



Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Câmpus Valparaíso
Licenciatura em Matemática

CURSO DE LICENCIATURA EM MATEMÁTICA

O TEOREMA DA CORRESPONDÊNCIA DE GRUPOS

MIKÉIAS CARVALHO DE LIMA

VALPARAÍSO DE GOIÁS

2024



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
SISTEMA INTEGRADO DE BIBLIOTECAS

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

- | | |
|--|---|
| ☐ Tese | ☐ Artigo Científico |
| ☐ Dissertação | ☐ Capítulo de Livro |
| ☐ Monografia – Especialização | ☐ Livro |
| ☒ TCC - Graduação | ☐ Trabalho Apresentado em Evento |
| ☐ Produto Técnico e Educacional - Tipo: _____ | |

Nome Completo do Autor: Mikéias Carvalho de Lima

Matrícula: 20191150040341

Título do Trabalho: O Teorema da Correspondência de Grupos

Autorização - Marque uma das opções

1. (**X**) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. () Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ____/____/____ (Embargo);
3. () Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

- () O documento está sujeito a registro de patente.
() O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
() Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

- i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Valparaíso de Goiás, 16/10/2024.
Local Data

Mikéias Carvalho de Lima

Assinatura do Autor e/ou Detentor dos Direitos Autorais

MIKÉIAS CARVALHO DE LIMA

O TEOREMA DA CORRESPONDÊNCIA DE GRUPOS

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal de Goiás - IFG - Câmpus Valparaíso, como requisito parcial para obtenção do título de Licenciada em Matemática.

Orientador: Bruno de Paula Miranda

Co-orientadora: Lucimeire Alves de Carvalho

VALPARAÍSO DE GOIÁS

2024

Dados Internacionais de Catalogação na Publicação (CIP)

L732t Lima, Mikéias Carvalho de

O teorema da correspondência de grupos [recurso eletrônico]
/ Mikéias Carvalho de Lima. -- 2024.
Dados eletrônicos (1 arquivo).
29 f. : il.

Orientador: Prof. Dr. Bruno de Paula Miranda.
Trabalho de conclusão de curso (Licenciatura em Matemática)
- Instituto Federal de Educação, Ciência e Tecnologia de
Goiás, câmpus Valparaíso, 2024.
Modo de acesso: World Wide Web.
Arquivo de texto em formato PDF.
Disponível em: <https://repositorio.ifg.edu.br>.

1. Álgebra. 2. Teoria dos grupos. 3. Isomorfismos
(Matemática). I. Título. II. Miranda, Bruno de Paula, orient.

CDD 512



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS
CÂMPUS VALPARAÍSO

Termo de Aprovação

MIKEIAS CARVALHO DE LIMA

O TEOREMA DA CORRESPONDÊNCIA DE GRUPOS

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Valparaíso de Goiás, como parte dos requisitos para a obtenção do título de Licenciado em Matemática.

Monografia defendida e aprovada em 23 de setembro de 2024 pela banca examinadora constituída pelos seguintes membros:

BANCA EXAMINADORA

Prof. Dr. Bruno de Paula Miranda
Presidente da banca / Orientador
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Hércules de Carvalho Bezerra
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Me. Renno Santos Guedes
Universidade Estadual de Montes Claros

Valparaíso de Goiás – GO

2024

Documento assinado digitalmente



RENNO SANTOS GUEDES
Data: 24/09/2024 15:10:35-0300
Verifique em <https://validar.iti.gov.br>

Documento assinado eletronicamente por:

- Hércules de Carvalho Bezerra, PROF ENS BAS TEC TECNOLÓGICO-SUBSTITUTO, em 24/09/2024 14:36:56.
- Bruno de Paula Miranda, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 24/09/2024 14:28:30.

Este documento foi emitido pelo SUAP em 23/09/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifg.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 567449
Código de Autenticação: 69b8c7a79b



Instituto Federal de Educação, Ciência e Tecnologia de Goiás

BR 040, KM 6, Avenida Saia Velha, S/Nº, Área 8, None, Parque Esplanada V, VALPARAÍSO DE GOIÁS / GO, CEP 72876-601
Sem Telefones cadastrados

Agradecimentos

Agradeço, primeiramente, à minha família, por todo o apoio e suporte, especialmente à minha mãe, Liliane, que esteve ao meu lado em cada etapa desta jornada, oferecendo sempre incentivo e motivação.

Aos amigos que fiz ao longo do curso, com uma menção honrosa a Gabriel Lucas, Diogo Alves e Jordanna Maria, pela parceria e pelas muitas experiências compartilhadas que tornaram essa trajetória mais leve e divertida.

Aos professores que me incentivaram e ajudaram a moldar o meu caminho acadêmico, destaco meu orientador Bruno de Paula Miranda, cuja orientação e dedicação foram essenciais para a conclusão deste trabalho. Agradeço também à professora Lucimeire Alves de Carvalho, que despertou meu interesse pelo tema escolhido e me guiou nos primeiros passos deste projeto.

Por fim, sou imensamente grato pela oportunidade de ter cursado o ensino superior em uma instituição pública, o Instituto Federal de Goiás. É um privilégio poder fazer parte de uma instituição que valoriza o conhecimento e oferece educação de qualidade.

Resumo

O Teorema da Correspondência de Grupos é um dos pilares fundamentais na teoria dos grupos, uma área central da álgebra abstrata. Este trabalho tem como objetivo principal explorar e apresentar uma compreensão detalhada do Teorema da Correspondência, abordando conceitos essenciais como homomorfismos de grupos, subgrupos normais, e grupos quociente. Inicialmente, são introduzidos os conceitos básicos de grupos abelianos e não abelianos, seguidos por uma análise aprofundada dos homomorfismos de grupos e suas propriedades. Em seguida, o Teorema de Lagrange é discutido, estabelecendo a base para a introdução dos subgrupos normais e dos grupos quociente. O trabalho culmina na demonstração e aplicação do Teorema da Correspondência, destacando sua importância teórica e prática. A pesquisa foi fundamentada em uma extensa revisão bibliográfica, utilizando fontes renomadas na área de matemática. Os resultados obtidos reforçam a relevância do Teorema da Correspondência na estrutura da teoria dos grupos e sua aplicabilidade em diversas áreas da matemática.

Palavras-chave: Teorema da Correspondência. Teoria dos Grupos. Homomorfismos de Grupos. Subgrupos Normais. Grupos Quociente.

Abstract

The Correspondence Theorem for Groups is one of the fundamental pillars in group theory, a central area of abstract algebra. This paper aims to explore and present a detailed understanding of the Correspondence Theorem, covering essential concepts such as group homomorphisms, normal subgroups, and quotient groups. Initially, the basic concepts of abelian and non-abelian groups are introduced, followed by an in-depth analysis of group homomorphisms and their properties. Next, Lagrange's Theorem is discussed, establishing the basis for the introduction of normal subgroups and quotient groups. The paper culminates in the demonstration and application of the Correspondence Theorem, highlighting its theoretical and practical importance. The research is based on an extensive literature review, utilizing renowned sources in the field of mathematics. The results obtained reinforce the relevance of the Correspondence Theorem in the structure of group theory and its applicability in various areas of mathematics.

Keywords: Correspondence Theorem. Group Theory. Group Homomorphisms Normal Subgroups. Quotient Groups.

Sumário

Introdução	1
1 Grupos	2
1.0.1 Exemplos de Grupos Abelianos	3
1.0.2 Exemplos de Grupos não Abelianos	4
1.1 Homomorfismo de grupos	7
1.2 Subgrupos	9
1.3 O Teorema de Lagrange	14
1.4 Subgrupos Normais e Grupo Quociente	16
2 Teoremas de isomorfismo de grupos e Teorema da correspondência	21
Conclusão	28
Referências Bibliográficas	29

Introdução

A teoria dos grupos é uma área central da matemática moderna, com aplicações em várias disciplinas, como física quântica, química e álgebra abstrata. Inicialmente desenvolvida para resolver equações polinomiais, a teoria dos grupos se expandiu e passou a influenciar diversos campos científicos. Com essa base, o estudo dos grupos nos leva a explorar estruturas mais complexas e suas inter-relações.

