UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE ARAGUAÍNA
CURSO DE LICENCIATURA EM MATEMÁTICA

KARLA MAIANI DE SOUSA SOARES

O TEOREMA DO HOMOMORFISMO DE GRUPOS

ARAGUAÍNA
2016

KARLA MAIANI DE SOUSA SOARES

O TEOREMA DO HOMOMORFISMO DE GRUPOS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciada em Matemática.
Orientadora: Prof. Msc. Renata Alves da Silva.

ARAGUAÍNA
2016

KARLA MAIANI DE SOUSA SOARES

O TEOREMA DO HOMOMORFISMO DE GRUPOS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciada em Matemática.
Orientadora: Prof. Msc. Renata Alves da Silva.

Aprovada em: / / .

BANCA EXAMINADORA

Prof. Msc. Renata Alves da Silva (orientadora)

Prof. Dr. José Carlos de Oliveira Junior

Prof. Msc. Samara Leandro Matos da Silva

À minha família. Em especial aos meus pais, Carlos Galvão Soares e Maria Marlene Ribeiro de Sousa.

AGRADECIMENTOS

Primeiramente agradeço a Deus, por está sempre presente na minha vida, me dando saúde e força para enfrentar as dificuldades. E por me proporcionar a oportunidade de concluir mais essa fase em minha vida.

À toda minha família, meu alicerce, pelo carinho que sempre demonstraram por mim. Em especial aos meus pais, Carlos Galvão Soares e Maria Marlene Ribeiro de Sousa por estarem ao meu lado, sempre acreditando, quando muitas vezes eu duvidava. Por investir em mim, pelo apoio, compreensão e amor. Aos meus irmãos, Karina e Karley, pelas alegrias e o companheirismo.

Aos meus amigos, Cinthia Vaqueiro, Edna Alencar, Jonielder Silva e Tayara Oliveira, pela amizade que construímos durante o curso, por representarem a expressão amigos de toda as horas, pelas as inúmeras ajudas e por todos os momentos inesquecíveis que passamos juntos.

Agradeço meu amigo João Marcos, pelo apoio, paciência, pelos momentos compartilhados e por todo o suporte no decorrer do curso, principalmente nessa fase de conclusão, pelo o companheirismo e o auxílio no manuseamento do látex.

A todos os professores, por todas as contribuições para a minha formação.

Ao projeto Galois, a bolsista Lohanne Araújo e aos coordenadores pela chance de participar, e por meio desse projeto, despertar meu interesse pelo objeto em estudo.

Em especial, agradeço a minha orientadora Renata Alves da Silva, por me aceitar como sua orientanda, pela paciência, pelos conhecimentos transmitidos, pela dedicação, pela atenção e disponibilidade.

Agradeço, todos os meus colegas, pelos bons momentos juntos, principalmente, Camila Bomfim, Janete Moreira, Lee-andro e Mariane Araújo pela a hospitalidade.

Agradeço também, Cícero Júnior, por toda a ajuda durante o curso e por todas as alegrias divididas.

Enfim, agradeço a todos que contribuíram de forma direta e indireta para a realização deste trabalho.

*E*sperei com paciência no Senhor, e ele se inclinou para mim, e ouviu meu clamor.

Salmos 40:1

Resumo

Neste trabalho, apresentamos uma introdução da Teoria de Grupos com ênfase em homomorfismo de grupos. Temos como principal objetivo enunciar e demonstrar o Teorema do Homomorfismo. Este teorema nos dá uma caracterização do grupo quociente do domínio de um homomorfismo pelo seu núcleo e uma maneira explícita de se obter a partir de um homomorfismo um grupo quociente. Para isso, fazemos todo um estudo sobre isomorfismo de grupos. Este estudo se faz relevante, devido às vantagens em se conhecer grupos isomorfos. Dizemos que grupos isomorfos se comportam, em sua estrutura algébrica, da mesma maneira. Então, não há distinção quando se trata de suas operações, propriedades, ou seja, os elementos operam da mesma forma. Além desse teorema, traremos outros resultados importantes para a teoria de grupos, como por exemplo: o Teorema de Cayley e o Teorema de Lagrange.

Palavras-chave: Teoria de Grupos. Grupo Quociente. Homomorfismo de Grupos.

Abstract

In this work we present an introduction of Groups Theory with emphasis on group homomorphism. Our main goal is to enunciate and demonstrate the Homomorphism Theorem. This theorem gives us a characterization of the quotient group of the domain of a homomorphism by its nucleus and an explicit way of obtaining from a homomorphism a quotient group. For this, we do a whole study on group isomorphism. This study becomes relevant, due to the advantages of knowing isomorphic groups. We say that isomorphic groups behave, in their algebraic structure, in the same way. So there is no distinction when it comes to its operations, properties, that is, the elements operate in the same way. Besides this theorem, we will bring other important results for group theory, as for example: the Cayley Theorem and the Lagrange Theorem.

Keywords: Theory of Groups. Quotient Group. Homomorphism of Groups.

Sumário

1 Introdução **10**

2 Introdução à Teoria de Grupos **11**

2.1 Grupos 11

2.1.1 Conjunto das Classes de Restos 12

2.2 Grupo Cíclico 13

2.3 Grupo de Permutação 14

2.4 Subgrupos 17

2.5 Classes Laterais e Teorema de Lagrange 19

2.6 Subgrupos normais e Grupo Quociente 21

3 Homomorfismo de Grupos **27**

3.1 Isomorfismo de Grupos 31

4 Considerações Finais **35**

Referências bibliográficas **36**

1 Introdução

O estudo da Teoria de Grupos teve seu início com o matemático francês Evariste Galois. Ao longo dos anos, a Teoria de Grupos foi se desenvolvendo e despertando o interesse de muitos matemáticos, consagrando o nome de muitos pesquisadores brilhantes. E nos dias atuais, a mesma está presente em diversas áreas do conhecimento, como por exemplo, na criptografia.

Este trabalho tem como finalidade fazer um estudo sobre alguns tópicos da Teoria de Grupos, dando ênfase em homomorfismo e isomorfismo de grupos. Um homomorfismo de grupos é uma aplicação entre dois grupos que preserva as suas operações e chamamos de isomorfismo, um homomorfismo bijetor.

Apresentaremos também outros resultados importantes da Teoria de Grupos, como por exemplo: O Teorema de Cayley, que mostra que todo grupo finito é isomorfo a algum subgrupo do grupo de permutações de um conjunto G não vazio, Grupo Quociente, e também o Teorema do Homomorfismo. Sendo o principal objetivo do nosso trabalho mostrar, que através deste último podemos formar novos grupos quocientes.

Essa pesquisa será dividida da seguinte maneira: no segundo capítulo, trataremos de grupos e subgrupos, onde será apresentado um importante teorema, o Teorema de Lagrange, que é essencial para a determinação de subgrupos de uma maneira mais simples. Abordaremos também conceitos essenciais para determinar grupo quociente. Já no terceiro capítulo, iremos apresentar homomorfismo e isomorfismo de grupos e seus principais teoremas. Por fim apresentaremos as considerações finais a cerca dos resultados estudados.

2

Introdução à Teoria de Grupos

Neste capítulo, iremos abordar à teoria de grupos. Iniciaremos trazendo definições, propriedades e exemplos de grupos e subgrupos. Em seguida, apresentaremos o conceito de classes laterais e o importante Teorema de Lagrange. Por fim, definiremos subgrupos normais e grupo quociente. Os conceitos mencionados nesse capítulo, podem ser encontrados em [2, 3, 4, 6, 7, 8].

2.1 Grupos

Definição 2.1 *Seja G um conjunto não vazio e $*$ uma operação binária em G. Dizemos que G é um grupo em relação a essa operação se forem satisfeitas as seguintes propriedades:*

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

ii) Elemento neutro:
$\exists\ e \in G;\ a * e = a = e * a, \forall\ a \in G.$

iii) Elemento inverso:
$\forall\ a \in G, \exists\ \ a^{-1} \in G$ *tal que* $a * a^{-1} = e = a^{-1} * a.$

Observação 2.2 *Os elementos neutros e inversos são únicos:*

i) Sejam $e, e' \in G$ elementos neutros de G, assim

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

Logo, o elemento neutro é único.

ii) Sejam $a \in G$ e $a^{-1}, a_1^{-1} \in G$ dois elementos inversos de a. Assim,

$$a^{-1} = a^{-1} * e = a^{-1} * (a * a_1^{-1}) = (a^{-1} * a) * a_1^{-1} = e * a_1^{-1} = a_1^{-1}$$

Logo, o elemento inverso é único.

