UNIVERSIDADE FEDERAL DE OURO PRETO

DEPARTAMENTO DE MATEMÁTICA

Ana Twayene Pereira

O Problema do Isomorfismo de Anéis de Grupos sobre os Inteiros

Para grupos abelianos finitos

Ouro Preto, Brasil

2021

UNIVERSIDADE FEDERAL DE OURO PRETO

Ana Twayene Pereira

O Problema do Isomorfismo de Anéis de Grupos sobre os Inteiros

Para grupos abelianos finitos

Monografia submetida ao Curso de Matemática da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do Grau de Graduado em Bacharelado em Matemática.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira

Universidade Federal de Ouro Preto – UFOP

Instituto de Ciências Exatas e Biológicas

Departamento de Matemática

Ouro Preto, Brasil

2021

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
COLEGIADO DO CURSO DE BACHARELADO EM MATEMATICA

FOLHA DE APROVAÇÃO

Ana Twayene Pereira

O Problema do Isomorfismo de Anéis de Grupos sobre os Inteiros Para Grupos Finitos Abelianos

Monografia apresentada ao Curso de Bacharelado em Matemática da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Matemática

Aprovada em 14 de outubro de 2021

Membros da banca

Dr. Edney Augusto Jesus de Oliveira - Orientador - Universidade Federal de Ouro Preto
Dra. Ana Paula da Silva Cota - Universidade Federal de Ouro Preto
Dr. Juliano Soares Dias - Universidade Federal de Ouro Preto

Edney Augusto Jesus de Oliveira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em XX/XX/XXXX

Documento assinado eletronicamente por **Edney Augusto Jesus de Oliveira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 14/12/2021, às 19:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0223400** e o código CRC **2482AFEC**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.009930/2021-59 SEI nº 0223400

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: - www.ufop.br

Aos meus pais Leidiane e Sérgio
Às minhas irmãs Tatielle e Tainah
Às minhas amigas e amigos que estiveram ao meu lado ao longo da minha trajetória, em especial ao meu grande amigo Alisson.

Agradecimentos

Ao meu orientador Edney pela calma, paciência, dedicação, incentivo, conselhos e pelos momentos enriquecedores ao longo dos anos, um verdadeiro orientador.

À professora Regina pelos sábios conselhos e amizade ao longo do curso, uma grande inspiração.

Ao Pedro pelas conversas tranquilas que acalmaram minha mente.

À Stefani pela docura e risadas ao longo da minha caminhada.

À Júlia por ser eternamente minha duplinha de curso e amiga além da UFOP.

À Mônica pela alegria, pelas conversas e conselhos, uma grande amiga que parece que me conhece a vida toda.

Ao Raphael que me traz paz, felicidade e carinho na maioria dos momentos, meu confidente a qualquer hora.

Ao meu amigo Alisson pela pacência de escutar minhas lamúrias, pelo apoio, sem você nada disso seria possível, como diria Emicida "quem tem um amigo tem tudo", com todo meu amor.

Aos meus colegas Allan, Bárbara, Cyndi, Rafael e Thallys que se tornaram amigos ao longo da minha trajetória.

À minha família pelo apoio, em especial, à minha mãe que sempre fez o possível para me ajudar, ao meu pai por me busca da UFOP e às minhas irmãs por aguentarem a luz acesa de madrugada.

"Liberte a tua mente pra ela não desandar
Lembra que é valente como as águas do mar
É que é tapete de serpente que dão pra nois pisar
Andai com passo firme que é pra não bambear."
(Valente - MC Tha)

Resumo

Neste trabalho iremos abordar a teoria de anéis de grupo, em particular o problema intitulado como *O Problema do Isomorfismo para Anéis de Grupos*. Para obtermos um embasamento teórico para a análise do problema estudaremos as teorias de anéis, grupos, representação de grupos, módulos, produto tensorial e anéis de grupos, estruturas importantes na área capes Álgebra Abstrata.

O Problema do Isomorfismo de Anéis de Grupo, resultado central da monografia, consiste em determinar se é suficiente KG ser isomorfo a KH para obtermos G isomorfo a H, com K um corpo e G, H dois grupos. Vale salientar que iremos restringir o problema para o caso dos anéis dos inteiros e grupos abelianos finitos, ou seja, provando que se G um grupo finito abeliano e $\mathbb{Z}G$ é isomorfo a $\mathbb{Z}H$, então G será isomorfo a H, utilizando os resultados obtidos nos fundamentos teóricos descritos ao longo do trabalho.

Palavras-chave: anel. grupo. anel de grupo. problema do isomorfismo. Isomorfismo de anel de grupo.

Abstract

In this work we will approach the theory of group rings, in particular the problem entitled "The Problem of Isomorphism for Group Rings". In order to obtain a theoretical basis for the analysis of the problem, we will study the theories of rings, groups, representation of groups, modules, tensor product and group rings, important structures in the field of Abstract Algebra capes.

The Group Rings Isomorphism Problem, central result of the monograph, consists in determining whether it is enough for KG to be isomorphic to KH to obtain G isomorphic to H, with K a body and G , H two groups. It is worth noting that we will restrict the problem to the case of integer rings and finite abelian groups, that is, proving that if G is a finite abelian group and $\mathbb{Z}G$ is isomorphic to $\mathbb{Z}H$, then G will be isomorphic to H, using the results obtained in the theoretical foundations described throughout the work.

Keywords: ring. group. group ring. problem of isomorphism. group ring isomorphism.

Lista de abreviaturas e siglas

UFOP	Universidade Federal de Ouro Preto

Lista de símbolos

R	Anel
RG	Anel de grupo
$\varepsilon(\alpha)$	Aumento de α
$\|A\|$	Cardinalidade do conjunto A
$Z\,(G)$	Centro do grupo
$\mathbb{Z}_m$	Conjunto das classes de residuais módulo m
G/H	Conjunto das classes laterais à esquerda
$\mathbb{M}_{n\times n}\,(\mathbb{R})$	Conjunto das matrizes de ordem n sobre R
$Ddz(R)$	Conjunto dos divisores de zero do anel R
R^*	Conjunto dos elementos invertíveis de R
$U(\mathbb{Z}G)$	Conjunto dos elementos invertíveis de $\mathbb{Z}G$
$U_1(\mathbb{Z}G)$	Conjunto dos elementos invertíveis normalizados de $\mathbb{Z}G$
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$Reg(R)$	Conjunto dos regulares de R
$\langle S\rangle$	Conjunto gerado por S
$det(A)$	Determinante de A
G	Grupo
$W(n,K)$	Grupo de Weyl
$SL(n,K)$	Grupo linear especial
$GL(n,K)$	Grupo linear geral
$O(n,K)$	Grupo ortogonal

$SO(n, K)$	Grupo ortogonal especial
S_X	Grupo de permutação
$H < G$	H é subgrupo de G
$H \triangleleft G$	H é subgrupo normal de G
I	Ideal
0_R	Identidade da soma do anel
e	Identidade do grupo
I_{RG}	Identidade do RG
$Im(\phi)$	Imagem da função ϕ
$-a$	Inverso aditivo de a
$\cong$	Isomorfo a
ξ_k	$k-$ésima raiz $n-$ésima da unidade
Id	Matriz identidade
$Ker(\phi)$	Núcleo de da função ϕ
$\rho(g)$	Representação regular do elemento g
M	$R-$módulo
$S \leq R$	S é subanel de R
$tr(A)$	Traço de A
$\otimes_R$	Tensor sobre R
1_R	Unidade de R

Sumário

Introdução

A primeira menção do conceito anel de grupo ocorreu de maneira implícita no artigo do A. Cayley (1821 - 1895) que também cita a teoria abstrata de grupos. De maneira explícita o termo anel de grupo foi mencionado por T. Molien (1861-1941) em 1897, ganhando grande destaque nas aplicações associadas à teoria de representações de grupos (MILIES; SEHGAL, 2002). Entre os conceitos, resultados e problemas da teoria de anéis de grupos podemos destacar o Problema do Isomorfismo de Anéis de Grupos que teve sua primeira aparição em 1947 como um problema na conferência de álgebra em Michigan por T.M. Thrall (1914-2006), que o formulou da seguinte maneira:

"Dado um grupo G e um corpo K, determine todos os grupos H de forma que KG é isomorfo à KH".

Alguns anos depois, em 1950 S. Perlis (1913-2009) e G. Walker (1912-2001) provaram que grupos abelianos finitos são determinados por seus anéis de grupo sobre o campo dos números racionais (MILIES; SEHGAL, 2002).

A presente monografia busca analisar um caso particular do *Problema do Isomorfismo em Anéis de Grupo* em que consideraremos o isomorfismo sobre o conjunto dos inteiros e para grupos abelianos finitos. Dessa maneira, podemos enunciar o questionamento central do trabalho como:

Sejam G um grupo finito abeliano e H um grupo, se $\mathbb{Z}G$ é isomorfo à $\mathbb{Z}H$ podemos afirmar que G é isomorfo à H?

Buscando embasamento teórico para responder a pergunta realizada anteriormente o trabalho foi dividido em três capítulos: o primeiro capítulo trata-se dos fundamentos teóricos referente à teoria de anéis, abordando a definição do conceito, exemplos, definição de corpo, ideal. Também dissertaremos sobre a teoria de grupos como a definição da estrutura, grupo abeliano, subgrupo, grupo cíclico, exemplos, classes laterais, homomorfismo de grupos, grupo de permutação raízes da unidade, grupos clássicos matriciais, representação de grupos. No segundo capítulo, estudaremos a teoria dos módulos, algumas propriedades, além de produto tensorial. No terceiro capítulo, abordamos um breve histórico, a definição de anel de grupo, a aplicação de aumento, isomorfismo normalizado. Após o estudo dos temas tratados nos capítulos anteriores, finalizamos com alguns resultados envolvendo isomorfismo normalizado e elementos de ordem finita de $\mathbb{Z}G$ para auxiliar na demonstração do teorema central da monografia. Por fim, temos o anexo com algumas definições e

resultados sobre matrizes, determinante e traço para a consulta dos leitores, se necessário, atuando como o apoio didático.

Dentre as referências consultadas ao longo do nosso trabalho, destacamos o livro intitulado *An introduction to group rings* dos autores César Polcino Milies e Sudarshan Sehgal.

1 Fundamentos Teóricos

Dentro das diversas áreas da Matemática, a Álgebra é um ramo que vem sendo estudado pelos estudiosos ao longo dos séculos, sejam conceitos atualmente tratados no Ensino Básico à Pós Graduação. Neste capítulo, estudaremos algumas estruturas importantes da Álgebra: anel e grupo.

1.1 Anel

Segundo Hefez (HEFEZ, 1993), Gauss iniciou o estudo dos anéis dos inteiros algébricos e tal estudo teve continuidade por Kummer, Dedekind, Kronecker, Dirichlet e Hibelrt ao longo do século 19 e 20. Assim, a noção abstrata de anel foi introduzida, um dos principais assuntos abrangidos pela álgebra abstrata. Logo, nesta seção estudaremos em destaque: anel, corpo, subanel e ideal, uma vez que são tópicos necessários para a continuidade dos estudos para alcançar nosso objetivo central.

Definição 1 (Anel)**.** *Sejam R um conjunto não vazio munido de duas operações binárias sobre R denominadas soma $(+)$ e multiplicação $(\cdot)$ respectivamente:*

$$\begin{array}{ccccc} + : R \times R & \to & R & & \cdot : R \times R & \to & R \\ (a,b) & \longmapsto & a+b & e & (a,b) & \longmapsto & a \cdot b. \end{array}$$

A terna $(R, +, \cdot)$ é dita ser um anel se para todo $a, b, c \in R$ as operações $+$ e $\cdot$ satisfazem:

i. $(a+b)+c = a+(b+c)$;

ii. existe um elemento $\alpha \in R$ tal que

$$a + \alpha = \alpha + a = a,$$

chamaremos α de identidade da soma de R.

iii. para cada $a \in R$ existe $\beta \in R$ tal que

$$a + \beta = \beta + a = \alpha,$$

dizemos que β é simétrico de a;

iv. $a + b = b + a$;

v. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

vi. $a \cdot (b + c) = a \cdot b + a \cdot c$;

vii. $(b + c) \cdot a = b \cdot a + c \cdot a$.

Proposição 1. *Seja* $(R, +, \cdot)$ *um anel, então:*

i. a identidade da soma do anel R *é única;*

ii. o simétrico de cada elemento de R *é único.*

Demonstração.

i. Suponhamos que α e β sejam duas identidades da soma do anel R, por definição, temos que para todo $a \in R$:

$$\alpha + a = a + \alpha = a \ \ e \ \ \beta + a = a + \beta = a.$$

Assim, como $\alpha \in R$ e β é a identidade de R notemos que

$$\alpha + \beta = \alpha. \tag{1.1}$$

Da mesma forma, considerando $\beta \in R$ e α a identidade da soma de R temos que

$$\alpha + \beta = \beta. \tag{1.2}$$

Logo, pelas equações 1.1 e 1.2, concluímos que

$$\alpha = \beta,$$

portanto, a identidade da soma de $(R, +, \cdot)$ é única.

ii. Considerando e a identidade da soma do anel e $a \in R$, suponhamos que α, β sejam dois inversos de a, logo, por definição,

$$\alpha + a = a + \alpha = e \tag{1.3}$$

e

$$\beta + a = a + \beta = e. \tag{1.4}$$

Assim, igualando as equações 1.3 e 1.4, e posteriormente. multiplicando por β temos que

$$a+\alpha = a+\beta \Rightarrow \beta+(a+\alpha) = \beta+(a+\beta) \Rightarrow (\beta+a)+\alpha = \beta+(a+\beta) \Rightarrow e+\alpha = \beta+e \Rightarrow \alpha = \beta.$$

Portanto, o simétrico de a é único.

□

Assim, denotaremos a identidade da soma por 0_R, além disso, pode ser nomeada como elemento neutro. O simétrico de um elemento a também denominado de inverso aditivo será denotado por $-a$. Por fim, se $a, b \in R$, então $a + (-b)$ denotaremos como $a - b$ sempre que necessário, assim como na operação multiplicação que podemos denotar $a \cdot b$ como ab.

Definição 2 (anel comutativo)**.** *Dizemos que $(R, +, \cdot)$ é um anel comutativo se possui a comutatividade em relação à multiplicação, ou seja, para todo $a, b \in R$ temos que $ab = ba$.*

Definição 3 (Anel com unidade)**.** *Denominamos $(R, +, \cdot)$ como anel de unidade se existe um elemento $\alpha \in R$, tal que para todo $a \in R$ temos que $\alpha a = a\alpha = a$. Chamamos α de unidade do anel ou de identidade da multiplicação do anel.*

Ao longo do texto, podemos referir $(R, +, \cdot)$ como R caso as operações estejam subentendidas.

Proposição 2. *A unidade do anel R, se existir, é única.*

Demonstração. Seja R um anel com unidade. Suponhamos que α e β sejam unidades do anel R, ou seja, para todo $a \in R$ temos

$$a\alpha = \alpha a = a \text{ e } a\beta = \beta a = a,$$

em particular,

$$\alpha\beta = \alpha \quad \text{e} \quad \alpha\beta = \beta.$$

Assim, $\alpha = \beta$, logo a unidade do anel é única. □

Denotaremos a unidade do anel R como 1_R.

Exemplo 1.

i. O conjunto dos números inteiros, munido das operações usuais de soma e multiplicação, $(\mathbb{Z}, +, \cdot)$, é um anel comutativo com unidade.

ii. O conjunto das classes residuais módulo n, representado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ associado com as operações $\overline{x} + \overline{y} = \overline{x + y}$ e $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ é um anel comutativo com unidade.

iii. Seja $m \in \mathbb{Z}$ temos que $(m\mathbb{Z}, +, \cdot)$ é um anel comutativo sem unidade se $m \notin \{-1, 0, 1\}$.

iv. O conjunto das matrizes quadradas 2×2 com entradas reais com as operações usuais, $(\mathbb{M}_{2\times 2}(\mathbb{R}), +, \cdot)$, é um anel com unidade, mas não é comutativo.

v. *Seja X um conjunto não vazio. Então $A = \{f : X \to \mathbb{R} \mid f \text{ é contínua}\}$ com as operações usuais ponto a ponto*

$$(f+g)(x) = f(x) + g(x) \text{ e } (f \cdot g)(x) = f(x) \cdot g(x).$$

Temos que A é uma anel comutativo com unidade denominado anel de funções.

vi. *Seja $\mathbb{Z}\left[\sqrt{-1}\right] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$. Considerando as operações*

$$\left(a_1 + b_1\sqrt{-1}\right) + \left(a_2 + b_2\sqrt{-1}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-1}$$

e

$$\left(a_1 + b_1\sqrt{-1}\right) \cdot \left(a_2 + b_2\sqrt{-1}\right) = (a_1a_2 - b_1b_2) + (a_1b_1 + a_2b_1)\sqrt{-1}$$

temos que $\mathbb{Z}\left[\sqrt{-1}\right]$ é um anel comutativo com unidade denominado anel dos inteiros Gaussianos.

