UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE EDUCAÇÃO

Curso de Graduação em Licenciatura em Matemática

Edvenilson Venâncio Dantas

TEOREMA DOS ISOMORFISMOS DE GRUPOS E APLICAÇÕES

Cuité-PB

2015

Edvenilson Venâncio Dantas

TEOREMA DOS ISOMORFISMOS DE GRUPOS E APLICAÇÕES

TCC apresentado ao curso Graduação em Licenciatura em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Graduado em Licenciatura em Matemática.

Orientadora: Glageane da Silva Souza
Coorientadora: Edna Cordeiro de Souza

Cuité-PB
2015

Biblioteca Setorial do CES.

Junho de 2021.

Cuité - PB

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes – CRB 15 – 256

D192t Dantas, Edvenilson Venâncio.

Teorema dos isomorfismo de grupos e aplicações. / Edvenilson Venâncio Dantas. – Cuité: CES, 2015.

43 fl.

Monografia (Curso de Licenciatura em Matemática) – Centro de Educação e Saúde / UFCG, 2015.

Orientadora: Glageane da Silva Souza.
Coorientador: Edna Cordeiro de Souza.

1. Teorema de grupos. 2. Homomorfismo de grupos. 3. Isomorfismo. I. Título.

CDU 512

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG
CENTRO DE EDUCAÇÃO E SAÚDE - CES
UNIDADE ACADÊMICA DE EDUCAÇÃO – UAE

Edvenilson Venâncio Dantas

TEOREMA DOS ISOMORFISMOS DE GRUPOS E APLICAÇÕES

Monografia de Trabalho de Conclusão de Curso submetida à banca examinadora como parte dos requisitos necessários a obtenção do grau de Graduação em Licenciatura em Matemática.

Trabalho de Conclusão de Curso (TCC) aprovado em 10 de março de 2015.

Banca Examinadora

Glageane da Silva Souza
Profª. Glageane da Silva Souza
(Orientadora)

Aluizio Freire da S. Júnior
Prof. Aluizio Freire da Silva Júnior

Edna Cordeiro de Souza
Profª. Édna Cordeiro de Souza

Dedico este trabalho primeiramente a Deus, pois sem ele eu não teria forças para essa longa jornada, por ser essencial em minha vida, autor de meu destino, meu guia, socorro bem presente na hora da angústia, a minha esposa Gigliola, meu pai Evenilson, minha mãe Josefa Venâncio e meu irmão Edjanilson.

Agradecimentos

A Deus, o soberano Senhor e Criador do Universo, sou e serei eternamente grato pelo dom da vida e pela capacidade de discernimento.

A Gigliola Gilmara de Sousa Farias Dantas minha esposa, pelo companheirismo e compreensão durante todo o transcorrer desta trajetória. A você, minha eterna admiração e gratidão pelo incentivo.

Aos meus pais Evenilson Cunha Dantas e Josefa dos Santos Venâncio Dantas, que foram bases solidas na construção do meu caráter; há vocês o meu muito obrigado.

A meu irmão José Edjanilson Venâncio Dantas, pela amizade e apoio durante está etapa da minha vida.

A meu sogro Gerson Farias, adotado como meu segundo pai, sou grato por todas as atitudes que imensuravelmente me beneficiaram.

Aos meus cunhados e parentes, sou grato pelo apoio e incentivo; meu muito obrigado.

A meus avós Eliacim e Francisca, de forma afetivamente cariosa digo meu muito obrigado.

Aos meus grandes amigos o Teólogo Lourival dos Santos Borges e Edilson Batista de Farias pela força e apoio, durante este tempo de convivência.

À minha orientadora profª MSc. Glageane da Silva Souza, pela amizade, incentivo, dedicação e por ter me ajudado e acreditado em mim, aceitando o convite de orientar-me nesse trabalho. Foram valiosas suas contribuições para o meu crescimento acadêmico.

Agradeço aos professores, profª. MSc. Edna Cordeiro de Souza e Prof. MSc. Aluizio Freire da Silva Junior, que fizeram parte da banca examinadora.

Aos professores do curso de matemática, os meus agradecimentos por toda a atenção e dedicação.

Aos meus colegas de curso e especialmente a Clebson Huan, Valda Lúcia, Crispim, Maciel, Joelson, Ana Élia entre outros. Sou grato pela parceria e incentivo.

A Universidade Federal de Campina Grande, UFCG/Campus Cuité, pela oportunidade e acolhimento aos acadêmicos.

" Aquele que quer aprender gosta que lhe digam quando está errado; só o tolo não gosta de ser corrigido."

Provérbios 12.1.

Resumo

A Teoria de Grupos surge naturalmente em muitas linhas de pesquisas da matemática com implicações estendidas a outras ciências. O objetivo principal deste trabalho é enunciar, demonstrar e aplicar o Teorema dos Isomorfismos de Grupos. Neste desenvolvimento, apresentaremos as principais definições e propriedades da Teoria de Grupos, sendo os homomorfismos e isomorfismos de grupos os mais enfatizados, por serem a base do teorema.

Palavras-chave: Teoria de Grupos. Homomorfismo de Grupos. Isomorfismo.

Abstract

The Group Theory arises naturally in many lines of research in mathematics with implications extended to other sciences. The main objective of this study is to enunciate, demonstrate and apply the Group Isomorphisms Theorem. In this development, we will present the main definitions and properties of the Group Theory, emphasizing the homomorphism and isomorphism of groups, because they are the base of the theorem.

Keywords: Groups Theory. Homomorphism of groups. Isomorphism.

Lista de Símbolos

$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}$	Conjunto dos Números Complexos
$(G, *)$	Grupo munido da operação $*$
$\leq$	subgrupo
$Z(G)$	Centro do grupo G
$< s >$	Subgrupo gerado por s
$\|G\|$	Ordem do grupo G
$\varphi(g)$	Ordem de um elemento $g \in G$
$(G : H)$	índice do subgrupo H em G
$\triangleleft$	subgrupo normal
ψ	representa um homomorfismo
$Ker(\psi)$	Núcleo do homomorfismo
$G \simeq J$	G é isomorfo a J
$Aut(G)$	Grupo dos automorfismo de G
$\mathcal{I}(G)$	Conjunto dos automorfismo internos de G
$Im(\psi)$	Imagem do Homomorfismo
e_G	Elemento neutro do grupo G

Sumário

Introdução

Na disciplina de Estruturas Algébricas estuda-se, na Teoria de Grupos, o Teorema dos Isomorfismos que garante que dado um homomorfismo $\psi : (G, *) \longrightarrow (J, \times)$, o grupo formado pelas classes laterais do núcleo $Ker(\psi)$ com a operação induzida de G é isomorfo a imagem do homomorfismo, ou seja, mantêm uma relação bijetiva por meio do homomorfismo a imagem do homomorfismo.

No capítulo 1 é apresentado a história sobre Teoria de Grupos dando ênfase as equações algébricas junto a seu questionamento de resolubilidade por radicais, dando também destaques aos principais matemáticos e autores que influenciaram no surgimento da mesma.

No capítulo 2 temos a teoria básica de grupos, apresentamos definições de grupos e subgrupos, destacando algumas propriedades dos mesmos e dando alguns exemplos, também enfatisamos subgrupos gerado por um subconjunto. Falamos de classes laterais e também demonstramos o Teorema de Lagrange, que garante que a ordem e o índice de um subgrupo dividem a ordem do grupo. Apresentamos também algumas aplicações do Teorema de Lagrange. Em seguida apresentamos um sistema de afirmações equivalentes para identificarmos quando um subgrupo é normal e a partir dele definimos o subgrupo quociente.

No capítulo 3 trabalhamos primeiro com os homomorfismos de grupos, definindo–os, exemplicando–os e demonstrando algumas propriedades dos mesmos. Depois definimos núcleo de um homomorfismo e logo em seguida definimos isomorfismo de grupo e como caso particular dos isomorfismos temos os automorfismos. A partir destes conceitos enunciamos e demonstramos o Teorema dos Isomorfismos de Grupos, e para finalizar aplicamos o referido Teorema.

Capítulo 1

História sobre Teoria de Grupos

Ao contrário da maioria das descobertas matemáticas, verificamos que ninguém estava procurando uma Teoria de Grupos quando o conceito foi descoberto. Muito pelo contrário, a Teoria de Grupo apareceu meio que pelo dom do acaso, nascendo de uma procura por uma solução para uma equação algébrica. "Condizente com sua descrição como um conceito que cristalizou simplicidade a partir do caos, a própria Teoria de Grupos nasceu de um episódio mais tumultuado na história da matemática" (Livio, 2011, p. 66)[6]. Quase quatro mil anos de curiosidade e luta intelectual, temperadas com intriga, tormentos e perseguições, resultaram na criação da teoria no século XIX. Aqui, iremos se concentrar na emergência das "equações", já que esta é a parte mais relevante para a história da Teoria de Grupos.

