UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VI - POETA PINTO DO MONTEIRO
CENTRO DE CIÊNCIAS HUMANAS E EXATAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

IZANETE NUNES DE LIMA

AUTOMORFISMOS DE GRUPOS CÍCLICOS: UM BREVE ESTUDO

MONTEIRO
2019

IZANETE NUNES DE LIMA

AUTOMORFISMOS DE GRUPOS CÍCLICOS: UM BREVE ESTUDO

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Álgebra

Orientador: Prof. Me. Luiz Lima de Oliveira Junior

MONTEIRO
2019

L372a Lima, Izanete Nunes de.

Automorfismos de grupos cíclicos [manuscrito] : um breve estudo / Izanete Nunes de Lima. - 2019.

35 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas , 2019.

"Orientação : Prof. Me. Luiz Lima de Oliveira Junior , Coordenação do Curso de Matemática - CCHE."

1. Automorfismos de grupos cíclicos . 2. Teorema de Lagrange. 3. Teoria de grupos. 4. Grupos cíclicos. I. Título

21. ed. CDD 512.2

Elaborada por Suzana Q. da Costa - CRB - 15/660 CCHE/UEPB

IZANETE NUNES DE LIMA

AUTOMORFISMOS DE GRUPOS CÍCLICOS: UM BREVE ESTUDO

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Álgebra

Aprovada em: 17/06/2019.

BANCA EXAMINADORA

Prof. Me. Luiz Lima de Oliveira Junior
Orientador

Prof. Me. Robson Batista de Sousa
Examinador interno (CCHE/UEPB)

Prof. Esp. Raquel Priscilla Ibiapino
Examinador interno (CCHE/UEPB)

Dedico este trabalho aos meus pais, Ivete Nunes e João Batista (In memoria) pelas preocupações para comigo e por terem dedicado suas vidas a me,em especial ao meu pai que plantou em mim forças para que eu pudesse concluir e a minha mãe que sempre me apoiou em minhas decisões, aos meus irmãos Izaildo Nunes e Izailma Nunes por todo apoio durante o curso de graduação em matemática e a todos que de forma direta ou indireta contribuíram com esse trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus por mais um ciclo concluído e por me conceder saúde, coragem e sabedoria no decorrer de todo o curso, pois sem a presença dele em minha vida, eu não estaria concluindo mais esse ciclo.

Ao meu pai João Batista de lima (In memoria), que nestes últimos semestres do curso acabei o perdendo o que tornou minha vida acadêmica mais difícil, pois ao primeiro momento pensei em desistir. Agradeço a ele por me educar da melhor maneira possível e por me colocar na escola aos três anos de idade e que sempre trabalhando na agricultura nunca mediu esforços para dar aos seus filhos tudo aquilo que ele não teve a oportunidade de ter. Agradeço ainda por ele ter me ensinado a nunca desistir dos meus sonhos, me encorajando para enfrentar os desafios do dia a dia, por ele me acordar cedo todos os dias para eu vir para a faculdade e que mesmo chovendo me falava que eu teria que ir pois meu futuro dependia somente de mim mesma.

A minha mãe Ivete Nunes de Lima que sempre me dava os melhores conselhos e que sempre me apoiava a buscar o melhor para minha vida. Agradeço por ela não ter me deixado desistir do curso quando perdi o meu pai e no momento em que cheguei para ela e falei que iria desistir do curso que não tinha mais importância, ela chegou para mim e disse: “Não desista, onde quer que seu pai esteja ele vai sentir orgulho de você”.

Aos meus irmãos Izaildo Nunes e Izailma Nunes que sempre estiveram ao meu lado e me apoiaram durante todo o decorrer do curso, além de me ensinarem a nunca desistir diante de uma dificuldade.

Ao meu sobrinho Luiz Felipe que esta a caminho para nos trazer mais alegrias e assim me preenchendo um vazio desde a partida do meu pai.

Ao meu noivo Sérgio Vinícius por todo o apoio durante o curso e por sempre está ao meu lado em todos os momentos.

A Maciel de Souza Assis que se tornou um irmão mais velho desde o início da minha vida acadêmica, fazendo que nossa vida na universidade se tornasse mais feliz e nas dificuldades ajudasse um ao outro.

Ao meu orientador Luiz Lima, pelas horas dedicadas e por todos os ensinamentos nesta reta final do curso, e que nunca mediu esforços para me orientar com todo o carinho possível, e sinto grata por ter aceitado o meu convite para ser sua orientanda. Os meus mais sinceros agradecimentos.

Aos professores Robson Batista, Tiago Madureira, Luiz Lima, Luciano dos Santos,

que me ensinaram muito mais que matemática, sempre me deram os melhores conselhos e que sempre irei sentir orgulho dos professores que tive na vida acadêmica.

A professora Raquel Priscila que ao chegar na universidade para ministrar aulas, tive a oportunidade de ela ser professora de logica matemática, mostrando-nos sempre que eramos capazes.

Agradeço a banca examinadora nas pessoas de Robson Batista e Raquel Priscila que durante o curso se fizeram presentes, e principalmente pelo carinho para com este trabalho e pelas palavras que irão o enriquecer.

Em fim, agradeço a todos os funcionários da universidade, em especial a Sr. Roberto, motorista da universidade que sempre me desejava Bom dia e quem em duas palavras tão simples tornava o meu dia mais feliz, e aos demais funcionários que de forma direta ou indireta fizeram parte desta jornada.

"Querido Deus, Tu és minha proteção, a minha fortaleza. Tu és o meu Deus, eu confio em Ti."
(Bíblia Sagrada, Salmo 91:2)

RESUMO

Neste trabalho apresentamos uma revisão bibliográfica sobre os automorfismos de grupos e também algumas aplicações. Para o desenvolvimento da Matemática, a comparação entre estruturas algébricas é de fundamental interesse para a obtenção de informações e extensão de propriedades. O desenvolvimento do trabalho se deu a partir de questionamentos sobre o que seria os automorfismos de grupos,depois de participar de um minicurso ministrado pelo professor orientador, onde me despertou curiosidades a respeito dos automorfismos de grupos.Este trabalho busca introduzir alguns conceitos e explorar alguns resultados da teoria dos grupos de automorfismos.

Palavras-chave: Homomorfismos.Isomorfismos .Automorfismos de grupos cíclicos .

ABSTRACT

In this work we present a bibliographic review on the automorphisms of groups and also some applications. For the development of Mathematics, the comparison between algebraic structures is of fundamental interest for the obtaining of information and extension of properties. The development of the work was based on questions about what would be the automorphisms of groups, after participating in a mini-course taught by the tutor, where I was curious about the automorphisms of groups. This work seeks to introduce some concepts and explore some results of the theory of automorphism groups.

textbf Keywords: Homomorphisms. Isomorphisms. Cyclic group autonomy.

