UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

GESSICA SANTOS SOUZA

TEOREMA FUNDAMENTAL DOS HOMOMORFISMOS DE ANÉIS

PATOS – PB
2022

GESSICA SANTOS SOUZA

TEOREMA FUNDAMENTAL DOS HOMOMORFISMOS DE ANÉIS

Trabalho de conclusão do curso (monografia) de Licenciatura Plena em Matemática – CCEA da Universidade Estadual da Paraíba como requisito parcial para obtenção do título de Licenciada em Matemática.

Área de concentração: Matemática

Orientador: Prof. Me. José Ginaldo de Souza Farias

PATOS – PB
2022

S729t Souza, Gessica Santos.
Teorema fundamental dos homomorfismos de anéis [manuscrito] / Gessica Santos Souza. - 2022.
61 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2022.
"Orientação : Prof. Me. José Ginaldo de Souza Farias , Coordenação do Curso de Ciências Exatas - CCEA."

1. Teoria dos anéis. 2. Homomorfismo de anéis. 3. Anéis quocientes. I. Título

21. ed. CDD 512.5

Elaborada por Edson M. A. Monteiro - CRB - CRB 15/743 BSC7/UEPB

GESSICA SANTOS SOUZA

TEOREMA FUNDAMENTAL DOS HOMOMORFISMOS DE ANÉIS

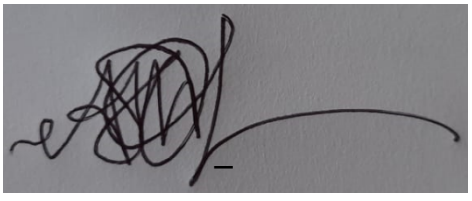
Trabalho de Conclusão de Curso (Monografia) apresentado ao Departamento do Curso de Matemática da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Licenciado em Matemática.

Área de concentração: Àlgebra

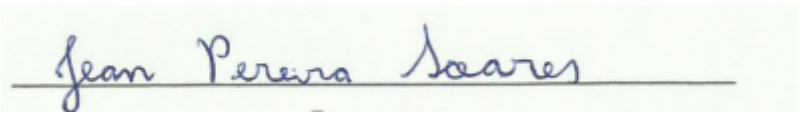
Aprovada em: _14_/_12_/_2022_.

BANCA EXAMINADORA

Prof. Me. José Ginaldo de Souza Farias.(Orientador)
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Arlandson Matheus Silva Oliveira (UEPB)
Examinador



Prof. Jean Pereira Soares (UEPB)
Examinador

AGRADECIMENTOS

Sem o auxílio e a proteção divina nada seria possível em minha vida, por isso, venho primeiramente agradecer a Deus.

A meus pais, Antônio Lisboa e Maria do Socorro e a meu irmão Alexson agradeço o encorajamento e suporte durante toda a jornada acadêmica, sem eles, todo o esforço seria insignificante para mim.

Agradeço também a todos os meus colegas de graduação, todos, de alguma forma, colaboraram com minha formação. Nos momentos mais difíceis, não foram poucos, nos apoiávamos e juntos encontrávamos soluções que pareciam muito distantes.

Agradeço imensamente aos professores que contribuíram com a minha formação acadêmica, especialmente, meu orientador, o Professor Me. José Ginaldo de Souza Farias, por todo compartilhamento de conhecimento que foi preciso para a realização desse trabalho.

Além disso, tenho a mais profunda gratidão aos professores Dr. Arlandson Matheus Silva Oliveira e Jean Pereira Soares que aceitaram fazer parte da banca examinadora deste trabalho.

"A natureza do objeto matemático define-se no tempo e no espaço"

(Ledo Vaccaro)

SUMÁRIO

1. INTRODUÇÃO 7

2. ANÉIS 9

2.1. Definição e exemplos 9

2.2. Propriedades elementares de um anel 12

2.2.1. Característica de um anel 17

2.3. Subanéis 18

2.4. Domínios 21

2.5. Corpos 24

2.6. Homomorfismo de anéis 28

2.6.1 Núcleo de um homomorfismo 31

2.6.2 Isomorfismo de anéis 33

2.7 Ideais 34

2.7.1 Domínios de ideais principais 36

2.7.2 Operações com ideais 37

2.7.3 Ideais primos e maximais 41

2.8. Anéis quocientes 44

3. TEOREMA FUNDAMENTAL DOS HOMOMORFISMOS PARA ANÉIS 49

4. CONCLUSÃO 59

REFERÊNCIAS

RESUMO

Este trabalho objetiva realizar a demonstração do teorema fundamental dos homomorfismos para anéis, teorema esse que, relaciona um tipo específico de homomorfismo (isomorfismo) com o com núcleo de uma função homomórfica, ideais e anéis quocientes, matematicamente nos deparamos com: Se $f : A \to B$ um homomorfismo de anéis. Então, $A/\ker(f) \simeq Im\,(f)$. Além da prova do teorema, serão ilustrados resultados e aplicações inerentes a ele. Dessa forma, para ter um entendimento mais claro, foi feito um estudo aprofundado referente aos conceitos básicos da teoria dos anéis, destacando os principais tópicos desse trabalho, a noção de homomorfismos, ideais e anéis quocientes.

Palavras-chave: Teoria dos anéis. Homomorfismo de anéis. Ideais. Anéis quocientes.

ABSTRACT

This paper aims to demonstrate the fundamental theorem of homomorphisms for rings, a theorem that relates a specific type of homomorphism (isomorphism) to the kernel of a homomorphic function, ideals and quotient rings, mathematically we have: if $f : A \to B$ a ring homomorphism. Then, $A/\ker(f) \simeq Im\ (f)$. Besides the proof of the theorem, results and applications inherent to it will be illustrated. Thus, to have a clearer understanding, a thorough study was made concerning the basic concepts of the theory of rings, highlighting the main topics of this work, the notion of homomorphisms, ideals and quotient rings.

Keywords: Ring theory. Homomorphism of rings. Ideals. Quotient rings.

1. INTRODUÇÃO

Historicamente a álgebra abstrata é marcada pelas diversas e distintas personalidades que contribuíram para a sua construção, destacaremos nomes como Adolf Fraenkel (1891 – 1965), Richard Dedekind (1831 – 1916), David Hilbert (1862 – 1945) e Emmy Noether (1882 – 1935). O conceito de anel já era conhecido e utilizado por volta do século XIX, nos trabalhos de Teoria dos números de Richard Dedekind e Leopoldo Kroneker (1823 – 1891), no entanto o termo utilizado para esse conceito era *ordem*. Em 1897 o termo *anel* foi introduzido pelo matemático David Hilbert, mas ainda era utilizado na de teoria dos números.

No ano de 1914 surgiu a primeira definição abstrata de anel pelo matemático Adolf Fraenkel num artigo denominado *On zero divisors and the decomposition of rings*, no *jour. fur die Reine und Angew. Math*, além da abrangência do conceito de anel, ele dá vários exemplos, como inteiros módulos n, sistemas de números hipercomplexos, matrizes e inteiros p-àdicos.

Segundo Milies, a definição de anel segundo Adolf é muito semelhante a atual, ele considera um sistema com duas operações, chamado soma e produto, e estipula que a soma entre os elementos seja associativa, que exista um elemento neutro e um elemento simétrico nesse sistema, em relação ao produto deve haver a associatividade e distributividade em relação à soma, além disso, ele inclui a existência de um elemento unidade. A comutatividade da soma não está dentre os axiomas, ela é demonstrada a partir deles.

Outro nome que dedicou sua vida à construção da álgebra foi a alemã Amalie Emmy Noether foi umas das principais responsáveis pelo avanço da teoria dos anéis, em seu artigo intitulado *Ideal Theory in Rings* de 1921 Noether prova que cada ideal em um anel é finitamente gerado se, e somente se, a condição de inclusão em cadeia ascendente é satisfeita, anos depois, em 1927, no artigo *Abstract Study of Ideal Theory in Algebraic Number and Function filds* ela caracteriza os anéis comutativos nos quais todo ideal é um produto único de ideais primos. Tais anéis são conhecidos atualmente como Domínios de Dedekind, nos dois artigos Noether traz uma generalização dos trabalhos que Dedekind realizou para o anel dos números algébricos.

O desenvolvimento desse trabalho se encontra nos capítulos 2 e 3. No segundo capítulo deste trabalho será mostrado a construção da estrutura algébrica munida de duas

operações (adição e multiplicação) que obedece a uma série de propriedades, definiremos e mostraremos exemplos dessa estrutura, assim como propriedades fundamentais para caracterizá-las. Abordaremos os tipos mais importantes de anéis comutativos com unidade e o que diferencia cada um deles, como domínios de integridade, corpos e anéis quocientes.

Veremos também estruturas familiares que são exemplos clássicos de anéis, como o conjunto dos números inteiros, racionais, reais e complexos além de conhecer a natureza de anéis contidos em outros anéis (subanel). Esse último conceito é de suma importância para esse trabalho, pois a partir dele iremos conhecer a definição de ideal, subanel de extrema importância para o desenvolvimento do terceiro capítulo.

No terceiro capítulo vamos estudar mais profundamente as funções que relacionam os anéis, tendo como foco principal a demonstração do Teorema Fundamental dos Homomorfismos de anéis, esse teorema é responsável por garantir que existe um isomorfismo entre um anel quocientado por um núcleo de uma função homomórfica e a imagem dessa função. Esse resultado relaciona tipos de anéis e subanéis de extrema relevância no estudo da álgebra, além de gerar resultados significativos. Por fim, será mostrado as considerações finais desse trabalho.

2. ANÉIS

No estudo da álgebra abstrata, comumente nos deparamos com determinadas estruturas dotadas de características que despertam a curiosidade e o interesse de muitos matemáticos no decorrer dos anos. Pode-se citar como exemplo o Anel, estrutura que é munida de duas operações específicas (não necessariamente usuais) onde obedecem a uma série de propriedades elementares. Nesse capítulo será mostrado diversos tipos de anéis e alguns cenários encontrados nessas estruturas, tais como, teoremas, proposições e corolários.

2.1. Definição e exemplos

Definição 2.1 *Um conjunto A, não vazio, munido de duas operações, adição* (+) *e multiplicação* ($\cdot$) *chamam-se Anel* $(A, +, \cdot)$ *quando:*

I. $a + (b + c) = (a + b) + c, \ \forall\, a, b, c \in A$ *(Associatividade da adição);*

II. $a + b = b + a, \ \forall\, a, b \in A$ *(Comutatividade da adição);*

III. $\exists\, O_A \in A\ ;\ O_A + a = a, \ \forall\, a \in A$ *(Elemento neutro da adição);*

IV. $\exists\, (-a) \in A\ ; (-a) + a = O_A, \ \forall\, a \in A$ *(Elemento simétrico ou inverso aditivo);*

V. $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall\, a, b, c \in A$ *(Associatividade da multiplicação);*

VI. $a \cdot (b + c) = a \cdot b + a \cdot c = a \cdot c + a \cdot b, \ \forall\, a, b, c \in A$ *(Distributividade da multiplicação em relação à adição).*

No decorrer desse trabalho, ao se referir a um anel $(A, +, \cdot)$ este será indicado apenas por A, desde que não haja nenhuma dúvida inerente as operações nele contidas. Além disso, muitas vezes o produto $a \cdot b \in A$ será representado por ab. Quando não houver dúvidas em relação ao elemento neutro da adição do anel A, este será indicado por 0_A ou apenas por 0, de modo que $a + (-a) = 0_A$. Ademais, dados $a, b \in A$ a soma $a + (-b)$ será representada por $a - b$, ou seja, $a + (-b) = a - b$.

No estudo de teoria dos anéis é possível observar algumas estruturas com características que definem sua identidade, temos:

Definição 2.2 *Um anel* $(A, +, \cdot)$ *diz-se* ***comutativo*** *se a multiplicação em A for comutativa, ou seja,*

$$a \cdot b = b \cdot a, \ \ \forall\, a, b \in A;$$

Definição 2.3 *Um anel* (A, +, ·) *chama-se* ***anel com unidade*** *quando existe um elemento neutro da multiplicação em A, isto é,*

$$\exists\, e \ \in A\,; ae = ea = a, \ \ \forall\, a \ \in A$$

O elemento *e* é chamado unidade do anel (1_A). Em alguns casos a unidade do anel é representada por 1, no entanto, deve-se ficar atento que essa representação não significa, a princípio, o número inteiro 1.

Exemplo 2.1 Para exemplificar estruturas algébricas que são anéis comutativos com unidade, pode-se tomar os conjuntos dos números inteiros $(\mathbb{Z}, +, \cdot)$, racionais $(\mathbb{Q}, +, \cdot)$, reais $(\mathbb{R}, +, \cdot)$e complexos $(\mathbb{C}, +, \cdot)$, munidos das operações de soma e produto usuais. Pode-se afirmar que o número inteiro 1 é a unidade destes anéis.

Exemplo 2.2 Dada a estrutura algébrica $A = \{0_A\}$, observe que:

$$0_A + 0_A = 0_A \qquad \text{e} \qquad 0_A \cdot 0_A = 0_A$$

Percebe-se que 0_A além de ser o elemento neutro da adição é também a unidade do anel *A*, ou seja, $1_A = 0_A$. Esse é o único caso em que isso ocorre. A estrutura $A = \{0_A\}$ é chamada *anel trivial.*

Exemplo 2.3 O conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, sendo $n \in \mathbb{N}$, com suas operações de adição e multiplicação é um anel comutativo com unidade $\bar{1}$.

