito ou tem ordem infinita.

Exemplo 2.8. Pra $n, m \in \mathbb{Z}$, $n, m > 1$, temos

$$|\mathbb{Z}_n \times \mathbb{Z}_m| = n \cdot m, \quad |\mathbb{Z}_n| = n, \quad |S_n| = n!.$$

Subgrupos

Definição 2.7. Seja G um grupo. Um subconjunto não vazio H de G é um **subgrupo** de G quando H, com a operação induzida de G, também é um grupo.

Utilizaremos a notação $H < G$ para informar que H é um subgrupo de G.

Proposição 2.2. *Sejam G um grupo e H um subgrupo de G. Então,*
(i) *O elemento neutro de H, e_H, é igual ao elemento neutro de G.*
(ii) *Dado $h \in H$, o inverso de h em H é igual ao inverso de h em G.*

Prova. (i) Para $h \in H$, em G, $h^{-1} \cdot h = e$. Mas, como em H, $h \cdot e_H = h$, então $h^{-1} \cdot h \cdot e_H = h^{-1} \cdot h$, de forma que, $e \cdot e_H = e$, isto é, $e_H = e$.
(ii) Se h^{-1} é o inverso de h em H, então $h \cdot h^{-1} = h^{-1} \cdot h = e_H = e$. Desse modo, h^{-1} é o inverso de h em G. ∎

Teorema 2.1. *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:*
(i) $h_1 \cdot h_2 \in H$ *e* $h_1^{-1} \in H, \forall\ h_1, h_2 \in H$.
(ii) $h_1 \cdot h_2^{-1} \in H, \forall\ h_1, h_2 \in H$.

Prova. Seja H é um subgrupo de G, logo H também é um grupo e, assim, as condições (i) e (ii) são satisfeitas. Reciprocamente, suponhamos que H satisfaz a condição (i). A associatividade de $\cdot$ em H, segue da Associatividade de $\cdot$ em G. Se provarmos que $e \in H$,em que e é o elemento neutro em G, a prova está completa, uma vez que, da condição (i), todos os elementos possuem inverso. Agora, de (i), para qualquer $h \in H$, temos que $h^{-1} \in H$. Assim, $h \cdot h^{-1} = e \in H$ e $H < G$.

Para a segunda parte, se H satisfaz a condição (ii), então dado $h \in H$, temos

$$h \cdot h^{-1} = e \in H,$$

logo, de (ii),

$$h^{-1} = e \cdot h^{-1} \in H, \forall h \in H.$$

Ainda, se $h_1, h_2 \in H$, então $h_2^{-1} \in H$ e, por (ii),

$$h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H.$$

Do item (i), segue que H é subgrupo de G. ■

Proposição 2.3. *Sejam G um grupo e $H_i, i \in I$, subgrupos de G. Então,*

$$H = \bigcap_{i \in I} H_i$$

é um subgrupo de G.

Com efeito, sejam $h_1, h_2 \in H$. Daí,

$$h_1, h_2 \in H_i, \forall i \in I \Rightarrow h_1, h_2^{-1} \in H_i, \forall i \in I \Rightarrow h_1 H_2^{-1} \in H_i, \forall i \in I \Rightarrow h_1 h_2^{-1} \in H.$$

Logo pelo item 2 do Teorema 2.1, $H < G$.

Observação 2.7. Segue imediatamente da Definição de Subgrupo que, se H e K são subgrupos de um mesmo grupo G, com $K \subset H$, então $K < H$.

Definição 2.8. Seja G um grupo e S um subconjunto de G. Definimos o subgrupo de G gerado por S, denotado por $\langle S \rangle$, como sendo a interseção de todos os subgrupos de G que contém S, isto é, $\langle S \rangle = \bigcap_{\substack{H<G \\ S \subseteq H}} H$.

Proposição 2.4. *Sendo G um grupo, temos:*

i) $\langle \varnothing \rangle = \{e\}$.

ii) *Se $S \subseteq G$, então $S \subseteq \langle S \rangle$. Além disso, se H é um subgrupo de G e $S \subseteq H$, então $\langle S \rangle \subseteq H$, ou seja, $\langle S \rangle$ é o menor subgrupo que contém S.*

iii) *Se $S_1 \subseteq S_2 \subseteq G$, então $\langle S_1 \rangle \subseteq \langle S_2 \rangle$.*

iv) *Se H é subgrupo de G, então $\langle H \rangle = H$.*

Prova. (i) Aplicando a definição com $S = \varnothing$, temos que $\langle \varnothing \rangle$ significa a interseção de todos os subgrupos de G que contém $\varnothing$. Por outro lado, note que qualquer subgrupo de G vai conter $\varnothing$. Como todos os subgrupos de G, contém o subgrupo $\{e\}$, temos que $\langle \varnothing \rangle = \{e\}$.

(ii) Por definição, temos que $\langle S\rangle$ é a interseção de todos os subgrupos de G contém S, logo $S \subseteq \langle S\rangle$. Para a segunda parte, se $H < G$ e $S \subseteq H$, segue que $\bigcap_{\substack{K<G \\ S\subseteq K}} K \subseteq H$, logo $\langle S\rangle \subseteq H$.
(iii) Pelo ítem (ii), $S_2 \subseteq \langle S_2\rangle$ e, por hipótese, $S_1 \subseteq S_2 \subseteq \langle S_2\rangle$. Como $\langle S_2\rangle < G$, do item (ii) segue que $\langle S_1\rangle \subseteq \langle S_2\rangle$.
(iv) Temos $H \subseteq \langle H\rangle = \bigcap_{\substack{K<G \\ H\subseteq K}} K \subseteq H$, pois $H < G$. ■

Sejam G um grupo e H um subgrupo de G. Se $H = \langle S\rangle$, dizemos que S gera H ou que S é um conjunto gerador de H. Especialmente, se $\langle S\rangle = G$, enunciamos que S gera G ou que S é um conjunto gerador de G.

Dizemos que H é finitamente gerado se H contém algum conjunto gerador finito, S, tal que $H = \langle S\rangle$.

Sendo $S = \{x_1, x_2, ..., x_n\}$ indicamos $\langle S\rangle$ simplesmente por $\langle x_1, x_2, ..., x_n\rangle$.

Teorema 2.2. *Se G é um grupo e S é um subconjunto não vazio de G, então*

$$\langle S\rangle = \{x_1x_2...x_n \mid n \in \mathbb{N},\ x_i \in S \cup S^{-1}\},\ \textit{em que}\ S^{-1} = \{x^{-1} \mid x \in S\}.$$

Prova. Inicialmente, seja $H = \{x_1x_2...x_n \mid n \in \mathbb{N}, x_i \in S \cup S^{-1}\}$ e observemos que H é subgrupo de G. De fato, dados $x, y \in H$, temos $x = x_1x_2 \cdots x_n$ e $y = y_1y_2 \cdots y_m$ com $x_i, y_j \in S \cup S^{-1}$, $\forall i = 1, ..., n$ e $\forall j = 1, ..., m$, assim

$$xy^{-1} = \underbrace{x_1...x_n}_{\in S\cup S^{-1}}\underbrace{y_m^{-1}...y_1^{-1}}_{\in S\cup S^{-1}} \in H,$$

pois, $y_j^{-1} \in S \cup S^{-1}$, $\forall j = 1, ..., m$, logo, do Teorema 2.1, $H < G$.

Agora, pela definição de H, temos $S \subseteq H$, logo, da Observação 2.4, $\langle S\rangle \subseteq H$. Por outro lado, como $S \subseteq \langle S\rangle$, temos que $S^{-1} \subseteq \langle S\rangle$, pois $\langle S\rangle < G$. Logo, $S \cup S^{-1} \subseteq \langle S\rangle$ e assim $H \subseteq \langle S\rangle$. Disso temos o resultado. ■

Exemplo 2.9. Seja $(\mathbb{Q}, +)$, o grupo aditivo dos inteiros e o subconjunto $S = \{1/3, 1/5\}$ de $\mathbb{Q}$. Assim

$$\begin{aligned}
\langle S\rangle &= \left\langle \frac{1}{3}, \frac{1}{5}\right\rangle &&= \left\{n\cdot\frac{1}{3} + m\cdot\frac{1}{5};\ n, m \in \mathbb{Z}\right\} \\
&= \left\{\frac{5n+3m}{15}; n, m \in \mathbb{Z}\right\} &&= \left\{\frac{k}{15};\ k \in \mathbb{Z}\right\} \\
&= \left\langle \frac{1}{15}\right\rangle.
\end{aligned}$$

Exemplo 2.10. Seja $\mathbb{Z}$ o grupo aditivo dos inteiros e o produto direto $\mathbb{Z}\times\mathbb{Z}$. Considere os elementos $\alpha = (1, 0)$ e $\beta = (0, 1)$, temos $\langle \alpha, \beta\rangle = \{n\alpha + m\beta\ ;\ n, m \in \mathbb{Z}\} = \{(n, m); n, m \in \mathbb{Z}\} = \mathbb{Z}\times\mathbb{Z}$, e deste modo $\mathbb{Z}\times\mathbb{Z}$ é um grupo finitamente gerado.

Exemplo 2.11. Para qualquer grupo G, denotamos por G^2 o subgrupo de G gerado por quadrados de elementos em G, ou seja, $G^2 = \langle \{x^2 : x \in G\} \rangle$, com $x^2 = x \cdot x$. Dizemos que G é **gerado por quadrados** se $G = G^2$.

Teorema 2.3. *Sejam G_1 e G_2 grupos. Então*

$$(G_1 \times G_2)^2 = G_1^2 \times G_2^2$$

Prova. Dados $g_1 \in G_1$ e $g_2 \in G_2$, pelo Exemplo 2.6, temos

$$(g_1, g_2)^2 = (g_1, g_2) \cdot (g_1, g_2) = (g_1 \cdot g_1, g_2 \cdot g_2) = (g_1^2, g_2^2) \times G_2^2$$

logo, $(g_1, g_2)^2 \in (G_1 \times G_2)^2 \Leftrightarrow (g_1^2, g_2^2) \in G_1^2 \times G_2^2$. ■

Grupos Cíclicos

Ressaltaremos nesta seção os grupos cíclicos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$, pois são os mais relevantes na Teoria dos grupos, visto que, qualquer grupo cíclico possui as mesmas propriedades algébricas de $(\mathbb{Z}, +)$ ou $(\mathbb{Z}_n, +)$ para algum n.

Inicialmente, começaremos com a seguinte Definição.

Definição 2.9. (Potências e Múltiplos num Grupo). Seja $(G, \cdot)$ um grupo. Sejam $a \in G$ e $n \in \mathbb{Z}$, define-se a n–ésima potência de a, em símbolos a^n, da seguinte maneira:

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

Segundo a definição, dado $n \in \mathbb{N}$,

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ fatores}}$$

e

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ fatores}}.$$

Caso G possua operação aditiva, usa-se a notação de múltiplo de a, ou seja, $n \cdot a$, em lugar de potências de a. Deste modo,

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

Do mesmo modo, para $n \in \mathbb{N}$,

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ fatores}}$$

e

$$-n \cdot a = n \cdot (-a) = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ parcelas}}.$$

Proposição 2.5. *Seja $(G, \cdot)$ um grupo. Dados $a \in G$ e $n, m \in \mathbb{Z}$, temos:*
(1) $a^n \cdot a^m = a^{n+m}$.
(2) $(a^m)^n = a^{m \cdot n}$.