LISTA DE SÍMBOLOS

γ	Letra grega Gama
λ	Lambda
ζ	Letra grega minúscula zeta
$\in$	Pertence
x^g	conjugado de x por g, ou seja, gxg^{-1}
G'	subgrupo derivado de G, ou seja, $[G, G]$
H_g	uma classe lateral de H em G.
$Z(G)$	centro do grupo G
$\|G : H\|$	índice do subgrupo H em G
$C_G(H)$	centralizador do subgrupo H em G
$N_G(H)$	normalizador do subgrupo H em G
$Im(f)$	imagem da função f
$\langle s \rangle$	grupo gerado por s
$\lhd$	subgrupo normal
$\times$	produto direto
$\ltimes$	produto semi-direto
C_n	grupo cıclico de ordem n
Aut(G)	grupo dos automorfismos de G
End(G)	conjunto dos endomorfismos de G
Inn(G)	grupo dos automorfismos internos de G
$O(g)$	ordem de um elemento $g \in G$
$\|G\|$	ordem do grupo G
$Cl(g)$	classe de conjugação de $g \in G$
$ker(\varphi)$	núcleo do homomorfismo φ
$G \cong H$	G é isomorfo a H

SUMÁRIO

1 INTRODUÇÃO 12
2 GRUPOS 14
2.1 Grupos 14
2.2 Subgrupos 14
2.3 Classes laterais e teorema de Lagrange 16
2.4 Subgrupos normais 18
3 HOMOMORFISMOS DE GRUPOS 20
3.1 Homomorfismos de Grupos 20
3.2 Isomorfismos de Grupos 21
3.3 Grupos Cíclicos 27
3.4 Homomorfismos e Automorfismos de Grupos Cíclicos 28
4 AUTOMORFISMOS DE GRUPOS 30
5 CONCLUSÃO 34

REFERÊNCIAS 35

1 INTRODUÇÃO

A teoria dos grupos desempenha um papel unificador em toda matemática e revela analogias e semelhanças entre os mais distintos ramos da matemática. A noção de grupo é antecedida, por uma outra noção também muito importante: A estrutura.

O que é uma estrutura?

Muitos sistemas matemáticos são estruturas relativamente a uma ou mais relações. Assim o conjunto dos números reais é uma estrutura relativamente a relação de ordem $x \leq y$ (x é menor ou igual a y); o conjunto dos inteiros não negativos é uma estrutura relativamente a relação $\frac{x}{y}$ (x é um divisor de y).

Ao longo dos anos constatou-se que a ideia de Grupo era muito importante em várias áreas da matemática, tanto que o estudo de grupos foi considerado o início da Álgebra Abstrata, quando passou-se a utilizar variáveis para representar números. As três principais áreas onde os estudos realizados motivaram a definição de grupo foram: a geometria do início do século XIX, a teoria dos números do fim do século XVIII, e a teoria das equações algébricas do fim do século XVIII. A Teoria dos grupos surge naturalmente em muitas áreas da matemática com implicações estendidas a outras ciências.

O objetivo principal deste trabalho é introduzir alguns conceitos e explorar resultados da Teoria dos Grupos de Automorfismos. Neste desenvolvimento, apresentamos as principais propriedades de automorfismos de grupos e as consequências obtidas para as estruturas avaliadas. Na matemática, um automorfismo é um isomorfismo de um objeto matemático nele mesmo. Em certo sentido, o automorfismo é uma simetria do objeto, ou uma forma de mapear o objeto nele mesmo mantendo a sua estrutura. Normalmente, o conjunto dos automorfismos de um objeto nele mesmo forma um grupo, chamado de grupo dos automorfismos, que pode ser chamado de grupo de simetria do objeto.

(GIL, 2002) A pesquisa é do tipo bibliográfica,pois é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos.

A justificativa deste trabalho se deu a partir de querer estudar os automorfismos de grupos,pois não tinha o conhecimento na graduação, também por não terem desenvolvido nenhum trabalho relacionado ao assunto e devido a curiosidade depois de participar de um minicurso ministrado pelo professor orientador.

Este trabalho é composto por três capítulos.

No capítulo 1, apresentamos os conceitos básicos relativos a teoria dos grupos,

pois estes conceitos permeiam a maior parte dos resultados abordados.

No capítulo 2, apresentamos os conceitos básicos relativos aos homomorfismos dos grupos, pois estes conceitos leva ao principal objetivo que são os automorfismos de grupos.

Finalmente, no capítulo 3, apresentamos o que é um automorfismos de grupos e alguns exemplos sobre os mesmos.

2 GRUPOS

O objetivo deste capitulo é introduzir os conceitos e propriedades da teoria de grupos necessário para este trabalho. Toda a sequencia teórica desenvolvida neste capitulo é a mesma apresentada por (GARCIA; LEQUAIN, 1988),(VIEIRA, 2013),(DOMINGUES; IEZZI, 2003).

2.1 Grupos

Definição 2.1. Um conjunto G com uma operação $\cdot : G \times G \to G$ dada por $(a, b) = a \cdot b$ é um grupo se as condições seguintes são satisfeitas:

i) A operação é associativa, isto é

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

ii) Existe um elemento neutro, isto é

$\exists \ e \in G \mid e \cdot a = a \cdot e = a, \ \forall \ a \in G.$

iii) Todo elemento possui um inverso, isto é $\forall \ a \in G, \ \exists \ b \in G \mid a \cdot b = b \cdot a = e$

Se além disso satisfaz a propriedade:

iv) A operação é comutativa, isto é

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

é chamado de grupo abeliano ou comutativo.

Exemplo 2.1. Vejamos

- $(\mathbb{Z}, +)$ é um grupo abeliano finito.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ é um grupo abeliano finito com n elementos.
- $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são grupos (aditivos) abelianos

2.2 Subgrupos

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

i) H é fechado, isto é, $\forall h_1, h_2 \in H$, temos $h_1 * h_2 \in H$

ii) H é um grupo.

Observação 2.1. Na definição de subgrupo a associatividade é sempre satisfeita, pois, a igualdade

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$$

é válida para todos os elementos de G.

2) O elemento neutro $e \in H$ de H é necessariamente igual ao elemento neutro e de G De fato, tomando

$$\alpha \in H \subseteq G,$$

temos $e \in H \cdot \alpha = \alpha$ e portanto, $eH = e$.

3) Dado $h \in H$, o inverso de h em H e necessariamente igual ao inverso de h em G. De fato, se k é o inverso de h em H, então $hk = kh = eH$, logo $hk = kh = eH$ pois $eH = e$, e portanto k é o inverso de h em G

Proposição 2.1. *Seja H um subconjunto não vazio do grupo G. Então H é um subgrupo de G se e somente se as duas condições seguintes são satisfeitas*

1) $\forall\ h_1, h_2 \in H$, temos $h_1 \times h_2 \in H$

2) $\forall\ H \in H$, temos $h^{-1} \in H$

Demonstração: Suponhamos que H seja um subgrupo de G. A condição

1) é então claramente satisfeita. Agora, seja $h \in H$; sendo H um grupo, h possui um inverso em H; mas, pela observação 3 precedente, tal inverso e necessariamente igual ao inverso de h em G, isto é, é necessariamente igual a h^{-1}, logo $h^{-1} \in H$, e a condição

2) é satisfeita. Reciprocamente, suponhamos que as duas condições 1) e 2) sejam satisfeitas. Então, a condição 0) é claramente satisfeita. Como já observamos, a condição i) sempre é satisfeita. Para ver que ii) é satisfeita, basta ver que $e \in H$; isto de fato acontece pois, tomando $h \in H$, temos que $h^{-1} \in H$ pela condição 2) e logo que $e = hh^{-1} \in H$ pela condição 1). Finalmente, que a condição iii) é satisfeita decorre da condição 2) ser satisfeita.

Exemplo 2.2. Exemplos de Subgrupos:

1) Dado um grupo G, $\{e\}$ e G são subgrupos de G.