Quando a operação $*$ for de adição, chamamos o grupo de grupo aditivo, e se for de multiplicação, chamamos de grupo multiplicativo.

Exemplo 2.3 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ *e* $(\mathbb{C}, +)$ *são exemplos de grupos aditivos.*

Exemplo 2.4 $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$ *e* $(\mathbb{C}^*, \cdot)$ *são exemplos de grupos multiplicativos, onde* $\mathbb{Q}^*, \mathbb{R}^*$ *e* $\mathbb{C}^*$ *são os conjuntos* $\mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$ *sem o elemento zero.*

Observação 2.5 *O conjunto* $(\mathbb{Z}^*, \cdot)$ *não é um grupo multiplicativo, pois os únicos elementos que possuem inverso multiplicativo são os números -1 e 1.*

Exemplo 2.6 *O conjunto das matrizes de ordem* $m \times n$ *sobre* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$ *com a operação de adição de matrizes são exemplos de grupos aditivos. Os mesmos serão denotados por* $(M_{m\times n}(K), +)$*, para* $k = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$*.*

Exemplo 2.7 *Sabe-se que nem toda matriz quadrada possui inverso multiplicativo. Por exemplo, matrizes que possuem uma linha ou uma coluna nula. Desta forma, vamos definir o seguinte conjunto* $GL_n(\mathbb{Q}) = \{A \in Mn(\mathbb{Q}) | det(A) \neq 0\}$*, o conjunto das matrizes inversíveis. Esse conjunto com a operação de multiplicação de matrizes forma um grupo multiplicativo. Chamamos esse grupo de grupo linear geral de ordem n. Analogamente, são definidos os grupos lineares gerais sobre* $\mathbb{R}$ *e* $\mathbb{C}$*.*

2.1.1 Conjunto das Classes de Restos

Definição 2.8 *Sejam* x, y *em* $\mathbb{Z}$*, dizemos que* $x \sim y$ *se, e somente se,* $x \equiv y (mod\ n)$*. Ou seja, x é congruo a y se, e somente se, deixam o mesmo resto na divisão por n.*

Vamos indicar o conjunto de todos os elementos que deixam resto zero na divisão por n pela classe $\overline{0}$ e assim por diante. Obtemos, dessa forma, o conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, cojunto das classes de restos da divisão por n. Podemos definir nesse conjunto as operações de adição e multiplicação de classes da seguinte maneira: $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{ab}$.

Exemplo 2.9 $(\mathbb{Z}_n, +)$ *é um grupo aditivo.*

Exemplo 2.10 $(\mathbb{Z}_n^*, \cdot)$ *é um grupo multiplicativo se, e somente se, n é primo.*

Demonstração: Vamos supor que n não é primo. Como $n > 1$, existem x, y dois inteiros, maiores que 1, tais que $xy = n$. Assim, $\overline{xy} = \overline{n}$, mas pela a operação definida $\overline{x} \cdot \overline{y} = \overline{xy}$ e $\overline{n} = 0$, então $\overline{x} \cdot \overline{y} = \overline{0}$, o que é impossível, visto que $\overline{x}, \overline{y} \in \mathbb{Z}_n^*$. Reciprocamente, sejam $\overline{x}, \overline{y} \in \mathbb{Z}_n^*$. Se $\overline{xy} = \overline{0}$, então $xy \equiv 0\,(mod\, n)$, ou seja, $n \,|\, xy$. Como n é primo, logo $n \,|\, x$ ou $n \,|\, y$, quer dizer $\overline{x} = 0$ ou $\overline{y} = 0$, o que é impossível. Agora, vamos mostrar que todo elemento $\overline{a} \in \mathbb{Z}_n^*$ possui inverso multiplicativo. Dado $\overline{a} \in \mathbb{Z}_n^*$, então a não é multiplo de n. Como por hipótese n é primo, $mdc(n, a) = 1$. Então, $\exists\ x_0, y_0 \in \mathbb{Z}_n^*$, tais que $ax_0 + ny_0 = 1$. (Veja [4], pág. 144). Desse modo,

$$\overline{ax_0 + ny_0} = \overline{ax_0} + \overline{ny_0} = \overline{ax_0} = \overline{a} \cdot \overline{x_0} = 1.$$

Isso mostra que $\overline{x_0}$ é inverso multiplicativo de $\overline{a}$. Logo, $(\mathbb{Z}_n^*, \cdot)$ é um grupo multiplicativo. □

Como vimos, para que que um conjunto não vazio seja um grupo, não necessariamente deve satisfazer a propriedade comutativa. Os grupos que satisfazem essa propriedade recebem um nome especial.

Definição 2.11 (Grupo abeliano) *Dizemos que G é um grupo abeliano ou comutativo se $a * b = b * a$, $\forall\ a, b \in G$.*

Exemplo 2.12 *$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ e $(\mathbb{C}, +)$ são grupos aditivos abelianos.*

Exemplo 2.13 *Se G é um grupo multiplicativo e $x^2 = 1$, $\forall\ x \in G$, então G é abeliano.*

Demonstração: De fato, sejam $x, y \in G$. Por hipótese, $(x \cdot y)^2 = 1$. Logo, $(x \cdot y)^2 = 1 \Rightarrow x \cdot y \cdot x \cdot y = 1$. Multiplicando por x à direita e y à esquerda. Obtemos, $x \cdot x \cdot y \cdot x \cdot y \cdot y = x \cdot 1 \cdot y \Rightarrow y \cdot x = x \cdot y$. □

2.2 Grupo Cíclico

Definição 2.14 *Seja G um grupo. Se exitir um elemento $x \in G$ tal que x gere todo o grupo, isto é, se*

$$G = \langle x \rangle = \{x^m |\ m \in \mathbb{Z}\}.$$

Chamamos G de grupo cíclico. Em caso de G ser um grupo aditivo, usaremos a notação

$$G = \langle x \rangle = \{mx |\ m \in \mathbb{Z}\}.$$

Exemplo 2.15 $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.

Exemplo 2.16 *O grupo* $G = \{1, -1, i, -i\} = \langle i \rangle$.

Exemplo 2.17 $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

Proposição 2.18 *Todo subgrupo de um grupo cíclico é também cíclico.*

Demonstração: A demonstração dessa proposição, pode ser encontrada em [4], pág. 178. □

Proposição 2.19 *Todo grupo cíclico é abeliano.*

Demonstração: Sejam $G = \langle x \rangle = \{x^m | \ m \in \mathbb{Z}\}$ e $a, b \in G$. Mostraremos que $a \cdot b = b \cdot a$.
Existem $m, n \in \mathbb{Z}$ tais que $a = x^m$ e $b = x^n$. Logo,

$$a \cdot b = x^m \cdot x^n = x^{m+n} = x^{n+m} = x^n \cdot x^m = b \cdot a.$$

Portanto, G é abeliano. □

Exemplo 2.20 *Como vimos* $(\mathbb{Z}, +)$ *é um grupo cíclico e, portanto, pela proposição 2.19, ele é abeliano.*

2.3 Grupo de Permutação

Devido à importância do grupo simétrico de ordem n para o nosso trabalho, traremos a seguir alguns de seus principais resultados.

Exemplo 2.21 *O conjunto* $S_G = \{\sigma : G \to G, \sigma \text{ é bijeção } \}$ *munido da operação de composição de funções é um grupo.*

Demonstração: De fato, vamos verificar as seguintes condições:

i) Associativa:
Sejam $f, g, h \in S_G$. Tem-se

$$\begin{aligned}(f \circ g) \circ h(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x))) \\ &= f(g \circ h)(x) \\ &= f \circ (g \circ h)(x).\end{aligned}$$

ii) Elemento neutro:
Seja $I_G \in S_G$, a função identidade. Vamos mostrar que I_G é o elemento neutro desse conjunto. Com efeito, $\forall\ f \in S_G$, temos

$$(I_G \circ f)(x) = I_G(f(x)) = f(x) = f(I_G(x)) = (f \circ I_G)(x).$$

iii) Elemento inverso:
Para todo $f \in S_G$, existe $f^{-1} \in S_G$, tal que,

$$f \circ f^{-1} = f^{-1} \circ f = I_G.$$

Portanto, $(S_G, \circ)$ é um grupo. □

O grupo $(S_G, \circ)$ também é chamado de grupo das permutações do conjunto G. Se $G = \{1, 2, 3, ..., n\}$, chamamos de grupo simétrico. Esse grupo será denotando por S_n, cuja ordem, ou seja, o número de elementos do conjunto é $|S_n| = n!$.

