Universidade Federal de São João del-Rei
Coordenadoria do Curso de Matemática
Curso de Matemática

Ana Paula Cançado

Grupo Diedral: o estudo de grupos de simetrias em polígonos regulares

São João del Rei - MG

2016

ANA PAULA CANÇADO

Grupo Diedral: o estudo de grupos de simetrias em polígonos regulares

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Matemática da Universidade Federal de São João del-Rei para a obtenção do grau de licenciado em Matemática.

Orientadora:

Profª. Ma. LORENA MARA COSTA OLIVEIRA

São João del Rei - MG

2016

ANA PAULA CANÇADO

Grupo Diedral: o estudo de grupos de simetrias em polígonos regulares

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Matemática Universidade Federal de São João del-Rei para a obtenção do grau de licenciado em Matemática.

Aprovada em novembro de 2016.

BANCA EXAMINADORA

Profª. Ma. Lorena Mara Costa Oliveira - Orientadora

UFMG

Prof. Dr. Fábio Alexandre de Matos

UNICAMP

Prof. Me. Gustavo Terra Bastos

UFV

São João del Rei - MG

2016

À memória de meu avô João Miguel da Silva.

Agradecimentos

Quero agradecer a todas as pessoas, que colaboraram diretamente ou indiretamente na realização deste trabalho.

Primeiramente, agradeço a Deus pelas oportunidades que me foram dadas. Além do mais, até aqui Ele tem me sustentado, dando-me direcionamento, força e vontade em prosseguir e, jamais desistir, por mais que sejam difíceis as circunstâncias.

Aos meus pais, que em meio às dificuldades se empenharam em me ajudar de todas as formas possíveis, proporcionando-me bem estar, carinho e incentivo.

A minha orientadora Profª Ma. Lorena Mara Costa Oliveira pela sua dedicação, paciência e por tudo o que me ensinou ao longo deste trabalho. Certamente, o que aprendi será de grande valia para minha carreira.

E também, a todos os professores do Curso de Matemática da UFSJ, que contribuíram para meu crescimento profissional e pessoal. Mas, em especial a profª Drª Romélia Mara Alves Souto por ser um exemplo a ser seguido, além do que, suas palavras e ensinamentos tornaram-me uma pessoa melhor.

"Só sei que nada sei, e o fato de saber isso, me coloca em vantagem sobre aqueles que acham que sabem alguma coisa." (Sócrates)

Resumo

Este presente trabalho tem por objetivo estudar o *Grupo Diedral* (denotado por D_n) de ordem $2n$, o qual torna-se grupo (não abeliano) com a operação composição de aplicações. Os elementos de D_n podem ser obtidos a partir de rotações ao redor do centro de gravidade e reflexões em torno dos eixos de simetria em polígonos regulares. Sendo assim, verificaremos o caso geral em um polígono regular de n lados e, em seguida, abordaremos alguns exemplos, em que destacaremos as simetrias do triângulo equilátero e do quadrado. Para esse fim, serão necessários conceitos elementares da teoria de Grupos para o desenvolvimento deste trabalho.

Palavras-chave: *Teoria de Grupos, Grupo Diedral, Polígonos Regulares.*

Sumário

Lista de Símbolos **8**

Introdução **9**

1 Grupos **12**

1.1 Definição e Exemplos de Grupos 12

1.2 Subgrupos 20

1.3 Grupos Cíclicos 23

2 Classes Laterais e Conjugadas **27**

2.1 Classes Laterais 27

2.2 Subgrupos Normais 29

2.3 Teorema de Lagrange 31

2.4 Classes Conjugadas 31

3 Homomorfismo de Grupos e Grupos de Permutações **34**

3.1 Homomorfismo de Grupos 34

3.2 Isomorfismo de Grupos 36

3.3 Grupos de Permutações 37

4 *Grupo Diedral*: Generalização e Exemplos **39**

4.1 Generalização do *Grupo Diedral* 39

4.2 Exemplos de *Grupos Diedrais* 45

4.2.1 Simetrias do Triângulo Equilátero 45

4.2.2 Simetrias do Quadrado 48

5 Considerações Finais **53**

Referências Bibliográficas **54**

Lista de Símbolos

$\emptyset$	vazio
$\geq$	maior ou igual
$\in$	pertence
$\forall$	para todo e qualquer
$\exists$	existe
$\cap$	interseção
I_n	matriz identidade
$\notin$	não pertence
$\subseteq$	contido e igual
$\neq$	diferente
$(G : H)$	índice do subgrupo H em G
$\triangleleft$	subgrupo normal
$Ker\ f$	núcleo do homomorfismo f
$Im\ f$	imagem de uma função
$\circ$	composição de aplicações
$\mathbb{Z}_m$	conjunto das classes dos restos módulo m
$G \simeq J$	G é isomorfo a J
det	determinante
S_n	conjunto de permutações de n elementos
D_n	conjunto de rotações e reflexões de um polígono regular de n lados
$Bij(E)$	conjunto de bijeções de E em E
$M_n(\mathbb{R})$	matriz $n \times n$ com entrada nos reais
$GL_n(\mathbb{R})$	conjunto de matizes $n \times n$, cujo $det\ M \neq 0$
i_E	função identidade que leva E em E
g^{-1}	função inversa que leva E em E
$H < G$	H é subgrupo de G
$[a]$	gerador de um grupo cíclico
R	relação de equivalência
$n!$	n fatorial, corresponde a $n.(n-1).(n-2)\ldots 2.1$
$o(G)$	ordem de G
C_x	classe de conjugação determinada por x

Introdução

Apresentaremos neste trabalho a Teoria de Grupos, a qual será importante para o desenvolvimento do mesmo. Sendo assim, essa teoria voltada para o estudo do *Grupo Diedral* será o foco de nossa pesquisa.

Neste sentido, podemos fazer duas perguntas essenciais para esclarecer melhor o leitor: *"o que é um Grupo?"* e *"como surgiu essa teoria?"*

Grupo é definido por um conjunto não vazio e as suas operações, as quais satisfazem as seguintes propriedades: a associatividade, a existência dos elementos neutro e inverso. Essa simples estrutura matemática transformou toda a ciência Matemática.

Por conseguinte, o estudo de Grupos - a "Teoria de Grupos", decorre do estudo de vários matemáticos na busca da solução por radicais de equações algébricas.

A seguir, trataremos brevemente da história da Teoria de Grupos e, como ela emerge da "teoria de permutações ou simetrias". Esta última, será fundamental para nosso estudo, pois o *Grupo Diedral* está diretamente relacionado a esse conceito.

Segundo Iezzi (2003), entre 1500 e 1515, o matemático italiano Scipione del Ferro (1456 - 1526) descobriu um método para resolver a equação cúbica $x^3 + px = q$ $(p; q > 0)$. Del Ferro verificou que a equação dada é resolúvel por radicais. No entanto, a solução de Del Ferro apresentou o seguinte desafio para os algebristas: *"será que toda equação algébrica é resolúvel por radicais?"* Essa questão só começou a ser esclarecida genericamente na segunda metade do século XVII, através das pesquisas de Joseph-Louis Lagrange (1736 - 1813). Assim, Lagrange observou que a "teoria das permutações ou simetrias" era de grande relevância para a resolução de equações.

Em 1824, o matemático norueguês Niels Henrik Abel (1802 - 1829) mostrou que não há nenhuma fórmula geral por radicais para resolver as equações de grau ≥ 5. Contudo, uma questão permanecia em pé: *"por que algumas equações de grau* ≥ 5 *são resolúveis por radicais e, o que caracteriza esse tipo de equação?* (IEZZI, 2003)

De acordo com Baumgart (1992), estimulado pelo trabalho de Abel, o jovem francês Évariste Galois (1811 - 1832) mostrou que toda equação pode ser associada a um grupo característico e que as propriedades desse grupo podem ser usadas para determinar se a equação é solúvel por radicais ou não.

Portanto, o termo grupo foi utilizado em seu sentido atual pela primeira vez por Ga-

lois, que grosso modo, procurou descrever os grupos de simetrias satisfeitos pelas soluções da equação algébrica.

A ideia de grupo se tornou um instrumento útil para a Matemática e as outras áreas do conhecimento. Ela reflete na teoria das equações, na teoria dos números, na geometria diferencial, na cristalografia, em estudos sobre o átomo e partículas subatómicas, etc. Essencialmente, o *Grupo Diedral* é usado para retratar simetrias de figuras bi(tri)-dimensionais regulares.

Neste trabalho, o leitor conhecerá os principais conceitos, propriedades e resultados da Teoria de Grupos que, como mencionado anteriormente, servirá de base para o estudo do *Grupo Diedral*. Para isso, pretendemos nos três capítulos iniciais, trabalhar apenas essa teoria, com intuito de fixar melhor os conceitos estudados. E, o último capítulo será exclusivo para o estudo do grupo em questão. Sendo assim, o trabalho será distribuído da seguinte maneira:

No capítulo 1, serão dadas noções básicas de Grupos, Subgrupos e Grupos Cíclicos, em que destacaremos propriedades, proposições e exemplos relativos a esses tópicos.

No capítulo 2, estudaremos Classes Laterais e daremos exemplos das mesmas. A partir desse conceito, definiremos Subgrupos Normais e destacaremos alguns de seus exemplos. Além do mais, apresentaremos o Teorema de Lagrange e definiremos Classes Conjugadas. Esta última, será relacionada com Subgrupos Normais.

No capítulo 3, apresentaremos Homormofismo de Grupos e as principais propriedades que envolvem o mesmo. Partindo desse conceito, definiremos Isomorfismo de Grupos e mostraremos exemplos. Além disso, abordaremos o Grupo de Permutações e importantes resultados desse conceito, que será relevante para estudo do *Grupo Diedral*.

Por fim, o capítulo 4 será o centro deste trabalho, em que será tratado da generalização e exemplificação do *Grupo Diedral*. Neste sentido, pretendemos por meio da generalização, apresentar os movimentos de rotações e reflexões, que ocorrem no polígono regular P_n e, formam o conjunto D_n. Além do mais, provaremos que D_n é grupo (não abeliano) com a composição de aplicações. Esse grupo pode ser chamado de *Grupo Diedral ou Simétrico* ou até mesmo de *Grupo de Permutações*, já que os movimentos são representados por permutações. Os resultados obtidos na generalização serão observados através de exemplos, em que destacaremos os grupos de simetrias do triângulo equilátero e do quadrado. Além disso, dispomos da teoria elementar de Grupos, vista nos capítulos

iniciais para estudar melhor o *Grupo Diedral*. Sendo assim, veremos toda essa teoria sendo "aplicada" nos exemplos de *Grupos de Simetrias*.

1 Grupos

Neste capítulo, apresentaremos as definições de Grupos, Subgrupos e Grupos Cíclicos, algumas de suas propriedades e destacaremos exemplos.

1.1 Definição e Exemplos de Grupos

Definição 1.1.1: Seja A um conjunto não vazio. Uma operação binária $*$ é uma aplicação de $A \times A$ em A, que associa a cada par ordenado de elementos de A, algum elemento em A:

$$* : A \times A \to A$$

$$(a, b) \mapsto a * b.$$

Definição 1.1.2: Um grupo é um par ordenado $(G, *)$; em que G é um conjunto não vazio, onde está definida uma operação binária entre pares de elementos de G, denotada por:

$$* : G \times G \to G$$

$$(x, y) \ \mapsto x * y$$

Dizemos que $(G, *)$ é um grupo, se as seguintes condições são satisfeitas:

(i) A operação $*$ é associativa, ou seja, $x * (y * z) = (x * y) * z, \forall\ x, y, z \in G$.

(ii) Existe um elemento neutro (denotado por e) tal que $x * e = e * x = x, \forall\ x \in G$.

(iii) Existe um elemento inverso (denotado por x^{-1}) tal que $x * x^{-1} = x^{-1} * x = e, \forall\ x \in G$.

(iv) Um grupo $(G, *)$ é abeliano ou comutativo se: $x * y = y * x, \forall\ x, y \in G$.

Propriedades 1.1.3: Se $(G, *)$ é grupo, tem-se as seguintes propriedades:

(P_1) O elemento neutro é único.

(P_2) O elemento inverso de cada elemento de G é único.

(P_3) $(x^{-1})^{-1} = x, \forall\ x \in G$.

(P_4) $(x * y)^{-1} = y^{-1} * x^{-1}, \forall\ x, y \in G$.

Demonstração:

(P_1) Se e_1, e_2 são elementos neutros de G, logo $e_1 = e_1 * e_2 = e_2$.

(P_2) Sejam $x \in G$ e seus dois elementos inversos $x_1, x_2 \in G$ tais que $x * x_1 = x_1 * x = e$ e $x * x_2 = x_2 * x = e$. Seque que $x_1 = e * x_1 = x_2 * x * x_1 = x_2 * e = x_2$ e, portanto, o inverso é único.

(P_3) Queremos encontrar um inverso de x^{-1}. Como G é grupo, existe $y \in G$ tal que $y = (x^{-1})^{-1}$. Segue que $x^{-1} * y = e$, logo $x * x^{-1} * y = x * e \Rightarrow y = x$ e, portanto, $(x^{-1})^{-1} = x$.

(P_4) Sejam $x, y \in G$ e $z^{-1} = (x * y)^{-1} \in G$. Temos que $(x * y) * z^{-1} = e$, então $x^{-1} * (x * y) * z^{-1} = x^{-1} * e \Rightarrow y * z^{-1} = x^{-1} \Rightarrow y^{-1} * y * z^{-1} = y^{-1} * x^{-1}$. Daí, $z^{-1} = y^{-1} * x^{-1}$ e, portanto, $(x * y)^{-1} = y^{-1} * x^{-1}$. ∎

Observação 1.1.4: A operação do grupo pode ser definida por uma soma ou multiplicação usual, sendo representadas por $(G, +)$ grupo aditivo e $(G, \cdot)$ grupo multiplicativo, respectivamente. Temos outras operações como, a composição de funções, representada por $(G, \circ)$ e, operações não triviais que satisfazem as propriedades de Grupo. Se a operação estiver implícita, vamos nos referir ao grupo $(G, *)$ simplesmente por grupo G.

Exemplo 1.1.5: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ são grupos (aditivos) abelianos.

Exemplo 1.1.6: $\mathbb{C}$ é grupo abeliano com a soma usual.

Demonstração:

(i) Associativo: Sejam $x, y, z \in \mathbb{C}, \exists\ a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$ tais que $x = a_1 + b_1 i, y = a_2 + b_2 i, z = a_3 + b_3 i$. Segue que, $(x + y) + z = [(a_1 + b_1 i) + (a_2 + b_2 i)] + (a_3 + b_3 i) = [(a_1 + a_2) + (b_1 + b_2)i] + (a_3 + b_3 i) = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)i = (a_1 + b_1 i) + [(a_2 + a_3) + (b_2 + b_3)i] = x + (y + z)$.