2) $(2\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$. De maneira mais geral, se n é um inteiro qualquer, $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$

Definição 2.3. Um grupo G é dito cíclico quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$

Exemplo 2.3. Exemplos: $\mathbb{Z} = \langle 1 \rangle$, $\dfrac{\mathbb{Z}}{n\mathbb{Z}} =< \overline{1} >$.

Definição 2.4. Seja $\alpha \in G$. A ordem do elemento $\alpha \in G$ (e a denotamos por $0(\alpha)$) é a ordem do subgrupo gerado por α, isto é: por $0(\alpha) = |\langle \alpha \rangle|$.

Proposição 2.2. *Seja $\alpha \in G$ tal que $o(\alpha) = n < \infty$. Então*

$$n = min\{N \in \mathbb{N}^* | \alpha^N = e\}$$

e

$$\langle \alpha \rangle = \{e, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}.$$

Demonstração. Como $\langle \alpha \rangle = \{\alpha^m | m \in \mathbb{Z}\}$, e como, por hipótese, o grupo $\langle \alpha \rangle$ é finito, temos que existem $p, q \in \mathbb{Z}, p \neq q$ tais que $\alpha^p = \alpha^q$. Sem perda de generalidade, podemos supor que $p > q$. De $\alpha^p = \alpha^q$, temos que $\alpha^{p-q} = e$, isto é, obtemos que $\exists\ N > 0$ tal que $\alpha^N = e$ ($N = p - q$). Podemos então considerar o inteiro $r = min\{N \in \mathbb{N}^* | \alpha^N = e\}$. □

Afirmação: $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ e os elementos e, $\alpha, \alpha^2, \ldots, \alpha^{r-1}$ são todos distintos.

Demonstração da afirmação: Suponhamos que $\alpha^p = \alpha^q$ com $0 \leq p \neq q \leq r - 1$; podemos supor $p > q$. Temos então $\alpha^{p-q} = e$ com $0 < p - q < r$ e isso contradiz a minimalidade de r. Logo temos que $e, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ são elementos distintos de G. Para provar que $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, devemos mostrar que $\forall m \in \mathbb{Z}, \alpha^m = \alpha^l$ para algum $0 \leq l < r$. Para isso, observe que pelo algoritmo de Euclides, temos $m = qr + l$ com $r > l > 0$, e portanto $\alpha^m = \alpha^{qr+l} = (\alpha^r)^q \cdot \alpha^l = e^q \cdot \alpha^l = \alpha^l$

2.3 Classes laterais e teorema de Lagrange

Sejam G um grupo, H um subconjunto de G e a um elemento de G. Usamos as seguintes notações:

$$aH = \{ah\ | h \in H\} \text{ e } Ha = \{ha\ | h \in H\}.$$

Definição 2.5. (Classe lateral de H em G) Seja H um subgrupo do grupo G. O conjunto aH diz-se a classe lateral esquerda de H em G contendo a. O conjunto Ha diz-se a classe lateral direita de H em G contendo a. O elemento a diz-se um representante da classe lateral aH (ou Ha).

Exemplo 2.4. Sejam $G = \mathbb{Z}_9$ e $H = \{0, 3, 6\}$. Como a operação que estamos a considerar é a adição, usamos a notação $a + H$ em vez de aH. As classes laterais (esquerdas) de H em $\mathbb{Z}_9$ são:

i) $0 + H = \{0, 3, 6\} = 3 + H = 6 + H = H$;

ii) $1 + H = \{1, 4, 7\} = 4 + H = 7 + H$;

iii) $2 + H = \{2, 5, 8\} = 5 + H = 8 + H$.

Proposição 2.3. *Todas as classes laterais tem a mesma cardinalidade, igual a cardinalidade de H.*

Demonstração: De fato, a função

$$H \to xH$$

$$H \mapsto xh$$

É claramente uma bijeção.

Teorema 2.1. *(Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então vale que $|G| = |H| \cdot (G : H)$; em particular, a ordem e o índice de um subgrupo dividem a ordem do grupo.*

Demonstração. Considerando a relação de equivalência a esquerda em G, obtemos uma partição de G em classes de equivalência. A proposição anterior mostra que em cada uma dessas classes temos $|H|$ elementos. Como, por definição, o número de classes é $(G : H)$, temos a igualdade: $|G| = |H| \cdot (G : H)$ □

Corolário 2.1. Seja G um grupo finito e seja $\alpha \in G$. Então a ordem de α divide a ordem de G.

Demonstração. Por definição, $0(\alpha) = |\langle \alpha \rangle|$. Aplique agora o teorema de Lagrange ao subgrupo $\langle \alpha \rangle$. Note que, equivalentemente, este corolário diz que $\alpha|G| = e$. □

Corolário 2.2. (Pequeno Teorema de Fermat) Seja p um número primo.

Então

$$\alpha^{p-1} \equiv 1 mod p, \forall \alpha \in \mathbb{Z}/p\mathbb{Z}.$$

Demonstração. Seja $\alpha \in \mathbb{Z}/p\mathbb{Z}$; então $\bar{a} \in \mathbb{Z}/p\mathbb{Z}\ \{\bar{0}\}$. Agora, $\mathbb{Z}/p\mathbb{Z}\ \{\bar{0}\} = (\mathbb{Z}/p\mathbb{Z})^*$ é um grupo de $(p-1)$ elementos, logo $\bar{a}^{p-1} = \bar{1}$, ou seja $\alpha^{p-1} \equiv 1 (mod p)$. □

Corolário 2.3. (Euler) Sejam x e n inteiros relativamente primos , então temos $x\Phi(n) \equiv 1\ (mod n)$, onde Φ é a função de Euler.

Demonstração. Segue do corolário 1 depois de observar que $|(\mathbb{Z}/n\mathbb{Z})*| = \Phi(n)$. □

Corolário 2.4. Se G é um grupo de ordem prima, então G é cíclico.

Demonstração. Seja $\alpha \in G\ \{e\}$ e considere $\langle\alpha\rangle$ o subgrupo gerado por α. Pelo teorema de Lagrange temos que $|\langle\alpha\rangle|$ divide $|G|$ e portanto que $|\langle\alpha\rangle| = |G|$, pois $|G|$ é primo. Logo $G = \langle\alpha\rangle$. □

2.4 Subgrupos normais

Seja G um grupo e H um subgrupo de G. Queremos ver se á operação de G induz de maneira natural uma operação sobre o conjunto das classes laterais á esquerda de H em G, isto é se a operação

$$(xH, yh) \mapsto xyH$$

é bem definida no sentido de não depender da escolha dos representantes x e y. Dados $x, y \in G$ e $h, k \in H$ arbitrários, temos que x e xh são representantes da mesma classe xH e y e yk são representantes da mesma classe yH. Assim, a operação induzida sobre as classes laterais é bem definida se e só se

$$xyH = xhykH\ \forall\ x, y \in G,\ \forall\ h, k \in H$$

Logo, se e só se

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

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

Definição 2.6. Seja N um subgrupo de G. Dizemos que N é um subgrupo normal de G (e denotamos $H \lhd G$) se $xN = Nx$ para qualquer $x \in G$.

Exemplo 2.5. O subgrupo $2\mathbb{Z}$ é um subgrupo normal em $\mathbb{Z}$.

Proposição 2.4. *Seja H um subgrupo de G. As afirmações abaixo são equivalentes:*

i) a operação induzida sobre as classes laterais á esquerda de H 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, $\forall g \in G$, classe lateral de g á esquerda de H= classe lateral de g a direita de H.

Demonstração: Veja (DOMINGUES; IEZZI, 1982).