Uma permutação σ em S_n pode ser representada também da seguinte forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}$$

Exemplo 2.22 *Se S_n é um grupo de ordem igual ou maior que 3, então S_n é um grupo não abeliano. Considere S_3 sendo $\sigma = \{1, 2, 3\}$.*

De fato, note que o grupo S_3 tem 6 permutações diferentes, $S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$. Sendo elas iguais a

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Vamos usar a composição de funções para provar que S_3 é um grupo não abeliano. Faremos a composição de elementos da direita para à esquerda.

$$\sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma_4.$$

$$\sigma_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_5.$$

Concluímos que $\sigma_2 \circ \sigma_3 \neq \sigma_3 \circ \sigma_2$. Logo, S_3 não é abeliano.

Definição 2.23 *Uma permuntação $\sigma \in S_n$ é chamada um r-ciclo se existem elementos distintos $a_1, \cdots, a_r \in \{1, \cdots, n\}$ tais que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\cdots$, $\sigma(a_{r-1}) = a_r$, $\sigma(a_r) = a_1$, e $\sigma(j) = j$, $\forall j \in \{1,...,n\} \setminus \{a_1, \cdots, a_r\}$; e esse r-ciclo será denotado por $(a_1, \cdots, a_r)$; o número r é chamado de comprimento do r-ciclo. Os 2-ciclos são também chamados de transposições.*

Exemplo 2.24 *Seja S_4 a permutação definida por:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Como $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2, \sigma(4) = 4$, então σ é um ciclo de comprimento 3 e é denotado por (1 3 2).

Exemplo 2.25 *Considere em S_3 a permutação:*

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

Como $\phi(1) = 1, \phi(2) = 3, \phi(3) = 2$, temos uma transposição, porque o ciclo tem comprimento 2 e é denotado por (2 3).

Proposição 2.26 *Toda permutação $\sigma \in S_n$ pode ser escrita como produto de ciclos disjuntos.*

Demonstração: O leitor pode encontrar essa demonstração em [4], pág.202. □

Exemplo 2.27 *Escreva a seguinte permutação de S_6 como produto de ciclos disjuntos:*

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

Começando pelo o primeiro ciclo, que se inicia com o elemento 1:

$$\varphi(1) = 6, \varphi(6) = 3, \varphi(3) = 1.$$

Logo,

$$\varphi_1 = (1\ 6\ 3).$$

Repetindo, agora com o ciclo que se inicia no elemento 2:

$$\varphi(2) = 5, \varphi(5) = 4, \varphi(4) = 2.$$

Logo,

$$\varphi_2 = (2\ 5\ 4).$$

Portanto, $\varphi = \varphi_1 \circ \varphi_2 = (1\ 6\ 3) \circ (2\ 5\ 4)$.

2.4 Subgrupos

Definição 2.28 *Seja $(G, *)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G, se as seguintes condições forem satisfeitas:*

i) $e \in H$;

ii) $\forall\ a,\ b \in H$ *tem-se* $ab \in H$;

iii) $\forall\ a \in H$ *tem-se* $a^{-1} \in H$;

Pode-se resumir as três condições acima em apenas uma.

iv) $H \neq \emptyset$ *e* $\forall\ a,\ b \in H$ *tem-se* $ab^{-1} \in H$.

Exemplo 2.29 *O conjunto $H = \mathbb{Z} \cdot m = \{rm : r \in \mathbb{Z}\}$, $m \in \mathbb{Z}$, é um subgrupo do grupo aditivo dos inteiros.*

Demonstração: Para H ser um subgrupo de G, onde $G = (\mathbb{Z}, +)$, precisamos verificar a seguinte condição:

$$H \neq \emptyset \text{ e } \forall\ a, b \in H \text{ tem-se } a + b^{-1} \in H.$$

Para isso, temos:

$$r = 0 \Rightarrow rm = 0 \Rightarrow 0 = 0 \cdot m \in H. \text{ Logo } H \neq \emptyset.$$

$a, b \in H \Rightarrow a = r_1 m$ e $b = r_2 m$, com $r_1, r_2 \in \mathbb{Z}$. Assim, $b = r_2 m \in \mathbb{Z} \Rightarrow b^{-1} = -b = -r_2 m$. Então,

$$a + b^{-1} = r_1 m + (-r_2 m) = (r_1 - r_2)m \in H.$$

Portanto, H é um subgrupo de $\mathbb{Z}$. □

A seguir, mostraremos que todo subgrupo aditivo de $\mathbb{Z}$ são dessa maneira.

Proposição 2.30 *Todos os subgrupos de $(\mathbb{Z}, +)$ são da forma $\mathbb{Z}m$.*

Demonstração: Acabamos de provar que $(\mathbb{Z}m, +)$ é um subgrupo de $\mathbb{Z}$. Agora, iremos mostrar que todos os subgrupos de $\mathbb{Z}$ são dessa forma. De fato, seja H um subgrupo qualquer de $\mathbb{Z}$. Suponhamos que $H = \{0\}$. Logo, $H = \mathbb{Z} \cdot 0$. Mas, se $H \neq \{0\}$, considere n o menor elemento positivo de H. Assim, $n \in H$ e, por hipótese, H é um subgrupo, então $\mathbb{Z}m \subseteq H$. Tomemos um $h \in H$. Pelo o algorítmo de Euclides, existem dois inteiros q, r tais que

$$h = qn + r \quad (0 \leq r < n).$$

Logo, como $h, n \in H$, então r também pertence a H. Mas, como pegamos n como menor inteiro positivo, concluímos que $r = 0$ e, portanto, $h = qn$. Então, $h \in \mathbb{Z}m$. Assim, mostramos que $H = \mathbb{Z}m$. □

Definiremos o conjunto $Z(G)$ e em seguida, provaremos que é um subgrupo.

Definição 2.31 *Dado G um grupo, seja $Z(G) = \{a \in G : a \cdot x = x \cdot a, \forall\ x \in G\}$. Dizemos que $Z(G)$ é o centro do grupo G.*

Exemplo 2.32 *Seja G um grupo. Então $Z(G)$ é um subgrupo de G.*

Demonstração: De fato, note que:

$$e \in G \Rightarrow e \cdot x = x \cdot e,\ e \in Z(G). \text{ Logo, } Z(G) \neq \emptyset.$$

$a, b \in Z(G)$, então $a \cdot x = x \cdot a$ e $b \cdot x = x \cdot b$, $\forall\ x \in G$. Dessa forma, $a = x \cdot a \cdot x^{-1}$ e $b = x \cdot b \cdot x^{-1}$. Assim, $b = x \cdot b \cdot x^{-1} \Rightarrow b^{-1} = (x \cdot b \cdot x^{-1})^{-1} = x \cdot b^{-1} \cdot x^{-1}$. Então,

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

Operando x à direita em ambos os lados da igualdade, tem-se

$$a \cdot b^{-1} \cdot x = x \cdot a \cdot b^{-1}$$

Portanto, $Z(G)$ é um subgrupo de G. □

Exemplo 2.33 *Sejam G um grupo e $x \in G$. Então, $H = \langle x \rangle$ é um subgrupo de G.*

Demonstração: De fato, temos que:

$$e = x^0,\ e \in H \Rightarrow H \neq \emptyset.$$

$a, b \in H \Rightarrow a = x^n$ e $b = x^q$, onde $n, q \in \mathbb{Z}$. Assim, $b^{-1} = (x^q)^{-1} = x^{-q}$.

$$a \cdot b^{-1} = x^n \cdot x^{-q} = x^{n-q} \in H.$$

Logo, H é um subgrupo. □

2.5 Classes Laterais e Teorema de Lagrange

Nessa seção, apresentaremos um dos teoremas mais importantes da teoria de grupo, conhecido como Teorema de Lagrange. O mesmo relaciona a ordem dos subgrupos e a ordem do grupo e nos dá uma maneira prática de determinarmos os possíveis subgrupos de um grupo finito qualquer.