(ii) Elemento neutro: Tomemos $x, e \in \mathbb{C}, \exists\ a_1, b_1, e_1, e_2 \in \mathbb{R}$ tais que $x = a_1 + b_1 i, e = e_1 + e_2 i$. Mostraremos que $\exists\ e \in \mathbb{C}$ tal que $x + e = e + x = x$. Se $x + e = x$, então $(a_1 + b_1 i) + (e_1 + e_2 i) = a_1 + b_1 i \Rightarrow (a_1 + e_1) + (b_1 + e_2)i = a_1 + b_1 i$. Logo, dispomos do

seguinte sistema:

$$\begin{cases} a_1 + e_1 = a_1 \quad (1) \\ b_1 + e_2 = b_1 \quad (2) \end{cases}$$

De (1) e (2), temos $e_1 = 0$ e $e_2 = 0 \Rightarrow e = e_1 + e_2 i = 0 + 0i \in \mathbb{C}$. Daí, a seguinte igualdade é válida: $e + x = x \Rightarrow (e_1 + e_2 i) + (a_1 + b_1 i) = a_1 + b_1 i$, pois $(0 + 0i) + (a_1 + b_1 i) = a_1 + b_1 i$.

(*iii*) Elemento inverso: Tomemos $x \in \mathbb{C}$ tal que $x = a_1 + b_1 i$, queremos encontrar $x^{-1} \in \mathbb{C}$, que satisfaça $x + x^{-1} = x^{-1} + x = e$. Daí, substituindo em $x + x^{-1} = e$, temos $(a_1 + b_1 i) + x^{-1} = 0 \Rightarrow x^{-1} = -a_1 - b_1 i$. E, retomando $x^{-1} + x = e$, percebemos que, de fato, $a_1 + b_1 i - a_1 - b_1 i = 0 + 0i$.

(*iv*) Comutativo: Sejam $x, y \in \mathbb{C}, \exists\ a_1, a_2, b_1, b_2 \in \mathbb{R}$ tais que $x = a_1 + b_1 i, y = a_2 + b_2 i$. Então, $x + y = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i = (a_2 + a_1) + (b_2 + b_1)i = (a_2 + b_2 i) + (a_1 + b_1 i) = y + x$. Como $(\mathbb{C}, +)$ satisfaz as propriedades acima, concluimos que $\mathbb{C}$ é grupo abeliano com a soma. ∎

Exemplo 1.1.7: $\mathbb{Q}^*$ e $\mathbb{R}^*$ são grupos abelianos com a multiplicação usual.

Exemplo 1.1.8: $\mathbb{C}$ é grupo abeliano com a multiplicação usual.

Demonstração:

(*i*) Associatividade: Sejam $x, y, z \in \mathbb{C}$ tais que $x = a_1 + b_1 i, y = a_2 + b_2 i, z = a_3 + b_3 i$, com $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$. Provaremos que $(x.y).z = x.(y.z)$.

(1) $(x.y).z = [(a_1 + b_1 i).(a_2 + b_2 i)].(a_3 + b_3 i) = (a_1 a_2 + a_1 b_2 i + a_2 b_1 i - b_1 b_2).(a_3 + b_3 i) = a_1 a_2 a_3 + a_1 a_3 b_2 i + a_2 a_3 b_1 i - a_3 b_1 b_2 + a_1 a_2 b_3 i - a_1 b_2 b_3 - b_1 b_2 b_3 i - a_2 b_1 b_3$.

(2) $x.(y.z) = (a_1 + b_1 i) + [(a_2 + b_2 i).(a_3 + b_3 i)] = (a_1 + b_1 i).(a_2 a_3 + a_2 b_3 i + a_3 b_2 i - b_2 b_3) = a_1 a_2 a_3 + a_1 a_2 b_3 i + a_1 a_3 b_2 i - a_1 b_2 b_3 + a_2 a_3 b_1 i - a_2 b_1 b_3 - a_3 b_1 b_2 - b_1 b_2 b_3 i$.

Como (1) e (2) são iguais, dizemos que vale a associatividade.

(*ii*) Elemento neutro: Sejam $x, e \in \mathbb{C}$ tais que $x = a_1 + b_1 i, e = e_1 + e_2 i$, com $a_1, b_1, e_1, e_2 \in \mathbb{R}$. Queremos encontrar $e \in \mathbb{C}$ tal que $x.e = e.x = x$. De $x.e = x$, temos $(a_1 + b_1 i).(e_1 + e_2 i) = a_1 + b_1 i \Rightarrow (a_1 e_1 - b_1 e_2) + (a_1 e_2 + b_1 e_1)i = a_1 + b_1 i$. Resultando no sistema:

$$\begin{cases} a_1 e_1 - b_1 e_2 = a_1 \quad (1) \\ a_1 e_2 + b_1 e_1 = b_1 \quad (2) \end{cases}$$

Multiplicamos (1) e (2) por a_1 e b_1, respectivamente:

$$\begin{cases} a_1^2 e_1 - a_1 b_1 e_2 = a_1^2 \\ a_1 b_1 e_2 + b_1^2 e_1 = b_1^2 \end{cases}$$

Somando ambas as equações, temos $a_1^2 e_1 + b_1^2 e_1 = a_1^2 + b_1^2 \Rightarrow e_1(a_1^2 + b_1^2) = a_1^2 + b_1^2$. Dividindo os membros da equação resultante por $a_1^2 + b_1^2$, com $a_1 \neq 0$ e $b_1 \neq 0$, obtemos $e_1 = 1$. E, substituindo em (1), segue que $a_1 - b_1 e_2 = a_1 \Rightarrow e_2 = 0$. Se $e = 1 + 0i \in \mathbb{C}$, então $(1 + 0i).(a_1 + b_1 i) = a_1 + b_1 i$.

(*iii*) Elemento inverso: Tomemos $x, x^{-1} \in \mathbb{C}, \exists\ a_1, b_1, x_1, x_2 \in \mathbb{R}$ tais que $x = a_1 + b_1 i, x^{-1} = x_1 + x_2 i$. Queremos encontrar $x^{-1} \in \mathbb{C}$ tal que $x.x^{-1} = x^{-1}.x = e$. Se $x.x^{-1} = e$, então $(a_1 + b_1 i).(x_1 + x_2 i) = (1 + 0i)$ e, portanto, $(a_1 x_1 - b_1 x_2) + (a_1 x_2 + b_1 x_1)i = 1 + 0i$. Construindo o sistema, temos:

$$\begin{cases} a_1 x_1 - b_1 x_2 = 1 \quad (1) \\ a_1 x_2 + b_1 x_1 = 0 \quad (2) \end{cases}$$

Multiplicamos (1) e (2) por a_1 e b_1, respectivamente:

$$\begin{cases} a_1^2 x_1 - a_1 b_1 x_2 = a_1 \\ a_1 b_1 x_2 + b_1^2 x_1 = 0 \end{cases}$$

Somando as equações, temos $a_1^2 x_1 + b_1^2 x_1 = a_1 \Rightarrow x_1 (a_1^2 + b_1^2) = a_1 \Rightarrow x_1 = \dfrac{a_1}{a_1^2 + b_1^2}$ com $a_1 \neq 0$ e $b_1 \neq 0$. Substituindo em (2), temos $a_1 x_2 + b_1 \left(\dfrac{a_1}{a_1^2 + b_1^2} \right) \Rightarrow x_2 = \dfrac{-b_1}{a_1^2 + b_1^2}$ com $a_1 \neq 0$ e $b_1 \neq 0$.

(*iv*) Comutativo: Sejam $x, y \in \mathbb{C}$ tais que $x = a_1 + b_1 i$ e $y = a_2 + b_2 i$. Segue que $x.y = (\mathrm{a}_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + a_2 b_1 i - b_1 b_2 = (a_2 + b_2 i)(a_1 + b_1 i) = y.x$. ∎

Definição 1.1.9: Seja $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, onde $\overline{a} \in \mathbb{Z}_m$ é dado por $\overline{a} = \{\overline{qm + a} \mid q, m \in \mathbb{Z}\ e\ m \geq 1\}$. O conjunto $\mathbb{Z}_m$ é denominado conjunto das classes de restos módulo m.

Exemplo 1.1.10: $(\mathbb{Z}_m, +)$ é grupo abeliano.

Demonstração:

(*i*) Fechado: Tomemos $\overline{x_1}, \overline{x_2} \in \mathbb{Z}_m$. Se $\overline{x_1} + \overline{x_2} = \overline{x_1 + x_2} < m$, então $\overline{x_1} + \overline{x_2} = \overline{x_1 + z_2} \in \mathbb{Z}_m$. Se $\overline{x_1} + \overline{x_2} = \overline{x_1 + x_2} > m$, $\exists\ q, r \in \mathbb{Z}$ tais que $x_1 + x_2 = qm + r$, para $0 \leq r < m$. Daí, $\overline{x_1 + x_2} = \overline{qm + r} = \overline{qm} + \overline{r} = \overline{r} \in \mathbb{Z}_m$.

(*ii*) Associativo: Sejam $\overline{x_1}, \overline{x_2}, \overline{x_3} \in \mathbb{Z}_m$ temos $(\overline{x_1} + \overline{x_2}) + \overline{x_3} = (\overline{x_1 + x_2}) + \overline{x_3} = \overline{x_1 + x_2 + x_3} = \overline{x_1} + (\overline{x_2 + x_3}) = \overline{x_1} + (\overline{x_2} + \overline{x_3})$.

(*iii*) Elemento neutro: $\forall\ \overline{x} \in \mathbb{Z}_m$, provaremos que $\exists\ \overline{e} \in \mathbb{Z}_m$ tal que $\overline{x} + \overline{e} = \overline{x + e} = \overline{e + x} = \overline{e} + \overline{x} = \overline{x}$. Se $\overline{x} + \overline{e} = \overline{x}$, então $\overline{e} = \overline{0} \in \mathbb{Z}_m$. Substituindo na segunda equação, temos $\overline{0} + \overline{x} = \overline{0 + x} = \overline{x}$.

(*iv*) Elemento inverso: $\forall\ \overline{x} \in \mathbb{Z}_m$, verificaremos que $\exists\ \overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x} = \overline{e}$. Segue que $\overline{x} + \overline{y} = \overline{0}$, assim $\overline{y} = -\overline{x} \in \mathbb{Z}_m$. Substituindo em $\overline{y} + \overline{x} = \overline{e}$, temos $-\overline{x} + \overline{x} = \overline{-x + x} = \overline{0}$.

(*v*) Comutativo: Sejam $\overline{x_1}, \overline{x_2} \in \mathbb{Z}_m$, note que $\overline{x_1} + \overline{x_2} = \overline{x_1 + x_2} = \overline{x_2 + x_1} = \overline{x_2} + \overline{x_1}$. ∎

Proposição 1.1.11: $(\mathbb{Z}_m^*, \cdot)$ é grupo se, e somente se, m é primo.

Demonstração:

($\Rightarrow$) Por hipótese, temos que $(\mathbb{Z}_m^*, \cdot)$ é grupo, logo a multiplicação está bem definida. Provaremos por absurdo, partindo da ideia que m é composto. Suponhamos que $\exists\ \overline{x}, \overline{y} \in \mathbb{Z}_m^*$ tais que $\overline{x}.\overline{y} = \overline{x.y} = \overline{m}$. Segue que $\overline{x.y} = \overline{m} = \overline{0}$, o que é um absurdo, pois $\overline{0} \notin \mathbb{Z}_m^*$.

($\Leftarrow$) Se m é primo, então $mdc\ (x, m) = 1$, para $x \in \mathbb{Z}_m^*$. Provaremos que $(\mathbb{Z}_m^*, \cdot)$ é grupo.

(*i*) Fechado: Sejam $\overline{x}, \overline{y} \in \mathbb{Z}_m^*$, temos $\overline{x}.\overline{y} = \overline{x.y} \neq m$ (pela hipótese) e, portanto, $\overline{x}.\overline{y} = \overline{x.y} \neq \overline{0} \in \mathbb{Z}_m^*$.

(*ii*) Vale a associatividade, basta tormarmos $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m^*$. Assim, temos $(\overline{x}.\overline{y}).\overline{z} = (\overline{x.y}).\overline{z} = \overline{x.y.z} = \overline{x}.(\overline{y.z}) = \overline{x}.(\overline{y}.\overline{z})$.

(*iii*) Elemento neutro: $\forall\ \overline{x} \in \mathbb{Z}_m^*, \exists\ \overline{e} \in \mathbb{Z}_m^*$ tal que $\overline{x}.\overline{e} = \overline{x.e} = \overline{e.x} = \overline{e}.\overline{x} = \overline{e}$. Se $\overline{x}.\overline{e} = \overline{x}$, então $\overline{e} = \overline{1} \in \mathbb{Z}_m^*$. Verificando na segunda equação, temos $\overline{1}.\overline{x} = \overline{1.x} = \overline{x}$.

(*iv*) Elemento inverso: Seja $\overline{x} \in \mathbb{Z}_m^*$, provaremos que existe um inverso $\overline{y} \in \mathbb{Z}_m^*$. Se m é primo, logo $mdc\ (x, m) = 1 \Rightarrow \exists\ a, b \in \mathbb{Z}_m^*$ tal que $\overline{ax + bm} = \overline{1}$. Então, $\overline{ax + bm} = \overline{1}$ $\Rightarrow \overline{ax} + \overline{bm} = \overline{1}$. Como $\overline{bm} = \overline{0}$, temos que $\overline{ax} = \overline{1}$ e, portanto, $\overline{a} = \overline{y}$. ∎

Exemplo 1.1.12: Seja $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$. Mostraremos que G é grupo abeliano com relação à composição de funções.

Demonstração:

(i) Fechado: Sejam $f(x) = a_1x + b_1$ e $g(x) = a_2x + b_2$. Segue que $f(x) + g(x) = (a_1x + b_1) + (a_2x + b_2) = a_1x + a_2x + b_1 + b_2 = (a_1 + a_2)x + (b_1 + b_2) \in G$.

(ii) Associativo: Tomemos $f(x) = a_1x + b_1, g(x) = a_2x + b_2$ e $h(x) = a_3x + b_3$.
(1) $f \circ (g \circ h) = f[g(a_3x + b_3)] = f[a_2(a_3x + b_3) + b_2] = f[a_2a_3x + a_2b_3 + b_2] = a_1(a_2a_3x + a_2b_3 + b_2) + b_1 = a_1a_2a_3x + a_1a_2b_3 + a_1b_2 + b_1$.
(2) $(f \circ g) \circ h = [f(a_2x + b_2)] \circ h = [a_1(a_2x + b_2) + b_1] \circ h = [a_1a_2x + a_1b_2 + b_1] \circ h = a_1a_2(a_3x + b_3) + a_1b_2 + b_1 = a_1a_2a_3x + a_1a_2b_3 + a_1b_2 + b_1$.