Exemplo 2.4 Seja $\mathcal{F} = \mathbb{R}^{\mathbb{R}}$ o conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$. Onde para cada $x \in \mathbb{R}$ tem-se:

$$(f + g)(x) = f(x) + \ g(x) \qquad e \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

É um anel comutativo com unidade. Veja que,

I. A adição é associativa:

$$\begin{aligned}[f + (g + h)](x) &= f(x) + (g + h)(x) \\ &= f(x) + \big(g(x) + h(x)\big) \\ &= \big(f(x) + g(x)\big) + \ h(x) \\ &= (f + g)(x) + g(x) \\ &= [(f + g) + h)](x). \quad \forall\, f, g, h \ \in \mathcal{F}\end{aligned}$$

II. A adição é claramente comutativa, pois $\mathcal{F}$ tem domínio e imagem nos reais.

III. A adição possui elemento neutro, nesse caso, será a função nula:

$$(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x). \forall f \in \mathcal{F}$$

Com isso, $0_{\mathcal{F}} = 0$.

IV. A adição possui elemento oposto:

$$\begin{aligned}\big(f + (-f)\big)(x) = f(x) + \big(-f(x)\big) = f(x) - f(x)\\ = 0. \ \forall f \in \mathcal{F}\end{aligned}$$

Observe que a soma dos elementos opostos é 0, que é o zero do anel $\mathcal{F}$ logo, $\big(-f(x)\big)$ é o elemento simétrico de $\mathcal{F} = \mathbb{R}^{\mathbb{R}}$.

V. A multiplicação é associativa:

$$\begin{aligned}[f \cdot (g \cdot h)](x) &= f(x) \cdot (g \cdot h)(x)\\ &= f(x) \cdot \big(g(x) \cdot h(x)\big)\\ &= \big(f(x) \cdot g(x)\big) \cdot h(x)\\ &= (f \cdot g)(x) \cdot g(x)\\ &= [(f \cdot g) \cdot h)](x). \quad \forall f, g, h \in \mathcal{F}\end{aligned}$$

VI. A multiplicação é distributiva em relação à adição:

$$\begin{aligned}[f \cdot (g + h)](x) &= f(x) \cdot (g + h)(x)\\ &= f(x) \cdot [g(x) + h(x)]\\ &= [f(x) \cdot g(x)] + [f(x) \cdot h(x)]\\ &= (f \cdot g)(x) + (f \cdot h)(x)\\ &= [(f \cdot g) + (f \cdot h)](x). \quad \forall f, g, h \in \mathcal{F}\end{aligned}$$

VII. A multiplicação em $\mathcal{F}$ é claramente comutativa, pelo mesmo motivo que a adição.

VIII. A unidade do anel $\mathcal{F} = \mathbb{R}^{\mathbb{R}}$, neste caso será a função constante $1(1_{\mathcal{F}} = 1)$, visto que $1_{\mathcal{F}}(x) \in \mathcal{F}$ e $1_{\mathcal{F}}(x) = 1 \ \forall x \in \mathbb{R}$:

$$(f \cdot 1_{\mathcal{F}})(x) = f(x) \cdot 1_{\mathcal{F}}(x) = f(x) \cdot 1 = f(x)$$

Portanto, $(\mathcal{F}, +, \cdot)$ é um anel comutativo com unidade.

2.2. Propriedades elementares de um anel

Serão mostradas algumas propriedades de um anel A, que são consequências imediatas das propriedades de suas operações, sendo assim, elementares. Essas, auxiliaram no processo de diversas demonstrações no decorrer deste trabalho.

Teorema 2.1 *Seja A um anel. Então, para quaisquer* $a, b \in A$,

(I) $0_A \cdot a = a \cdot 0_A = 0_A$.

(II) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

(III) $(-a) \cdot (-b) = a \cdot b$.

Demonstração: ***(I)*** Sabemos que $0_A + 0_A = 0_A$, com isso, pela distributividade da multiplicação em relação à adição de A, temos

$$0_A \cdot a = (0_A + 0_A) \cdot a = 0_A \cdot a + 0_A \cdot a \tag{1.0}$$

Sabendo que A é um anel, então $-(0_A \cdot a) \in A$ de tal forma que $-(0_A \cdot a) + 0_A \cdot a = 0_A$.
Diante disso, adicionando $-(0_A \cdot a)$ a ambos os membros da igualdade (1.0), temos

$$-(0_A \cdot a) + 0_A \cdot a = -(0_A \cdot a) + 0_A \cdot a + 0_A \cdot a$$

$$0_A = 0_A + 0_A \cdot a$$

$$0_A = 0_A \cdot a$$

Da mesma forma prova-se que $a \cdot 0_A = 0_A$.

(II) Pela propriedade *(I)* temos

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0_A = 0_A \text{ daí,}$$

$$a \cdot (-b) + a \cdot b = 0_A$$

$$a \cdot (-b) = -(a \cdot b) \tag{1.1}$$

Por outro lado,

$$(-a) \cdot b + ab = (-a + a) \cdot b = 0_A \cdot b = 0_A \text{ daí,}$$

$$(-a) \cdot b + ab = 0_A$$

$$(-a)\cdot b = -(ab) \tag{1.2}$$

Com isso, pelas igualdades (1.1) e (1.2) chega-se à conclusão que,

$$a\cdot(-b) = (-a)\cdot b = -(ab)$$

(III) Pela propriedade *(II)* sabe-se que,

$$\begin{aligned}(-a)\cdot(-b) = \big(-(a\cdot b)\big) &= (-a)\cdot(-b) + ((-a)\cdot b)\\ &= (-a)\cdot(-b+b)\\ &= (-a)\cdot 0_A\\ &= 0_A\end{aligned}$$

Logo, é evidente que, $(-a)\cdot(-b) + \big(-(a\cdot b)\big) = 0_A$ e assim, $(-a)\cdot(-b) = a\cdot b$.

Definição 2.4 (Potência de um Anel). *Sejam A um anel e* $n \in \mathbb{N}$ *dado* $a \in A$*, define-se a potência* a^n *da seguinte forma:*

$$a^n = \begin{cases} a & se\ n = 1. \\ a^{n-1}\cdot a & se\ n > 1. \end{cases}$$

Se o anel A tem unidade 1_A*, então define-se* a^n *para* $n \in \mathbb{N}\cup\{0\}$ *por*

$$a^n = \begin{cases} 1_A & se\ n = 1. \\ a^{n-1}\cdot a & se\ n > 1. \end{cases}$$

Pela definição de potência de um anel, valem as seguintes propriedades:

I. $a^n\cdot a^m = a^{n+m}$.
II. $(a^n)^{\,m} = a^{nm}$.

Demonstração (I): Será utilizado indução sobre m:

Para $m = 1$ temos,

$$a^n\cdot a^1 = a^n\cdot a$$

$$= a^{n+1-1} \cdot a = a^{(n+1)-1}a$$

Por definição, temos que

$$a^{(n+1)-1}a = a^{n+1}$$

Agora suponha que a propriedade é válida para $m = k$, logo

$$a^n \cdot a^k = a^{n+k} \text{ (H.I.)}$$

Agora vamos demostrar que a propriedade é válida para $m = k + 1$, temos

$$a^n \cdot a^{k+1}$$

Vamos reescrever a^{k+1} como sendo $a^{(k+1)-1} \cdot a$, com isso,

$$\begin{aligned} a^n \cdot a^{k+1-1} \cdot a &= a^n \cdot a^k \cdot a \\ &= (a^n \cdot a^k) \cdot a \text{ pela (H.I.)}^1, \\ &= a^{n+k} \cdot a \\ &= a^{n+k+1-1} \cdot a \\ &= a^{[n+(k+1)]-1} \cdot a \\ &= a^{n+(k+1)} \end{aligned}$$

Portanto, o resultado é válido para $m + 1$ e consequentemente, $a^n \cdot a^m = a^{n+m}$ para quaisquer $m, n \in \mathbb{N}$.

Demonstração (II): De maneira análoga à (I), também será utilizado indução sobre m:

Para $m = 1$ temos,

$$(a^n)^1$$

vamos reescrever $(a^n)^1$ como sendo $(a^n)^{1-1} \cdot a^n$, isto é,

$$\begin{aligned} (a^n)^1 &= (a^n)^{1-1} \cdot a^n \\ &= (a^n)^0 \cdot a^n \\ &= 1 \cdot a^{n \cdot 1} \end{aligned}$$

[1] (H.I.) significa Hipótese de Indução.

$$= a^{n\cdot 1}$$

Vamos supor que a proposição é válida para $m = k$, com isso temos que,

$$(a^n)^{\,k} = a^{n\cdot k} \text{ (H.I.)}$$

Vamos provar que a proposição é válida para $m = k + 1$, temos,

$$(a^n)^{\,k+1}$$

Se reescrevermos $(a^n)^{\,k+1}$ como sendo $(a^n)^{\,k+1-1} \cdot a^n$ ficaremos com,

$$(a^n)^{\,k+1} = (a^n)^{\,k+1-1} \cdot a^n$$

$$= (a^n)^{\,k+0} \cdot a^n$$

$$= (a^n)^{\,k} \cdot a^n, \text{ pela (H.I.) temos,}$$

$$= a^{n\cdot k} \cdot a^n, \text{ por } \textit{(I)} \text{ têm-se que,}$$

$$= a^{n\cdot k+n}$$

$$= a^{n(k+1)}$$

Portanto, o resultado é válido para $m + 1$ e por conseguinte, $(a^n)^{\,m} = a^{nm}$ para quaisquer $m, n \in \mathbb{N}$.

É de fácil entendimento que no anel dos números inteiros $(\mathbb{Z}, +, \cdot)$,

$$(a + b)^2 = a^2 + 2ab + b^2, \quad \forall\, a, b \in \mathbb{Z}. \tag{1.3}$$

Isto é válido pelo fato de $\mathbb{Z}$ ser um anel comutativo. No entanto, em um anel A não comutativo, com $a, b \in A$,

$$(a + b)^2 = (a + b) \cdot (a + b)$$

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

$$= a^2 + ab + ba + b^2,$$

Ou seja,

$$(a + b)^2 = a^2 + ab + ba + b^2 \tag{1.4}$$

A igualdades (1.3) e (1.4) são formas simples e análogas de calcular $(a + b)^2$, porém esta última é para um anel não comutativo.

Exemplo 2.5 Seja A um anel tal que $x^2 = x$ para todo $x \in A$, vamos mostrar que A é comutativo.

Solução: Sabendo que para cada $x \in A$, a soma $x + x$ também pertence a A, logo, por hipótese, $x + x = (x + x)^2$, veja que,

$$\begin{aligned} x + x &= (x + x)^2 \\ &= (x + x) \cdot (x + x) \\ &= x^2 + x^2 + x^2 + x^2 \\ &= x + x + x + x, \end{aligned}$$

então

$$x + x = x + x + x + x$$

Agora somando $-x \in A$ duas vezes a ambos os lados da igualdade temos,

$$x + (-x) + x + (-x) = (-x) + x + (-x) + x + x + x$$

$$0_A = x + x$$

Ou seja,

$$x = -x \tag{1.5}$$

Agora vamos considerar x e y elementos quaisquer do anel A. Como $x + y \in A$, temos,

$$\begin{aligned} x + y &= (x + y)^2 \\ &= (x + y) \cdot (x + y) \\ &= x \cdot (x + y) + y \cdot (x + y) \\ &= x^2 + xy + yx + y^2 \end{aligned}$$

Onde temos

$$x + y = x^2 + xy + yx + y^2 \tag{1.6}$$

Somando $-x, -y \in A$ em ambos os lados da igualdade (1.6), teremos,

$$(-x) + (-y) + x + y = (-x) + (-y) + x^2 + xy + yx + y^2$$

$$0_A = xy + yx$$

Ou seja,

$$xy = -yx = yx$$

De acordo com (1.5). Portanto, $xy = yx$, isto é A é um anel comutativo.

Se $(A, +, \cdot)$ é um anel, e dados $n, m \in \mathbb{Z}$ e $a, b \in A$, valem as seguintes propriedades:

a. $(m + n) \cdot a = m \cdot a + n \cdot a$.
b. $m \cdot (n \cdot a) = (mn) \cdot a$.
c. $(m \cdot a) \cdot (n \cdot b) = (mn) \cdot (ab)$.
d. $(-m) \cdot a = m \cdot (-a) = -(m \cdot a)$.

2.2.1. Característica de um anel

Será mostrado um tipo de propriedade algébrica que constata um tipo de comportamento da unidade de um anel com relação a soma do mesmo anel.

Definição 2.5 *Seja A um anel. Se existe* $n \in \mathbb{N}$ *tal que*

$$n \cdot a = 0_A, \quad \forall\, a \in A,$$

Então o menor número natural[2] *que satisfaz essa condição é chamado* ***característica*** *de A. Se não existir tal número que satisfaça a igualdade acima, então diz-se que A é de característica zero.*

Indica-se a característica m de um anel A por $car(A)$,

$$m = car(A)$$

Exemplo 2.6 Considere A como sendo qualquer um dos seguintes anéis: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$. Então a $car(A) = 0$. Veja que se considerarmos $a = 1$, temos

$$n \cdot 1 = n \neq 0 \quad \forall\, n \in \mathbb{N}$$

Isto significa que não existe $m \in \mathbb{N}$ tal que

[2] Tal número existe, em conformidade com o Princípio da Boa Ordenação (PBO).

$$m \cdot a = 0_A, \quad \forall\, a \in A.$$

Pode ser um tanto quanto trabalhoso determinar a característica de um anel A, a menos que a $car(A) = 0$, já que seria necessário examinar todo elemento $a \in A$. No entanto, o próximo teorema irá mostrar que se A tem unidade, então basta examinar apenas o caso em que $a = 1_A$.