Definição 2.34 *Se H é um subgrupo de G e $a \in G$, denominamos classe lateral à esquerda de H em G o conjunto*

$$aH = \{a \cdot h \mid h \in H\}.$$

De modo análogo, denominamos classe lateral à direita de H em G o conjunto

$$Ha = \{h \cdot a \mid h \in H\}.$$

Exemplo 2.35 *Sejam $G = \{-1, 1, i, -i\}$ e $H = \{1, -1\}$ seu subgrupo.*
Vamos determinar as classes laterias à esquerda e à direira de H em G.
$1 \cdot H = H = H \cdot 1$;
$(-1) \cdot H = \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\} = H \cdot (-1)$;
$i \cdot H = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} = H \cdot i$;
$(-i) \cdot H = \{(-i) \cdot 1, (-i) \cdot (-1)\} = \{-i, i\} = H \cdot (-i)$.

É possível mostrar que existe uma bijeção entre elas. Assim, tanto faz considerar classes laterais à esquerda quanto à direita. Por isso, a partir de agora, iremos trabalhar apenas com as classes laterias à esquerda.

A proposição que daremos a seguir mostra que o conjunto das classes laterais à esquerda forma uma partição de G. Por não fazer parte dos nossos objetivos, iremos omitir suas demonstrações, que podem ser vistas no livro [2], pág. 203.

Proposição 2.36 *Sejam G um grupo e H um subrupo de G. $\forall\ a, b \in G$, temos*

i) $aH = bH$ *ou* $aH \cap bH = \emptyset$.

ii) Todas as classes laterais têm $|H|$ elementos, isto é, $|aH| = |H|$ para todo $a \in G$.

iii) Existem elementos $a_1, a_2, ..., a_n \in G$, com $a_1 = e_G$, tais que,

$$G = a_1H \cup a_2H \cup ... \cup a_nH,$$

ou seja, a união de todas as classes módulo H é igual a G.

Denotamos o índice de G em H por $(G : H)$, a quantidade de classes laterais módulo H em G.

Exemplo 2.37 *Sejam $G = (\mathbb{Z}_6, +)$ e $H = \{\overline{0}, \overline{2}, \overline{4}\}$. As classes laterias à esquerda de H em G são:*
$H = \overline{0} + H = \{\overline{0}, \overline{2}, \overline{4}\}$ *e* $\overline{1} + H = \{\overline{1}, \overline{3}, \overline{5}\}$, *já que as outras coincidem com uma dessas. Logo, a partição de $\mathbb{Z}_6$ é feita por essas duas classes. Portanto, $(G : H) = 2$.*

Teorema 2.38 (Lagrange) *Se G é um grupo finito e H é um subgrupo de G, então $|H|$ é um divisor de $|G|$.*

Para demonstrar o Teorema de Lagrange, usaremos a Proposição 2.36. Vamos denotar por $G/H = \{xH \mid x \in G\}$ como o conjunto de todas classes laterais à esquerda.

Demonstração: Suponhamos que G é um grupo finito, assim

$$|G/H| = n, \text{ então } G/H = \{x_1H, x_2H, ..., x_nH\},$$

onde $x_1, x_2, ..., x_n \in G$, com $x_1 = e_G$. Pelo item *iii)* da Proposição 2.36 , G é igual à união disjuntas de todas as classes laterais à esquerda de H em G, ou seja,

$$G = x_1H \cup x_2H \cup ... \cup x_nH.$$

Em decorrência da união ser disjunta, temos

$$|G| = |x_1H| + |x_2H| + ... + |x_nH|.$$

Mas, pela Proposição 2.36, o item *ii)*, todas as classes têm a mesma cardinalidade

$$|x_iH| = |H| \qquad \forall\ i = 1, 2, ..., n.$$

Logo,

$$\begin{aligned} |G| &= |x_1H| + |x_2H| + ... + |x_nH| \\ |G| &= |H| + |H| + ... + |H| \\ |G| &= n|H|. \end{aligned}$$

Portanto, $|H|$ divide $|G|$. □

Corolário 2.39 *Todo grupo finito de ordem prima é cíclico.*

Demonstração: Seja G um grupo tal que $|G| = p$, onde p é um número primo qualquer. Como p é número primo e $|G| = p$, então $p > 1$. Assim, o grupo G possui um elemento x diferente do elemento neutro. Considere o subgrupo H gerado pelo elemento x, $H = \langle x \rangle$. Pelo teorema de Lagrange, $|\langle x \rangle|$ é um divisor de $|G|$, ou seja, $|\langle x \rangle|\ /p$. Como p é primo, os seus únicos divisores são 1 e p. Visto que $|\langle x \rangle| > 1$, logo $|\langle x \rangle| = p$. Portanto, G é um grupo cíclico. □

Exemplo 2.40 $(\mathbb{Z}_p^*, \cdot)$, *onde p é primo, é um grupo cíclico.*

2.6 Subgrupos normais e Grupo Quociente

Nessa seção, vamos introduzir os conceitos de classes de conjugação e subgrupos normais, que são essenciais para a construção do grupo quociente.

Muitas vezes na Álgebra é importante separar elementos de um mesmo conjunto que estão relacionados por uma certa condição. Aqui, iremos tratar de um tipo dessas relações, o que chamamos de relação de equivalência.

Lema 2.41 *Se G é um grupo e* $x, y \in G$, *a relação*

$$x \sim y \Leftrightarrow \exists\ g \in G \text{ tal que } y = g^{-1}xg$$

é uma relação de equivalência em G, isto é, tal relação satisfaz:

i) $x \sim x$ (Reflexiva);

ii) Se $x \sim y$, então $y \sim x$ (Simétrica);

iii) Se $x \sim y$ e $y \sim z$, então $x \sim z$ (Transitiva).

Demonstração:

i) $\forall\ x \in G$, temos que

$$x = e^{-1} \cdot x \cdot e = x \cdot e = x.$$

Logo, $x \sim x$.

ii) Se $x \sim y$, então existe $g \in G$ tal que:

$$y = g^{-1} \cdot x \cdot g.$$

Operando à esquerda por g e à direita por g^{-1} em ambos os lados da igualdade, temos

$$g \cdot y \cdot g^{-1} = x.$$

Logo, $y \sim x$.

iii) Se $x \sim y$ e $y \sim z$, existem g_1 e g_2 em G tais que $y = g_1^{-1} \cdot x \cdot g_1$ e $z = g_2^{-1} \cdot y \cdot g_2$, onde $g = g_1 g_2$. Assim, $z = g_2^{-1} \cdot y \cdot g_2$

$$g_2^{-1} \cdot (g_1^{-1} \cdot x \cdot g_1) \cdot g_2 = (g_2^{-1} \cdot g_1^{-1}) \cdot x \cdot (g_1 \cdot g_2) = (g_1 \cdot g_2)^{-1} \cdot x \cdot (g_1 \cdot g_2) = g^{-1} \cdot x \cdot g.$$

Segue que $x \sim z$. □

Definição 2.42 (Classes de conjugação) *A classe* $\overline{x} = \{y : x \sim y\} = \{x^g = g^{-1}xg : g \in G\}$ *é chamada classe de conjugação em* G *determinada pelo elemento* $x \in G$. *Se* $y \in \overline{x}$, *dizemos que* x *e* y *são elementos conjugados em* G.

Definição 2.43 *Seja* $\sim$ *uma relação de equivalência sobre* G. *O conjunto de todas as classes de equivalência será indicado por* $G/\sim$ *e chamado de conjunto quociente.*

Quando $\sim$ é uma relação de equivalência em G e $x, y \in G$, usaremos a notação $x \equiv y (\text{mod } G)$ para significar que $x \sim y$, isto é, x é equivalente a y.

Introduziremos agora a noção de subgrupo normal. Esse tipo de subgrupo será fundamental para definirmos grupo quociente.

Definição 2.44 *Dados G um grupo e N um subrupo de G, N é chamado de subgrupo normal de G se, $\forall g \in G$, tivermos $gng^{-1} \in N$ para qualquer $n \in N$. Denotando por*

$$N^g = \{gng^{-1}, n \in N\},$$

segue que N é um subgrupo normal de G se $N^g \leq N$ e escrevemos $N \trianglelefteq G$.