O conceito de grupo, introduzido por Évariste Galois no início do século XIX, revolucionou a álgebra ao estabelecer uma nova perspectiva sobre a solubilidade de equações. Ao longo dos anos, a teoria dos grupos se dividiu em várias subáreas, cada uma com seus próprios problemas e aplicações, consolidando-se como uma ferramenta essencial na modelagem de sistemas com simetrias e na compreensão das estruturas matemáticas.

Neste trabalho, focaremos especificamente no Teorema da Correspondência de Grupos, um dos resultados mais profundos e úteis dessa teoria. Esse teorema estabelece uma relação entre os subgrupos de um grupo e os subgrupos de um grupo quociente, proporcionando uma compreensão mais detalhada das estruturas internas dos grupos. Para isso, começaremos revisando conceitos básicos, como homomorfismos, subgrupos normais e grupos quociente, que são fundamentais para a compreensão e aplicação do teorema.

A relevância do Teorema da Correspondência não se limita apenas ao campo teórico, mas também abrange diversas áreas aplicadas da matemática, onde a análise da estrutura dos grupos e suas propriedades é essencial. Através de uma análise aprofundada e de demonstrações rigorosas, este trabalho busca não só apresentar o teorema em detalhes, mas também explorar suas implicações e aplicações.

Capítulo 1

Grupos

A Teoria de Grupos é uma área fundamental da matemática que estuda conjuntos de elementos que, combinados por uma operação, seguem regras específicas. Essa teoria nos permite entender simetrias e padrões em várias áreas do conhecimento. Neste capítulo, daremos os primeiros passos nesse estudo, apresentando definições, exemplos, teoremas e resultados fundamentais sobre Grupos. Começaremos discutindo a definição e exemplos de grupos, tanto abelianos quanto não abelianos, antes de avançarmos para tópicos mais específicos como homomorfismos e subgrupos, que serão essenciais para a demonstração do Teorema da Correspondência de Grupos.

Definição 1. Um grupo é um conjunto não vazio G com uma operação binária, denotada inicialmente por $(*)$, que satisfaz as seguintes propriedades. No entanto, para fins de simplicidade, adotaremos a notação multiplicativa $(\cdot)$ para essa operação.

Fechamento: Para todo $a, b \in G$, o resultado da operação $a \cdot b$ também pertence a G .

Associatividade: Para todos $a, b, c \in G$, vale

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Elemento neutro: Existe um elemento $e \in G$ tal que, para todo $a \in G$,

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

Esse elemento é chamado de elemento neutro ou identidade e é usualmente denotado por

$e = 1$, no contexto de grupo multiplicativo, $e = 0$ para grupo aditivo.

Inverso: Para todo $a \in G$, existe um elemento $b \in G$ tal que

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

Esse elemento b é chamado de elemento inverso de a e denotado por a^{-1} .

No caso de, além das propriedades acima, a operação do grupo satisfizer a comutatividade, isto é,

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

dizemos que G é um **Grupo Abelian**.

1.0.1 Exemplos de Grupos Abelianos

Exemplo 1.0.1. O conjunto $\mathbb{Z}$ dos números inteiros, com a operação de adição $(+)$, forma um grupo abeliano. Claramente, o elemento neutro é o número 0 e, dado um inteiro m , seu inverso é o inteiro $-m$.

Exemplo 1.0.2. Analogamente, o conjunto $2\mathbb{Z}$ dos números inteiros pares com a operação de adição $(+)$ herdada dos inteiros forma um grupo abeliano.

Exemplo 1.0.3. O conjunto $\mathbb{R}^*$ dos números reais não nulos com a operação de multiplicação $(\cdot)$ forma um grupo abeliano. O elemento neutro é o número 1. Dado um real não nulo x , seu inverso é o real x^{-1} .

Exemplo 1.0.4. O conjunto $G = \{1, -1\}$ com a operação de multiplicação herdada dos reais $(\cdot)$ forma um grupo abeliano.

Exemplo 1.0.5. Para cada inteiro positivo n , o conjunto

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

das classes de equivalência da relação de congruência módulo n , com a operação soma definida por

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

forma um grupo abeliano. O elemento neutro é $\bar{0}$. Dado $\bar{a} \in \mathbb{Z}_n$, temos que seu inverso é $\overline{n - a}$.

Exemplo 1.0.6. Seja n um número primo. O conjunto $\mathbb{Z}_n^*$ é o conjunto dos inteiros $\{1, 2, \dots, n-1\}$ com a operação de multiplicação módulo n . Ou seja, tomamos os inteiros de 1 a $n-1$, e multiplicamos seus representantes, tomando o resto da divisão por n .

Exemplo 1.0.7. Seja $n \in \mathbb{N}$, o Grupo das unidades de $\mathbb{Z}_n$, denotado por $U(\mathbb{Z}_n)$, é composto por todos os elementos de $\mathbb{Z}_n$ que admitem inverso multiplicativo. Isto é,

$$\begin{aligned}\bar{a} \in U(\mathbb{Z}_n) &\iff \exists b \in \mathbb{Z} \text{ tal que } a \cdot b \equiv 1 \pmod{n} \\ &\iff \bar{a} \cdot \bar{b} = \bar{1}.\end{aligned}$$

Isto é, se $a \in \mathbb{Z}$, $\bar{a}$ será elemento de $U(\mathbb{Z}_n)$ se, e somente se, a e n forem coprimos, isto é, $\text{mdc}(n, a) = 1$. Lembre-se que a função ϕ de Euler é a função que para cada natural n retornar $\phi(n)$ o número de naturais menores que n e relativamente primos com n . Em particular, temos que o número de elementos em $U(\mathbb{Z}_n)$ é precisamente $\phi(n)$.

Agora que discutimos os grupos abelianos, que possuem a propriedade comutativa, vamos explorar os grupos não abelianos, onde a ordem das operações influencia o resultado, trazendo estruturas e aplicações mais complexas.

1.0.2 Exemplos de Grupos não Abelianos

Exemplo 1.0.8. Seja $n \in \mathbb{N}$ e consideremos S_n o conjunto das bijeções $\sigma : I_n \rightarrow I_n$, onde

$$I_n = \{1, 2, \dots, n\}.$$

Este conjunto, munido da operação de composição de funções, forma um grupo. Obviamente, o número de elementos em S_n é $n!$ (o número de permutações de n elementos), o elemento neutro e é a função identidade. Dado $\sigma \in S_n$, temos que seu inverso é a função inversa de σ (que existe, pois σ é uma bijeção).

Seja j um elemento de I_n e α um elemento do conjunto S_n . Dizemos que α fixa j se a

imagem de j por α é o próprio j (ou seja, $\alpha(j) = j$). Por outro lado, dizemos que α *move* j se a imagem de j por α é diferente de j (ou seja, $\alpha(j) \neq j$).

Sejam $i_1, i_2, \dots, i_r$ inteiros distintos entre 1 e n . Dizemos que $\alpha \in S_n$ é um *r-ciclo* se

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1$$

e α fixa os $n - r$ elementos restantes de I_n . Também dizemos que α é um ciclo de *comprimento* r . Denotamos α por $(i_1, i_2, \dots, i_r)$. Chamamos de **transposição** qualquer 2-ciclo de S_n , isto é, permutações que só trocam dois números de lugar.