Teorema 2.2 *Seja A um anel com unidade* 1_A. *Se* $n \cdot 1_A \neq 0_A$ *para todo* $n \in \mathbb{N}$, *então A tem característica zero. Além disso, se* $n \cdot 1_A = 0_A$ *para algum* $n \in \mathbb{N}$, *então o menor número* $m \in \mathbb{N}$ *satisfazendo a condição*

$$m \cdot 1 = 0_A$$

é a característica de A.

Demonstração: Suponha que $n \cdot 1_A \neq 0_A$ para todo $n \in \mathbb{N}$. Logo, não podemos ter $n \cdot a = 0_A$ para todo $a \in A$. Assim, por definição $car(A) = 0$. Agora, se $n \cdot 1_A = 0_A$ para algum $n \in \mathbb{N}$, então, para qualquer $a \in A$, temos

$$\begin{aligned} n \cdot a &= a + a + \cdots + a \qquad (n \text{ parcelas}) \\ &= a \cdot 1_A + a \cdot 1_A + \cdots + a \cdot 1_A \\ &= a \cdot (1_A + 1_A + \cdots + 1_A) \\ &= a \cdot (n \cdot 1_A) \\ &= a \cdot 0_A \\ &= 0_A. \end{aligned}$$

O que conclui a demonstração.

2.3. Subanéis

Estudaremos agora o conceito de subanel, estrutura algébrica muito específica contida em um anel que, por sua vez, herda as características do conjunto que o contém, sendo assim, será possível gerar novos anéis a partir de anéis já conhecidos.

Definição 2.6 *Sejam A um anel e B um subconjunto não vazio de A. Diz-se que B é subanel de A quando B juntamente com as operações de adição e multiplicação induzidas de A, é também um anel.*

Exemplo 2.7 Para um anel qualquer A, $B_1 = \{0_A\}$ e $B_2 = A$ são claramente subanéis de A. São **os subanéis triviais**.

Exemplo 2.8 Se $n \in \mathbb{Z}$ é um subanel de $\mathbb{Z}$, que por sua vez é um subanel de $\mathbb{Q}$. De modo geral, temos a seguinte cadeia de subanéis

$$n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Exemplo 2.9 Dado $n \in \mathbb{N}$, segue que $M_n(\mathbb{Z})$ é um subanel de $M_n(\mathbb{Q})$. Temos também a cadeia de subanéis

$$M_n(\mathbb{Z}) \subset M_n(\mathbb{Q}) \subset M_n(\mathbb{R}) \subset M_n(\mathbb{C}).$$

Até agora foi mostrado alguns exemplos de subanéis, no entanto, antes de dar continuidade veremos um resultado que estabelece um critério que verifica quando um subconjunto não vazio B é um subanel de um anel A.

Teorema 2.3 *Sejam A um anel e B um subconjunto não vazio de A. Então, B é um subanel de A se, e somente se,*

$$a - b \in B \quad e \quad ab \in B$$

para quaisquer $a, b \in B$.

Demonstração: ($\Longrightarrow$) Vamos supor que B é um subanel de A, com isso, $(B, +)$ é um grupo abeliano e, por isso, $a - b \in B \quad \forall\, a, b \in B$. Ainda por hipótese, $ab \in B$ para quaisquer $a, b \in B$.

($\Longleftarrow$) Agora vamos supor que $a - b \in B$ *e* $ab \in B$ para quaisquer $a, b \in B$. Com isso, $(B, +)$ é um grupo abeliano. Por outro lado, sabendo que $ab \in B$ e $B \subset A$, então as propriedades associativa e distributiva da multiplicação em relação à adição em A são válidas em B. Portanto, $(B, +, \cdot)$ é um anel e consequentemente, B é um subanel de A.

Exemplo 2.10 Sejam $A = M_2(\mathbb{Q})$ e B o subconjunto de A dado por

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Q} \right\} \neq \emptyset.$$

Dados $x, y \in B$, digamos

$$x = \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad y = \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}.$$

Sendo $a_1,\ a_2,\ b_1,\ b_2 \in \mathbb{Q}$, temos

$$x - y = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in B \quad \text{e} \quad xy = \begin{pmatrix} a_1 a_2 & b_1 b_2 \\ 0 & 0 \end{pmatrix} \in B.$$

Portanto, B é subanel de A.

Exemplo 2.11 Sejam $\mathcal{F}$ o anel de todas as funções de $\mathbb{R}$ em $\mathbb{R}$ e

$$B = \{ f \in \mathcal{F} : f(1) = 0 \}.$$

Veja que,

$$(f + (-g))(1) = (f - g)(1) = f(1) - g(1) = 0 - 0 = 0.$$

Logo, $f - g \in B$ para quaisquer $f, g \in B$. Considerando ainda estes elementos, temos que

$$(f \cdot g)(1) = f(1) \cdot g(1) = 0 \cdot 0 = 0,$$

isto é, $f \cdot g \in B$, de maneia que B é um subanel de $\mathcal{F}$.

Proposição 2.1 *Se B_1e B_2 são subanéis de um anel A, então $B_1 \cap B_2$ também é um subanel de A.*

Demonstração: Como $0_A \in B_1$ e $0_A \in B_2$, segue que $B_1 \cap B_2 \neq \emptyset$. Por isso, se $a, b \in B_1 \cap B_2$, então

$$a, b \in B_1 \quad \text{e} \quad a, b \in B_2$$

de modo que,

$$a - b \in B_1 \quad \text{e} \quad ab \in B_1,$$

$$a - b \in B_2 \quad \text{e} \quad ab \in B_2,$$

já que B_1 e B_2 são subanéis. Desse modo,

$$a - b \in B_1 \cap B_2 \quad \text{e} \quad ab \in B_1 \cap B_2,$$

portanto, $B_1 \cap B_2$ é um subanel de A.

Proposição 2.2 *Sejam A um anel e* $\{\mathcal{B}_i\}_{i\in\wedge}$ *uma coleção de subanéis de A. Então a* $\bigcap_{i\in\wedge} \mathcal{B}_i$ *é um subanel de* A.

Demonstração: Analogamente à proposição anterior,

$$a, b \in \bigcap_{i\in\wedge} \mathcal{B}_i \quad ,$$

então, sabe-se que,

$$a, b \in \mathcal{B}_i \quad \forall\, i \in \wedge .$$

Sabendo que $\mathcal{B}_i$ é uma coleção de subanéis, então sabemos que

$$a - b \in \mathcal{B}_i \quad \text{e} \quad ab \in \mathcal{B}_i \ ,$$

com isso,

$$a - b \in \bigcap_{i\in\wedge} \mathcal{B}_i \quad \text{e} \quad a \cdot b \in \bigcap_{i\in\wedge} \mathcal{B}_i \, .$$

Portanto, $\bigcap_{i\in\wedge} \mathcal{B}_i$ é um subanel de A.

2.4. Domínios

Antes de adentrar de fato no tema, reflita sobre a seguinte questão: é possível que um produto entre dois elementos não nulos de um conjunto seja nulo? Se for considerado dois números reais como fatores, então isso é impossível, mas se considerarmos outros conjuntos como $M_2(\mathbb{R})$ teremos uma situação contrária. Com isso, obtemos a seguinte definição:

Definição 2.7 *Sejam A um anel e* $a \in A, a \neq 0_A$. *Diz-se que a é um* **divisor de zero** *quando existe* $b \in A, b \neq 0_A$, *de modo que*

$$a \cdot b = 0_A \qquad ou \qquad b \cdot a = 0_A.$$

Exemplo 2.12 Para o anel $A = M_2(\mathbb{R})$, temos

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_{A.}$$

Portanto,

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

é um divisor de zero. De moto geral, para cada número real $a \neq 0$,

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Com isso, temos que $M_2(\mathbb{R})$ possui infinitos divisores de zero.

Definição 2.8 *Um anel comutativo com unidade e sem divisores de zero chama-se* **domínio**[3]. *Equivalentemente, $\mathcal{D}$ é um domínio quando dados $a, b \in \mathcal{D}$,*

$$ab = 0_{\mathcal{D}} \Rightarrow a = 0_{\mathcal{D}} \quad \text{ou} \quad b = 0_{\mathcal{D}}.$$

Exemplo 2.13 Os anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são todos exemplos clássicos de domínios.

Exemplo 2.14 O anel $A = M_2(\mathbb{R})$ não é um domínio, pois não é comutativo e possui divisores de zero (visto no exemplo 2.12).

Exemplo 2.15 No anel $A = \mathbb{Z}_8, a = \bar{2}$ é um divisor de zero, já que $\bar{2} \cdot \bar{4} = \bar{0}$. Da mesma forma que $b = \bar{4}$ e $c = \bar{6}$ também são.

Teorema 2.4 *O anel $\mathbb{Z}_n$ é um domínio se, e somente se, n é primo.*

Demonstração: ($\Longrightarrow$) Suponha a princípio que $\mathbb{Z}_n$ é um domínio. Se n não é primo, então existem $a, b \in \mathbb{N}$ tal que $1 < a, b < n$ e $n = a \cdot b$. Sabendo que $\bar{n} = \bar{0}$ em $\mathbb{Z}_n$ então,

$$\bar{0} = \bar{n} = \bar{a} \cdot \bar{b}$$

mas, $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$, com isso, $\bar{a}$ é um divisor próprio de $\mathbb{Z}_n$, no entanto, isso contradiz a fato de $\mathbb{Z}_n$ ser um domínio. Logo, n é necessariamente primo.

($\Longleftarrow$) Agora suponha que n é primo. Dados $\bar{a}, \bar{b} \in \mathbb{Z}_n$ tais que $\bar{a} \cdot \bar{b} = \bar{0}$, isto é, $\overline{a \cdot b} = \bar{0}$, temos que,

[3] Ou *domínio de integridade* ou *domínio integral*.

$$a \cdot b \equiv 0 \ (\mathrm{mod}\ n),$$

ou seja, $n|ab$ e com isso, $n|a$ ou $n|b$ já que n é primo. Em termos de classe de equivalência isso significa que $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$, ou seja, $\mathbb{Z}_n$ é um domínio.

Proposição 2.3 *Um anel D comutativo com unidade é um domínio se, e somente se, todo elemento não nulo $a \in D$ é regular em relação à multiplicação, ou seja, dados $b, c \in D$,*

$$ab = ac \Rightarrow b = c$$

Demonstração: ($\Longrightarrow$) Supondo que D é um domínio, tomemos $a, b, c \in D$ com $a \neq 0$. Temos que,

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$$

como $a \neq 0$ e D é um domínio, então $b - c = 0$, com isso $b = c$. Portanto a é regular.

($\Longleftarrow$) Sejam $a, b \in D$ com $ab = 0$. Se a e b são diferentes de zero, então como $a \cdot b = 0$ e por hipótese a é regular segue que

$$a \cdot b = 0 = a \cdot 0 \Rightarrow b = 0,$$

isso é contrário ao fato de b ser diferente de zero, logo, isso implica que D é um domínio.

Proposição 2.4 *A característica de um domínio D é zero ou é um número primo.*

Demonstração: Seja D um domínio de característica diferente de zero. Consideremos, pois $car(D) = p$ e mostraremos que p é primo. Vamos supor que p é composto, logo existem $n, m \in \mathbb{N}$ tais que,

$$p = n \cdot m, \text{ com } 1 < n, \quad m < p.$$

Assim, naturalmente $n \cdot 1_D \neq 0_D$ e $m \cdot 1_D \neq 0_D$. Contudo, de acordo com o teorema 2.1,

$$(n \cdot 1_D)(m \cdot 1_D) = (nm) \cdot 1_D = p \cdot 1_D = 0_D.$$

Ou seja, $n \cdot 1_D$ e $m \cdot 1_D$ são divisores de zero de D, o que é uma contradição. Portanto, p é um número primo.

Definição 2.9 *Sejam D um domínio e S um subconjunto não vazio de D. Diz-se que S é um subdomínio de D quando com as operações de adição e multiplicação induzidas de D, S também é um domínio.*

2.5. Corpos

Neste tópico será abordado um tipo de anel muito especial, ele é comutativo com unidade e cada elemento não nulo que pertence a ele possui inverso multiplicativo, a esses elementos dá-se o nome de **inversíveis**. Observe que em $\mathbb{Z}$ temos 1 e -1 como elementos inversíveis, pois, $1 \cdot 1 = 1$ e $(-1) \cdot (-1) = 1$, no entanto esses são os únicos elementos em $\mathbb{Z}$ que possuem tal característica. Assim, os anéis cujos elementos não nulos são inversíveis são nomeados corpos.