Sejam R um anel com unidade e $a \in R$ não nulo. Se existe $\beta \in R$ tal que $a\beta = \beta a = 1_R$, então dizemos que a é *invertível* em R e β é um inverso multiplicativo de a e vice-versa. Não é necessário que cada elemento do anel tenha um inverso multiplicativo, mas caso o tenha ele será único. De fato, suponhamos que α e β são inversos multiplicativos de $a \in R$ tais que

$$\alpha = \alpha \cdot 1_R = \alpha(a\beta) = (\alpha a)\beta = 1_R \cdot \beta = \beta.$$

Deste modo denotamos $\beta = a^{-1}$. Assim, podemos definir R^*, o conjunto dos elementos invertíveis de R, o qual é não vazio já que $1_R \in R^*$. Além disso, associando o conjunto R^* com a operação multiplicação obtemos que esta é bem definida. De fato, considerando $a, b \in R^*$, então

$$(ab)\left(b^{-1}a^{-1}\right) = 1_R \text{ e } \left(b^{-1}a^{-1}\right)(ab) = 1_R,$$

o que equivale a dizer que $a \cdot b$ é invertível e $(ab)^{-1} = b^{-1}a^{-1}$.

É possível observar que no anel das matrizes 2×2 com entradas reais, temos que as matrizes não nulas $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$ são tais que $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Em contrapartida, no anel $\mathbb{Z}$ com suas operações usuais, se $a, b \in \mathbb{Z} \setminus \{0\}$, então $ab \neq 0$. Por fim se tomarmos $\mathbb{Z}_6$ notemos que $\overline{2} \cdot \overline{3} = \overline{0}$. Assim podemos definir um novo conceito.

Definição 4. *Sejam R um anel e $a \in R$ com $a \neq 0_R$. Dizemos que a é um divisor de zero se existir um $b \in R$, $b \neq 0_R$, em que $ab = 0_R$. Se $x, y \in R$, então $xy = 0_R$ se, somente se, $x = 0_R$ ou $y = 0_R$, dizemos que R é um anel sem divisores de zero.*

Definição 5. *Um anel será dito domínio de integridade ou simplesmente domínio se for um anel comutativo com unidade sem divisores de zero .*

Podemos também definir $Ddz(R)$ como o conjunto que contém todos do divisores de zero do anel R. Em contrapartida, quando temos $a \in R$ com a não nulo, em que $ab = 0_R$ somente para b nulo, dizemos que a é *regular*, assim definimos $Reg(R)$ como o conjunto dos regulares de R.

Exemplo 2.

i. O conjunto dos números inteiros, assim como os conjuntos dos números racionais e reais associados com as operações usuais são domínios de integridade;

ii. O conjunto dos múltiplos de $m \in \mathbb{Z}$ com as operações usuais $(m\mathbb{Z}, +, \cdot)$ é um anel sem divisor de zero, e para $m \in \{-1, 0, 1\}$, é um domínio de integridade;

iii. O conjunto das matrizes de dimensão n por n com as operações usuais, $(\mathbb{M}_{n\times n}(\mathbb{R}), +, \cdot)$, possui divisores de zero para $n > 1$. De fato, se tomarmos $(a_{ij})_{n\times n}$ e $(b_{ij})_{n\times n}$, em que $a_{11} = b_{21} \neq 0$ e 0 para as demais entradas. Temos desse modo que $(a_{ij})_{n\times n} \cdot (b_{ij})_{n\times n}$ é a matriz nula. Para exemplificar, temos que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

iv. O anel $\mathbb{Z}_m$ é um domínio de integridade se m for primo.

Definição 6. *Um anel R é dito anel de divisão se possui unidade e todo $a \in R$, com $a \neq 0_R$, é invertível.*

Proposição 3. *Se R um anel de divisão, então R não possui divisor de zero.*

Demonstração. Suponhamos, por absurdo, que $a \in R$ seja um divisor de zero, assim existe $b \in R$, com a e b não nulos, tais que $ab = 0_R$. Por outro lado, temos também que existe $c \in R$ em que $ac = ca = 1_R$. Notemos que

$$(ca)\, b = 1_R \cdot b = b.$$

Além disso,

$$c\,(ab) = c \cdot 0_R = 0_R,$$

assim temos que $(ca)\, b \neq c\,(ab)$, contradizendo o fato de R ser anel. Portanto, se R é um anel de divisão, então não há divisor de zero. □

Definição 7. *Dizemos que um anel R é um corpo se for um anel de divisão comutativo.*

Observação 1. *Notemos que pela Proposição 3 que afirma que um anel de divisão não possui divisores de zero, concluímos que um corpo é um domínio de integridade com todo elemento não nulo invertível.*

Sejam R um anel, $a \in R$, e $n \in \mathbb{Z}$, podemos definir

$$na = \begin{cases} a + a + \cdots + a, & \text{se } n > 0. \\ 0_R, & \text{se } n = 0. \\ -(a + a + \cdots + a), & \text{se } n < 0. \end{cases}$$

A partir da definição acima, se $a, b \in R$ e $m, n \in \mathbb{Z}$, notemos que

$$\begin{aligned} n(ab) = ab + ab + \cdots + ab &= a(b + b + \cdots + b) = a(nb). \\ &= (a + a + \cdots + a)\, b = (na)\, b. \end{aligned}$$

Além disso, como $nb \in R$, pela propriedade anterior

$$(ma)(nb) = m(a(nb)) = m(n(ab)) = (mn)(ab),$$

portanto $(ma)(nb) = (mn)(ab)$.

Definição 8 (Subanel)**.** *Seja S um subconjunto não vazio de um anel $(R, +, \cdot)$. Dizemos que S é um subanel de R, denotado por $S \leq R$, se $(S, +, \cdot)$ for um anel.*

Proposição 4. *Seja R um anel e S um subconjunto não vazio. Então S é um subanel de R se, somente se, para todo $a, b \in S$ temos que*

i. $a - b \in S$;

ii. $ab \in S$.

Demonstração. Se S for um subanel, logo S é um anel, e disso decorre imediatamente que $a - b \in S$ e $ab \in S$, para todos a, $b \in S$.

Reciprocamente, seja S um subconjunto de R no qual para todo $a, b \in S$ temos que $a - b \in S$ e $ab \in S$.

Notemos que $0_R = b - b \in S$. Além disso, considerando $0_R, a \in S$ temos que $0_R - a = -a \in S$. Portanto, para todo $a \in S$, temos que o inverso aditivo de a está em S.

Por fim, como $a, -b \in S$, obtemos que $a - (-b) \in S$ implicando que $a + b \in S$. Assim a adição é fechada sobre S. Como as propriedades *i.*, *iv.*, *v.*, *vi.* da Definição 1 são herdadas de R e pelo item *ii.* da hipótese que nos fornece que a multiplicação é fechada sobre S, concluímos que S é um anel com as operações de R, e portanto $S \leq R$. □

Dizemos que $\{0_R\}$ e R são os *subaneis triviais* de R. Além disso, se R não possui divisores de zero, então S também não possuirá.

Seja S um subanel com unidade de R. Se R for um domínio de integridade, dizemos também que S é um *subdomínio* de R, e se S e R forem corpos, diremos que S é um *subcorpo* de R.

Exemplo 3. *O anel do inteiros $\mathbb{Z}$ é um subdomínio de $\mathbb{Q}$, por sua vez, $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$ e $\mathbb{R}$ é um subcorpo de $\mathbb{C}$. Por sua vez, $2\mathbb{Z}$ não é subdomínio de $\mathbb{Z}$, já que não possui unidade.*

Definição 9 (Ideal)**.** *Sejam R um anel e I um subanel de R não vazio. Dizemos que I é um ideal à esquerda de R se*

$$\begin{array}{rcl} R \times I & \to & I \\ (a, x) & \longmapsto & ax \end{array}$$

é bem definida, isto é, $ax \in I$ para todo $a \in R$.

Além disso, chamamos I de ideal à direita de R se

$$\begin{array}{rcl} I \times R & \to & I \\ (x, a) & \longmapsto & xa \end{array}$$

é bem definida, isto é, $xa \in I$ para todo $a \in R$.

Se, por ventura, I for ideal à esquerda e à direita, ou seja, $x - y \in I$ e $ax, xa \in I$ com $x, y \in I$ e $a \in R$, denominamos I de ideal bilateral de R ou simplesmente que I é ideal de R.

Chamamos $\{0_R\}$ e R de *ideias triviais de R*.

Observação 2. *Caso R seja abeliano, temos que se I é um ideal à esquerda de A, então I também será um ideal à direita de R, ou seja, I é um ideal.*

Exemplo 4.

i. Seja $\mathbb{Z}$ um subanel de $\mathbb{Q}$, notemos que $\mathbb{Z}$ não é um ideal, uma vez que $\dfrac{1}{2} \notin \mathbb{Z}$.

ii. Consideraremos o anel $\mathbb{M}_{2\times 2}(\mathbb{R})$. Seja I o conjunto das matrizes 2×2 com $a_{12} = a_{22} = 0$. Podemos afirmar que é ideal à esquerda de $\mathbb{M}_{2\times 2}(\mathbb{R})$, mas não ideal à direita.

De fato, primeiramente $I \leq \mathbb{M}_{2\times 2}(\mathbb{R})$, pois

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix} = \begin{pmatrix} a - a_1 & 0 \\ b - b_1 & 0 \end{pmatrix} \in I \text{ e } \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ ba_1 & 0 \end{pmatrix} \in I.$$

Se $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, *então*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a + a_{12}b & 0 \\ a_{21}a + a_{22}b & 0 \end{pmatrix} \in I,$$

mas

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} aa_{11} & aa_{12} \\ ba_{11} & ba_{12} \end{pmatrix}$$

que não necessariamente pertence à I.

Por outro lado, temos que J, *o conjunto das matrizes* 2×2 *com* $a_{21} = a_{22} = 0$, *é ideal à direita de* $\mathbb{M}_{2\times 2}(\mathbb{R})$, *porém não é ideal à esquerda, uma vez que* $J \leq \mathbb{M}_{2\times 2}(\mathbb{R})$, *pois*

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a - a_1 & b - b_1 \\ 0 & 0 \end{pmatrix} \in J$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa_1 & ab_1 \\ 0 & 0 \end{pmatrix} \in J.$$

E, por fim,

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} aa_{11} + ba_{21} & aa_{12} + ba_{22} \\ 0 & 0 \end{pmatrix} \in J \text{ e}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a & a_{11}b \\ a_{21}a & a_{21}b \end{pmatrix},$$

que não pertence necessariamente à J.

Ao longo do texto, iremos utilizar a terminologia ideal para nos referir ao ideal bilateral.

Definição 10. *Dizemos que* R *é um anel simples se os únicos ideais de* R *são os triviais.*

Exemplo 5. *Sejam* R *um anel com unidade e* I *ideal de* R. *Suponhamos que* $1_R \in I$ *e seja* $a \in R$, *assim temos que* $ax \in I$ *para todo* $x \in I$, *em particular, para* $x = 1_R \in I$, *ou seja,* $a = a \cdot 1_R \in I$. *Logo podemos concluir que* $R \subseteq I$, *e portanto,* $I = R$. *Mais ainda, seja* I *um ideal de* R *em que* R *possui unidade. Se* I *possui um elemento invertível de* R, *então* $R = I$. *De fato, se* $x \in I$ *é invertível, então para* $a \in R$, *em particular,* $ax^{-1} \in R$, *logo* $a = \left(ax^{-1}\right) x \in I$. *Portanto* $R = I$.

Exemplo 6. *Seja* R *um anel comutativo e* $x \in R$, *então* $xR = \{xa \mid a \in R\}$ *é um ideal de* R, *chamado ideal principal que pode ser denotado por* $\langle x \rangle$.

1.2 Teoria de Grupos

Nesta seção, trataremos das definições e resultados da Teoria dos grupos. Tal teoria teve início com o matemático francês Évariste Galois (1811-1832) em 1830, que pela primeira vez usou o termo grupo restrito para permutações na sua definição moderna e introduziu outros termos, e posteriormente, outros estudiosos como Augustin-Louis Cauchy $(1789-1857)$, Arthur Cayley $(1821-1895)$, que foi o primeiro a definir o conceito de grupo abstrato em 1845, entre outros, construíram essa nova teoria que viria a revolucionar a matemática (MILIES; SEHGAL, 2002).

Definição 11 (Grupo)**.** *Seja G um conjunto não vazio munido com uma operação binária denotada por $\cdot$. Dizemos que G, associado à operação binária $\cdot$, é um grupo se satisfaz as seguintes propriedades:*

i. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *para todo* $a, b, c \in G$*;*

ii. existe um elemento $\alpha \in G$ *tal que para todo* $a \in G$ *temos*

$$a \cdot \alpha = \alpha \cdot a = a.$$

Chamaremos α *de identidade de G;*

iii. para cada $a \in G$ *existe um elemento* $\beta \in G$ *tal que*

$$a \cdot \beta = \beta \cdot a = \alpha.$$

Ao longo dos nossos estudos, nomeamos β como *inverso de a*, e além disso, usaremos a notação $(G, \cdot)$ para denotar o conjunto G associado à operação binária $\cdot$, por fim, também nos referiremos à operação binária apenas como operação.

Definição 12. *Considerando $(G, \cdot)$ um grupo, se para todo $a, b \in G$ tivermos que*

$$a \cdot b = b \cdot a,$$

então nomeamos $(G, \cdot)$ como grupo abeliano.

Exemplo 7. *Seja $\mathbb{Z}$ o conjunto dos números inteiros associado à soma usual $+$, podemos afirmar que $(\mathbb{Z}, +)$ é um grupo abeliano, assim como o conjunto das matrizes 2×2 com entradas reais associado à soma usual de matrizes, denotado por $(\mathbb{M}_{2\times 2}(\mathbb{R}), +)$, também o é. Assim como o conjunto de todas as classes residuais módulo n, $\mathbb{Z}_n = \{\overline{1}, \overline{2}, \cdots, \overline{n}\}$ associado com a operação $\overline{x} + \overline{y} = \overline{x+y}$ é um grupo abeliano.*

Proposição 5. *Seja $(G, \cdot)$ um grupo, então:*

i. a identidade do grupo é única;

ii. o inverso de cada elemento de G é único.

Demonstração. As demonstrações são similares às realizadas na Proposição 1. □

Neste trabalho, a identidade do grupo $(G, \cdot)$ será denotada como e.[1] Além disso, o inverso de a terá como notação a^{-1}, mas no caso particular em que estejamos em um grupo com a operação aditiva a notação será $-a$. Eventualmente, o conjunto G é dito um grupo ao longo do texto referindo-se ao grupo $(G, \cdot)$ sempre que não houver risco de confusão.

Observação 3. *Seja $a, b, c \in G$, G um grupo. Temos as seguintes igualdades:*

i. $\left(a^{-1}\right)^{-1} = a$;

ii. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$;

iii. $a \cdot b = a \cdot c \Rightarrow b = c \quad e \quad b \cdot a = c \cdot a \Rightarrow b = c$.

Definição 13 (Subgrupo)**.** *Sejam $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se $(H, \cdot)$ for um grupo e denotaremos $H < G$. Além disso, os conjuntos $\{0\}$ e G são ditos subgrupos triviais de G.*

Teorema 1. *Seja H um subconjunto não vazio de G. Então $H < G$ se, somente se, dados $a, b \in H$ implica que $a \cdot b^{-1} \in H$.*

Demonstração. Primeiramente, se $H < G$, temos que H é um grupo, então, para cada $b \in H$, existe $b^{-1} \in H$, e consequentemente, $a \cdot b^{-1} \in H$. Reciprocamente, se $a \cdot b^{-1} \in H$, para todo $a, b \in H$, consideremos $h_1 \in H$:

$$e_G = h_1 \cdot h_1^{-1} \in H.$$

Agora, considerando $h_2 \in H$ notemos que:

$$e_G, h_2 \in H \Rightarrow h_2^{-1} = e_G \cdot h_2^{-1} \in H. \tag{1.5}$$

Logo, $h_1, h_2^{-1} \in H$ implica que $h_1 \cdot h_2 \in H$, logo a operação é fechada sobre H, além disso, como $H \subset G$, dados $h_1, h_2, h_3 \in H$, então $h_1, h_2, h_3 \in G$. Portanto, $(h_1 \cdot h_2) \cdot h_3 = h_1 \cdot (h_2 \cdot h_3)$ em G, acarretando que $\cdot$ também é associativa em H. Assim, $(H, \cdot)$ é um grupo. □

[1] Caso seja necessário iremos utilizar um subíndice para expressar a qual grupo a identidade se refere, por exemplo, e_G como sendo a identidade do grupo G.

Antes de definirmos o que é um subgrupo gerado iremos determinar a notação a^n. Sejam G um grupo, $a \in G$ e $n \in \mathbb{Z}$, definimos

$$a^n = \begin{cases} e, & se\, n = 0. \\ a^{n-1} \cdot a, & se\, n > 0. \\ \left(a^{-1}\right)^{-n}, & se\, n < 0. \end{cases}$$

Observação 4. *Sejam $(G, \cdot)$ um grupo, $a, b \in G$ e $n, m \in \mathbb{N}$.*[2] *Podemos afirmar que:*

i. $a^m \cdot a^n = a^{m+n}$;

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

iii. $(a \cdot b)^n = a^n \cdot b^n$ *quando* $a \cdot b = b \cdot a$;

iv. $\left(a^{-1}\right)^n = (a^n)^{-1}$.

Definição 14. *Seja S um subconjunto não vazio de um grupo G. Definimos o subconjunto gerado por S como:*

$$\langle S \rangle = \{a_1 \cdot a_2 \cdot \ldots \cdot a_{m-1} \cdot a_m \mid a_i \in S, m \in \mathbb{N}\}.$$

Se G é um grupo abeliano, a definição acima pode ser reescrita como:

$$\langle S \rangle = \{a_1^{n_1} \cdot a_2^{n_2} \cdot \cdots \cdot a_m^{n_m} \mid m, n_i \in \mathbb{Z},\ a_i \in S \text{ para } a_i's \text{ distintos dois a dois }\}.$$

Por convenção, temos que o conjunto vazio gera o subgrupo trivial $\{e\}$.