Por exemplo, consideremos o grupo S_4 , que contém todas as permutações possíveis de 4 elementos distintos $\{1, 2, 3, 4\}$. O 3-ciclo $(1, 4, 3)$ é a permutação $\alpha \in S_4$ que satisfaz

$$\alpha(1) = 4, \alpha(2) = 2, \alpha(3) = 1, \alpha(4) = 3.$$

Já o 4-ciclo $(1, 3, 2, 4)$ é a permutação $\beta \in S_4$ que satisfaz

$$\alpha(1) = 3, \alpha(2) = 4, \alpha(3) = 2, \alpha(4) = 1.$$

Denotamos simplesmente por $(1) = (j)$, $j \in I_n$ o elemento neutro de S_n .

A notação de ciclos é vantajosa para se visualizar as permutações e facilitar o cálculo de operações. Por exemplo, se temos $\alpha, \beta \in S_4$ como acima, valerá (operamos da direita para a esquerda)

$$\alpha \circ \beta = (1, 4, 3) \circ (1, 3, 2, 4) = (1)(2, 3)(4) = (2, 3)$$

enquanto

$$\beta \circ \alpha = (1, 3, 2, 4) \circ (1, 4, 3) = (1)(2, 4)(3) = (2, 4).$$

Em particular, notamos que S_4 é um grupo não abeliano! em realidade, isso é verdade para todo S_n maior ou igual a 3.

Dizemos que duas permutações $\alpha, \beta \in S_n$ são **disjuntas** se todo elemento movido por α é fixo em β , e vice-versa. Simbolicamente: se

$$\alpha(j) \neq j \implies \beta(j) = j$$

e

$$\beta(l) \neq l \implies \alpha(l) = l.$$

Claramente pode haver elementos $j \in S_n$ tais que $\alpha(j) = j = \beta(j)$. Uma família de permutações $\alpha_1, \alpha_2, \dots, \alpha_m$ é **disjunta** se cada par delas é disjunto. É sabido que toda permutação $\alpha \in S_n$ é um ciclo ou um produto de ciclos disjuntos.

Exemplo 1.0.9. Neste exemplo, destrincharemos o conjunto S_3 das permutações de 3 elementos $\{1,2,3\}$ apresentando sua tabela de multiplicação, isto é, avaliando $\alpha \circ \beta$ para todos $\alpha, \beta \in S_3$. Primeiramente, notemos que na notação de ciclos temos

$$S_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}.$$

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Note que a tabela de multiplicação apresentada não é simétrica em relação à diagonal principal.

Exemplo 1.0.10. O conjunto $GL_2(\mathbb{R})$ das matrizes 2×2 inversíveis (determinante não nulo) com entradas reais, sob a operação de multiplicação de matrizes, forma um grupo. O elemento neutro claramente é a matriz identidade. E dada uma matriz $A \in GL_2(\mathbb{R})$, temos que sua matriz inversa A^{-1} atua como inverso de A enquanto elemento do grupo. Note que

$$\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$$

enquanto

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 2 \end{pmatrix}$$

e temos que o grupo é não abeliano.

Compreendemos as distinções fundamentais entre grupos abelianos e não abelianos. Agora, para entendermos como esses grupos se relacionam e como suas propriedades podem ser comparadas, introduziremos o conceito de homomorfismo.

1.1 Homomorfismo de grupos

Definição 2. Uma aplicação ϕ de um grupo $(G, \cdot)$ em um grupo $(\overline{G}, \times)$ é dita um *homomorfismo* se para todos $a, b \in G$, vale

$$\phi(a \cdot b) = \phi(a) \times \phi(b).$$

Usualmente, não explicitamos as operações dos grupos e simplesmente escrevemos

$$\phi(ab) = \phi(a)\phi(b).$$

Definição 3. Seja $f : G \rightarrow \overline{G}$ um homomorfismo de grupos. Então, f mapeia o elemento neutro de G , denotado por e_G , para o elemento neutro de $\overline{G}$, denotado por $e_{\overline{G}}$. Em outras palavras, temos a seguinte propriedade fundamental de homomorfismos:

$$f(e_G) = e_{\overline{G}}.$$

Definição 4. Um **isomorfismo** é um homomorfismo que também é uma bijeção. Dizemos que G é **isomorfo** a $\overline{G}$, denotando por $G \cong \overline{G}$, se existe um isomorfismo $\phi : G \rightarrow \overline{G}$.

Exemplo 1.1.1. Seja $\mathbb{Z}$ o grupo dos inteiros com a operação de adição e seja $\overline{G} = 2\mathbb{Z}$. Para o inteiro $x \in \mathbb{Z}$, definimos ϕ por $\phi(x) = 2x$. Resulta de $\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y)$ e concluímos que ϕ é um homomorfismo de G em $\overline{G}$.

Exemplo 1.1.2. Seja G o grupo dos números reais não nulos com a operação de multiplicação, $\overline{G} = \{1, -1\}$. Definimos $\phi : G \rightarrow \overline{G}$ por $\phi(x) = 1$ se x é positivo e $\phi(x) = -1$ se x é negativo. O fato de que ϕ é um homomorfismo é equivalente às afirmações: positivo vezes positivo resulta positivo, positivo vezes negativo resulta negativo, negativo vezes negativo resulta positivo.

Exemplo 1.1.3. Seja G o grupo dos inteiros com a operação de adição, seja $\mathbb{Z}_n$ o grupo dos inteiros com a operação de adição módulo n . Definamos ϕ por $\phi(x) = \overline{x}$. Pode-se verificar facilmente que ϕ é um homomorfismo.

Exemplo 1.1.4. Neste exemplo, demonstraremos que os grupos $G = \{-1, 1\}$ e $\mathbb{Z}_2$ são isomorfos. Para tal, apresentaremos um isomorfismo entre os grupos.

Consideremos os grupos $G = \{-1, 1\}$ e $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, ambos com operação de multiplicação. Um isomorfismo entre esses grupos pode ser definida por:

$$f(x) = \begin{cases} \overline{0}, & \text{se } x = 1; \\ \overline{1}, & \text{se } x = -1 \end{cases}$$

Verificação das Propriedades do Isomorfismo:

Preservação da Operação: Analisamos os casos possíveis:

$$f(1 \cdot 1) = f(1) = \overline{0} = \overline{0} + \overline{0} = f(1) + f(1).$$

$$f(1 \cdot (-1)) = f(-1) = \overline{1} = \overline{0} + \overline{1} = f(1) + f(-1).$$

$$f((-1) \cdot (-1)) = f(1) = \overline{0} = \overline{1} + \overline{1} = f(-1) + f(-1).$$

Em todos os casos, a igualdade $f(a \cdot b) = f(a) + f(b)$ é satisfeita.

Injetividade: A função f é injetora, pois para cada elemento em $2\mathbb{Z}$ há apenas um pre-imagem em G . Por exemplo, se $f(x) = 1$, então x só pode ser 1 em G .

Sobrejetividade: A função f é sobrejetora, pois todo elemento em $2\mathbb{Z}$ tem pelo menos uma pre-imagem em G . Por exemplo, o elemento 1 em $2\mathbb{Z}$ pode ter como pre-imagem 1 ou -1 em G .

Entendido o papel dos homomorfismos na preservação da estrutura dos grupos, voltamos nossa atenção para os subgrupos. Esses subconjuntos são fundamentais para a análise da estrutura interna dos grupos, permitindo a decomposição e estudo detalhado das propriedades dos grupos maiores.

1.2 Subgrupos

Definição 5. Seja G um grupo e H um subconjunto não vazio de G . Dizemos que H é um **Subgrupo** de G , denotando por $H \leq G$, se:

- i) **Fechamento:** para todos $a, b \in H$, o elemento $a \cdot b$ também pertence a H .
- ii) **Elemento inverso:** para todo $a \in H$, tem-se $a^{-1} \in H$.

Observação. É fácil ver que se H é subgrupo de G , então H é um grupo por si só. Sendo assim, a tarefa de verificar que um dado conjunto é grupo, fica bem mais simples se este conjunto pode ser visto como subconjunto de um grupo, visto que não teríamos que trabalhar os detalhes envolvendo associatividade, elemento neutro, etc.