Definição 2.10 *Um anel K, comutativo com unidade, é denominado corpo quando todo elemento não nulo de K tem inverso multiplicativo. Ou seja, dado $a \in K$, $a \neq 0_K$, existe $b \in K$ tal que*

$$a \cdot b = 1_K$$

A definição acima nos revela que em um corpo K sempre é possível estabelecer uma divisão por qualquer elemento não nulo. Logo o conjunto K^* dos elementos não nulos de K é um corpo com isso,

$$U_{\bullet}(K) = K^*.$$

Além disso, se for desconsiderada a comutatividade no anel K dizemos que ele é um **anel de divisão**.

Exemplo 2.16 Os anéis $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são exemplos clássicos de corpos.

Exemplo 2.17 O anel $\mathcal{F} = \{f: \mathbb{R} \longrightarrow \mathbb{R}\}$ é comutativo e possui unidade, no entanto, não é um corpo pois $U_{\bullet}(\mathcal{F}) \neq \mathcal{F}^*$. Veja que, dada a função $f \in \mathcal{F}$, sendo que,

$$f(x) = \begin{cases} 2 \text{ se } x \neq 0, \\ 0 \text{ se } x = 0. \end{cases}$$

Considere $g \in \mathcal{F}$ uma função tal que $f \cdot g = 1_{\mathcal{F}}$, então

$$(f \cdot g)(0) = 1_{\mathcal{F}}(0) = 1$$

ou seja,

$$f(0) \cdot g(0) = 1 \Rightarrow 0 \cdot g(0) = 1.$$

Observe que obtemos uma contradição ao nos deparar com a igualdade $0 = 1$, logo, f não é invertível e consequentemente não é um corpo.

Teorema 2.5 *Todo corpo K é um domínio.*

Demonstração: Sabendo que K é um anel comutativo com unidade, vamos mostrar que K não possui divisores de zero. Sejam $a, b \in K$ tais que $a \cdot b = 0_K$. Vamos supor que $a \neq 0$, logo existe $a^{-1} \in K$ de modo que $a \cdot a^{-1} = 1_K$. Agora, multiplicando a^{-1} na igualdade $a \cdot b = 0_K$ temos,

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K = 0_K$$

isto é, $(a^{-1} \cdot a) \cdot b = 0_K \Rightarrow 1_K \cdot b = 0_K \Rightarrow b = 0_K$.

Veja que no produto $a \cdot b = 0_K$ um dos fatores é igual a zero ($b = 0$) logo K é um domínio.

Teorema 2.6 *Todo domínio finito é um corpo.*

Demonstração: Para realizar a demonstração desse teorema vamos utilizar o seguinte resultado[4]: *seja A um conjunto finito não vazio. Então, toda função $f: A \to A$ injetora é também bijetora*. Tendo isso em mente, seja D um domínio formado de n elementos vamos mostrar que todo elemento não nulo de D possui inverso multiplicativo. Seja $a \in D$ com $a \neq 0_D$ considere a seguinte função

$$f: D \to D$$

$$a_i \mapsto a \cdot a_i.$$

Se a_i e $a_j \in D$, são tais que $f(a_i) = f(a_j)$ então $a \cdot a_i = a \cdot a_j$, sendo assim, $a_i = a_j$, já que D é um domínio. Com isso, f é injetora e pelo resultado dito acima, f é bijetora. Isso significa que existe $a_i \in D$ tal que $f(a_i) = 1_D$, isto é, existe $a_i \in D$ em que

$$a \cdot a_i = 1_D.$$

Isso implica que a tem inverso multiplicativo e como a é diferente de zero então conclui-se que D é um corpo.

Proposição 2.5 *$\mathbb{Z}_n$ é um corpo se, e somente se n é primo.*

[4] Resultado de teoria dos conjuntos, é o teorema 1.7 do primeiro capítulo do livro Álgebra abstrata para licenciatura de Vandemberg Lopes Vieira.

Demonstração: já sabemos que se $\mathbb{Z}_n$ é um corpo então $\mathbb{Z}_n$ é um domínio (teorema 2.5) com isso, pelo teorema 2.4 n é primo. Reciprocamente, se n é primo, então também pelo teorema 2.4 $\mathbb{Z}_n$ é domínio, como $\mathbb{Z}_n$ é finito segue do teorema 2.6 que $\mathbb{Z}_n$ é um corpo.

Se K é um corpo e $a, b \in K$, com $b \neq 0$ então podemos transformar o produto $a \cdot b^{-1} \in K$ em $\frac{a}{b}$, ou seja,

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

Chamamos de **quociente** de a por b. Existem algumas propriedades relacionadas a quocientes em um corpo K, essas, são análogas às do corpo $\mathbb{Q}$:

Propriedade (I) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

Prova: Se $ab^{-1} = cd^{-1}$ segue que,

$$\begin{aligned} ad = (ab^{-1}b)d &= (ab^{-1})bd \\ &= (cd^{-1})bd \\ &= c(d^{-1}d)b \\ &= bc. \end{aligned}$$

Por outro lado,

$$\begin{aligned} \frac{a}{b} = ab^{-1} &= a(dd^{-1})b^{-1} \\ &= ad(d^{-1}b^{-1}) \\ &= bc(d^{-1}b^{-1}) \\ &= c(bb^{-1})d^{-1} \\ &= cd^{-1} \\ &= \frac{c}{d}. \end{aligned}$$

Propriedade (II) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$.

Prova:

$$\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1}$$

$$= a(dd^{-1})b^{-1} \pm c(bb^{-1})d^{-1}$$

$$= ad(d^{-1}b^{-1}) \pm bc(b^{-1}d^{-1})$$

$$= \frac{ad}{bd} \pm \frac{bc}{bd}$$

$$= \frac{ad \pm bc}{bd}.$$

Propriedade (III) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Prova:

$$\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1}) \cdot (cd^{-1})$$

$$= (ac) \cdot (b^{-1}d^{-1})$$

$$= \frac{ac}{bd}.$$

Propriedade (IV) $\frac{a}{b} + \frac{-a}{b} = 0_K$

Prova:

$$\frac{a}{b} + \frac{-a}{b} = ab^{-1} + (-a)b^{-1}$$

$$= (a - a)b^{-1}$$

$$= (0_K)b^{-1}$$

$$= 0_K.$$

Propriedade (V): Se $a \neq 0_K$, então $\frac{a}{b} \cdot \frac{b}{a} = 1_K$.

Prova:

$$\frac{a}{b} \cdot \frac{b}{a} = (ab^{-1}) \cdot (ba^{-1})$$

$$= (aa^{-1}) \cdot (bb^{-1})$$

$$= 1_K \cdot 1_K$$

$$= 1_K.$$

Definição 2.11 *Sejam K um corpo e $\mathcal{F}$ um subconjunto não vazio de K. Dizemos que $\mathcal{F}$ é um* ***subcorpo*** *de K quando com as operações de adição e multiplicação induzidas de K, $\mathcal{F}$ também é um corpo.*

Se $\mathcal{F}$ é um subcorpo de K, pode-se dizer que K é uma **extensão** de $\mathcal{F}$. Uma vez que $\mathcal{F}$ é subcorpo de K então $1_K = 1_{\mathcal{F}}$. Existe um critério que mostra quando um subconjunto não vazio de um corpo é uma extensão desse corpo.

Proposição 2.6 *Um subconjunto não vazio $\mathcal{F}$ de um corpo K é subcorpo de K se, e somente se, para todos $a, b \in \mathcal{F}$,*

$$a - b \in \mathcal{F} \quad e \quad a \cdot b^{-1} \in \mathcal{F}, \quad para\ b \neq 0.$$

Demonstração: Se $\mathcal{F}$ é um subcorpo de K, então por definição $\mathcal{F}$ é também um corpo e, por isso, para quaisquer $a, b \in \mathcal{F}$, temos que, $a - b = a + (-b) \in \mathcal{F}$ e $a \cdot b \in \mathcal{F}$. Não obstante, se $b \neq 0$, tem-se $b^{-1} \in \mathcal{F}$. Com isso, $a \cdot b^{-1} \in \mathcal{F}$.

Reciprocamente, sejam $a, b \in \mathcal{F}$, por hipótese, $a + b = a - (-b) \in \mathcal{F}$ e $a \cdot b \in \mathcal{F}$. Ademais, se $b \neq 0$, segue que $a \cdot b = a(b^{-1})^{-1} \in \mathcal{F}$. Em particular, se $a \neq 0$, então $a \cdot a^{-1} = 1_K \in \mathcal{F}$. Observe que, $\mathcal{F}$ tem propriedades de corpo, como $\mathcal{F} \subset K$ então $\mathcal{F}$ é subcorpo de K.

2.6. Homomorfismo de anéis

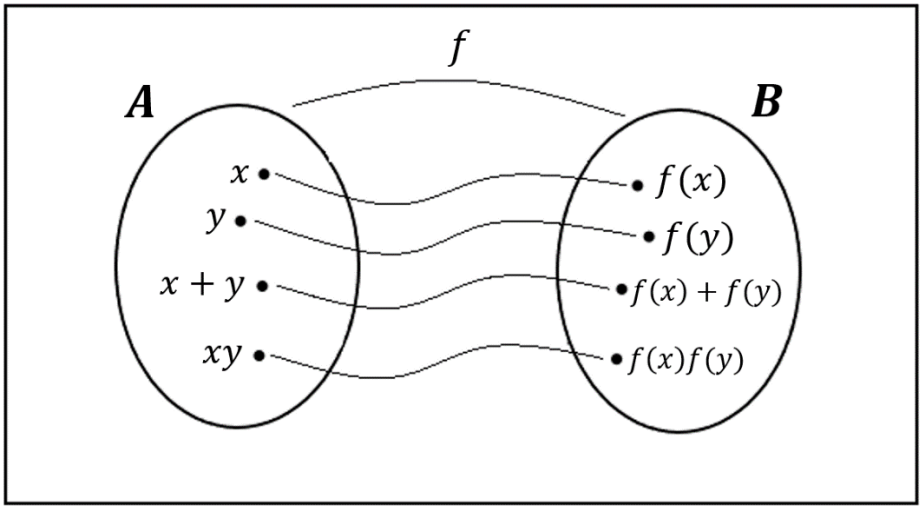
O principal objetivo desse tópico é mostrar e exemplificar funções entre anéis, sabendo que anéis não são conjuntos comuns é importante ressaltar que tais funções preservam as operações inerentes aos anéis, a essas funções dá-se o nome de ***homomorfismo***.

Definição 2.12 *Sejam A e B anéis. Uma função $f : A \to B$ é chamada de* ***homomorfismo*** *de A em B quando é válido que:*

(a) $f(a + b) = f(a) + f(b), \quad \forall\ a, b \in A$;
(b) $f(a \cdot b) = f(a) \cdot f(b), \quad \forall\ a, b \in A$.

Vale ressaltar que em (a) a adição do lado esquerdo da igualdade diz respeito à adição do anel A, já o lado direito refere-se à adição do anel B. Tais relações funcionam de maneira análoga para a multiplicação, expressa em (b). Além disso, se um homomorfismo é uma função injetora, o chamamos de *homomorfismo injetor*. Caso a função f seja sobrejetora, então teremos um *homomorfismo sobrejetor*. Mas se f for bijetora chegamos ao conceito de **isomorfismo** (abordado no tópico 2.6.2). Para um melhor entendimento do conceito de homomorfismo, observe a figura 2.1.

Figura 2.1: Homomorfismo de A em B



Fonte: Elaborada pela autora, 2022.

Se $f: A \to B$ é um homomorfismo, então as seguintes propriedades são imediatas para f:

1. $f(0_A) = 0_B$;
2. $f(-a) = -f(a), \quad \forall\, a \in A$;
3. $f(a-b) = f(a) - f(b), \quad \forall\, a, b \in A$.

Demonstração:

1. $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow f(0_A) = 0_B$;
2. $f(a) + f(-a) = f(a-a) = f(0_A) = 0_B \Rightarrow f(-a) = -f(a)$;
3. $f(a-b) = f(a+(-b) = f(a) + f(-b) = f(a) - f(b), \quad \forall\, a, b \in A$.

Exemplo 2.18 Para quaisquer A e B, a função $f : A \to B$ dada por $f(a) = 0_B, \ \forall\, a \in A$, é um homomorfismo, nomeado de **homomorfismo trivial**.

Exemplo 2.19 Seja A um anel qualquer. Então, a função $f : A \to A$ dada por $f(a) = a$, para todo $a \in A$ é chamado **homomorfismo identidade**.

Exemplo 2.20 Dada a função $f : \mathbb{Z} \to 2\mathbb{Z}$ definida por $f(x) = 2x, \ \forall\, x \in \mathbb{Z}$ e dados $x, y \in \mathbb{Z}$ já sabemos que $f(x + y) = f(x) + f(y)$. Porém,

$$f(x \cdot y) = 2xy \quad \text{e} \quad f(x) \cdot f(y) = 2x \cdot 2y = 4xy.$$

Assim, temos que $f(x \cdot y) \neq f(x) \cdot f(y)$, a não ser quando $x = 0$ ou $y = 0$. Portanto, a função $f : \mathbb{Z} \to 2\mathbb{Z}$ não é um homomorfismo.

Exemplo 2.21 Sejam os anéis $A = \mathbb{C}$ e $B = M_2(\mathbb{R})$, considere a função $f : \mathbb{C} \to M_2(\mathbb{R})$, definida por

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \ \forall\, a + bi \in \mathbb{C}.$$

Vamos mostrar que f é um homomorfismo.