Definição 15. *Sejam G um grupo e S um subconjunto de G, dizemos que G é um grupo gerado por S se $G = \langle S \rangle$.*

Se o conjunto S for finito temos que G é finitamente gerado. Ainda nesse sentido, se $a \in G$, o subgrupo gerado por $S = \{a\}$ é chamado por subgrupo cíclico de G gerado por a, e nesse caso, escrevemos

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

Um grupo G é dito ser cíclico se existe $a \in G$ tal que $G = \langle a \rangle$.

Proposição 6. *O conjunto $\langle a \rangle$ é subgrupo de G.*

Demonstração. Suponhamos que $a, b \in \langle a \rangle$, em que $a = a^n$ e $b = a^m$, com $m \leq n$. Assim

[2] Em nossos estudos não consideramos o número zero um elemento do conjunto dos números naturais.

$$ab^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle.$$

Segue do Teorema 1 que $\langle a \rangle$ é um subgrupo de G. □

Proposição 7. *Todo grupo cíclico é abeliano.*

Demonstração. Seja $(G, \cdot)$ um grupo cíclico, logo $G = \langle a \rangle$, para algum $a \in G$. Se $x, y \in G$ então $x = a^n$ e $y = a^m$ para $n, m \in \mathbb{Z}$, assim:

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

□

Exemplo 8. *Sejam $C_n = \{u^0 = e, u^1, \cdots, u^{n-1}\}$ e $\cdot$ uma operação definida sobre C_n tal que $u^i \cdot u^j = u^{[i+j]}$ em que $[i+j]$ representa o resto da divisão de $i+j$ por n.*

Assim, se $u^i, u^j, u^k \in C_n$ e $u^i \cdot u^j := u^i u^j$, observemos que a operação é associativa:

$$\left(u^i u^j\right) u^k = u^{[[i+j]+k]} = u^{[i+[j+k]]} = u^i \left(u^j u^k\right).$$

Além disso, tomando u^i um elemento qualquer do conjunto C_n obtemos que

$$u^0 u^i = u^{[0+i]} = u^{[i]} = u^i,$$

em que a última passagem ocorre pois $0 \leq i \leq n-1$. Assim u^0 é a identidade da operação.

Por outro lado, se $i \neq 0$ temos que

$$u^i u^{n-i} = u^{[n]} = u^0.$$

Ainda assim u^{n-i} pertence ao conjunto C_n, uma vez que $0 \leq n-i < n$. Com isso, temos que $(C, \cdot)$ é um grupo. Por fim, notemos que

$$u^i = u^{[1+\cdots+1]} = u^1 \cdots u^1 = \left(u^1\right)^i,$$

logo u gera o conjunto C_n. Portanto, $(C_n, \cdot)$ é um grupo cíclico.

Ademais, temos que quaisquer dois grupos cíclicos de mesma ordem são isomorfos[3], assim utilizaremos a notação C_n para designar um grupo cíclico de ordem n de um modo geral, não levando em conta a natureza dos elementos e a operação associada ao significado destes, mas dispondo da teoria que engloba os grupos cíclicos.

Exemplo 9.

[3] Para mais informações sugerimos consultar o Teorema 1.3.1 na página 85 da bibliografia (YARTEY, 2017)

i. Notemos que o conjunto dos números pares, $2\mathbb{Z}$, é gerado pelo número 2 com a adição usual para os números inteiros. Generalizando, $m\mathbb{Z}$ é um grupo cíclico gerado por m com a operação adição usual com $m \in \mathbb{N}$;

ii. O conjunto das classes residuais módulo 6, $\mathbb{Z}_6$, associado à adição usual é um grupo aditivo gerado pelo $\overline{1}$ ou pelo $\overline{5}$. Ainda nesse sentido, é possível notar que $\mathbb{Z}_n$, munido com a adição usual, é um grupo cíclico gerado ao menos pelo elemento $\overline{1}$ e mais, $\overline{m}$ é gerador de $\mathbb{Z}_n$ se m e n são primos entre si.

Definição 16. *Sejam G um grupo e $I_n = \{1, \ldots, n\}$ um conjunto com $n \in \mathbb{N}$. Se existe uma bijeção entre G e I_n dizemos que G é um grupo finito de ordem n. Denotaremos a ordem de um grupo finito por $|G|$. Caso não exista algum n tal que G e I_n sejam bijetivos, dizemos que G é um grupo infinito.*

Definição 17 (Subgrupo Normal)**.** *Seja H um subgrupo de G. Dizemos que H é um subgrupo normal de G, com a seguinte notação $H \triangleleft G$, se para todo $a \in G$ temos:*

$$aHa^{-1} \subset H.$$

Definição 18. *Seja H um subgrupo de G, dizemos que a classe lateral à esquerda de H contendo a é o conjunto*

$$aH := \{ah \mid a \in G,\, h \in H\}.$$

A classe lateral à direita de H contendo a é o conjunto

$$Ha := \{ha \mid a \in G,\, h \in H\}.$$

Quando realizamos a operação em um grupo aditivo normalmente a notação usual para denotar as classes aH e Ha são as seguintes, respectivamente:

$$a + H := \{a + h \mid a \in G,\, h \in H\} \text{ e } H + a := \{h + a \mid a \in G,\, h \in H\}.$$

Observação 5. *Seja $H \triangleleft G$, notemos que se $aha^{-1} \in aHa^{-1}$, então*

$$aha^{-1} = h_1 \Leftrightarrow ah = h_1 a, \tag{1.6}$$

para algum $h_1 \in H$, logo $aH \subset Ha$. De maneira similar obtemos que $Ha \subset aH$, portanto $aH = Ha$.

Reciprocamente, se $aH = Ha$, pela equação 1.6 temos que $aHa^{-1} = H$. Assim H é um subgrupo normal de G se, somente, se $aH = Ha$.

Observamos que ao considerarmos G um grupo, temos que $\{e\} \triangleleft G$ e $G \triangleleft G$. De fato, seja $H = \{e\}$ e $a \in G$, notemos que se $x \in aHa^{-1}$

$$x = a \cdot e \cdot a^{-1} \Leftrightarrow x = a \cdot a^{-1} = e \in H,$$

Logo $aHa^{-1} = H$. Por fim,

$$aGa^{-1} = \{a \cdot b \cdot a^{-1} \mid b \in G\},$$

como G é um grupo com a operação $\cdot$, temos que a operação é fechada, assim $aGa^{-1} = G$. Denominamos $\{e\}$ e G de *subgrupo normais triviais de G*.

Definição 19 (Grupo Simples)**.** *Seja G um grupo, $G \neq \{e\}$. Quando os únicos subgrupos normais de G são os triviais, dizemos que G é um grupo simples.*

Teorema 2. *Sejam G um grupo, $a, b \in G$ e H um subgrupo de G. Então:*

i. $aH = bH$ *se, e somente se,* $b^{-1}a \in H$*;*

ii. $aH = bH$ *se, e somente se,* $a \in bH$*;*

iii. Se $aH \cap bH \neq \varnothing$*, então* $aH = bH$*;*

iv. A aplicação

$$\begin{array}{rccc} f_a : H & \to & aH \\ h & \longmapsto & ah \end{array}$$

é uma bijeção.

v. Seja G um grupo finito, então existem $g_i \in G$, para $i = 1, 2, \cdots, n$, com $g_1 = e$ tal que

$$G = g_1H \cup g_2H \cup \cdots \cup g_nH$$

é uma união disjunta.

Demonstração.

i. Primeiramente tomaremos como hipótese $aH = bH$, assim notemos que $a \in aH$, consequentemente $a \in bH$, ou seja, existe $h \in H$ tal que $a = bh$. Logo

$$b^{-1}a = h \in H.$$

Reciprocamente, considere $b^{-1}a \in H$. Desta forma, temos que existe $h_1 \in H$ tal que

$b^{-1}a = h_1$, logo

$$a = bh_1. \tag{1.7}$$

Tomando $ah \in aH$ e utilizando 1.7 temos que

$$ah = bh_1h.$$

Como H é subgrupo de G então $h_1h = h_2 \in H$, logo

$$ah = bh_2 \in bH.$$

Portanto, $aH \subseteq bH$. Para o caso de $bH \subseteq aH$, a demonstração é análoga e, deste modo, obtemos que $aH = bH$. Em particular, $aH = H$ se, somente se, $a \in H$.

ii. Suponhamos que $aH = bH$. Como $e \in H$ temos que $ae = a \in aH = bH$.

Reciprocamente, se $a \in bH$, obtemos que $a = bh_1$ com $h_1 \in H$. Seja $ah \in aH$, então

$$ah = bh_1h \in bH.$$

Assim $aH \subseteq bH$. Obtemos que $bH \subseteq aH$ de modo similar ao que realizamos anteriormente, concluindo que $aH = bH$.

iii. Por hipótese, existe $c \in aH \cap bH$ e daí, $c \in aH$ e $c \in bH$. Porém, pelo item *ii*. da mesma proposição temos que $cH = aH$ e $cH = bH$, logo $aH = bH$.

iv. Sejam $h_1, h_2 \in H$. Considerando $f_a(h_1) = f_a(h_2)$ temos que

$$f_a(h_1) = f_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2.$$

Portanto, f_a é injetiva.

Se $b \in aH$ então existe $h \in H$ tal que $b = ah$, logo $b = f_a(h)$. Assim podemos concluir que f_a é sobrejetiva, consequentemente, f_a é uma bijeção, implicando que $|aH| = |H|$.

v. Seja $G = \{g_1 = e, g_2, \cdots, g_m\}$ um grupo. Notemos que $g_1H \cup g_2H \cup \cdots \cup g_mH = G$, uma vez que $H < G$. Além disso, pelo item *iii*. podemos definir Λ como o conjunto dos índices $i \in I_m$ em que se $g_iH \neq g_jH$, para todo $j \in I_m$. Se $g_iH = g_jH$, então i pertence a I_m enquanto $j \notin I_m$, implicando que $G = \bigcup_{i \in \Lambda} g_iH$, com as classes duas a duas disjuntas.

□

Sejam G um grupo e $H \triangleleft G$. O *conjunto das classes laterais à esquerda* com respeito a H é denotado como

$$G/H = \{aH \mid a \in G\}.$$

Exemplo 10. *Sejam G um grupo e $H \triangleleft G$. Então G/H é um grupo com a seguinte operação:*

$$\begin{array}{rccl} * : & G/H \times G/H & \to & G/H \\ & (aH,\ bH) & \longmapsto & aH * bH := (ab)H. \end{array}$$

Chamamos esse grupo de grupo quociente de G módulo H.

Definição 20. *Dizemos que o centro de um grupo G é definido pelo conjunto*

$$Z(G) = \{\ a \in G \mid ab = ba \text{ para todo } b \in G\ \}.$$

Proposição 8. *Seja G um grupo. Então $Z(G) \triangleleft G$.*

Demonstração. Sejam $a, b \in Z(G)$, notemos que, para todo $g \in G$,

$$eg = ge \Rightarrow bb^{-1}g = gbb^{-1} \to b^{-1}bb^{-1}g = b^{-1}bgb^{-1} \Rightarrow b^{-1}g = gb^{-1},$$

logo $b^{-1} \in Z(G)$. Além disso,

$$\left(ab^{-1}\right)g = a\left(b^{-1}g\right) = a\left(gb^{-1}\right) = (ag)\,b^{-1} = (ga)\,b^{-1} = g\left(ab^{-1}\right),$$

portanto $ab^{-1} \in Z(G)$, assim $Z(G)$ é um subgrupo de G pelo Teorema 1.

Por definição, se $a \in Z(G)$, então temos que $ag = ga$ para todo $g \in G$, logo $Z(G)\,g = gZ(G)$, ou seja, $Z(G) \triangleleft G$. □

Definição 21 (Homomorfismo de Grupos)**.** *Sejam $(G, \cdot)$ e $(H, *)$ grupos. Uma aplicação*

$$\Phi : G \to H$$

é um homomorfismo se para todo $a, b \in G$

$$\Phi(a \cdot b) = \Phi(a) * \Phi(b).$$

Considerando $\Phi : G \to H$ um homomorfismo, temos que se Φ é injetiva a denominamos de *monomorfismo*. Por sua vez, se Φ for sobrejetiva a chamamos de *epimorfismo*. Ainda nesse sentido, se Φ for uma bijeção, dizemos que Φ é um *isomorfismo*, nesse caso dizemos que G é isomorfo a H e denotamos por $G \cong H$. Por fim, se $\Phi : G \to G$ é um isomorfismo chamamos Φ de *automorfismo*.

Seja $\Phi : G \to H$ um homomorfismo de grupos. O *núcleo de Φ* é o conjunto

$$Ker(\Phi) := \{a \in G \mid \Phi(a) = e_H\},$$

enquanto a *imagem de Φ* é o conjunto

$$Im(\Phi) := \{a \in H \mid \text{existe } b \in G \text{ em que } \Phi(b) = a\}.$$

Proposição 9. *Seja $\Phi : G \to H$ um homomorfismo com $(G, \cdot)$ e $(H, *)$ grupos, então*

i. $\Phi(e_G) = e_H$;

ii. $\Phi\left(b^{-1}\right) = \Phi(b)^{-1}$.

De fato, considerando $a \in G$ temos que:

$$\Phi(a) = \Phi(e_G \cdot a) = \Phi(e_G) * \Phi(a) \Rightarrow \Phi(e_G) = e_H.$$

Por sua vez, partindo que $\Phi(e_G) = e_H$ e que $b \cdot b^{-1} = e_G$ obtemos que $\Phi(e_G) = \Phi(b) * \Phi\left(b^{-1}\right) = e_H$, implicando que $\Phi\left(b^{-1}\right) = \Phi(b)^{-1}$.

Proposição 10. *Seja $\Phi : G \to H$ um homomorfismo, com $(G, \cdot)$ e $(H, *)$ grupos. Temos que $Ker(\Phi)$ é subgrupo de G enquanto $Im(\Phi)$ é subgrupo de H.*

Demonstração. Se $a, b \in Ker(\Phi)$, notemos que

$$\Phi\left(a \cdot b^{-1}\right) = \Phi(a) * \Phi(b)^{-1} = e_H,$$

e, portanto, pelo Teorema 1, $Ker(\Phi) < G$.

Por outro lado, se $a, a_1 \in Im(\Phi)$, existem $b, b_1 \in G$ tais que $\Phi(b) = a$ e $\Phi(b_1) = a_1$. Assim

$$a \cdot a_1^{-1} = \Phi(b) * \Phi(b_1)^{-1} = \Phi\left(b \cdot b^{-1}\right) \in Im(\Phi),$$

acarretando que $Im(\Phi)$ é subgrupo de H pelo Teorema 1. □

Teorema 3. *Seja $\Phi : G \to H$ um homomorfismo de grupos. Então Φ é monomorfismo se e somente se, $Ker(\Phi) = \{e_G\}$.*

Demonstração. Primeiramente, seja Φ um monomorfismo. Se a $\in Ker(\Phi)$ então $\Phi(a) = e_H$, porém $\Phi(e_G) = e_H$. Logo $a = e_G$, implicando que $Ker(\Phi) = \{e_G\}$. Reciprocamente, se $\Phi(a) = \Phi(b)$ então

$$\Phi\left(a \cdot b^{-1}\right) = \Phi(a) * \Phi\left(b^{-1}\right) = \Phi(b) * \Phi\left(b^{-1}\right) = \Phi\left(b \cdot b^{-1}\right) = \Phi(e_G).$$

Como $Ker(\Phi) = \{e_G\}$, então

$$a \cdot b^{-1} = e_G \Rightarrow a = b.$$

□

Proposição 11. *Se $\Phi : G \to H$ um homomorfismo de grupos, então $Ker(\Phi) \triangleleft G$.*

Demonstração. Sejam $a \in G$ e b um elemento de $aKer(\Phi)a^{-1}$, por definição, temos que existe $c \in Ker(\Phi)$ tal que

$$b = aca^{-1} \Rightarrow \Phi(b) = \Phi\left(aca^{-1}\right) = \Phi(a)\Phi(c)\Phi\left(a^{-1}\right) = \Phi(a)e_H\Phi\left(a^{-1}\right) = e_H.$$

Portanto, $b \in Ker(\Phi)$, implicando que $aKer(\Phi)a^{-1} \subseteq Ker(\Phi)$, concluindo que $Ker(\Phi) \triangleleft G$. □

Teorema 4 (Primeiro Teorema dos Isomorfismos)**.** *Se $\Phi : G \to H$ é um homomorfismo de grupos então*

$$\frac{G}{Ker(\Phi)} \cong Im(\Phi).$$

Demonstração. Para essa demonstração, definimos

$$\begin{array}{rccc} \theta : & \dfrac{G}{Ker(\Phi)} & \to & Im(\Phi) \\ & aKer(\Phi) & \longmapsto & \Phi(a). \end{array}$$

Inicialmente, provaremos que a aplicação θ é bem definida. De fato, sejam $a, b \in G$ tal que $aKer(\Phi) = bKer(\Phi)$, assim $a = bg$, com $g \in Ker(\Phi)$ pelo item *ii.* do Teorema 2, então

$$\theta(aKer(\Phi)) = \Phi(a) = \Phi(bg) = \Phi(b)e_H = \Phi(b) = \theta(bKer\Phi).$$

Além disso, sabendo que $Ker(\Phi) \triangleleft G$ temos que

$$\theta(aKer(\Phi)bKer(\Phi)) = \theta(abKer(\Phi)) = \Phi(ab) = \Phi(a)\Phi(b) = \theta(aKer\Phi)\theta(bKer\Phi),$$

donde verificamos que θ é um homomorfismo.