A grande escola grega de Alexandria produziu muitos matemáticos notáveis durante duas eras. Um dos pensadores mais originais da escola alexandrina foi Diofanto. Livio (2011, p. 75)[6] nos mostra que detalhes da vida de Diofanto estão ocultos, não sabemos com exatidão em que século ele viveu, a menos que deve ter sido depois de cerca de 150 a.C. (já que ele cita o matemático Hipsicles, que viveu por volta de 180 a.C. a 120 a.C.) e antes de cerca de 270 d.C. (já que ele é mencionado por Anatólio, bispo de Laodiceia, que assumiu o cargo por volta dessa época), em geral, supõe-se que Diofanto tenha vivido por volta de 250 d.C., mas não possa ser descartada a possibilidade de que tenha vivido um século antes. Diofanto é um homem às vezes chamado o "pai da álgebra" (Livio, 2011, p.75)[6].

Diofanto representa um estágio crucial na evolução da álgebra, intermediário en-

tre o estilo puramente retórico dos babilônicos e as formas simbólicas das equações (por exemplo, $2x^2 + x = 3$) que usamos hoje. Ele é hoje mais conhecido por uma classe especial de equação que leva o seu nome - equação diofantina. As equações diofantinas são verdadeiramente estranhas no sentido de, à primeira vista, parecerem admitir qualquer número como solução. Como, por exemplo, a equação: $29x + 4 = 8y$.

A mais famosa equação diofantina da história é aquela conhecida como o último teorema de Fermat, a célebre afirmação de Pierre Fermat (1601 - 1655) de que não existem soluções com números inteiros para a equação $x^n + y^n = z^n$, onde n seja qualquer número maior que 2. E esta afirmativa levou cerca de 360 anos para ser demonstrada, a qual foi provado só agora em 1995 pelo americano Andrew Wiles.

No início do século XVI, mais precisamente entre 1500 e 1515, o matemático italiano Scipione del Ferro (1465 - 1526), sem perceber, torna-se parte de um drama que se desenrolava. Ele promoveu um importante avanço na matemática ao descobrir um procedimento para resolver a equação cúbica $x^3 + ax = b(a, b > 0)$. Esse procedimento se traduz, na linguagem atual, na seguinte fórmula:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Del Ferro mostrou, com essa fórmula, que é possível expressar as raízes da equação cúbica considerada em termos de seus coeficientes, usando apenas adição, subtração, multiplicação, divisão e radiciação, ou seja, que a equação dada é resolúvel por radicais. Como já se sabia há muitos séculos que as equações de grau um e dois também são resolúveis por radicais (no caso desta última, lembrar a chamada fórmula de Bhaskara), a solução de del Ferro colocou um desafio para os algebristas: será que toda equação algébrica é resolúvel por radicais? As pesquisas feitas na tentativa de responder a esse desafio se estenderam por mais de dois séculos e meio, frustrando alguns dos grandes matemáticos da época e contribuindo para a criação do conceito de "grupos".

A questão da resolubilidade das equações algébricas só começou a ser esclarecida de forma genérica na segunda metade do século XVIII. Na obra *Réflexions sur la résolution albébrique des équations* (Reflexões sobre a resolução algébrica de equação)(1770 - 1771), o ítalo-francês Joseph-Louis Lagrange (1736 - 1813) faz primeiro uma revisão com grande cuidado das contribuições de Leonhard Euller (1707 - 1783)(onde em uma de suas obras, Euller, conjecturou que a solução da equação de

grau 5 poderia ser expressa em termos de cerca de quatro quantidades e concluiu em um tom cheio de esperança: "Poderíamos suspeitar que a eliminação, se feita meticulosamente, pudesse talvez levar a uma equação de grau 4" (Livio, 2011, p.106)[6].) e de outros matemáticos da época. Depois mostrou que para os graus 2, 3 e 4, as equações poderiam ser resolvidas pela redução da equação a uma de um grau menor que aquela em questão (ou seja, reduzindo a quártica para uma cúbica). Quando o mesmo processo foi tentado numa equação de grau 5, aconteceu algo inesperado, a equação resultante, em vez de uma quártica, acabou sendo uma de grau 6.

Decepcionado com o resultado, Lagrange conclui que "é, portanto, improvável que tais métodos levem à solução da quíntica - um dos problemas mais celebres e importantes da ágebra." (Livio, 2011, p.106)[6]

Como uma maneira de sair do impasse, Lagrange introduziu uma discussão mais geral das permutações, provavelmente ele foi o primeiro matemático a perceber o caminho a ser seguido para abordar o problema, observou que a "teoria das permutações" era de grande importância para a resolução de equações. Lagrange referia-se a permutações envolvendo as raízes da equação.

Em 1824, o matemático norueguês Niels Henrik Abel (1802 - 1829) provaria aquilo que Lagrange já suspeitara: que não há nenhuma fórmula geral por radicais para resolver as equações de grau ≥ 5. Ainda assim uma questão permanecia: já que as equações de grau ≥ 5 não são, de modo geral, resolúveis por radicais, o que caracteriza matematicamente estas últimas? A resposta para essa pergunta seria dada pelo matemático francês Evariste Galois (1811 - 1832), em cuja obra aparece pela primeira vez o conceito de grupo. Livio (2011, p. 310)[6] relata-nos que "Galois realizou todo o trabalho brilhantemente seminal sobre Teoria de Grupos antes dos 21 anos, a genialidade de Galois fascinou o mundo da matemática antes que este pobre matemático tivesse 27."

Boyer (1974, p.434)[1] afirma que o conceito de grupos foi essencial para o aparecimento das ideias abstratas na primeira metade do século XIX. O autor evidencia que os trabalhos de Galois sobre resolução de equações algébricas foram considerados não apenas pelos seus resultados específicos, mas especialmente pela natureza de uma estrutura algébrica que Galois denominou primeiramente de grupo.

Resumidamente, a ideia de Galois para responder a essa pergunta em questão foi associar a cada equação um grupo formado por permutações de suas raízes e condici-

onar a resolubilidade por radicais a uma propriedade desse grupo. E, como para toda equação de grau ≤ 4 o grupo de permutações que lhe é associado goza dessa propriedade e para $n > 4$ sempre há equações cujo grupo não se sujeita a essa propriedade, a questão da resolubilidade por radicais estava por fim esclarecida.

Com o passar dos anos, os pesquisadores da área e de áreas correlatas foram verificando que a ideia de grupos era muito importante como instrumento para a organização e estudos de muitas partes da matemática. Em nível mais elementar, um exemplo é a teoria das simetrias, muito importante para a cristalografia e a química, por exemplo.

Capítulo 2

Conceitos Preliminares

Neste capítulo temos como objetivo introduzir os conceitos preliminares que serão usados no capítulo seguinte onde enunciamos, demosntramos e apresentamos algumas aplicações do Teorema dos Isomorfismos de Grupos.

2.1 Grupos

Definição 2.1. *Um sistema matemático constituído de um conjunto não vazio G e uma operação $(x, y) \mapsto x * y$ sobre G é chamado* **grupo** *se essa operação se sujeita aos seguintes axiomas:*

1. **Associatividade**

   $(a * b) * c = a * (b * c)$, *quaisquer que sejam* $a, b, c \in G$.

2. **Existência de elemento neutro**

   Existe um elemento $e \in G$ *tal que* $a * e = e * a = a$, *para todo* $a \in G$.

3. **Existência dos simétricos**

   Para todo $a \in G$ *existe um elemento* $a' \in G$ *tal que* $a * a' = a' * a = e$.

Se, além disso, ainda se cumprir o axioma da **comutatividade**, ou seja, $a * b = b * a$, quaisquer que sejam $a, b \in G$, o grupo recebe o nome de **grupo comutativo** ou **abeliano**.

Observações:

- Mantidas as notações da definição, um grupo poderá ser indicado apenas por $(G, *)$, em que para facilitar, o símbolo $*$ indica a operação sobre G.
- Para simplificar a notação usamos ab ao invés de $a * b$, e indicamos por a^{-1} o simétrico de $a \in G$.

2.1.1 Propriedades de Grupos

P1. O elemento neutro de um grupo é único.

Prova: De fato, suponhamos que e_1 e e_2 são elementos neutros de G, então:

$$\begin{aligned} e_1 &= e_1 e_2 && \text{pois } e_2 \text{ é elemento neutro de } G, \\ &= e_2 && \text{pois } e_1 \text{ é elemento neutro de } G. \end{aligned}$$

■

P2. O elemento simétrico é único.

Prova: De fato, seja $a \in G$, e sejam $b_1, b_2 \in G$ dois elementos simétricos de a, temos

$$\begin{aligned} b_1 &= b_1 e = b_1(ab_2) && \text{pois } b_2 \text{ é simétrico de } a, \\ &= (b_1 a)b_2 = eb_2 = b_2 && \text{pois } b_1 \text{ é simétrico de } a. \end{aligned}$$

■

P3. $(a^{-1})^{-1} = a, \forall\ a \in G$.