Exemplo 2.6. 1) $\{e\}, G$ são subgrupos normais de G.

2) $Z(G) \lhd G$; aliás,temos que $H < Z(G) \rightarrow H \lhd G$. Como $Z(G) < G$ deve mostrar que $\forall\ a \in G\ e\ x \in Z(G)$, temos que $axa^{-1} \in Z(G)$ então: $axa^{-1} = xaa^{-1} = x \in Z(G)$

$Z(G) \lhd GX \in aHa^{-1} \rightarrow x \in HX = aha^{-1} = haa^{-1} = h \in H$. Logo $aha^{-1} \subseteq H,\ \forall\ a \in G$ Portanto, $H \lhd G$.

3) $G' = \langle \{xyx^{-1}y^{-1} | x, y \in G\} \rangle$ é um subgrupo normal de G.

De fato, primeiro, observe que chamamos de S o conjunto $S = \{xyx^{-1}y^{-1} \| x, y \in G\}$, temos $\alpha \in S \rightarrow \alpha^{-1} \in S$, e consequentemente, se x_i é um elemento qualquer de $G' = \langle S \rangle, x_i$ se escreve da forma $x_i = \alpha_1 \dots \alpha_n$ com $\alpha_1, \dots, \alpha_[n] \in S$; segundo, se $g \in G$, temos $gx_[i]g^{-1} = g(\alpha_1 \dots \alpha_n)g^{-1} = (g\alpha_1 g^{-1})(g \dots \alpha_2 g^{-1}) \dots (g\alpha_n g^{-1})$ e consequentemente, para ver que $gx_i g^{-1} \in G'$, basta ver que $g\alpha g^{-1} \in S$ quando $\alpha \in S$; então $\alpha = xyx^{-1}y^{-1}$ um elemento de S; temos $g\alpha g^{-1} = g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in S$; isso acaba a prova de que $G' \lhd G$.

4) Se $(G : H) = 2$ então $H \lhd G$. Para mostrar isso, vamos mostrar que $xH = Hx\ \forall x \in G$. Se $x \in H$ então $xH = H = Hx$. Se $x \notin H$ temos

$$\begin{cases} xH \neq H \\ Hx \neq H. \end{cases}$$

Como $(G : H) = 2$, temos que existem exatamente 2 classes laterais á esquerda que são então xH e H. Agora, uma relação de equivalencia num espaço decompõe o espaço como união disjunta de suas classes de equivalência e assim $xH = G/H$; da mesma forma, $Hx = G/H$; portanto $xH = G/H = Hx$.

Teorema 2.2. *Seja H um subgrupo normal de G. Então o conjunto das classes laterais com a operação induzida de G é um grupo (chamado grupo quociente e denotado por G/H.*

Demonstração. Sejam xH, yH e $zh \in \dfrac{G}{H}$ e $x, y, z \in G$. Logo, $(zH \cdot xH) \cdot yH = (zxH)H \Longrightarrow xyzH = zHXYh = zH(xH \cdot yH)xH \cdot H = xH$, onde H é o elemento neutro. $x^{-1}H \cdot xH \Longrightarrow x^{-1} \cdot H \cdot xH = x^{-1} \cdot xH = H$. □

3 HOMOMORFISMOS DE GRUPOS

3.1 Homomorfismos de Grupos

Definição 3.1. Sejam $(G, *)$ e (J, Δ) dois grupos. Uma função $f : G \to J$ é um homomorfismo se ela é compatível com as estruturas dos grupos, isto é, se $f(a * b) = f(a)\Delta f(b)$ para todo a, b pertencente a G.

Exemplo 3.1. Considere os exemplos

1) $Id : (G, *) \to (G, *), Id(g) = g$, é um homomorfismo chamado identidade.

2) Seja H operado com G, então $Q : G \to G/H, Q(g) = gH$, é um homomorfismo chamado de projeção canônica.

4) Seja g pertencente a G fixo. Então, $I_g : G \to G, i_g(x) = gxg^{-1}$, é um homomorfismo bijetivo.

Propriedades Elementares:

Seja $f : (G, \cdot) \to (J, \times)$ um homomorfismo de grupos.

1 $f(e_G) = e_J$; de fato:

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \times f(e_G)$$

2) $f(x^{-1}) = f(x)^{-1}$; de fato:

$$e_J = f(e_G) = f(x \cdot x^{-1}) = f(x) \times f(x^{-1})$$

3) $kerf = \{x \in G | f(x) = e_J\}$, temos que $kerf \lhd G$ ($kerf$ é chamado de núcleo do homomorfismo de f).

Demonstração. Vejamos primeiramente que $kerf < G$. Dados $x, y \in kerf$, temos:

$$f(x \cdot y) = f(x) \times f(y) = e_g \times e_g = e_g$$

$$f(x^{-1}) = f(x)^{-1} = e_g^{-1} = e_g$$

Portanto, $kerf < G$. Para provar que $kerf \lhd G$ devemos mostrar que:

$$gxg^{-1} \in kerf, \forall g \in G, \forall x \in kerf.$$

Isto segue das igualdades abaixo:

$$f(gxg^{-1}) = f(g) \times f(x)f(g^{-1}) = f(g) \times e_g \times f(g)^{-1} = f(g) \times f(g)^{-1} = eg.$$

□

3.2 Isomorfismos de Grupos

Definição 3.2. Sejam G e J grupos. Um isomorfismo $f : G \longrightarrow J$ é um homomorfismo bijetor.

Exemplo 3.2. Exemplos de Isomorfismos

1) Os grupos S_3 e $S_\triangle$ são isomorfos. De fato considere a bijeção φ abaixo:

$$\varphi : S_3 \longrightarrow S_\triangle$$
$$id \longmapsto id$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha \longmapsto R_{\frac{2}{3}\pi}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha_2 \longmapsto R_{\frac{4}{3}\pi}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta \longmapsto R_3$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha\beta \longmapsto R_2$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha_2\beta \longmapsto R_1$$

como φ é um homomorfismo, logo, φ homomorfismo bijetivo e portanto um isomorfismo.

Teorema 3.1 (Teorema dos Homomorfismos)**.** *Seja $f : (G, \cdot) \to (\mathcal{G}, \Delta)$ um homomorfismo de grupos. Então*

1) *A função*

$$\bar{f}\colon \frac{G}{Kerf} \longrightarrow f(G)$$

$$g(Kerf) \longmapsto f(g)$$

É um isomorfismo.

2) *Temos as seguintes bijeções:*

$$\{Subgrupos\ de\ G\ que\ contém\ ker(f)\} \overset{1-1}{\longleftrightarrow} \{\ subgrupos\ de\ \ f(G)\}$$

$$H \longmapsto f(H)$$

$$f^{-1}(\mathscr{H}) \longleftarrow (\mathscr{H})$$

Além disso, estas bijeções levam subgrupos normais em subgrupos normais, isto é:

a) $H \lhd G \Rightarrow f(H) \lhd f(G)$.

b) $\mathscr{H} \lhd f(G) \Longrightarrow f^{-1}(\mathscr{H}) \lhd G$.

Demonstração.