Prova. Provaremos a propriedade (1) considerando dois casos:
Caso 1: $n \geq 0$ e $n + m \geq 0$. Vamos usar indução sobre n. Se $n = 0$,

$$a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}.$$

Suponhamos que o resultado seja válido para n, ou seja, $a^n \cdot a^m = a^{n+m}$. Assim como $a^n \cdot a = a^{(n+1)-1} \cdot a = a^{n+1}$. Agora mostrando que é válido para o caso $n + 1$. temos

$$\begin{aligned} a^m \cdot a^{n+1} &= a^m \cdot a^n \cdot a \overset{H.I}{=} a^{n+m} \cdot a \\ &= a^{(n+m+1)-1} \cdot a \\ &= a^{n+m+1}. \end{aligned}$$

Portanto, é válido para $n + 1$.

Assim, $a^n \cdot a^m = a^{n+m} \ \forall \ n \geq 0$ com $n + m \geq 0$.

Caso 2: Consideremos que m e n sejam quaisquer inteiros. Seja um inteiro $r > 0$ de tal forma que $r + m > 0$, $r + n > 0$ e $r + m + n > 0$. Logo pelo fato que $a^r \cdot a^{-r} = e$, conseguimos usando a primeira parte da demonstração,

$$\begin{aligned} a^{m+n} = a^{m+n} \cdot (a^r \cdot a^{-r}) &= (a^{m+n} \cdot a^r) \cdot a^{-r} \\ &= a^{m+n+r} \cdot a^{-r} \\ &= a^{m+(n+r)} \cdot a^{-r} \\ &= a^m \cdot (a^{n+r}) \cdot a^{-r} \\ &= a^m \cdot (a^n \cdot a^r) \cdot a^{-r} \\ &= a^m \cdot a^n \cdot (a^r \cdot a^{-r}) \\ &= a^m \cdot a^n. \end{aligned}$$

Desse modo $a^m \cdot a^n = a^{m+n} \ \forall \ m, n \in \mathbb{Z}$.

Provando a propriedade (2). Usando indução sobre n temos,
Para $n = 1$,

$$(a^m)^1 = a^m = a^{m \cdot 1}.$$

Suponhamos que o resultado seja válido para n, ou seja,

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

Agora mostrando que o resultado é válido para $n+1$,

$$(a^m)^{n+1} = (a^m)^n \cdot a^m \overset{H.I}{=} a^{m\cdot n}\cdot a^m = a^{m\cdot n+m} = a^{m\cdot(n+1)}.$$

Portanto, é válido para o caso $n+1$.

Assim, $(a^m)^n = a^{m\cdot n}\ \forall\ n \in \mathbb{N}$. ■

Definição 2.10. Sejam G um grupo e $a \in G$, e o subgrupo H de G dado por,

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

H é intitulado **subgrupo cíclico gerado por** a.

Exemplo 2.12. Para o grupo aditivo $\mathbb{Z}_2 \times \mathbb{Z}_2$, se $a = (\overline{x}, \overline{y}) \in \mathbb{Z}_2 \times \mathbb{Z}_2, a \neq (\overline{0}, \overline{0})$

$$a + a = (\overline{x}, \overline{y}) + (\overline{x}, \overline{y}) = (\overline{x}+\overline{x}, \overline{y}+\overline{y}) = (2\overline{x}, 2\overline{y}) = (\overline{0}, \overline{0}).$$

Dessa forma, $\langle a\rangle = \{(\overline{0}, \overline{0}), a\}\ \forall\ a \in \mathbb{Z}_2 \times \mathbb{Z}_2, a \neq (\overline{0}, \overline{0})$.

Definição 2.11. Um grupo G é dito **cíclico** se existir $a \in G$ tal que

$$G = \langle a\rangle.$$

Exemplo 2.13. O grupo $G = (\mathbb{Z}, +)$ é cíclico. Pois,

$$\langle 1\rangle = \{n\cdot 1 : n \in \mathbb{Z}\} = \{n : n \in \mathbb{Z}\} = \mathbb{Z}.$$

Desta forma, $\mathbb{Z} = \langle 1\rangle$. Ainda $a = -1$ também é um gerador de $\mathbb{Z}$.

Exemplo 2.14. Para cada $n \in \mathbb{N}, n > 1$ o grupo $(\mathbb{Z}_n, +)$ é cíclico. Com efeito, dado $\overline{a} \in \mathbb{Z}_n$,

$$\overline{a} = \overline{1+1+\cdots+1} = \underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{a \text{ vezes}},$$

isto é, $\overline{a} = a\cdot\overline{1}$, de maneira que $\overline{a} \in \langle\overline{1}\rangle$. Assim, $\mathbb{Z}_n \subset \langle\overline{1}\rangle$, e como $\langle\overline{1}\rangle \subset \mathbb{Z}_n$, então $\langle\overline{1}\rangle = \mathbb{Z}_n$.

Observação 2.8. Para um grupo cíclico $G = \langle a\rangle$ existem duas possibilidades:
(a) $a^n = e$ para algum $n \in \mathbb{N}$. Nesta circunstância, G tem ordem finita. Ou,
(b) $a^n \neq e$ para todo $n \in \mathbb{N}$. Nesta circunstância, todas as potências de a são distintas e G tem ordem infinita.

Definição 2.12. Sejam G um grupo e $a \in G$. Se existir $n \in \mathbb{N}$ tal que $a^n = e$, dizemos que o elemento a tem **ordem finita** (ou é de ordem finita). Diante disso, o menor inteiro positivo m tal que $a^m = e$ é chamado de **ordem** de a, a qual indicaremos por $O(a)$. Se por acaso não exista nenhum $n \in \mathbb{N}$ atendendo tal propriedade, o elemento a é dito ser de **ordem infinita.**

Em um grupo G, tem-se sempre

$$O(a) = 1 \Leftrightarrow a = e.$$

Exemplo 2.15. Considere o elemento

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix} \in S_6$$

disso temos

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix} \neq e,$$

calculando α^3 temos

$$\alpha^3 = \alpha\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 3 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e,$$

dessa forma temos $\alpha^3 = e$. Portanto $O(\alpha) = 3$.

Definição 2.13. Seja G um grupo, indicamos por G^I o subgrupo de G gerado por elementos de ordem ímpar de G.

Observação 2.9. Seja G um grupo e I o subconjunto de todos os elementos de ordem ímpar de G e $a \in I$, logo $O(a)$ é ímpar, digamos $O(a) = 2r + 1, r \in \mathbb{Z}$. Daí,

$$a^{2r+1} = e \Leftrightarrow aa^{2r+1} = a \Leftrightarrow a^{2r+2} = a \Leftrightarrow a^{2(r+1)} = a \Leftrightarrow a^{2k} = a \Leftrightarrow \left(a^k\right)^2 = a,$$

com $k = r + 1 \in \mathbb{Z}$. Logo, $I \subseteq G^2$. Como $\langle I \rangle = G^I$, segue do Item (iii) da Observação 2.4 que $G^I \subseteq G^2$.

Proposição 2.6. *Seja G um grupo.*
(i) *Dado $a \in G$, $a \neq e$, tem-se*

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

(ii) $O(a) = O(a^{-1}),\ \forall a \in G.$
(iii) *Se $O(a) = 2$ para todo $a \in G - \{e\}$, então G é abeliano.*
(iv) *Se $O(a) = nm$, então $O(a^m) = n$.*

Prova. (i) Se $O(a) = 2$, então $a^2 = e$. Desse modo,

$$a^{-1}a^2 = a^{-1} \Leftrightarrow a = a^{-1}.$$

Reciprocamente, se $a = a^{-1}$, então $aa = aa^{-1}$, isto é, $a^2 = e$, o que acarreta em $O(a) = 2$, visto que $a \neq e$.
(ii) Se $a \in G$ possui ordem finita, então existe $n \in \mathbb{N}$ tal que $a^n = e$. Mas,

$$a^n = e \Leftrightarrow a^{-n} = e \Leftrightarrow (a^{-1})^n = e. \tag{2.2}$$

Em razão disso, o menor $m \in \mathbb{N}$ atendendo $a^m = e$ é o menor que atende $(a^{-1})^n = e$. Logo, $O(a) = O(a^{-1})$. Por outro lado, se a tem ordem infinita, então por (2.2) a ordem de a^{-1} também é infinita.
(iii) Por hipótese, $O(a) = 2$ para todo $a \in G - \{e\}$. Logo, pelo item (i),

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

Agora, dados $a, b \in G$, temos que $ab \in G$. Dessa forma, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, o que mostra que G é abeliano.
(iv) Primeiramente,

$$O(a) = nm \Rightarrow a^{nm} = e \Rightarrow (a^m)^n = e.$$

Só nos resta mostrar que n é o menor inteiro positivo atendendo $(a^m)^n = e$. Se $r \in \mathbb{N}$ e $r < n$ é tal que $(a^m)^r = e$, então

$$\begin{cases} a^{mr} = e, \\ mr < mn. \end{cases}$$

Isto opõe-se ao fato de mn ser a ordem de a. Logo, $O(a^m) = n$. ∎

Grupos Diedrais

Seja $A \subset \mathbb{R}^2$. Dados $x, y \in A$, seja $d(x, y)$ a distância (euclidiana) entre x, y. Uma permutação $\alpha \in S_A$ é intitulada **simetria** de A quando

$$d(\alpha(x), \alpha(y)) = d(x, y), \ \forall \ x, y \in A.$$

Isto é, α é considerada uma simetria de A quando preserva distância entre quaisquer dois pontos de A.

Indicaremos por T_A o conjunto de todas as simetrias de A. Provaremos que $T_A < S_A$. Considere $\alpha, \beta \in T_A$ e $x, y \in A$. Temos,

$$\begin{aligned} d((\alpha\cdot\beta)(x),(\alpha\cdot\beta)(y)) &= d(\alpha(\beta(x)),\alpha(\beta(y))) \\ &= d(\beta(x),\beta(y)) && (\text{pois } \alpha \in T_A) \\ &= d(x,y), && (\text{pois } \beta \in T_A) \end{aligned}$$

ou seja, $\alpha\cdot\beta \in T_A$. Ainda temos,

$$\begin{aligned} d(\alpha^{-1}(x),\alpha^{-1}(y)) &= d(\alpha(\alpha^{-1}(x)),\alpha(\alpha^{-1}(y))) && (\text{pois } \alpha \in T_A) \\ &= d(x,y). && (\text{pois } \alpha\cdot\alpha^{-1} = id_A) \end{aligned}$$

Assim, $\alpha^{-1} \in T_A$ e, portanto, $T_A < S_A$, chamado **grupo de simetrias** de A.

Temos interesse em grupos de simetria em que A é o conjunto de vértices de um $n-$ágono regular, ou melhor, um polígono regular P_n de n lados.

Definição 2.14. O grupo de simetrias de P_n é intitulado Grupo Diedral de grau n.

Iremos indicar o Grupo de Simetrias de P_n por $D_{n.}$

Exemplo 2.16 (O grupo D_3)**.** Para $n = 3$, temos o triângulo equilátero P_3, mostrado na Figura 1, com os vértices $1,2,3$ e alturas h_1,h_2,h_3.