Ademais, se $\theta(aKer(\Phi)) = \theta(bKer(\Phi))$, então

$$\Phi(a) = \Phi(b) \Rightarrow \Phi(a)\Phi\left(b^{-1}\right) = e_H \Rightarrow \Phi\left(ab^{-1}\right) = e_H.$$

Assim, obtemos que $ab^{-1} \in Ker(\Phi)$, acarretando que $a \in bKer(\Phi)$, logo, pelo item *ii.* do Teorema 2, temos $aKer(\Phi) = bKer(\Phi)$. Desse modo, podemos afirmar que a aplicação θ é um monomorfismo.

Por fim, se $b \in Im(\Phi)$ então existe $a \in G$ tal que $\Phi(a) = b$, assim $\theta(aKer(\Phi)) = b$, logo θ é um epimorfismo. Portanto podemos concluir que

$$\frac{G}{Ker(\Phi)} \cong Im(\Phi).$$

□

Definiremos um importante exemplo de grupo a seguir.

Definição 22 (Permutação)**.** *Seja X um conjunto qualquer. Se a aplicação $\tau : X \to X$ é uma bijeção dizemos que τ é uma permutação de X.*

O conjunto de todas as permutações de X associado com a operação composição de funções, denotado por S_X, é um grupo denominado *grupo de permutação*. Além disso, considerando o conjunto $I_n = \{1, 2, \cdots, n\}$, podemos definir o grupo S_n como todas as funções bijetivas da forma $\tau : I_n \to I_n$.

Seja $\tau \in S_n$, usaremos $(a_1\, a_2\, \cdots\, a_n)$ para denotar τ em que $\tau(a_i) = a_{i+1}$, $\tau(a_n) = a_1$ e se $\tau(a_i) = a_i$, então $a_i \notin (a_1\, a_2\, \cdots\, a_n)$ em que $1 \leq i \leq n$, caso $\tau(a_i) = a_i$, para todo i, dizemos que a permutação é a identidade e é expressada por e ou Id.

Exemplo 11. *O grupo de permutação para $n = 3$ é $S_3 = \{Id, (1\,2)\,(1\,3)\,(2\,3)\,(1\,2\,3)\,(1\,3\,2)\}$.*

Exemplo 12. *Sejam $B = \{e_1, e_2, \cdots, e_m\}$ e $C = \{x_1, x_2, \cdots, x_m\}$ e a função bijetiva f*

$$\begin{array}{rccc} f: & B & \to & C \\ & e_i & \longmapsto & x_j. \end{array}$$

Note que f induz ma bijeção de I_m em I_m do seguinte modo

$$\begin{array}{rccc} g: & I_m & \to & I_m \\ & i & \longmapsto & g(i) \end{array}$$

em que $g(i)$ é definido como sendo o índice j dado na definição f, ou seja, se $f(e_i) = x_j$, então $g(i) = j$.

Podemos observar que se $g(i) = g(j)$, então $f(e_i) = f(e_j)$, como f é injetiva obtemos que $e_i = e_j$, acarretando que $i = j$. Por sua vez, se $k \in I_m$ temos que existe um e_i tal que $f(e_i) = x_k$, uma vez que f é sobrejetiva, logo $g(i) = k$. Portanto g é uma bijeção.

Por exemplo, se $B = \{e_1, e_2, e_3, e_4\}$ e $C = \{x_1, x_2, x_3, x_4\}$ e considerando

$$f(e_1) = x_3,\ f(e_2) = x_4,\ f(e_3) = x_2,\ f(e_4) = x_1,$$

temos que

$$g(1) = 3,\ g(2) = 4,\ g(3) = 2,\ g(4) = 1,$$

logo podemos associar a função g a permutação com $(1\,3\,2\,4)$.

Teorema 5. *Para $n \geq 1$ o grupo de permutação S_n possui $n!$ elementos.*

Demonstração. Seja S_n o grupo de permutação de I_n, notemos que para a imagem de 1 há n possibilidades, já para a imagem de 2 são $n-1$ possibilidades, uma vez que as aplicações desse conjunto são injetivas e uma das possibilidades iniciais será para a imagem de 1. Ainda nesse sentindo, temos $n-2$ possibilidades para a imagem de 3 assim recursivamente

até 2 possibilidades para a imagem de $n-1$ e restar apenas 1 possibilidade para a imagem de n. Assim, temos $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ bijeções. Portanto, S_n possui $n!$ elementos. □

Nosso enfoque a seguir é analisar conceitos e resultados relacionados com o grupo das raízes da unidade que nos dará um embasamento básico para alguns tópicos futuros dos nossos estudos.

Seja z um número complexo, podemos escrevê-lo, de forma algébrica, como $z = a+bi$ com $a, b \in \mathbb{R}$ e $i^2 = -1$. Utilizando trigonometria obtemos, a partir da forma algébrica, a forma polar de z:

$$z = |z| \left(cos\theta + isen\theta\right),$$

em que $|z|$ é dito o módulo de z, dado por $\sqrt{a^2+b^2}$ e θ está em radianos. Além disso, temos a seguinte propriedade a fim de facilitar algumas passagens posteriormente: sejam $z_1 = |z_1| \left(cos\ \theta_1 + isen\ \theta_1\right)$ e $z_2 = |z_2| \left(cos\ \theta_2 + isen\ \theta_2\right)$, temos que

$$z_1 \cdot z_2 = |z_1||z_2| \left(cos\left(\theta_1 + \theta_2\right) + isen\left(\theta_1 + \theta_2\right)\right). \tag{1.8}$$

Definição 23. *Sejam $n \in \mathbb{N}$ e $z \in \mathbb{C}$. O número complexo que satisfaz a equação $x^n = z$ é denominado de raiz n-ésima complexa de z.*

Note que como $1 = 1(cos0 + isen0)$, segundo (HEFEZ, 1993, pág. 187), temos que as raízes n-ésimas da unidade são da forma

$$\xi_k = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$$

com $k = 0, \cdots, n-1$.

Agora se $m \in \mathbb{Z}$ e considerando que $m = qn + r$ com $q \in \mathbb{Z}$ e $0 \leq r < n$ obtemos que

$$\xi_m = \xi_{qn+r} = \xi_r,$$

uma vez que

$$\begin{aligned}
\xi_{qn+r} &= cos\left(\frac{2\pi(qn+r)}{n}\right) + isen\left(\frac{2\pi(qn+r)}{n}\right) \\
&= cos(2\pi q)cos(\frac{2\pi r}{n}) - sen(2\pi q)sen\left(\frac{2\pi r}{n}\right) + \\
&+ i\left[sen(2\pi q)cos\left(\frac{2\pi r}{n}\right) + cos(2\pi q)sen\left(\frac{2\pi r}{n}\right)\right] \\
&= cos\left(\frac{2\pi r}{n}\right) + isen\left(\frac{2\pi r}{n}\right) = \xi_r.
\end{aligned}$$

Logo, para todo $m \in \mathbb{Z}$, temos que $\xi_j \in \{\xi_0, \xi_1, \xi_2, \cdots, \xi_{n-1}\}$, implicando que $m \equiv j \bmod n$ se, somente se, $\xi_m = \xi_j$.

Proposição 12. *Sejam ξ_α e ξ_β raízes n-ésimas complexas da unidade e $j \in \mathbb{N}$. Então:*

i. $\xi_\alpha \cdot \xi_\beta = \xi_{\alpha+\beta}$;

ii. $(\xi_\alpha)^j = \xi_{j\alpha}$;

iii. $(\xi_\alpha)^{-1} = \xi_{n-\alpha}$.

Demonstração. i. Notemos pela Equação 1.8

$$\xi_\alpha \cdot \xi_\beta = cos\left(\frac{2\pi}{n}(\alpha+\beta)\right) + isen\left(\frac{2k\pi}{n}(\alpha+\beta)\right) = \xi_{\alpha+\beta}.$$

ii. Segue imediatamente da Fórmula de De Moivre, segundo (HEFEZ, 1993) na página 183, anunciada da seguinte maneira: se $z = |z|(cos\,\theta + isen\,\theta)$ e $n \in \mathbb{N}$, então

$$z^n = |z|^n (cos\,(n\theta) + isen\,(n\theta)).$$

Uma vez que

$$(\xi_\alpha)^j = \left(cos\left(\frac{2\alpha\pi}{n}\right) + isen\left(\frac{2\alpha\pi}{n}\right)\right)^j = cos\left(\frac{2j\alpha\pi}{n}\right) + isen\left(\frac{2j\alpha\pi}{n}\right) = \xi_{j\alpha}.$$

iii. Notemos que, pelo item *i.*, $\xi_\alpha \cdot \xi_{n-\alpha} = \xi_n = 1$, logo $(\xi_\alpha)^{-1} = \xi_{n-\alpha}$.

□

Proposição 13. *O conjunto das raízes n-ésimas da unidade é um grupo cíclico com a operação de multiplicação de $\mathbb{C}$, gerado pela raiz n-ésima ξ_1 da unidade.*

Demonstração. Temos que $(\mathbb{C} \setminus \{0\}, \cdot)$ é um grupo, além disso, $R = \{\xi_0, \xi_1, \cdots, \xi_{n-1}\}$ está contido em $\mathbb{C} \setminus \{0\}$. Notemos que para $0 \leq x, y \leq n-1$ temos

$$\xi_x \cdot (\xi_y)^{-1} = \xi_x \cdot \xi_{n-y} = \xi_{x+n-y} \in R.$$

Assim, pelo Teorema 1, o conjunto das raízes n-ésimas da unidade é um subgrupo de $(\mathbb{C}^*, \cdot)$, consequentemente, é um grupo. Além disso, temos que $\xi = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ gera o conjunto das raízes n-ésimas da unidade, logo o conjunto das raízes n-ésimas da unidade é um grupo cíclico. □

Definição 24. *Dizemos que ξ_k é uma raiz n-ésima primitiva da unidade se ξ_k gera o conjunto das raízes n-ésimas da unidade, ou seja,*

$$\langle \xi_k \rangle = \{\xi_0, \xi_1, \cdots, \xi_{n-1}\}.$$

Sejam $\xi = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ e $k \in \{0, 1, ..., n-1\}$, notemos que $\xi^n = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$, assim o conjunto $\{\xi^0, \xi^1, \cdots, \xi^{n-1}\}$ é constituído pelas raízes n-ésimas complexa da unidade.

1.3 Grupos Clássicos Matriciais

Nesta seção apresentaremos alguns grupos matriciais, focando no embasamento teórico da Teoria de Grupos e relembrando de alguns conceitos e resultados referentes as propriedades de matrizes.

Sejam A e B matrizes invertíveis $n \times n$, então $AB = C$ em que $(C)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ para cada par i e j, $1 \leq i \leq n$ e $1 \leq j \leq n$.

Ainda nesse sentido, se A e B matrizes $n \times n$ invertíveis, temos que A^{-1} e B^{-1} também são invertíveis e

$$det\,(AB) = det\ A \cdot det\ B \neq 0 \text{ e } (AB)\left(B^{-1}A^{-1}\right) = I_n,$$

logo AB é invertível, e além disso, $(AB)^{-1} = B^{-1}A^{-1}$ com determinante não nulo, provando deste modo que a operação usual de multiplicação de matrizes é fechada no conjunto das matrizes invertíveis, além disso, se A é invertível, sua inversa também o é. Ademais a multiplicação usual de matrizes $n \times n$ invertíveis é associativa, e a matriz identidade é invertível e satisfaz $AI_n = I_nA = A$, para toda matriz invertível A. Portanto, o conjunto das matrizes $n \times n$ invertíveis munido com a multiplicação usual das matrizes é um grupo.

Definição 25. *O grupo linear geral sobre um corpo K, denotado por $GL(n, K)$, é o grupo de todas as matrizes $n \times n$ invertíveis, com entradas pertencentes ao corpo K, associado à operação multiplicativa usual das matrizes.*

Por outro lado, seja A e B matrizes com determinante igual a $1 = 1_K$, notemos que $det\,B \cdot det\,B^{-1} = 1$, implicando que $det\,B^{-1} = 1$. Assim,

$$det\,\left(AB^{-1}\right) = det\,A \cdot det\,B^{-1} = 1,$$

logo AB^{-1} também possui determinante igual a um, acarretando que o conjunto das matrizes com determinante igual à um é um subgrupo de $GL(n, K)$, pelo Teorema 1.

Definição 26. *Definimos o grupo linear especial sobre um corpo K como o grupo das matrizes invertíveis $n \times n$ com entradas em K, com determinante igual a um, que denotaremos como $SL(n, K)$.*

Ainda assim, o fato de que geralmente $AB \neq BA$ acarreta que $GL(n, K)$ e $SL(n, K)$ não são, em geral, abelianos. Antes de novos conceitos vamos relembrar como é enunciado a ortogonalidade em relação à matrizes.

Definição 27. *Dizemos que uma matriz A é ortogonal se $A^tA = AA^t = I_n$, ou seja, $A^{-1} = A^t$, em que A^t denota a matriz transposta.*

Nesse sentido, é possível notar também que devido a igualdade $det\, A = det\, A^t$, obtemos que

$$det\left(AA^t\right) = det\, A \cdot det\, A^t = 1 \Rightarrow (det\, A)^2 = 1 \Rightarrow det\, A = \pm 1.$$

Portanto, temos que as matrizes ortogonais são invertíveis e ainda assim observemos que se A e B são matrizes $n \times n$ ortogonais, então

$$AB^tBA^t = I_n,$$

implicando que

$$\left(AB^t\right)^{-1} = BA^t = \left(AB^t\right)^t.$$

Logo AB^t é uma matriz ortogonal, resultando que o conjunto das matrizes ortogonais, associado com a operação multiplicação, é um subgrupo de $GL(n, K)$, ou seja, o conjunto das matrizes ortogonais forma o *grupo ortogonal*, que denotaremos por $O(n, K)$.

Ainda nesse seguimento, se A, B são matrizes ortogonais com determinante igual a 1, então $det\left(AB^t\right) = det\, A \cdot det\, B^t = 1$ e como a multiplicação de matrizes ortogonais resulta em uma matriz ortogonal, podemos afirmar que o conjunto das matrizes ortogonais com determinante igual a 1 é o subgrupo de $O(n, K)$.

Definição 28. *Dizemos que o grupo ortogonal especial, $SO(n, K)$, é o grupo das matrizes ortogonais sobre K com determinante igual a 1_K.*

Agora consideraremos o conjunto $W(n, K)$ das matrizes $n \times n$ pertencentes ao conjunto $GL(n, K)$ com entradas no conjunto $\{0 = 0_K, 1\}$ e que em cada linha e em cada coluna de A tenha apenas uma entrada preenchida por 1. Assim, sendo $AB = C_{ij}$ temos

$$C_{ij} = \begin{cases} 1, & \text{se } a_{ik} = b_{kj} = 1, \\ 0, & \text{caso contrário.} \end{cases}$$

Notemos que, como em cada linha de A possui apenas uma entrada igual a 1, considerando a i-ésima linha, suponhamos que tal entrada não nula ocorra na k-ésima coluna, ou seja,

$a_{ik} = 1$ e $a_{il} = 0$ para todo $l \neq k$. Pelo mesmo raciocínio vemos que na k-ésima linha da matriz B temos $b_{kj} = 1$ e $a_{kl} = 0$, para algum $1 \leq j \leq n$, para todo $l \neq j$. Portanto $c_{ij} = 1$. Agora, supondo que na i-ésima linha de C possua pelo menos duas entradas iguais a 1, digamos c_{ij} e c_{ik}, com $j < k$, implicaria que $a_{il} = b_{lk} = 1$ e $a_{im} = b_{mk} = 1$, para $l \neq m$, $1 \leq l < m \leq n$. Logo na i- ésima linha de A há duas entradas preenchidas com 1, o que é uma afirmação falsa, pois $A \in W(n, K)$. Assim necessariamente cada linha da matriz C possui exatamente uma entrada igual a 1. Raciocínio análogo para obter que cada coluna da matriz C possui exatamente uma entrada igual a 1.

Portanto, temos que o produto de A com B resulta em uma matriz também pertence a $W(n, K)$ mesmo conjunto, ou seja, a operação multiplicação é fechada. Notemos também que se $L_1, L_2, \cdots, L_n$ são as linhas da matriz A com $L_i = [a_{ki}]$ e $L_j = [a_{kj}]$ para $i, j \in \{1, .., n\}$ e $k = 1, \ldots, n$, então

$$L_i \cdot L_j^t = \sum_{k=1}^{n} a_{kl} a_{lk} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{caso contrário.} \end{cases}$$

Observamos que como $c_{ij} = \left(L_i \cdot L_j^t\right)$, então $C_{ij} = AA^t = I_n$, acarretando que A é ortogonal, assim temos que $W(n, K)$ é subconjunto de $O(n, K)$. Além disso, se $A, B \in W(n, K)$, então

$$AB^{-1} = AB^t \in W(n, K),$$

pois $B^t \in W(n, K)$ e $W(n, K)$ munido com a multiplicação é um conjunto fechado. Portanto, $W(n, K)$ é um subgrupo de $O(n, K)$.