1) Primeiramente, devemos verificar que $\bar{f}$ é uma função bem definida, isto é, se $g(kerf) = \tilde{g}(kerf)$ então $f(g) = f(\tilde{g})$. Mas, $g(kerf) = \tilde{g}(kerf)$ implica que $g = \tilde{g}\cdot k$, para algum $k \in kerf$ é portanto $f(g) = f(\tilde{g}\cdot k) = f(\tilde{g}) \times f(k) = f(\tilde{g}) \times e_g = f(\tilde{g}$. Agora,$\bar{f}$ é claramente uma função sobrejetora e, para $g, g' \in G$, obtemos:

$$\bar{f}(g(kerf))\cdot g'(kerf)) = \bar{f}(g\cdot g'(kerf)) = f(g\cdot g') = f(g) \times f(g') = \bar{f}(g(kerf)) \times \bar{f}(g'(kerf));$$

Assim $\bar{f}$

é um homomorfismo. Agora,

$$Ker\bar{f} = \{g(kerf)|f(g) = eg\} = \{g(kerf)|g \in kerf\};$$

Assim $ker\bar{f} = \left\{e\frac{G}{Kerf}\right\}$ ou seja, $\bar{f}$ é injetiva.

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

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

Prova de b): Dados $g \in G$ *e* $\alpha \in f^{-1}(\mathscr{H})$ quaisquer, devemos mostrar que $g\alpha g^{-1} \in f^{-1}(\mathscr{H})$. Temos $f(g\alpha g^{-1}) = f(g)f(\alpha)f(g^{-1})$ e $f(\alpha) \in \mathscr{H}$; como, por hipótese, $\mathscr{H} \triangleleft f(G)$, temos $f(g\alpha g^{-1}) \in \mathscr{H}$ e portanto $g\alpha g^{-1} \in f^{-1}(\mathscr{H})$. □

Corolário 3.1. Seja $f : G \to \mathscr{G}$ um homomorfismo de grupos e seja H um subgrupo de G. Então a função

$$\frac{H}{H \cap kerf} \longrightarrow f(H)$$
$$h(H \cap kerf) \mapsto f(h)$$

é um isomorfismo.

Demonstração. Considere o homomorfismo f restrito a H :

$$f|_H \colon H \longrightarrow \mathscr{G}$$
$$h \longmapsto f(h)$$

.

Claramente $f|_H(H) = f(H)$ e $(kerf) \cap H$. Aplicando a parte 1) do Teorema 3.1 dos homomorfismos ao homomorfismo $f|_H$, obtemos o corolário. □

Corolário 3.2. Seja H um subgrupo normal de G. Então temos a seguinte bijeção:

$$\{\ Subgrupos(normais)de\ G \text{ que contém } H\ \} \overset{1-1}{\longleftrightarrow} \left\{Subgrupos(normais)de\frac{G}{H}\right\}$$

Demonstração. Considere o homomorfismo projeção $\varphi \colon G \to \frac{G}{H}, \varphi(g) = gH$. Claramente, φ é um homomorfismo sobrejetor e $ker\varphi = H$. Aplicando a parte 2) do Teorema 3.1 dos homomorfismos ao homomorfismo φ, obtemos o corolário. □

Corolário 3.3. Sejam $H \triangleleft G$ e $k < G$. Então,

$$\frac{K}{H \cap K} \simeq \frac{HK}{H}$$

.

Demonstração. Já que $H \triangleleft G$, sabemos que KH é um subgrupo de G e que $HK = KH$. Claramente, $H \triangleleft G \Rightarrow H \triangleleft KH$ e portanto faz sentido considerar o grupo quociente $\frac{KH}{H}$. Considere o homomorfismo projeção $KH \xrightarrow{\varphi} KH/H$ e seja $\varphi|_k$ a sua restrição ao subgrupo $k < KH$, isto é:

$$\begin{aligned} \varphi|_k \colon K &\longrightarrow \frac{KH}{H} \\ k &\longmapsto kH \end{aligned}$$

Claramente,$Ker(\varphi|_k) = \{k \in K | kH = H\} = H \cap K$. Seja agora $\alpha \in KH/H$;temos $\alpha = (kh)H$ para algum $k \in K$ e algum $h \in H$; logo $\alpha = (kh)H = kH = \varphi|_k(k)$ e portanto $\varphi|_k$é sobrejetor. Aplicando agora a parte 1) do teorema dos homomorfismos ao homomorfismo $\varphi|_k$, obtemos o corolário. □

Corolário 3.4. Sejam $k < H < G$ com $K \triangleleft G$ e $H \triangleleft G$. Então,$\frac{G/K}{H/K} \simeq \frac{G}{H}$.

Demonstração. Considere o homomorfismo

$$\begin{aligned} \psi \colon \frac{G}{K} &\longrightarrow \frac{G}{H} \\ gK &\longmapsto gH \end{aligned}$$

A função ψ é bem definida pois $gK = \tilde{g}K$ implica que $g = \tilde{g}k$ para algum $k \in K$ e portanto $gH = \tilde{g}kH = \tilde{g}H$ pois $k \in K \subseteq H$. Claramente, ψ é sobrejetor e $ker\psi = H/K$. Aplicando a parte 1) do teorema dos homomorfismos ao homomorfismo ψ, obtemos o corolário. □

Exemplo 3.3. Considere

$$\begin{aligned} (\mathbb{Z}, +) &\longrightarrow U_n \\ k &\longmapsto e^{2\pi ki/n} \end{aligned}$$

Claramente φ é um homomorfismo sobrejetor e $ker\varphi = n\mathbb{Z}$; portanto $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq U_n$.

Observação 3.1. Seja H um subgrupo normal de G. Claramente, se $g : \frac{G}{H} \to \mathscr{G}$ é um homomorfismo injetivo de grupos, obtemos um homomorfismo $f : G \to \mathscr{G}$ com núcleo H, considerando $f = g \circ \varphi$, onde φ e a projeção canônica de G em $\frac{G}{H}$. Note que homomorfismos injetivos distintos de $\frac{G}{H}$ em $\mathscr{G}$ dão origem a homomorfismos de G em $\mathscr{G}$ também distintos.

O teorema dos homomorfismos mostra que todos os homomorfismos de G em $\mathscr{G}$ com núcleo H podem ser obtidos desta maneira. De fato, se $f : G \to \mathscr{G}$ é um tal

homomorfismo, tomando $g = \bar{f} : \frac{G}{H} \to \mathscr{G}$ (que é um homomorfismo injetivo), obtemos $f = g \circ \varphi$,

Assim, o problema de determinar todos os homomorfismos de G em $\mathscr{G}$ fica reduzido a determinação dos homomorfismos injetivos de $\frac{G}{H}$ em $\mathscr{G}$, onde H percorre os subgrupos normais de G.

Exemplo 3.4. Para determinar os homomorfismos de S_3 em $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ vamos considerar os subgrupos normais de S_3 que são:

$$\{id\}, \left\{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\} \text{ e } S_3$$

Se $H = \left\{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$, S_3/H é um grupo com dois elementos e existem exatamente três homomorfismos injetivos de S_3/H em $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$; portanto existem exatamente três homomorfismos de S_3 em $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ com núcleo $\left\{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$. Se $H = \{id\}$, não obtemos nenhum homomorfismo com núcleo {id}

Exemplo 3.5. Se $H = S_3$, existe exatamente um homomorfismo com núcleo S_3, a saber o homomorfismo trivial.

Definição 3.3. Seja $(G, \cdot)$ um grupo. Um automorfismo de G e um isomorfismo $f : G \to G$. O conjunto dos automorfismos de G será denotado por $Aut(G)$. É fácil verificar que a composição de dois automorfismos de G é um automorfismo de G e que $(Aut(G), \circ)$ é um grupo, onde " $\circ$ " denota a operação composição de funções.