Prova: Temos,

$$\begin{aligned} (a^{-1})^{-1} &= (a^{-1})^{-1} e = (a^{-1})^{-1}(a^{-1}a) \\ &= [(a^{-1})^{-1}(a^{-1})]a = ea = a && \text{pois } (a^{-1})^{-1} \text{ é simétrico de } a^{-1}. \end{aligned}$$

■

P4. $(ab)^{-1} = b^{-1}a^{-1}, \forall\ a, b \in G$.

Prova: Temos que $(ab)^{-1}(ab) = e$, pois $(ab)^{-1}$ é simétrico de (ab).

Operando b^{-1} nos dois lados pela direita, obtemos

$$\begin{aligned} [(ab)^{-1}(ab)]b^{-1} &= eb^{-1} \\ (ab)^{-1}[(ab)b^{-1}] &= b^{-1} \\ (ab)^{-1}[a(bb^{-1})] &= b^{-1} \\ (ab)^{-1}[ae] &= b^{-1} \\ (ab)^{-1}a &= b^{-1}. \end{aligned}$$

Agora operando a^{-1} nos dois lados também pela direita, temos

$$\begin{aligned}[(ab)^{-1}a]a^{-1} &= b^{-1}a^{-1}\\ (ab)^{-1}(aa^{-1}) &= b^{-1}a^{-1}\\ (ab)^{-1}e &= b^{-1}a^{-1}\\ (ab)^{-1} &= b^{-1}a^{-1}.\end{aligned}$$

■

P5. Do fato que o simétrico de um elemento $a \in G$ é único, obtém-se o caso mais geral seguinte:

"Se $a, b \in G$, então a equação $Xa = b$ tem uma única solução em G, a saber ba^{-1}."

Prova: De fato, se c é uma solução de $Xa = b$, então temos $ca = b$, daí operando a^{-1} pela direita em ambos os membros, obtemos

$$\begin{aligned}(ca)a^{-1} &= ba^{-1}\\ c(aa^{-1}) &= ba^{-1}\\ ce &= ba^{-1}\\ c &= ba^{-1}.\end{aligned}$$

Por outro lado, ba^{-1} é claramente uma solução.

De forma análoga, obtém-se que a equação $aX = b$, tem uma única solução em G, a saber $a^{-1}b$. ■

P6. Todo elemento do grupo G é regular para a operação $*$, ou seja:

Se $ax = ay$ (ou $xa = ya$), então $x = y$.

Prova:

$ax = ay$ Operando a^{-1} pela esquerda em ambos os membros,

$a^{-1}(ax) = a^{-1}(ay)$

$(a^{-1}a)x = (a^{-1}a)y$

$ex = ey$

$x = y.$

■

2.1.2 Exemplos de Grupos

Exemplo 2.1. *O conjunto $\mathbb{Z}$ com a operação de adição usual é um grupo abeliano aditivo.*

Solução: De fato,

- Associatividade

  Para quaisquer $x, y, z \in \mathbb{Z}$ tem-se

  $$(x + y) + z = x + (y + z).$$

- Existência de elemento neutro

  $\exists\ 0 \in \mathbb{Z}$ tal que $\forall\ x \in \mathbb{Z}$ tem-se que

  $$x + 0 = 0 + x = x.$$

- Existência de elemento simétrico

  Para cada $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ tal que

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

- Comutatividade

  Para quaisquer $x, y \in \mathbb{Z}$ tem-se que

  $$x + y = y + x.$$

■

Exemplo 2.2. $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$, *onde $+$ é a operação aditiva usual, são todos grupos abelianos aditivos.*

A solução é análoga ao Exemplo 2.1.

Exemplo 2.3. *Sejam G um conjunto não vazio e " $*$ " uma operação associativa em G tal que:*

i) Existe $e \in G$ tal que $x * e = x$, para todo $x \in G$.

ii) Para cada $x \in G$, existe $x^{-1} \in G$ tal que $x * x^{-1} = e$.

Mostre que $(G, *)$ é um grupo.

Solução: Para mostrar que $(G, *)$ é um grupo, basta mostra que

1. Existe $e \in G$ tal que $e * x = x$, para todo $x \in G$.

2. Para cada $x \in G$, existe $x^{-1} \in G$ tal que $x^{-1} * x = e$.

Faremos primeiro algumas observações:

- Para cada $x \in G$, existe $x^{-1} \in G$ tal que $x^{-1} * x \in G$.

- Para cada $x^{-1} * x \in G$, existe $(x^{-1} * x)^{-1} \in G$ (pelo item " ii ") tal que

$$(x^{-1} * x) * [(x^{-1} * x)^{-1}] = e.$$

- Existe $e \in G$ (pelo item " i ") tal que $(x^{-1} * x) * e = x^{-1} * x$, para todo $(x^{-1} * x) \in G$.

- Existe $e \in G$ tal que $x^{-1} * e = x^{-1}$, para todo $x^{-1} \in G$.

Agora começaremos realmente a demonstração, começando pelo item 2, temos:

$$(x * x^{-1}) * x = (x * x^{-1}) * x$$

usando $x * x^{-1} = e$ no lado esquerdo da igualdade, temos

$$e * x = (x * x^{-1}) * x$$

operando x^{-1} em ambos os membros pela esquerda, obtemos

$$x^{-1} * (e * x) = x^{-1} * [(x * x^{-1}) * x]$$

$$(x^{-1} * e) * x = (x^{-1} * x) * (x^{-1} * x)$$

usando $x^{-1} * e = x^{-1}$, encontramos

$$x^{-1} * x = (x^{-1} * x) * (x^{-1} * x)$$

operando $(x^{-1} * x)^{-1}$ em ambos os membros pela direita, temos

$$(x^{-1} * x) * (x^{-1} * x)^{-1} = [(x^{-1} * x) * (x^{-1} * x)] * [(x^{-1} * x)^{-1}]$$

$$(x^{-1} * x) * (x^{-1} * x)^{-1} = (x^{-1} * x) * [(x^{-1} * x) * (x^{-1} * x)^{-1}]$$

usando $(x^{-1} * x) * [(x^{-1} * x)^{-1}] = e$, chegamos a

$$e = (x^{-1} * x) * e$$

usando $(x^{-1} * x) * e = x^{-1} * x$, concluimos

$$e = (x^{-1} * x)$$

o que nos mostra que $(x^{-1} * x) = e$. Agora vamos mostrar o item 1:

Temos,

$$e * x = (x * x^{-1}) * x = x * (x^{-1} * x) = x * e = x$$

o que nos garante que $e * x = x$.

Portanto $(G, *)$ é um grupo. ∎

Exemplo 2.4. *Consideremos o conjunto dos números reais* $\mathbb{R}$ *munido da operação "*$*$*" definida por* $x * y = x + y - 3, \forall\ x, y \in \mathbb{R}$. *Mostre que* $(\mathbb{R}, *)$ *é um grupo comutativo.*

Solução: De fato,

- Associatividade

  $\forall\ x, y, z \in \mathbb{R}$, temos

  $(x * y) * z = (x + y - 3) * z = (x + y - 3) + z - 3 = x + (y - 3 + z) - 3 =$

  $x + (y + z - 3) - 3 = x + (y * z) - 3 = x * (y * z)$

  $\Rightarrow (x * y) * z = x * (y * z)$.

- Existência do elemento neutro

  $\forall\ x \in \mathbb{R}$, temos

$$\begin{aligned} x * e &= x \\ x + e - 3 &= x \end{aligned}$$

somando $-x$ pela esquerda em ambos os membros

$$\begin{aligned} (-x) + (x + e - 3) &= -x + x \\ (-x + x) + e - 3 &= -x + x \\ 0 + e - 3 &= 0 \\ e - 3 &= 0 \end{aligned}$$

somando 3 em ambos os membros

$$\begin{aligned} e-3+3 &= 3 \\ e+0 &= 3 \\ e &= 3 \end{aligned}$$

Com isso, temos que o elemento neutro $e = 3$ daí

$x * 3 = x + 3 - 3 = x + 0 = x$ e $3 * x = 3 + x - 3 = x + 3 - 3 = x + 0 = x$.

O que nos garante $x * e = e * x = x$.

- Existência do simétrico

  Para cada $x \in \mathbb{R}$, existe $x^{-1} \in \mathbb{R}$, tal que

$$\begin{aligned} x * x^{-1} &= e \\ x + x^{-1} - 3 &= 3 \end{aligned}$$

somando $-x$ pela esquerda em ambos os membros, temos

$$\begin{aligned} -x + (x + x^{-1} - 3) &= -x + 3 \\ (-x + x) + x^{-1} - 3 &= -x + 3 \end{aligned}$$

somando 3 em ambos os membros temos

$$\begin{aligned} 0 + x^{-1} - 3 &= -x + 3 \\ 0 + x^{-1} - 3 + 3 &= -x + 3 + 3 \\ x^{-1} - 0 &= -x + 6 \\ x^{-1} &= -x + 6 \end{aligned}$$

O que nos mostra que o elemnto simétrico $x^{-1} = -x + 6$, daí

$x * x^{-1} = x + x^{-1} - 3 = x + (-x + 6) - 3 = (x + -x) + 6 - 3 = 0 + 3 = 3 = e$ e

$x^{-1} * x = x^{-1} + x - 3 = (-x + 6) + x - 3 = (x + -x) + 6 - 3 = 0 + 3 = 3 = e$.