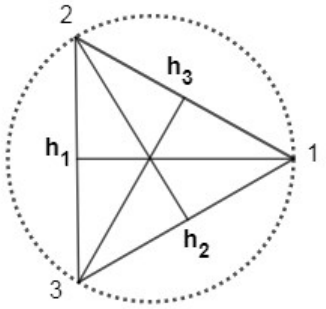

Figura 1: O polígono P_3

Considerando

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

Observamos que α_1,α_2 e α_3 são geradas pelas rotações de ângulos $0, \frac{2\pi}{3}$rad e $\frac{4\pi}{3}$rad no sentido anti-horário sobre os vértices $1,2,3$, respectivamente, da seguinte maneira: uma rotação de zero grau sobre P_3 o deixa constante (a ação de α_1 sobre P_3). Já, rotacionando P_3 em um ângulo de $\frac{2\pi}{3}$rad, obtem-se o triângulo dado na Figura 1, no qual relacionamos à simetria α_2. Igualmente, obtém-se α_3. As simetrias restantes de P_3 são

$$\beta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \beta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \beta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Vejamos que β_1, β_2 e β_3 são geradas pelas reflexões de P_3 em volta das mediatrizes de P_3 (neste caso, pelas alturas do triângulo), h_1, h_2 e h_3, respectivamente. As permutações α_i e β_i, com $i = 1, 2, 3$, são as únicas simetrias de D_3.

Dessa forma, D_3 tem ordem 6 e $D_3 < S_3$ e é dado pelo seguinte conjunto

$$D_3 = \{\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3\},$$

logo $D_3 = S_3$. Este é o caso único em que $D_n = S_n$.

Teorema 2.4. *O grupo diedral D_n é um grupo cuja a ordem é $2n$ gerado por dois elementos α e β, satisfazendo $\alpha^n = \beta^n = Id$, em que*

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

Prova. A prova deste Teorema se encontra-se em Vieira (2015, p. 210). ∎

Observação 2.10. Verifica-se também que o grupo D_n contém propriamente um subgrupo de ordem n. De fato,

$$R_n = \{Id, \alpha, \alpha^2, ..., \alpha^{n-1}\} = \langle \alpha \rangle$$

em que α é como no Teorema 2.10. R_n é um subgrupo de D_n de ordem n, chamado de **grupo das rotações do polígono** P_n.

Além disso, D_n possui também n reflexões, $\beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3, ..., \beta\alpha^{n-1}$ estabelecidas da seguinte forma: se n é ímpar, são estabelecidas em torno das mediatrizes do polígono de P_n, agora se n é par, metade das reflexões são obtidas através das mediatrizes do polígono de P_n, e a outra metade através do diâmetro da circunferência que circuncreve P_n e contém os seus vértives. Indicaremos o conjunto das reflexões de um polígono P_n da seguinte forma

$$R_e = \{\beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3, ..., \beta\alpha^{n-1}\}.$$

Observe que todos os elementos de R_e possuem ordem 2, uma vez que ao refletir um vértice por um segmento duas vezes, o vértice volta ao estado inicial.

Classes Laterais e o Teorema de Lagrange

Antes de apresentar o Teorema de Lagrange que é a base da teoria do grupos finitos devemos falar da concepção de classe lateral, que a partir desse o devido teorema segue normalmente.

Sejam G um grupo e H um subgrupo de G. Sobre G, iremos considerar a relação "$\equiv_E \ (mod\ H)$" dada, para quaisquer $a, b \in G$, por

$$a \equiv_E b \ (mod\ H) \Leftrightarrow a^{-1}b \in H. \tag{2.3}$$

Quando 2.3 acontece, diremos que a é congruente a b módulo H.

Proposição 2.7. *A relação* $\equiv_E (mod\ H)$ *acima é de equivalência. Além disso, a classe de equivalência de um elemento* $a \in G$*, referente a esta relação, é dada por* $aH = \{ah : h \in H\}$.

Prova. Sejam $a, b, c \in G$.

i) ($\equiv_E$ **é reflexiva**) Como $a^{-1}a = e \in H$, então $a \equiv_E\ a \pmod H$, isto é, $\equiv_E$ é reflexiva.

ii) ($\equiv_E$ **é simétrica**) Se $a \equiv_E\ b \pmod H$, então $a^{-1}b \in H$. Deste modo,

$$(a^{-1}b)^{-1} \in\ H \Rightarrow\ b^{-1}a \in H \Rightarrow b \equiv_E\ a \pmod H,$$

de modo que $\equiv_E$ é simétrica.

iii) ($\equiv_E$ **é transitiva**) Se $a \equiv_E\ b \pmod H$ e $b \equiv_E\ c \pmod H$, então $a^{-1}b = h_1 \in H$ e $b^{-1}c = h_2 \in H$. Desta forma,

$$(a^{-1}b)(b^{-1}c) = h_1h_2 \in H \Rightarrow a^{-1}c \in H \Rightarrow a \equiv_E\ c \pmod H.$$

Desta maneira, $\equiv_E$ é transitiva e, em vista disso, é de equivalência.

Agora, dado $a \in G$, seja $\overline{a}$ a classe de equivalência de a referente à relação $\equiv_E$. Por definição, $\overline{a} = \{b \in G : a \equiv_E b(\mathrm{mod}H)\}$. Logo para $b \in G$,

$$b \in \overline{a} \Leftrightarrow a \equiv_E b \pmod H \Leftrightarrow a^{-1}b \in H,$$

isto é, $a^{-1}b = h \in H$, ou melhor, $b = ah \in aH$. Isto nos diz que $\overline{a} \subset aH$. Agora, se $b \in aH$, então existe $h \in H$ tal que $b = ah$, ou seja, $a^{-1}b = h$. Por conseguinte, $a \equiv_E\ b \pmod H$ e, assim, $b \in \overline{a}$. Logo, $aH \subset \overline{a}$, mostrando que $\overline{a} = aH$. ∎

A classe aH de um elemento $a \in G$ de acordo a relação $\equiv (mod\ H)$ em 2.3 é denominada de **classe lateral à esquerda** de H em G determinada por a, ou simplesmente **classe lateral de** a **à esquerda**.

De maneira análoga, mostra-se que a relação $\equiv_D \pmod H$ sobre G dada, para quaisquer $a, b \in G$, por

$$a \equiv_D b\ (mod\ H) \Leftrightarrow ab^{-1} \in H$$

é de equivalência. E ainda, para cada $a \in G$, a classe de equivalência de a relativa esta relação é $Ha = \{ha : h \in H\}$, a qual é denominada **classe lateral à direita** de H em G definida por a, ou **classe lateral** de a **à direita**.

Como as classes à esquerda são classes de equivalência, ocorrem duas coisas relevantes. Primeiramente,

$$G = \bigcup_{a \in G} aH,$$

e em seguida observa-se também pelos resultados da teoria de Relações de Equivalência, que, para $a, b \in G$,

$$aH = bH \text{ ou } aH \cap bH = \varnothing,$$

ou seja, duas classes laterais são iguais ou disjuntas. Desta forma, indicando por H_E o conjunto de todas as classes laterais à esquerda de H, ou seja,

$$H_E = \{aH : a \in G\} = G/\equiv_E {}^{1},$$

e H_E se consiste numa partição de G.

Considerações análogas são válidas para as classes laterais à direita. Especialmente, se H_D é o conjunto das classes laterais à direita de H,

$$H_D = \{Hg : g \in G\} = G/\equiv_D,$$

portanto H_D é uma partição de G.

Observação 2.11. Sejam G um grupo e $H < G$.
(i) Se G é um grupo abeliano, então para cada $a \in G$,

$$aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha.$$

Logo, a classe lateral à direta de a coincide com sua classe lateral à esquerda.
(ii) O próprio subgrupo H é uma classe lateral de H tanto à esquerda quanto à direita, visto que

$$eH = \{eh : h \in H\} = H = \{he : h \in H\} = He.$$

(iii) Para $a \in G$,

$$aH = H \Leftrightarrow aH = eH \Leftrightarrow a \equiv_E e \ (mod\ H) \Leftrightarrow a^{-1}e \in H \Leftrightarrow a \in H.$$

Analogamente,

$$Ha = H \Leftrightarrow a \in H.$$

Exemplo 2.17. Consideremos $G = (\mathbb{Z}_6, +)$ e o subgrupo $H = \{\overline{0}, \overline{2}, \overline{4}\}$. Assim temos

$$\overline{0} + H = \overline{2} + H = \overline{4} + H, \text{ pois } \overline{0}, \overline{2}, \overline{4} \in H.$$

Agora,

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

[1] a notação indica o quociente de G pela relação $\equiv_E$

Dessa maneira, existem duas classes laterais à esquerda (à direita) de H, que são H e $\{\overline{1}, \overline{3}, \overline{5}\}$. E ainda podemos dizer que $\overline{0}, \overline{2}, \overline{4}$ são congruentes módulo H entre eles. Da mesma forma com $\overline{1}, \overline{3}, \overline{5}$.

Teorema 2.5. *Sejam G um grupo e H um subgrupo de G. Então, toda classe lateral à esquerda (à direita) possui a mesma cardinalidade de H. Ademais, os conjuntos H_E e H_D possuem a mesma cardinalidade.*

Prova. A prova deste Teorema encontra-se em Vieira (2015, p. 234). ■

Definição 2.15. Sejam G um grupo e H um subgrupo de G. A cardinalidade do conjunto H_E (a mesma de H_D) é chamada **índice** de H em G, o qual será denotado por $(G : H)$.

Teorema 2.6 (**Teorema de Lagrange**)**.** *Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G. Particularmente,*

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

Prova. Como G é finito, então $(G : H)$ também o é, digamos $(G : H) = r$. Consideremos então $H_E = \{a_1H, a_2H, ..., a_rH\}$. Como H_E é uma partição de G,

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH,$$

com, $a_iH \cap a_jH = \varnothing$ para $i \neq j$. Desta forma, pelo fato da cardinalidade de cada classe em H_E ser a igual a ordem de H, tem-se

$$|G| = \underbrace{|H| + |H| + ... + |H|}_{r \text{ vezes}} = |H| \cdot r,$$

isto é, $|G| = |H| \cdot (G : H)$. ■

Exemplo 2.18. Se G é um grupo de ordem ímpar e H é um subgrupo de G, então H não pode ter índice 2, pois, pelo Teorema de Lagrange, o índice de H divide a ordem de G.

Observação 2.12. Segue do Teorema de Lagrange que, se G é um grupo finito de ordem n e $a \in G$, então $a^n = e$.

De fato, se $a \in G$, então $\langle a \rangle = \{a^k; k \in \mathbb{Z}\} < G$. Como G é finito, segue que $\langle a \rangle = \{e, a, a^2, \ldots, a^{r-1}\}$ e $O(a) = r = |\langle a \rangle|$. Como $\langle a \rangle < G$, do Teorema de Lagrange, $n = rs$, com $s \in \mathbb{N}$. Assim, da Proposição 2.6 e de $a^r = e$, temos

$$a^n = a^{rs} = (a^r)^s = e^s = e.$$

Subgrupos Normais

Definição 2.16. Seja G um grupo. Um subgrupo H de G chama-se normal quando

$$ghg^{-1} \in H, \ \forall g \in G \text{ e } \forall h \in H,$$

ou equivalentemente ,

$$gHg^{-1} \subset H, \forall g \in G.$$

Desde que $g \in G$ é qualquer, então a expressão $ghg^{-1} \in H$ é equivalente a $g^{-1}hg \in H$. Da mesma forma vale para as expressões $gHg^{-1} \subset H$ e $g^{-1}Hg \subset H$.