Solução: Sejam $x = a + bi$ e $y = c + di$ elementos quaisquer de A. Temos que $x + y = (a + c) + (b + d)i$ de modo que,

$$\begin{aligned} f(x + y) &= \begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= f(x) + f(y). \end{aligned}$$

Por outro lado, temos que $x \cdot y = (ac - bd) + (ad + bc)i$, segue que

$$\begin{aligned} f(x \cdot y) &= \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= f(x) \cdot f(y). \end{aligned}$$

Portanto, f é um homomorfismo.

Proposição 2.7 *Sejam A_1 e A_2 anéis, e $f : A_1 \to A_2$ um homomorfismo, então vale que,*

(a) Se B é subanel de A_1, então $f(B)$ é subanel de A_2. Em particular, $Im(f)$ é subanel de A_2.

(b) Se f é uma função sobrejetora e A_1 é comutativo, então A_2 é comutativo.

(c) Se f é uma função sobrejetora e existe 1_{A_1}, então A_2 tem unidade e $1_{A_2} = f(1_{A_1})$.

Demonstração: (a) Por hipótese B é subanel, logo $f(B) \neq \emptyset$, agora, sejam $a, b \in f(B)$ digamos que $a = f(x)$ e $b = f(y)$, em que $x, y \in B$. Logo,

$$a - b = f(x) - f(y) = f(x - y) \in f(B),$$

já que f é homomorfismo e $x - y \in B$. Analogamente, temos $a \cdot b \in f(B)$, por isso, $f(B)$ é subanel de A_2. Em particular, como A_1 é subanel de si próprio, então $Im(f) = f(A_1)$ é subanel de A_2.

(b) Dados $c, d \in A_2$, elementos quaisquer, como f é sobrejetora existem $a, b \in A_1$ tal que,

$$f(a) = c \text{ e } f(b) = d.$$

Mas como $f : A_1 \to A_2$ é um homomorfismo então, sabemos que $f(a \cdot b) = f(a) \cdot f(b)$. Com isso, vale que,

$$c \cdot d = f(a) \cdot f(b) = f(a \cdot b) = f(b \cdot a) = f(b) \cdot f(a) = d \cdot c \in A_2.$$

Sendo assim, chegamos que A_2 é comutativo.

(c) Seja b um elemento qualquer de A_2. Como f é sobrejetivo, existe $a \in A_1$ de modo que $f(a) = b$, logo,

$$b \cdot f(1_{A_1}) = f(a) \cdot f(1_{A_1}) = f(a \cdot 1_{A_1}) = f(a) = b.$$

Similarmente, $f(1_{A_1}) \cdot b = b$. Assim, A_2 tem unidade e $1_{A_2} = f(1_{A_1})$.

2.6.1 Núcleo de um homomorfismo

O núcleo de um homomorfismo é um dos subconjuntos de anéis mais especiais. Quando existe um homomorfismo entre os anéis, A e B por exemplo, cada elemento de um subconjunto de A tem como imagem o zero do anel B. A esse subconjunto dá-se o nome de ***núcleo*** (***ou Kernel***).

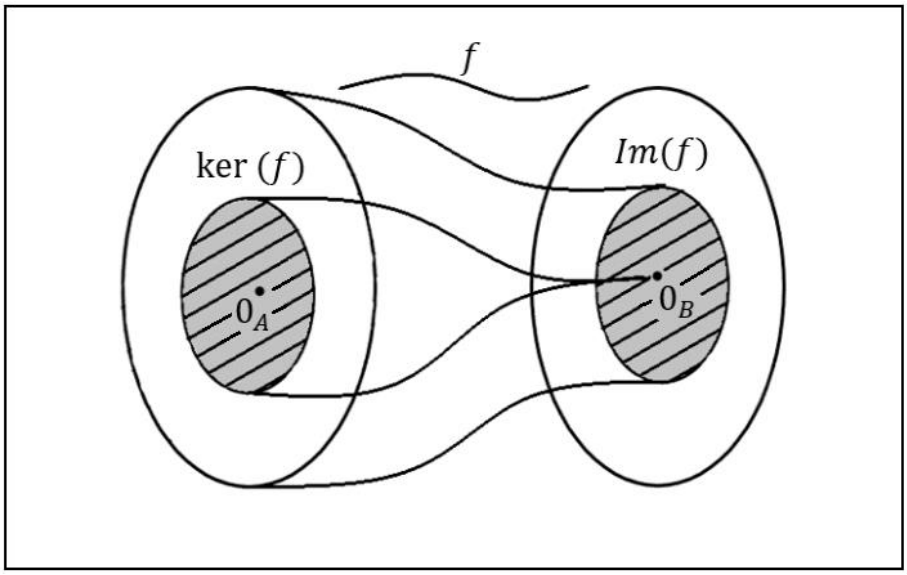
Definição 2.13 *Sejam A e B anéis e $f : A \to B$ um homomorfismo. O subconjunto de A definido por*

$$\ker(f) = \{ x \in A : f(x) = 0_B \}$$

é chamado ***núcleo*** *o homomorfismo.*

Observe que $\ker(f)$ sempre é um conjunto não vazio, pois $0_A \in \ker(f)$, dado que $f(0_A) = 0_B$ para qualquer que seja o homomorfismo de f.

Figura 2.2: Núcleo de um homomorfismo



Fonte: Elaborada pela autora, 2022.

Exemplo 2.22 Pelo exemplo 2.21 sabemos que função $f : \mathbb{C} \to M_2(\mathbb{R})$, definida por

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad \forall\, a + bi \in \mathbb{C},$$

é um homomorfismo. Agora, dado $x = a + bi \in \mathbb{C}$, temos

$$x \in \ker(f) \Leftrightarrow f(x) = 0_B,$$

isto é, se, e somente se,

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

de onde obtemos que $x = 0$. Sendo assim, $\ker(f) = \{0\}$.

Proposição 2.8 *Um homomorfismo de anéis* $f : A \to B$ *é injetivo se, e somente se,* $\ker(f) = \{0_A\}$.

Demonstração: Se f é um homomorfismo injetivo e $x \in \ker(f)$, então $f(x) = 0_B$. Como $f(0_A) = 0_B$, temos que $f(x) = f(0_A)$. Com isso, por hipótese, $x = 0_A$, logo $\ker(f) = \{0_A\}$. Reciprocamente, sejam $x_1,\ x_2 \in A$ tais que $f(x_1) = f(x_2)$. Assim, $f(x_1) - f(x_2) = 0_B$, ou seja, $f(x_1 - x_2) = 0_B$. Por isso, $x_1 - x_2 \in \ker(f)$, isto é, $x_1 - x_2 = 0_A$. Logo, $x_1 = x_2$ e, por isso, f é injetivo.

2.6.2 Isomorfismo de anéis

Agora estudaremos os homomorfismos bijetores, nesse caso, se existir uma bijeção entre dois anéis, isso implica que as propriedades são válidas para um se, e somente se, for válida para o outro.

Definição 2.14 *Sejam A e B anéis. Chama-se* ***isomorfismo*** *um homomorfismo* $f : A \to B$ *quando a função f é bijetora. Particularmente, um isomorfismo* $f : A \to A$ *é dito um* ***automorfismo*** *de A.*

O conjunto dos automorfismos de um anel A é indicado por,

$$Aut(A) = \{f : A \to A\ ; f \text{ é autmorfismo}\}.$$

Como foi dito anteriormente, um isomorfismo é um tipo particular de homomorfismo (quando a função f é bijetora) com isso, todas as propriedades de homomorfismo são válidas para um isomorfismo.

Se a função $f : A \to B$ é um isomorfismo, então vale que, $f^{-1} : A \to B$ é também um isomorfismo, nesse caso dizemos que esses anéis são **isomorfos** (existe um isomorfismo entre eles), e representamos por

$$A \simeq B.$$

Diferentemente de um homomorfismo $g : A \to B$, um isomorfismo $f : A \to B$ conserva todas as propriedades do anel A, sendo assim, é possível considerar os anéis A e B como

sendo os mesmos. Sendo assim, cada elemento $a \in A$ é identificado via o isomorfismo f, com o elemento $f(a) \in B$. Simbolicamente temos,

$$a \leftrightarrow f(a).$$

Isto significa que o elemento a é visto como se fosse igual ao elemento $f(a)$, de modo que esses elementos têm as mesmas propriedades algébricas. Além disso, existe uma relação de equivalência entre um isomorfismo de anéis, ou seja, dados A_1, A_2 e A_3 anéis quaisquer temos,

1. $A_1 \simeq A_1$.
2. Se $A_1 \simeq A_2$, então $A_2 \simeq A_1$.
3. Se $A_1 \simeq A_2$ e $A_2 \simeq A_3$, então $A_1 \simeq A_3$.

Exemplo 2.23 A função $f : \mathbb{C} \to M_2(\mathbb{R})$ definida por

$$f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad \forall\, a+bi \in \mathbb{C},$$

é um homomorfismo, com $\ker(f) = \{0\}$. Com isso, pela proposição 2.8 f é injetivo. Logo, $\mathbb{C} \simeq Im(f)$.

2.7 Ideais

Apesar de ser estudado na álgebra moderna, os ideais foram ferramentas que auxiliaram no estudo da teoria dos números. A noção de **ideal** foi introduzida ainda no século XIX pelo matemático Richard Dedekind.

Definição 2.15 *Seja A um anel. Um subconjunto não vazio de I de A é chamado de* ***ideal*** *de A quando as seguintes condições são satisfeitas:*

$$a - b \in I, \qquad \forall\, a, b \in I;$$

$$ax \in I, \quad \forall\, a \in I \;\; e \;\; \forall\, x \in A.$$

Existe subanel I de A que satisfaz $ax \in I$ para todo $a \in I$ e $x \in A$, no entanto, não satisfaz a condição $xa \in I$, ou vice-versa, para casos como esse há a seguinte definição:

Definição 2.16 *Um subconjunto não vazio I de um anel A chama-se* ***ideal à esquerda*** *(à direita) de A quando são satisfeitas:*

(a) $x - y \in I, \quad \forall\, x, y \in I$;

(b) $ax \in I\ (xa \in I), \quad \forall\, a \in A \ \ e \ \ \forall\, x \in I.$

A expressão $xa \in I$ se refere à condição do ideal à direita. De modo geral, um subanel I de um anel A é um ideal se, e somente se, I é um ideal à esquerda e à direita de A simultaneamente.

Exemplo 2.24 Para qualquer que seja o anel A, $I_1 = \{0_A\}$ e $I_2 = A$ são ideais de A. A estes dá-se o nome de **ideais triviais**.

Exemplo 2.25 Considere o anel $A = \mathbb{R}^{\mathbb{R}}$ (comutativo) de todas as funções $f : \mathbb{R} \to \mathbb{R}$. Dado $a \in \mathbb{R}$, seja $I = \{f \in A\,; f(a) = 0\}$. É imediato verificar que $f - g \in I$ para quaisquer que sejam $f, g \in I$. Agora, dado $h \in A$,

$$(f \cdot h)(a) = f(a) \cdot h(a) = 0 \cdot h(a) = 0,$$

ou seja, $f \cdot h \in I$. Logo, I é um ideal de A.

Exemplo 2.26 Sabemos que $\mathbb{Z}$ é subanel de $\mathbb{Q}$. No entanto, $\mathbb{Z}$ não é ideal à direita e nem à esquerda de $\mathbb{Q}$. Note que,

$$1h \in \mathbb{Z}, \quad \tfrac{1}{2} \in \mathbb{Q}, \text{ mas } 1 \cdot \tfrac{1}{2} \notin \mathbb{Z} \ \ e \ \ \tfrac{1}{2} \cdot 1 \notin \mathbb{Z}.$$

Exemplo 2.27 Se $f : A \to B$ é um homomorfismo de anéis, então $\ker(f)$ é um ideal de A. De fato, dados $x, y \in \ker(f)$, temos

$$f(x - y) = f(x) - f(y) = 0_B - 0_B = 0_B \Rightarrow x - y \in \ker(f),$$

agora para $a \in A$,

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0_B = 0_B \Rightarrow a \cdot x \in \ker(f).$$

Da mesma forma que $x \cdot a \in \ker(f)$. Logo, $\ker(f)$ é ideal de A.

Sabendo que I é um ideal de A, então é evidente que $-a \in I$ e $a + b \in I$ para todo $a, b \in I$, já que I é subanel de A.

Proposição 2.9 *Sejam A um subanel comutativo com unidade e I um ideal de A. Se* $u \in A$ *é invertível e* $u \in I$*, então* $I = A$.

Demonstração: Tomando um elemento qualquer $a \in A$, podemos escrevê-lo na forma $a = a \cdot 1$ (1 é a unidade de A). Sabendo que u é invertível, existe $u^{-1} \in A$ de maneira que $1 = u^{-1} \cdot u^{-1}$. Logo,

$$a = a \cdot 1 = a(u \cdot u^{-1}) = (a \cdot u) \cdot u^{-1}.$$

Como I é um ideal, temos que $au \in I$ e daí, $a = (a \cdot u)u^{-1} \in I$. Com isso, provamos que $A \subset I$, e como $I \subset A$, então $I = A$.