O que nos garante $x * x^{-1} = x^{-1} * x = e$.

- Comutatividade

  $\forall\, x, y \in \mathbb{R}$ temos

  $x * y = x + y - 3 = y + x - 3 = y * x$

  $\Rightarrow x * y = y * x$.

  Portanto, $(\mathbb{R}, *)$ é um grupo abeliano. ∎

2.2 Subgrupos

Definição 2.2. *Seja $(G, *)$ um grupo. Um subconjunto não vazio H de G é um* **subgrupo** *de G (denotaremos $H \leq G$) quando H, com a operação $*$ do grupo G, satisfaz as seguintes condições:*

0) $h_1 * h_2 \in H, \forall\ h_1, h_2 \in H.$

i) $h_1 * (h_2 * h_3) = (h_1 * h_2) * h_3, \forall\ h_1, h_2, h_3 \in H.$

ii) $\exists\ e_H \in H$ *tal que* $e_H * h = h * e_H = h, \forall\ h \in H.$

iii) Para cada $h \in H$, *existe* $h^{-1} \in H$ *tal que* $h * h^{-1} = h^{-1} * h = e_H.$

Notação: Será denotado por e_G, a menos de menção contrária, o elemento neutro do grupo G.

Observações:

O1. A condição " i " é sempre satisfeita, pois a igualdade $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ é válida $\forall\ g_1, g_2, g_3 \in G$;

O2. O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G. De fato, tomando $a \in H \leq G$, temos $e_H * a = a$, operando os dois lados por a^{-1} a direita, obtemos

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

O3. O simétrico de um elemento de H é o mesmo em G. De fato, se h^{-1} é o simétrico de h em H, então,
$h * h^{-1} = h^{-1} * h = e_H$, logo
$h * h^{-1} = h^{-1} * h = e$, pois $e_H = e$
e portanto h^{-1} é o simétrico de h em G.

Proposição 2.1. *Seja H um subconjunto não-vazio de G. Então $H \leq G$ se, e somente se, são satisfeita as condições:*

i) $h_1 * h_2 \in H, \forall\ h_1, h_2 \in H$.

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

Prova:

($\Rightarrow$) Suponhamos que H seja um subgrupo de G.

- A condição " i " já é satisfeita.
- Agora, se $h \in H$, sendo H um subgrupo, h possui simétrico em H, mas pela observação O3 precedente, tal simétrico é necessariamente igual ao simétrico de h em G, isto é, é necessariamente igual a h^{-1}, logo a condição " ii " também é satisfeita.

($\Leftarrow$) Reciprocamente, suponhamos que as duas condições " i " e " ii " sejam satisfeita.

- O item " i " garante o fechamento da operação em H.
- Os elementos de H são elementos de G, logo vale a associatividade.
- Dado $h \in H$, existe $h^{-1} \in H$ tal que $e = h * h^{-1} \in H$, e pelo item " ii " qualquer elemento de H possui simétrico em H. ∎

2.2.1 Exemplos de Subgrupos

Exemplo 2.5. *Se G é um Grupo, então $\{e\}$ e G são subgrupos de G.*

A verificação de que estes dois subconjuntos de G são subgrupos é imediata. Tais subgrupos são chamados subgrupos triviais de G.

Exemplo 2.6. *Considere o subconjunto $Z(G) = \{x \in G \mid x * g = g * x, \forall\ g \in G\}$ onde G é um grupo. $Z(G)$ é chamado de* **centro** *de G. Observe que $e \in Z(G)$ e $Z(G) = G \Leftrightarrow G$ é abeliano. Mostremos que $Z(G)$ é um subgrupo de G.*

Solução: De fato,

i) Sejam $x_1, x_2 \in Z(G)$.

Dado $g \in G$, como G é abeliano $\Leftrightarrow\ Z(G) = G$, temos

$x_1 * g = g * x_1$ pois $x_1 \in Z(G)$ e

$x_2 * g = g * x_2$ pois $x_2 \in Z(G)$

Daí,

$$x_1 * x_2 * g = x_1 * g * x_2 = g * x_1 * x_2$$

Logo $x_1 * x_2 \in Z(G)$

ii) Seja $x \in Z(G)$.

Sabe-se que $x * g = g * x$. Operando x^{-1} em ambos os membros pela esquerda, temos

$$\begin{aligned} x^{-1} * (x * g) &= x^{-1} * (g * x) \\ (x^{-1} * x) * g &= x^{-1} * (g * x) \\ e * g &= x^{-1} * (g * x). \end{aligned}$$

Agora operando x^{-1} em ambos os membros pela direita, temos

$$\begin{aligned} (e * g) * x^{-1} &= x^{-1} * (g * x) * x^{-1} \\ g * x^{-1} &= x^{-1} * g * (x * x^{-1}) \\ g * x^{-1} &= x^{-1} * g * e \\ g * x^{-1} &= x^{-1} * g. \end{aligned}$$

Logo $x^{-1} \in Z(G)$.

Portanto $Z(G) \leq G$. ∎

2.2.2 Subgrupo gerado por um subconjunto

Fixemos algumas notações. Sejam H e K subconjuntos de um grupo G. O conjunto $\{hk \mid h \in H \text{ e } k \in K\}$ será denotado por HK, e o conjunto $\{h^{-1} \mid h \in H\}$ será denotado por H^{-1}. Seja S um subconjunto não vazio do grupo G, o conjunto $\{a_1 a_2 \dots a_n \mid n \in \mathbb{N}, a_i \in S^1 \text{ ou } a_i \in S^{-1}\}$ será denotado por $\langle S \rangle$.

Proposição 2.2. *Sejam G um grupo e S um subconjunto não-vazio de G. Então o conjunto $\langle S \rangle$ é um subgrupo de G.*

Prova: Devemos mostrar que:

i) $\forall\, x, y \in \langle S \rangle$, temos $xy \in \langle S \rangle$.

ii) $\forall\, x \in \langle S \rangle$, temos $x^{-1} \in \langle S \rangle$.

De fato, sejam $x, y \in \langle S \rangle$, temos

$$x = a_1 a_2 \dots a_n, \text{ com } a_i \in S^1 \text{ ou } a_i \in S^{-1}, \forall\, i \in \mathbb{N}$$
$$y = b_1 b_2 \dots b_m, \text{ com } b_j \in S^1 \text{ ou } b_j \in S^{-1}, \forall\, j \in \mathbb{N}.$$

Logo, $xy = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$ e $x^{-1} = {a_n}^{-1} {a_{n-1}}^{-1} \dots {a_2}^{-1} {a_1}^{-1}$ estão também em $\langle S \rangle$. ∎

Definição 2.3. *Sejam G um grupo e S um subconjunto não-vazio de G. Então $\langle S \rangle$ é o* **subgrupo gerado** *por S.*

Definição 2.4. *Um grupo G é* **cíclico** *quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.*

Exemplo 2.7. $\mathbb{Z} = \langle 1 \rangle$.

Definição 2.5. *Seja G um grupo. O subgrupo $\langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$ é o* **subgrupo dos comutadores** *de G; ele será denotado por G'. Note que G é abeliano se, e somente se, $G' = \{e\}$.*

Definição 2.6. *A* **ordem** *de um grupo G é o número de elementos em G; ela será denotada por $|G|$. Se g é um elemento do grupo G, a* **ordem** *do subgrupo gerado por g, será denotada por $\varphi(g)$.*

Proposição 2.3. *Seja G um grupo. Se G é cíclico, então G é abeliano.*

Prova: Seja G um grupo cíclico e seja x um gerador de G, de modo que

$$G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}.$$

Se g_1 e g_2 são quaisquer dois elementos de G, existem inteiros r e s tais que $g_1 = x^r$ e $g_2 = x^s$. Então

$$g_1 g_2 = x^r x^s = x^{r+s} = x^{s+r} = x^s x^r = g_2 g_1.$$

Portanto G é abeliano. ∎

2.2.3 Classes Laterais e Teorema de Lagrange

Definição 2.7. *Sejam G um grupo e H um subgrupo de G. Sendo $g \in G$, definimos:*

a) A classe lateral à direita de H contendo g, como sendo

$$Hg = \{hg \mid h \in H\}.$$

b) A classe lateral à esquerda de H contendo g, como sendo

$$gH = \{gh \mid h \in H\}.$$

Observação:

Temos $g \in gH$, pois $g = g * e \in gH$. Em geral $gH \neq Hg$, tome como exemplo $H = \langle \vartheta \rangle$ em S_3 com $\vartheta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Se $\mu = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, temos que $\mu H \neq H\mu$.
De fato, temos que

- $\vartheta^2 = \vartheta * \vartheta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$
- $\mu * e = \mu$
- $\mu * \vartheta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
- $\mu H = \left\{\mu, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$

  e
- $\vartheta * \mu = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- $H\mu = \left\{\mu, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$

Logo, $\mu H \neq H\mu$.