Um subgrupo normal H de um grupo G, também dito invariante, será indicado por

$$H \lhd G.$$

Exemplo 2.19. Seja G um grupo, então $G^2 \lhd G$. De fato, dados $x = x_1^2x_2^2\cdots x_n^2 \in G^2$ e $a \in G$ temos

$$\begin{aligned} axa^{-1} &= ax_1^2x_2^2\cdots x_n^2a^{-1} \\ &= ax_1x_1x_2x_2\cdots x_nx_na^{-1} \\ &= ax_1a^{-1}ax_1a^{-1}ax_2a^{-1}ax_2a^{-1}\cdots ax_na^{-1}ax_na^{-1} \\ &= (ax_1a^{-1})^2(ax_2a^{-1})^2\cdots(ax_na^{-1})^2 \in G^2. \end{aligned}$$

Teorema 2.7. *Seja H um subgrupo de um grupo G. Então, as seguintes condições são equivalentes:*

(i) $H \lhd G$

(ii) $gHg^{-1} = H, \forall g \in G.$

(iii) $gH = Hg, \forall g \in G.$

Prova. $(i) \Rightarrow (ii)$ Por hipótese, para cada $g \in G$, tem-se a inclusão $gHg^{-1} \subset H$. Agora, dado $h \in H$,

$$h = g(g^{-1}hg)g^{-1} \in gHg^{-1},$$

visto que $g^{-1}hg \in H$, uma vez que $H \lhd G$. Isto nos mostra que $H \subset gHg^{-1}$ e, sendo assim, $gHg^{-1} = H$.

$(ii) \Rightarrow (iii)$ Para $g \in G$, seja $x \in gH$, digamos $x = gh$ para algum $h \in H$. Então, por hipótese,

$$xg^{-1} = ghg^{-1} \in gHg^{-1} = H,$$

ou seja, $xg^{-1} = h_1$ com $h_1 \in H$. Portanto, $x = h_1g \in Hg$, de maneira que $gH \subset Hg$. Analogamente, mostra-se que $Hg \subset gH$. Consequentemente, $Hg = gH$.

$(iii) \Rightarrow (i)$ Sejam $g \in G$ e $h \in H$. Como $gH = Hg$ e $gh \in Hg$, segue que $gh = h_2g$ para algum $h_2 \in H$, isto é, $ghg^{-1} = h_2 \in H$. Logo, $H \lhd G$. ■

Proposição 2.8. *Se H é um subgrupo de um grupo G tal que $(G : H) = 2$, então $H \lhd G$.*

Prova. Pelo Teorema 2.7, é preciso apenas mostrar que $gH = Hg$ para todo $g \in G$. Sabe-se que o próprio H é uma classe lateral à esquerda de si próprio. Como $(G : H) = 2$, então H_E possui exatamente dois elementos, sendo ele uma partição de G, $G \setminus H$ é a outra classe lateral à esquerda. Se $g \in H$, então $gH = H = Hg$. No entanto, para $g \notin H$,

$$gH \neq H.$$

Em vista disso, $gH = G \setminus H$. Analogamente, $Hg = G \setminus H$. Desta forma, $gH = Hg$ para todo $g \in G$. Logo, $H \lhd G$. ∎

Grupos Quocientes

Daqui pra frente, quando H for um subgrupo normal em G, denotaremos o conjunto H_E e H_D por G/H ou $\frac{G}{H}$, ou seja,

$$G/H = \{gH : g \in G\}.$$

Denotaremos uma classe lateral gH por $\overline{g}$. Além do mais chamaremos as classes laterais à esquerda (ou à direita) por apenas classes laterais.

Teorema 2.8. *Sejam $(G, \cdot)$ um grupo e H um subgrupo normal de G. Então,*

$$\begin{array}{rcl} \cdot : G/H \times G/H & \to & G/H \\ (xH, yH) & \mapsto & (xH) \cdot (yH) = xyH \end{array}$$

define uma operação sobre G/H com $e_{G/H} = H$ e se $xH \in G/H$, então $(xH)^{-1} = x^{-1}H$. Além do mais, G/H é um grupo com esta operação.

Prova. A prova deste Teorema encontra-se em Vieira (2015, p. 249). ∎

Proposição 2.9. *Sejam G um grupo e $H \lhd G$.*
(1) *Se G é abeliano, então G/H é abeliano.*
(2) *Se G é cíclico, então G/H é cíclico.*

Prova. (1) Para $xH, yH \in G/H$,

$$(xH) \cdot (yH) = (xy)H = (yx)H \text{ (pois } G \text{ é abeliano)}$$

$$= (yH) \cdot (xH),$$

isto é, G/H é abeliano.
(2) Suponhamos que $G = \langle a \rangle$ e seja $xH \in G/H$. Como $x \in G$, existe $n \in \mathbb{Z}$ tal que $x = a^n$. Deste modo,

$$xH = a^n H = (aH)^n \in \langle aH \rangle.$$

Assim, $G/H \subset \langle aH \rangle$, e como $\langle aH \rangle \subset G/H$, então $G/H = \langle aH \rangle$. ■

Proposição 2.10. *Se G é um grupo finito e $H \lhd G$, então*

$$\left|\frac{G}{H}\right| = \frac{|G|}{|H|}.$$

Prova. De acordo com o Teorema de Lagrange,

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

Por definição, tem-se $(G : H) = \left|\frac{G}{H}\right|$, então

$$|G| = |H| \cdot \left|\frac{G}{H}\right| \Rightarrow \left|\frac{G}{H}\right| = \frac{|G|}{|H|}.$$

■

Teorema 2.9. *Seja um grupo finito G e considere que mais da metade dos elementos de G possuam ordem ímpar. Então G não possui subgrupos de índice 2.*

Prova. Seja $n = |G|$ e suponha que existe $H < G$, tal que $(G : H) = 2$. Nesse caso, $|H| = \frac{n}{2}$ e da Proposição 2.8, temos $H \lhd G$ com $G/H = \{H, aH\}$, para $a \in G \setminus H$. Como $|G/H| = 2$, da Observação 2.12, segue que

$$H = (xH)^2 = x^2H, \forall x \in G$$

e, consequentemente, da Observação 2.11, temos $x^2 \in H$, para todo $x \in G$.

Daí, $G^2 \subset H$. Mas, $G^I \subset G^2$, logo $G^I \subset H$. Como $|G^I| > \frac{n}{2}$, por hipótese, uma vez que G^I contém todos os elementos de ordem ímpar de G, segue que $|H| > \frac{n}{2} = |H|$, o que é um absurdo. ■

Proposição 2.11. *Sejam G um grupo e H e K subgrupos de G com $K \lhd G$. Se $K \subset H$, então $K \lhd H$. Ademais, $H/K < G/K$.*

Prova. Como $K \lhd G$, então dados $a \in G$ e $k \in K$, $aka^{-1} \in K$. Como $K \subset H$, segue, da Observação 2.7, que $K < H$. Como $aka^{-1} \in K$ vale para todo $a \in G$, em particular, vale para $h \in H$, ou seja $hkh^{-1} \in K$, $\forall\, h \in H$ e $\forall\, k \in K$. Donde $K \lhd H$.

Para a segunda parte, como $K \lhd H$, então $e_{H/K} = K = e_{G/K}$. Ainda, dados h_1K e $h_2K \in H/K$, pelo Teorema 2.8, temos

$$(h_1K)(h_2K)^{-1} = (h_1K)(h_2^{-1}K) = \underbrace{(h_1h_2^{-1})}_{\in H} K \in H/K$$

logo $H/K < G/K$. ■

Proposição 2.12. *Sejam G um grupo e $H \lhd G$. Então*

$$K < G/H \Leftrightarrow K = S/H, \text{ com } S < G \text{ e } H \subset S.$$

Prova. Suponha $K < G/H$. Nesse caso, como $K \subset G/H$

$$K = \{a_iH; a_i \in G \text{ e } i \in I\}.$$

Tomando $S = \bigcup_{i\in I} a_iH$, temos $S < G$. De fato, sejam $x, y \in S$, temos $x \in a_iH$ e $y \in a_jH$, para algum $i, j \in I$. Daí,

$$x = a_ih_1 \text{ e } y = a_jh_2$$

para algum $h_1, h_2 \in H$. Assim,

$$xy^{-1} = a_ih_1(a_jh_2)^{-1} = a_i \underbrace{h_1h_2^{-1}a_j^{-1}}_{\in Ha_j^{-1}=a_j^{-1}H} = a_ia_j^{-1}h_3$$

em que $h_1h_2^{-1}a_j^{-1} = a_j^{-1}h_3$, pois $H \lhd G$. Logo,

$$xy^{-1} \in a_ia_j^{-1}H = (a_iH)(a_j^{-1}H) \in K,$$

pois $K < G/H$. Donde, $xy^{-1} \in S$ e $S < G$. Ainda, como $H \subset K$, pois $H = e_{G/H}$ temos $H \subset S$ e segue da construção que $K = S/H$. A recíproca segue da Proposição 2.11. ■

Homomofismos de Grupos

Homomorfismo é um conteúdo essencial para o estudo de grupos, pois é uma função entre dois grupos que preserva as operações binárias. Desta forma dado dois grupos G_1 e G_2, podemos obter informações algébricas de G_2, à partir de informações algébricas de G_1, ou vice versa. Assim, temos a seguinte definição.

Definição 2.17. Sejam $(G_1, \star)$ e $(G_2, \cdot)$ grupos quaisquer. Uma função $f : G_1 \to G_2$ é denominada homomorfismo de G_1 em G_2 quando $f(a \star b) = f(a) \cdot f(b), \forall a, b \in G_1$.

Observação 2.13. Se $f : G_1 \to G_2$ é um homomorfismo e $a_1, a_2, ..., a_n \in G_1$, então por indução, temos.

$$f(a_1a_2\cdots a_n) = f(a_1) \cdot f(a_2) \cdots f(a_n).$$

Exemplo 2.20. Sejam $n \in \mathbb{Z}$ fixo e $f_n : \mathbb{Z} \to \mathbb{Z}$ dada por $f_n(a) = n \cdot a$. Se $a, b \in \mathbb{Z}$, então

$$f_n(a + b) = n \cdot (a + b) = n \cdot a + n \cdot b = f_n(a) + f_n(b),$$

isto é, f_n é um homomorfismo.

Podemos generalizar da seguinte maneira: se $(G,\cdot)$ é um grupo abeliano e $n \in \mathbb{Z}$, então $\varphi_n : G \to G$ definida por $\varphi_n(g) = g^n$ para todo $g \in G$, atende, para quaisquer $g_1, g_2 \in G$,

$$\begin{aligned} \varphi_n(g_1g_2) &= (g_1g_2)^n \\ &= g_1^n g_2^n \qquad \text{(pois G é abeliano)} \\ &= \varphi_n(g_1)\varphi_n(g_2), \end{aligned}$$

de forma que φ_n é um homomorfismo.