2.7.1 Domínios de ideais principais

Seja A um anel comutativo. Considere os elementos fixos $a_1, \dots, a_n \in A$ e I um subconjunto de A construído a partir desses elementos:

$$I = \{x_1 \cdot a_1 + \cdots + x_n \cdot a_n : x_i \in A, \quad \forall\, i = 1, \dots, n\}.$$

Vamos mostrar que I é um ideal de A. Primeiramente, note que I é não vazio, já que $0 = 0 \cdot a_1 + \cdots + 0 \cdot a_n \in I$. Agora considere os elementos $x, y \in I$, onde

$$x = x_1 \cdot a_1 + \cdots + x_n \cdot a_n \text{ e } y = y_1 \cdot a_1 + \cdots + y_n \cdot a_n,$$

veja que

$$x - y = (x_1 - y_1) \cdot a_1 + \cdots + (x_n - y_n) \cdot a_n \in I,$$

e, se $a \in A$,

$$ax = (ax_1) \cdot a_1 + \cdots + (ax_n) \cdot a_n \in I.$$

Portanto, I é um ideal de A, chamado **ideal gerado** por $a_1, \dots, a_n$. Podemos indicar esse ideal por $\langle a_1, \dots, a_n \rangle$, isto é,

$$\langle a_1, \dots, a_n \rangle = \{x_1 \cdot a_1 + \cdots + x_n \cdot a_n : x_i \in A, \quad \forall\, i = 1, \dots, n\}.$$

Em particular, se $a \in A$ chamamos de **ideal principal gerado** por a o ideal

$$I = \langle a \rangle = \{x \cdot a : x \in A\}.$$

É comum indicar o ideal $I = \langle a \rangle$ por $a \cdot A$.

Definição 2.17 *Um domínio D é chamado de* ***domínio de ideais principais*** *ou* ***domínio principal*** *(DIP) quando todos os ideais de D são principais.*

Teorema 2.7 *$\mathbb{Z}$ é um domínio de ideais principais.*

Demonstração: Seja I um ideal de $\mathbb{Z}$. Se $I = \{0\}$, então $I = \langle 0\rangle$, de modo que I é principal. Agora suponha que $I \neq \langle 0\rangle$. Logo existe $a \in I,\ a \neq 0$ e como I é ideal, $-a \in I$. Com isso, pode-se garantir que existem em I elementos que são estritamente positivos. Portanto, o conjunto $\{x \in I : x > 0\}$ é não vazio. Com isso, vamos considerar

$$b = \min\{x \in I : x > 0\}.$$

Vamos mostrar que $I = \langle b\rangle$. Dado $x \in I$, pelo algoritmo da divisão existem $r, q \in \mathbb{Z}$ tais que

$$x = bq + r, \quad \text{com} \quad 0 \leq r \leq b.$$

Logo,

$$r = x - bq \in I,$$

pois $x, bq \in I$ como b é o menor elemento positivo de I e $0 \leq r \leq b$, então devemos ter $r = 0$. Daí, $x = bq$, ou seja, $x \in \langle b\rangle$. Isso quer dizer que $I \subset \langle b\rangle$, e como $\langle b\rangle \subset I$, pois $b \in I$ $(b = 1 \cdot b)$, então $I = \langle b\rangle$, sendo assim, $\mathbb{Z}$ é um DIP.

Teorema 2.8 *Seja K um anel comutativo com unidade. Então K é um corpo se, e somente se, os únicos ideais de K são os triviais.*

Demonstração: Primeiramente vamos supor que K é um corpo e tomemos um ideal I de K tal que $I \neq \{0\}$. Com isso, existe $a \in I$, com $a \neq 0$. Como K é um corpo, então a é invertível, e pela proposição 3.1, pode-se concluir que $I = K$.

Reciprocamente, seja $a \in K$ com $a \neq 0$. Logo i ideal $I = \langle a\rangle$ é tal que $I \neq \{0\}$. Com isso, temos por hipótese que $I = K$. Como $1 \in K$, existe $x \in K$ com

$$1 = ax.$$

Logo, a é invertível, e como a é não nulo e arbitrário de K, conclui-se que K é um corpo.

2.7.2 Operações com ideais

Vamos considerar os ideais I e J de um anel comutativo A. Vamos mostrar que a intersecção entre esses dois ideais de A é um ideal de A.

Sabendo que I e J são ideais de A então, $0_A \in I$ e $0_A \in J$, daí $I \cap J \neq \emptyset$. Com isso, dados $x, y \in I \cap J$, temos que $x, y \in I$ e $x, y \in J$. Logo $x - y \in I \cap J$. Agora, seja $a \in A$ e I, J ideais de A então, I e J são ideais de $ax \in I$ e $ax \in J$. Logo, $ax \in I \cap J$ e portanto, $I \cap J$ é ideal de A.

Além disso, se $(I_\lambda)_{\lambda \in \Lambda}$ é uma família de ideais de A, então

$$\bigcap_{\lambda \in \Lambda} I_\lambda$$

é também um ideal de A. Agora vamos mostrar que a soma entre os ideais I_1 e I_2, indicada por $I_1 + I_2$, definida por

$$I_1 + I_2 = \{x_1 + x_2 : \ x_1 \in I_1 \ e \ x_2 \in I_2\}$$

é um ideal.

É certo que, $0_A \in I_1$, $0_A \in I_2$ e $0_A = 0_A + 0_A$, então$0_A \in I_1 + I_2$, ou seja, $I_1 + I_2 \neq \emptyset$. Assim, sejam $x, y \in I_1 + I_2$, digamos que

$$x = x_1 + x_2 \quad \text{e} \quad y = y_1 + y_2,$$

em que $x_1 \cdot y_1 \in I_1$ e $x_2 \cdot y_2 \in I_2$. Logo,

$$x - y = (x_1 - y_1) + (x_2 - y_2) \in I_1 + I_2,$$

Já que, $x_1 - y_1 \in I_1$ e $x_2 - y_2 \in I_2$. Agora, se $a \in A$, então

$$ax = a(x_1 + x_2) = ax_1 + ax_2 \in I_2 + I_2,$$

desde que $ax_1 \in I_1$ e $ax_2 \in I_2$. Portanto, $I_1 + I_2$ é um ideal de A, chamado de ideal soma de I_1 e I_2. Observe que

$$I_1 \subset I_1 + I_2 \quad \text{e} \quad I_2 \subset I_1 + I_2.$$

pois se $x \in I_1$ e $y \in I_2$, então $x = x + 0_A \in I_1 + I_2$ e $y = 0_A + y \in I_1 + I_2$. Além disso, $I + I = I$, para qualquer ideal I de um anel A.

Na proposição a seguir será usado os termos *maior* e *menor* (itens *I* e *II*), estes, se referem à inclusão dos conjuntos.

Proposição 2.10 *Sejam A um anel comutativo e I_1 e I_2 ideais de A. Então,*

I. $I_1 \cap I_2$ *é o maior ideal de A contido em* I_1 *e em* I_2.

II. $I_1 + I_2$ *é o menor ideal de A que contém* I_1 *e* I_2.

III. $I_1 + I_2 = I_1$ *se, e somente se,* $I_2 \subset I_1$.

Demonstração: *(I)* Consideremos um ideal $\mathcal{J}$ de A tal que $\mathcal{J} \subset I_1$ e $\mathcal{J} \subset I_2$. Assim, claramente, $\mathcal{J} \subset I_1 \cap I_2$. Note que em relação a esta inclusão foi usado resultados sobre Teoria dos Conjuntos.

(II) Seja $\mathcal{J}$ um ideal de A, em que $I_1 \subset \mathcal{J}$ e $I_2 \subset \mathcal{J}$. Logo, se $x = x_1 + x_2 \in I_1 + I_2$, com $x_1 \in I_1$ e $x_2 \in I_2$, então $x_1 \in \mathcal{J}$ e $x_2 \in \mathcal{J}$. Desse modo, $x \in \mathcal{J}$, isto é, $I_1 + I_2 \subset \mathcal{J}$.

(III) Suponha que $I_1 + I_2 = I_1$. Com isso, dado $x \in I_2$,

$$x = 0_A + x \in I_1 + I_2 = I_1 \Rightarrow x \in I_1 \Rightarrow I_2 \subset I_1.$$

Reciprocamente, vamos supor que $I_2 \subset I_1$. Por isso, se $x = x_1 + x_2 \in I_1 + I_2$, então

$$x = x_1 + x_2 \in I_1 + I_1 = I_1.$$

Por isso, $I_1 + I_2 \subset I_1$, e como $I_1 \subset I_1 + I_2$, segue que $I_1 + I_2 = I_1$.

Definição 2.18 *Sejam* I_1 *e* I_2 *ideais de um anel comutativo A. Define-se o produto* $I_1 \cdot I_2$ *de* I_1 *e* I_2 *como o conjunto constituído por todos os elementos (somas) da forma*

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n, \quad x_i \in I_1 \quad e \quad y_i \in I_2,$$

Para $i = 1, 2, \ldots, n$. *Ou seja, para cada* $n \in \mathbb{N}$,

$$I_1 \cdot I_2 = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in I_1 \ \ e \ \ y_i \in I_2 \right\}.$$

É claro que sendo A comutativo, então $I_1 \cdot I_2 = I_2 \cdot I_1$.

Teorema 2.9 *Sejam* I_1, I_2 *e* I_3 *ideais de um anel comutativo A. Então,*

(1) $(I_1 \cdot I_2) \cdot I_3 = I_1 \cdot (I_2 \cdot I_3)$. *(o produto de ideais é associativo)*

(2) $I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3$ *(o produto de ideais é distributivo sobre a adição)*

Demonstração: (1) Veja que,

$$(I_1 \cdot I_2) \cdot I_3 = \sum_{i=1}^{n} w_i z_i,$$

onde temos que $w_i \in I_1 \cdot I_2$, ou seja, $w_i = \sum_{j=1}^{m} x_i y_i$, onde $x_i \in I_1$, $y_i \in I_2$ e $z_i \in I_3$, com isso,

$$\sum_{i=1}^{n} w_i z_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_i y_i \right) z_i$$

$$= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} (x_i y_i z_i) \right)$$

$$= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_i (y_i z_i) \right)$$

$$= \sum_{i=1}^{n} x_i \left(\sum_{j=1}^{m} (y_i z_i) \right).$$

Por definição, $\sum_{j=1}^{m} (y_i z_i) = I_2 \cdot I_3$, logo temos,

$$\sum_{i=1}^{n} x_i \left(\sum_{j=1}^{m} (y_i z_i) \right) = I_1 \cdot (I_2 \cdot I_3).$$

(2) Considere,

$$x = \sum_{i=1}^{m} x_i y_i \in I_1 \cdot (I_2 + I_3),$$

por definição, $x_i \in I_1$ e $y_i \in I_2 + I_3$, ou seja, $y_i = a_i + b_i$, em que $a_i \in I_2$ e $b_i \in I_3$. Por isso, para cada i,

$$x_i y_i = x_i (a_i + b_i) = x_i a_i + x_i b_i,$$

portanto,

$$x = \sum_{i=1}^{m} x_i \, y_i = \sum_{i=1}^{m} (x_i a_i + x_i b_i)$$

$$= \sum_{i=1}^{m} x_i a_i + \sum_{i=1}^{m} x_i\, b_i \in I_1 \cdot I_2 + I_1 \cdot I_3,$$

ou seja, $I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3$.

Para a outra inclusão, tomemos $y \in I_1 \cdot I_2 + I_1 \cdot I_3$. Logo,

$$y = \sum_{i=1}^{m} x_i\, y_i + \sum_{i=1}^{n} x_i\, z_i,$$

Em que $x_i \in I_1,\ y_i \in I_2$ e $z_i \in I_3$. Como $x_i y_i = x_i(y_i + 0),\ x_i z_i = x_i(0 + z_i)$ e, além disso, $0 \in I_2$ e $0 \in I_3$, então y é uma soma de produtos da forma $x_i \cdot (y_i + z_i)$, com $x_i \in I_1,\ y_i \in I_2$ e $z_i \in I_3$. Portanto, $y \in I_1 \cdot (I_2 + I_3)$. Com isso, conclui-se que

$$I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3.$$

2.7.3 Ideais primos e maximais

Nesta seção abordaremos o estudo de dois importantes subanéis, os ideais primos e os ideais maximais. Veremos exemplos desses dois ideais, assim como teoremas e proposições inerentes à cada um, além disso, veremos proposições que estabelecem relações entre estes dois ideais.

2.7.3.1 Ideais primos

Definição 2.19 *Sejam A um anel comutativo e P um ideal de A, em que $P \neq A$. Diz-se que P é um* ***ideal primo*** *quando toda vez que $ab \in P$, com $a, b \in A$, então $a \in P$ ou $b \in P$. Isto é, dados $a, b \in A$,*

$$ab \in P \Rightarrow a \in P \quad ou \quad b \in P.$$

Exemplo 2.28 Temos que $I = \{0\}$ é um ideal primo. De fato, dados $a, b \in \mathbb{Z}$ tais que $ab \in I$. Então, $ab = 0$, de modo que, $a = 0 \in I$ ou $b = 0 \in I$, pois $\mathbb{Z}$ é um domínio.

Exemplo 2.29 Podemos afirmar que $6\mathbb{Z}$ não é um ideal primo. De fato, $2 \cdot 3 = 6 \in 6\mathbb{Z}$. No entanto, note que $2 \notin 6\mathbb{Z}$ assim como $3 \notin 6\mathbb{Z}$.

A seguinte proposição irá generalizar o tipo dos ideais primos do anel $\mathbb{Z}$.