Definição 2.8. *A cardinalidade do conjunto das classes laterais à esquerda é o* **índice** *de H em G, ele será denotado por $(G : H)$.*

Proposição 2.4. *O índice de H em G também é a cardinalidade do conjunto das classes laterais à direita de H em G, pois a aplicação*

$$\begin{aligned} \phi : \{\textit{classes laterais à esquerda}\} &\longrightarrow \{\textit{classes laterais à direita}\} \\ xH &\longmapsto Hx^{-1} \end{aligned}$$

é uma bijeção.

Prova: De fato, seja $Hg_1 = Hg_2$.
Note que $g_1 \in Hg_2$, daí existe $h_1 \in H$ tal que

$$g_1 = h_1 g_2 \Rightarrow g_1 {g_2}^{-1} = h_1 \Rightarrow {g_2}^{-1} = {g_1}^{-1} h_1.$$

Dado $h \in H$, temos

$${g_2}^{-1} h = {g_1}^{-1} h_1 h \in {g_1}^{-1} H$$

Como h é arbitrário em H, temos

$${g_2}^{-1} H \subseteq {g_1}^{-1} H \Rightarrow {g_2}^{-1} H = {g_1}^{-1} H \Rightarrow \phi(Hg_2) = \phi(Hg_1).$$

Logo, ϕ é injetiva. A sobrejetividade segue da definição de ϕ.
Considerando $g^{-1} \in G$

$$\phi(Hg^{-1}) = H(g^{-1})^{-1} = Hg$$

Portanto ϕ é bijetiva. ∎

Teorema 2.1. *(Teorema de Lagrange) Se G é um grupo finito e H um subgrupo de G, então $|H|$ divide $|G|$.*

Prova: Sejam $Hx_1, Hx_2, \ldots, Hx_n$ as distintas classes laterais à direita de H em G.
Sabemos que

$$\begin{aligned} G &= Hx_1 \cup Hx_2 \cup \ldots \cup Hx_n \\ |G| &= |Hx_1| + |Hx_2| + \ldots + |Hx_n| \\ |G| &= |H| + |H| + \ldots + |H| \\ |G| &= n|H| = (G : H) \cdot |H|. \end{aligned}$$

Logo, $|H|$ divide $|G|$. ∎

Aplicações do Teorema de Lagrange

Aplicação 2.1. *Se G é um grupo finito e $x \in G$, então a ordem de x divide a ordem de G.*

Prova: Por definição, $\varphi(x) = |\langle x \rangle|$. Aplicando o Teorema de Lagrange ao subgrupo $\langle x \rangle$, temos que $|\langle x \rangle|$ divide $|G|$. Ademais, $x^{|G|} = e$, de fato, existe $k \in \mathbb{Z}$ tal que $|G| = \varphi(x) \cdot k$, daí

$$x^{|G|} = x^{\varphi(x)\cdot k} = (x^{\varphi(x)})^k = e^k = e.$$

■

Aplicação 2.2. *Todo grupo G tal que $|G| = p$ (p é primo) é cíclico.*

Prova: Considere $x \in G$ tal que $x \neq e$. Note que $|\langle x \rangle|$ divide $|G| = p$. Daí, pelo Teorema de Lagrange, $\varphi(x)$ divide p, então $\varphi(x) = 1$ ou $\varphi(x) = p$, como $x \neq e$, temos que $\varphi(x) = p$. Portanto, $\langle x \rangle = G$. ■

Aplicação 2.3. *Seja G um grupo e H e K subgrupos de G, tais que $|H|$ e $|K|$ são relativamentes primos, então $H \cap K = \{e\}$.*

Prova: Seja $x \in H \cap K$, então $x \in H$ e $x \in K$. Note que $\langle x \rangle \subset H$ e $\langle x \rangle \subset K$. Daí, pelo Teorema de Lagrange $\varphi(x)$ divide $|H|$ e $\varphi(x)$ divide $|K|$, o que nos garante $\varphi(x) = 1$, e assim, $x = e$. ■

Aplicação 2.4. *Se $|G| \leq 5$, então G é abeliano.*

Prova:

- Se $|G| = 1$, temos $G = \{e\}$.
- Se $|G| = 2, 3$ ou 5, temos que $|G|$ é prima, logo pela aplicação 2.2, G é cíclico, portanto abeliano.
- Agora, para $|G| = 4$: se $\exists\ x \neq e,\ x \in G$ tal que $\langle x \rangle = G$ então G é cíclico e portanto abeliano. Suponhamos então que : $\forall\ x \in G, x \neq e$, temos $\langle x \rangle \neq G$. Ora pelo Teorema de Lagrange segue imediatamente que $|\langle x \rangle| = 2$. Assim, $x^2 = e, \forall\ x \in G$, logo se $x, y \in G$ tem-se $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, ou seja, G é abeliano. ■

2.3 Subgrupo normal e subgrupo quociente

Proposição 2.5. *Seja H um subgrupo de G. As afirmações abaixo são equivalentes:*

(i) A operação induzida sobre as classes laterais à esquerda em G é bem definida.

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

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

(iv) $\forall\ g \in G$, vale $gH = Hg$, isto é, $\forall\ g \in G$, as classes laterais à esquerda de H é igual as classes laterais à direita de H.

Prova:

(i) $\Leftrightarrow$ (ii) Sejam $x, y \in G$ e $h, k \in H$ arbitrários, assim, x e xh são representantes da mesma classe xH, y e yk são representantes da mesma classe yH. Assim a operação induzida sobre as classes laterais é bem definida se, e somente se,
$xyH = xhykH,\ \forall\ x, y \in G, \forall\ h, k \in H$.
Logo, se, e somente se,

$$H = y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhykH = y^{-1}hyH, \forall\ y \in G, \forall h \in H$$

e portanto se, e somente se,

$$yhy^{-1} \in H, \forall\ y \in G,\ \forall\ h \in H.$$

(iii) $\Leftrightarrow$ (ii) Temos que $gHg^{-1} = H$, logo $gHg^{-1} \subseteq H$.

(ii) $\Leftrightarrow$ (iii) Suponhamos que $gHg^{-1} \subseteq H, \forall\ g \in G$, o objetivo é mostrar que $H \subseteq gHg^{-1}, \forall\ g \in G$. Sejam então $h \in H$ e $g \in G$, temos que

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

pois $g^{-1}Hg \subset H$, por hipótese.

(iii) $\Leftrightarrow$ (iv)

$$gHg^{-1} = H \Rightarrow gHg^{-1}g = Hg \Rightarrow gH = Hg, \forall\ g \in G$$

(iv) $\Leftrightarrow$ (iii)

$$gH = Hg \Rightarrow gHg^{-1} = Hgg^{-1} \Rightarrow gHg^{-1} = H, \forall\ g \in G.$$

■

Definição 2.9. *Um subgrupo H é um* **subgrupo normal** *de G (e denotaremos por $H \triangleleft G$) se ele satisfaz as afirmações equivalentes da proposição anterior. Neste caso, as classes laterais à esquerda de H são iguais às classes laterais à direita de H.*

Definição 2.10. *Seja H um subgrupo normal de um grupo G e considere o conjunto G/H de G pela relação de equivâlencia H. Os elementos desse conjunto são as classes laterais $xH = Hx$, $x \in G$. Sejam xH e yH duas classes laterais quaisquer. Definimos em G/H a operação*

$$(xH) \cdot (yH) \to (xy)H$$

Logo, o produto de duas classes laterais de H é uma classe lateral de H. Fica assim definida uma operação sobre o conjunto G/H.

Proposição 2.6. *Seja H um subgrupo normal de um grupo G e considere o conjunto quociente G/H. A operação*

$$(xH) \cdot (yH) \to (xy)H$$

define uma estrutura de grupo sobre o conjunto G/H.

Prova: O axioma da associatividade segue da associatividade de G e da definição da operação em G/H. Assim pelo Exemplo 2.3 basta verificar " i " e " ii ".

(i) Considerando o conjunto H temos que, para toda classe lateral xH de G/H:

$$(xH)H = (xH)(eH) = (xe)H = xH.$$

(ii) Seja xH uma classe lateral qualquer e considere a classe lateral $x^{-1}H \in G/H$. Logo,

$$(xH)(x^{-1}H) = (xx^{-1})H = eH = H.$$

■

Definição 2.11. *Sejam G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais com a operação induzida de G é o grupo quociente de G por H.*

Proposição 2.7. *Seja G um grupo e seja $Z(G)$ seu centro. Se $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.*

Prova: Seja $\overline{z}$ um gerador do grupo $G/Z(G)$. Então, $\forall\ g \in G\ \exists\ i$ tal que $\overline{g} = \overline{z}^i$, logo tal que $g = z^i h$ com $h \in Z(G)$. Se g_1 e g_2, definido como $z^{i_1}h_1$ e $z^{i_2}h_2$ respectivamente, são dois elementos quaisquer de G, temos

$$g_1 g_2 = z^{i_1}h_1 z^{i_2}h_2 = z^{i_1+i_2}h_1 h_2 = z^{i_2+i_1}h_2 h_1 = z^{i_2}h_2 z^{i_1}h_1 = g_2 g_1,$$

pois h_1 e h_2 comutam com qualquer elemento de G. Isto mostra que o grupo G é abeliano, isto é, que $Z(G) = G$. ∎

Capítulo 3

Teorema dos Isomorfismos e Aplicações

Neste capítulo provaremos o Teorema dos Isomorfismos de Grupos e faremos algumas aplicações do mesmo.