Proposição 2.13. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Então*
(i) $f(e_1) = e_2$.
(ii) $f(a^{-1}) = f(a)^{-1}, \forall\ a \in G_1$.
(iii) $Im(f) = \{f(a) : a \in G_1\}$ *é um subgrupo de G_2 - a* ***imagem*** *de f.*
(iv) $Ker(f) = \{a \in G_1; f(a) = e_2\} \lhd G_1$- *o* ***Núcleo*** *de f.*

Prova. **(i)** Como $e_1 = e_1 \cdot e_1$, então

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1).$$

Dessa forma, $f(e_1)$ é a identidade de G_2, isto é, $f(e_1) = e_2$.
(ii) Para todo $a \in G_1$, $a \cdot a^{-1} = e_1$. Desse modo,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_1) = e_2,$$

o que acarreta dizer que $f(a^{-1}) = f(a)^{-1}$.
(iii) 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 $f(b) = y$. Assim,

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

de forma que $xy^{-1} \in Im(f)$ e $Im(f) < G_2$.
(iv) Do item (i), temos $\mathrm{Ker}(f) \neq \varnothing$. Sejam $a, b \in \mathrm{Ker}(f)$, logo $f(a) = e_2 = f(b)$, daí

$$f(ab^{-1}) = f(a)f(b)^{-1} = e_2,$$

logo $ab^{-1} \in \mathrm{Ker}(f)$ e $\mathrm{Ker}(f) < G$. Agora, se $g \in G_1$ e $a \in \mathrm{Ker}(f)$, então

$$f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)e_2f(g)^{-1} = f(g)f(g)^{-1} = e_2$$

e $\mathrm{Ker}(f) \lhd G_1$. ∎

Definição 2.18. Um homomorfismo de grupos, $f : G_1 \to G_2$, bijetivo é intitulado **isomorfismo**.

Proposição 2.14. *Se $f : G_1 \to G_2$ é um isomorfismo, então $f^{-1} : G_2 \to G_1$ também é um isomorfismo.*

Prova. É preciso apenas mostar que $f^{-1} : G_2 \to G_1$ é um homomofismo. Dados $x, y \in G_2$, existem $a, b \in G_1$ tais que

$$f(a) = x \Leftrightarrow f^{-1}(x) = a \quad \text{e} \quad f(b) = y \Leftrightarrow f^{-1}(y) = b.$$

Dessa forma,

$$\begin{aligned} f^{-1}(xy) &= f^{-1}(f(a)f(b)) \\ &= f^{-1}(f(ab)) \qquad (f \text{ é homomorfismo}) \\ &= ab \qquad (f^{-1} \circ f = id_{G_1}) \\ &= f^{-1}(x)f^{-1}(y), \end{aligned}$$

o que demonstra que f^{-1} é um homomorfismo. ■

Definição 2.19. Dois grupos G_1 e G_2 são ditos **isomorfos** se existir um isomorfismo entre eles.

Para denotar que os grupos G_1 e G_2 são isomorfos usaremos a seguinte notação

$$G_1 \simeq G_2.$$

Teorema 2.10 (**Teorema Fundamental**)**.** *Sejam G um grupo abeliano finitamente gerado. Então:*

i) $G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_n} \times \mathbb{Z}^m$, *onde* $n, m \geq 0$, d_i *divide* d_{i+1}, *para todo* $i = 1, ..., n-1$, *e* $d_i \geq 2$.

ii) *Se* $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_n} \times \mathbb{Z}^m \simeq \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times ... \times \mathbb{Z}_{q_u} \times \mathbb{Z}^v$, *com* $d_i, q_j \geq 2$, d_i *divide* d_{i+1}, q_j *divide* q_{j+1} *e* $n, m, u, v \geq 0$, *então* $n = u$, $m = v$ *e* $d_i = q_i$ *para todo* $i = 1, ..., n$

Prova. A prova deste Teorema encontra-se em Hungerford (1980, p. 78). ■

Grupos Alternados

Definição 2.20. Uma permutação $\alpha \in S_n$ chama-se **ciclo** de comprimento r ou r-ciclo quando existem elementos distintos $a_1, a_2, ..., a_r \in I_n$ tais que

$$\alpha(a_1) = a_2, \ \alpha(a_2) = a_3, ..., \alpha(a_{r-1}) = a_r, \ \alpha(a_r) = a_1 \tag{2.4}$$

e

$$\alpha(i) = i, \ \forall i \in I_n - \{a_1, a_2, ..., a_r\}.$$

em particular, um 2–ciclo chama-se **transposição**.

De maneira geral, representa-se um $r-$ciclo α como em 2.4 por

$$\alpha = (a_1\ a_2 \cdots a_r).$$

Exemplo 2.21. Em S_n, o único 1−ciclo (o ciclo trivial) é a identidade $\alpha = Id$, a qual caracteriza-se por $\alpha = (1)$ ou por $\alpha = (a)$, com $a \in I_n$.

Definição 2.21. Se $\alpha \in S_n$ e $i \in I_n$, diz-se que α move i quando $\alpha(i) \neq i$; e diz-se que α fixa i quando $\alpha(i) = i$.

No conjunto $\alpha = (a_1 a_2 \cdots a_r)$, naõ são mostrados os inteiros $i \in I_n$ que são fixados por a. Nesta situação, obtemos que $\alpha(i) = i$ para qualquer $i \in I_n - \{a_l, a_2, ..., a_r\}$.

Exemplo 2.22. Em S_5, a permutação $\alpha = (1\ 2\ 5)$ move os inteiros $i = 1, i = 2$ e $i = 5$, e fixa $i = 3$ e $i = 4$; α é um 3−ciclo.

Proposição 2.15. *Um $r-$ciclo em S_n tem ordem r.*

Prova. A prova desta Proposição encontra-se em Vieira (2015, p. 293). ■

Exemplo 2.23. Obtemos que o 4−ciclo $\alpha = (1\ 2\ 3\ 6) \in S_6$ tem ordem quatro e o 5-ciclo $\beta = (1\ 3\ 5\ 7\ 8) \in S_9$ tem ordem cinco.

Definição 2.22. Dois ciclos $\alpha, \beta \in S_n$, digamos

$$\alpha = (a_1\ a_2 \cdots a_r) \text{ e } \beta = (b_1\ b_2 \cdots\ b_k),$$

são chamados de **ciclos disjuntos** quando nenhum elemento de $I_n = \{1, 2, ..., n\}$ é movido por ambos. Ou seja, quando

$$\{a_1, a_2, ..., a_r\} \cap \{b_1, b_2, ..., b_k\} = \varnothing.$$

Uma família de ciclos $\alpha_1, \alpha_2, ..., \alpha_t$ é **disjunta** quando α_i e α_j são disjuntos para quaisquer $i, j \in \{1, ..., t\}$, com $i \neq j$.

Teorema 2.11. *Toda a permutação $\alpha \in S_n$ pode ser escrita como um produto de ciclos disjuntos aos pares. Além disso, esta fatoração é única, a menos da ordem dos fatores.*

Prova. A prova deste Teorema encontra-se em Vieira (2015, p. 296). ■

Corolário 2.1. *Qualquer permutação $\alpha \in S_n$, pode ser escrita como produto de transposições.*

Prova. De acordo com Teorema 2.11, basta mostrar que qualquer ciclo em S_n é um produto de transposições. Deste modo, dado $\mu = (a_1 a_2 \cdots a_r)$, podemos reescrevê-lo da forma

$$\mu = (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1 a_2).$$

■

Definição 2.23. Uma permutação $\alpha \in S_n$ é **par** se α é capaz de ser escrito como um produto de um número par de transposições; e α é **ímpar** se α é capaz de ser escrita como um produto de um número ímpar de transposições.

Teorema 2.12. *Para $n \geq 2$, S_n contém $\frac{n!}{2}$ permutações pares e $\frac{n!}{2}$ permutações ímpares.*

Prova. A prova deste Teorema encontra-se em Vieira (2015, p. 304). ■

Observação 2.14. Indicaremos por A_n o conjunto de todas as permutações pares de S_n. Em verdade, $A_n < S_n$. De fato, se $\alpha, \beta \in A_n$, digamos

$$\alpha = (a_1 a_r) \cdots (a_1 a_2) \text{ e } \beta = (b_1 b_k) \cdots (b_1 b_2),$$

temos

$$\alpha\beta^{-1} = \underbrace{(a_1 a_r) \cdots (a_1 a_2)}_{2s \text{ transposições}} \underbrace{(b_1 b_2) \cdots (b_1 b_k)}_{2t \text{ transposições}} \in A_n, \text{ com } s, t \in \mathbb{N}.$$

Portanto A_n, pelo Teorema 2.1, é um subgrupo de S_n.

O grupo A_n é denominado por **grupo alternado** de grau n ou grupo das permutações pares de grau n.

Proposição 2.16. *Para $n \geq 2$, o grupo alternado A_n é um subgrupo normal de S_n.*

Prova. De acordo com o Teorema de Lagrange, temos $|S_n| = |A_n| \cdot (S_n : A_n)$. Daí e, do Teorema 2.12, segue que

$$(S_n : A_n) = \frac{|S_n|}{|A_n|} = \frac{n!}{\frac{n!}{2}} = 2.$$

Em vista disso, de acordo com a Proposição 2.8, temos que A_n é um subgrupo normal de S_n. ■

Teorema 2.13. *Se $n \geq 3$, então A_n contém todos os $3-$ciclos. Além disso, todo o elemento em A_n é um produto de $3-$ciclos.*

Prova. A prova deste Teorema encontra-se em Vieira (2015, p. 305). ■

2.1.2 Teoria de Anéis

Definição 2.24. Um conjunto não vazio A munido de duas operações de adição "+"e multiplicação " $\cdot$ "chama-se **anel** quando as seguintes propriedades são satisfeitas:
(a_1) $(A, +)$ é um grupo abeliano.
(a_2) A multiplicação é associativa, ou seja,

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

(a_3) A multiplicação é distributiva sobre a adição, isto é,

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ e } (x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in A.$$

Iremos indicar um anel $(A, +, \cdot)$ por A quando não houver dúvida em relação às operações indicadas. Além disso, vamos representar o elemento neutro da adição de A por 0_A, de modo que para todo $a \in A$,

$$a + (-a) = 0_A.$$

Ainda, dados $a, b \in A$, a soma $a + (-b)$ será indicada por $a - b$,

$$a - b = a + (-b).$$

Definição 2.25. Um anel $(A, +, \cdot)$ é dito **comutativo** quando sua multiplicação for comutativa, ou seja,

$$ab = ba, \forall a, b \in A.$$

Definição 2.26. Um anel $(A, +, \cdot)$ chama-se **anel com unidade** quando sua multiplicação possui elemento neutro, isto é, quando existe $e \in A$ tal que

$$ae = a = ea, \forall a \in A.$$

O elemento neutro da multiplicação de um anel A chama-se **unidade** do anel A, a qual será representada por 1_A.

Definição 2.27. Um anel $\mathbb{K}$, comutativo com unidade, chama-se **corpo** quando todo elemento não nulo de $\mathbb{K}$ tem inverso multiplicativo. Ou seja, dado $a \in \mathbb{K}$, $a \neq 0_{\mathbb{K}}$, existe $b \in \mathbb{K}$ tal que

$$a \cdot b = 1_{\mathbb{K}}. \tag{2.5}$$

Exemplo 2.24. Do estudado na Seção de Teoria de Grupos, temos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são anéis comutativos com unidade, em que todos os elementos possuem inverso sob a multiplicação. Logo, são corpos. Ainda, notemos que $(\mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade, mas não é corpo, pois os únicos elementos inversíveis sob a multiplicação são 1 e -1.