Como (1) = (2), vale a associatividade.

(iii) Elemento Neutro: Sejam $f, e \in G$ tais que $f(x) = ax + b, e(x) = e_1x + e_2$. Queremos encontrar $e(x) \in G$ tal que $(f \circ e)(x) = (e \circ f)(x) = f(x)$. Daí, $(f \circ e)(x) = f(e_1x+e_2) = a(e_1x+e_2)+b = ae_1x+(ae_2+b)$. Como $(f \circ e) = f(x)$, temos $ae_1x+(ae_2+b) = ax + b$. Assim, obtemos o seguinte sitema:

$$\begin{cases} ae_1 = a \\ ae_2 + b = b \end{cases}$$

Então, $e_1 = 1$ e $e_2 = 0$, com $a \neq 0$ e, portanto, $e(x) = x \in G$. Substituindo $e(x)$ na segunda equação, temos $(e \circ f)(x) = e(ax + b) = 1(ax + b) + 0 = ax + b = f(x)$.

(iv) Elemento inverso: Sejam $f, f^{-1} \in G$ tais que $f(x) = ax + b, f^{-1}(x) = a'x + b'$. Queremos encontrar $f^{-1}(x) \in G$ tal que $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = e(x)$. Se $aa'x + ab' + b = 1x + 0$, então

$$\begin{cases} aa' = 1 \\ ab' + b = 0 \end{cases}$$

Resolvendo o sistema, temos $a' = \frac{1}{a}, b' = \frac{-b}{a}$, logo $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a} \in G$. Substituindo em $(f^{-1} \circ f)(x) = e(x)$, temos $f^{-1}(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x = e(x)$.

(v) Comutativo: Tomemos $f, g \in G$ tais que $f(x) = ax + b$ e $g(x) = cx + d$. Como $(f \circ g)(x) = f(cx + d) = a(cx + d) + b = acx + (ad + b)$. E, $(g \circ f)(x) = g(ax + b) = c(ax + b) + d = cax + (cb + d)$. Temos que $(f \circ g)(x) \neq (g \circ f)(x)$. ∎

Exemplo 1.1.13: $(M_n(\mathbb{R}), +)$ é grupo abeliano.

Demonstração:

(i) Associativo: Sejam $A, B, C \in M_n(\mathbb{R})$, temos que $(A + B) + C = A + (B + C)$.

(ii) Elemento neutro: Verificaremos a existência de uma matriz $E \in M_n(\mathbb{R})$ tal

que $A + E = E + A = A$. Tomemos A e $E \in M_n(\mathbb{R})$ tais que $A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$ e $E = \begin{bmatrix} e_{11} & \dots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{n1} & \dots & e_{nn} \end{bmatrix}$. Segue que $A + E = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} e_{11} & \dots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{n1} & \dots & e_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} + e_{11} & \dots & a_{1n} + e_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} + e_{n1} & \dots & a_{nn} + e_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \Rightarrow E = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} \Rightarrow A + 0 = A.$

(*iii*) Elemento inverso: Queremos encontrar uma matriz $A^{-1} \in M_n(\mathbb{R})$ tal que $A + A^{-1} = A^{-1} + A = E$. Para isso, tomemos A e $A^{-1} \in M_n(\mathbb{R})$ tais que $A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$ e $A^{-1} = \begin{bmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{n1} & \dots & a'_{nn} \end{bmatrix}$. Segue que $A + A^{-1} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \dots & -a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} + a'_{11} & \dots & a_{1n} + a'_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} + a'_{n1} & \dots & a_{nn} + a_{nn'} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} \Rightarrow A^{-1} = \begin{bmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \dots & -a_{nn} \end{bmatrix} \Rightarrow A - A = E = 0.$

(*iv*) Comutativo: Tomemos $A, B \in M_n(\mathbb{R})$, temos $A + B = B + A$. ∎

Exemplo 1.1.14: $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid det\ M \neq 0\}$ é grupo com a multiplicação usal de matrizes.

Demonstração:

(*i*) Associativo: Sejam $A, B, C \in GL_n(\mathbb{R})$, então vale a igualdade $(AB)C = A(BC)$.

(*ii*) Elemento neutro: Seja $A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in GL_n(\mathbb{R})$. Nota-se que a ma-

triz $I_n = \begin{bmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{bmatrix}$ é o elemento neutro de $GL_n(\mathbb{R})$. Pois, $AI_n = I_nA = A$. Segue que

$$AI_n = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{bmatrix} = \begin{bmatrix} a_{11}.1 + ... + a_{1n}.0 + & \dots & a_{11}.0 + ... + a_{1n}.1 \\ \vdots & \ddots & \vdots \\ a_{n1}.1 + ... + a_{nn}.0 & \dots & a_{n1}.0 + ... + a_{nn}.1 \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} = A.$$

(*iii*) Elemento inverso: Verificaremos a existência de uma matriz A^{-1}, que satisfaça a igualdade $AA^{-1} = A^{-1}A = I_n$. Para isso, é sufuciente mostrar que $A^{-1} \in GL_n(\mathbb{R})$, ou seja, $det\ (A^{-1}) \neq 0$. Temos que $AA^{-1} = I_n$ (hipótese), logo $det\ (A).det\ (A^{-1}) = det\ (I_n)$. Sabemos que $det\ (I_n) = 1$, então $det\ (A^{-1}) = \frac{1}{det\ (A)}$. Como $A \in GL_n(\mathbb{R})$, temos $det\ A \neq 0$ e, portanto, $det\ (A^{-1}) \neq 0 \in GL_n(\mathbb{R})$.

(*iii*) Comutativo: Mostraremos que nem sempre $GL_n(\mathbb{R})$ com a multiplicação usual será comutativa. Podemos observar o contraexemplo a seguir:

Sejam $A = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \in M_2(\mathbb{R})$ e $B = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \in M_2(\mathbb{R})$.

$$AB = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 10 \\ 10 & 20 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 9 \\ 14 & 18 \end{bmatrix}$$

Como $AB \neq BA$, $GL_n(\mathbb{R})$ não comuta. ∎

Exemplo 1.1.15: Mostre que $\mathbb{Z} \times \mathbb{Z}$ munido com a operação $\triangle$ definida por $(a, b)\ \triangle\ (c, d) = (a + c, b + d)$ é grupo abeliano.

Demonstração:

(*i*) Associativo: Sejam $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{Z} \times \mathbb{Z}$.

(1) $[(a, b)\ \triangle\ (c, d)]\ \triangle\ (e, f) = [(x_1, y_1)\ \triangle\ (x_2, y_2)]\ \triangle\ (x_3, y_3) = (x_1 + x_2, y_1 + y_2)\ \triangle\ (x_3, y_3) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$.

(2) $(a, b)\ \triangle\ [(c, d)\ \triangle\ (e, f)] = (x_1, y_1)\ \triangle\ [(x_2, y_2)\ \triangle\ (x_3, y_3)] = (x_1, y_1)\ \triangle\ (x_2 +$

$x_3, y_2 + y_3) = (x_1 + x_2 + x_3, y_1 + y_2 + y_3)$

Como (1) = (2), vale a associatividade.

(ii) Elemento neutro: Tomemos $(x_1, y_1) \in \mathbb{Z}\times\mathbb{Z}$, provaremos que $\exists\ (e_1, e_2) \in \mathbb{Z}\times\mathbb{Z}$ tal que $(x_1, y_1) \triangle (e_1, e_2) = (e_1, e_2) \triangle (x_1, y_1) = (x_1, y_1)$. Segue que $(x_1, y_1) \triangle (e_1, e_2) = (x_1, y_1)$, resulta no sistema:

$$\begin{cases} x_1 + e_1 = x_1 \quad (1) \\ y_1 + e_2 = e_1 \quad (2) \end{cases}$$

Logo, $(e_1, e_2) = (0, 0) \in \mathbb{Z} \times \mathbb{Z}$. Verificando o resultado na segunda equação, temos $(e_1, e_2) \triangle (x_1, y_1) = (0, 0) \triangle (x_1, y_1) = (0 + x_1, 0 + y_1) = (x_1, y_1)$.

(iii) Elemento inverso: Seja $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$, mostraremos que $\exists\ (x_1', y_1') \in \mathbb{Z} \times \mathbb{Z}$ tal que $(x_1, y_1) \triangle (x_1', y_1') = (x_1', y_1') \triangle (x_1, y_1) = (e_1, e_2)$. Segue que $(x_1, y_1) \triangle (x_1', y_1') = (e_1, e_2) \Rightarrow (x_1 + x_1', y_1 + y_1') = (0, 0)$. Resultando em:

$$\begin{cases} x_1 + x_1' = 0 \quad (1) \\ y_1 + y_1' = 0 \quad (2) \end{cases}$$

Assim, $(x_1', y_1') = (-x_1, -y_1) \in \mathbb{Z} \times \mathbb{Z}$. Substituindo em $(x_1', y_1') \triangle (x_1, y_1)$, temos $(-x_1, -y_1) \triangle (x_1, y_1) = (-x_1 + x_1, -y_1 + y_1) = (0, 0)$.

(iv) Comutativa: Sejam $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Segue que $(x_1, y_1) \triangle (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) \triangle (x_1, y_1)$. ∎

1.2 Subgrupos

Definição 1.2.1: Seja $(G, *)$ um grupo e H um subconjunto não vazio de G. Diz-se que H é um subgrupo de G se H for grupo com a operação de G. Isto é, H é subgrupo de G (denotado por $H < G$), quando satisfaz as seguintes condições:

(i) $x_1 * x_2 \in H, \forall\ x_1, x_2 \in H$.

(ii) $x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3, \forall\ x_1, x_2, x_3 \in H$.

(iii) $\exists\ e_H \in H$ tal que $e_H * x = x * e_H = x, \forall\ x \in H$.

(iv) $\exists\ k \in H$ tal que $k * x = x * k = e_H, \forall\ x \in H$.

Observação 1.2.2: Seja H um subgrupo de G, temos:

1) O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G.

Prova: Tomemos $x \in H \subseteq G$ e $e_H \in H$, logo $x * e_H = e_H * x = x$. Segue que $x * e_H = x \Rightarrow x^{-1} * x * e_H = x^{-1} * x$. Como $x^{-1} * x = e$, obtemos $e_H = e$. ∎

2) Seja $x \in H$, seu inverso em H é necessariamente igual ao inverso de x em G.

Prova: Tomemos $x \in H \subseteq G$ e $k \in H$ tal que $k * x = x * k = e_H$. Como $e_H = e$, então $k * x = x * k = e$ e, portanto, k é inverso de x em G. ∎

Exemplo 1.2.3: Mostraremos que o conjunto H das matrizes do tipo $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ com $a, b \in \mathbb{R}$ e a e b não nulos simultaneamente, constitui um subgrupo do grupo $GL_2(\mathbb{R})$.

Demonstração:

(i) Fechado: Sejam $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in H$ e $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in H$. Segue que $AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & bc + ad \\ -(bc + ad) & ac - bd \end{bmatrix} \in H$.

(ii) Vale a associatividade: Sejam $A, B, C \in H$, temos que $(AB)C = A(BC)$.

(iii) Elemento neutro: A matriz I_n satisfaz a condição imposta pelo exercício. E, como já sabemos $AI_n = I_nA = A$, para $A \in H$.

(iv) Elemento inverso: Seja $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in H$, mostraremos a existência de uma matriz $A^{-1} \in H$ tal que $AA^{-1} = A^{-1}A = I_n$. Como $det\ (A) \neq 0$, então existe A^{-1} tal que $A^{-1} = \dfrac{1}{det\ (A)} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \Rightarrow A^{-1} = \dfrac{1}{a^2 + b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in H$. ∎

Proposição 1.2.4: Seja G um grupo e H um subconjunto não vazio de G. Assim, H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas:

(i) $x_1 * x_2 \in H, \forall\ x_1, x_2 \in H$.

(ii) $x^{-1} \in H, \forall\ x \in H$.

Demonstração:

$(\Rightarrow)$ Por hipótese, temos que H é subgrupo de G, daí $x_1 * x_2 \in H$, $\forall\ x_1, x_2 \in H$. Além disso, pela propriedade (iii) de subgrupo, temos que $\exists\ k \in H$ tal que $k * x = x * k = e, \forall\ x \in H$; como já observamos $k = x^{-1} \in H$, pois ao tomarmos $x \in H$, o seu inverso em

H é necessariamente igual ao inverso de x em G.

($\Leftarrow$) Sabemos que $x_1 * x_2 \in H, \forall\ x_1, x_2 \in H$ (por hipótese), isto é, H é fechado para a operação de G; o que nos mostra que a operação de G induz uma operação em H, e a mesma será associativa, já que a operação é associativa em G. Além do mais, temos que $x^{-1} \in H, \forall\ x \in H$ e, $e = x^{-1} * x$, segue que $e \in H$. ∎

Exemplo 1.2.5 Consideremos o grupo aditivo $M_2(\mathbb{R})$. Mostraremos pela proposição 1.2.4, que o conjunto H das matrizes $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, com $a + d = 0$, é subgrupo de $M_2(\mathbb{R})$.

Demonstração:

(i) Sejam as matrizes $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in H$ e $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \in H$. Como $a_{11} + a_{22} = 0$ e $b_{11} + b_{22} = 0$, temos respectivamente: $a_{22} = -a_{11}$ e $b_{22} = -b_{11}$.

Logo, $A + B = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & -b_{11} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & -(a_{11} + b_{11}) \end{bmatrix} \in H.$

(ii) Seja $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in H$. Como $A^{-1} = -A \in H$ e $-a_{22} = a_{11}$, temos $A^{-1} = \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \in H.$ ∎

Exemplo 1.2.6: Seja o grupo $G = (\mathbb{Z}, +)$, verificaremos se $H = (2\mathbb{Z}, +)$ é subgrupo de G.

Demonstração:

(i) Sejam $x, y \in H$ tais que $x = 2n$ e $y = 2m$, com $n, m \in \mathbb{Z}$. Daí, $x + y = 2n + 2m = 2(n + m) \in H$.