Teorema 1.1. Um subconjunto S de um grupo G é subgrupo se, e somente se, $1 \in S$ e $s, t \in S$ implicar $st^{-1} \in S$.

Demonstração. Se $s \in S$, então $1s^{-1} = s^{-1} \in S$, e se $s, t \in S$, então $s(t^{-1})^{-1} = st \in S$. Reciprocamente, admita que S seja subgrupo. Dados $s, t \in S$, temos $t^{-1} \in S$ e pelo fechamento do produto $st^{-1} \in S$ e $1 = ss^{-1} \in S$. $\square$

Exemplo 1.2.1. Seja $H_5 \subseteq \mathbb{Z}$ o conjunto dos múltiplos de 5, tem-se $H_5 \leq \mathbb{Z}$. De modo geral, o conjunto dos múltiplos de n , denotado por H_n é subgrupo de $\mathbb{Z}$.

Exemplo 1.2.2. o grupo $G = \{-1, 1\}$ pode ser considerado um subgrupo do grupo dos reais não nulos $\mathbb{R}^*$ sob a operação de multiplicação. Basta notar que o grupo é fechado sob a operação de multiplicação, O número 1, elemento neutro da multiplicação, pertence ao grupo G e o seu inverso é -1 .

Exemplo 1.2.3. Seja G um grupo. Então

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\}$$

é um subgrupo de G e $Z(G)$ é denominado centro do grupo G . Além disso, $Z(G)$ é um subgrupo abeliano do grupo G .

De fato, dados $a, b \in Z(G)$, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, para todo $x \in G$. Logo, $ab \in Z(G)$ o que nos mostra que $Z(G)$ é fechado. Tomando $a \in Z(G)$, então $ax = xa, \forall x \in G$. Além disso, $a^{-1}(ax) = a^{-1}(xa) \Rightarrow x = (a^{-1}x)a \Rightarrow xa^{-1} = (a^{-1}x)aa^{-1} = a^{-1}x$, ou seja, $xa^{-1} = a^{-1}x, \forall x \in G$ e portanto, $a^{-1} \in Z(G)$. É fácil ver que $Z(G)$ é abeliano já que por sua própria composição os seus elementos comutam.

Exemplo 1.2.4. Subgrupos de S_3

Subgrupo trivial: Todo grupo possui um subgrupo trivial, que é o conjunto que contém apenas o elemento neutro da operação do grupo. No caso de S_3 , o elemento neutro é a permutação identidade, representada por (1) e tem ordem 1. O subgrupo trivial de S_3 é, portanto,

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

Subgrupos de ordem 2: S_3 possui três subgrupos de ordem 2, cada um formado por duas permutações que trocam dois elementos e deixam o terceiro elemento fixo. Estes subgrupos são:

$$H_1 = \{(12), (1)\}, H_2 = \{(13), (1)\} \text{ e } H_3 = \{(23), (1)\}.$$

Subgrupo de ordem 3: S_3 possui um subgrupo de ordem 3, formado pelas permutações que possuem um número ímpar de trocas. Este subgrupo é:

$$H = \{(123), (132), (1)\}.$$

Exemplo 1.2.5. Considere o grupo simétrico S_4 , que é o grupo de todas as permutações dos números $\{1, 2, 3, 4\}$. Existem quatro subgrupos de ordem 3 em S_4 . Cada um desses

subgrupos é gerado por uma permutação cíclica de três elementos:

$$H_1 = \langle (1\ 2\ 3) \rangle = \{(1)\ (1\ 2\ 3)\ (1\ 3\ 2)\}$$

$$H_2 = \langle (1\ 2\ 4) \rangle = \{(1)\ (1\ 2\ 4)\ (1\ 4\ 2)\}$$

$$H_3 = \langle (1\ 3\ 4) \rangle = \{(1)\ (1\ 3\ 4)\ (1\ 4\ 3)\}$$

$$H_4 = \langle (2\ 3\ 4) \rangle = \{(1)\ (2\ 3\ 4)\ (2\ 4\ 3)\}$$

Definição 6. Seja $f : G \longrightarrow \overline{G}$ um homomorfismo. Definimos o **núcleo de f** , denotado por $N(f)$, como sendo o conjunto

$$N(f) = \{a \in G \mid f(a) = 1_{\overline{G}}\},$$

isto é, o conjunto de elementos em G que são mapeados para o elemento neutro de $\overline{G}$ por f . Também definimos o conjunto **Imagem de f** , denotado por $Im(f)$, por meio de

$$Im(f) = \{h \in \overline{G} \mid h = f(a), a \in G\},$$

isto é, o conjunto dos elementos de $\overline{G}$ que são imagem de algum $a \in G$ por f .

Exemplo 1.2.6. Afirmamos que $K = N(f)$ é um subgrupo de G e $Im(f)$ é um subgrupo de $\overline{G}$. Para verificar que $K \leq G$, observe que se $s, t \in K$, então $f(s) = 1_{\overline{G}} = f(t)$, e assim

$$f(st) = f(s)f(t) = 1_{\overline{G}},$$

donde concluimos o fechamento do Núcleo. Similarmente, se

$$1_{\overline{G}} = f(1) = f(s \cdot s^{-1}) = f(s)f(s^{-1}) = 1 \cdot f(s^{-1}) = f(s^{-1})$$

donde $s^{-1} \in K$, e temos o desejado. Similarmente, mostramos que $Im(f) \leq \overline{G}$.

Exemplo 1.2.7. Seja $f : G \longrightarrow G^*$ um homomorfismo e seja S^* um subgrupo de G^* , então

$$f^{-1}(S^*) = \{x \in G; f(x) \in S^*\}$$

é um subgrupo de G contendo o Núcleo de f .

Demonstração. Para mostrar que $f^{-1}(S^*)$ é um subgrupo de G , precisamos verificar que ele satisfaz as condições do Teorema 1.1:

Contém o elemento identidade: Seja e o elemento identidade de G . Então, $f(e) = e^*$, onde e^* é o elemento identidade de G^* . Como $e^* \in S^*$, temos que $e \in f^{-1}(S^*)$.

Fechamento sob o produto: Sejam $x, y \in f^{-1}(S^*)$. Isso significa que $f(x) \in S^*$ e $f(y) \in S^*$. Como S^* é um subgrupo de G^* , então $f(x)f(y) \in S^*$. Como f é um homomorfismo, $f(xy) = f(x)f(y)$. Portanto, $f(xy) \in S^*$ e assim $xy \in f^{-1}(S^*)$.

Fechamento sob inversos: Seja $x \in f^{-1}(S^*)$. Isso significa que $f(x) \in S^*$. Como S^* é um subgrupo de G^* , então $f(x)^{-1} \in S^*$. Como f é um homomorfismo, $f(x^{-1}) = f(x)^{-1}$. Portanto, $f(x^{-1}) \in S^*$ e assim $x^{-1} \in f^{-1}(S^*)$.

Portanto, $f^{-1}(S^*)$ é um subgrupo de G . Agora, vamos mostrar que $f^{-1}(S^*)$ contém o Núcleo de f . O Núcleo de f é definido como $N(f) = \{x \in G \mid f(x) = e^*\}$, onde e^* é o elemento identidade de G^* . Queremos mostrar que $N(f) \subseteq f^{-1}(S^*)$. Seja $x \in N(f)$. Então, $f(x) = e^*$. Como S^* é um subgrupo, ele contém o elemento identidade e^* . Portanto, $f(x) \in S^*$ e assim $x \in f^{-1}(S^*)$. Logo, $N(f) \subseteq f^{-1}(S^*)$, como queríamos mostrar. $\square$

Definição 7. Se G é um grupo e $a \in G$, então o subgrupo cíclico gerado por a , denotado por $\langle a \rangle$, é o conjunto de todas as potências inteiras de a (ou múltiplos de a , se for um grupo aditivo). Mais precisamente, temos:

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

se a operação de G for multiplicativa, e

$$\langle a \rangle = \{m \cdot a \mid m \in \mathbb{Z}\}$$

se a operação for aditiva. Um grupo G é chamado cíclico se existe um elemento $a \in G$ tal que $G = \langle a \rangle$; ou seja, G consiste em todas as potências (ou múltiplos) de a .