Definição 29. *Definimos o grupo de Weyl de $GL(n, K)$, que denotaremos por $W(n, K)$, como o grupo das matrizes $n \times n$ pertencentes ao conjunto $GL(n, K)$, associado à operação multiplicação usual das matrizes, cujas entradas pertencem ao conjunto $\{0, 1\}$ e em cada linha e em cada coluna de A a unidade ocorre exatamente uma única vez.*

Exemplo 13. *Notemos que o grupo de Weyl $W(2, K)$ contém apenas os elementos* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *e* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

1.4 Representação de Grupos

Nesta seção, realizaremos uma pequena abordagem da teoria de representação de grupos [4]. De maneira simplória, uma representação de um dado grupo G é um modo de

[4] A referência bibliográfica pode ser consulta em <http://mtm.ufsc.br/coloquiosul/notas_minicurso_9-corrigido.pdf> (acesso em 16/09/2021).

enxergá-lo por meio de uma estrutura bem conhecida, como as matrizes, e desta forma, podemos utilizar propriedades matriciais. Considerando a complexidade desta teoria, focaremos nossa atenção a representação de grupos finitos.

Definição 30. *Sejam G um grupo finito, V um espaço vetorial sobre um corpo K e $GL(V)$ o conjunto dos automorfismo de V. Uma representação de G em V é um homomorfismo*

$$\begin{array}{rccl} \rho: & G & \to & GL(V) \\ & s & \longmapsto & \rho_s: \quad V \to V \\ & & & \qquad\quad v \longmapsto \rho_s(v). \end{array}$$

Nesse caso, denominamos V como o espaço da representação do grupo G e a dimensão de V chamamos de grau da representação.

Exemplo 14. *Sejam V um espaço vetorial sobre um corpo e G um grupo finito. A representação unitária ρ é dada por $\rho(s) = ID_v$ para todo $s \in G$.*

Exemplo 15. *Sejam $G = \{g_1, g_2, \cdots, g_n\}$ um grupo finito de ordem n, V um espaço vetorial n-dimensional e $B = \{e_1, e_2, \cdots, e_n\}$ uma base de V tal que exista uma função bijetiva*

$$\begin{array}{rccl} f: & G & \to & B \subset V \\ & g_i & \longmapsto & e_i. \end{array}$$

Sabendo que para obter $\rho(g)$ basta determinar as imagens dos elementos da base, podemos definir a representação regular de $(G, \cdot)$ como:

$$\begin{array}{rccl} \rho: G & \to & GL(V) & \\ g_i & \longmapsto & \rho(g_i): & V \to V \\ & & & e_k \longmapsto e_{\sigma_{g_i}(k)}, \end{array}$$

para algum $\sigma_g \in S_n$, isto é, $\rho(g_i)(e_k) = f(g_i \cdot f^{-1}(e_k)) = f(g_i \cdot g_k)$. Assim conseguimos representar $\rho(g_i)$, para cada $i = 1, 2, \cdots, n$, por meio de uma matriz de transformação $[\rho(g_i)]_B$. Denotaremos $[\rho(g_i)]_B$ como $\rho(g_i)$ ao longo do nosso trabalho.

Notemos que se $\rho(g_i) = \rho(g_j)$ então, para todo e_k, com $k = 1, \cdots, n$, temos que

$$\rho(g_i)(e_k) = \rho(g_j)(e_k) \Rightarrow e_{\sigma_{g_i}(k)} = e_{\sigma_{g_j}(k)} \Rightarrow \sigma_{g_i}(k) = \sigma_{g_j}(k) \Rightarrow g_i = g_j.$$

Portanto, ρ é injetiva.

Vale ressaltar que as matrizes da representação regular pertencem à $W(n, K)$, uma vez que $\rho(g_i)(e_k) = e_j$, ou seja, $\rho(g_i)(e_k) = 0 \cdot e_1 + 0 \cdot e_2 + \cdots + 1 \cdot e_j + \cdots + 0 \cdot e_n$, para algum $j \in \{1, 2, \cdots, n\}$, assegurando que cada coluna terá uma única entrada preenchida

com 1. Como ρ é injetiva obtemos que cada linha terá apenas uma entrada preenchida com 1.

Para ilustrar o exemplo acima, consideraremos o grupo $(\mathbb{Z}_2, +)$ e $V = P_1$ o espaço vetorial dos polinômios na incógnita de x com grau menor ou igual a 1 e a base canônica $B = \{1, x\}$. Assim, considerando $f(\bar{0}) = 1 = e_1$ e $f(\bar{1}) = x = e_2$, temos que

$$\begin{cases} \rho(\bar{0})(1) = f(\bar{0} + \bar{0}) = f(\bar{0}) = e_1, \\ \rho(\bar{0})(x) = f(\bar{0} + \bar{1}) = f(\bar{1}) = e_2. \end{cases}$$

Com os dados acima podemos representar o elemento $\bar{0}$ via matriz de transformação.

$$1 = 1 \cdot 0 + 0 \cdot x \leftrightarrow e_1 = 1 \cdot e_1 + 0 \cdot e_2$$
$$x = 0 \cdot 1 + 1 \cdot x \leftrightarrow e_2 = 0 \cdot e_1 + 1 \cdot e_2,$$

e assim,

$$\rho(\bar{0}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

De modo similar

$$\rho(\bar{1}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Assim $\mathbb{Z}_2 \cong \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ *sobre* P_1.

Sejam $p(x) \in P_1$ e $B = \{e_1, e_2\}$ uma base de P_1. Assim temos que $p(x) = \alpha e_1 + \beta e_2$. Então

$$\rho(g)(\alpha e_1 + \beta e_2) = \alpha \rho(g)(e_1) + \beta \rho(g)(e_2).$$

Se $g = \bar{0}$ temos $\rho(\bar{0})(\alpha e_1 + \beta e_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_B^t = \begin{bmatrix} \alpha & \beta \end{bmatrix}_B = \alpha e_1 + \beta e_2.$

Mas, por outro lado, se $g = \bar{1}$, obtemos que

$$\rho(\bar{1})(\alpha e_1 + \beta e_2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_B^t = \begin{bmatrix} \beta & \alpha \end{bmatrix}_B = \beta e_1 + \alpha e_2.$$

Notemos que a representação regular independe do espaço vetorial se os espaços vetoriais em questão tiverem a mesma dimensão. Isso ocorre devido ao fato de que operamos

a ordem dos elementos da base ordenada e a ordem da matriz resultante é de acordo com a dimensão do espaço vetorial. Por exemplo, no caso anterior, se houvéssemos tomado $V = \mathbb{R}^2$ *teríamos a mesma representação para* $\mathbb{Z}_2$.

Dessa vez, consideraremos $G = (\mathbb{Z}_3, +)$, $V = \mathbb{R}^3$ *e a base canônica* $\{e_1, e_2, e_3\}$, *em que* $f(\bar{0}) = e_1$, $f(\bar{1}) = e_2$ *e* $f(\bar{2}) = e_3$. *Assim,*

$$\begin{cases} \rho(\bar{0})(e_1) = e_{\sigma_{\bar{0}}(1)} = e_1, \\ \rho(\bar{0})(e_2) = e_{\sigma_{\bar{0}}(2)} = e_2, \\ \rho(\bar{0})(e_3) = e_{\sigma_{\bar{0}}(3)} = e_3. \end{cases}$$

Portanto,

$$\rho(\bar{0}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

De modo similar, obtemos

$$\rho(\bar{1}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ \rho(\bar{2}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Concluímos assim que a representação de $\mathbb{Z}_3$ *em* $\mathbb{R}^3$ *é*

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}.$$

Exemplo 16. *Analisaremos a seguir as representações dos grupos de mesma ordem* $S_4, \mathbb{Z}_4, \mathbb{Z}_5^*$ *em um espaço vetorial* V *sobre* $\mathbb{C}^4$ *considerando uma base qualquer. Primeiramente examinaremos o grupo de Klein, ou seja, o conjunto*

$$K = \{Id, (12)(34), (13)(24), (14)(23)\}.$$

Notemos que

$$K \cong \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\} \text{ em } \mathbb{C}^4.$$

Por outro lado, seja o grupo $(\mathbb{Z}_4, +)$, *obtemos que*

$$\mathbb{Z}_4 \cong \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\} \text{ em } \mathbb{C}^4.$$

Ainda nesse sentido, $(\mathbb{Z}_5^*, \cdot)$ *grupo em que* $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ *temos que*

$$\mathbb{Z}_5^* \cong \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\} \text{ em } \mathbb{C}^4.$$

Ao analisarmos o traço de cada matriz obtida por meio das representações do exemplo acima concluímos que os traços serão iguais a zero ou iguais a quatro. A matriz possui traço igual a 4, quando obtemos a matriz identidade, ou traço igual a 0 nos demais casos.

Proposição 14. *Seja* ρ *uma representação regular de um grupo* G *de ordem* n*, então*

$$tr(\rho(g)) = 0, \text{ para todo } g \neq e;$$

$$tr(\rho(e)) = n.$$

Demonstração. Temos que $\rho(g)(e_k) = e_j$ com $j \in \{1, ..., n\}$, logo a k-ésima coluna da matriz da representação de g terá apenas a entrada a_{jk} preenchida com 1. Além disso, devido ao fato de ρ ser injetiva, temos que cada linha da matriz da representação de g terá exatamente uma entrada com o número 1. Desse modo, para o traço de uma matriz de uma representação regular $M = [a_{ij}]$ ser diferente de zero é necessário que, para algum k, a_{kk} seja não nulo, ou seja, $a_{kk} = 1$, tal fato ocorre se $\rho(g)(e_k) = e_k$, acarretando que $g \cdot g_k = g_k$, logo g é a identidade do grupo, concluindo também que $g \cdot e_k = e_k$ para todo k. Assim, somente a matriz associada à $\rho(g)(e_k)$ com g sendo a identidade do grupo possui o traço distinto de nulo, além disso, esta matriz será a matriz identidade $n \times n$, portanto terá traço igual à n . □

Por outro lado, consideremos uma representação regular arbitrária e M uma matriz desta representação associada a um elemento ordem finita n de G, disto obtemos que, $M^n = Id$, implicando que $M^n - Id = 0$, ou seja, M é raiz do polinômio $x^n - 1$. Assim, seja $m_M(x)$ o polinômio minimal de A, temos que $m_A(x) | x^n - 1$.

Além disso, pelo *Teorema Fundamental da Álgebra*, $x^n - 1$ se decompõe em fatores lineares distintos sobre $\mathbb{C}$, uma vez que $x^n - 1$ possui n raízes distintas, todas as n raízes n-ésimas da unidade, o que nos permite concluir que $m_M(x)$ é o produto de fatores lineares

distintos em $\mathbb{C}$. Sabendo que uma matriz é diagonalizável se, só se, o polinômio minimal da mesma é produto de fatores lineares, [5] concluímos que M é diagonalizável, ou seja, existe uma matriz P invertível tal que $D = P^{-1}MP$, com D uma matriz diagonal que possui sua diagonal principal preenchida pelos seus autovalores que coincidem com os autovalores de M. Denotaremos tais autovalores como λ_i, com $i \in \{1, 2, \cdots, n\}$. Assim,

$$D = P^{-1}MP \Rightarrow D^n = \left(P^{-1}MP\right)^n = P^{-1}M^nP = P^{-1}P = Id.$$

Como duas matrizes são iguais se, somente se, suas entradas correspondentes também os são, obtemos que $\lambda_i^n = 1$, logo o autovalor é uma raiz n-ésima da unidade.

[5] A afirmação citada é proveniente da definição de polinômio minimal e da Observação 5 encontrada na página 89 da bibliografia (NICHOLSON, 2014).

2 Teoria de Módulos

A teoria dos módulos é considerada um ramo recente dentro da Matemática que teve seu desenvolvimento no século XX. Sua primeira aparição, mesmo que implicitamente foi na obra de Richards Dedekind (1831 -1916) em Teoria dos Números. Mas, somente em 1929 a matemática alemã Amallie Emmy Noether (1882 -1935) publicou sobre teoria dos módulos, uma das muitas contribuições realizadas na Álgebra Abstrata. A teoria de módulos está relacionada com representação de grupos e é empregada fortemente nas áreas de álgebra comutativa, álgebra homológica, topologia algébrica e geometria algébrica (MILIES, 2018).

Neste capítulo, trataremos do tema de modo objetivo abordando os conceitos e resultados necessários para os estudos do problema central desse trabalho.

Definição 31. *Seja R um anel comutativo com unidade. Nomeamos como um R-módulo (ou um módulo sobre R) um conjunto não vazio M, munido com as operações denominadas adição $(\oplus)$ e produto por escalar $(\odot)$, tais que, para todo $r, s \in R$ e $u, v \in M$, satisfazem:*

i. $(M, \oplus)$ *é um grupo abeliano;*

ii. $r \odot (u \oplus v) = r \odot u \oplus r \odot v$;

iii. $(r + s) \odot u = r \odot u \oplus s \odot u$;

iv. $(r \cdot s) \odot u = r \odot (s \odot u)$;

v. $1_R \odot u = u$.

Chamamos R de anel base de M e seus elementos de escalares.

Exemplo 17.

i. Todo anel comutativo com unidade R é um R-módulo;

ii. Espaços vetoriais são módulos sobre corpos.

Proposição 15. *Seja M um R-módulo, se $m \in M$ e $r \in R$ temos que*

i. $0_R \odot m = 0_M$;

ii. $r \odot 0_M = 0_M$;

iii. $(-r) \odot m = -(r \odot m) = r \odot (-m)$.

Demonstração. *i*. Notemos que

$$0_R \odot m = (0_R + 0_R) \odot m = 0_R \odot m \oplus 0_R \odot m,$$

assim,

$$0_M = (-0_R \odot m) \oplus (0_R \odot m) = (-0_R \odot m) \oplus (0_R \odot m) \oplus (0_R \odot m) = 0_R \odot m.$$

ii. Observemos que

$$\begin{aligned} 0_M = -(r \odot 0_M) \oplus (r \odot 0_M) = -(r \odot 0_M) \oplus (r \odot (0_M + 0_M)) = \\ = -(r \odot 0_M) \oplus (r \odot 0_M) \oplus (r \odot 0_M) = r \odot 0_R. \end{aligned}$$

iii. Temos que $-(r \odot m)$ é o elemento inverso da adição de $r \odot m$, ou seja, $-(r \odot m) \oplus r \odot m = 0_M$, assim

$$(-r) \odot m \oplus r \odot m = (-r + r) \odot m = 0_R \odot m = 0_M,$$

e

$$r \odot (-m) \oplus r \odot m = r \odot (-m + m) = r \odot 0_M = 0_M.$$

Pela unicidade do elemento inverso, concluímos que $-(r \odot m) = (-r \odot m) = r \odot (-m)$. □

Doravante, para $r \in R$ e $v \in M$, denotaremos $r \odot v$ como rv por justaposição.

Definição 32. *Seja M um R-módulo. Um subconjunto S não vazio de M é chamado de R-submódulo de M se com as operações de M temos que S também é um R-módulo.*

Teorema 6. *Um subconjunto S não vazio de M é submódulo de M se, e somente se, para todos $r, s \in R$ e $u, v \in S$, implica que $ru + sv \in S$.*

Demonstração. Primeiramente consideremos $r, s \in R$, $u, v \in S$ com $ru + sv \in S$ notemos que como $S \subseteq M$ a associatividade da soma válida para M também é válida para o subconjunto S, assim como a comutatividade da soma. Tomando $r = s = 0_R$ obtemos que $0_R u + 0_R v = 0_M \in S$, ainda nesse sentindo se $r = 0_R$ e $s = -1_R$, então $-1_R v \in S$, logo existe o elemento inverso da adição de v. Assim provamos o item *i*. da Definição 31. Por fim, os itens *ii*,*iii*, *iv* e *v* decorrem do fato de $S \subseteq M$.Logo S é um submódulo de M. □

Teorema 7. *Sejam T e S dois R-submódulos de um R-módulo M, temos que $S \cap T$ e $S + T = \{s + t \mid s \in S \, e \, t \in T\}$ são R-submódulos de M.*

Demonstração. Sejam $r, s \in R$ e $u, v \in S \cap T$, então $u, v \in S$ e $u, v \in T$, assim como S e T são R-submódulos temos que $ru + sv \in S$ e $ru + sv \in T$, implicando que $ru + sv \in S \cap T$, logo $S \cap T$ é um R-submódulo.

Por fim, sejam $u = s_1 + t_1$, $v = s_2 + t_2 \in S + T$ e $r, s \in R$ temos que

$$ru + sv = r\left(s_1 + t_1\right) + s\left(s_2 + t_2\right) = rs_1 + ss_2 + rt_1 + st_2,$$

como S e T são R-submódulos concluímos que $rs_1 + ss_2 \in S$ e $rt_1 + st_2 \in T$, implicando que $ru + sv \in S + T$. □

Definição 33. *Seja M um R-módulo. Chamamos de combinação linear finita toda soma expressa como*

$$r_1 v_1 \oplus \cdots \oplus r_n v_n,$$

com $r_i \in R$, $v_i \in M$ e $n \in \mathbb{N}$.

Seja S um subconjunto do R-módulo de M, consideremos $x = \sum_{i=1}^{k} r_i v_i, y = \sum_{i=1}^{l} s_i u_i$ com $r_i, s_i \in R, v_i, u_i \in S$ e $k, l \in \mathbb{N}$, notemos que

$$x - y = \sum_{i=1}^{k} r_i v_i - \sum_{i=1}^{l} s_i u_i = \sum_{i=1}^{k} r_i v_i \oplus \sum_{i=1}^{l} - s_i u_i = \sum_{i=1}^{k+l} \tilde{r}_i \tilde{v}_i,$$

com $\tilde{r}_i \in R, \tilde{v}_i \in S$.