(ii) Tomemos $x \in H$ tal que $x = 2n$, com $n \in \mathbb{Z}$. Queremos provar que $x^{-1} \in H$. De fato, $x^{-1} = -2n \in H$ e, portanto, H é subgrupo de G. De maneira mais geral, temos $(n\mathbb{Z}, +)$ com $n \in \mathbb{Z}$ é subgrupo de $(\mathbb{Z}, +)$. ∎

Exemplo 1.2.7: Se H_1 e H_2 são subgrupos de G, então $H_1 \cap H_2$ é um subgrupo de G.

Demonstração:

(i) Por hipótese, temos que H_1 e H_2 são subgrupos de G. Tomemos $x, y \in H_1 \cap H_2$, logo $x, y \in H_1$ e $x, y \in H_2 \Rightarrow x * y \in H_1$ e $x * y \in H_2$. Assim, temos que $x * y \in H_1 \cap H_2$.

(ii) Se $x \in H_1$ e $x \in H_2$, então $\exists\ x^{-1} \in H_1$ e $x^{-1} \in H_2$. Como $x \in H_1 \cap H_2$, temos que $x^{-1} \in H_1 \cap H_2$. ∎

1.3 Grupos Cíclicos

Definição 1.3.1: Sejam a e x um número real, em que a é a base e x é o expoente. Uma potência pode ser escrita na forma a^x, isto é, a é multiplicado por ele mesmo x vezes.

Definição 1.3.2: Seja G um grupo multiplicativo. Diz-se que G é cíclico se existir um elemento $a \in G$ tal que todo elemento x de G pode ser escrito na forma a^m (potência m-ésima de a), para algum inteiro m. Logo, se um elemento $a \in G$ satisfaz a essa condição é chamado de gerador de G, denotado por $G = [a] = \{a^m \mid m \in \mathbb{Z}\}$.

Observação 1.3.3:

- Se $m \geq 0$, tem-se $a^0 = e$ (elemento neutro de G) e $a^m = a^{m-1}.a$; essa última definição pode ser interpretada da seguinte forma: $a^1 = a^{1-1}.a = a^0.a = e.a = a; a^2 = a^{2-1}.a = a^1.a = a.a$; etc.
- Se $m < 0$, tem-se $a^m = a^{(-m)(-1)} = (a^{-m})^{-1}$.

Proposição 1.3.4: Seja G um grupo multiplicativo. Se $a \in G$ e $m, n \in \mathbb{Z}$, segue que:

(i) $a^m a^n = a^{m+n}$;

(ii) $(a^m)^n = a^{mn}$.

Demonstração:

Demonstraremos apenas a proposição (i). A demonstração da proposição (ii) encontra-se disponível em refência [3] (p. 176). Desta forma, provaremos por indução sobre n, o caso particular $n \geq 0$ e $m + r \geq 0$.

(1) Para $n = 0$, temos que $a^m.a^n = a^m.a^0 = a^m.e = a^m = a^{m+0} = a^{m+n}$. Logo, a proposição é válida para $n = 0$.

(2) Suponhamos que a seguinte proposição seja verdadeira: $a^{m+r} = a^m.a^r$, para $n = r$. Provaremos o caso em que $n = r + 1$. Sejam $r \geq 0$ e $m + r \geq 0$, para qualquer inteiro m, temos $a^{m+n} = a^m.a^{r+1} = a^m.a^{(r+1)-1}.a = a^m.a^r.a = a^{m+r}.a = a^{(m+r)+1}$. ∎

Proposição 1.3.5:

(i) O subconjunto $[a]$ é subgrupo de G;

(ii) Se H é um subgrupo de G ao qual a pertence, então $[a] \subset H$.

Demonstração:

(i) Sabemos que $[a] \neq \emptyset$, pois $e \in [a]$, em que $e = a^0$. Além disso, provaremos que a operação está bem definida e, que o inverso pertence a $[a]$. Tomemos $x = a^m$ e $y = a^n$, com $m, n \in \mathbb{Z}$. Daí, $xy = a^m a^n = a^{m+n} \in H$. Observe que o inverso está em $[a]$, pois tomando $a^m \in [a]$, temos que $\exists\ a^{-1}$ tal que $a^{-m} = a^{-1} \in [a]$. Assim, temos que $a^m a^{-1} = 1$ $\Rightarrow a^{-m}a^m a^{-1} = a^{-m} \Rightarrow a^{-m+m}a^{-1} = a^{-m} \Rightarrow a^0 a^{-1} = a^{-m} \Rightarrow a^{-1} = a^{-m} \in [a]$.

(ii) Por hipótese, temos que $a \in H$. Daí, $a^m \in H$ e, portanto, $[a] \subset H$. ∎

Proposição 1.3.6: Todo subgrupo de um grupo cíclico também é cíclico.

Demonstração:

Seja $(G, \cdot)$ um grupo cíclico e H um subconjunto de G. Se H é um subgrupo do grupo cíclico $G = [a]$, então todo elemento de H é da forma a^m, para $m \in \mathbb{Z}$. Supondo que $H = \{a^0\} = e$, então H é gerado por e. Assim, qualquer potência de e será igual a ele mesmo e, portanto, H é cíclico. Agora para o caso de $H \neq \{e\}$, então H inclui um elemento a^m, com $m \neq 0$. Daí, podemos observar os casos a seguir: Se $m > 0 \Rightarrow a^m \in H$; Se $m < 0 \Rightarrow (a^m)^{-1} = a^{-m} \in H$. Logo, existe um elemento $b = a^h \in H$. E nesse caso, h é o menor inteiro extritamente positivo. Provaremos que $b = a^h$ gera H. Para isso, tomemos $x = a^n \in H$. Usando Algoritmo de Euclides, podemos tomar n como dividendo e h como divisor, daí $\exists\ q, r \in \mathbb{N}$ tais que $n = hq + r$, com $0 \leq r < h$.

Segue que $x = a^n = a^{hq+r} = a^{hq}a^r = (a^h)^q a^r = b^q a^r$. Observe que, $x = b^q a^r$ $\Rightarrow x(a^r)^{-1} = b^q a^r (a^r)^{-1} \Rightarrow x(a^r)^{-1} = b^q \Rightarrow x^{-1}x(a^r)^{-1} = x^{-1}b^q \Rightarrow (a^r)^{-1} = x^{-1}b^q \Rightarrow$ $((a^r)^{-1})^{-1} = (x^{-1}b^q)^{-1} \Rightarrow a^r = b^{-q}x$. Logo, $a^r \in H$, pois $x \in H$ e, como $b \in H \Rightarrow$

$b^{-q} \in H$. Se $r \geq 0$, temos que:
(1) Se $r > 0$, então existiria um elemento em H com expoente estritamente positivo e menor que h, o que contradiz a hipótese (pois h é o menor);
(2) Se $r = 0 \Rightarrow x = a^n = a^{hq} = (a^h)^q = b^q$, assim $x \in [b] = [a^h]$. Isso significa que $H \subset [b]$. Por outro lado, se $b \in H$, então as potências de b pertencem a H, daí $[b] \subset H$ e, portanto $H = [b]$. ∎

Definição 1.3.7: Seja G um grupo aditivo. Se $a \in G$ e tomando $x \in G$ escrito na forma $m.a$ (múltiplo m-ésimo de a), para algum inteiro m, então G é grupo cíclico. Diz-se a é um gerador de G, se existir $a \in G$ tal que $G = [a] = \{m.a \mid m \in \mathbb{Z}\}$.

Observação 1.3.8:

- Se $m \geq 0$, então $0.a = e$ (elemento neutro de G) e $m.a = (m-1).a + a$, se $m \geq 1$.
- Se $m < 0$, tem-se $m.a = -[(-m).a]$.

Exemplo 1.3.9: Tomemos o grupo multiplicativo $\mathbb{Z}_7^*$ das classes de resto módulo 7 e, seja $\overline{a} = \overline{3}$.

Segue que $\overline{3}^0 = \overline{1},\ \overline{3}^1 = \overline{3},\ \overline{3}^2 = \overline{2},\ \overline{3}^3 = \overline{6},\ \overline{3}^4 = \overline{4},\ \overline{3}^5 = \overline{5},\ \overline{3}^6 = \overline{1}, \ldots$
daí, $[\ \overline{3}\ ] = \{\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\} = \mathbb{Z}_7^*$.

Exemplo 1.3.10: Sejam $G = \{\ 1,\ -1,\ i,\ -i\}$ com a multiplicação usual e $a = i$.

Temos que $i^0 = 1,\ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1, \ldots$ e, portanto, $[\ i\ ] = \{\ 1,\ -1,\ i,\ -i\} = G$.

Exemplo 1.3.11: Sejam $(\mathbb{Z}, +)$ e $a = 1$, temos $[\ 1\ ] = \mathbb{Z}$.

De fato, $\forall\ m \in \mathbb{Z} \Rightarrow 1.m = \{\ \ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\ \} = \mathbb{Z}$.

Observe que um grupo cíclico pode possuir mais de um gerador. Retomando os exemplos anteriores (respectivamente), temos que:

Exemplo 1.3.12: Seja $\overline{a} = \overline{5}$, temos $\overline{5}^0 = \overline{1},\ \overline{5}^1 = \overline{5},\ \overline{5}^2 = \overline{4},\ \overline{5}^3 = \overline{6},\ \overline{5}^4 = \overline{2},\ \overline{5}^5 = \overline{3},\ \overline{5}^6 = \overline{1},\ \ldots$ daí, $[\ \overline{5}\ ] = \{\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}, \overline{6}\} = \mathbb{Z}_7^*$.

Exemplo 1.3.13: Tomemos $a = -i$, assim $(-i)^0 = -1,\ (-i)^1 = -i,\ (-i)^2 = 1,\ (-i)^3 = i \ldots$ e, portanto, $[\ -i\ ]$ também é gerador de G.

Exemplo 1.3.14: Seja $a = -1$, temos $\mathbb{Z} = \{(-1).m \mid m \in \mathbb{Z}\}$.

2 Classes Laterais e Conjugadas

Neste capítulo, abordaremos os conceitos de classes laterias à esquerda e à direita. Posteriormente, definiremos Subgrupos Normais a partir desses conceitos. Além do mais, apresentaremos o Teorema de Lagrange e definiremos Classes Conjugadas.

2.1 Classes Laterais

Proposição 2.1.1: Sejam G um grupo, H um subgrupo de G e $x, y \in H$. Sobre G, a relação R definida por:

$$yRx \Leftrightarrow x^{-1}y \in H$$

é uma relação de equivalência.

Demonstração:

(i) Reflexiva: Seja $x \in G, \exists\ x^{-1} \in G$ tal que $x^{-1}x = e$. Como $e \in H$, temos que xRx.

(ii) Simétrica: Tomemos $x, y \in G$. Provaremos que, se yRx, então xRy. Temos $yRx \Leftrightarrow x^{-1}y \in H$, então $(x^{-1}y)^{-1} = y^{-1}x \in H$ e, portanto, xRy.

(iii) Transitiva: Sejam $x, y, z \in G$. Provaremos que, se yRx e xRz, então yRz. Por hipótese, temos que $yRx \Leftrightarrow x^{-1}y \in H$ e $xRz \Leftrightarrow z^{-1}x \in H$. Logo, $(z^{-1}x)(x^{-1}y) \in H$, então $z^{-1}y \in H$ e, portanto, yRz. ∎

Observação 2.1.2:

1) De maneira análoga, se G é um grupo e H um subgrupo de G, a relação $xR^*y \Leftrightarrow yx^{-1} \in H$ também é uma relação de equivalência.

2) Se $yRx \Leftrightarrow x^{-1}y \in H$, então $\exists\ h \in H$ tal que $x^{-1}y = h$ e, portanto, $y = xh$. Pois, tomando $y = xh$ e, substituindo em $x^{-1}y \Rightarrow x^{-1}xh = eh = h \Leftrightarrow y \in xH = \{xh \mid h \in H\}$. Logo, a classe de equivalência de $x \in G$, definida pela relação R é $\{y \in G\ |yRx\} = xH$. Quando a relação é $yR^*x \Leftrightarrow yx^{-1}$, a classe de equivalência de $y \in G$ é $\{y \mid yR^*x \in H\} = Hx$.

Definição 2.1.3: Sejam $(G, \cdot)$ um grupo e H um subgrupo. A classe de equivalência

$xH = \{xh \mid h \in H\}$ (respectivamente $Hx = \{hx \mid h \in H\}$) é chamada classe lateral de x à esquerda (respectivamete à direita) de H em G.

Definição 2.1.4: Sejam $(G, +)$ um grupo e H um subgrupo. A classe de equivalência $x + H = \{x + h \mid h \in H\}$ (respectivamente $H + x = \{h + x \mid h \in H\}$) é chamada classe lateral de x à esquerda (respectivamete à direita) de H em G.

Exemplo 2.1.5: Seja $H = [a]$ um subgrupo de $G = GL_2(\mathbb{R})$, onde $a = \begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix}$ e, seja $x = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$. Calcule as todas as classes laterais em relação ao subgrupo de G.

Sabemos que G é grupo multiplicativo, e que o subgrupo H constitui-se de potências tais que $[a] = \{a^m \mid m \in \mathbb{Z}\}$.

Então, $a^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e$; $\mathrm{a}^1 = \begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = a$; $a^2 = a.a = \begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} =$

$= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$; $\mathrm{a}^3 = a^2a = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -\frac{1}{2} & 0 \end{bmatrix}$; $a^4 = a^3a =$

$= \begin{bmatrix} 0 & 2 \\ -\frac{1}{2} & 0 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Segue que $H = \{e,\ a,\ a^2,\ a^3\}$.

$$xH = \{x,\ xa,\ xa^2,\ xa^3\} = \left\{ \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & -2 \\ \frac{3}{2} & 0 \end{bmatrix}, \begin{bmatrix} -1 & -2 \\ 0 & -3 \end{bmatrix}, \begin{bmatrix} -1 & 2 \\ -\frac{3}{2} & -1 \end{bmatrix} \right\}.$$

$$Hx = \{x,\ ax,\ a^2x\ a^3x\} = \left\{ \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & -6 \\ \frac{1}{2} & 1 \end{bmatrix}, \begin{bmatrix} -1 & -2 \\ 0 & -3 \end{bmatrix}, \begin{bmatrix} 0 & 6 \\ -\frac{1}{2} & -1 \end{bmatrix} \right\}.$$

Exemplo 2.1.6: Sejam $G = (\mathbb{Z}_{12}, +)$ e $H = \{\overline{0}, \overline{4}, \overline{8}\}$ um subgrupo de G. Calcule as classes laterais $x + H$ e $H + x, \forall\ x \in G$.