Exemplo 3.6. Já observamos que $I_g : G \to G, I_g(x) = gxg^{-1}$, é um homomorfismo bijetivo e portanto um automorfismo de G, chamado automorfismo interno associado ao elemento $g \in G$. O conjunto dos automorfismos internos será denotado por $I_g(G)$; assim

$$I_g = \{I_g | g \in G\} \subseteq Aut(G)$$

Proposição 3.1. $(I(G), \circ)$ *é um subgrupo normal de* $(Aut(G), \circ)$.

Demonstração: Que $I(G)$ seja um subgrupo de $Aut(G)$ segue das igualdades:

$$I(g)^{-1} = I(g)_{g-1} e I_{g1} \circ I_{g2} = I_{g1g2}$$

Vamos agora mostrar que $I(G)$ é normal em $(Aut(G), \circ)$, isto é, dado $\sigma \in (Aut(G)$ e $g \in G$ quaisquer, temos $\sigma \circ I_g \circ \sigma^{-1} \in I(G)$.

Para todo $x \in G$, temos:

$$(\sigma \circ I_g \circ \sigma^{-1})(x) = \sigma \circ I_g(\sigma^{-1}(x)) = \sigma(g\sigma^{-1}(x)g^{-1})$$

$$= \sigma(g)x\sigma(g)^{-1} = I_{\sigma(g)}(x);$$

Portanto $\sigma \circ I_g \circ \sigma^{-1} = I_{\sigma(g)} \in I(G)$.

Observação 3.2. 1) Seja G um grupo e seja $g \in G$. Temos que g comuta com todos os elementos de G se e só se $I_g = id$. Portanto, G é um grupo abeliano $\Leftrightarrow I(G) = \{id\}$.

2) $H \lhd G \Leftrightarrow H$ é estável por todos os automorfismos internos de $G(i.e. I_g(H) \subseteq H \ \forall \ g \in G)$. 3) Existem automorfismos que não são automorfismos internos. Por exemplo, Seja G um grupo abeliano que possui um elemento y de ordem ≥ 3; é fácil ver que $\rho : G \to G, \rho(x) = x^{-1}$, é um homomorfismo bijetivo e portanto um automorfismo de G; ρ não é a aplicação identidade pois $\rho(y) = y^{-1} \neq y$ e portanto, pela observação 1),ρ não é um automorfismo interno Assim, em particular, obtemos que

$$\mathbb{Z} \to \mathbb{Z}$$

$$n \mapsto -n$$

e

$$\frac{\mathbb{Z}}{d\mathbb{Z}} \to \frac{\mathbb{Z}}{d\mathbb{Z}}$$

$$\bar{r} \mapsto \bar{r}$$

(com $d \geq 3$)

São exemplos de automorfismos que não são automorfismos internos.

Definição 3.4. Um subgrupo H de G é um subgrupo característico (denotado por $H \star G$) se ele é estável por todos os automorfismos de G, isto é, se $\sigma(H) \subset H \ \forall \ \sigma \in Aut(G)$. (Equivalente, se $\sigma(H) = H \forall \sigma \in Aut(G)$). Claramente, $H \star G \Rightarrow H \lhd G$.

Exemplo 3.7. $\{e\}, G, Z(G)$ e G' são subgrupos característicos de G.

Proposição 3.2. *Seja $K \star H \lhd G$. Então $K \lhd G$.*

Demonstração. Queremos mostrar que $I_g(K) = K, \ \forall \ g \in G$. Seja $g \in G$ e $I_g : G \to G, I_g(x) = gxg^{-1}$. Considere a restrição de I_g a H :

$$I_g|_H \longrightarrow G$$

$$h \longmapsto gxg^{-1}$$

Como, por hipótese, $H \lhd G$, temos que $I_g|_H(H) = H$ e portanto $\sigma : H \to H, \sigma(h) = gxg^{-1}$, é um automorfismo de H (não é um automorfismo interno de H em geral, quando g não pertence a H). Como, por hipótese, $K \star H$ e $\sigma,\ \forall\ Aut(H)$, temos $I_g(K) = \sigma(K) = K$.

□

Observação 3.3. Em geral, $K \lhd H \lhd G$ não implica que K seja normal em G. Por exemplo no grupo $D_\square$, temos: $\langle R_1 \rangle \lhd \langle R_2, R_\pi \rangle \lhd D_\square$ mas normal em $\langle R_1 \rangle$ é $D_\square$.

3.3 Grupos Cíclicos

Proposição 3.3. *a) Os subgrupos de* $(\mathbb{Z}, +)$ *são* (0) *e* $(n\mathbb{Z}, +)$ *com* $n = 1, 2, 3, \ldots$ *b)* $m\mathbb{Z} \supseteq n\mathbb{Z} \Leftrightarrow m|n$*; nesse caso* $(m\mathbb{Z} : n\mathbb{Z}) = n/m$.

Demonstração. a) Já foi feita. b) É claro que $m\mathbb{Z} \supseteq n\mathbb{Z} \Leftrightarrow m|n$. Suponhamos que $n\mathbb{Z} < m\mathbb{Z} < \mathbb{Z}$; tomando $K = n\mathbb{Z}$ e $H = m\mathbb{Z}$ no corolário 3.4, obtemos

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}}$$

,

Portanto, $\frac{n}{m\mathbb{Z}/n\mathbb{Z}} = m$ e daí $m\mathbb{Z} : n\mathbb{Z} = n/m$.

□

Exemplo 3.8. 1- $\mathbb{Z} =< 1 >=< -1 >$,

2- $n\mathbb{Z} =< n >=< -n >$,

3- $\mathbb{Z}_8 =< 1 >=< 3 >=< 5 >=< 7 >$

Proposição 3.4. *Seja* $G = \{\ldots, \alpha^{-1}, e, \alpha, \alpha^{-2}, \ldots\}$ *um grupo cíclico de ordem infinita. Então: a) A função* $f : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$, $f(z) = \alpha^z$*, é um isomorfismo. b) O elemento* α^z *gera G se e somente se* $z = 1$ *ou* $z = -1$.

Demonstração. a) A função $f : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$, $f(z) = \alpha^z$, é um homomorfismo pois $f(z_1 + z_2) = a^{z_1+z_2} = a^{z_1} \cdot a^{z_2} = f(z_1) \cdot f(z_2)\ \forall\ z_1, z_2 \in \mathbb{Z}$ f é claramente uma bijeção e portanto um isomorfismo. b) A função $f : z \mapsto \alpha^z$, sendo um isomorfismo, α^z gera $\mathbb{Z}$ se e somente se z gera $\mathbb{Z}$. Agora, claramente, os únicos elementos que geram $\mathbb{Z}$ são $z = 1$ ou $z = -1$.

□

Proposição 3.5. *Seja* $G = \{e, \alpha, \ldots, \alpha^{n-1}\}$ *um grupo cíclico de ordem finita igual a n. Então:*

a) A função $f : (\mathbb{Z}/n\mathbb{Z}, +_n) \longrightarrow (G, \cdot)$, $f(\bar{m}) = \alpha^m$*, é um isomorfismo.*

b) O elemento α^m *gera G se e somente se M.D.C.*$\{m, n\} = 1$.