Além disso, se $r \in R$, então

$$rx = r\sum_{i=1}^{k} r_i v_i = \sum_{i=1}^{k} r r_i v_i = \sum_{i=1}^{k} \tilde{s}_i v_i.$$

Assim, sejam M um R-módulo e S um subconjunto de M, o conjunto

$$\langle\langle S \rangle\rangle = \left\{ \sum_{i=1}^{k} r_i v_i \mid r_i \in R \, e \, v_i \in S \right\}$$

é denominado *R-submódulo de M gerado por S*. E mais, para $v \in M$,

$$\langle\langle v \rangle\rangle = \{rv \mid r \in R\}$$

é chamado de R-submódulo cíclico gerado por v.

Definição 34. *Seja M um R-Módulo, dizemos que um subconjunto S não vazio de M é linearmente independente se para quaisquer $v_1, \cdots, v_n \in S$ e $r_1, \cdots, r_n \in R$ tais que*

$r_1v_1 \oplus \cdots \oplus r_nv_n = 0$ *implicando que* $r_i = 0$ *para todo* $i = 1, \cdots, n$ *com* $n \in \mathbb{N}$.

Definição 35. *Seja M um R-módulo. Dizemos que um conjunto B, com $B \subseteq M$, é uma base de M se*

i. B *é linearmente independente;*

ii. $M = \langle\langle B \rangle\rangle$.

Se um R-módulo M possui uma base B, então denominamos M como um Módulo Livre.

Definição 36. *Seja R um anel comutativo com unidade. O posto de um R-módulo livre não nulo M é a cardinalidade de qualquer base para M.*

O seguinte Teorema pode ser consultado em *Advanced Linear Álgebra. 2ªEd. Springer. 2005.* de Roman, Steven.

Teorema 8. *Dois R-módulos livres sobre um R comutativo são isomorfos, se, e somente se, tiverem o mesmo posto.*

Definição 37. *Seja R um anel comutativo. Um R-módulo A é dito uma R-álgebra se existe uma multiplicação definida em A tal que, com a adição em A, A é um anel para qual se verifica para todos $r \in R$ e $a, b \in A$:*

$$r(ab) = (ra)b = a(rb).$$

Definição 38. *Sejam M e N R-módulos. Definimos o produto tensorial de M com N sobre R, denotado por $M \otimes_R N$, como um conjunto que satisfaz as seguintes propriedades para todo $r \in R$, $m, m' \in M$, $n, n' \in N$:*

i. $r\,(m \otimes n) = rm \otimes n$;

ii. $r\,(m \otimes n) = m \otimes rn$;

iii. $(m + m') \otimes n = m \otimes n + m' \otimes n$;

iv. $m \otimes (n + n') = m \otimes n + m \otimes n'$.

Exemplo 18. *Seja $a \otimes b \in \mathbb{Z} \otimes_{\mathbb{Z}} 2\mathbb{Z}$. Assim, $b = \bar{0}$ ou $b = \bar{1}$, se $b = \bar{0}$, notemos*

$$a \otimes \bar{0} = 0_{\otimes_{\mathbb{Z}}}.$$

Se $b = \bar{1}$, e a par, isto é, $a = 2k$ com $k \in \mathbb{Z}$. Daí,

$$2k \otimes_{\mathbb{Z}} \bar{1} = k \otimes_{\mathbb{Z}} \bar{2} = k \otimes \bar{0} = 0_{\otimes_{\mathbb{Z}}}.$$

Por sua vez, se a for ímpar, ou seja, $2k+1$*, com* $k \in \mathbb{Z}$*,*

$$(2k+1) \otimes \bar{1} = 2k \otimes \bar{1} + 1 \otimes \bar{1} = k \otimes \bar{0} + 1 \otimes \bar{1} = 1 \otimes \bar{1}.$$

Portanto, $\mathbb{Z} \otimes_{\mathbb{Z}} 2\mathbb{Z} = \{0_{\otimes_{\mathbb{Z}}}, 1 \otimes \bar{1}\}$.

3 Teoria de Anéis de Grupo e o Problema do Isomorfismo para o Anel dos Inteiros em Grupos Finitos Abelianos

Neste capítulo, estudaremos a estrutura denominada anel de grupo que surge no século XIX por meio da análise dos números da forma $\alpha = a + bi + cj + dk$ com a, b, c, d números reais e i, j, k unidades básicas. Tais números nomeados como quarténios foram estudados pelo Willian Roman Hamilton em 1837, e posteriormente, John T. Graves, analisou os números conhecidos como octônios, da forma $a_0 + a_1e_1 + \cdots + a_7e_7$, em que a_i é um número real e e_i unidades básicas com $0 \leq i \leq 7$. Mas de forma independente Arthur Cayley em 1845 publicou o estudo dos octônios, ficando assim conhecidos como números de Cayley (MILIES; SEHGAL, 2002).

Definição 39. *Seja G um grupo e R um anel. Definimos o conjunto RG como toda combinação linear finita formal de elementos de G com escalares em R, isto é, $\alpha \in RG$ se, e somente se, $\alpha = \sum_{g \in G} \alpha_g \circledast g$.*

Para melhor compreensão consideremos o anel $\mathbb{Z}_3$ e o grupo S_2. Listemos a seguir os elementos de $\mathbb{Z}_3S_2$:

$$\begin{array}{lll} \overline{0} \circledast Id + \overline{0} \circledast (12) & \overline{0} \circledast Id + \overline{1} \circledast (12) & \overline{0} \circledast Id + \overline{2} \circledast (12) \\ \overline{1} \circledast Id + \overline{0} \circledast (12) & \overline{1} \circledast Id + \overline{1} \circledast (12) & \overline{1} \circledast Id + \overline{2} \circledast (12) \\ \overline{2} \circledast Id + \overline{0} \circledast (12) & \overline{2} \circledast Id + \overline{1} \circledast (12) & \overline{2} \circledast Id + \overline{2} \circledast (12)\,. \end{array}$$

Vale ressaltar que a operação $\circledast$ é uma operação formal que aplica o par $(\overline{a}, \alpha)$ com $\overline{a} \in \mathbb{Z}_3$, $\alpha \in S_2$, em $\overline{a} \circledast \alpha$. Omitiremos tal operação ao longo do nosso texto, desde que não haja risco de equívoco por parte do leitor ou da leitora. Assim, denotaremos por justa posição $\sum_{g \in G} \alpha_g \circledast g = \sum_{g \in G} \alpha_g g$.

Além disso, o conjunto RG não necessariamente é finito, mas seus elementos são uma soma finita. A finitude de RG se dará no caso em que o grupo e o anel sejam finitos, pois haverá um número finito de combinações lineares. Além da observação anterior, considerando $\alpha = \sum \alpha_g g$ e $\beta = \sum \beta_g g$, podemos afirmar que se $\alpha = \beta$, então $\alpha_g = \beta_g$ para todo $g \in G$.

Após tais considerações podemos questionar se é possível construir operações para um anel de grupo, uma vez que tal conjunto é definido a partir de duas estruturas algébricas,

as quais possuem operações. Assim, estabelecemos as seguintes operações básicas para o conjunto RG:

$$\text{i.} \quad \begin{array}{rcl} + : RG \times RG & \to & RG \\ \left(\sum_{g\in G}\alpha_g g, \sum_{g\in G}\beta_g g\right) & \longmapsto & \sum_{g\in G}(\alpha_g+\beta_g)\,g. \end{array}$$

$$\text{ii.} \quad \begin{array}{rcl} \cdot : RG \times RG & \to & RG \\ \left(\sum_{g\in G}\alpha_g g, \sum_{g\in G}\beta_g g\right) & \longmapsto & \sum_{g,h\in G}(\alpha_g\beta_h)\,gh \end{array}$$

$$\text{iii.} \quad \begin{array}{rcl} * : R \times RG & \to & RG \\ \left(\lambda, \sum_{g\in G}\alpha_g g\right) & \longmapsto & \sum_{g\in G}(\lambda\alpha_g)\,g. \end{array}$$

Após as definições acima podemos abordar o conceito principal deste capítulo: anel de grupo, e construir a teoria necessária para os nossos estudos.

Teorema 9. *Dados um anel R e um grupo G, o conjunto RG munido com as operações i. e ii. é um anel.*

Demonstração. Sejam $\alpha, \beta, \gamma \in RG$, assim temos que:

$$\sum_{g\in G}\alpha_g g + \sum_{g\in G}0_R g = \sum_{g\in G}(\alpha_g + 0_R)g = \sum_{g\in G}\alpha_g g.$$

Ou seja, existe o elemento neutro da soma. Assim, obtemos que, para cada elemento $\alpha \in RG$, existe o elemento invertível da soma, uma vez que

$$\alpha + (-\alpha) = \sum_{g\in G}\alpha_g g + \left(-\sum_{g\in G}\alpha_g g\right) = \sum_{g\in G}\alpha_g g + \sum_{g\in G} - \alpha_g g = \sum_{g\in G}(\alpha_g - \alpha_g)g = \sum_{g\in G}0_R g.$$

Além disso,

$$\alpha + \beta = \sum_{g\in G}\alpha_g g + \sum_{g\in G}\beta_g g = \sum_{g\in G}(\alpha_g + \beta_g)g = \sum_{g\in G}(\beta_g + \alpha_g)g = \sum_{g\in G}\beta_g g + \sum_{g\in G}\alpha_g g = \beta_g + \alpha_g.$$

$$(\alpha + \beta) + \gamma = \sum_{g\in G}[(\alpha_g + \beta_g) + \gamma_g]g = \sum_{g\in G}[\alpha_g + (\beta_g + \gamma_g)]g = \alpha + (\beta + \gamma).$$

Concluindo que a operação $i.$ é comutativa e associativa. Ainda nesse sentido, observemos a demonstração da associatividade do produto e da distributiva a seguir:

$$(\alpha\cdot\beta)\cdot\gamma = \sum_{g,h\in G}(\alpha_g\beta_h)\,gh \cdot \sum_{g,\in G}\gamma_g g = \sum_{g,h,j\in G}[(\alpha_g\beta_h)\,\gamma_j]ghj = \sum_{g,h,j\in G}[\alpha_g(\beta_h\gamma_j)]ghj = \alpha\cdot(\beta\cdot\gamma);$$

$$(\alpha+\beta)\cdot\gamma=\sum_{g,\in G}(\alpha_g+\beta_h)\,g\cdot\sum_{g,\in G}\gamma_g g=\sum_{g,h\in G}[(\alpha_g+\beta_g)\,\gamma_h]gh=\sum_{g,h\in G}(\alpha_g\gamma_h+\beta_g\gamma_h)gh$$

$$=\sum_{g,h\in G}(\alpha_g\gamma_h)\,gh+\sum_{g,h,\in G}(\beta_g\gamma_h)gh=\alpha\gamma+\beta\gamma.$$

A prova de $\gamma(\alpha+\beta)=\gamma\alpha+\gamma\beta$ é análoga à anterior. Portanto, após as demonstrações das propriedades podemos afirmar que RG é um anel. □

Vale ressaltar que o elemento da forma $I_{RG}=1_Re\in RG$ e mais

$$\alpha\cdot I_{RG}=\sum_{g\in G}\alpha_g g\cdot 1_Re=\sum_{g\in G}(\alpha_g 1_R)ge=\sum_{g\in G}\alpha_g g=\alpha.$$

De modo similar, obtemos que $I_{RG}\cdot\alpha=\alpha$, assim obtemos que I_{RG} é a unidade do anel RG.

Definição 40. *O anel RG é denominado como anel de grupo de G sobre R.*

Desse modo, a partir das operações deste capítulo, podemos concluir que o anel RG é um R-módulo. Em particular, $\mathbb{Z}G$ é um $\mathbb{Z}$-módulo Livre de posto $|G|$.

Observação 6. *Sejam $\alpha,\beta\in RG$ com G um grupo abeliano e R comutativo, notemos que*

$$\alpha\cdot\beta=\sum_{g,h\in G}(\alpha_g\beta_h)\,gh=\sum_{g,h\in G}(\alpha_g\beta_h)\,hg=\beta\cdot\alpha,$$

assim, concluímos que G é um grupo abeliano se, e somente se, RG é comutativo.

Dentro da teoria de Anel de Grupo nos deparamos com a seguinte função denominada *Aplicação de Aumento de RG*:

$$\begin{array}{rccc}\varepsilon:\ RG & \to & R\\ \sum_{g\in G}\alpha_g g & \longmapsto & \sum_{g\in G}\alpha_g.\end{array}$$

Sejam $\alpha,\beta\in RG$, notemos que

$$\varepsilon(\alpha+\beta)=\varepsilon\left(\sum_{g\in G}\alpha_g g+\sum_{g\in G}\beta_g g\right)=\varepsilon\left(\sum_{g\in G}(\alpha_g+\beta_g)\,g\right)=\sum_{g\in G}(\alpha_g+\beta_g)=\sum_{g\in G}\alpha_g+$$
$$+\sum_{g\in G}\beta_g=\varepsilon(\alpha)+\varepsilon(\beta).$$

Além disso, considerando $r\in R$, é possível observar que $r=\varepsilon(rg)$ para todo $g\in G$. Assim, concluímos que a função ε é um homomorfismo sobrejetivo, cujo núcleo denominamos como *ideal de aumento de RG*.

A seguir, abordaremos os resultados que auxiliam a demonstração do Problema do Isomorfismo de Anéis de Grupo, restringindo para o caso particular dos anéis dos inteiros e grupos finitos abelianos. O primeiro registro do problema se deu por meio do Graham Higman $(1917-2008)$, em 1940, em *"The units of group-rings"*, e posteriormente, em 1947,o problema foi apresentado na conferência de álgebra em Michigan pelo T.M. Thrall com os dizeres: *"Dado um grupo G e um corpo K, determine todos os grupos H de forma que KG é isomorfo à KH"* (MILIES; SEHGAL, 2002).

Primeiramente provaremos o seguinte lema que trata-se da recíproca de um caso particular do teorema acima.

Lema 1. *Sejam G e H dois grupos, tais que $\mathbb{Z}G$ é isomorfo à $\mathbb{Z}H$, então RG é isomorfo à RH para qualquer anel comutativo R (como R- álgebra).*

Demonstração. Definindo

$$\begin{array}{rccc} \phi: & R\otimes_{\mathbb{Z}}\mathbb{Z}G & \to & RG \\ & \sum\limits^{finita}(r_i\otimes_{\mathbb{Z}}\alpha_i) & \longmapsto & \sum\limits^{finita} r_i\alpha_i, \end{array}$$

podemos realizar algumas observações sobre a aplicação ϕ. Primeiramente, se $\alpha_i=\sum\limits_{g\in G}\alpha_{ig}g$, então

$$\sum^{finita}(r_i\otimes_{\mathbb{Z}}\alpha_i)=\sum^{finita}\left(r_i\otimes_{\mathbb{Z}}\sum_{g\in G}\alpha_{ig}g\right)=\sum^{finita}\sum_{g\in G}(r_i\otimes_{\mathbb{Z}}\alpha_{ig}g)=\sum^{finita}\sum_{g\in G}((r_i\alpha_{ig})\otimes_{\mathbb{Z}}g).$$

Considerando que a ordem de G é n, notemos que

$$\sum^{finita}\sum_{g\in G}((r_i\alpha_{ig})\otimes_{\mathbb{Z}}g)=$$

$$=r_1\alpha_{1g_1}\otimes_{\mathbb{Z}}g_1+\cdots+r_1\alpha_{1g_n}\otimes_{\mathbb{Z}}g_n+\cdots+r_m\alpha_{mg_1}\otimes_{\mathbb{Z}}g_1+r_m\alpha_{mg_2}\otimes_{\mathbb{Z}}g_2+\cdots+r_m\alpha_{mg_n}\otimes_{\mathbb{Z}}g_n$$

$$=(r_1\alpha_{1g_1}+r_2\alpha_{2g_1}+\cdots+r_m\alpha_{mg_1})\otimes_{\mathbb{Z}}g_1+\cdots+(r_1\alpha_{1g_n}+r_2\alpha_{2g_n}+\cdots+r_m\alpha_{mg_n})\otimes_{\mathbb{Z}}g_n.$$

Como α_{ig_j} são escalares inteiros, temos uma ação de grupo que nos possibilita afirmar que

$$\sum^{finita}\sum_{g\in G}((r_i\alpha_{ig})\otimes_{\mathbb{Z}}g)=\sum_{g\in G}(r_g\otimes_{\mathbb{Z}}g).$$

Além disso,

$$\sum^{finita}r_i\alpha_i=\sum^{finita}r_i\left(\sum_{g\in G}\alpha_{ig}g\right)=\sum^{finita}r_i(\alpha_{ig_1}g_1+\cdots+\alpha_{ig_n}g_n)=\sum^{finita}r_i\alpha_{ig_1}g_1+\cdots+r_i\alpha_{ig_n}g_n$$

$$= r_1\alpha_{1g_1}g_1 + \cdots + r_1\alpha_{1g_n}g_n + \cdots + r_m\alpha_{mg_1}g_1 + \cdots + r_m\alpha_{mg_n}g_n,$$

agrupando os escalares correspondentes ao mesmo elemento do grupo, obtemos

$$\sum^{finita} r_i\alpha_i = \sum_{i=1}^{n}(r_1\alpha_{1g_i} + \cdots + r_m\alpha_{mg_i})g_i.$$

Pela mesma argumentação realizada acima em relação à ação de grupos, concluímos que

$$\sum^{finita} r_i\alpha_i = \sum_{g\in G} r_g g.$$

Assim, após descrevermos a forma dos elementos que estão no domínio e contra-domínio podemos analisar a injetividade e sobrejetividade da ϕ.