(1) As classes laterais à esquerda são:

$\overline{0} + H = \{\overline{0} + \overline{0}, \overline{0} + \overline{4}, \overline{0} + \overline{8}\} = \{\overline{0}, \overline{4}, \overline{8}\}$

$\overline{1} + H = \{\overline{1} + \overline{0}, \overline{1} + \overline{4}, \overline{1} + \overline{8}\} = \{\overline{1}, \overline{5}, \overline{9}\}$

$$\overline{2}+H=\{\overline{2}+\overline{0},\overline{2}+\overline{4},\overline{2}+\overline{8}\}=\{\overline{2},\overline{6},\overline{10}\}$$

$$\overline{3}+H=\{\overline{3}+\overline{0},\overline{3}+\overline{4},\overline{3}+\overline{8}\}=\{\overline{3},\overline{7},\overline{11}\}$$

$$\overline{4}+H=\{\overline{4}+\overline{0},\overline{4}+\overline{4},\overline{4}+\overline{8}\}=\{\overline{4},\overline{8},\overline{0}\}$$

$$\overline{5}+H=\{\overline{5}+\overline{0},\overline{5}+\overline{4},\overline{5}+\overline{8}\}=\{\overline{5},\overline{9},\overline{1}\}$$

$$\overline{6}+H=\{\overline{6}+\overline{0},\overline{6}+\overline{4},\overline{6}+\overline{8}\}=\{\overline{6},\overline{10},\overline{2}\}$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

(2) As classes laterais à direita são:

$$H+\overline{0}=\{\overline{0}+\overline{0},\overline{4}+\overline{0},\overline{8}+\overline{0}\ =\{\overline{0},\overline{4},\overline{8}\}$$

$$H+\overline{1}=\{\overline{0}+\overline{1},\overline{4}+\overline{1},\overline{8}+\overline{1}\}=\{\overline{1},\overline{5},\overline{9}\}$$

$$H+\overline{2}=\{\overline{0}+\overline{2},\overline{4}+\overline{2},\overline{8}+\overline{2}\}=\{\overline{2},\overline{6},\overline{10}\}$$

$$H+\overline{3}=\{\overline{0}+\overline{3},\overline{4}+\overline{3},\overline{8+\overline{3}}\}=\{\overline{3},\overline{7},\overline{11}\}$$

$$H+\overline{4}=\{\overline{0}+\overline{4},\overline{4}+\overline{4},\overline{8}+\overline{4}\}=\{\overline{4},\overline{8},\overline{0}\}$$

$$H+\overline{5}=\{\overline{0}+\overline{5},\overline{4}+\overline{5},\overline{8}+\overline{5}\}=\{\overline{5},\overline{9},\overline{1}\}$$

$$H+\overline{6}=\{\overline{0}+\overline{6},\overline{4}+\overline{6},\overline{8}+\overline{6}\}=\{\overline{6},\overline{10},\overline{2}\}$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

Observe que as classes laterais à direita (respectivamente à esquerda) repetem a partir de $\overline{6}+H$ (respectivamente $H+\overline{6}$).

2.2 Subgrupos Normais

Definição 2.2.1: Sejam G um grupo e H um subgrupo de G. Diz-se que H é subgrupo normal (denotado por $H \triangleleft G$) se, $\forall\ x \in G$, se verifica a igualdade $xH = Hx$ (respectivamente $x + H = H + x$).

Observação 2.2.2: O número de classes laterias à esquerda de H é igual ao número de classes laterais à direita de H.

Proposição 2.2.3: Sejam $(G, \cdot)$ um grupo e H um subgrupo normal de G. Então, $(xH)(yH) = (xy)H$, $\forall\ x, y \in G$.

Demonstração:

Verificaremos se uma operação em G induz uma operação sobre o conjunto de classes laterais à esquerda de H em G. Desta forma, faremos a demonstração em duas etapas:

(i) Provaremos que $(xH)(yH) \subset (xy)H$.

Seja $x' \in (xH)(yH)$. Assim, $\exists\ h_1, h_2 \in H$ tal que $x' = (xh_1)(yh_2) = x(h_1y)h_2$. Sabemos que, $Hy = yH$ (por hipótese) e, além disso, temos que $h_1y \in Hy$. Então, $\exists\ h_3 \in H$ tal que $h_1y = yh_3$. Assim, $x' = x(h_1y)h_2 = x(yh_3)h_2 = (xy)\overbrace{h_3h_2}^{\in H}$ e, portanto, $x' \in (xy)H \Rightarrow (xH)(yH) \subset (xy)H$.

(ii) Provaremos que $(xy)H \subset (xH)(yH)$. Sejam $x' \in (xy)H$ e $h \in H$, logo $x' = xyh$. Tomemos $e \in H$ tal que $x' = \overbrace{(xe)}^{\in xH}\overbrace{(yh)}^{\in yH}$, assim $x' \in (xH)(yH) \Rightarrow (xy)H \subset (xH)(yH)$.

De (i) e (ii), segue que $(xH)(yH) = (xy)H$. ∎

Exemplo 2.2.4: Seja $(G, \cdot)$ tal que $G = \{-1, 1, -i, i\}$ e seu subgrupo $H = \{-1, 1\}$.

$(-1).H = \{(-1).1, (-1).(-1)\} = \{-1, 1\} = H.(-1)$

$1.H = \{1.(-1), 1.1\} = 1, -1\} = H.1$

$(-i).H = \{(-i).(-1), (-i).1\} = \{-i, i\} = H.(-i)$

$i.H = \{i.1, i.(-1)\} = \{i, -i\} = H.i$

Exemplo 2.2.5: Tomemos $(\mathbb{Z}_6, +)$ um grupo e $H = \{0, 3\}$ um subgrupo de G.

$\overline{0} + H = \{\overline{0} + \overline{0}, \overline{0} + \overline{3}\} = \{\overline{0}, \overline{3}\} = H + \overline{0}$

$\overline{1} + H = \{\overline{1} + \overline{0}, \overline{1} + \overline{3}\} = \{\overline{1}, \overline{4}\} = H + \overline{1}$

$\overline{2} + H = \{\overline{2} + \overline{0}, \overline{2} + \overline{3}\} = \{\overline{2}, \overline{5}\} = H + \overline{2}$

Observação 2.2.6: Os grupos apresentados nos exemplos são abelianos, por isso H é subgrupo normal. No entanto, temos subgrupos normais de grupos não abelinos, como veremos nos exemplos de D_n no capítulo 4.

2.3 Teorema de Lagrange

Definição 2.3.1: A cardinalidade do conjunto de classes laterais à esquerda é o índice de H em G, denotado por $(G : H)$.

Exemplo 2.3.2: Sejam o grupo $(\mathbb{Z}_6, +)$ e seu subgrupo $H = \{\overline{0}, \overline{2}, \overline{4}\}$. As classes laterais de H em G à esquerda são:

$$\overline{0} + H = \{\overline{0}, \overline{2}, \overline{4}\} \; e \; \overline{1} + H = \{\overline{1}, \overline{3}, \overline{5}\}.$$

Lembrando que as demais classes laterais coincidem com uma dessas duas. Portanto, $(\mathbb{Z}_6 : H) = \{\overline{0} + H, \overline{1} + H\} = 2$.

Teorema 2.3.3: (Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então, $o(G) = o(H)(G : H)$ e, portanto, a ordem e o índice de H (denotado por $o(H)$) dividem a ordem de G.

A demonstração desse teorema encontra-se disponível em referência [3] (p. 189).

Exemplo 2.3.4: Tomemos G um grupo finito, H um subgrupo de G e K um subgrupo de H. Provaremos que $(G : K) = (G : H)(H : K)$.

Demonstração:

Note que, se H é subgrupo de G, então (pelo Teorema de Lagrange) $o(G) = o(H)(G : H)$. Assim, de forma análoga, temos que $o(H) = o(K)(H : K)$, pois K é subgrupo de H; e, $o(G) = o(K)(G : K)$, porque K é subgrupo de G. Desta forma, tomaremos $o(G)$ (terceira equação) e $o(H)$, em seguida, substituiremos em $o(G) = o(H)(G : H)$. Assim, $o(K)(G : K) = (G : H)o(K)(H : K) \Rightarrow (G : K) = (G : H)(H : K)$. ∎

2.4 Classes Conjugadas

Definição 2.4.1: Se G é um grupo, então uma relação R em G é difinida por:

$$x, y \in G, \; yRx \Leftrightarrow \exists \; g \in G \; tal \; que \; x = g^{-1}yg.$$

Proposição 2.4.2: Seja G um grupo. Sobre G, a relação R define uma relação de equivalência.

Demonstração:

(i) Reflexiva: Se xRx, então $x = g^{-1}xg$. Seja $g = e$, temos $x = e^{-1}xe$.

(ii) Simétrica: Se yRx, então $xRy, \forall\ x, y \in G$.

Se yRx, então $x = g^{-1}yg$. Segue que $gx = gg^{-1}yg \Rightarrow gx = yg \Rightarrow gxg^{-1} = y$. Agora, tomemos $g = g_1^{-1}$ e $g^{-1} = g_1$, logo $y = g_1^{-1}xg_1$.

(iii) Transitiva: Se yRx e xRz, então yRz, $\forall\ x, y, z \in G$.

Se $yRx \Rightarrow x = gyg^{-1}$ e $xRz \Rightarrow z = hxh^{-1}$, sendo $g, h \in G$. Substituindo x em $z = hxh^{-1}$, temos $z = hgyg^{-1}h^{-1} \Rightarrow z = (hg)y(g^{-1}h^{-1})$. Por fim, tome $hg = g_1^{-1}$ e $g^{-1}h^{-1} = g_1$, logo $z = g_1^{-1}yg_1$. ∎

Definição 2.4.3: A classe $\overline{x} = \{y : xRy\} = \{x^g : g \in G\}$ é chamada classe de conjugação (em G) determinada pelo elemento $x \in G$ (denotada por C_x).

Exemplo 2.4.4: Seja $(G, *)$ um grupo, então $C_e = \{e\}$.

Exemplo 2.4.5: Seja $(G, *)$ um grupo abeliano, logo $C_x = \{x\}$. De fato:

$$C_x = \{y \in G, y = g^{-1} * x * g,\ com\ g \in G\}$$

$$C_x = \{y \in G, y = g^{-1} * g * x,\ com\ g \in G\}$$

$$C_x = \{y \in G, y = e * x,\ com\ g \in G\} = \{x\}.$$

Observação 2.4.6: Veremos um exemplo de classes conjugadas em grupos não abelinos no capítulo 4, que será abordado o grupo D_n.

Após definirmos classes conjugadas, faremos então, algumas considerações importantes acerca da mesma, a fim de relaciná-la com subgrupos normais.

Observação 2.4.7: Sejam G um grupo e H um subgrupo de G. Se $g \in G$ definiremos a função φ (conjugação pelo elemento $g \in G$) por:

$$\varphi : G \to G$$

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

Temos que $\varphi(H) = \{\varphi(h) : h \in H\} = \{h^g = g^{-1}hg : h \in H\}$ que será denotada por H^g ou $g^{-1}Hg$.

Proposição 2.4.8:

(i) H^g é subgrupo de G;

(ii) Dizemos que um subgrupo $H \leq G$ é normal em G se, e somente se, $\varphi(H) = H^g \subseteq H, \forall\ g \in G$.

As demonstrações dos itens acima encontram-se disponíveis em referência [5] (p. 139 - 140).

Exemplo 2.4.9: Se G é grupo abeliano, então $\forall\ g \in G, H^g = \{g^{-1} * h * g\} = \{h : h \in H\} = H$ e, portanto H é normal.

Exemplo 2.4.10: No capítulo 4, veremos um interessante exemplo, em que um grupo não abelino também satisfaz essa condição.

3 Homomorfismo de Grupos e Grupos de Permutações

Neste capítulo, definiremos Homomorfismo de Grupos e apresentaremos as principais propriedades e alguns exemplos relacionados ao mesmo. E também, trataremos de Grupos de Permutações e importantes resultados desse conceito, que será útil para o estudo do *Grupo Diedral*.

3.1 Homomorfismo de Grupos

Definição 3.1.1: Sejam $(G, *)$ e $(J, \cdot)$ grupos. Uma aplicação $f : G \to J$, de G em J é um homomorfismo, se ela satisfaz a seguinte propriedade:

$$f(x * y) = f(x)f(y), \forall\ x, y \in G.$$

Exemplo 3.1.2: Sejam $(\mathbb{Z}, +)$ e $(\mathbb{C}^*, \cdot)$ grupos. Verificaremos se $f : \mathbb{Z} \to \mathbb{C}^*$ dada por $f(m) = i^m$ é homormofismo.

Tomemos $m_1, m_2 \in \mathbb{Z}$. Segue que $f(m_1 + m_2) = i^{m_1+m_2} = i^{m_1}i^{m_2} = f(m_1)f(m_2)$.

Exemplo 3.1.3: Sejam os grupos $(\mathbb{R}^*_+, \cdot)$ e $(\mathbb{R}, +)$. Verificaremos se $f : \mathbb{R}^*_+ \to \mathbb{R}$ definida por $f(x) = log(x), \forall\ x \in \mathbb{R}^*_+$ é homomorfismo.

Segue que $f(x_1x_2) = log(x_1x_2) = log(x_1) + log(x_2) = f(x_1) + f(x_2)$.

Exemplo 3.1.4: $f : \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) = |x|$, sendo $\mathbb{R}^*$ grupo multiplicativo dos reais é homomorfismo.

Temos que $f(x_1x_2) = |x_1x_2| = |x_1||x_2| = f(x_1)f(x_2)$.

Propriedades 3.1.5: Seja $(G, *) \to (J, \cdot)$ um homomorfismo de grupos. Assim:

(P_1) $f(e_G) = e_J$.

(P_2) $f(x^{-1}) = f(x)^{-1}$.

(P_3) $Im(f) = \{y \in J \mid y = f(x)$, para algum $x \in G\ \}$ é subgrupo de J, chamado imagem de f.

(P_4) $ker f := \{x \in G \mid f(x) = e_J\}$ é um subgrupo normal de G chamado núcleo do homomorfismo f.

(P_5) $ker f = \{e_G\} \Leftrightarrow f$ é injetiva.

(P_6) Sejam os seguintes homomorfismos de grupos:

$$f : (G, *) \to (J, \cdot) \; e \; h : (J, \cdot) \to (H, \odot)$$

A composição $h \circ f : (G, *) \to (H, \odot)$ também é homomorfismo.

Demonstração:

(P_1) Temos que $f(e_G) = f(e_G * e_G) = f(e_G)f(e_G)$, logo $f(e_G) = f(e_G)f(e_G)$. Assim, $f(e_G)^{-1}f(e_G) = f(e_G)^{-1}f(e_G)f(e_G) \Rightarrow e_J = f(e_G)$.

(P_2) Segue que $f(x)f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_J = f(x)f(x)^{-1}$ e, portanto, $f(x^{-1}) = f(x)^{-1}$.