Observação: É evidente que $\langle a \rangle$ é, de fato, um subgrupo de G . Observe que elementos diferentes podem gerar o mesmo subgrupo cíclico. Por exemplo, $\langle a \rangle = \langle a^{-1} \rangle$.

Definição 8. Se G é um grupo e $a \in G$, então a ordem de a é o número de elementos em $\langle a \rangle$. Denotamos por $|\langle a \rangle|$.

Definição 9. Se G é um grupo e $a \in G$, então a ordem de a é $|\langle a \rangle|$, que representa o número de elementos no subgrupo cíclico gerado por a .

No exemplo 1.2.1, temos $H_5 = \langle 5 \rangle$ e $H_n = \langle n \rangle$. No exemplo 1.2.2, o elemento -1 gera todos os elementos no grupo $G = \{-1, 1\} = \langle -1 \rangle$, tornando-se seu gerador. Por outro lado, no exemplo 1.2.3, o centro ($Z(G)$) de um grupo G geralmente não tem um único gerador para todos os seus elementos, dependendo das propriedades específicas do grupo. No exemplo 1.2.4 todos subgrupos que apresentamos são cíclicos, exceto S_3 .

Exemplo 1.2.8. Consideremos o grupo $U(\mathbb{Z}_8)$ das unidades de $\mathbb{Z}_8$ (ver exemplos 1.0.7), que é composto pelos elementos 1, 3, 5 e 7. Observe que todos elementos deste grupo tem ordem 2. Portanto, trata-se de um grupo não cíclico. Já no caso do grupo $U(\mathbb{Z}_5)$ das unidades de $\mathbb{Z}_5$, temos $U(\mathbb{Z}_5) = \langle 2 \rangle$.

Exemplo 1.2.9. Considerando o grupo aditivo $\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$, vamos analisar dois subgrupos cíclicos específicos:

Subgrupo cíclico gerado por $\bar{2}$: Começando com o gerador $\bar{2}$, aplicamos a operação aditiva do grupo $\mathbb{Z}_{10}$ repetidamente obtemos

$$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}.$$

Subgrupo cíclico gerado por $\bar{3}$: Já neste caso, temos

$$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{2}, \bar{5}, \bar{8}, \bar{1}, \bar{4}, \bar{7}\} = \mathbb{Z}_{10}.$$

De modo geral, $\mathbb{Z}_n = \langle \bar{a} \rangle$ se, e somente se, $(a, n) = 1$.

Uma vez definidos e exemplificados os subgrupos, estamos prontos para explorar o Teorema de Lagrange. Este teorema proporciona uma importante conexão entre a ordem de um grupo e seus subgrupos.

1.3 O Teorema de Lagrange

Definição 10. A ordem de G , denotada por $|G|$, é definida como o número de elementos distintos em G . Ou seja, $|G|$ é a cardinalidade do conjunto G .

Definição 11. Se S é um subgrupo de G e se $t \in G$, então uma **classe lateral à direita** de S em G é um subconjunto de G da forma

$$St = \{st : s \in S\}$$

(Uma classe lateral à esquerda é $tS = \{ts : s \in S\}$.) Chamamos t de um **representante** de St (e também de tS).

Exemplo 1.3.1. Seja G o grupo aditivo $\mathbb{Z}$ dos números inteiros, seja S o conjunto de todos os múltiplos de um inteiro n ($S = \langle n \rangle$, subgrupo cíclico gerado por n), e seja $a \in \mathbb{Z}$. Então, a classe lateral à esquerda de S com representante a é

$$a + S = \{a + qn : q \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv a \pmod{n}\},$$

isto é, a classe lateral à esquerda $a + \langle n \rangle$ é precisamente a classe de congruência $\bar{a}$ de a ($\pmod{n}$).

Exemplo 1.3.2. Seja $G = S_3$ e seja $H = \langle \tau \rangle = \{1, \tau\}$, onde $\tau = (1\ 2)$. As classes laterais à direita de H em G são:

$$H = \{1, \tau\}; \quad H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}; \quad H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}.$$

As classes laterais à esquerda de H em G são:

$$H = \{1, \tau\}; \quad (1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}; \quad (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}.$$

Observamos que elementos distintos podem ser representantes de uma mesma classe lateral. Por exemplo, temos que

$$H(123) = \{(123), (23)\} = H(2, 3).$$

De modo geral, temos que se $S \leq G$ e $a, b \in G$, então

$$Sa = Sb \iff ab^{-1} \in S.$$

Além disso, temos que as classes laterais de S particionam o grupo G em “pacotes” disjuntos e de mesma cardinalidade. Denotamos por $[G : S]$ o número de classes laterais de S e chamamos de **índice de S em G** . Em particular, vale o seguinte teorema.

Teorema 1.2 (Lagrange). *Se G é um grupo finito e S é um subgrupo de G , então $|S|$ divide $|G|$ e $[G : S] = \frac{|G|}{|S|}$.*

Como aplicação direta do Teorema de Lagrange, obtemos o seguinte resultado, devido a Euler, que é uma generalização do Pequeno Teorema de Fermat.

Teorema 1.3. *Seja n um inteiro positivo e a um inteiro qualquer que seja relativamente primo com n . Então, a seguinte congruência é válida (ver exemplo 1.0.7):*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Demonstração. Pelo Teorema de Lagrange, se G é um grupo finito e a é um elemento de G , então a ordem de a divide a ordem de G . Portanto, temos que $a^{|G|} = 1$ para todo a em G . Considere o grupo $U(\mathbb{Z}_n)$ das unidades de $\mathbb{Z}_n$, que consiste em todas as classes de congruência módulo n com representantes primos relativos a n . Pelo teorema de Lagrange, a ordem de um elemento $\bar{a} \in U(\mathbb{Z}_n)$ divide a ordem de $U(\mathbb{Z}_n)$, que é igual a $\phi(n)$. Portanto, temos que $\bar{a}^{\phi(n)} = 1$ para todo $\bar{a}$ em $U(\mathbb{Z}_n)$. Finalmente, no caso do enunciado, temos que a é relativamente primo com n , isto é, $\bar{a} \in U(\mathbb{Z}_n)$. Portanto, $a^{\phi(n)} \equiv 1 \pmod{n}$, como queríamos demonstrar. $\square$

Com o Teorema de Lagrange, entendemos a relação entre a ordem de um grupo e seus subgrupos. A partir dessa base, avançamos para o estudo dos subgrupos normais e grupos quociente, conceitos que desempenham um papel central no Teorema da Correspondência de Grupos.

1.4 Subgrupos Normais e Grupo Quociente

A noção de subgrupo normal surge da necessidade de definir quocientes no contexto de grupos. Quando queremos “reduzir” parte da estrutura de um grupo G , formamos o quociente G/N , onde N é um subgrupo de G . No entanto, para que essa construção seja válida, é necessário garantir que a operação de G se mantenha bem definida no quociente. Isso leva à condição de normalidade: um subgrupo N de G é considerado normal quando ele é “preservado” em relação à conjugação por elementos de G , ou seja, para todo $g \in G$ e $h \in N$, temos $ghg^{-1} \in N$. Esse comportamento garante que os elementos do quociente G/N formam um grupo bem definido, preservando a estrutura algébrica do grupo original.

Definição 12. Um subgrupo N é dito um **subgrupo normal** (ou invariante) de G se para todo $g \in G$ e $h \in N$, $ghg^{-1} \in N$. Isto é, para todo $g \in G$, tem-se $gNg^{-1} \subseteq N$. Denotamos por $N \triangleleft G$.