Proposição 2.11 *Se $p \in \mathbb{Z}$ é um inteiro primo, então $p\mathbb{Z}$ é um ideal primo.*

Demonstração: Considere $ab \in \mathbb{Z}$. Então $p|ab$. Como por hipótese p é um inteiro primo, temos que $p|a$ ou $p|b$. Com isso, temos que $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$.

2.7.3.2. Ideais maximais

Definição 2.20 *Sejam A um anel comutativo e M um ideal de A, em que $M \neq A$. Diz-se que M é um* ***ideal maximal*** *quando os únicos ideais de A que contém M são M e A. Equivalentemente, M é maximal quando para todo ideal $\mathcal{J}$ de A tal que*

$$M \subsetneq \mathcal{J}$$

tem-se que $\mathcal{J} = A$.

Exemplo 2.30 Note que $\{0\} \subsetneq 2\mathbb{Z} \neq \mathbb{Z}$, com isso, o ideal $\{0\}$ em $\mathbb{Z}$ não é maximal.

Proposição 2.12 *Seja A um anel comutativo com unidade. Então todo ideal maximal de A é primo.*

Demonstração: Consideremos M um ideal maximal de A e sejam $a, b \in A$ tais que $ab \in M$. Vamos mostrar que $a \in M$ ou $b \in M$. Suponha que $a \neq M$ e tomemos o seguinte ideal soma

$$I = \langle a \rangle + M.$$

Veja que $I \neq M$, pois $a \in I$. Assim, $M \subsetneq I$ e sendo M maximal, então por definição, $I = A$. Como $1 \in A = \langle a \rangle + M$, existem $x \in A$ e $y \in M$ tais que

$$1 = x \cdot a + y.$$

Multiplicando ambos os lados dessa última igualdade por b, temos

$$b = x(ab) + by.$$

Como por hipótese $ab \in M$, e $y \in M$, conclui-se que $b \in M$. Portanto, M é primo.

Teorema 2.10 *Se D é um domínio de ideais principais, então todo ideal primo não nulo de D é maximal.*

Demonstração: Seja P um ideal primo não nulo de D, e suponhamos que exista um ideal $\mathcal{J}$ de D tal que $P \subset \mathcal{J}$. Como D é um DIP, então

$$P = \langle a \rangle \quad \text{e} \quad \mathcal{J} = \langle b \rangle, \quad \text{com } a, b \in D.$$

Além disso, $P \subset \mathcal{J}$ e $a \in P$ (pois $a = 1 \cdot a$) implicam que $a \in \mathcal{J}$, ou seja,

$$a = b \cdot c, \tag{3.4}$$

para algum $c \in D$. Assim, $b \cdot c \in P$, e como P é primo,

$$b \in P \quad \text{ou} \quad c \in P.$$

Se $b \in P$, então $b = a \cdot y_1$ para algum $y_1 \in D$, de modo que, para todo $x \in \mathcal{J}$, $x = b \cdot y_2 \in D$, temos

$$x = b \cdot y_2 = a \cdot (y_1 \cdot y_2) \in P.$$

Isso implica que $\mathcal{J} \subset P$, ou seja, $P = \mathcal{J}$. Para a outra parte, se $c \in P$, então $c = a \cdot d$, para algum $d \in D$. Desse modo, usando a igualdade em (3.4), segue que

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

Assim

$$a = 0 \quad \text{ou} \quad b \cdot d = 1,$$

Já que D é um domínio. Como por hipótese $P \neq \{0\}$, então $a \neq 0$. Por isso, $b \cdot d = 1$, ou seja, b é invertível e, portanto $\mathcal{J} = A$.

Teorema 2.11 *Seja K um anel comutativo com unidade. Então, K é um corpo se, e somente se, os únicos ideais de K são os triviais.*

Demonstração: Suponha que K seja um corpo e consideremos I um ideal de K, em que $I \neq \{0\}$. Vamos mostrar que $I = K$. Para tanto, tomemos $a \in I$, com $a \neq 0$. Como K é um corpo existe $\in K$ tal que

$$a \cdot a^{-1} = 1.$$

Mas $1 = a \cdot a^{-1} \in K$, pois $a \in I$ portanto, $I = K$.

Reciprocamente, vamos supor que os únicos ideais de K sejam os triviais. Para mostrar que K é um corpo, é necessário provar que todo elemento não nulo de K tem inverso multiplicativo. Para cada $a \in K$, $a \neq 0$, consideremos o ideal principal $I = \langle a \rangle$. Como, $a = a \cdot 1$ então $a \in I$ e, por isso, $I \neq \{0\}$. Logo, por hipótese, $I = \langle a \rangle = K$. Por outro lado, existe $b \in K$ de modo que

$$1 = a \cdot b,$$

pois $1 \in K$, o que mostra que a é invertível. Portanto K é um corpo.

2.8. Anéis quocientes

Sejam A um anel e I um ideal de A, vamos agora definir a relação "$\equiv (\mathrm{mod}\, I)$" sobre o anel A. Dado $x, y \in A$, temos

$$x \equiv y\ (\mathrm{mod}\, I) \Leftrightarrow x - y \in I.$$

Vamos mostrar que essa relação é de equivalência demonstrando as seguintes propriedades:

i. *Reflexividade:* $x \equiv x\ (mod\ I)$.
De fato, seja $x \in A$, temos que $x \equiv x\ (\mathrm{mod}\, I)$ então $x - x = 0_A \in I$.

ii. *Simetria: Se* $x \equiv y\ (\mathrm{mod}\, I)$ *então* $y \equiv x\ (\mathrm{mod}\, I)$.
Sabemos que, por hipótese $x - y \in I$, assim como

$$-(x - y) \in I \Rightarrow -x + y = y - x \in I,$$

Ou seja, $y \equiv x\ (\mathrm{mod}\, I)$.

iii. *Transitividade: Dados* x, y *e* $z \in A$. *Se* $x \equiv y\ (\mathrm{mod}\, I)$ *e* $y \equiv z\ (\mathrm{mod}\, I)$ *então* $x \equiv z\ (\mathrm{mod}\, I)$.
De fato, se $x \equiv y\ (\mathrm{mod}\, I)$ e $y \equiv z\ (\mathrm{mod}\, I)$ então $(x - y) \in I$ e $(y - z) \in I$. Como I é fechado para a soma, temos que,

$$(x - y) + (x - z) \in I,$$

ou seja, $(x - z) \in I$. Portanto, $x \equiv z\ (\mathrm{mod}\, I)$.

Agora vamos indicar a classe de equivalência de x segundo a relação $x \equiv y\ (\mathrm{mod}\, I)$. Temos que,

$$\bar{x} = \{y \in A : y \equiv x\ (\mathrm{mod}\, I)\}.$$

Veja que

$$y \in \bar{x} \Leftrightarrow y \equiv x\ (mod\ I) \Leftrightarrow y = x + a,$$

para algum $a \in I$, logo,

$$\bar{x} = \{x + a : a \in I\}.$$

Chamaremos de **conjunto quociente** do anel *A* o conjunto denotado por A/I que é dado pela relação "$\equiv \pmod{I}$". Portanto,

$$A/I = \{x + I : x \in A\}.$$

O teorema a seguir nos ajudará a definir duas operações (soma e produto) sobre o conjunto A/I, com o intuído de torná-lo um anel.

Teorema 2.12 *Sejam A um anel e I um ideal de A, e tomemos* $x_1, x_2, y_1, y_2 \in A$. *Se* $x_1 \equiv x_2 \pmod{I}$ *e* $y_1 \equiv y_2 \pmod{I}$, *então*

(a) $\overline{x_1 + y_1} = \overline{x_2 + y_2}$ *ou* $(x_1 + y_1) + I = (x_2 + y_2) + I$.

(b) $\overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}$ *ou* $x_1 \cdot y_1 + I = x_2 \cdot y_2 + I$.

Demonstração: ***(a)*** Por hipótese, sabe-se que

$$x_1 = x_2 + a_1 \quad \text{e} \quad y_1 = y_2 + a_2,$$

com $a_1, a_2 \in I$. Somando as igualdades acima membro a membro, temos

$$x_1 + y_1 = x_2 + y_2 + (a_1 + a_2)$$

Como $a_1 + a_2 \in I$, segue que

$$(x_1 + y_1) - (x_2 + y_2) \in I \Leftrightarrow (x_1 + y_1) \equiv (x_2 + y_2)(mod\ I)$$

$$\Leftrightarrow \overline{x_1 + y_1} = \overline{x_2 + y_2}.$$

(b) Da hipótese temos que

$$x_1 = x_2 + a_1 \quad \text{e} \quad y_1 = y_2 + a_2,$$

Multiplicando as igualdades acima membro a membro, temos

$$x_1 \cdot y_1 = (x_2 + a_1) \cdot (y_2 + a_2)$$

$$= x_2 y_2 + x_2 a_2 + a_1 y_2 + a_1 a_2.$$

Como I é um ideal e $a_1, a_2 \in I$ então $x_2 y_2 + x_2 a_2 + a_1 y_2 + a_1 a_2 \in I$. Portanto,

$$x_1 \cdot y_1 \equiv (x_2 y_2) \pmod{I} \Leftrightarrow \overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}.$$

Teorema 2.13 *Sejam A um anel e I um ideal de A. Então,*

$$+ : {}^{A}/_{I} \times {}^{A}/_{I} \to {}^{A}/_{I} \qquad e \qquad \cdot : {}^{A}/_{I} \times {}^{A}/_{I} \to {}^{A}/_{I}$$

$$(\bar{x}, \bar{y}) \mapsto \bar{x} + \bar{y} = \overline{x + y} \qquad (\bar{x}, \bar{y}) \mapsto \bar{x} \cdot \bar{y}$$

definem duas operações de adição e multiplicação sobre ${}^{A}/_{I}$. Além disso, $\left({}^{A}/_{I}, +, \cdot\right)$ é um anel, chamado anel quociente de A por I.

Demonstração: Primeiramente vamos mostrar que os resultados das operações não dependem dos representantes de classes. Veja que, se $x_1, x_2, y_1, y_2 \in A$ e $\overline{x_1} = \overline{x_2}$ e $\overline{y_1} = \overline{y_2}$, então $x_1 \equiv x_2 \pmod{I}$ e $y_1 \equiv y_2 \pmod{I}$, então pelo teorema 2.12, temos

$$\overline{x_1 + y_1} = \overline{x_2 + y_2} \quad e \quad \overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}.$$

Agora veremos que ${}^{A}/_{I}$ satisfaz as propriedades de anel. Sejam $x, y, z \in A$,

i) $\bar{x} + (\bar{y} + \bar{z}) = \bar{x} + (\overline{y + z}) = \overline{x + (y + z)} = \overline{(x + y) + z} = \overline{(x + y)} + \bar{z} = (\bar{x} + \bar{y}) + \bar{z}$, ou seja, a soma é associativa;

ii) $\bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x}$. A soma é comutativa;

iii) Note que a classe $\bar{0}$ satisfaz $\bar{x} + \bar{0} = \overline{x + 0} = \bar{x} \ \forall\, x \in A$, logo $\bar{0} = 0_A$ é o elemento neutro da soma em ${}^{A}/_{I}$;

iv) Para todo $x \in A$, $\bar{x} + \overline{(-x)} = \overline{x + (-x)} = \bar{0}$. Logo o conjunto quociente possui elemento simétrico;

v) $\bar{x} \cdot (\bar{y} \cdot \bar{z}) = \bar{x} \cdot (\overline{y \cdot z}) = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = (\overline{x \cdot y}) \cdot \bar{z} = (\bar{x} \cdot \bar{y}) \cdot \bar{z}$, ou seja, o produto é associativo;

vi) $\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot (\overline{y + z}) = \overline{x \cdot (y + z)} = \overline{(x \cdot y) + (x \cdot z)} = \overline{(x \cdot y)} + \overline{(x \cdot z)} = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}$, isto é, a multiplicação é distributiva sobre a soma;

vii) $\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \cdot \bar{x}$, a multiplicação também é comutativa;

viii) $\bar{x} \cdot \bar{1} = \overline{x \cdot 1} = \bar{x}$, logo $\bar{1}$ é a unidade do anel ${}^{A}/_{I}$, além disso, $x + I = I \Leftrightarrow x \in I$.

Portanto $\left({}^{A}/_{I}, +, \cdot\right)$ é um anel comutativo com unidade.

Exemplo 2.31 Para cada $n \in \mathbb{N}$, $\langle n \rangle = n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. Como a relação de congruência módulo n sobre $\mathbb{Z}$ coincide com a relação " $\equiv (mod\ \langle n \rangle)$ ", então

$$\mathbb{Z}/_{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Teorema 2.14 *Sejam A um anel comutativo com unidade e M um ideal de A. Então M é maximal se, e somente se,* $A/_M$ *é um corpo.*

Demonstração: Vamos supor inicialmente que M é maximal, com isso vamos supor que todo elemento não nulo de $\bar{a} \in A/_M$ é invertível (note que $A/_M$ é comutativo com unidade). Seja $\bar{a} \in A/_M$, com $\bar{a} \neq \bar{0}$, e tomemos o ideal $\mathcal{J} = \langle a \rangle$. Assim, $M + \mathcal{J}$ é um ideal de A que contém M. Além disso, sendo $\bar{a} \neq \bar{0}$, então $a \notin M$, pois de acordo com o teorema 2.13,

$$\bar{a} = M \Leftrightarrow a \in M.$$

Como $a = a \cdot 1 \in \mathcal{J} \subset \mathcal{J} + M$, segue que $\mathcal{J} + M \neq M$. Por isso, M sendo maximal e $M \subset \mathcal{J} + M$, concluímos que

$$\mathcal{J} + M = A.$$

Com isso, existem $x \in \mathcal{J}$ e $y \in M$ tais que

$$1 = x + y,$$

pois $1 \in A$. Mas $x \in \mathcal{J}$ implica que $x = a \cdot b$, para algum $b \in A$. Portanto,

$$\bar{1} = \overline{ab} + \bar{y} = \overline{ab} + \bar{0} = \overline{ab},$$

desde que $y \in M$. A igualdade $\bar{1} = \overline{ab}$ nos diz que $\bar{a}$ é invertível e, por isso, $A/_M$ é corpo.