(P_3) Verificaremos que $Im(f) < J$. Para esse fim, tomemos $f(x_1) = y_1$ e $f(x_2) = y_2$, com $x_1, x_2 \in G$. Segue que $f(x_1 * x_2) = f(x_1)f(x_2) = y_1y_2 \in Im(f)$. Agora, provaremos que $y^{-1} \in G$. Logo, $f(x^{-1}) = f(x)^{-1} = y^{-1} \in Im(f)$.

(P_4) Provaremos que $ker f < G$. Para isso, tome $x, y \in ker f$, então:

$$f(x * y) = f(x)f(y) = e_Je_J = e_J \in ker f,$$

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

Por fim, provaremos que $ker f \triangleleft G$. Seja $a \in xH$, daí $\exists \; h_1 \in H$ tal que $a = xh_1$. Repare que $a = xh_1 = (xh_1x^{-1})x$. Além disso, temos que $f(xh_1x^{-1}) = f(x)f(h_1)f(x^{-1}) = f(x)e_Jf(x^{-1}) = f(x)f(x^{-1}) = e_J$. Daí, $xh_1x^{-1} \in ker f$. Como $a = xh_1 = (xh_1x^{-1})x \in Hx$, então $xH \subset Hx$. Analogamente, podemos tomar $a' \in Hx$. Assim, $\exists \; h_2 \in H$ tal que $a' = h_2x = (h_2xx^{-1})x$. Logo, $f(h_2xx^{-1}) = f(h_2)f(x)f(x^{-1}) = e_Je_J = e_J \in ker f$. Se $a' \in xH$, então $Hx \subset xH$. Portanto, $xH = Hx$.

(P_5) ($\Rightarrow$) Sejam x_1 e $x_2 \in G$. Assumindo que $f(x_1) = f(x_2)$, temos $f(x_1)f(x_2)^{-1} = f(x_2)f(x_2)^{-1} \Rightarrow f(x_1)f(x_2)^{-1} = e_J$. Como $f(x_1)f(x_2)^{-1} = f(x_1x_2^{-1})$, temos $f(x_1x_2^{-1}) =$

e_J. Logo, $x_1x_2^{-1} \in kerf = e_G$, assim $x_1x_2^{-1}x_2 = e_Gx_2$. Segue que, $x_1 = x_2$ e, portanto, f é injetivo.

($\Leftarrow$) Tomemos $x \in kerf$, então $f(x) = e_J = f(e_G)$ (por hipótese f é injetivo) $\Rightarrow$ $x = e_G$.

(P_6) Tomemos $x_1, x_2 \in G$. Então, $h \circ f = h \circ f(x_1 * x_2) = h(f(x_1 * x_2)) = h(f(x_1)f(x_2)) = h(f(x_1)) \odot h(f(x_2)) = (h \circ (f(x_1)) \odot (h \circ (f(x_2))$. ■

3.2 Isomorfismo de Grupos

Definição 3.2.1: Sejam $(G, *)$ e $(J, \cdot)$ dois grupos quaisquer. Diz-se $f : G \to J$ é um *isomorfismo* se, e somente se:

(i) f é homomorfismo de grupos;

(ii) f é bijetivo.

Quando existe um isomorfismo entre dois grupo G e J, dizemos que G e J são isomorfos (denotado por $G \simeq J$).

Exemplo 3.2.2: Mostraremos que $f : (\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +)$, dada por $f(x) = log(x), \forall\ x \in \mathbb{R}_+^*$ é isomorfismo.

Demonstração:

(i) *Homomorfismo:* (Exemplo 3.1.3).

(ii) *f é bijetiva:*

(1) Se $f(x_1) = f(x_2)$, então $x_1 = x_2$. Para isso, tomemos $x_1, x_2 \in \mathbb{R}_+^*$. Daí, $f(x_1) = f(x_2) \Rightarrow log(x_1) = log(x_2) \Rightarrow x_1 = x_2$.

(2) Seja $z \in \mathbb{R}, \exists\ x \in \mathbb{R}_+^*$ tal que $f(x) = z$. Segue que $f(x) = z \Rightarrow x = e^z \in \mathbb{R}_+^*$. ■

Exemplo 3.2.3: Sejam $G = \{2^m3^n \mid m, n \in \mathbb{Z}\}$ e $J = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} \mid m, n \in \mathbb{Z} \right\}$. Provaremos que $f : (G, \cdot) \to (J, +)$ é isomorfismo.

Demonstração:

(i) *Homomorfismo:* Verificaremos que $f(xy) = f(x) + f(y)$. Para isso, tome $x =$

2^t3^u e $y = 2^r3^s$. Temos que $f(xy) = f(2^t3^u2^r3^s) = f(2^{t+r}3^{u+s}) = \begin{bmatrix} t+r & u+s \\ -(u+s) & t+r \end{bmatrix} = \begin{bmatrix} t & u \\ -u & t \end{bmatrix} + \begin{bmatrix} r & s \\ -s & r \end{bmatrix} = f(x) + f(y) \in J.$

(ii) f é bijetiva:

(1) Se $f(2^{n_1}3^{m_1}) = f(2^{n_2}3^{m_2})$, mostraremos que $n_1 = n_2$ e $m_1 = m_2$. Sejam $n_1, m_1, n_2, m_2 \in \mathbb{Z}$. Segue que $f(2^{n_1}3^{m_1}) = f(2^{n_2}3^{m_2}) \Rightarrow \begin{bmatrix} n_1 & m_1 \\ -m_1 & n_1 \end{bmatrix} = \begin{bmatrix} n_2 & m_2 \\ -m_2 & n_2 \end{bmatrix} \Rightarrow n_1 = n_2$ e $m_1 = m_2$.

(2) Provaremos que $\exists\ x \in G$ tal que $f(x) = Z \in J$, sendo Z uma matriz. Para isso, tomemos $n_1,\ m_1 \in \mathbb{Z}$ e $x \in G$ tal que $x = 2^{n_1}3^{m_1}$. Temos que $f(x) = f(2^{n_1}, 3^{m_1}) = \begin{bmatrix} n_1 & m_1 \\ -m_1 & n_1 \end{bmatrix} = Z \in J.$ ∎

3.3 Grupos de Permutações

Seja E um conjunto não vazio, designaremos $Bij(E)$ o conjunto de todas as bijeções de E em E:

$$Bij(E) = \{f : E \to E; f \text{ é bijeção}\}.$$

A composição de aplicações é uma operação em $Bij(E)$. Pois, se $f : E \to E$ e $g : E \to E$ são bijeções, então a composta $g \circ f$, também é uma bijeção.

Proposição 3.3.1: Se E é um conjunto não vazio, então $(Bij(E), \circ)$ é grupo.

Demonstração:

(i) Associativo: Tomemos $x \in E$ e $f, g, h \in Bij(E)$. Segue que $f \circ (g \circ h) = (f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x) = (f \circ g) \circ h$.

(ii) Elemento neutro: A função identidade de E ($i_E : E \to E$) que é uma bijeção, é o elemento neutro de $Bij(E)$. Tomemos $f \in Bij(E)$ e $x \in E$, temos que $(i_E \circ f)(x) = i_E(f(x)) = f(x)$.

(iii) Elemento inverso: Tomemos a função $g \in Bij(E)$. Como g é uma bijeção,

logo existe uma função inversa $g^{-1} : E \to E$, que também é uma bijeção. Daí, temos $(g \circ g^{-1})(x) = g(g^{-1}(x)) = i_E$. ∎

Definição 3.3.2: O grupo $(Bij(E), \circ)$ é chamado de grupo de permutações do conjunto E.

Observação 3.3.3: O conjunto $Bij(E)$ possui outras notações como $P(E)$ ou $S(E)$. Além disso, se E é um conjunto finito com n elementos, então podemos indicar $Bij(E)$ por S_n. E portanto, S_n terá $n!$ elementos.

Exemplo 3.3.4: Construiremos a tábua de S_2. Sabemos que $S_2 = 2$ elementos, logo $S_2 = \left\{ f_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$. Fazendo $f_1 \circ f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} =$ $= \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = f_0$. Assim, podemos construir a seguinte tábua:

$\circ$	f_0	f_1
f_0	f_0	f_1
f_1	f_1	f_0

Observação 3.3.5: O Grupo de Permutações também é chamado de Grupo de Simetrias. Trataremos desse tema no próximo capítulo.

4 *Grupo Diedral*: Generalização e Exemplos

Este capítulo tem por objetivo estudar o *Grupo Diedral*. Para esse fim, traremos inicialmente de sua generalização e, em seguida, abordaremos alguns exemplos, dispondo da teoria elementar de Grupos, vista nos capítulos iniciais.

4.1 Generalização do *Grupo Diedral*

O conjunto D_n das simetrias de um polígono regular de n lados é grupo com a operação composição de aplicações. O grupo $(D_n, \circ)$, também é conhecido como *Grupo Diedral* de ordem $2n$ e, constituí-se por n rotações de $k\frac{2\pi}{n}$ em torno do centro de gravidade, para $k \in \{0, \ldots, n-1\}$, e por n reflexões em torno dos eixos de simetria do polígono.

O *Grupo Diedral ou Grupo de Simetrias* pode ser entendido como Grupo de Permutações. Isso porque, existe uma bijeção f de D_n em D_n e, os movimentos de rotação e reflexão de D_n são representados por permutações, que veremos nos exemplos da seção 4.2.

Definiremos a seguir as transformações espaciais deste polígono. Para isso, tomaremos um polígono regular P_n (Figura 01), em que n é o número de lados do polígono ($n \in \mathbb{N}$, com $n \geq 3$). O centro de gravidade é o ponto O, e existem n retas do espaço que passam pelas mediatrizes e diagonais (eixos de simetria) do polígono.

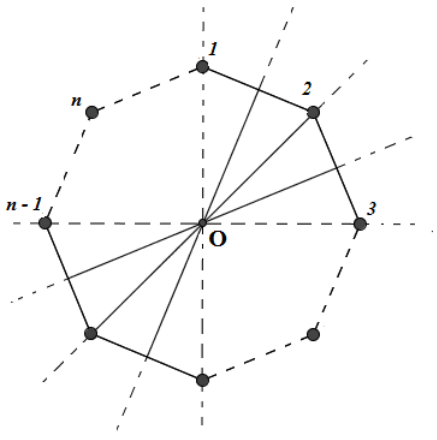

Figura 01

As transformações espaciais que preservam o polígono regular de n lados são:

(*i*) *Transformações Planas*:

Denotadas por $r_0, r_1, r_2, \ldots, r_n$, as rotações de $0, \frac{2\pi}{n}, 2\frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}$ *radianos* em torno do centro O, no sentido anti-horário.

(*ii*) *Transformações Espaciais:*

Denotadas por $s_1, s_2, \ldots, s_n$, as reflexões espaciais de π *radianos* em torno das retas (eixos de simetrias) $S_1, S_2, \ldots, S_n$.

Portanto, D_n é o conjunto formado por n rotações e n reflexões:

$$D_n = \{r_0, \ldots, r_n, s_1, \ldots, s_n\}.$$

Sejam R_n o conjunto de rotações do polígono regular de n lados e a operação composição de aplicações.

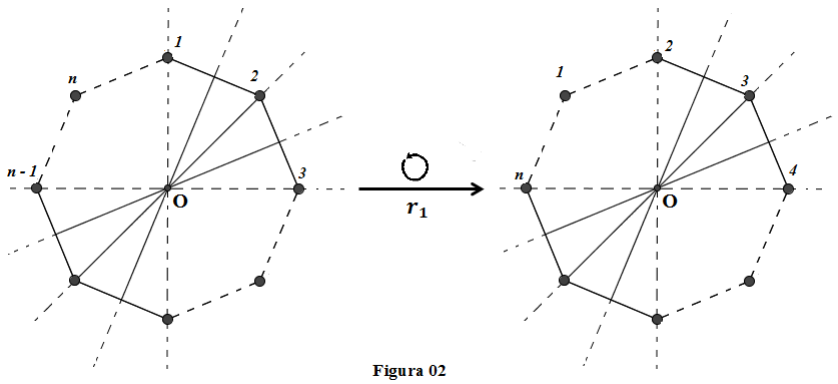

Figura 02

Podemos observar que r_1 gera R_n:

$$\begin{aligned} e = r_0 = r_1^0 &\text{ é a rotação de ângulo } 0;\\ r_1 = r_1^1 &\text{ é a rotação de ângulo } \tfrac{2\pi}{n};\\ r_2 = r_1^2 &\text{ é a rotação de ângulo } 2\tfrac{2\pi}{n};\\ r_3 = r_1^3 &\text{ é a rotação de ângulo } 3\tfrac{2\pi}{n};\\ \vdots \qquad &\vdots \qquad \vdots\\ r_{n-1} = r_1^{n-1} &\text{ é a rotação de ângulo } (n-1)\tfrac{2\pi}{n}. \end{aligned}$$

Segue que $r_1^0 = e$, $r_1^2 = r_1 \circ r_1 = r_2$, $r_1^3 = r_1^2 \circ r_1 = r_3$, ... , $r_1^{n-1} = r_1^{n-2} \circ r_1 = r_{n-1}$. (#) Assim, R_n é o conjunto das potências de r_1:

$$R_n = \{e, r_1, r_1^2, \ldots, r_1^{n-1}\}.$$

Proposição 4.1.1: O conjunto R_n com a operação composição de aplicações é grupo abeliano.

Demonstração:

(i) Provaremos que a operação composição está bem definida:

$$\circ : R_n \times R_n \to R_n$$

$$(r_1^i, r_1^j) \mapsto r_1^{i+j}$$

(1) Para $i + j < n$: Esse caso, decorre de $(\#)$.

(2) Para $i + j > n$: Usando o Algoritmo da divisão, temos que $\exists\ q, r \in \mathbb{N}$ tais que $i + j = qn + r$, com $0 \leq r < n$. Então, $r_1^i \circ r_1^j = r_1^{i+j} = r_1^{nq+r} = r_1^{nq} \circ r_1^r = (r_1^n)^q \circ r_1^r = e^q \circ r_1^r = r_1^r \in R_n$.

(ii) Associatividade: Sejam $r_1^i, r_1^j, r_1^k \in R_n$. Provaremos que $(r_1^i \circ r_1^j) \circ r_1^k = r_1^i \circ (r_1^j \circ r_1^k)$. Temos que $(r_1^i \circ r_1^j) \circ r_1^k = r_1^{i+j} \circ r_1^k = r_1^{i+j+k} = r_1^i \circ r_1^{j+k} = r_1^i \circ (r_1^j \circ r_1^k)$.