3.1 Homomorfismos de Grupos

Definição 3.1. *Sejam $(G, *)$ e $(J, \times)$ dois grupos. Uma função $\psi : G \longrightarrow J$ é um homomorfismo se ela é compatível com as estruturas dos grupos, isto é, se*

$$\psi(a * b) = \psi(a) \times \psi(b), \forall\ a, b \in G.$$

Observações:

i) Se ψ é injetiva, dizemos que ψ é um homomorfismo injetor.

ii) Se ψ é sobrejetiva, dizemos que ψ é um homomorfismo sobrejetor.

iii) O caso em que ψ é bijetiva corresponde ao conceito de isomorfismo e será apresentado separadamente.

3.1.1 Exemplos de Homomorfismos de Grupos

Exemplo 3.1. *A aplicação $\psi : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \cdot)$, definida por $\psi(m) = i^m$ é um homomorfismo.*

Solução: De fato, sejam $m, n \in \mathbb{Z}$, temos

$$\psi(m+n) = i^{m+n} = i^m \cdot i^n = \psi(m) \cdot \psi(n)$$

fica provado que é um homomorfismo. Esse homomorfismo não é injetor, pois $\psi(2) = -1 = \psi(6)$, e também não é sobrejetor, pois $Im(\psi) = \{1, i, -1, -i\} \neq \mathbb{C}^*$. ∎

Exemplo 3.2. *A aplicação $\psi : (\mathbb{C}^*, \cdot) \longrightarrow (\mathbb{R}_+^*, \cdot)$ definida por $\psi(Z) = |Z|$ onde $Z = a + bi$, $|Z| = a^2 + b^2$, é um homomorfismo de grupos.*

Solução: De fato, dado $Z, W \in \mathbb{C}^*$, temos

$$\psi(Z \cdot W) = |Z \cdot W| = |Z| \cdot |W| = \psi(Z) \cdot \psi(W).$$

∎

Exemplo 3.3 (Homomorfismo identidade)**.** *Seja*

$$\begin{aligned} \psi : \ G &\longrightarrow G \\ g &\longmapsto id(g) = g \end{aligned}$$

é um homomorfismo identidade.

Exemplo 3.4. *A aplicação $e : (G, \cdot) \longrightarrow (J, \cdot)$, definida por $e(g) = e_J$, para todo $g \in G$ é um homomorfismo chamado homomorfismo trivial.*

3.1.2 Propriedades de Homomorfismos de Grupos

Seja $\psi : (G, *) \longrightarrow (J, \times)$ um homomorfismo de grupo. Então

P1. $\psi(e_G) = e_J$.

Prova: De fato, $\psi(e_G) = \psi(e_G * e_G) = \psi(e_G) \times \psi(e_G)$. ∎

P2. $\psi(g^{-1}) = \psi(g)^{-1}$

Prova: Usaremos aqui a propriedade anterior

$$\psi(g) \times \psi(g^{-1}) = \psi(g * g^{-1}) = \psi(e_G) = e_J = \psi(g) \times [\psi(g)]^{-1}$$

$$\Rightarrow \psi(g) \times \psi(g^{-1}) = \psi(g) \times [\psi(g)]^{-1}$$

Pela unicidade do simétrico segue $\psi(g^{-1}) = \psi(g)^{-1}$. ∎

P3. Se H é um subgrupo de G então $\psi(H)$ é um subgrupo de J.

Prova: Lembremos primeiro que $\psi(H) = \{\psi(x) \mid x \in H\}$.

Sejam $Z, W \in \psi(H)$, existe $x, y \in H$ tal que $\psi(x) = Z$ e $\psi(y) = W$. Então,

i) $Z \times W = \psi(x) \times \psi(y) = \psi(\underbrace{x * y}_{\in H}) \in \psi(H)$.

ii) $Z^{-1} = \psi(x)^{-1} \overset{\text{por P2}}{=} \psi(\underbrace{x^{-1}}_{\in H}) \in \psi(H)$.

Portanto $\psi(H)$ é subgrupo de J. ∎

P4. G é abeliano se, e somente se, $\psi : (G, *) \longrightarrow (G, *)$ definida por $\psi(x) = x^{-1}$ é um homomorfismo.

Prova:

($\Rightarrow$) Temos, por hipótese, que G é abeliano. Dados $x, y \in G$, temos

$$\psi(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = x^{-1} * y^{-1} = \psi(x) * \psi(y).$$

($\Leftarrow$) Reciprocamente temos que se ψ é um homomorfismo, então

$$\begin{aligned}
\psi(xy) &= \psi(x)\psi(y) \\
(xy)^{-1} &= x^{-1}y^{-1} \\
(xy)(xy)^{-1} &= (xy)(x^{-1}y^{-1}) \\
e &= xyx^{-1}y^{-1} \\
ey &= (xyx^{-1}y^{-1})y \\
y &= xyx^{-1}(y^{-1}y) \\
y &= xyx^{-1}e \\
y &= xyx^{-1} \\
yx &= (xyx^{-1})x \\
yx &= xy(x^{-1}x) \\
yx &= xye \\
yx &= xy.
\end{aligned}$$

Logo G é abeliano. ∎

3.1.3 Núcleo de um Homomorfismo

Definição 3.2. *Seja $\psi : G \longrightarrow J$ um homomorfismo de grupos. Se e_J indica o elemento neutro de J, o seguinte subconjunto de G será chamado núcleo de ψ e denotado por $Ker(\psi)$:*

$$Ker(\psi) = \{x \in G \mid \psi(x) = e_J\}.$$

Observemos que, como $\psi(e_G) = e_J$ (Propriedade 1), então $e_G \in Ker(\psi)$. Assim, pelo menos o elemento neutro de G pertence ao núcleo de ψ.

Exemplo 3.5. *Determinemos o núcleo do homomorfismo de grupos $\psi : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ definida por $\psi(m) = i^m$ (ver exemplo 3.1). Como o elemento neutro de $\mathbb{C}^*$ é o número 1, então basta resolver a equação $i^m = 1$. Mas, como é bem conhecido do estudo dos números complexos, o conjunto das soluções dessa equação, ou seja, o núcleo de ψ, é:*

$$Ker(\psi) = \{0, \pm 4, \pm 8, \ldots\}.$$

Exemplo 3.6. *Consideremos agora o homomorfismo $\psi : \mathbb{Z} \longrightarrow \mathbb{Z}$ definido por $\psi(m) = am$, em que a é um número inteiro dado. Como o elemento neutro de $\mathbb{Z}$ é o número 0, temos que resolver a equação $am = 0$. Mas é claro que o conjunto das soluções depende de a. Se $a = 0$, então o núcleo é $\mathbb{Z}$, pois, para todo inteiro m, vale a igualdade $m \cdot 0 = 0$. Mas, se $a \neq 0$, então a única solução de $am = 0$ é o número 0, e, portanto, neste caso, $Ker(\psi) = \{0\}$.*

3.2 Isomorfismos de Grupos

Um isomorfismo de grupo é uma função entre dois grupos que gera uma correspondência biunívoca entre os elementos de ambos respeitando-se as operações de cada grupo. Se existe um isomorfismo entre dois grupos, ele são chamados de isomorfos.

Definição 3.3. *Seja $\psi : G \longrightarrow J$ um homomorfismo de grupos. Se ψ for também uma bijeção, então será chamado de isomorfismo do grupo G no grupo J. Neste caso diz-se que ψ é um isomorfismo de grupos. Quando existe um isomorfismo entre dois grupos G e J, dizemos que G e J são isomorfos e denotamos por $G \simeq J$.*

Exemplo 3.7. *Os grupos $G = (\mathbb{R}, +)$ e $J = (\mathbb{R}^*, \cdot)$ são isomorfos. De fato, basta mostrar que a função $\psi : G \longrightarrow J$ definida por $\psi(x) = 2^x$ é um isomorfismo:*

- *não é difícil ver que ψ é bijetiva, sendo log_2 a função inversa;*
- *ψ preserva as operações:*

$$\psi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \psi(x) \cdot \psi(y).$$

Exemplo 3.8. *Seja $G = (\mathbb{R}, +)$. A função $\psi : G \longrightarrow G$ definida por $\psi(x) = x^3$, embora seja bijetiva, não é um isomorfismo, pois existem números reais x e y tais que $(x+y)^3 \neq x^3 + y^3$, ou seja, ψ não preserva a operação.*

Exemplo 3.9. *Seja $g \in G$ fixo. Então, $\mathcal{I}_g : G \to G$, $\mathcal{I}_g(x) = gxg^{-1}$, é um homomorfismo bijetivo.*

Solução: Observemos que $\mathcal{I}_g$ é:

i) Um homomorfismo, pois $\forall\, x, y \in G$, temos que $\mathcal{I}_g(xy) = g(xy)g^{-1} = g(xey)g^{-1} = (gxg^{-1})(gyg^{-1}) = \mathcal{I}_g(x)\mathcal{I}_g(y)$.

ii) Injetiva, pois se $x \in Ker(\mathcal{I}_g)$ temos que
$gxg^{-1} = e \Rightarrow gx = g \Rightarrow x = e$.

iii) Sobrejetiva, pois escolhendo $a \in G$, existe um elemento $b \in G$ tal que $\mathcal{I}_g(b) = a$. Tome $b = g^{-1}ag \in G$. Logo, $\mathcal{I}_g(b) = \mathcal{I}_g(g^{-1}ag) = g(g^{-1}ag)g^{-1} = a$.