Pela definição acima, podemos obter a seguinte proposição.

Proposição 2.45 *Seja G um grupo. Então, N é subgrupo normal de G se, e somente se, $gN = Ng$.*

Demonstração: Supondo que N é um subgrupo normal de G, temos que $g^{-1}ng \in N$, para todo g em G e para todo n em N. Vamos mostrar que $gN = Ng$ para todo $g \in G$. De fato, para $n \in N$, temos que $gn = (gng^{-1})g = n_1 g$, onde $n_1 = gng^{-1} \in N$ por hipótese. Assim, $gN \subseteq Ng$. A igualdade contrária segue de maneira análoga. Reciprocamente, se $gN = Ng$ para todo $g \in G$, vamos mostrar que N é um subgrupo normal de G. Com efeito, esta igualdade implica que $N = g^{-1}Ng$ e, portanto, N é um subgrupo normal de G. □

A proposição anterior nos dá uma alternativa para dizer quando um subgrupo é normal. Temos que um subgrupo N é normal em G se, e somente se, $N = gNg^{-1}$, $\forall\ g \in G$.

Apresentaremos, a seguir, um dos resultados mais importante do trabalho. Definiremos uma operação entre classes laterias. Veremos mais adiante que através dessa operação, será possível obter um tipo especial de grupo, denominado grupo quociente, que é um exemplo fundamental de grupo para a demonstração do teorema principal.

Proposição 2.46 *Sejam G um grupo e N um subgrupo de G. Então, $(aN)(bN) = (ab)N$, $\forall\ a, b \in G$.*

Demonstração: Seja $g \in (aN)(bN)$, onde $g = pq$, com $p \in aN$ e $q \in bN$. Assim, $p = an_1$ e $q = bn_2$, com $n_1, n_2 \in N$. Logo,

$$g = pq = (an_1)(bn_2) = (ab)(b^{-1}n_1bn_2).$$

Como N é subgrupo normal de G, então temos que $b^{-1}n_1bn_2 \in N$. Portanto, $g \in (ab)N$. Com isso, mostramos que $(aN)(bN) \subset (ab)N$. Por outro lado, seja $g \in (ab)N$. Para algum $n \in N$, temos que

$$g = (ab)n = (ae)(bn).$$

Como $ae \in aN$ e $bn \in bN$, temos que $g \in (aN)(bN)$. Portanto, $(ab)N \subset (aN)(bN)$, e o resultado segue. □

Daremos a seguir exemplos de subgrupos normais.

Exemplo 2.47 *Dado $(G, *)$ um grupo abeliano, então todo subgrupo de G é normal.*

De fato, como G é abeliano, segue que $gN = Ng$ para todo $g \in G$ e N subgrupo de G.

Exemplo 2.48 *Dado G um grupo e $Z(G)$ seu centro. Então, $Z(G)$ é um subgrupo normal de G.*

De fato, como todos os elementos de $Z(G)$ comutam com qualquer outro elemento de G. Assim, $gZ(G) = Z(G)g$ para todo $g \in G$. Logo, $Z(G)$ é normal de G.

Iremos agora construir o conceito de grupo quociente. Para isso, vamos relembrar que, dados um grupo G e uma relação de equivalência $\sim$ definida em G, o conjunto quociente $G/\sim$ nada mais é que o conjunto de todas as classes de equivalência módulo $\sim$ (veja a Definição 2.43). Para que este conjunto tenha a estrutura de grupo, vamos precisar de um aparato diferente.

Considere N um subgrupo normal de G e $\sim$ a relação tal que

$$x \sim y \Leftrightarrow xy^{-1} \in N.$$

Deixamos para o leitor a demonstração de que $\sim$ é, de fato, uma relação de equivalência. Ao conjunto $G/\sim$, damos uma nova notação, a saber, G/N. É usual escrevermos que, para $x \sim y$ em G,

$$x \equiv y \ mod \ N.$$

Neste caso, note que a classe de equivalência de um elemento $g \in G$ é dada por:

$$\begin{aligned} \overline{g} &= \{x \in G : x \equiv g \, mod \, N\} \\ &= \{x \in G : xg^{-1} \in N\} \\ &= \{x \in G : xg^{-1} = n \in N\} \\ &= \{x \in G : x = ng\} \\ &= Ng = gN, \end{aligned} \tag{2.1}$$

onde usamos o fato de N ser subgrupo normal de G. Sobre o conjunto G/N, considere a operação $\cdot$ definida por $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$. Provaremos a seguir, que o conjunto quociente G/N com a operação multiplicação é um grupo. E esse grupo é chamado grupo quociente.

Lema 2.49 *Seja G um grupo e $N \trianglelefteq G$. Então, $(G/N, \cdot)$ é um grupo.*

Demonstração: Vamos usar (2.1) e escrever a classe de um elemento $g \in G$ como gN.

i) (Associativa) Sejam a, b e $c \in G$. Pela Proposição 2.46, segue que

$$\begin{aligned}(aN \cdot bN) \cdot cN &= (ab)N \cdot cN \\ &= ((ab)c)N \\ &= (a(bc))N \\ &= aN \cdot (bc)N \\ &= aN \cdot (bN \cdot cN).\end{aligned}$$

ii) (Elemento Neutro) Afirmamos que $N = eN$ é o elemento neutro de G/N. De fato, para todo $a \in G$, novamente pela Proposição 2.46, temos que

$$(aN) \cdot (eN) = (ae)N = aN = (ea)N = (eN) \cdot (aN).$$

iii) (Elemento inverso) Para todo $a \in G$, vamos mostrar que $a^{-1}N$ é o elemento inverso de aN. Com efeito,

$$(aN) \cdot (a^{-1}N) = (aa^{-1}N) = eN = (a^{-1}a)N = (a^{-1}N) \cdot (aN).$$

Assim, provamos que (G/N, $\cdot$) é um grupo. □

Proposição 2.50 *Dados G um grupo e N um subgrupo normal de G, vale que:*

i) Se G é abeliano, então G/N é abeliano.

ii) Se G é cíclico, então G/N é cíclico.

Demonstração:

i) Sejam $aN, bN \in G/N$. Segue do fato de G ser abeliano e da Proposição 2.46 que

$$\begin{aligned}(aN) \cdot (bN) &= abN \\ &= baN \\ &= (bN) \cdot (aN).\end{aligned}$$

Portanto, G/N é abeliano.

ii) Se $G = \langle x \rangle = \{x^m : m \in \mathbb{Z}\}$. Afirmamos que o elemento xN é um gerador de G/N. Com efeito, se $aN \in G/N$, pela Proposição 2.46, temos

$$aN = x^m N = (xN)^m, \text{ para algum } m \in \mathbb{Z}.$$

Portanto, G/N é cíclico. □

Exemplo 2.51 *Sejam* $G = \mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$ *e* $H = \{\overline{0}, \overline{4}\}$. *Como os restos da divisão de qualquer inteiro por* 4 *são* $0, 1, 2$ *e* 3, *segue que as classes laterais nesse caso são:* $\overline{0} + H = H$, $\overline{1} + H$, $\overline{2} + H$ *e* $\overline{3} + H$. *Como* G *é abeliano, segue que* H *é subgrupo normal de* G. *A tabela abaixo mostra as operações no grupo quociente* G/H.

$+$	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	$\overline{3}+H$	H
$\overline{2}+H$	$\overline{2}+H$	$\overline{3}+H$	H	$\overline{1}+H$
$\overline{3}+H$	$\overline{3}+H$	H	$\overline{1}+H$	$\overline{2}+H$

Tabela 2.1: Tábua do grupo quociente G/H.