(iii) Elemento neutro: Seja $r_1^i \in R_n$, com $i \in \{0, 1, \ldots, n-1\}$. Então, $\exists\ e \in R_n$ tal que $r_1^i \circ e = e \circ r_1^i = r_1^i$. Como $r_1^i \circ r_1^0 = r_1^i \Rightarrow e = r_1^0$.

(iv) Elemento inverso: Tomemos r_1^i, com $i \in \{0, 1, \ldots, n-1\}$. Note que, $r_1^i \circ r_1^{n-i} = r_1^i \circ r_1^n \circ r_1^{-i} = r_1^i \circ e \circ r_1^{-i} = r_1^i \circ r_1^{-i} = e$. Daí, r_1^{-i} ou r_1^{n-i} é o inverso de r_1^i em R_n.

(v) Comutatividade: Sejam $r_1^i, r_1^j \in R_n$, logo $r_1^i \circ r_1^j = r_1^{i+j} = r_1^{j+i} = r_1^j \circ r_1^i$. ∎

Sejam Re o conjunto das reflexões do polígono regular de n lados e a operação composição de aplicações.

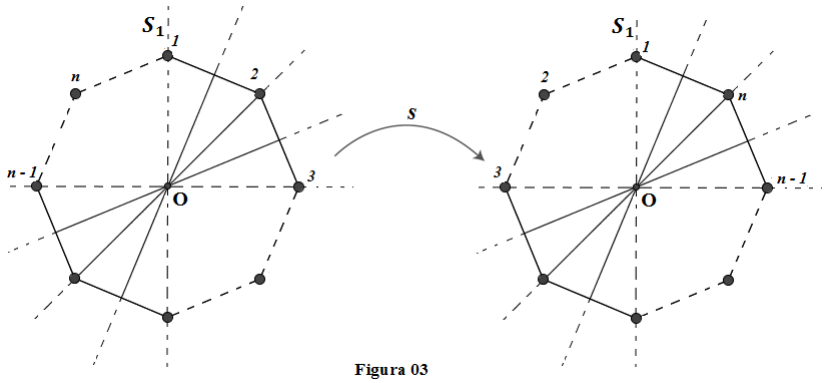

Figura 03

Observe que:

s_1 é a reflexão em torno da reta S_1 pelo vértice 1 e pelo centro O;

s_2 é a reflexão em torno da reta S_2 pelo vértice 2 e pelo centro O;

$\vdots \qquad \vdots \qquad \vdots$

s_n é a reflexão em torno da reta S_n pelo vértice n e pelo centro O.

Observação 4.1.2: O caso acima ocorre se n for ímpar. Caso n seja par, temos:

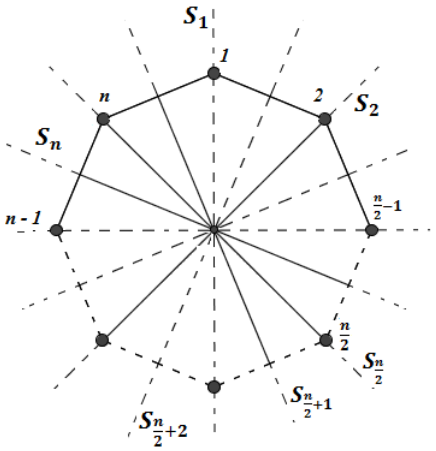

Figura 04

Note que:

s_1 é a reflexão em torno da reta S_1 pelo vértice 1 e pelo centro O;

s_2 é a reflexão em torno da reta S_2 pelo vértice 2 e pelo centro O;

s_3 é a reflexão em torno da reta S_3 pelo vértice 3 e pelo centro O;

$\vdots \qquad \vdots \qquad \vdots$

$s_{\frac{n}{2}}$ é a reflexão em torno da reta $S_{\frac{n}{2}}$ pelo vértice $\frac{n}{2}$ e pelo centro O;

$s_{\frac{n}{2}+1}$ é a reflexão em torno da reta $S_{\frac{n}{2}+1}$ que intercepta o segmento $\overline{1n}$ e o centro O;

$s_{\frac{n}{2}+2}$ é a reflexão em torno da reta $S_{\frac{n}{2}+2}$ que intercepta o segmento $\overline{12}$ e o centro O;

$\vdots \qquad \vdots \qquad \vdots$

s_n é a reflexão em torno da reta S_n que intercepta o segmento $\overline{(\frac{n}{2}-1)(\frac{n}{2})}$ e o centro O.

Observação 4.1.3: Se n for ímpar, existem n retas do espaço que passam pelas mediatrizes do polígono. E, se n for par, existem $\frac{n}{2}$ retas do espaço que passam pelas mediatrizes e $\frac{n}{2}$ retas que passam pelas diagonais do polígono.

Para facilitar nossa generalização, tomaremos s a reflexão de π *radianos* em torno da reta S_1 pelo vértice 1 e pelo centro do polígono. Assim, cada reflexão pode ser escrita

como combinação de s com as potência de r_1. Segue que:

$$s_1, s_2 = s \circ r_1, s_3 = s \circ r_1^2, \ldots, s_n = s \circ r_1^{n-1}.$$

Podemos definir o conjunto das reflexões Re como:

$$Re = \{s, s \circ r_1, s \circ r_1^2, \ldots, s \circ r_1^{n-1}\}.$$

No entanto, Re não é grupo com a composição de aplicações. Observe que, esse conjunto não possui um elemento neutro: $s^2 = s \circ s = r_0 = e \notin Re$.

D_n é definido como $R_n \cup Re$, sendo gerado por s e r_1:

$$D_n = \{e, r_1, r_1^2, \ldots, r_1^n, s, s \circ r_1, s \circ r_1^2, \ldots, s \circ r_1^{n-1}\}$$

A seguir, mostraremos que $(D_n, \circ)$ é grupo (não abeliano). Para isso, usaremos a rotação r_1 e a reflexão s, os geradores de D_n:

$$r_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix} e\ s = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}.$$

Tais representações podem ser visualizadas nas figuras 02 e 03 desta seção.

Lema 4.1.4: A igualdade $s \circ r_1^r = r_1^{n-r} \circ s$ é válida em D_n.

Demonstração: Usaremos o Princípio de Indução sobre r:

(i) Se $r = 1$, então $s \circ r_1 = r_1^{n-1} \circ s$. Segue que:

$$(1)\ s \circ\ r_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & 2 & 3 & \ldots & n-1 & n \end{pmatrix} \xrightarrow{\boldsymbol{r_1}} \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix} \xrightarrow{\boldsymbol{s}}$$

$$\xrightarrow{\boldsymbol{s}} \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ n & n-1 & n-2 & \ldots & 2 & 1 \end{pmatrix}.$$

(2) Como $r_1^{n-1} \circ r_1 = r_1^n = e$, então $r_1^{n-1} = r_1^{-1}$ (inverso). Daí, r_1^{-1} é a rotação de $\frac{2\pi}{n}$ *radianos* em torno do centro O, no sentido horário.

$$r_1^{n-1} \circ s = r_1^{-1} \circ s = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & 2 & 3 & \ldots & n-1 & n \end{pmatrix} \xrightarrow{\boldsymbol{s}} \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

$$\xrightarrow{r_1^{-1}} \quad \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}.$$

Como (1) = (2), temos que a igualdade acima vale para $r = 1$.

(*ii*) Supondo que vale para $r = k$, assim $s \circ r_1^k = r_1^{n-k} \circ s$, com $k > 1$. Provaremos para $r = k + 1 \Rightarrow s \circ r_1^{k+1} = r_1^{n-(k+1)} \circ s$. Então, $s \circ r_1^{k+1} = s \circ r_1^k \circ r_1 = \overbrace{r_1^{n-k} \circ s}^{Hipótese} \circ r_1 = r_1^{n-k} \circ r_1^{n-1} \circ s = r_1^n \circ r_1^{n-k-1} \circ s = r_1^n \circ r_1^{n-(k+1)} \circ s = e \circ R_1^{n-(k+1)} \circ s = r_1^{n-(k+1)} \circ s$. ∎

Lema 4.1.5: A composição é uma operação em D_n.

Demonstração: Provaremos que a operação composição está bem definida, ou seja, $r_1^i \circ s^u \circ r_1^j \circ s^v \in D_n$. Tomemos $(r_1^i \circ s^u, r_1^j \circ s^v) \in D_n \times D_n$, com $i, j \in \{0, 1, \dots, n-1\}$ e $u, v \in \{0, 1\}$. Para isso, observaremos os seguintes casos:

(1) Para $u = 0 \Rightarrow r_1^i \circ s^0 \circ r_1^j \circ s^v = r_1^i \circ e \circ r_1^j \circ s^v = r_1^i \circ r_1^j \circ s^v = \overbrace{r_1^{i+j}}^{\in D_n} \circ s^v \in D_n$.

(2) Para $u = 1 \Rightarrow r_1^i \circ s \circ r_1^j \circ s^v = r_1^i \circ r_1^{n-j} \circ s \circ s^v = r_1^{n+i-j} \circ s^{v+1} \in D_n$.

Note que $s^2 = s \circ s = e$ ou $s^3 = s \circ s \circ s = e \circ s = s$ e, portanto, podemos reduzir as potências de $\boldsymbol{s}$ a $\boldsymbol{e}$ ou $\boldsymbol{s}$. ∎

Proposição 4.1.6: D_n é grupo (não abeliano) com a composição de funções.

Demonstração:

(*i*) Vale a associatividade em D_n, pois é decorrente da operação composição.

(*ii*) D_n possui um elemento neutro, em que $r_0 = e$.

(*iii*) Existe um elemento inverso:

Provaremos que $r_1^i \circ s^u \in D_n$ possui um inverso. Desta forma, observaremos os casos a seguir:

(1) Para $u = 0$: Se $r_1^i \circ s^0 = r_1^i$, então r_1^{n-i}. Basta verificarmos que $r_1^i \circ r_1^{n-i} = e$.

(2) Para $u = 1$: Como $r_1^i \circ s \circ r_1^i \circ s = r_1^i \circ r_1^{n-i} \circ s \circ s = r_1^n \circ s^2 = e \circ e = e$. Portanto, o inverso de $r_1^i \circ s$ é ele mesmo.

Tadavia, não vale a comutatividade. Pois, pelo Lema 4.1.4, temos que $s \circ r_1 = r_1^{n-1} \circ s = r_1^{-1} \circ s \neq r_1 \circ s$, para $r = 1$. Logo, $(D_n, \circ)$ é grupo (não abeliano). ∎

Proposição 4.1.7 $(D_n, \circ)$ é grupo (não abeliano) com $2n$ elementos.

Demonstração:

Basta tomarmos $i, j \in \{0, 1, \ldots, n-1\}$ e $u, v \in \{0, 1\}$ tais que $r_1^i \circ s^u = r_1^j \circ s^v$. Provaremos que $i = j$ e $u = v$.

Segue que $r_1^i \circ s^u = r_1^j \circ s^v \Rightarrow (r_1^j)^{-1} \circ r_1^i \circ s^u = (r_1^j)^{-1} \circ r_1^j \circ s^v \Rightarrow (r_1^j)^{-1} \circ r_1^i \circ s^u = s^v$ $\Rightarrow (r_1^j)^{-1} \circ r_1^i \circ s^u \circ (s^u)^{-1} = s^v \circ (s^u)^{-1} \Rightarrow (r_1^j)^{-1} \circ r_1^i = s^v \circ (s^u)^{-1} \Rightarrow r_1^{-j} \circ r_1^i = s^v \circ s^{-u}$ $\Rightarrow r_1^{i+(-j)} = s^{v+(-u)}$.

Se $u = v$, então $s^{v+(-u)} = e \in \{e, r_1, \ldots, r_1^{n-1}\}$. Por outro lado, se $u \neq v$, logo $s^{v+(-u)} = s \notin \{e, r_1, \ldots, r_1^{n-1}\}$, o que contradiz o fato de $r_1^{i+(-j)} = s^{v+(-u)}$. Daí, $u = v$ e $r_1^i = r_1^j$ e, portanto, $i = j$. Logo, D_n possui $2n$ elementos, sendo dois a dois distintos. ∎

Definição 4.1.8: O grupo $(D_n, \circ)$ é denominado *Grupo Diedral* de ordem $2n$ ou *Grupo de Simetrias em polígonos regulares de n lados.*

4.2 Exemplos de *Grupos Diedrais*

Veremos a seguir alguns exemplos de *Grupos Diedrais*, destacaremos os grupos de simetrias do triângulo equilátero e quadrado.

4.2.1 Simetrias do Triângulo Equilátero

Seja D_3 o conjunto de simetrias do triângulo equilátero de vértices 1,2 e 3 (Figura 05).

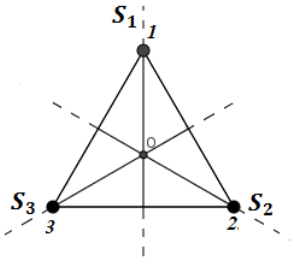

Figura 05

(*i*) *Transformações Planas:*

Denotadas por e, r_1 e r_2, as rotações de 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ *radianos* em torno do centro O, no sentido anti-horário. Representadas pelas permutações:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

(*ii*) *Transformações Espaciais:*

Denotadas por s_1, s_2 e s_3, as reflexões espaciais de π *radianos* em torno das retas S_1, S_2 e S_3. Representadas pelas seguintes permutações:

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Segue que $D_3 = \{e, r_1, r_2, s_1, s_2, s_3\} = \{e, r_1, r_1^2, s, s \circ r_1, s \circ r_1^2\}$. Em seguida, faremos a construção da tábua de D_3. Temos que:

$$r_1 \circ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2;$$

$$s_1 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = r_2.$$

Realizando-se todas as possíveis composições, temos a seguinte tábua:

$\circ$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_2	s_3	s_1
r_2	r_2	e	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r_2	r_1
s_2	s_2	s_1	s_3	r_1	e	r_2
s_3	s_3	s_2	s_1	r_2	r_1	e

Podemos observar que $(D_3, \circ)$ é grupo (não abeliano). Através da tábua, verificamos a existência do elemento neutro $e = r_0$ e dos inversos de $r_1^{-1} = r_2,\ s_1^{-1} = s_1,\ s_2^{-1} = s_2,\ s_3^{-1} = s_3,\ r_2^{-1} = r_1$. Além disso, vale a associatividade por se tratar da composição de aplicações. Contudo, não vale a comutatividade, pois $s_3 \circ s_1 \neq s_1 \circ s_3$. Como já havíamos demonstrado anteriormente.

Observação 4.2.1.1: $D_3 = S_3 = 3! = 6$ elementos, que corresponde a ordem de D_3.