Exemplo 2.25. Dos Exemplos 2.4 e 2.5, segue que $(\mathbb{Z}_n, +, \cdot)$, em geral, é anel comutativo com unidade, mas não é corpo. Ainda, $(\mathbb{Z}_n, +, \cdot)$ é corpo se, e somente se, n é um número primo.

2.2 Tópicos em Álgebra Linear

A Álgebra Linear é a área da matemática que se trata do estudo de Espaços Vetorias e Transformações Lineares. O nosso resultado principal necessita de conceitos de Álgebra Linear. Assim, iremos apresentar aqui resultados que servirão como pré-requisitos do Teorema principal apresentado no Capítulo seguinte.

Nestas seção nos basearemos nas seguintes referências Coelho e Lourenço (2007), Hefez (2016), Louredo e Oliveira (2015) e Steinbruch e Winterle (1997). Recomenda-se essas referências para uma leitura mais aprofundada.

2.2.1 Espaços Vetoriais

Definição 2.28 (Espaços Vetoriais)**.** Dizemos quer o conjunto $V \neq \varnothing$, munido de duas operações, uma de "soma"e uma "multiplicação por escalar":

$$\begin{array}{rcl} +: V \times V & \to & V \\ (u,v) & \mapsto & u+v \end{array} \quad \text{e} \quad \begin{array}{rcl} \cdot: \mathbb{K} \times V & \to & V \\ (\alpha, v) & \mapsto & \alpha \cdot v, \end{array}$$

é um **espaço vetorial** sobre um corpo $\mathbb{K}$, se satisfaz as seguintes propriedades:

1. $u + v = v + u \ \forall \ u, v \in V$;
2. $(u + v) + w = u + (v + w), \ \forall u, v \text{ e } w \in V$;
3. $\exists \ 0 \in V$, tal que $0 + v = v + 0 = v, \ \forall v \in V$;
4. $\forall v \in V, \exists - v \in v$, tal que $v + (-v) = -v + v = 0$;
5. $\forall v \in V \text{ e } \forall \alpha, \beta \in \mathbb{K}, (\alpha\beta)v = \alpha(\beta v)$;
6. $\forall u, v \in V \text{ e } \forall \alpha \in \mathbb{K}, \alpha(u + v) = \alpha u + \alpha v$;
7. $\forall \alpha, \beta \in \mathbb{K} \text{ e } \forall v \in V, (\alpha + \beta)v = \alpha v + \beta v$;
8. $\forall v \in V, 1v = v$.

Observação 2.15. Nas condições da definição acima, segue dos itens 1-4 que $(V, +)$ é um grupo abeliano.

Exemplo 2.26. O conjunto $\mathbb{R}^n$, com $n \in \mathbb{N}$, é um Espaço Vetorial sobre $\mathbb{R}$ com as operações de adição e multiplicação por escalar definidas de forma usual.

Exemplo 2.27. O conjunto $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 = \mathbb{Z}_2^n = \{(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}); \overline{a_i} \in \mathbb{Z}_2\}$, munido das operações

$$(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}) + (\overline{b_1}, \overline{b_2}, ..., \overline{b_n}) = (\overline{a_1} + \overline{b_1}, ..., \overline{a_n} + \overline{b_n}) = (\overline{a_1 + b_1}, \overline{a_2 + b_2}, ..., \overline{a_n + b_n})$$

e

$\overline{r}u = \overline{r}(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}) = (\overline{r} \cdot \overline{a_1}, \overline{r} \cdot \overline{a_2}, ..., \overline{r} \cdot \overline{a_n})$, para $(\overline{a_1}, \overline{a_2}, ..., \overline{a_n})$ e $(\overline{b_1}, \overline{b_2}, ..., \overline{b_n}) \in \mathbb{Z}_2^n$ e $\overline{r} \in \mathbb{Z}_2$, é um espaço vetorial sobre $\mathbb{Z}_2$.

Solução. Como $(\mathbb{Z}_2, +)$ é grupo abeliano, segue daí e do Exemplo 2.6, que as propriedades 1-4 são satisfeitas. O restante, segue do Exemplo 2.5 e do fato das operações serem realizadas entrada a entrada.

Como todos os axiomas de espaços vetoriais foram satisfeitos, temos que $\mathbb{Z}_2^n$ é um espaço vetorial sobre $\mathbb{Z}_2$.

Definição 2.29 (Subespaço Vetorial)**.** Seja V um espaço vetorial sobre um corpo $\mathbb{K}$ e W um subconjunto de V. Dizemos que W é um subespaço vetorial de V ou simplesmente um subespaço de V, se as seguintes condições são satisfeitas:

(i) $0 \in W$;

(ii) $\lambda u \in W$, para todo $\lambda \in \mathbb{K}$ e todo $u \in W$;

(iii) $u + v \in W$, para todo $u, v \in W$.

Exemplo 2.28. Todo o espaço vetorial V admite pelo menos dois subespaços: o conjunto $\{0\}$, chamado subespaço zero ou subespaço nulo, e o próprio espaço vetorial V. Esses dois são subespaços triviais de V. Os demais são chamados de subespaços própios de V.

Observação 2.16. Sejam V um espaço vetorial sobre um corpo $\mathbb{K}$ e W um subespaço de V. Como $(V, +)$ é um grupo, segue da definição de Subespaço, que $(W, +)$ é subgrupo de $(V, +)$.

Definição 2.30. Sejam V um espaço vetorial sobre um corpo $\mathbb{K}$, e $v_1, ..., v_n \in V$ e $a_1, ..., a_n \in \mathbb{K}$. Então, o vetor

$$v = a_1 v_1 + ... + a_n v_n$$

é um elemento de V ao qual chamamos de combinação linear de $v_1, ..., v_n$.

Proposição 2.17. *Sejam os vetores $v_1, ..., v_n \in V$, o conjunto W de todos os vetores de V, que são combinação linear destes, o qual é denotada por*

$$W = [v_1, ..., v_n] = \{v \in V : v = a_1 v_1 + ... + a_n v_n,\ a_i \in \mathbb{K}, 1 \leq i \leq n\}.$$

é um subespaço de V e W é chamado de subespaço gerado por $v_1, ..., v_n$.

Prova. Vamos provar que W satisfaz as três propriedades da Definição de Subespaço.

(i) $0 \in W$, pois,

$$0 = 0v_1 + ... + 0v_n.$$

(ii) Sejam $v = a_1v_1 + ... + a_nv_n$, $w = b_1v_1 + ... + b_nv_n \in W$. Então, pela propriedade de associatividade e comutatividade em V, podemos escrever:

$$v + w = (a_1v_1 + ... + a_nv_n) + (b_1v_1 + ... + b_nv_n) = (a_1 + b_1)v_1 + ... + (a_n + b_n)v_n \in W.$$

(iii) Sejam $\alpha \in \mathbb{K}$ e $v = a_1v_1 + ... + a_nv_n \in W$. Então,
$\alpha v = \alpha(a_1v_1 + ... + a_nv_n) = \alpha(a_1v_1) + ... + \alpha(a_nv_n) = (\alpha a_1)v_1 + ... + (\alpha a_n)v_n \in W$.
Portanto, de $(i) - (iii)$ segue-se que $[v_1, ..., v_n]$ é um subespaço de V.

■

Exemplo 2.29. Os vetores $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ e $e_3 = (0, 0, 1)$, geram o espaço vetorial $\mathbb{R}^3$, pois qualquer $v = (x, y, z) \in \mathbb{R}^3$ é uma combinação linear de e_1, e_2, e_3

$$(x, y, z) = x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1)$$

ou

$$v = xe_1 + ye_2 + ze_3,$$

então $[e_1, e_2, e_3] = \mathbb{R}^3$.

Definição 2.31. Sejam V um espaço vetorial e $A = \{v_1, ..., v_n\} \subset V$. O conjunto A se diz **linearmente independente** (LI) ou que os vetores $v_1, ..., v_n$ são LI, caso a equação

$$a_1v_1 + ... + a_nv_n = 0,$$

admita apenas a solução trivial, isto é,

$$a_1 = a_2 = ... = a_n = 0.$$

Se exixtir $a_i \neq 0$, para algum $i = 1, ..., n$, diz que o conjunto A é linermente dependente (LD) ou que os vetores $v_1, ..., v_n$ são LD.

Definição 2.32 (Base de um Espaço Vetorial)**.** Um conjunto $B = \{v_1, ..., v_n\} \subset V$ é uma base para o espaço vetorial V se:

(i) B é LI;

(ii) B gera V.

Exemplo 2.30. Sejam

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ e } M_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R}).$$

O conjunto $\alpha = \{M_1, M_2, M_3, M_4\}$ é base de $M_2(\mathbb{R})$. Com efeito, para vermos que α gera $M_2(\mathbb{R})$, observemos que um vetor qualquer

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

em $M_2(\mathbb{R})$ pode ser escrito como

$$M = aM_1 + bM_2 + cM_3 + dM_4.$$

Para verificarmos que α é linearmente independente, suponhamos que

$$M = aM_1 + bM_2 + cM_3 + dM_4 = 0,$$

ou seja,

$$a_1\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a_2\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a_3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + a_4\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Segue-se que $a_1 = a_2 = a_3 = a_4 = 0$ e, portanto, α é linearmente independente. A base α é chamada de base canônica de $M_2(\mathbb{R})$.

Teorema 2.14. *Se $B = \{v_1, ..., v_n\}$ for uma base de um espaço vetorial V, então todo conjunto com mais de n vetores em V será linearmente dependente.*

Prova. A prova deste Teorema encontra-se em Louredo e Oliveira (2015, p. 23) ■

Definição 2.33 (Dimensão de um Espaço Vetorial)**.** Seja V um espaço vetorial sobre umj corpo $\mathbb{K}$. Se V possui uma base com n vetores, então V tem dimensão n e denota-se $dim\ V = n$.

Quando um espaço vetorial V admite uma base finita, dizemos que V é um espaço vetorial de dimensão finita. Se V tem uma base com infinitos vetores, então a dimensão de V é infinita e denota-se $dimV = \infty$.

Exemplo 2.31. Os conjuntos dos Exemplos 2.29 e 2.30 são bases para $\mathbb{R}^3$ e $M_2(\mathbb{R})$, respectivamente. Logo, $\dim\mathbb{R}^3 = 3$ e $\dim M_2(\mathbb{R}) = 4$.