Exemplo 2.52 *Dados* $G = \{1, -1, i, -i\}$ *o grupo multiplicativo das raízes quárticas da unidade e* $N = \{1, -1\}$, *então* $G/N = \{N, iN\}$, *é um grupo, uma vez que* N *é subgrupo normal de* G, *que é abeliano.*

Exemplo 2.53 *Seja* $S_3 = \{I, \alpha, \alpha^2, \lambda, \lambda\alpha, \lambda\alpha^2\}$ *um grupo e* $N = \{I, \lambda\}$ *é um subgrupo de* S_3. *Sendo,*

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

Assim, $\alpha H = \alpha\{I, \lambda\} = \{\alpha I, \alpha\lambda\} = \{\alpha, \alpha\lambda\}$ *e* $H\alpha = \{I, \lambda\}\alpha = \{I\alpha, \lambda\alpha\} = \{\alpha, \lambda\alpha\}$. *Como as classes laterais são diferentes, tem-se que* N *não é um subgrupo normal de* S_3. *Então* S_3/N *não é um grupo.*

3

Homomorfismo de Grupos

Abordaremos nesse capítulo, a teoria de homomorfismo de grupos. Apresentaremos o Teorema de Homomorfismo, sendo esse o principal resultado deste trabalho. Este teorema nos dá uma caracterização do quociente de um grupo. Para isso, tomaremos como referência [2, 4, 6, 10, 13].

Definição 3.1 *Sejam $(G, *)$ e $(J, \circledast)$ dois grupos. Um homomorfismo de grupos é uma função $f : G \to J$, tal que, para todos $a, b \in G$, tem-se:*

$$f(a * b) = f(a) \circledast f(b).$$

Ou seja, um homomorfismo de grupo é uma função que preserva as operações dos grupos.

Definição 3.2 *Sejam $(G, *)$ e $(J, \circledast)$ grupos quaisquer. Dizemos que a função $f : G \to J$ é um epimorfismo quando f for um homomorfismo sobrejetor e um monomorfismo quando f for um homomorfismo injetor.*

Exemplo 3.3 *Sejam os grupos $(\mathbb{C}^*, \cdot)$ e $(\mathbb{R}^*_+, \cdot)$. A função*

$$\begin{aligned} f : \mathbb{C}^* &\to \mathbb{R}^*_+ \\ z &\to |z| \end{aligned}$$

é um homomorfismo de grupos. De fato, $f(z_1 \cdot z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2| = f(z_1) \cdot f(z_2)$, com $z_1, z_2 \in \mathbb{C}^*$.

Exemplo 3.4 *Se $G = \langle g \rangle = \{gm |\ m \in \mathbb{Z}\}$ é um grupo cíclico aditivo infinito, então definimos:*

$$\begin{aligned} \phi : \mathbb{Z} &\to G \\ m &\to gm. \end{aligned}$$

ϕ é um homomorfismo de grupos. De fato, $\phi(m_1 + m_2) = g(m_1 + mr_2) = gm_1 + gm_2 = \phi(m_1) + \phi(m_2)$, sendo $m_1, m_2 \in \mathbb{Z}$.

Exemplo 3.5 *Seja $\mathbb{Z}$ o grupo aditivo dois inteiros. A aplicação*

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ x &\to -2x \end{aligned}$$

é um homomorfismo de grupos, pois, $f(x+y) = -2(x+y) = -2x - 2y = (-2x) + (-2y) = f(x) + f(y)$, com $x, y \in \mathbb{Z}$.

Proposição 3.6 *Sejam $(G, *)$ e $(J, \circledast)$ dois grupos e $f : G \to J$ um homomorfismo de grupos. Então,*

i) $f(e_G) = e_J$.

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

iii) A imagem de f é um subgrupo de J.

Demonstração: *i)* Temos que

$$\begin{aligned} f(e_G) &= f(e_G * e_G) \\ &= f(e_G) \circledast f(e_G). \end{aligned}$$

Multiplicando $f(e_G)^{-1}$ em ambos os lados

$$\begin{aligned} f(e_G) * f(e_G)^{-1} &= f(e_G) \circledast f(e_G) \circledast f(e_G)^{-1} \\ e_J &= f(e_G). \end{aligned}$$

ii) Pelo item *i)*, $e_J = f(e_G) = f(a * a^{-1}) = f(a) \circledast f(a^{-1})$.
De maneira análoga, dado $a \in G$, temos

$$e_J = f(e_G) = f(a^{-1} * a) = f(a^{-1}) \circledast f(a).$$

Como o elemento inverso é único, temos que $f(a^{-1}) = f(a)^{-1}$.

iii) O conjunto imagem de f é dado por: $Im(f) = \{f(a); a \in G\}$.
Para que $Im(f)$ seja um subgrupo, devemos mostrar que:

I) $Im(f) \neq \emptyset$.

II) $a, b \in Im(f) \Rightarrow a \circledast b \in Im(f)$.

III) $b \in Im(f) \Rightarrow b^{-1} \in Im(f)$.

Temos que

I) Pelo item *i)*, $f(e_G) = e_J$. Assim $f(e_G) \in Im(f)$. Portanto, $Im(f) \neq \emptyset$.

II) Se a, $b \in Im(f)$, então existem a' e b' pertencentes a G tais que $f(a') = a$ e $f(b') = b$. Então,

$$\begin{aligned} a * b &= f(a') * f(b') \\ &= f(a' \circledast b') \in Im(f). \end{aligned}$$

III) Se $b \in Im(f)$, então existe $b' \in G$ tal que $f(b') = b$. Logo,

$$b^{-1} = (f(b'))^{-1} = f(b'^{-1}), \in Im(f).$$

Portanto, a imagem de f é um subgrupo de J. □

Mostraremos a seguir que a composição de homorfismo de grupos também é um homomorfismo.

Proposição 3.7 *Sejam $(G, *), (J, \circledast)$ e $(L, \odot)$ grupos quaisquer. Se $f : G \to J$ e $g : J \to L$ são homomorfismos de grupos, então $g \circ f : G \to L$ também é um homomorfismo de grupos.*

Demonstração: Sejam $a, b \in G$. Temos

$$g \circ f(a * b) = g(f(a * b)) = g(f(a) \circledast f(b)) = g(\, f(a)) \odot g(\, f(b)) = (g \circ f)(a) \odot (g \circ f)(b).$$

Concluímos que $g \circ f$ é um homomorfismo. □

Definição 3.8 *Sejam $(G, *)$ e $(J, \circledast)$ dois grupos e e_J o elemento neutro de J. Dado um homomorfismo de grupos $f : G \to J$, o conjunto de todos os elementos de G que tem como imagem o elemento neutro de J é denominado núcleo de f e é denotado por $N(f)$, tem-se:*

$$N(f) = \{x \in G : f(x) = e_J\}.$$

Exemplo 3.9 *Considere os grupos $(\mathbb{C}^*, \cdot)$ e $(\mathbb{R}_+^*, \cdot)$ e o homomorfismo $f : \mathbb{C}^* \to \mathbb{R}_+^*$ tal que $f(z) = |z|$. O núcleo de f é dado por:*
$N(f) = \{z \in \mathbb{C}^* | \, f(z) = 1\} = \{z \in \mathbb{C}^* | \, |z| = 1\}$, *ou seja, é o conjunto de todos os pontos de $\mathbb{C}^*$ que pertencem ao círculo unitário.*

Exemplo 3.10 *Sejam G um grupo cíclico aditivo infinito e o homomorfismo $\phi : \mathbb{Z} \to G$ definido por $\phi(m) = gm$. O núcleo de ϕ é dado por:*

$$N(\phi) = \{m \in \mathbb{Z} | \, \phi(m) = 0\} = \{m \in \mathbb{Z} | \, gm = 0\} = \{0\}.$$

Exemplo 3.11 *Sejam o grupo* $(\mathbb{Z}, +)$ *e o homomorfismo* $f : \mathbb{Z} \to \mathbb{Z}$ *tal que* $f(x) = -2x$. *Assim, o núcleo de* f *é dado por:*

$$N(f) = \{x \in \mathbb{Z} |\, f(x) = 0\} = \{x \in \mathbb{Z} |\, -2x = 0\} = \{0\}.$$

Proposição 3.12 ***(Propriedades do Núcleo)***
Sejam $(G, *)$ *e* $(J, \circledast)$ *grupos e* $f : G \to J$ *um homomorfismo de grupos. Então,*

i) N(f) é um subgrupo normal de G.

ii) f *é injetora* $\Leftrightarrow N(f) = \{e_G\}$.