Exemplo 4.2.1.2: Determinaremos os subgrupos de D_3. Para isso, usaremos o Teorema de Lagrange (teorema 2.3.3). Como já sabemos, a ordem de D_3 é seis, ou seja, seis é a quantidade de elementos do grupo. Assim, os possíveis subgrupos de D_3 possuem $1, 2, 3$ ou 6 elementos. Os subgrupos de ordem 1 e 6 são formados pelo elemento neutro e o próprio D_3, respectivamente. Enquanto, os subgrupos de ordem 2, totalizam-se 3, representados por $A = \{e, s_1\}, B = \{e, s_2\}$ e $C = \{e, s_3\}$. E, apenas um subgrupo possui ordem 3, que corresponde a $H = \{e, r_1, r_2\}$.

Observação 4.2.1.3: Use a proposição 1.2.4, para verificar se um conjunto não-vazio é subgrupo de D_3. Para exemplificar, tomaremos o conjunto $A = \{e, s_1\}$. Segue que $s_1^{-1} = s_1 \in D_3$, além do mais, $e \circ s_1 = s_1 \in D_3$ e, portanto, A é subgrupo de D_3. Procedimento análogo aos demais subconjuntos de D_3.

Exemplo 4.2.1.4: Seja $a = r_1 \in D_3$, temos $r_1^0 = e,\ r_1^1 = r_1,\ r_1^2 = r_2,\ r_1^3 = e,\ r_1^4 = r_1,\ r_1^5 = r_2, \ldots$ Daí, $[r_1] = \{e, r_1, r_2\} = H$ e, portanto, H é cíclico.

Exemplo 4.2.1.5: Tomemos o subgrupo $H = \{e, r_1, r_2\}$. Pelo Teorema do Lagrange, temos que $(D_3 : H) = 2$. Podemos determinar as classes laterais à esquerda e à direita de H em D_3. Segue que:

$$e \circ H = \{e \circ e, e \circ r_1, e \circ r_2\} = \{e, r_1, r_2\} = H \circ e;$$

$$r_1 \circ H = \{r_1 \circ e, r_1 \circ r_1, r_1 \circ r_2\} = \{r_1, r_2, e\} = H \circ r_1;$$

$$r_2 \circ H = \{r_2 \circ e, r_2 \circ r_1, r_2 \circ r_2\} = \{r_2, e, r_1\} = H \circ r_2;$$

$$s_1 \circ H = \{s_1 \circ e, s_1 \circ r_1, s_1 \circ r_2\} = \{s_1, s_3, s_2\} = H \circ s_1;$$

$$s_2 \circ H = \{s_2 \circ e, s_2 \circ r_1, s_2 \circ r_2\} = \{s_2, s_1, s_3\} = H \circ s_2;$$

$$s_3 \circ H = \{s_3 \circ e, s_3 \circ r_1, s_3 \circ r_2\} = \{s_3, s_2, s_1\} = H \circ s_3.$$

Portanto, só existem duas classes laterais (distintas) à esquerda de H, sendo essas, $e \circ H$ e $s_1 \circ H$. Segue que H é normal, pois ambas as classes são iguais.

Exemplo 4.2.1.6: Os grupos S_3 e D_3 são isormorfos. Podemos observar a seguir, que de fato, existe uma bijeção f de S_3 em D_3:

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

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = r_1 \longmapsto r_1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = r_1^2 \longmapsto r_2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s \longmapsto s_1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s \circ r_1 \longmapsto s_2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s \circ r_1^2 \longmapsto s_3$$

Agora, verificaremos se f é homomorfismo. Para isso, tomaremos $s_1, r_1 \in D_3$ tais que $f(s_1 \circ r_1) = f(s_1) \circ f(r_1)$. Segue que $f(s_1 \circ r_1) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f(s_1) \circ f(r_1)$. Procedimento análogo aos demais elementos de D_3. Portanto, temos um isomorfismo.

4.2.2 Simetrias do Quadrado

Seja D_4 o conjunto de simetrias do quadrado de vértices 1,2,3 e 4 (Figura 06).

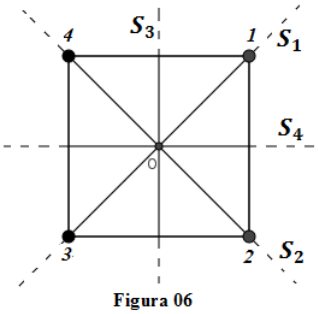

Figura 06

(*i*) *Transformações Planas:*

Denotadas por e, r_1, r_2 e r_3, as rotações de 0, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$ *radianos* em torno do centro O, no sentido anti-horário. Representadas pelas permutações a seguir:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ e } r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

(*ii*) *Transformações Espaciais:*

Denotadas por s_1, s_2, s_3 e s_4, as reflexões espaciais de π *radianos* em torno das retas S_1, S_2, S_3 e S_4. Representadas pelas permutações:

$$s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \text{ e } s_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Temos que $D_4 = \{e, r_1, r_2, r_3, s_1, s_2, s_3, s_4\} = \{e, r_1, r_1^2, r_1^3, s, s \circ r_1, s \circ r_1^2, s \circ r_1^3\}$. Posteriormente, construiremos a tábua de D_4. Segue que:

$$s_1 \circ r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = s_4;$$

$$s_2 \circ r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = s_1.$$

Após efetuarmos todas as composições, obtemos a seguinte tábua:

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_3	s_4	s_2	s_1
r_2	r_2	r_3	e	r_1	s_2	s_1	s_4	s_3
r_3	r_3	e	r_1	r_2	s_4	s_3	s_1	s_2
s_1	s_1	s_4	s_2	s_3	e	r_2	r_3	r_1
s_2	s_2	s_3	s_1	s_4	r_2	e	r_1	r_3
s_3	s_3	s_1	s_4	s_2	r_1	r_3	e	r_2
s_4	s_4	s_2	s_3	s_1	r_3	r_1	r_2	e

Por meio da tábua, podemos verificar que $(D_4, \circ)$ é grupo (não abeliano). Lembremos que $r_1^0 = e,\ r_2 = r_1 \circ r_1 = r_1^2,\ r_3 = r_1 \circ r_1^2 = r_1^3,\ s_3 = \ s \circ r_1^2,\ s_4 = s \circ r_1^3$. Portanto, D_4 é gerado por r_1 e s.

Exemplo 4.2.2.1: Tomemos o subconjuto D_4 de S_4. Provaremos que D_4 é subgrupo de S_4. Para isso, usaremos a proposição 1.2.4. Ao visualizarmos a tábua, percebemos a existência dos inversos $r_1^{-1} = r_3,\ r_2^{-1} = r_2,\ r_3^{-1} = r_1,\ s_1^{-1} = s_1,\ s_2^{-1} = s_2,\ s_3^{-1} = s_3$, todos eles pertecem a D_4. Além do mais, a operação está bem definida, pois ao tomarmos $r_1, s_1 \in D_4$, temo $r_1 \circ s_1 = s_3 \in D_4$. O mesmo vale para os demais elementos de D_4. Logo, D_4 é subgrupo de S_4.

Observação 4.2.2.2: Sabemos que a ordem de D_4 é oito. Enquanto, $S_4 = 4! = 24$ elementos, logo $o(S_4) = 24$. Pelo Teorema de Lagrange (teorema 2.3.3), S_4 possue subgrupos de ordem $1, 2, 3, 4, 6, 8, 12$ e 24. No entanto, nos interessa apenas o subgrupo de ordem oito, que corresponde a D_4.

Exemplo 4.2.2.3: Seja o subgrupo $H = \{e, r_1, r_2, r_3\}$. Identificaremos as classes laterais à esquerda e à direita de H em D_4. Temos que:

$$e \circ H = \{e \circ e, e \circ r_1, e \circ r_2, e \circ r_3\} = \{e, r_1, r_2, r_3\} = H \circ e;$$

$$s_1 \circ H = \{s_1 \circ e, s_1 \circ r_1, s_1 \circ r_2, s_1 \circ r_3\} = \{s_1, s_4, s_2, s_3\} = H \circ s_1.$$

Enquanto, as outras classes laterais à esquerda de H coincidem com essas duas. Além do mais, temos que $e \circ H = H \circ e$ e $s_1 \circ H = H \circ s_1$, logo H é subgrupo normal.

Observação 4.2.2.4: Através da visualização da tábua, facilmente nota-se que $H = \{e, r_1, r_2, r_3\}$ é subgrupo de D_4. Isso porque, a operação está bem definida e os inversos dos elementos estão em H.

Exemplo 4.2.2.5: Provaremos que f é isomorfismo. Sendo assim, podemos observar a existência de uma bijeção f de D_4 em D_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 3 \end{pmatrix} = e \longmapsto e$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 2 & 3 & 4 & 1 \end{pmatrix} = r_1 \longmapsto r_1$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix} = r_1^2 \longmapsto r_2$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 4 & 1 & 2 & 3 \end{pmatrix} = r_1^3 \longmapsto r_3$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 1 & 4 & 3 & 2 \end{pmatrix} = s \longmapsto s_1$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix} = s \circ r_1 \longmapsto s_2$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix} = s \circ r_1^2 \longmapsto s_3$$

$$\begin{pmatrix} 1 & 2 & 3 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix} = s \circ r_1^3 \longmapsto s_4$$

Verificaremos que f é homomorfismo. Para isto, tomemos $r_1, r_2 \in D_4$ tais que $f(r_1 \circ r_2) = f(r_1) \circ f(r_2)$. Segue que $f(r_1 \circ r_2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = f(r_1) \circ f(r_2)$. O mesmo procedimento vale para os outros elementos de D_4. Assim, f é isomorfismo.

Exemplo 4.2.2.6: A seguir, calcularemos as classes de conjugação do grupo D_4. Para isso, tomaremos $r_1 \in D_4$. Segue que $C_{r_1} = \{y \in D_4, y = g^{-1} \circ r_1 \circ g, \ com \ g \in D_4\}$:

$$g = e \Longrightarrow e^{-1} \circ r_1 \circ e = e \circ r_1 = r_1;$$

$$g = r_1 \in D_4 \Longrightarrow r_1^{-1} \circ r_1 \circ r_1 = r_3 \circ r_1 \circ r_1 = e \circ r_1 = r_1;$$

$$g = r_2 \in D_4 \Longrightarrow r_2^{-1} \circ r_1 \circ r_2 = r_2 \circ r_1 \circ r_2 = r_3 \circ r_2 = r_1;$$

$$g = r_3 \in D_4 \Longrightarrow r_3^{-1} \circ r_1 \circ r_3 = r_1 \circ r_1 \circ r_1 = r_2 \circ r_1 = r_3;$$

$$g = s_1 \in D_4 \Longrightarrow s_1^{-1} \circ r_1 \circ s_1 = s_1 \circ r_1 \circ s_1 = s_4 \circ s_1 = r_3;$$

$$g = s_2 \in D_4 \Longrightarrow s_2^{-1} \circ r_1 \circ s_2 = s_2 \circ r_1 \circ s_2 = s_3 \circ s_2 = r_3;$$

$$g = s_3 \in D_4 \Longrightarrow s_3^{-1} \circ r_1 \circ s_3 = s_3 \circ r_1 \circ s_3 = s_1 \circ s_3 = r_3;$$

$$g = s_4 \in D_4 \Longrightarrow s_4^{-1} \circ r_1 \circ s_4 = s_4 \circ r_1 \circ s_4 = s_2 \circ s_4 = r_3.$$

Portanto, os conjugados de r_1 são r_3 e ele mesmo. O procedimento é análogo aos desmais elementos de D_4. Sendo assim, ao realizarmos todos os cálculos, obtemos:

$$C_e = \{e\}; C_{r_1} = \{r_1\} \text{ e } C_{r_1} = \{r_3\}; C_{r_2} = \{r_2\} \text{ e } C_{r_2} = \{r_3\};$$

$$C_{r_3} = \{r_1\} \text{ e } C_{r_3} = \{r_3\}; C_{s_1} = \{s_1\} \text{ e } C_{s_1} = \{s_2\}; C_{s_2} = \{s_1\}$$

$$\text{e } C_{s_2} = \{s_2\}; C_{s_3} = \{s_3\} \text{ e } C_{s_3} = \{s_4\}; C_{s_4} = \{s_3\} \text{ e } C_{s_3} = \{s_4\}.$$

Observação 4.2.2.7: Sabemos que $H = \{e, r_1, r_2, r_3\}$ é subgrupo de D_4. Segundo a proposição 2.4.8 (ii), $\forall\ g \in D_4$, o subgrupo H satisfaz a seguinte condição: $\{g^{-1} * h * g\} = H$. Portanto, H é subgrupo normal de G. Como já havíamos provado no exemplo 4.2.2.3. No entanto, o conceito de subgrupos normais, pode ser entendido através de classes conjugadas.

5 Considerações Finais

Vimos que a Teoria de Grupos é uma área da Matemática voltada para o estudo de estruturas algébricas chamadas de Grupos. Tal teoria é relevante para a Álgebra Moderna, pois está por trás de estruturas algébricas como corpos, anéis e espaços vetoriais, e é uma ferramenta importante para o estudo de simetrias. Além do mais, o estudo de Grupos, em particular do *Grupo Diedral* é útil para outras áreas do conhecimento, por exemplo, na Química a geometria molecular e as propriedades moleculares estão diretamente relacionadas a esse conceito.

Portanto, a construção do *Grupo Diedral* ocorre por meio do estudo das simetrias, o qual é significante para este trabalho. Sendo assim, apresentamos a teoria elementar de Grupos para enriquecer o estudo do *Grupo de Simetrias* em polígonos regulares.

Referências Bibliográficas

[1] BAUMGART, J. K. *Tópicos de História da Matemática para o uso em sala de aula - Álgebra*. São Paulo: Atual, 1992.

[2] BOYER, C. B. *História da Matemática*. Tradução: Elza F. Gomide. 2ª ed. Editora: Edigar Blucher Ltda. São Paulo. 1974.

[3] DUMMIT, D. S. FOOTE, R. M. *Abstract algebra*. Third edition. John Wiley Sons, Inc., Hoboken, NJ, 2004.

[4] GARCIA, A. LEQUAIN, Y. A. *Elementos de Álgebra*. 6ª ed. Rio de Janeiro: IMPA, 2015.

[5] GONÇALVES, A. *Introdução à Algebra*. 5ª ed. Rio de Janeiro: IMPA, 2015.

[6] IEZZI, G. DOMINGUES, H. H. *Álgebra Moderna*. 4ª ed. São Paulo: Atual, 2003.

[7] JANESCH, O. R. *Álgebra II*. Florianópolis : UFSC/CED/CFM, 2008.

[8] LANG, S. *Estruturas Algébricas*. Ao livro técnico, Rio de Janeiro, 1972.