Portanto, $\mathcal{I}_g$ é um homomorfismo bijetivo, ou seja, um isomorfismo. ∎

Definição 3.4. *Seja $(G, *)$ um grupo. Um automorfismo de G é um isomorfismo $\psi : G \to G$. O conjunto dos automorfismos de G será denotado por $Aut(G)$.*

Exemplo 3.10. *Já foi observado que $\mathcal{I}_g : G \to G$, $\mathcal{I}_g(x) = gxg^{-1}$, é um homomorfismo bijetivo e portanto um automorfismo de G, chamado automorfismo interno associado ao elemento $g \in G$. O conjunto dos automorfismos internos de G será denotado por $\mathcal{I}(G)$; assim*

$$\mathcal{I}(G) := \{\mathcal{I}_g \mid g \in G\} \subseteq Aut(G).$$

3.3 Teorema dos Isomorfismos de Grupos

Lema 3.1. *Sejam $(G,\cdot)$ e $(J,*)$ grupos com elementos neutros e_G e e_J, respectivamente, e $\psi : G \longrightarrow J$ um homomorfismo. Então*

a) $Im(\psi) = \{y \in J : y = \psi(g)$ para algum $g \in G\}$ é um subgrupo de J, chamado Imagem de ψ.

b) $Ker(\psi) = \{g \in G : \psi(g) = e_J\}$ é um subgrupo normal de G.

Prova:

a) Dados $y, z \in Im(\psi) \Rightarrow \exists\ x_1, x_2 \in G$ tal que $y = \psi(x_1), z = \psi(x_2)$.

Logo,

$$y * z^{-1} = \psi(x_1) * \psi(x_2)^{-1} = \psi(x_1) * \psi(x_2^{-1}) = \psi(x_1 \cdot x_2^{-1}).$$

Como $(x_1 \cdot x_2^{-1}) \in G$, segue que $y * z^{-1} \in Im(\psi)$ e pela Proposição 2.1, $Im(\psi) \leq J$.

b)Vejamos primeiro que $Ker(\psi) \leq G$. Dados $x, y \in Ker(\psi)$, temos:

$$(x \cdot y) = \psi(x) * \psi(y) = e_J * e_J = e_J$$
$$\psi(x^{-1}) = \psi(x)^{-1} = {e_J}^{-1} = e_J;$$

Portanto $Ker(\psi) \leq G$. Para mostrar que $Ker(\psi) \triangleleft G$ devemos mostrar que:

$$gxg^{-1} \in Ker(\psi), \forall\ g \in G \text{ e } \forall\ x \in Ker(\psi).$$

E de fato, temos

$\psi(gxg^{-1}) = \psi(g) * \psi(x) * \psi(g^{-1}) = \psi(g) * e_J * \psi(g)^{-1} = \psi(g) * \psi(g)^{-1} = e_J.$

Com isso provamos o lema. ∎

Lema 3.2. *Seja $\psi : (G,\cdot) \longrightarrow (J,\times)$ um homomorfismo de grupos. Então:*

i) Se H é um subgrupo de G, então $\psi(H)$ é um subgrupo de J e $\psi^{-1}(\psi(H)) = HKer(\psi)$;

ii) Se $\mathcal{H}$ é um subgrupo de J, então $\psi^{-1}(\mathcal{H})$ é um subgrupo de G contendo $Ker(\psi)$ e $\psi(\psi^{-1}(\mathcal{H})) = \mathcal{H} \cap Im(\psi)$.

iii) ψ é um homomorfismo injetor se, e somente se, $Ker(\psi) = \{e_G\}$.

Prova:

i) A prova de que $\psi(H)$ é um subgrupo de J é analoga à prova do item a) do lema 3.1(note que $Im(\psi) = \psi(G)$). Vamos provar agora a igualdade $\psi^{-1}(\psi(H)) = HKer(\psi)$. Seja $(h \cdot k) \in HKer(\psi)$, isto é, $h \in H$ e $k \in Ker(\psi)$; temos

$$\psi(h \cdot k) = \psi(h) \times \psi(k) = \psi(h) \times e_J = \psi(h) \in \psi(H);$$

provamos assim que

$$HKer(\psi) \subseteq \psi^{-1}(\psi(H)).$$

Para provar a inclusão contrária, tome $y \in \psi^{-1}(\psi(H))$. Por definição, $\psi(y) \in \psi(H)$; existe então $h \in H$ tal que $\psi(y) = \psi(h)$, logo, multiplicando por $\psi(h^{-1})$ à esquerda, tal que $\psi(h)^{-1} \times \psi(y) = e_J$, isto é, tal que $h^{-1} \cdot y \in Ker(\psi)$. Temos assim que $y = h \cdot (h^{-1} \cdot y) \in HKer(\psi)$.

ii) Sejam $a, b \in \psi^{-1}(\mathcal{H})$. Então, $\psi(a), \psi(b) \in \mathcal{H}$ e $\psi(a) \times \psi(b)^{-1} \in \mathcal{H}$. Como,

$$\psi(a) \times \psi(b)^{-1} = \psi(a) \times \psi(b^{-1}) = \psi(a \cdot b^{-1}) \in \mathcal{H},$$

então $a \cdot b^{-1} \in \psi^{-1}(\mathcal{H})$, donde $\psi^{-1}(\mathcal{H}) \leq G$.

Seja $x \in Ker(\psi)$. Então, $\psi(x) = e_J \in \mathcal{H}$ e consequentemente $x \in \psi^{-1}(\mathcal{H})$. Donde $Ker(\psi) \subset \psi^{-1}(\mathcal{H})$. Concluimos então que $\psi(\psi^{-1}(\mathcal{H})) = \mathcal{H} \cap Im(\psi)$.

iii)($\Rightarrow$) Suponha ψ injetiva. Portanto

$$x \in Ker(\psi) \Rightarrow \psi(x) = e_J \Rightarrow \psi(x) = \psi(e_G) \Rightarrow x = e_G \Rightarrow Ker(\psi) = \{e_G\}$$

($\Leftarrow$) Suponha $Ker(\psi) = \{e_G\}$. Como

$$\psi(x) = \psi(y) \Rightarrow \psi(xy^{-1}) = e_J \Rightarrow xy^{-1} \in Ker(\psi) = \{e_G\} \Rightarrow x = y$$

temos que ψ é injetiva. ∎

Teorema 3.1. *(Teorema dos Isomorfismos de Grupos) Seja $\psi : (G, \cdot) \longrightarrow (J, \times)$ um homomorfismo de grupos. Então,*

1) A função induzida

$$\begin{array}{rccc} \overline{\psi}: & \dfrac{G}{Ker(\psi)} & \longrightarrow & \psi(G) \\ & gKer(\psi) & \longmapsto & \psi(g) \end{array}$$

é um isomorfismo.

2) As seguintes funções

$$\begin{array}{ccc} \left\{ \textit{subgrupos de } G \textit{ que contêm } Ker(\psi) \right\} & \overset{1-1}{\longleftrightarrow} & \left\{ \textit{subgrupos de } \psi(G) \right\} \\ H & \longmapsto & \psi(H) \\ \psi^{-1}(\mathcal{H}) & \longmapsto & \mathcal{H}, \end{array}$$

são bijeções, inversa uma da outra. Além disso, estas bijeções levam subgrupos normais em subgrupos normais, isto é:

a) $H \triangleleft G \Rightarrow \psi(H) \triangleleft \psi(G)$.

b) $\mathcal{H} \triangleleft \psi(G) \Rightarrow \psi^{-1}(\mathcal{H}) \triangleleft G$.