Demonstração: *i)* Para provar que $N(f)$ é um subgrupo normal, necesssitamos antes mostrar que $N(f)$ é um subrupo. De fato,

i) $e_G \in N(f)$, pois pela Proposição 3.6, item *i)*, $f(e_G) = e_J$. Logo, $N(f) \neq \emptyset$.

ii) Dados $a, b \in N(f)$, então $f(a) = f(b) = e_J$. Logo,

$$f(a * b) = f(a) \circledast f(b) = e_J \circledast e_J = e_J,$$

ou seja, $a * b \in N(f)$.

iii) Para $a \in N(f)$, vale $f(a) = e_J$. Logo, $f(a^{-1}) = (f(a))^{-1} = (e_J)^{-1} = e_J$. O que mostra que $a^{-1} \in N(f)$.

Portanto, $N(f)$ é subgrupo de G.

Agora, provaremos que $N(f)$ é um subgrupo normal. Sejam $a \in N(f)$ e $g \in G$. Tem-se

$$f(g^{-1} * a * g) = f(g^{-1}) \circledast f(a) \circledast f(g) = f(g^{-1}) \circledast e_J \circledast f(g) = f(g^{-1}) \circledast f(g) = e_J.$$

Logo, $(g^{-1} * a * g) \in N(f)$. Segue que $N(f)$ é um subgrupo normal.

ii) f é injetora $\Leftrightarrow N(f) = \{e_G\}$.

Suponhamos que f é injetora e vamos provar que $N(f) = e_J$. Se $a \in N(f)$, então $f(a) = e_J$. Pela Proposição 3.6, item *i)*, temos que $e_J = f(e_G)$. Como por hipótese, f é injetora, segue que $a = e_G$. Portanto, $N(f) = \{e_G\}$. Reciprocamente, suponhamos que $N(f) = \{e_G\}$, vamos provar que f é injetora. Sejam $a, b \in G$, tal que $f(a) = f(b)$. Assim,

$$f(a * b^{-1}) = f(a) \circledast f(b^{-1}) = f(a) \circledast f(b)^{-1} = f(a) \circledast f(a)^{-1} = e_J.$$

Então, $a * b^{-1} \in N(f)$. Como $N(f) = \{e_G\}$, segue que $a * b^{-1} = e_G$. Então, $a = b$. Portanto, f é injetora. □

Exemplo 3.13 *O homomorfismo $f : \mathbb{Z} \to \mathbb{Z}$, definido por $f(x) = 2x$, é injetor, pois $N(f) = \{0\}$. Assim, f é um monomorfismo.*

Exemplo 3.14 *G é um grupo cíclico infinito. A função $f : \mathbb{Z} \to G$, definida por $f(m) = gm$ é um homomorfismo injetor, pois $N(f) = \{0\}$. Portanto, f é um monomorfismo.*

3.1 Isomorfismo de Grupos

Estudar isomorfismo de grupos é de fundamental importância para teoria de grupos. Se existe um isomorfismo entre dois grupos, dizemos que esses grupos são isomorfos. Algebricamente falando, é o mesmo que dizer que eles possuem as mesmas propriedades e não é preciso fazermos distinção entre eles.

Definição 3.15 *Sejam dois grupos $(G, *)$ e $(J, \circledast)$ e $f : G \to J$ um homomorfismo de grupos. Dizemos que f é um isomorfismo de grupos se f for um homomorfismo bijetor. Nesse caso, os grupos $(G, *)$ e $(J, \circledast)$ são ditos isormofos e escrevemos $G \simeq J$.*

Exemplo 3.16 *Os grupos $(\mathbb{R}, +)$ e $(\mathbb{R}_+^*, \cdot)$ são grupos isomorfos, pois a função $f : \mathbb{R} \to \mathbb{R}_+^*$ definida por $f(x) = e^x$ é um isomorfismo de grupos.*

Exemplo 3.17 *Sejam os grupos $(\mathbb{R}_+^*, \cdot)$ e $(\mathbb{R}, +)$. A aplicação $f : \mathbb{R}_+^* \to \mathbb{R}$ definida por $f(x) = log(x)$ é um isomorfismo.*

Proposição 3.18 *Sejam $(G, *)$ e $(J, \circledast)$ dois grupos e $f : G \to J$ um isomorfismo de grupos. Então, $f^{-1} : J \to G$ é um isomorfismo de grupos.*

Demonstração: Devemos mostar que f^{-1} é um homomorfismo bijetor. De fato, como f é bijeção, segue que f^{-1} é também bijeção. Resta mostrar que f^{-1} é um homomorfismo de grupos. Para $a, b \in J$, existem $a', b' \in G$ tais que $a = f(a')$ e $b = f(b')$. Então,

$$f^{-1}(a \circledast b) = f^{-1}(f(a') \circledast f(b')) = f^{-1}(f(a' * b')) = a' * b' = f^{-1}(a) * f^{-1}(b).$$

Portanto, f^{-1} é um isomorfismo. □

Definição 3.19 *Seja $(G,*)$ um grupo. Um isomorfismo $f : G \to G$ é chamado automorfismo de G.*

Exemplo 3.20 *Considere o grupo $(\mathbb{R},+)$. A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 3x$ é um automorfismo.*

O Teorema a seguir, mostra a importância de se estudar os grupos de simetria S_n. Ele diz que todos os grupos finitos são, essencialmente, um subgrupo de S_n.

Teorema 3.21 (Cayley) *Sejam $(G,*)$ um grupo finito, $S_n = \{\sigma : G \to G; \sigma$ é uma bijeção$\}$ e $(S_n, \circ)$ o grupo das bijeções de G. Então, G é isomorfo a um subgrupo de S_n.*

Demonstração: Seja $a \in G$ e considere

$$\begin{aligned} \Psi_a : G &\to G \\ x &\to a * x. \end{aligned}$$

Mostraremos que Ψ_a é uma bijeção, ou seja, que é injetora e sobrejetora. De fato, sejam $x, y \in G$ tais que $\Psi_a(x) = \Psi_a(y)$. Então, $a * x = a * y$, o que implica em $x = y$ e mostra que Ψ_a é injetora. Agora, vamos mostrar que Ψ_a é sobrejetora. Dado $b \in G$, tome $x = a^{-1} * b$. Então,

$$\Psi_a(x) = a * (a^{-1} * b) = b.$$

Isso mostra que Ψ_a é sobrejetora e, como ela é também injetora, segue que $\Psi_a \in S_n$.

Considere agora a função $\sigma : G \to S_n$ definida por $\sigma(a) = \Psi_a$. Afirmamos que σ é um homomorfismo injetor. Com efeito, dados $a, b, x \in G$, temos que

$$\Psi_{a*b}(x) = (a * b) * (x) = a * (b * x) = \Psi_a(\Psi_b(x)) = (\Psi_a \circ \Psi_b)(x), \forall\ x \in G.$$

Assim, $\Psi_{a*b} = \Psi_a \circ \Psi_b$ e, portanto, $\sigma(a * b) = \sigma(a) \circ \sigma(b)$, isto é, a função σ é um homomorfismo. Agora, provaremos que σ é injetora. De fato, note que, se $a \in N(\sigma)$, então $\sigma(a) = e_{S_n} = Id$. Ou seja, $a * x = x$ para todo $x \in G$ e, portanto, multiplicando à direita em ambos os lados por x^{-1}, segue que $a = e$. Em outras palavras, o núcleo de σ tem apenas o elemento e. Isto mostra que σ é injetiva, como havíamos afirmado. Pela Proposição 3.6, item *iii)*, a imagem de σ é um subgrupo de S_n que, neste caso, é isomorfo a G. □

A seguir, apresentaremos o resultado principal deste trabalho: O Teorema do Homomorfismo. Essencialmente, ele caracteriza o quociente do domínio com o núcleo do homomorfismo.

Teorema 3.22 *Seja $f : A \to B$ um homomorfismo de grupos. Então, $A/N(f) \simeq Im(f)$.*

Demonstração: Seja $N = N(f)$ e considere $\overline{f} : A/N \to Im(f)$ definida por $\overline{f}(aN) = f(a)$. Mostraremos primeiro que $\overline{f}$ está bem definida. De fato, se $aN = bN$ com $a, b \in N$, temos que mostrar que $\overline{f}(aN) = \overline{f}(bN)$. Ora, isso vale se, e somente se, $f(a) = f(b)$ que, por sua vez, vale apenas se $f^{-1}(b)f(a) = e$. Como f é um homomorfismo, esta última igualdade vale só quando $f(b^{-1}a) = e$, isto é, só quando $b^{-1}a \in N$. Isto é verdade, uma vez que $a, b \in N$. Logo, $\overline{f}$ está bem definida e não depende da escolha de seus representantes. Provaremos, agora, que $\overline{f}$ é isomorfismo, e para isso, vamos mostrar que:

i) $\overline{f}$ é homomorfismo.

ii) $\overline{f}$ é injetora.

iii) $\overline{f}$ é sobrejetora.