Sejam $\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i) = \sum_{g\in G} r_g \otimes_{\mathbb{Z}} g$ e $\sum^{finita} (s_i \otimes_{\mathbb{Z}} \beta_i) = \sum_{g\in G} s_g \otimes_{\mathbb{Z}} g$ elementos de $R \otimes_{\mathbb{Z}} \mathbb{Z}G$, então

$$\phi\left(\sum_{g\in G} r_g \otimes_{\mathbb{Z}} g + \sum_{g\in G} s_g \otimes_{\mathbb{Z}} g\right) = \phi\left(\sum_{g\in G}(r_g + s_g) \otimes_{\mathbb{Z}} g\right) = \sum_{g\in G}(r_g + s_g)g = \sum_{g\in G} r_g g + \sum_{g\in G} s_g g$$

$$= \phi\left(\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i)\right) + \phi\left(\sum^{finita} (s_i \otimes_{\mathbb{Z}} \beta_i)\right).$$

Ainda nesse sentido, temos que

$$\phi\left(r\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i)\right) = \phi\left(\sum^{finita} (rr_i \otimes_{\mathbb{Z}} \alpha_i)\right) = \sum_{g\in G}(rr_i)g = r\sum_{g\in G} r_g g = r\phi\left(\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i)\right),$$

logo a aplicação ϕ é um homomorfismo.

Podemos notar também que se $\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i) \in Ker(\phi)$ então

$$\phi\left(\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i)\right) = \phi\left(\sum_{g\in G}(r_g \otimes_{\mathbb{Z}} g)\right) = \sum_{g\in G} r_g g = 0,$$

assim

$$r_g = 0 \text{ para todo } g \in G,$$

isto é,

$$\sum^{finita} (r_i \otimes_{\mathbb{Z}} \alpha_i) = \sum^{finita} (0 \otimes_{\mathbb{Z}} g) = 0.$$

Dessa maneira, $Ker(\phi) = \{0\}$, acarretando que ϕ é injetiva. Por outro lado, se $\beta \in RG$, ou seja, $\beta = \beta_{g_1}g_1 + \beta_{g_2}g_2 + \cdots + \beta_{g_n}g_n$ observemos que

$$\phi\left(\beta_{g_1} \otimes_{\mathbb{Z}} g_1 + \beta_{g_2} \otimes_{\mathbb{Z}} g_2 + \cdots + \beta_{g_n} \otimes_{\mathbb{Z}} g_n\right) = \sum_{i=1}^{n} \phi\left(\beta_{g_i} \otimes_{\mathbb{Z}} g_i\right) = \sum_{i=1}^{n} \beta_{g_i} g_i = \beta.$$

Assim ϕ é sobrejetivo, portanto, podemos afirmar que

$$R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong RG.$$

Analogamente, obtemos que

$$R \otimes_{\mathbb{Z}} \mathbb{Z}H \cong RH,$$

assim como $\mathbb{Z}G \cong \mathbb{Z}H$, concluímos que

$$RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong R \otimes_{\mathbb{Z}} \mathbb{Z}H \cong RH \Rightarrow RG \cong RH.$$

□

Por ventura, seja $g \in G$ é invertível, temos que existe g^{-1} em que

$$gg^{-1} = e \Rightarrow \varepsilon(gg^{-1}) = \varepsilon(e) \Rightarrow \varepsilon(g)\varepsilon(g^{-1}) = \varepsilon(e) \Rightarrow \varepsilon(g)\varepsilon(g)^{-1} = 1,$$

logo $\varepsilon(g)$ é invertível.

Além disso, sejam G e H grupos finitos e

$$\phi : \mathbb{Z}G \to \mathbb{Z}H$$

um isomorfismo, se G possui ordem n, temos que para todo $g \in G$, obtemos que $g^n = e$ logo $\phi(g)^n = e$. Portanto,

$$\phi(g)\phi(g)^{n-1} = e,$$

ou seja, $\phi(g)$ é invertível em $\mathbb{Z}H$ e possui ordem finita.

Lema 2. *Sejam G um grupo e $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo. Se g é invertível em G, então $\varepsilon(\phi(g))$ é invertível em $\mathbb{Z}$.*

Seja G um grupo, definimos o *conjunto dos elementos invertíveis de $\mathbb{Z}G$* como

$$U(\mathbb{Z}G) = \{\alpha \in \mathbb{Z}G \mid \alpha \text{ é invertível}\}.$$

Notemos que se $\alpha, \beta \in U(\mathbb{Z}G)$, então

$$\left(\alpha\beta^{-1}\right)(\beta\alpha^{-1}) = \alpha(\beta^{-1}\beta)\alpha^{-1} = \alpha\alpha^{-1} = I_{RG}.$$

De modo análogo, obtemos que $(\beta\alpha^{-1})(\alpha\beta^{-1}) = I_{RG}$, assim $\alpha\beta^{-1} \in U(\mathbb{Z}G)$, portanto, pelo Teorema 1, $U(\mathbb{Z}G)$ é um subgrupo de RG.

Seja α um elemento invertível de RG, dizemos que α é um *invertível normalizado* se, e somente se, $\varepsilon(\alpha) = 1$. Assim, definimos o conjunto dos *elementos invertíveis normalizados de $\mathbb{Z}G$*:

$$U_1(\mathbb{Z}G) = \{\alpha \in U(\mathbb{Z}G) \,|\, \varepsilon(\alpha) = 1\}.$$

Se $\alpha, \beta \in U_1(\mathbb{Z}G)$, então

$$\varepsilon(\beta\beta^{-1}) = \varepsilon(I_{RG}) \Rightarrow \varepsilon(\beta)\varepsilon(\beta^{-1}) = 1 \Rightarrow \varepsilon(\beta^{-1}) = 1,$$

e mais

$$\varepsilon(\alpha\beta^{-1}) = \varepsilon(\alpha)\varepsilon(\beta^{-1}) = 1,$$

assim, $U_1(\mathbb{Z}G)$ é subgrupo de $U(\mathbb{Z}G)$, pelo Teorema 1.

Definição 41. *Seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo. Dizemos que ϕ é um isomorfismo normalizado, se para todo elemento $\alpha \in \mathbb{Z}G$, temos que $\varepsilon(\phi(\alpha)) = \varepsilon(\alpha)$. É equivalente enunciar que, para cada elemento de $g \in G$, obtemos que $\varepsilon(\phi(g)) = 1$.*

Proposição 16. *Se existe um isomorfismo $\phi : \mathbb{Z}G \to \mathbb{Z}H$, então existe um isomorfismo normalizado entre $\mathbb{Z}G$ e $\mathbb{Z}H$.*

Demonstração. Consideraremos

$$\begin{array}{rccc} \tau: & \mathbb{Z}G & \to & \mathbb{Z}H \\ & \sum\limits_{g\in G}\alpha_g g & \longmapsto & \sum\limits_{g\in G}\varepsilon(\phi(g))^{-1}\alpha_g\phi(g). \end{array}$$

Temos que τ está bem definida pelo Lema 2, além disso, notemos que

$$\varepsilon\left(\varepsilon(\phi(g))^{-1}\alpha_g\phi(g)\right) = \varepsilon(\phi(g))^{-1}\varepsilon(\alpha_g)\varepsilon(\phi(g)) = \varepsilon(\phi(g))^{-1}\alpha_g\varepsilon(\phi(g)) = \alpha_g,$$

e assim

$$\varepsilon\left(\sum_{g\in G}(\varepsilon(\phi(g))^{-1}\alpha_g\phi(g)\right) = \sum_{g\in G}\varepsilon(\varepsilon(\phi(g)^{-1}\alpha_g\phi(g))) = \sum_{g\in G}\alpha_g.$$

Dessa forma, temos que τ é um isomorfismo normalizado de $\mathbb{Z}G$ em $\mathbb{Z}H$.

□

Vale observar que se ϕ é um isomorfismo normalizado temos que ϕ^{-1} também será um isomorfismo normalizado, pois para todo $\beta \in \mathbb{Z}H$ consideraremos $\phi^{-1}(\beta) = \alpha$, logo $\phi(\alpha) = \beta$, assim

$$\varepsilon(\phi^{-1}(\beta)) = \varepsilon(\alpha) = \varepsilon(\phi(\alpha)) = \varepsilon(\beta).$$

Lema 3. *Sejam G um grupo finito de ordem n, R um anel e ρ a representação regular de g sobre $\mathbb{C}$, temos que se $\alpha \in RG$, então*

$$tr\left(\rho\left(\alpha\right)\right) = \alpha_e n.$$

Demonstração. Sejam G um grupo tal que $|G| = n$, $\alpha = \sum_{g\in G} \alpha_g g$ e $\rho\left(g\right)$ a representação regular de g sobre $\mathbb{C}$, notemos que

$$\rho\left(\alpha\right) = \rho\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g \rho\left(g\right).$$

Assim,

$$tr\left(\rho\left(\alpha\right)\right) = tr\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g tr\left(\rho\left(g\right)\right),$$

como $tr\left(\rho(g)\right) = 0$ para todo $g \neq e \in G$ e $tr\left(\rho(e)\right) = n$ pela Proposição 14, obtemos que

$$tr\left(\rho\left(\alpha\right)\right) = \alpha_e n.$$

□

Lema 4. *Seja G um grupo finito de ordem n, Se $\alpha \in \mathbb{Z}G$ é um elemento invertível de ordem finita tal que $\alpha_e \neq 0$, então $\alpha_e = \pm 1$.*

Demonstração. Sabendo que α é invertível com ordem finita $m \in \mathbb{N}$, pelo Lema 3 temos que $tr(\rho\left(\alpha\right)) = \alpha_e n$.

Notemos também $\left(\rho\left(\alpha\right)\right)^m = \rho\left(\alpha^m\right) = \rho\left(e\right) = I$. Considerando que na representação de grupos os autovalores coincidem com as n-ésimas raízes da unidade, temos

$$D = \begin{pmatrix} \xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & \xi_n \end{pmatrix}.$$

Desse modo, observemos que

$$I = \rho\left(\alpha\right)^m = \left(PDP^{-1}\right)^m = PD^mP^{-1},$$

portanto,

$$PD^mP^{-1} = I \Rightarrow D^m = P^{-1}IP \Rightarrow D^m = I,$$

ou seja, $\xi_k^m = 1$ para todo $k = 1, 2, \cdots, n$.

Analisando o traço da matriz $\rho(\alpha)$ e aplicando o Lema 3, obtemos que

$$tr(\rho(\alpha)) = \sum_{k=1}^{n}\xi_k \Rightarrow \alpha_e n = \sum_{k=1}^{n}\xi_k \Rightarrow |\alpha_e n| = \left|\sum_{k=1}^{n}\xi_k\right| \leq \sum_{k=1}^{n}|\xi_k|, \tag{3.1}$$

como $|\xi_k| = \left|cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)\right| = \sqrt{cos^2\left(\frac{2k\pi}{n}\right) + sen^2\left(\frac{2k\pi}{n}\right)} = 1,$

temos que

$$|\alpha_e| n \leq n \Rightarrow |\alpha_e| \leq 1 \Rightarrow \alpha_e = \pm 1. \tag{3.2}$$

Assim, decorrente do fato de $\alpha_e \in \mathbb{Z}$, concluímos que $\alpha_e = \pm 1$, acarretando que necessariamente

$$\left|\sum_{k=1}^{n}\xi_k\right| = \sum_{k=1}^{n}|\xi_k|. \tag{3.3}$$

Assim, podemos concluir que $\xi_1 = \xi_2 = \ldots = \xi_n$. De fato, por indução, para n=2 notemos que

$$\left|\sum_{k=1}^{2}\xi_k\right| = |\xi_1 + \xi_2| = \left|cos\left(\frac{2\pi}{2}\right) + cos\left(\frac{4\pi}{2}\right) + i\left(sen\left(\frac{2\pi}{2}\right) + sen\left(\frac{4\pi}{2}\right)\right)\right| = |0| = 0,$$

mas, pela Equação 3.3, temos que

$$\left|\sum_{k=1}^{2}\xi_k\right| = 0 = 2,$$

logo obtemos uma contradição, assim para $n = 2$ temos que $\xi_1 = \xi_2$. Daí, consideraremos que para $n - 1$ temos que as raízes coincidem.

Suponhamos que para algum ξ_j tem-se $\xi_j \neq \xi_k$, em que $\xi_1 = \cdots = \xi_k = \xi_{j-1} = \xi_{j+1} = \cdots = \xi_n$. Então

$$\begin{aligned}
&\left|\sum_{k=1}^{n}\xi_k\right| = |(n-1)\xi_k + \xi_j| \\
&= \left|(n-1)cos\left(\frac{2k\pi}{n}\right) + cos\left(\frac{2j\pi}{n}\right) + i\left((n-1)sen\left(\frac{2k\pi}{n}\right) + sen\left(\frac{2j\pi}{n}\right)\right)\right| \\
&= \sqrt{(n-1)^2 + 2(n-1)\left(cos\left(\frac{2k\pi}{n}\right)cos\left(\frac{2j\pi}{n}\right) + sen\left(\frac{2k\pi}{n}\right)sen\left(\frac{2j\pi}{n}\right)\right) + 1} \\
&= \sqrt{(n-1)^2 + 2(n-1)cos\left(\frac{2k\pi}{n} - \frac{2j\pi}{n}\right) + 1}
\end{aligned}$$

Como $\left|\sum_{i=1}^{n}\xi_i\right| = n$ temos que

$$\sqrt{(n-1)^2 + 2(n-1)cos\left(\frac{2k\pi}{n} - \frac{2j\pi}{n}\right) + 1} = n \Rightarrow$$
$$(n-1)^2 + 2(n-1)cos\left(\frac{2k\pi}{n} - \frac{2j\pi}{n}\right) + 1 = n^2 \Rightarrow$$
$$n^2 - 2n + 1 + 2(n-1)cos\left(\frac{(k-j)2\pi}{n}\right) + 1 = n^2 \Rightarrow$$
$$cos\left(\frac{(k-j)2\pi}{n}\right) = 1 \Rightarrow k = j.$$

Logo $\xi_j = \xi_k$, ou seja, $\xi_1 = \xi_2 = \cdots = \xi_k = \xi_j = \cdots = \xi_n$, assim, pelas Equações 3.1 3.2 e 3.3, obtemos que

$$n\,|\alpha_e| = \sum_{k=1}^{n} |\xi_k| = n\,|\xi_1| \Rightarrow |\alpha_e| = |\xi_1| = 1 \Rightarrow \alpha_e = \xi_1 = \pm 1,$$

daí,

$$\rho(\alpha) = PDP^{-1} = P(\pm I)P^{-1} = \pm I,$$

acarretando que $\alpha = \pm e$.

□

Teorema 10. *Se G é um grupo abeliano finito, então o grupo dos elementos invertíveis de $\mathbb{Z}G$ é igual a $\pm G$.*

Demonstração. Pelo Lema 4, temos que os escalares dos elementos invertíveis são ± 1, assim o grupo dos elementos invertíveis é $\pm G$. □

Teorema 11. *Sejam G um grupo finito abeliano e H um grupo qualquer, se $\mathbb{Z}G$ é isomorfo à $\mathbb{Z}H$, então G é isomorfo à H.*

Demonstração. Primeiramente, notemos que se G é abeliano, obtemos que $\mathbb{Z}G$ é comutativo, assim decorrente do isomorfismo, concluímos que $\mathbb{Z}H$ também o é. Decorre da Observação 6 que H é abeliano.

Pela Proposição 16, existe um isomorfismo normalizado ϕ em que, para cada elemento $g \in G$, temos que $\phi(g)$ é invertível normalizado de ordem finita de $\mathbb{Z}H$. Assim, pelo Teorema 10, temos que $\phi(g) \in \pm H$, porém como ϕ é um isomorfismo normalizado, isto é, $\varepsilon(\phi(g)) = 1$, temos que $\phi(g) \in H$, assim $\phi(G) \subset H$.

Por sua vez, como $\mathbb{Z}G$ é um módulo livre de posto |G| e $\mathbb{Z}H$ é um módulo livre de posto |H|, pelo Teorema 8, obtemos

$$|G| = |H|\,.$$

Daí, concluímos que $\phi(G) = H$ e restringindo o domínio de ϕ a G obtemos um isomorfismo entre G e H.

□

4 Conclusão

De acordo com Francisco César Polcino Milies[1] a teoria dos anéis de grupo é um local de encontro de múltiplas teorias algébricas, naturalmente abordando a teoria de anel juntamente com a teoria de grupo, estruturas da Álgebra Abstrata, além de ter aplicação na representação de grupo. Como os anéis de grupo sobre os inteiros constituem um dos focos de particular atenção para os pesquisadores da área, a teoria algébrica de números também desempenha um papel fundamental no desenvolvimento do assunto. Finalmente, cabe observar que eles têm também um papel importante em outros ramos da matemática, como a álgebra homológica, a topologia algébrica e a K-teoria e que, nestes últimos anos, os anéis de grupo vêm sendo aplicados na teoria dos códigos corretores de erros, que são amplamente usados em transmissões digitais, permitindo a criação de novos códigos, ao mesmo tempo eficientes e confiáveis.