Prova:

1) Primeiramente, devemos verificar que $\overline{\psi}$ é uma função bem definida, isto é, se $gKer(\psi) = \tilde{g}Ker(\psi)$ então temos $\psi(g) = \psi(\tilde{g})$. Mas, $gKer(\psi) = \tilde{g}Ker(\psi)$ implica que $g = \tilde{g} \cdot k$, para algum $k \in Ker(\psi)$ e, portanto,

$$\psi(g) = \psi(\tilde{g} \cdot k) = \psi(\tilde{g}) \times \psi(k) = \psi(\tilde{g}) \times e_J = \psi(\tilde{g}).$$

Agora, $\overline{\psi}$ é claramente uma função sobrejetora e, para $g, g' \in G$, obtemos

$$\begin{aligned} \overline{\psi}(gKer(\psi) \cdot g'Ker(\psi)) &= \overline{\psi}((gg')Ker(\psi)) = \psi(g \cdot g') \\ &= \psi(g) \times \psi(g') = \overline{\psi}(gKer(\psi)) \times \overline{\psi}(g'Ker(\psi)); \end{aligned}$$

Assim $\overline{\psi}$ é um homomorfismo. Agora,

$$Ker(\overline{\psi}) = \{gKer(\psi) \mid \psi(g) = e_J\} = \{gKer(\psi) \mid g \in Ker(\psi)\} = eKer(\psi);$$

Assim $Ker(\overline{\psi}) = \{e_{G/Ker(\psi)}\}$, ou seja, $\overline{\psi}$ é injetiva.
Portanto, como $\overline{\psi}$ é um homomorfismo e é uma função bijetiva, temos que é isomorfismo.

2) Já sabemos que $\psi^{-1}(\psi(H)) = H(Ker(\psi)), \forall\, H \leq G$, e também que $\psi(\psi^{-1}(\mathcal{H})) = \mathcal{H} \cap \psi(G), \forall\, \mathcal{H} \leq J$. Daí, se $H \supseteq Ker(\psi)$ então $\psi^{-1}(\psi(H)) = H$, e se $\mathcal{H} \subseteq \psi(G)$ então $\psi(\psi^{-1}(\mathcal{H})) = \mathcal{H}$. Obtemos assim que as duas funções definidas em 2) são uma a inversa da outra. Só falta então mostrar que essas funções levam subgrupos normais em subgrupos normais.

Prova de a) Dados $y \in \psi(G)$ e $x \in \psi(H)$ quaisquer, devemos mostrar que $yxy^{-1} \in \psi(H)$. Temos $y = \psi(g)$ e $x = \psi(h)$, com $g \in G$ e $h \in H$, e logo $yxy^{-1} = \psi(g)\psi(h)\psi(g^{-1}) = \psi(ghg^{-1})$; como, por hipótese, $H \triangleleft G$, temos $ghg^{-1} \in H$ e portanto $yxy^{-1} \in \psi(H)$.

Prova de b) Dados $g \in G$ e $\alpha \in \psi^{-1}(\mathcal{H})$ quaisquer, devemos mostrar que $g\alpha g^{-1} \in \psi^{-1}(\mathcal{H})$. Temos

$$\psi(g\alpha g^{-1}) = \psi(g)\psi(\alpha)\psi(g^{-1}) = \psi(g)\psi(\alpha)\psi(g)^{-1}$$
$$\text{e } \psi(\alpha) \in \mathcal{H};$$

como, por hipótese, $\mathcal{H} \triangleleft \psi(G)$, temos $\psi(g\alpha g^{-1}) \in \mathcal{H}$ e portanto $g\alpha g^{-1} \in \psi^{-1}(\mathcal{H})$. E isto demonstra o Teorema 3.1. ∎

3.4 Aplicações

Aplicação 3.1. *Sejam $K \leq H \leq G$ com $K \triangleleft G$ e $H \triangleleft G$. Então,*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}.$$

Prova: Considere o homomorfismo

$$\begin{array}{rccc} \psi: & \frac{G}{K} & \longrightarrow & \frac{G}{H} \\ & gK & \longmapsto & gH \end{array}$$

A função ψ é bem definida; de fato $gK = \tilde{g}k$ implica que $g = \tilde{g}K$ para algum $k \in K$, e portanto que $gH = \tilde{g}kH = \tilde{g}H$ pois $k \in K \subseteq H$. Pela sua definição ψ é sobrejetiva e $Ker(\psi) = \{gK | \psi(gK) = H\} = \{aK | a \in H\} = H/K$. Aplicando a parte 1) do teorema 3.1 ao homomorfismo ψ, obtemos a aplicação. ∎

Aplicação 3.2. *Seja H um subgrupo normal de G. Então a função*

$$\begin{array}{rcl} \left\{\textit{subgrupos (normais) de } G \textit{ que contêm } H\right\} & \xrightarrow{1-1} & \left\{\textit{subgrupos (normais) de } \frac{G}{H}\right\} \\ K & \longmapsto & \frac{K}{H} \end{array}$$

é uma bijeção.

Prova: Consideremos o homomorfismo $\psi : G \longrightarrow \frac{G}{H}$, definido por $\psi(g) = gH$. Pela sua definição ψ é um homomorfismo sobrejetor e $Ker(\psi) = H$. Aplicando a parte 2) do teorema 3.1 ao homomorfismo ψ, e usando o fato que todo isomorfismo é uma bijeção, obtemos a aplicação. ∎

Aplicação 3.3. *Seja G um grupo e $Z(G)$ o centro do grupo G. Então, $\mathcal{I}(G) \simeq G/Z(G)$.*

Prova: Basta observar que a função,

$$\begin{aligned} \overline{\psi}: \ G &\to \mathcal{I}(G) \\ g &\longmapsto \psi_{g^{-1}} \end{aligned}$$

é um homomorfismo tal que: $Im(\overline{\psi}) = \mathcal{I}(G)$ e $Ker(\overline{\psi}) = Z(G)$.
De fato, ψ é um homomorfismo por $\overline{\psi}(gh) = \psi_{gh^{-1}}$ e $\psi_{gh^{-1}}(x) = (gh) \cdot x \cdot (h^{-1}g^{-1}) = g(h \cdot x \cdot h^{-1}) \cdot g^{-1} \Rightarrow \psi_{gh^{-1}}(x) = \psi_{g^{-1}}(\psi_{h^{-1}}(x)), \forall\, x \in G$.
Acabamos de ver que $\overline{\psi}$ é um homomorfismo e temos também que $Im(\overline{\psi}) = \mathcal{I}(G)$. Porém, $g \in G$ está em $Ker(\overline{\psi})$ se, e somente se, $\mathcal{I}_g = Id$, ou seja, $\mathcal{I}_g(x) = x, \forall x \in G$. Logo, $gx = xg$. Sendo assim $Ker(\psi) = Z(G)$. Portanto, pelo Teorema 3.1 temos que:

$$\mathcal{I}(G) \simeq G/Z(G)$$

∎

Aplicação 3.4. *Seja $\psi : G \to J$ um homomorfismo de grupos e seja H um subgrupo de G. Então a função*

$$\begin{aligned} \frac{H}{H \cap Ker(\psi)} &\longrightarrow \psi(H) \\ h \cdot (H \cap Ker(\psi)) &\longmapsto \psi(h) \end{aligned}$$

é um isomorfismo.

Prova: Consideremos o homomorfismo ψ restrito apenas ao subgrupo H e seja $K = H \cap Ker(\psi)$. Como $K \subset Ker(\psi)$ e $Ker(\psi) \lhd G$, então $K \lhd G$ e em particular $K \lhd H$. Assim, pelo teorema 3.1 a relação $h \cdot (H \cap Ker(\psi)) \longmapsto \psi(h)$ é um isomorfismo. ∎

Conclusão

Neste trabalho foram vistos alguns resultados já estudados na graduação durante a disciplina de estruturas algébricas que foram de grande importância para os estudos que se prosseguiram.

O estudo dos isomorfismos permite obter informações entre as estruturas isomorfas analisadas, com implicações importantes para a descrição de propriedades dentro e fora da matemática. O Teorema dos Isomorfismos de Grupos fornece um meio muito rico e interessante de trabalho, talvez por ser encontrado em alguns ramos da matemática, como a Álgebra e a Geometria. Além disso, as suas aplicações também podem ser vistas em outras áreas, como por exemplo na física, no que se diz respeito as propriedades ópticas dos cristais.

Referências Bibliográficas

[1] BOYER, C.B. *História da Matemática*. São Paulo: Editora Edgard Blücher Ltda, 1974.

[2] DOMINGUES, Hygino H.; IEZZI, Gelson. *Algebra Moderna*. 4ª ed. reformulada. São Paulo: Atual, 2003.

[3] EVES, Howard. *Introdução à história da matemática*. Tradução de Hygino H. Domingues. Campinas: UNICAMP, 2003.

[4] GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de Álgebra*. 4ª ed. Rio de Janeiro. IMPA, 2006.

[5] GONÇALVES, Adilson. *Introdução à álgebra*. 5ª ed. Rio de Janeiro. IMPA, 2006.

[6] LIVIO, Mario. *A equação que ninguém conseguiu resolver*: Como um gênio da matemática descobriu a linguagem da simetria. Tradução de Jesus de Paula Assis. 2ª ed. Rio de Janeiro. Recorde, 2011.

[7] Fraleigh, J. B. *A fisrt course in Abstract Algebra*. Disponível em https://uqu.edu.sa/files2/tiny_mce/plugins/filemanager/files/4290569/9/A%20First%20Course%20In%20Abstract%20Algebra-Jb%20Fraleigh,%207Ed%282003%29.pdf

(Acessado em 01/11/2014.)