Proposição 2.18 (Conjunto LI)**.** *Seja V um espaço vetorial sobre $\mathbb{K}$ e considere $B = \{v_1, ..., v_n\}$ um conjunto LI, em V. Se existir $v \in V$ que não seja combinação linear dos elementos de B, então $\{v_1, ..., v_n, v\}$ é linearmente independente.*

Prova. Sejam $\alpha_1, ..., \alpha_n, \alpha_{n+1}$ escalares tais que

$$\alpha_1 v_1 + ... + \alpha_n v_n + \alpha_{n+1} v = 0.$$

Se $\alpha_{n+1} \neq 0$, então podemos escrever

$$v = -\frac{\alpha_1}{\alpha_{n+1}}v_1 - ... - \frac{\alpha_n}{\alpha_{n+1}}v_m$$

o que é uma contradição com a hipótese de v não ser uma combinação linear de elementos de B.. Então $\alpha_{n+1} = 0$ e, portanto, $\alpha_1 v_1 + ... + \alpha_n v_n = 0$. Como o conjunto B é LI, segue então que $\alpha_1 = ... = \alpha_n = 0$. Portanto $\{v_1, ..., v_n, v\}$ é LI. ■

Proposição 2.19 (Base)**.** *Seja V um espaço vetorial com $dim V = n$ e $B = \{v_1, ..., v_n\}$ um conjunto LI em V. Então, B é uma base para V.*

Prova. Se B gerar V, então B é uma base para V. Se B não gera V, então existe um vetor $v \in V$, tal que $v \notin [B]$. Logo pela Proposição 2.18, o conjunto $A = \{v_1, ..., v_n, v\}$ é LI, o que contraria o Teorema 2.14, pois $n(A) = n + 1 > n = dim\ V$. ■

Definição 2.34 (Hiperplano)**.** Seja V um espaço vetorial não nulo. Um hiperplano de V é um subespaço próprio W tal que se W' for um subespaço de V satisfazendo $W \subseteq W' \subseteq V$, então $W = W'$ ou $W' = V$.

Proposição 2.20. *Sejam V um $\mathbb{K}$-espaço vetorial de dimensão $n \geq 1$ e W um subespaço próprio de V. Então W é um hiperplano de V se, e somente, dim $W = n - 1$.*

Prova. A prova deste Teorema encontra-se em Coelho e Lourenço (2007, p. 120) ■

3 CONTANDO OS SUBGRUPOS DE ÍNDICE 2

No Capítulo anterior trabalhamos alguns conceitos e resultados que servirão como pré-requisitos necessários para o entendimento deste Capítulo que trata- se de uma abordagem didática do texto "How Rare Are Subgroups of Index 2?", de autoria Jean B. Nganou, encontrado na referência Nganou (2012).

A motivação de Nagnou vem da procura por contraexemplos da recíproca do Teorema de Lagrange (Teorema 2.6), em particular, ele procura grupos de ordem n, com n par, que não possuem subgrupos de índice 2, consequentemente, que não possuem subgrupos cuja ordem é $n/2$. A ideia dele é generalizar o que acontece com o grupo alternado A_4, cuja ordem é 12, mas não possue subgrupos de ordem 6.

Diante dessa motivação, consideramos especialmente o papel desempenhado pelo subgrupos, de um grupo G, da forma G^2, como no Exemplo 2.11, para determinar subgrupos de índice 2. Usando esta abordagem, identificamos uma classe maior de grupos que não possuem subgrupos de índice 2, isto é, uma maior classe de contraexemplos da recíproca do Teorema de Lagrange.

Atentamos a importância do tema, pois os subgrupos de índice 2 são de interesse especial porque são sempre normais, como visto na Proposição 2.8.

3.1 A Contagem de Subgrupos de Índice 2

Do Exemplo 2.18, grupos de ordem ímpar não possuem subgrupos de índice 2, assim apenas os grupos finitos de ordem par serão importantes aqui.

Inicialmente, vamos tentar contar quantos subgrupos de índice 2 existem num grupo G. Para isso, considere o seguinte teorema:

Teorema 3.1. *Os grupos G e G/G^2 têm o mesmo número de subgrupos de índice 2.*

Prova. Seja H um subgrupo de índice 2 em G, logo H é um subgrupo normal em G, pela Proposição 2.8, e o quociente G/H tem ordem 2, pois $G/H = \{H, aH\}$, com $a \in G$ e $a \notin H$. Como,

$$a^2H = (aH)^2 = H,$$

para todo $a \in G$, pelo item (iii) da Observação 2.11, $a^2 \in H$ para todo $a \in G$ e assim $G^2 < H$. Pelo Exemplo 2.19, G^2 é normal em G, então pela Proposição 2.11, G^2 é normal em H.

Agora, consideramos o grupo quociente H/G^2 que, também pela Proposição 2.11, é um subgrupo de G/G^2. Pelo Teorema de Lagrange, $|G| = |H|(G : H)$. Como H tem índice 2, temos

$$|G| = |H|(G : H) \Rightarrow |G|/|H| = 2.$$

e, ainda,

$$|G/G^2| = |H/G^2|(G/G^2 : H/G^2).$$

Logo,

$$(G/G^2 : H/G^2) = |G/G^2|/|H/G^2| = |G|/|H| = 2. \tag{3.1}$$

Sejam $S = \{H < G; (G : H) = 2\}$ e $S_1 = \{H/G^2 < G/G^2; (G/G^2 : H/G^2) = 2\}$. Definindo uma função φ do conjunto se subgrupos de índice 2 de G, S, para o conjunto de subgrupos de índice 2 de G/G^2, S_1, definida da seguinte forma

$$\begin{array}{rcl} \varphi : S & \to & S_1 \\ H & \mapsto & \varphi(H) = H/G^2 \end{array}$$

temos φ bem definida, pelo argumentado acima. Além disso, φ é injetora, pois dados H_1 e $H_2 \in S$ temos

$$\varphi(H_1) = \varphi(H_2) \Leftrightarrow H_1/G^2 = H_2/G^2 \Leftrightarrow H_1 = H_2.$$

Isso mostra que a função φ é injetiva. Dado um quociente genérico $H/G^2 \in S_1$, temos, pela Proposição 2.12, $H < G$. Como $(G/G^2 : H/G^2) = 2$, assim por 3.1, temos

$$(G/G^2 : H/G^2) = |G|/|H| = 2$$

daí, $|G| = |H| \cdot 2$, assim $(G : H) = 2$. Como H tem índice 2, então $H \in S$ e

$$\varphi(H) = H/G^2.$$

Isto mostra que a função φ é sobrejetora. Portanto, φ é bijetiva. Ainda, sobre a sua inversa, para $H/G^2 \in S_1$, temos $\varphi^{-1}(H/G^2) = H$.

Como existe uma bijeção entre os conjuntos, então possuem a mesma cardinalidade.

■

Agora, vamos analisar o grupo quociente G/G^2.

Se G é um grupo que satifaz a seguinte condição $x^2 = e$ para todo $x \in G$, então pelo item (iii) da Proposição 2.6, G é um grupo abeliano. Assim, segue da Proposição acima, que G/G^2 é abeliano, pois

$$(aG^2)^2 = a^2G^2 = G^2$$

para todo $a \in G$, uma vez que $a^2 \in G^2$.

Assim, se $|G/G^2| > 1$, então G/G^2 é um grupo abeliano finito, em que todos os elementos, exceto a identidade, têm ordem 2. Daí, pelo Teorema 2.10, G/G^2 é isomorfo a um produto direto de grupos cíclicos, mas como todo elemento, exceto a identidade, tem

ordem 2, então o único grupo que pode aparecer na sua decomposição direta é $\mathbb{Z}_2$. Ou seja, existe um número inteiro $n \geq 0$ tal que

$$G/G^2 \simeq \mathbb{Z}_2^n \tag{3.2}$$

Em que $n = 0$, significa que $G/G^2 \simeq \{\bar{0}\}$ é o grupo trivial, o que acontece exatamente quando $G = G^2$.

Observação 3.1. Da análise combinatória, um subespaço k-dimensional sobre $\mathbb{Z}_2$, tem 2^k elementos, logo observando-o como subgrupo (o que é possível pela Observação 2.16) sua ordem será 2^k. Nesse contexto, considerando $\mathbb{Z}_2^n$ como espaço vetorial sobre $\mathbb{Z}_2$, Pelo Teorema de Lagrange (Teorema 2.6), subgrupos de índice 2 de $\mathbb{Z}_2^n$ tem ordem 2^{n-1}. Assim o subgrupo é composto por n coordenadas, onde uma é composta por $\overline{0}$, já as demais são compostas por elementos pertencentes a $\mathbb{Z}_2$ que, sem perda de generalidade, podemos representar da seguinte forma

$$(\overline{a_1}, ..., \overline{a_{n-1}}, \overline{a_n}),\ a_i \in \mathbb{Z}_2 \text{ e } \overline{a_j} = \overline{0} \text{ para algum } j = 1, ..., n,$$

o que corresponde a um espaço vetorial de dimensão $n-1$.

Teorema 3.2. *Cada espaço vetorial n−dimensional sobre $\mathbb{Z}_2$ tem exatamente $2^n - 1$ hiperplanos.*

Prova. Sem perda de generalidade, assumimos que $V = \mathbb{Z}_2^n = \{(\overline{a_1}, \overline{a_2}, \cdots, \overline{a_n}); \overline{a_i} \in \mathbb{Z}_2\}$ é um Espaço Vetorial definido sobre o corpo $\mathbb{Z}_2$. A prova do Teorema usa argumentos de análise combinatória e álgebra linear.

Primeiramente, contamos os conjuntos linearmente independentes de $n-1$ vetores de $\mathbb{Z}_2^n$. Para isso, escolhemos cuidadosamente $n-1$ vetores $v_1, v_2, ..., v_{n-1}$.

Para escolher o primeiro vetor, temos que evitar o vetor nulo de $\mathbb{Z}_2^n$ assim nos resta $2^n - 1$ possibilidades de escolhas para v_1. Depois de escolher v_1 devemos escolher v_2 de tal forma que $v_2 \notin [v_1] = \{0, v_1\}$, e há $2^n - 2$ possibilidades para a escolha do vetor.

Suponha que escolhemos de v_1 a v_k, escolhendo $v_{k+1} \notin [v_1, ..., v_k]$, o mesmo não pode pertencer ao subespaço gerado por $[v_1, ..., v_k]$ para permanecer a independência linear.

Como por análise combinatória, $[v_1, v_2, ..., v_k]$ possui ordem 2^k e $|V| = 2^n$, temos $2^n - 2^k$ possibilidades para a escolha do vetor v_{k+1} de modo a preservar a independência linear. Ou seja, por indução, para cada subespaço de dimensão k, existem $2^n - 2^k$ possibilidades para a escolha do próximo vetor LI com esse espaço. Assim, por análise combinatória, o número de subconjuntos de $n-1$ vetores LI sobre $\mathbb{Z}_2$ é dado pelo produto do número das possibidades para a escolha dos vetores v_1, v_2, ..., v_{n-1}, respectivamente dada por

$$(2^n - 2^0)(2^n - 2) \cdots (2^n - 2^{n-2}) \tag{3.3}$$

Como, pela Observação acima, cada hiperplano de $\mathbb{Z}_2^n$ tem 2^{n-1} vetores, de maneira análoga, temos

$$(2^{n-1} - 2^0)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2}) \tag{3.4}$$

bases distintas. Cada um desses conjuntos é a base de um hiperplano, mas por serem subespaços, bases diferentes podem dar origem ao mesmo hiperplano. Para calcularmos o número de hiperplanos sob V basta dividir o número de conjuntos LI de $n-1$ vetores de V pelo número de conjuntos de bases dos hiperplanos. Logo, se N_H é o números de hiperplanos de $\mathbb{Z}_2^n$, então

$$N_H = \frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})}{(2^{n-1} - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})}.$$

Multiplicando o numerador e denominador por 2^{n-2} temos

$$N_H = \frac{2^{n-2}(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})}{2^{n-2}(2^{n-1} - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})},$$

decompondo os fatores de 2^{n-2} do denominador entre os fatores do mesmo temos

$$\begin{aligned}
N_H &= \frac{2^{n-2}(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})}{2(2^{n-1} - 1)2(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})} \\
&= \frac{2^{n-2}(2^n - 1)\cancel{(2^n - 2)} \cdots \cancel{(2^n - 2^{n-2})}}{\cancel{(2^n - 2)}\cancel{(2^n - 2^2)} \cdots (2^{n-1} - 2^{n-2})} \\
&= \frac{2^{n-2}(2^n - 1)}{(2^{n-1} - 2^{n-2})} \\
&= \frac{\cancel{2^{n-2}}(2^n - 1)}{\cancel{2^{n-2}}\left(\frac{2^{n-1}}{2^{n-2}} - 1\right)}.
\end{aligned}$$

Assim, temos

$$N_H = \frac{2^n - 1}{\frac{2^{n-1}}{2^{n-2}} - 1} = \frac{2^n - 1}{2 - 1} = 2^n - 1,$$

logo, $N_H = 2^n - 1$ conforme determinado. ∎

Combinando o Teorema 3.1 com o Teorema 3.2 temos série de Corolários que nos ajudam a determinar o número de subgrupos de índice 2 de um grupo finito G, objetivo principal deste Capítulo.