Exemplo 1.4.1. Todo subgrupo de um grupo abeliano é normal.

Lema 1. N é subgrupo normal de G se, e somente se, $gNg^{-1} = N$ para todo $g \in G$

Demonstração. Se $gNg^{-1} = N$ para todo $g \in G$, é fácil ver que $gNg^{-1} \subseteq N$. Logo N é normal em G . Suponhamos agora que N seja normal em G , desta forma como $g^{-1}Ng \subseteq N$ para todo $g \in G$. Consequentemente

$$N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$$

para todo $g \in G$. Decorre disto que

$$gNg^{-1} \subseteq N \subseteq gNg^{-1}$$

e temos o desejado. □

Observação: Note que se o subgrupo N é normal em G , toda classe lateral à direita de N é também classe lateral à esquerda de N . Com efeito

$$gNg^{-1} = N \iff gN = Ng.$$

Sendo assim, no contexto de subgrupos normais, falaremos apenas em classe lateral, sem informar o lado.

Exemplo 1.4.2. O Núcleo K de um homomorfismo $f : G \longrightarrow H$ é um subgrupo normal: se $a \in K$, então $f(a) = 1$; se $g \in G$, então $f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = 1$, e, portanto, $gag^{-1} \in K$. Logo, $gKg^{-1} \subseteq K$ para todo $g \in G$, e, portanto, $K \triangleleft G$. Por outro lado, veremos mais tarde que todo subgrupo normal é o núcleo de algum homomorfismo.

Exemplo 1.4.3 (Subgrupos de índice 2). Se um subgrupo N de G tem índice 2, então N é normal em G . De fato, seja $g \in G$. Se $g \in N$, claramente vale $gNg^{-1} = N$. Admita $g \notin N$, então as classes laterais à direita de N são N e Ng e as classes laterais à esquerda de N são N e gN . Portanto, vale

$$gN = Ng \iff gNg^{-1} = N$$

e temos que N é normal em G .

Exemplo 1.4.4. Considere o grupo simétrico S_3 , (ver exemplo 1.2.4) que é o grupo de todas as permutações do conjunto $\{1 \ 2 \ 3\}$. Ele tem ordem $|S_3| = 6$, pois existem 6 maneiras diferentes de arranjar os 3 elementos.

Vamos examinar o subgrupo $H = \{(1 \ 2 \ 3) \ (1 \ 3 \ 2) \ (1)\}$. Esse subgrupo é formado pelas permutações que possuem um número ímpar de trocas.

O índice de H em S_3 pode ser calculado usando o Teorema de Lagrange:

$$[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{3} = 2$$

Como o índice de H é 2, podemos concluir que H é um subgrupo normal de S_3 .

Exemplo 1.4.5. Considere o grupo simétrico S_4 . O subconjunto

$$K = \{(1) (1\ 2)(3\ 4) (1\ 3)(2\ 4) (1\ 4)(2\ 3)\}$$

de S_4 formado por todas as permutações que são produtos de duas transposições disjuntas é um subgrupo normal.

A ideia é: considere

$$\{X_1 = \{1\ 2\}\{3\ 4\}, X_2 = \{1\ 3\}\{2\ 4\}, X_3 = \{1\ 4\}\{2\ 3\}\}$$

Note que se $\phi \in S_4$ e “aplicamos” ϕ aos X_i , estaremos efetuando uma permutação nos X'_i s. Claramente, todo $\phi \in K$ seria equivalente à identidade. Sendo assim, podemos visualizar um homomorfismo entre S_4 e S_3 com Núcleo K , donde temos o resultado.

Exemplo 1.4.6. Se S e T são subgrupos de G e se um deles é normal, então

$$ST = \{g \in G; g = st, s \in S, t \in T\}$$

é subgrupo de G . Utilizaremos o Teorema 1.1 para concluir o desejado. Naturalmente, tem-se $1 \in ST$. Suponha que $T \triangleleft G$. Se $s_1 t_1$ e $s_2 t_2 \in ST$, então

$$\begin{aligned} (s_1 t_1)(s_2 t_2)^{-1} &= s_1 t_1 t_2^{-1} s_2^{-1} \\ &= s_1 (s_2^{-1} s_2) t_1 t_2^{-1} s_2^{-1} \\ &= s_1 s_2^{-1} t_3 \\ &= (s_1 s_2^{-1}) t_3 \in ST, \end{aligned}$$

onde $t_3 = s_2(t_1 t_2^{-1})s_2^{-1} \in T$ porque $T \triangleleft G$. Logo, ST é subgrupo.

Seja $N \triangleleft G$ um subgrupo normal e sejam $a, b \in G$. Note que

$$\begin{aligned} NaNb &= Na(a^{-1}Na)b \text{ (porque } N \text{ é normal)} \\ &= N(aa^{-1})Nab = N Nab = Nab \text{ (porque } N \leq G). \end{aligned}$$

Isto é, no caso de N ser normal, podemos definir uma operação fechada no conjunto das classes laterais de N . É fácil ver que tal operação é associativa. Além disso, N atua como elemento neutro e dada a classe lateral Na , temos que Na^{-1} atua como inverso multiplicativo de Na . Acabamos de provar o seguinte teorema.

Teorema 1.4. *Se $N \triangleleft G$, então o conjunto das classes laterais de N , munido da operação*

$$NaNb = Nab$$

*forma um grupo chamado **grupo quociente** de G por N e denotado por G/N . Naturalmente, a ordem do grupo quociente é o índice de N em G .*

O seguinte corolário segue imediatamente.

Corolário 1.4.1. *Se $N \triangleleft G$, então a função $\nu : G \longrightarrow G/N$ definida por $\nu(a) = Na$ é um homomorfismo sobrejetor com Núcleo N .*

Observação: A função ν acima é usualmente chamada de *aplicação natural*.

Exemplo 1.4.7. A construção do grupo quociente é uma generalização da construção de $\mathbb{Z}_n$ a partir de $\mathbb{Z}$. Lembre-se que, se n é um inteiro fixo, então $\bar{a}$, a classe de congruência de $a \pmod{n}$, é a classe lateral $a + \langle n \rangle$. Como $\mathbb{Z}$ é abeliano, $\langle n \rangle \triangleleft \mathbb{Z}$, e o grupo quociente $\mathbb{Z}/\langle n \rangle$ possui elementos que são todos classes laterais $a + \langle n \rangle$, onde $a \in \mathbb{Z}$, e a operação é definida por $(a + \langle n \rangle) + (b + \langle n \rangle) = a + b + \langle n \rangle$; em notação de classes de congruência, $\bar{a} + \bar{b} = \overline{a + b}$. Portanto, o grupo quociente $\mathbb{Z}/\langle n \rangle$ é isomorfo a $\mathbb{Z}_n$, o grupo de inteiros módulo n . Devido a este exemplo, um grupo quociente arbitrário G/N é frequentemente chamado de G módulo N .

Exemplo 1.4.8. Considere o grupo de permutações S_3 e o subgrupo $H = \{(123), (132), (1)\}$. O conjunto quociente S_3/H é formado pelas classes laterais de H em S_3 . Como H tem 3 elementos e S_3 tem 6 elementos, existem apenas duas classes laterais, portanto, o conjunto quociente S_3/H tem dois elementos.

Denotaremos as classes laterais como H e gH , onde g é um elemento de S_3 que não está

em H . Assim, podemos montar uma tabela de multiplicação para o grupo quociente S_3/H :

$\circ$	H	gH
H	H	gH
gH	gH	H

Com a apresentação dos conceitos de grupos, homomorfismos e subgrupos, estabelecemos a base teórica necessária para explorar tópicos mais avançados na teoria de grupos. No próximo capítulo, nos aprofundaremos nos teoremas de isomorfismo, que são fundamentais para entender as relações entre diferentes grupos.