Desse modo,

i) Para $aN, bN \in A/N$, temos da Proposição 2.46 que

$$\begin{aligned}\overline{f}(aN \cdot bN) &= \overline{f}(abN)\\ &= f(ab)\\ &= f(a) \cdot f(b)\\ &= \overline{f}(aN) \cdot \overline{f}(bN).\end{aligned}$$

Portanto, $\overline{f}$ é um homomorfismo.

ii) Vamos mostrar que o núcleo de $\overline{f}$ possui apenas o elemento neutro. Se $aN \in N(\overline{f})$, então $\overline{f}(aN) = e$, isto é, $f(a) = e$. Portanto, $a \in N$. Assim, $aN = N$ é o único elemento do conjunto $N(\overline{f})$. Logo, $\overline{f}$ é injetora.

iii) Sejam $b \in Im(f)$ e $a \in A$, tais que $f(a) = b$. Tomamos, então, a classe aN em A/N para a qual $\overline{f}(aN) = f(a) = b$. Isso mostra que $\overline{f}$ é sobrejetora.

Portanto, $\overline{f}$ é um isomorfismo e $A/N(f) \simeq Im(f)$. □

Apresentaremos alguns exemplos de como se aplica o Teorema do Homomorfismo.

Exemplo 3.23 *Sejam $G = (\mathbb{R}^*, \cdot)$ e $N = (\mathbb{R}_+, \cdot)$. Considere $f : G \to N$ definida por $f(x) = x^2$. Mostre que $G/N(f) \simeq Im(f)$.*

Demonstração:

i) Provaremos primeiro que f é um homomorfismo. Com efeito,

$$\begin{aligned} f(x \cdot y) &= (x \cdot y)^2 \\ &= x^2 \cdot y^2 \\ &= f(x) \cdot f(y). \end{aligned}$$

Logo, f é um homomorfismo.

ii) Afirmamos que f não é injetora. De fato, $f(x) = 1$ se, e somente se, $x^2 = 1$, ou seja, $x = 1$ ou $x = -1$. Logo, $N(f) = \{1, -1\}$, mostrando que f não é injetora.

iii) Afirmamos que f é sobrejetora. Para provar isso, seja $b \in N$. Tomando $\sqrt{b} \in G$, segue que $f(\sqrt{b}) = (\sqrt{b})^2 = b$. Logo, f é sobrejetora.

Pelo Teorema do Homomorfismo, $G/N(f) \simeq Im(f)$. □

Exemplo 3.24 *Seja* $G = (\mathbb{C}^*, \cdot)$ *e seja* $N = \{a + bi \in \mathbb{C}^* : a^2 + b^2 = 1\}$. *Mostre que* $G/N \simeq \mathbb{R}_+^*$.

Demonstração: Seja f a função definida por

$$\begin{aligned} f : \mathbb{C}^* &\to \mathbb{R}_+^* \\ z &\to |z|. \end{aligned}$$

i) Pelo o exemplo 3.3, f é um homomorfismo.

ii) Vamos encontrar o núcleo de f. Para isso, seja $z = a + bi \in \mathbb{C}^*$. Tem-se que $f(z) = 1$ se, e somente se, $|z| = 1$. Ou seja, os elementos do núcleo de f são tais que $a^2 + b^2 = 1$.

iii) Claramente f é sobrejetora. Assim, $Im(f) = \mathbb{R}_+^*$.

Portanto, pelo teorema do homomorfismo, $\mathbb{C}^*/N \simeq \mathbb{R}_+^*$. □

4 Considerações Finais

Este trabalho teve como intuito mostrar parte da teoria de grupos, com ênfase em homomorfismo de grupos, tendo como parte fundamental enunciar e demonstrar o Teorema do Homomorfismo, que nos possibilita caracterizar o quociente do domínio com o núcleo do homomorfismo. Apesar de ser um estudo inicial, nos proporcionou abordar os principais conceitos e ainda aplicar o Teorema do Homomorfismo através de exemplos. Vimos também, através do Teorema de Cayley, que todo grupo finito é isomorfo a um subgrupo de S_n, mostrando o quanto é importante o estudo desse grupo que tem aplicações em diversas áreas do conhecimento. Um exemplo, seria a manipulação do cubo mágico, que usa a teoria de permutações.

Além disso, me possibilitou a oportunidade de aprimorar os meus conhecimentos sobre Álgebra Abstrata que é uma área na qual tive afinidade no curso. Foi uma chance de aprofundar o estudo já iniciado como bolsista de um projeto de extensão realizado no Curso de Matemática, intitulado Projeto Galois, além de servir como base para uma possível pós-graduação na área da Matemática Pura.

Referências Bibliográficas

[1] ANDRANDE, Lenimar N. **Introdução à Álgebra**. Disponível em: < http://www.ebah.com.br/content/ABAAAArqQAE/introducao-a-algebra>. Acesso em: 05 set. 2016.

[2] BEDOYA, Hernando; CAMELIER, Ricardo. **Álgebra II**. Rio de Janeiro: Fundação CECIERJ, 2010. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwidgISYoLLQAhWBEZAKHYdODgwQFggxMAM&url=http%3A%2F%2Fteca.cecierj.edu.br%2FpopUpVisualizar.php%3Fid%3D45669%26urlArquivo%3D..%2Farquivo%2Fdocumento%2F45669.pdf&usg=AFQjCNERl6cmlk1WA9gZzAxuuzzgDGW6nA&bvm=bv.139250283%2Cd.Y2I> . Acesso em: 05 out. 2016.

[3] DOMINGUES, Hygino H; EZZI, Gelson. **Álgebra Moderna**. 2 ed. São Paulo: Atual, 1982.

[4] DOMINGUES, Hygino H; EZZI, Gelson. **Álgebra Moderna**. 4 ed. São Paulo: Atual, 2003.

[5] DOURADO, Thiago A. S. **Elementos de Teoria dos Grupos**. 2009. 114f. Monografia (Bacharel em Matemática) - Universidade Federal de Mato Grosso do Sul, Três Lagoas, 2009. Disponível em: < http://www.ebah.com.br/content/ABAAAfPwYAE/elementos-teoria-dos-grupos-thiago-a-s-dourado> . Acesso em: 10 agos. 2016.

[6] GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**. 2 ed. Rio de Janeiro: IMPA, 2003.

[7] GONÇALVES, Adilson. **Introdução à Álgebra**. 5 ed. Rio de Janeiro: IMPA, 2003.

[8] HERSTEIN, I. N. **Tópicos de Álgebra**. Tradução: Adalberto P. Bergamasco e L.H. Jacy Monteiro. São Paulo: Polígono, 1970. (Topics in Algebra, 1964).

[9] NACHBIN, Leopoldo. **Introdução à Álgebra**. 1 ed. Rio de Janeiro: Mc GRAW-HILL do Brasil, 1971.

[10] SILVA, Marco A. **Grupos Finitos**. 2002. 73f. Monografia (Habilitação Licenciatura) - Universidade Federal de Santa Catarina, Florianópolis, 2002. Disponível em: < https://repositorio.ufsc.br/bitstream/handle/123456789/97162/MarcoAntoniodaSilva.PDF?sequence=1> . Acesso em: 03 set. 2016.

[11] SIMIS, Aron. **Introdução à Álgebra**. 2. ed. Rio de Janeiro: IMPA 1997. Disponível em: < http://www.impa.br/opencms/pt/biblioteca/mono/Mon23.pdf> . Acesso em: 07 mar. 2016.

[12] UNIVERSIDADE FEDERAL DO TOCANTINS. **Manual para Elaboração e Normalização de Trabalhos de Conclusão de Curso do Campus de Araguaína.** Araguaína: UFT, 2011.

[13] VILLELA, Maria L. T. **Grupos**. Disponível em: <http://www.professores.uff.br/marco/algebraII-2014/grupos-mod1.pdf>. Acesso em: 10 out. 2016.