Corolário 3.1. *Existem exatamente* $2^n - 1$ *subgrupos de índice* 2 *em* G *onde* n *é o número inteiro de isomorfismos em 3.2.*

Prova. Pelo Isomorfismo 3.2, os subgrupos de G/G^2 possuem o mesmo números de subgrupos de $\mathbb{Z}_2^n$. Pela Observação 2.16 , os subgrupos de G/G^2 se associam-se aos subspaços

de $\mathbb{Z}_2^n$ e, da Observação 3.1, os subgrupos de índice 2 de G/G^2 associam-se aos subespaços de $\mathbb{Z}_2^n$ de dimensão $n-1$ (os hiperplanos). Pelo Teorema 3.2, $\mathbb{Z}_2^n$ tem 2^n-1 hiperplanos. Logo existem 2^n-1 subgrupos de índice 2 em G/G^2, e pelo Teorema 3.1, concluímos que há 2^n-1 subgrupos de índice 2 em G. ■

Corolário 3.2. *Um grupo não tem subgrupo de índice* 2 *se, e somente se, ele for gerado por quadrados.*

Prova. Se G não tem subgrupos de índice 2, então do Corolário 3.1, $n = 0$ e,daí, tem-se $G = G^2$, assim temos que G é gerado por quadrados.

Se G é gerado por quadrados, então $G = G^2$, daí temos, pelo Isomorfismo 3.2, que $n = 0$ e, pelo Corolário 3.1, existem 0 subgrupos de índice 2 em G. ■

Corolário 3.3. *Um grupo G tem um único subgrupo de índice* 2 *se, e somente se, G^2 tem índice* 2 *em G.*

Prova. Se G tem um único subgrupo de índice 2, então, pelo Corolário 3.1, $n = 1$ assim pelo Isomorfismo 3.2 temos que $G/G^2 \simeq \mathbb{Z}_2$. Como a cardinalidade de $\mathbb{Z}_2$ é igual a 2 segue que a ordem de G/G^2 também é 2, o que implica que $(G : G^2) = 2$.

Se $(G : G^2) = 2$, segue que a ordem de G/G^2 é igual a 2, daí a cardinalidade de $\mathbb{Z}_2^n$ também é 2, pelo Isomorfismo 3.2, logo $G/G^2 \simeq \mathbb{Z}_2$, daí pelo Corolário 3.1, $n = 1$ e assim temos que G tem um único subgrupo de índice 2. ■

Pela Observação 2.13, $G^I \subseteq G^2$ segue do Teorema 2.9 que se mais da metade dos elementos de G têm ordem ímpar, então G não tem subgrupos de índice 2. Vale salientar que esta condição não é necessária para um grupo não ter subgrupos de índice 2, pois o grupo linear

$$SL_2(\mathbb{Z}_3) = \left\{ A = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in M_2(\mathbb{Z}_3);\ detA = \overline{1} \right\}$$

é um grupo de ordem 24 que não tem subgrupos de índice 2 e tem apenas 9 elementos de ordem ímpar que são

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{2} & \overline{0} \end{pmatrix},$$
$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{2} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{2} & \overline{2} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix},$$
$$\begin{pmatrix} \overline{2} & \overline{2} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{2} \end{pmatrix}.$$

3.2 Consequências Importantes

Apresentamos a seguir algumas consequências dos resultados vistos anteriormente.

Exemplo 3.1. Seja n um números inteiro com $n \geq 2$, o grupo alternado A_n não tem subgrupos de índice 2. De fato, pelo Corolário 3.2, se mostrarmos que A_n é gerado por quadrados o resultado estará provado. Pelo Teorema 2.4 cada permutação par é um produto de 3-ciclos. Assim só precisamos mostrar que cada 3-ciclos está em A_n^2.

Dado um 3-ciclo $\alpha \in A_n$, sendo $\alpha = (abc)$, temos $\alpha^{-1} = (cba)$. Fazendo $\alpha^{-1}\alpha^{-1} = (cba)(cba) = (abc)$, temos $\alpha = \alpha^{-2} = (\alpha^{-1})^2 \in A_n^2$, assim pelo Corolário 3.2, A_n não possui subgrupos de índice 2.

Exemplo 3.2. S_n tem um único subgrupo de índice 2, que é A_n. Sabemos que A_n tem índice 2. Se mostrarmos que $A_n = S_n^2$, então pelo Corolário 3.3 o exemplo estará provado.

Vimos no exemplo anterior que A_n não possui subgrupos de índice 2, logo pelo Corolário 3.2, $A_n = A_n^2$. Como $A_n \subseteq S_n$, assim temos que $A_n^2 \subseteq S_n^2$, daí temos que $A_n \subseteq S_n^2$. Como cada elemento de S_n^2 é uma permutação par, pois o quadrado de toda permutação é par, então temos que $S_n^2 \subseteq A_n$, daí segue que $A_n = S_n^2$.

Como A_n tem índice 2 e $A_n = S_n^2$, então pelo Corolário 3.3 o resultado está provado.

Teorema 3.3. *D_n tem um único subgrupo de índice 2 se n é ímpar e três subgrupos de de índice 2 quando n é par.*

Prova. Diante da descrição de D_n, temos que $D_n^2 = R_n^2$, pois pela Observação 2.10, os elementos de R_e são reflexões de ordem 2 da forma $\beta\alpha^i$, ou seja, quando são elevados ao quadrado não formam nenhum elemento, exceto Id, do subgrupo D_n^2.

Agora, da Proposição 2.6, se a é um elemento de ordem m, ou seja, $O(a) = m$ então para cada inteiro $k > 0$, temos $O(a^k) = m/mdc(m,k)$. Como $|R_n| = O(\alpha) = n$, temos

$$|R_n^2| = O(\alpha^2) = \begin{cases} n/2, \text{ se } n \text{ é par} \\ n, \text{ se } n \text{ é ímpar} \end{cases}.$$

Portanto,

$$|D_n/D_n^2| = |D_n/R_n^2| = \frac{2n}{|R_n^2|} = \begin{cases} 4, \text{ se } n \text{ for par} \\ 2, \text{ se } n \text{ for ímpar.} \end{cases}$$

E o Isomorfismo 3.2 para o grupo D_n é dado por:

$$D_n/D_n^2 \simeq \begin{cases} \mathbb{Z}_2^2, \text{ se } n \text{ for par} \\ \mathbb{Z}_2, \text{ se } n \text{ for ímpar .} \end{cases}$$

O resultado é dado a partir do Corolário 3.1.

O Teorema 2.3 nos fornece uma grande classe de contraexemplos da recíproca do Teorema de Lagrange.

Pelo Corolário 3.2 e do Teorema 2.3, se G_1 e G_2 não tem subgrupos de índice 2, então $G_1 \times G_2$ não tem subgrupos de índice 2. Pelo Exemplo 3.1, para cada $n \geq 4$ e pelo Teorema 2.6, para cada m natural ímpar, o grupo $A_n \times \mathbb{Z}_m$ não tem subgrupos de índice 2. Como a ordem é $n!m/2$, então temos um contraexemplo da recíproca do Teorema de Lagrange. Outros contraexemplos são $SL_2(\mathbb{Z}_3) \times A_n$, com $n \geq 4$ e $SL_2(\mathbb{Z}_3) \times \mathbb{Z}_n$, com n ímpar.

4 CONSIDERAÇÕES FINAIS

Este trabalho tem como objetivo aprender mais sobre a existência de subgrupos de índice 2 em outros grupos. Possibilitando o estudo de um resultado que permite determinar a quantidade de subgrupo de índice 2 sobre grupos finitos. A motivação sobre esse estudo se originou através da relevância que esse estudo tem na academia, como também, através de um aprimoramento visto no desenvolvimento da pesquisa realizada no Programa Institucional de Bolsas de Iniciação Cientifica (PIBIC), realizado durante o curso de Licenciatura plena em Matemática.

O estudo feito para a elaboração deste trabalho nos possibilitou um rico estudo sobre grupos finitos, através de ferramentas da Álgebra Abstrata e da Álgebra Linear vistas na graduação.

Espera-se colaborar com a produção de conhecimento científico, de forma que fornecemos aqui uma abordagem didática para apresentação de um resultado que, em geral não se encontra em livros didáticos de Álgebra Abstrata. Contribuindo para o enriquecimento e aprimoramento da bagagem de conhecimento ofertada ao final do curso.

REFERÊNCIAS

ALENCAR FILHO, E. *Teoria elementar dos Números*. São Paulo: Nobel, 1981.

COELHO, F. U.; LOURENÇO, C. L. *Um Curso de Algebra Linear*. São Paulo: EDUSP, 2007.

DOMINGUES, H. H. *Álgebra Moderna.* 4. ed. São Paulo: Atual Editora, 2003.

GARCIA, A. I.; LEQUAIN, Y. *Elementos de Álgebra.* Rio de Janeiro: IMPA, 2018. 363 p.

HEFEZ, A.; FERNANDES, C. S. *Introdução à Algebra Linear*. SBM, 2016.

HUNGERFORD, T. W. *Algebra* . Nova York: Springer-Verlag , 1980.

LOUREDO, A. T.; OLIVEIRA, A. M. *Um primeiro curso de Algebra Linear*. 21.ed. Campina Grande: EDUEPB, 2015.

NGANOU, J. B. *How Rare Are Subgroups of Index 2?*. Mathematics Magazine. Disponível em: `http://www.jstor.org/stable/10.4169/math.mag.85.3.215`. Acesso em: 16 dez. 2020.

SOUZA, J. A. *Uma nota sobre a Teoria dos Grupos: da Teoria de Galois à Teoria de Gauge*. Revista Brasileira de História da Matemática, Maringá, v. 12, ed. 24, p. 71-81, 2012. Disponível em:`https://www.rbhm.org.br/index.php/RBHM/article/view/108/92`. Acesso em: 20 set. 2021.

STEINBRUCH, A.; WINTERLE, P. Álgebra Linear. São Paulo: PEARSON EDUCATION DO BRASIL, 1997.

VIEIRA, V. L. *Álgebra Abstrata para Licenciatura* (2° edição), Editora da Universidade Estadual da Paraíba (coedição: editora livraria da Física), Campina Grande/São Paulo 2015.

VIEIRA, V. L. *Um curso Básico em Teoria dos Números*. Campina Grande: EDUEPB, 2013.