Capítulo 2

Teoremas de isomorfismo de grupos e Teorema da correspondência

Neste capítulo, exploraremos os teoremas de isomorfismo de grupos, que fornecem ferramentas poderosas para identificar e classificar grupos. Estes teoremas mostram como os grupos podem ser ‘mapeados’ uns nos outros de forma que preservem sua estrutura interna, facilitando a análise das suas propriedades.

Para iniciar, vamos considerar o Primeiro Teorema do Isomorfismo, que estabelece uma relação direta entre um grupo, seu quociente por um subgrupo normal e a imagem de um homomorfismo.

Teorema 2.1 (Primeiro Teorema do Isomorfismo). *Seja $f : G \longrightarrow H$ um homomorfismo com Núcleo K . Então, K é um subgrupo normal de G e $G/K \cong \text{Im} f$.*

Demonstração. Já vimos que $K \triangleleft G$ (Exemplo 1.4.2). Definimos $\varphi : G/K \longrightarrow H$ por

$$\varphi(Ka) = f(a).$$

Para verificar que φ é bem definida, suponhamos que $Ka = Kb$; isto é, $ab^{-1} \in K$. Então $1 = f(ab^{-1}) = f(a)f(b)^{-1}$, o que implica $f(a) = f(b)$. Logo, $\varphi(Ka) = \varphi(Kb)$, como desejado. Agora φ é um homomorfismo:

$$\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb).$$

É evidente que $\text{im}(\varphi) = \text{im}(f)$. Finalmente, demonstraremos que φ é uma injeção. Se $\varphi(Ka) = \varphi(Kb)$, então $f(a) = f(b)$; consequentemente, $f(ab^{-1}) = 1$, $ab^{-1} \in K$ e $Ka = Kb$ (note que φ ser injetiva é o inverso de φ ser bem definida). Mostramos que φ é um isomorfismo. $\square$

Disso decorre que não há diferença significativa entre um grupo quociente e uma imagem homomorfa.

Se $\nu : G \longrightarrow G/K$ é a aplicação natural, então o seguinte “diagrama comutativo” (isto é, $f = \varphi \circ \nu$) com sobrejeção ν e injeção φ descreve o teorema:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ & \searrow \nu & \nearrow \varphi \\ & G/K & \end{array}$$

Figura 2.1: Diagrama Comutativo do Primeiro Teorema do Isomorfismo

É fácil descrever $\varphi^{-1} : \text{im}(f) \longrightarrow G/K$: se $x \in \text{im}(f)$, então existe $a \in G$ tal que $f(a) = x$, e $\varphi^{-1}(x) = Ka$. Claramente, temos que φ^{-1} é bem definida; isto é, se $f(b) = x$, então $Ka = Kb$.

Exemplo 2.0.1. Como aplicação do primeiro teorema do isomorfismo, mostraremos que quaisquer dois grupos cíclicos de mesma ordem são isomorfos. Sejam $G = \langle g \rangle$ e $H = \langle h \rangle$ grupos cíclicos de ordem n . Suponha que G e H possuem ordem n . Definimos um homomorfismo $f : \mathbb{Z} \longrightarrow G$ por $f(k) = g^k$. Note que f é uma sobrejeção com $N(f) = \langle n \rangle$. O primeiro teorema do isomorfismo garante que $\mathbb{Z}/\langle n \rangle \cong G$. De maneira similar, $\mathbb{Z}/\langle n \rangle \cong H$, e então $G \cong H$. Em particular, como $\mathbb{Z}/\langle n \rangle = \mathbb{Z}_n$, concluímos que todo grupo cíclico de ordem n é isomorfo a $\mathbb{Z}_n$.

Suponha que $S \leq H \leq G$ sejam subgrupos com $S \triangleleft G$. Então $S \triangleleft H$ e o quociente H/S está definido; é o subgrupo de G/S consistindo de todas as classes Sh com $h \in H$. Em particular, se $S \triangleleft G$ e T é qualquer subgrupo de G , então $S \leq ST \leq G$ (veja exemplo

1.4.6) e ST/S é o subgrupo de G/S consistindo de todas as classes Sst , onde $st \in ST$. Como $Sst = St$, segue que ST/T consiste precisamente de todas as classes de S tendo um representante em T .

Tendo estabelecido as bases com o Primeiro Teorema do Isomorfismo, que relaciona grupos quocientes e imagens de homomorfismos, seguimos agora para o Segundo Teorema do Isomorfismo, que aprofunda nossa compreensão das relações entre subgrupos normais e quocientes.

Teorema 2.2 (Segundo Teorema do Isomorfismo). *Sejam N e T subgrupos de G com N normal. Então, $N \cap T$ é normal em T e $T/(N \cap T) \cong NT/N$.*

Demonstração. Seja $\nu : G \rightarrow G/N$ a aplicação natural, e seja $\nu' = \nu|_T$, a restrição de ν a T . Como ν' é um homomorfismo cujo núcleo é $N \cap T$, o Teorema 2.1 garante que $N \cap T \triangleleft T$ e $T/(N \cap T) \cong \text{Im}(\nu')$. Note que $\text{Im}(\nu')$ é apenas a família de todas aquelas classes laterais de N que possuem um representante em T . Portanto, como vimos no parágrafo anterior, $\text{Im}(\nu')$ consiste em todas as classes laterais em NT/N . $\square$

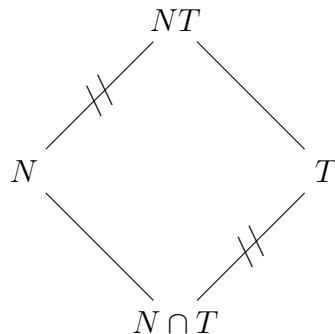


Figura 2.2: Diagrama Mnemônico do Segundo Teorema do Isomorfismo

Exemplo 2.0.2. Sejam n, m números naturais e denotemos por d e l o máximo divisor comum e o mínimo múltiplo comum de m e n , respectivamente. Consideremos $G = \mathbb{Z}$, $N = n\mathbb{Z}$ e $T = m\mathbb{Z}$. Como estamos trabalhando com um grupo aditivo, Denotamos $N+T$ em vez de NT . Sabemos que o mdc d é a menor combinação linear inteira positiva de

m, n . Em particular

$$\begin{aligned} N + T &= n\mathbb{Z} + m\mathbb{Z} \\ &= \{mx + ny; x, y \in \mathbb{Z}\} \\ &= d\mathbb{Z} \end{aligned}$$

Por outro lado, temos que

$$N \cap T = \{s \in \mathbb{Z}; n|s \text{ e } m|s\} = l\mathbb{Z}$$

Como aplicação do segundo teorema do isomorfismo, concluímos que vale

$$d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/l\mathbb{Z}$$

Com o Segundo Teorema do Isomorfismo, vimos como subgrupos normais e seus quocientes se relacionam. Agora, exploraremos o Terceiro Teorema do Isomorfismo, que nos permite compreender melhor as relações entre diferentes níveis de subgrupos dentro de um grupo.

Teorema 2.3 (Terceiro Teorema do Isomorfismo). *Sejam $K \leq H \leq G$, onde K e H são subgrupos normais de G . Então H/K é um subgrupo normal de G/K e*

$$(G/K)/(H/K) \cong G/H.$$

Demonstração. Mais uma vez, deixamos o Primeiro Teorema do Isomorfismo fazer o trabalho pesado. Definimos $f : G/K \rightarrow G/H$ por $f(Ka) = Ha$ (esta função é bem definida porque $K \leq H$). Claramente f é uma sobrejeção com núcleo H/K e o resultado segue imediatamente do primeiro teorema do isomorfismo. $\square$

Imagine tentar provar o Terceiro Teorema do Isomorfismo diretamente. Os elementos de $(G/K)/(H/K)$ são classes laterais cujos representantes são, por sua vez, classes laterais em G/K . Aplicaremos o terceiro teorema do isomorfismo na demonstração do Teorema da Correspondência.