Demonstração. a) Como vimos na prova da proposição 3.4, a função f de $\mathbb{Z}$ em G dada por $z \mapsto \alpha^z$ é um homomorfismo, claramente sobrejetor. Sendo isomorfo a $G, \mathbb{Z}/Kerf$ tem n elementos e portanto $Kerf = n\mathbb{Z}$.

b) A função $\bar{m} \mapsto \alpha^m$ sendo um isomorfismo, α^m gera G se e somente se $\bar{m}$ gera $(\mathbb{Z}/n\mathbb{Z}, +_n)$, se e somente se $M.D.C.\{m, n\} = 1$.

□

Proposição 3.6. *Seja $G = \langle\alpha\rangle = \{e, \alpha, \ldots, \alpha^{n-1}\}$ um grupo cíclico finito de ordem n.*

a) Se $H \neq \{e\}$ é um subgrupo de G, então H é cíclico; de maneira precisa, $H = \langle\alpha^m\rangle$ onde m é o menor inteiro positivo tal que $\alpha^m \in H$; H tem ordem igual a $\frac{n}{m}$.

b) Se d é um divisor de n, então existe um único subgrupo H de ordem igual a d; este subgrupo é $H = \langle\alpha^{\frac{n}{d}}\rangle$.

Demonstração. A proposição é uma consequência da proposição 3.3, do corolário 3.2 e da proposição 3.5. Fazemos abaixo uma prova direta que utiliza, essencialmente, os mesmos argumentos.

a) Seja m o menor inteiro positivo tal que $\alpha^m \in H$. Claramente, $\langle\alpha^m\rangle \subseteq H$. Reciprocamente, seja $\alpha^u \in H$; vamos mostrar que m|u (o que claramente implicara que $\alpha^u \in \langle\alpha^m\rangle$). Fazendo a divisão de u por m, temos

$$u = qm + r$$

com $0 \leq r < m$

Entao, $\alpha^u = (\alpha^m)^q \cdot \alpha^r$. Como $\alpha^u \in H$ e $\alpha^m \in H$, temos que $\alpha^u \in H$ e portanto, pela minimalidade de m,temos que $r = 0$ e logo que $m|u$. Agora, é fácil verificar que a ordem de α^m (e portanto a ordem de H) é igual a n/m.

b) Seja d um divisor de n. O subgrupo $\langle\alpha^{n/d}\rangle$ tem ordem d. Vamos agora provar a unicidade. Seja então H um subgrupo qualquer de ordem d; pela parte a), temos que $H = \langle\alpha^m\rangle$ com m inteiro tal que $\frac{n}{m}$ seja a ordem de H, isto é $\frac{n}{m} = d$, portanto $m = n/d$ e $H = \langle\alpha^{n/d}\rangle$.

□

Observação 3.4. Mas precisamente, é possível mostrar que:

$$(\frac{\mathbb{Z}}{2^r\mathbb{Z}}^*) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{r-2}\mathbb{Z}}, \forall r \geq 1, p^{r-1}(p-1)\mathbb{Z}, \forall p \text{ primo impar e } \forall r \geq 1.$$

3.4 Homomorfismos e Automorfismos de Grupos Cíclicos

Proposição 3.7. *Sejam $G = \langle a\rangle$ um grupo cíclico e J um grupo qualquer. Seja $b \in J$.*

a) Se $0(a) < \infty$ *e* $0(b) \nmid 0(a)$ *, então não existe nenhum homomorfismo* $f : G \to J$ *tal que* $f(a) = b$.

b) Se $0(a) < \infty$ *e* $0(b)|0(a)$ *, então existe um único homomorfismo* $f : G \to J$ *tal que* $f(a) = b$*; tal* f *é dado por* $f(a^r) = b^r$.

c) Se $0(a) = \infty$ *(com* $0(b)$ *qualquer), então existe um único homomorfismo* $f : G \to J$ *tal que* $f(a) = b$*; tal* f *é dado por* $f(a^r) = b^r$.

Demonstração. a) Já foi feita.

b) e c): Considere $f : G = \langle a \rangle \to J$, $f(a^r) = b^r$; observe que um mesmo elemento $\xi \in G$ pode ter duas representações $\xi = a^r$ e $\xi = a^s$; para que f seja uma função bem definida devemos verificar que o valor $f(\xi)$ é independente da representação, isto é, devemos verificar que se r e s são dois inteiros tais que $a^r = a^s$, então $b^r = b^s$.

Se $0(a) = \infty$, então todo elemento $\xi \in < a >$ tem uma representação única $\xi = a^r$ (pois $a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow r - s = 0 \Leftrightarrow r = s$). Portanto, se $0(a) = \infty$, f é realmente uma função, qualquer que seja a ordem do elemento $b \in g$.

Suponha agora que $0(a) < \infty$. Sejam $\xi = a^r$ e $\xi = a^s$ duas representações de ξ. Temos $a^{r-s} = e$, logo $r - s$ é múltiplo de $0(a)$; como por hipótese $0(b)|0(a)$, temos que $r - s$ é múltiplo da ordem de $0(b)$ e portanto $b^{r-s} = e$, donde $b^r = b^s$, Assim, vemos que também nesse caso a função f é bem definida. Deixamos a cargo do leitor a verificação de que a função f assim definida é realmente um homomorfismo. Este é o único homomorfismo que leva a em b pois, se g é um homomorfismo tal que $g(a) = b$, então temos:

$$g(a^r) = g(a)^r = b^r) \ \forall \ r \in \mathbb{Z},$$

E portanto temos $g = f$. □

Exemplo 3.9. Seja $G = \dfrac{\mathbb{Z}}{8\mathbb{Z}} = \langle \bar{1} \rangle$ e $J = \dfrac{\mathbb{Z}}{10\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{9}\}$.

Procuramos todos os homomorfismos f de G em J. Os elementos $b \in J$ tais que $0(b)|0(\bar{1}) = 8$ são $\bar{0}, \bar{5}$. Portanto, pela proposição anterior, os homomorfismos de $\dfrac{\mathbb{Z}}{8\mathbb{Z}}$ em $\dfrac{\mathbb{Z}}{10\mathbb{Z}}$ são:

$$\begin{aligned} f_1 : \frac{\mathbb{Z}}{8\mathbb{Z}} &\longrightarrow \frac{\mathbb{Z}}{10\mathbb{Z}} \\ \bar{n} &\longmapsto \bar{0} \end{aligned}$$

que é um homomorfismo trivial

$$\begin{aligned} f_2 : \frac{\mathbb{Z}}{8\mathbb{Z}} &\longrightarrow \frac{\mathbb{Z}}{10\mathbb{Z}} \\ \bar{n} &\longmapsto \bar{5n} \end{aligned}$$

4 AUTOMORFISMOS DE GRUPOS

Neste capítulo, veremos alguns resultados preliminares para uma melhor compreensão dos grupos e de seus automorfismos.

Definição 4.1. Sejam G e H dois grupos.

(i) Um homomorfismo $f : G \mapsto H$ é uma função tal que $f(ab) = f(a)f(b)$ $\forall a, b \in G$.

(ii) Um monomorfismo $f : G \mapsto H$ é um homomorfismo injetor.

(iii) Um epimorfismo $f : G \mapsto H$ é um homomorfismo Seja G um grupo.

(iv) Um isomorfismo $f : G \mapsto H$ é um homomorfismo bijetor.

(v) Um endomorfismo de um grupo G é um homomorfismo de grupos $\sigma : G \mapsto H$. O conjunto de todos os endomorfismos de G será denotado por

$$End(G) = \{\sigma : G \mapsto G : \sigma \text{ é um homomorfismo de grupos}\}.$$

Exemplo 4.1. A identidade $id : G \mapsto G$ é um exemplo de Endomorfismo.