Desta forma, neste projeto buscamos o embasamento teórico e os mecanismos necessários e possíveis para provar o Problema do Isomorfismos para Anéis de Grupos restringindo ao caso dos grupos finitos abelianos sobre o conjunto do números inteiros com o viés matemático rigoroso dessa teoria à mim, fornecendo-me uma base sólida na área da Álgebra.

Assim, o objeto de estudo deste projeto, os anéis de grupos, propicia-me, uma graduanda em bacharelado em Matemática na UFOP, a oportunidade de consolidar meus aprendizados curriculares em teoria de anéis, teoria de grupos e álgebra linear, além disso, a oportunidade de aprender um pouco sobre a teoria de módulos e álgebras, tópicos não integrantes do currículo do curso de bacharelado em Matemática da UFOP, configurando um diferencial para a minha formação, pois a apresenta uma interessante opção de estudo em um mestrado e/ou doutorado acadêmico em matemática pura.

Vale ressaltar que o problema para o caso geral ainda contínua em aberto, mas alguns casos já foram demonstrados, como para os grupos nilpotentes finitos, grupos metabelianos finitos, grupos simétricos e grupos alternados. Apesar do tema ser considerado recente temos várias pesquisas relevantes na área.

[1] sítio na USP (<https://www.ime.usp.br/~polcino/aneis_grupo/>, acessado em 26/08/2021)

Referências

HEFEZ, A. *Curso de Álgebra volume 1*. 5. ed. Rio de Janeiro/RJ: IMPA, 1993. (Coleção Matemática Universitária). Citado 3 vezes nas páginas 21, 40 e 41.

MILIES, C. P.; SEHGAL, S. K. *An Introduction to Grup Ring*. 1. ed. [S.l.]: KLUWER ACADEMIC PUBLISHERS, 2002. Citado 4 vezes nas páginas 19, 29, 57 e 60.

NICHOLSON, W. K. *Álgebra Linear*. 2. ed. [S.l.]: AMGH Editora Ltda, 2014. Citado na página 49.

YARTEY, J. N. A. *Álgebra II*. 1. ed. Salvador/BA: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017. Citado na página 32.

Anexos

ANEXO A – Determinante e Traço de uma Matriz

Neste anexo estudaremos as matrizes, dando enfoque em dois conceitos: determinante e traço. O determinante será uma importante ferramenta que utilizaremos para determinar se uma matriz é ou não invertível uma vez que iremos trabalhar com grupos de matrizes invertíveis. O traço será utilizado para associarmos uma matriz com seus autovalores, e em especial, matrizes cujos autovalores são raízes da unidade.

A.1 Determinante

Definição 42. *Dizemos que A é uma matriz sobre um anel comutativo R se for uma tabela retangular composta por elementos de R, estes elementos são chamados de entradas da matriz A. Podemos denotar A como*

$$A = [a_{ij}]_{m\times n} \text{ ou } A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Dizemos que a matriz A tem ordem m por n, se a matriz tem m linhas e n colunas, caso o número de linhas coincida com o de colunas, por exemplo n, dizemos que A tem ordem n e a chamamos de *matriz quadrada*. Além disso, considerando uma matriz quadrada de ordem n, chamamos as entradas da forma a_{ii} com $i = 1, 2, \cdots, n$ de *diagonal principal*. Assim, todas as entradas abaixo da diagonal principal são nulas(respectivamente, todas as entradas acima) nomeamos a matriz como *triangular superior (respectivamente, triangular inferior)*. Por sua vez, se as únicas entradas não nulas de uma matriz quadrada A são as da diagonal principal, chamamos A de *matriz diagonal*. Podemos destacar a matriz diagonal com a diagonal principal preenchida com 1_R[1], denominada como a matriz identidade denotada por Id.

Sejam $A = [a_{ij}]_{m\times n}$ e $B = [b_{ij}]_{m\times n}$ matrizes de mesma ordem, podemos definir a operação soma:

$$A + B = [a_{ij} + b_{ij}]_{m\times n}.$$

Ainda nesse sentido, se $A = [a_{ij}]_{m\times n}$ e $B = [a_{ij}]_{n\times p}$ o produto entre duas matrizes se dá

[1] iremos denotar ao longo desse anexo 1_R como 1.

$$A \cdot B = D \text{ com } D = [d_{ij}]_{m\times p} \text{ em que } d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Definição 43. *Sejam A e B matrizes. Uma matriz A é invertível se existe uma matriz, denotada por A^{-1}, em que*

$$A \cdot A^{-1} = A^{-1} \cdot A = Id.$$

Além disso, dizemos que A é semelhante à B se existe uma matriz P invertível tal que

$$A = PBP^{-1}.$$

Sejam A uma matriz quadrada de ordem n sobre um anel comutativo, $A = [a_{ij}]$, e A_{ij} a submatriz de ordem $n-1$ obtida a partir de A pela exclusão da i-ésima linha e a j-ésima coluna da matriz A. Definimos o *cofator* da entrada a_{ij} por $\Delta_{ij} = (-1)^{i+j}\, det\,(A_{ij})$. Assim, pelo cálculo de determinante via Teorema da expansão por Cofatores[2], para cada $i \in 1, ..., n$ fixado, obtemos que

$$det\,(A) = \sum_{j=1}^{n} a_{ij}\Delta_{ij}$$

e cada $j \in 1, ..., n$ fixado,

$$det\,(A) = \sum_{i=1}^{n} a_{ij}\Delta_{ij}.$$

Desse modo, basta escolhermos um i ou um j conveniente para efetuarmos a expansão por cofatores da matriz A, permitindo assim, trocar o cálculo do determinante de uma matriz de ordem n por uma soma ponderada de determinantes de matrizes de ordem $(n-1)$, e mais ainda, esse processo pode ser aplicado sucessivamente até que se tenha determinantes de matrizes 3×3, caso em que podemos aplicar a regra de Sarrus.

Exemplo 19. *Consideraremos* $A = \begin{pmatrix} 2 & 3 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 1 & 4 & 2 & 0 \\ 1 & 2 & 1 & 1 \end{pmatrix}$. *O cálculo do $det\,(A)$ pode ocorrer fixando a segunda linha de A, observemos*

$$det\,(A) = 1\cdot(-1)^4 \cdot det \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} + 1\cdot(-1)^5 \cdot det \begin{pmatrix} 2 & 3 & 2 \\ 1 & 4 & 0 \\ 1 & 2 & 1 \end{pmatrix} + 1\cdot(-1)^6 \cdot det \begin{pmatrix} 2 & 3 & 1 \\ 1 & 4 & 2 \\ 1 & 2 & 1 \end{pmatrix} = 1.$$

Nesse sentido, se A e B são matrizes quadradas de mesma ordem e k um escalar, então podemos enunciar, sem demonstrar, as seguintes propriedades:

[2] Para mais informações consultar [4] página 71.

- $det\,(A) = det\left(A^t\right)$;
- $det\,(A \cdot B) = det\,(A) \cdot det\,(B)$;
- $det\,(k \cdot A) = k \cdot det\,(A)$;
- se A e B são matrizes semelhantes, então $det\,(A) = det\,(B)$; se A possui uma linha ou uma coluna nula temos que $det\,(A) = 0$;
- se A possui duas linhas ou duas colunas coincidentes, então $det\,(A) = 0$;
- se A é uma matriz triangular, então $det\,(A)$ é igual o produto dos elementos da diagonal principal;

  Agora, por sua vez seja B obtida por meio de operações elementares com a matriz A, temos

- se A e B se diferenciam pela troca de posição de duas linhas ou duas colunas, então $det\,(B) = -det\,(A)$;
- se a matriz B é obtida através de A multiplicando-se ou uma linha ou uma coluna por um escalar k„ então $det\,(B) = k \cdot det\,(A)$.

A prova das propriedades citadas acima podem ser vistas ao longo do capítulo 2 em [4].

Proposição 17. *Se M é uma matriz invertível, então $det\,M \neq 0$.*

Demonstração. Se A é uma matriz $n \times n$ invertível, então, por definição, temos que existe A^{-1}, uma matriz $n \times n$, tal que $A \cdot A^{-1} = A^{-1} \cdot A = I_n$, em que I_n é a matriz identidade $n \times n$. Consequentemente, obtemos que $det\left(A \cdot A^{-1}\right) = det\,I_n = 1 \neq 0$. □

Considerando A e B matrizes se $det\,AB \neq 0$ com $det\,B \in R$, para toda matriz quadrada B sobre um domínio de integridade, então $det\,A \neq 0$.

A.2 Traço

Definição 44. *Seja A uma matriz quadrada de ordem n sobre um anel comutativo. Definimos o traço de A como a soma dos elementos da diagonal principal, isto é,*

$$tr\,(A) = \sum_{i=1}^{n} a_{ii}.$$

Proposição 18. *Sejam $A = [a_{ij}]_{n\times n}$, $B = [b_{ij}]_{n\times n}$ matrizes sobre um anel comutativo e k um escalar. Então:*

(i) $tr\,(A+B) = tr\,(A) + tr\,(B)\,;$

(ii) $tr\,(k\cdot A) = k\cdot tr\,(A)\,;$

(iii) $tr\,(A) = tr\,(A)^t\,;$

(iv) $tr\,(AB) = tr\,(BA)\,.$

Demonstração.

i. Por definição temos que $[A+B]_{n\times n} = [a_{ij}+b_{ij}]_{n\times n}$, acarretando que

$$tr\,(A+B) = \sum_{i=1}^{n}(a_{ii}+b_{ii}) = \sum_{i=1}^{n}a_{ii} + \sum_{i=1}^{n}b_{ii} = tr\,(A) + tr\,(B)\,.$$

ii. Como temos que $k\cdot A = [ka_{ij}]_{n\times n}$, então

$$tr\,(k\cdot A) = \sum_{i=1}^{n}(ka_{ii}) = k\sum_{i=1}^{n}a_{ii} = k\cdot tr\,(A)\,.$$

iii. Sabemos, por definição, que $A^t = [a_{ji}]_{n\times n}$, assim é possível notar que se $i=j$, então $a_{ij} = a_{ji}$, implicando que as diagonais principais das matrizes A e A^t coincidem. Portanto, $tr\,(A) = tr\,(A)^t$.

iv. Sejam $AB = [(ab)_{ij}]_{n\times n}$ em que $(ab)_{ij} = \sum_{r=1}^{n}a_{ir}b_{rj}$ e $BA = [(ba)_{rs}]_{n\times n}$ com $(ba)_{rs} = \sum_{i=1}^{n}a_{ri}b_{is}$, então

$$tr\,(AB) = \sum_{i=1}^{n}(ab)_{ii} = \sum_{i=1}^{n}\sum_{r=1}^{n}a_{ir}b_{ri} = \sum_{r=1}^{n}\sum_{i=1}^{n}b_{ri}a_{ir} = \sum_{r=1}^{n}(ba)_{rr} = tr\,(BA).$$

□

Definição 45 (Transformação Linear)**.** *Sejam V_1 e V_2 dois espaços vetoriais sobre um corpo K, dizemos que uma aplicação*

$$T : V_1 \to V_2$$

é uma transformação linear se para todo $a, b \in K$ e $u, v \in V_1$

$$T(au+bv) = aT(u) + bT(v).$$

Quando temos uma transformação linear cujos o domínio e o contra-domínio coincidem a chamamos de *operador linear*. Além disso, toda transformação linear cujos domínio e contra-domínio são espaços vetoriais com dimensão finita pode ser representada por uma matriz.

Assim, consideremos A uma matriz associada a um operador linear sobre um espaço vetorial com dimensão finita, Id o operador identidade e $\lambda_1, \lambda_2, \cdots, \lambda_n$ autovalores de A e $p(x)$ o polinômio característico de A.

Sabendo que o polinômio característico é decomposto em fatores $\lambda_i - x$ sobre $\mathbb{C}$, temos que

$$p(x) = (\lambda_1 - x)\cdots(\lambda_n - x) = (-1)^n x^n + (-1)^{n-1}(\lambda_1 + \lambda_2 + \cdots + \lambda_n) x^{n-1} + \cdots + \lambda_1 \cdots \lambda_n.$$

Considerando $P_{n-2}(x)$ um polinômio de grau igual ou menor à $n-2$ podemos notar que

$$p(x) = (-1)^n x^n + (-1)^{n-1}(\lambda_1 + \lambda_2 + \cdots + \lambda_n) x^{n-1} + P_{n-2}(x). \tag{A.1}$$

Por outro lado, por definição, obtemos que $p(x) = det(A - xId)$, assim

$$p(x) = det \begin{vmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - x & \cdots & a_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - x \end{vmatrix} = (a_{11} - x)\Delta_{11} + \sum_{i=2}^{n} a_{1i}\Delta_{1i}.$$

Notemos que o grau do polinômio $O_{n-2}(x)$ resultante do somatório $\sum_{i=2}^{n} a_{1i}\Delta_{1i}$ é menor que $n-2$, uma vez que ao eliminarmos a i-coluna para calcular Δ_{1i} os termos $(a_{11} - x), (a_{ii} - x)$ são eliminados e não são utilizados no seu cálculo. Por sua vez, foquemos no termo $(a_{11} - x)\Delta_{11}$.

$$\begin{aligned}
&(a_{11} - x)\Delta_{11} = \\
&= (a_{11} - x)[(a_{22} - x)\Delta_{22} + \sum_{i=3}^{n} a_{2i}\Delta_{2i}] = (a_{11} - x)(a_{22} - x)\Delta_{22} + (a_{11} - x)\sum_{i=3}^{n} a_{2i}\Delta_{2i} \\
&= (a_{11} - x)\left((a_{22} - x)\left((a_{33} - x)\Delta_{33} + \sum_{i=4}^{n} a_{3i}\Delta_{3i}\right)\right) + (a_{11} - x)\sum_{i=3}^{n} a_{2i}\Delta_{2i} \\
&= (a_{11} - x)(a_{22} - x)(a_{33} - x)\Delta_{33} + (a_{11} - x)(a_{22} - x)\sum_{i=4}^{n} a_{3i}\Delta_{3i} + (a_{11} - x)\sum_{i=3}^{n} a_{2i}\Delta_{2i}.
\end{aligned}$$

Realizando o processo recursivamente, obtemos que $(a_{11} - x)\Delta_{11}$ é igual à

$$(a_{11} - x)(a_{22} - x)\cdots\left(a_{(n-2)(n-2)} - x\right)\Delta_{(n-2)(n-2)} + \sum_{k=1}^{n-2}\left(\prod_{j=1}^{k}(a_{jj} - x)\sum_{i=k+2}^{n} a_{(k+1)i}\Delta_{(k+1)i}\right)$$

$$= \sum_{k=1}^{n-2}\left(\prod_{j=1}^{k}(a_{jj} - x)\sum_{i=k+2}^{n} a_{(k+1)i}\Delta_{(k+1)i}\right) + \prod_{j=1}^{n}(a_{jj} - x) - a_{(n-1)n}a_{n(n-1)}\prod_{j=1}^{n-2}(a_{jj} - x).$$

Em particular, ao analisarmos as parcelas acima temos que o grau do polinômio resultante do produtório $\prod_{j=1}^{n-2}(a_{jj}-x)$ é $n-2$. Ainda nesse sentido, o somatório $\sum_{i=k+2}^{n} a_{(k+1)i}\Delta_{(k+1)i}$ tem grau menor ou igual à $n-(k+2)$, enquanto o produtório $\prod_{j=1}^{k}(a_{jj}-x)$ possui grau igual à k, acarretando que o somatório $\sum_{k=1}^{n-2}\left(\prod_{j=1}^{k}(a_{jj}-x)\sum_{i=k+2}^{n} a_{(k+1)i}\Delta_{(k+1)i}\right)$ tem grau menor ou igual à $n-2$. Assim, podemos considerar

$$\tilde{O}_{n-2}(x)=\sum_{k=1}^{n-2}\left(\prod_{j=1}^{k}(a_{jj}-x)\sum_{i=k+2}^{n} a_{(k+1)i}\Delta_{(k+1)i}\right)-a_{(n-1)n}a_{n(n-1)}\prod_{j=1}^{n-2}(a_{jj}-x),$$

em que $\tilde{O}_{n-2}(x)$ é m polinômio de grau menor ou igual à $n-2$, logo

$$(a_{11}-x)\,\Delta_{11}=$$

$$=\prod_{j=1}^{n}(a_{jj}-x)+\tilde{O}_{n-2}(x)=(-1)^n x^n+(-1)^{n-1}\left(\sum_{i=1}^{n}a_{ii}\right)x^{n-1}+\tilde{O}_{n-2}(x)$$

$$=(-1)^n x^n+(-1)^{n-1}tr(A)x^{n-1}+\tilde{O}_{n-2}(x).$$

Portanto, temos que o polinômio característico é da forma

$$p(x)=(-1)^n x^n+(-1)^{n-1}tr(A)x^{n-1}+\tilde{O}_{n-2}(x)+O_{n-2}(x). \tag{A.2}$$

Daí, igualando comparando as A.1 e A.2 e relação os coeficientes de x^{n-1} concluímos que

$$tr\,(A)=\sum_{i=2}^{n}\lambda_i,$$

o que pode ser enunciado do seguinte modo

Teorema 12. *Sejam A uma matriz de ordem n e $\lambda_1,\lambda_2,\cdots,\lambda_n$ seus autovalores, então*

$$tr\,(A)=\sum_{i=2}^{n}\lambda_i.$$