Após explorar os três teoremas de isomorfismo, chegamos ao Teorema da Correspondência. Este teorema sintetiza muitas das ideias abordadas até agora, oferecendo uma poderosa ferramenta para entender as inter-relações entre subgrupos e seus quocientes.

Teorema 2.4 (Teorema da Correspondência). *Seja $K \triangleleft G$ e $\nu : G \longrightarrow G/K$ a aplicação natural. Então $S \mapsto \nu(S) = S/K$ é uma bijeção entre a família de todos os subgrupos S de G que contêm K e a família de todos os subgrupos de G/K .*

Além disso, se denotamos S/K por S^* , então:

- i) $T \leq S$ se e somente se $T^* \leq S^*$, e então $[S : T] = [S^* : T^*]$;
- ii) $T \triangleleft S$ se e somente se $T^* \triangleleft S^*$, e então $S/T \cong S^*/T^*$.

Demonstração. Mostramos primeiro que $S \mapsto S/K$ é uma injeção: se S e T são subgrupos contendo K , e se $S/K = T/K$, então $S = T$. Para ver isso, seja $s \in S$; como $S/K = T/K$, existe $t \in T$ com $Ks = Kt$. Logo, $s = kt$ para algum $k \in K \leq T$ e $s \in T$. A inclusão inversa é provada de forma semelhante. Para ver que a correspondência $S \mapsto S/K$ é uma sobrejeção, devemos mostrar que se $A \leq G/K$, então existe um subgrupo S de G contendo K com $A = S/K$. Pelo exemplo 1.2.7, $S = \nu^{-1}(A)$ é um subgrupo de G contendo K ; além disso, o fato de ν ser uma sobrejeção (Se $f : X \longrightarrow X^*$ é uma função e $A \subset X^*$, então $f(f^{-1}(A)) \subset A$; se f é uma sobrejeção, então $f(f^{-1}(A)) = A$.) implica que $S/K = \nu(S) = \nu\nu^{-1}(A) = A$.

É claro que se $K \leq T \leq S$, então $T/K \leq S/K$. Para provar que $[S : T] = [S^* : T^*]$, basta mostrar que existe uma bijeção da família de todas as classes da forma Ts , onde $s \in S$, para a família de todas as classes T^*s^* , onde $s^* \in S^*$. É fácil verificar que α , definida por $\alpha : Ts \mapsto T^*\nu(s)$, é tal bijeção. (Se G é finito, então podemos provar $[S : T] = [S^* : T^*]$ da seguinte maneira:

$$\begin{aligned} [S^* : T^*] &= |S^*|/|T^*| = |S/K|/|T/K| \\ &= (|S|/|K|)/(|T|/|K|) = |S|/|T| = [S : T]. \end{aligned}$$

Se $T \triangleleft S$, então o terceiro teorema do isomorfismo dá $T/K \triangleleft S/K$ e $(S/K)/(T/K) \cong S/T$; isto é, $T^* \triangleleft S^*$ e $S^*/T^* \cong S/T$. Resta mostrar que se $T^* \triangleleft S^*$, então $T \triangleleft S$. O leitor pode verificar que $T = N \mu v_0 : S \mapsto S^*/T^*$, onde $v_0 = v|_S$ e $\mu : S^* \mapsto S^*/T^*$ é o mapeamento natural.

Um diagrama mnemônico para este teorema é:

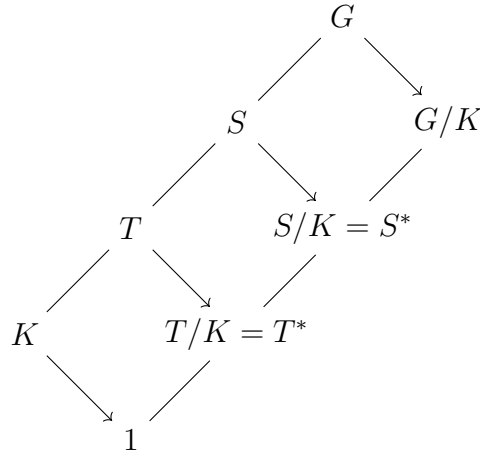


Figura 2.3: Diagrama Mnemônico do Teorema da Correspondência

□

Exemplo 2.0.3. Seja G um grupo com um subgrupo normal N de ordem 5, tal que G/N é isomorfo ao grupo simétrico S_4 de 4 símbolos. Prove que $|G| = 120$, G possui um subgrupo normal de ordem 20, e exatamente 4 subgrupos de ordem 15, nenhum dos quais é normal em G .

Demonstração. Observe que $|S_4| = 4! = 24$. Logo, $|G/N| = 24$. Então, pelo teorema de Lagrange, $|G/N| = [G : N]$ e assim $|G| = |G/N| \cdot |N| = 24 \cdot 5 = 120$.

Agora, considere o subgrupo (ver Exemplo 1.4.5)

$$K = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \leq S_4 \cong G/N.$$

Então $K \triangleleft G/N$, $|K| = 4$, e $[G/N : K] = 6$ (novamente pelo teorema de Lagrange). Logo, pelo teorema da correspondência, K corresponde a um subgrupo normal $H \triangleleft G$ tal que $[G : H] = 6$, e consequentemente (pelo teorema de Lagrange) $|H| = 120/6 = 20$.

Finalmente, como $G/N \cong S_4$ e S_4 possui quatro subgrupos de ordem 3 (ver exemplo 1.2.5)

$$\langle (1, 2, 3) \rangle, \langle (1, 2, 4) \rangle, \langle (2, 3, 4) \rangle, \langle (1, 3, 4) \rangle,$$

nenhum dos quais é normal em S_4 , o resultado desejado segue pela aplicação do teorema da correspondência.

Ajustando a estrutura para o Diagrama Mnemônico do Teorema da Correspondência:

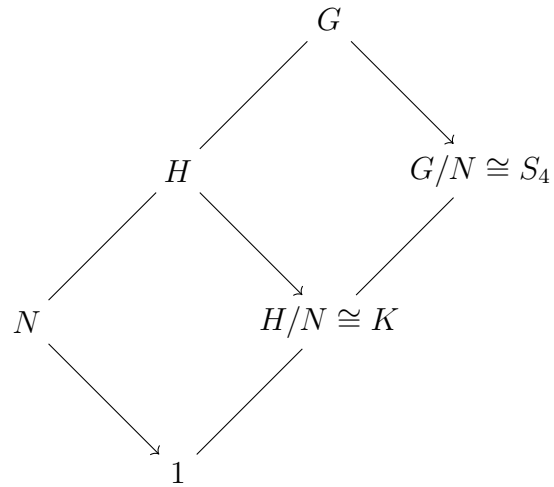


Figura 2.4: Diagrama Mnemônico do Teorema da Correspondência

Neste diagrama, G é o grupo total, H é o subgrupo normal de ordem 20, N é o subgrupo normal de ordem 5, e $\{1\}$ é o subgrupo trivial. No quociente, temos G/K , H/K , N/K e $\{1\}/K$ correspondendo aos respectivos subgrupos quocientes. $\square$

Conclusão

Concluimos que o Teorema da Correspondência de Grupos não apenas simplifica a análise da estrutura dos grupos, mas também oferece uma poderosa ferramenta para explorar novas relações entre grupos e seus quocientes. Com essa compreensão, finalizamos nosso estudo detalhado dos principais conceitos da teoria dos grupos, com destaque para o Teorema da Correspondência, que se mostrou um resultado central e de grande aplicabilidade.

Referências Bibliográficas

- [1] GONÇALVES, A. **Introdução à Álgebra**. 4. ed. Rio de Janeiro: SBM, 1999.
- [2] HERSTEIN, I. N. **Topics in Algebra**. 2. ed. New York: Wiley, 1975.
- [3] ROTMAN, Joseph J. **An Introduction to the Theory of Groups**. 4. ed. New York: Springer-Verlag, 1995.