Definição 4.2. Um automorfismo de um grupo G e um isomorfismo $f : G \to G$. O conjunto dos automorfismos de G será denotado por $Aut(G)$.

$$Aut(G) = \{f : G \mapsto G : f \text{ é um isomorfismo}\}$$

Claramente a função identidade é um automorfismo de G.

Exemplo 4.2. Seja G cíclico de ordem 9. então seus automorfismos so:

$g \longmapsto g$

$g \longmapsto g^2$

$g \longmapsto g^4$

$g \longmapsto g^5$

$g \longmapsto g^7$

$g \longmapsto g^9$

Portanto, $Aut(G)$ é um grupo abeliano de ordem 6, ou seja, $Aut(G) \cong \mathbb{Z}_6$.

Proposição 4.1. *O conjunto $Aut(G)$ é um grupo com a operação de composição de funções.*

Demonstração. Inicialmente provemos que $Aut(G)$ é fechado em relação á composição de funções. Sejam $f, g \in Aut(G)$ e $x, y \in G$. Daí

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

.

Como a composição, $f \circ g$, de funções bijetivas é também bijetiva, decorre que $f \circ g \in Aut(G)$. Agora, a função identidade

$$Id : G \to G$$

$$x \longmapsto x$$

é um automorfismo de G e será o elemento neutro de $Aut(G)$, já que, para todos $f \in Aut(G)$ e $x \in G$,

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

Além disso, para cada $f \in Aut(G)$, existe $f^{-1} \in Aut(G)$ tal que, para todo $x \in G$,

$$(f \circ f^{-1})(x) = Id(x) \text{ e } (f^{-1} \circ f)(x) = Id(x).$$

Logo todo elemento de $Aut(G)$ possui inverso. Finalmente, a composição de funções satisfaz a associatividade, pois

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

Portanto, $Aut(G)$ é um grupo com a composição de funções. □

Exemplo 4.3. A aplicação $\varphi \in \mathbb{Z}^{\mathbb{Z}}$ definida por

$$\varphi(x) = -x \ \forall x \in \mathbb{Z},$$

é um automorfismo de $(\mathbb{Z}, +)$

Exemplo 4.4. Seja $(M, \perp) = (\mathbb{R}, \cdot)$. A aplicação $\varphi \in \mathbb{R}^{\mathbb{R}}$, definida por

$$\varphi(x) = x^3 \forall x \in \mathbb{R},$$

é um automorfismo de $(M; \perp)$

Proposição 4.2. *Se G é um grupo cíclico então $Aut(G)$ é um grupo abeliano.*

Demonstração. Seja G um grupo cíclico e seja g um gerador de G. Considerando $f_1; f_2 \in Aut(G)$, queremos mostrar que $f_1 f_2 = f_2 f_1$. Para isto é suficiente mostrarmos que $(f_1 f_2)(g) = (f_2; f_1)(g)$. Suponha que $f_1(g) = g^r$ e $f_2(g) = g^s$. Assim

$$(f_1 f_2)(g) = f_1(f_2(g)) = f_1(g^s) = f_1(g)^s = g^{rs}$$

e

$$(f_2; f_1)(g) = f_2(f_1(g)) = f_2(g^r) = f_2(g)^r = g^{rs};$$

como queríamos demonstrar. □

Exemplo 4.5. Temos que

$$G \cong \mathbb{Z}; \text{ se } G \text{ é cíclico infinito, e}$$

$$G \cong \mathbb{Z}_n; \text{ se } G \text{ é cíclico finito, de } |G| = n < 1 :$$

Portanto, para conhecer o grupo de automorfismos de grupos cíclicos, devemos estudar $Aut(\mathbb{Z})$ e $Aut(\mathbb{Z}_n)$.

Proposição 4.3. $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$.

Demonstração. Considere $G = \langle g \rangle$ cíclico infinito, $f \in Aut(G)$ e $f(g) = g^k$. Como $Im(f) = G$ então g^k é um gerador de G, pois $G = Im(f) = h\langle(g)\rangle = \langle g^k \rangle$. Com isso $g = g^{kl}$, para algum $l \in \mathbb{Z}$. Como G é infinito então $kl = 1$ implica $k = 1$ e $l = 1$ ou $k = -1$ e $l = -1$. Desta maneira, um grupo cíclico infinito possui apenas dois automorfismos:

$$g \longmapsto g$$
$$g \longmapsto g^{-1}$$

ou seja, Aut(G) é um grupo de ordem 2, e portanto, cíclico. Isto implica

$$Aut(\mathbb{Z}) \cong \mathbb{Z}_2.$$

Agora vamos aproveitar a demonstração anterior para determinar a ordem de Aut(G) quando G é cíclico finito de ordem n.

Usando a informação acima, vemos que $g^{kl-1} = 1$. Logo, se $|G| = n$ então $n|(kl - 1)$. Portanto, $kl + sn = 1$, para algum $s \in Z$ o que implica, que $mdc(k, n) = 1$. Assim, os automorfismos de um grupo cíclico finito de ordem n são dados por:

$$g \longmapsto g^k$$

onde $mdc(k,n) = 1, 1 \leq k \leq n-1$. Logo, temos $\varphi(n)$ automorfismos de G, lembrando que φ é conhecida com a função de Euler. Assim, segue que $|Aut(G)| = \varphi(n)$.

□

Exemplo 4.6. Tome um grupo cíclico G de ordem $2^4 \cdot 3^2 \cdot 11$. Vejamos o que ocorre com o $Aut(G)$. Temos o seguinte grupo

$$\mathbb{Z}_2^4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_{11}.$$

Como eles possuem ordem relativamente primas entre si então teremos que:

$$Aut(\mathbb{Z}_2^4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_{11}) \cong Aut(\mathbb{Z}_2^4) \times Aut(\mathbb{Z}_3^2) \times Aut(\mathbb{Z}_{11})$$

Portanto,

$$Aut(\mathbb{Z}_{1584}) \cong Aut(\mathbb{Z}_2^4) \times Aut(\mathbb{Z}_3^2) \times Aut(\mathbb{Z}_{11}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_{10}.$$

5 CONCLUSÃO

Neste trabalho, estudamos alguns automorfismos de grupos, os quais são de grande importância no ensino de álgebra, especificamente em estruturas algébricas. Além de estudar os automorfismos de grupos, precisávamos de alguns resultados preliminares para chegarmos ao nosso objetivo de estudo, como o estudo de grupos, subgrupos, grupos cíclicos e entre outros.

A importância de estudar o grupo de automorfismos Aut(G) é que este tem aplicações em varias áreas da Matemática, tais como Teoria dos Grupos Finitos, Teoria de Representação de Grupos e Álgebras, K-Teoria, Combinatória, Geometria e Códigos Corretores de Erros.

REFERÊNCIAS

DOMINGUES, H. H.; IEZZI, G. Álgebra moderna. **Atual Editora**, 1982. Citado na página 19.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. fourth. [S.l.]: Atual, 2003. Citado na página 14.

GARCIA, A.; LEQUAIN, Y. **Álgebra: um curso de introdução**. [S.l.]: IMPA, 1988. Citado na página 14.

GIL, A. C. **Como elaborar projetos de pesquisa**. [S.l.]: Atlas, 2002. Citado na página 12.

VIEIRA, V. lopes. **Álgebra abstrata para licenciatura**. [S.l.]: eduepb, 2013. Citado na página 14.