Reciprocamente, tomemos um ideal $\mathcal{J}$ de A tal que $M \subsetneq \mathcal{J}$. Logo existe $a \in \mathcal{J}$ com $a \neq M$, de modo que $\bar{a} \neq \bar{0}$. Como $A/_M$ é um corpo, existe $\bar{b} \in A/_M$ tal que

$$\bar{a} \cdot \bar{b} = \bar{1} \Leftrightarrow ab \equiv 1 (\text{mod } M) \Leftrightarrow ab = 1 + m_0,$$

com $m_0 \in M$, isto é,

$$1 = ab - m_0.$$

Como $a \in \mathcal{J}$, então $ab \in \mathcal{J}$. Também, $m_0 \in M$ implica que$m_0 \in \mathcal{J}$, pois $M \subset \mathcal{J}$. Logo $1 \in \mathcal{J}$, ou seja, $\mathcal{J} = A$.

Teorema 2.15 *Sejam A um anel comutativo com unidade e P um ideal de A. Então P é primo se, e somente se,* $^{A}/_{P}$ *é um domínio.*

Demonstração: Suponha que P é um ideal primo de A e sejam $\bar{a}, \bar{b} \in {}^{A}/_{P}$ tais que $\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{0}$, ou seja, $ab \in P$. Como P é primo,

$$a \in P \quad \text{ou} \quad b \in P,$$

ou seja, $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Portanto, $^{A}/_{P}$ é um domínio.

Reciprocamente, sejam $a, b \in A$ são tais que $ab \in P$. Logo, em $^{A}/_{P}$,

$$\overline{a \cdot b} = \bar{0} \quad \Rightarrow \quad \bar{a} \cdot \bar{b} = \bar{0} \quad \Rightarrow \quad \bar{a} = \bar{0} \quad \text{ou} \quad \bar{b} = \bar{0},$$

já que $^{A}/_{P}$ é um domínio. Assim, $a \in P$ ou $b \in P$. Com isso, concluímos que P é primo.

3. TEOREMA FUNDAMENTAL DOS HOMOMORFISMOS DE ANÉIS

O principal tema desse capítulo, e desse trabalho de modo geral, é mostrar e demonstrar que um anel A quocientado por um núcleo de uma função homomórfica é isomorfo a imagem dessa função. A partir desse teorema iremos abordar alguns exemplos e aplicações.

Teorema 3.1 (Fundamental dos Homomorfismos). *Seja $f : A \to B$ um homomorfismo de anéis. Então,*

$$A/_{\ker(f)} \simeq Im\,(f).$$

Demonstração: Inicialmente vamos definir uma função $\varphi : A/_{\ker(f)} \to Im(f)$, e mostrar que está bem definida:

$$\begin{aligned} \varphi \;:\; A/_{\ker(f)} &\to Im(f) \\ x + \ker(f) &\mapsto f(x). \end{aligned}$$

De fato, se $\bar{x}, \bar{y} \in A/_{\ker(f)}$ são tais que $\bar{x}, = \bar{y}$, então

$$x \equiv y \,(\mathrm{mod}\ker(f)),$$

ou seja, $x = y + a$, sendo $a \in \ker(f)$. Assim, $f(a) = 0_B$, de modo que

$$\begin{aligned} \varphi\,(\bar{x}) \;=\; f(x) \;&=\; f(y + a) \\ &= f(y) + f(a) \\ &= f(y) \\ &= \varphi(\bar{y}). \end{aligned}$$

Portanto, φ está bem definida. Agora vamos mostrar que a função é bijetora. Veja que

$$\varphi\,(\bar{x}) = \varphi\,(\bar{y}) \Rightarrow f(x) = f(y) \Rightarrow f(x) - f(y) = f(x - y) = 0_B.$$

Logo, $x - y \in \ker(f)$, isto é, $x = y + a$ para algum $a \in \ker(f)$. Com isso,

$$\bar{x} = \overline{y + a} = \bar{y} + \bar{a} = \bar{y},$$

já que $\bar{a} = \bar{0}$. Dessa forma, φ é injetora. Veja que φ é sobrejetora, pois dado $y \in Im(f)$, então $y = f(x)$ para $x \in A$, logo

$$\varphi\,(x + \ker(f)) = f(x) = y.$$

Para finalizar veremos que a função φ é um homomorfismo. Dados $\bar{x}, \bar{y} \in {}^{A}/_{\ker(f)}$, temos

$$\begin{aligned}\varphi\,(\bar{x} + \bar{y}) &= \varphi(\overline{x + y}) \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= \varphi\,(\bar{x}) + \varphi\,(\bar{y})\end{aligned}$$

e

$$\begin{aligned}\varphi\,(\bar{x} \cdot \bar{y}) &= \varphi\,(\overline{x \cdot y}) \\ &= f(x \cdot y) \\ &= f(x) \cdot f(y) \\ &= \varphi\,(\bar{x}) \cdot \varphi\,(\bar{y}).\end{aligned}$$

Portanto φ é um homomorfismo. Concluímos que φ é um isomorfismo, isto é, ${}^{A}/_{\ker(f)} \simeq Im\,(f)$.

Exemplo 3.1 A função $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(a) = \bar{a}$ é claramente um homomorfismo sobrejetor, chama-se **homomorfismo canônico**. Vamos mostrar que ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ é isomorfo a $\mathbb{Z}_n$.

Solução: Considere a função

$$\begin{aligned}\gamma : \quad {}^{\mathbb{Z}}/_{n\mathbb{Z}} &\to \mathbb{Z}_n \\ x + n\mathbb{Z} &\mapsto \bar{x}\end{aligned}$$

Sem muitas dificuldades vemos que γ está bem definida. Assim, dados $x + n\mathbb{Z}$ e $y + n\mathbb{Z}$ elementos quaisquer de ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$, temos

$$\begin{aligned}\gamma\,[(x + n\mathbb{Z}) + (x + n\mathbb{Z}) &= \gamma((x + y) + n\mathbb{Z}) \\ &= \overline{x + y} \\ &= \bar{x} + \bar{y}\end{aligned}$$

$$= \gamma(x + n\mathbb{Z}) + \gamma(y + n\mathbb{Z})$$

e

$$\gamma\,[(x + n\mathbb{Z}) \cdot (y + n\mathbb{Z})] = \gamma(xy + n\mathbb{Z})$$

$$= \overline{x \cdot y}$$

$$= \bar{x} \cdot \bar{y}$$

$$= \gamma\,(x + n\mathbb{Z}) \cdot \gamma\,(y + n\mathbb{Z})$$

Logo, γ é um homomorfismo. Agora, dado $\bar{x} \in \mathbb{Z}_n$ com $x \in \mathbb{Z}$, é claro que $x + n\mathbb{Z} \in {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ e $\gamma(x + n\mathbb{Z}) = \bar{x}$, ou seja, γ é sobrejetora. Por fim,

$$\gamma\,(x + n\mathbb{Z}) = \gamma(y + n\mathbb{Z}) \Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow x = y + kn, \text{ para algum } k \in \mathbb{Z}.$$

Por isso,

$$x + n\mathbb{Z} = (y + kn) + n\mathbb{Z}$$

$$= (y + n\mathbb{Z}) + (kn + n\mathbb{Z})$$

$$= y + n\mathbb{Z}.$$

isto é,

$$x + n\mathbb{Z} = y + n\mathbb{Z}.$$

Já que $kn + n\mathbb{Z} = n\mathbb{Z}$ e $n\mathbb{Z}$ é o zero do anel ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$. Isso mostra que γ é injetora e, com isso, concluímos que ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ é isomorfo a $\mathbb{Z}_n$.

Exemplo 3.2 Vamos considerar o anel

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

e seja I o seguinte ideal de A

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Vamos mostrar que ${}^{A}/_{I}$ é isomorfo ao corpo dos números reais.

Solução: Claramente A é subanel de $M_2(\mathbb{R})$. Tomando agora

$$z = \left\{ \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in A, \quad \text{com} \quad c, d \in \mathbb{R} \right\}$$

e sendo $x, y \in I$ tais que

$$x = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} \quad e \quad y = \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix}, \quad \text{com} \quad b_1, b_2, c, d \in \mathbb{R},$$

implica que

$$x - y = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in I,$$

e

$$z \cdot x = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & cb_1 \\ 0 & 0 \end{pmatrix} \in I.$$

Logo, I é um ideal de A. Agora vamos descrever os elementos do anel A/I. Dado

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A,$$

temos que

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}.$$

Sabendo que

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I,$$

então

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + I.$$

Ademais, para $a, b \in \mathbb{R}$,

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} + I$$

se, e somente se,

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a-b & b \\ 0 & a-b \end{pmatrix} \in I,$$

isto é, se, e somente se, $a - b = 0$, de modo que $a = b$. Logo,

$$A/_I = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + I : a \in \mathbb{R} \right\}.$$

Agora vamos verificar que a função $f : A \to \mathbb{R}$ dada, para qualquer

$$x = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A$$

por

$$f(x) = a,$$

é um homomorfismo, pois dados $x_1, x_2 \in A$ tais que

$$x_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \quad e \quad x_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix},$$

então

$$f(x_1 + x_2) = f\left(\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & a_1 + a_2 \end{pmatrix} \right)$$

$$= a_1 + a_2$$

$$= f(x_1) + f(x_2)$$

e

$$f(x_1 \cdot x_2) = f\left(\begin{pmatrix} a_1 \cdot a_2 & b_1 \cdot b_2 \\ 0 & a_1 \cdot a_2 \end{pmatrix} \right)$$

$$= a_1 \cdot a_2$$

$$= f(x_1) \cdot f(x_2).$$

Com isso, vemos que f é um homomorfismo que é claramente sobrejetor. Para finalizar, dado

$$x = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A,$$

então

$$x \in \ker(f) \Leftrightarrow f(x) = 0 \Leftrightarrow a = 0.$$

Logo,

$$\ker(f) = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in A : b \in \mathbb{R}\right\}$$

$$= I.$$

Portanto, pelo primeiro teorema do homomorfismo temos que

$$A/_I \simeq \mathbb{R}.$$

Exemplo 3.3 Mostrar que $\frac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \simeq M_2(\mathbb{Z}_n)$.

Solução: Dada a função,

$$\omega \;:\; M_2(\mathbb{Z}) \;\longrightarrow\; M_2(\mathbb{Z}_n)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\mapsto\; \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$$

veja que,

$$Im(\omega) = \left\{\omega \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{Z}\right\}$$

ou seja,

$$Im(\omega) = \left\{\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix};\ \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n\right\}$$

$$= M_2(\mathbb{Z}_n).$$

Mostraremos que ω é um homomorfismo. Dados, $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in M_2(\mathbb{Z})$ temos que

$$\omega\left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right) = \omega \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a_1 + a_2} & \overline{b_1 + b_2} \\ \overline{c_1 + c_2} & \overline{d_1 + d_2} \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a_1} + \overline{a_2} & \overline{b_1} + \overline{b_2} \\ \overline{c_1} + \overline{c_2} & \overline{d_1} + \overline{d_2} \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a_1} & \overline{b_1} \\ \overline{c_1} & \overline{d_1} \end{pmatrix} + \begin{pmatrix} \overline{a_2} & \overline{b_2} \\ \overline{c_2} & \overline{b_2} \end{pmatrix}$$

$$= \omega \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \omega \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

e

$$\omega\left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right) = \omega \begin{pmatrix} (a_1a_2 + b_1c_2) & (a_1b_2 + b_1d_2) \\ (c_1a_2 + d_1c_2) & (c_1b_2 + d_1d_2) \end{pmatrix}$$

$$= \begin{pmatrix} \overline{(a_1a_2 + b_1c_2)} & \overline{(a_1b_2 + b_1d_2)} \\ \overline{(c_1a_2 + d_1c_2)} & \overline{(c_1b_2 + d_1d_2)} \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a_1} & \overline{b_1} \\ \overline{c_1} & \overline{d_1} \end{pmatrix} \cdot \begin{pmatrix} \overline{a_2} & \overline{b_2} \\ \overline{c_2} & \overline{b_2} \end{pmatrix}$$

$$= \omega \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \omega \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Logo, ω é um homomorfismo. Agora veja que

$$\ker(\omega) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \, ; \, \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \right\}.$$

Temos que,

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \Leftrightarrow \bar{a}, \bar{b}, \bar{c}, \bar{d} = \bar{0}$$

$$\Leftrightarrow a, b, c, d \in n\mathbb{Z}$$

logo, $\ker(\omega) = M_2(n\mathbb{Z})$. Portanto, pelo teorema fundamental do homomorfismo de anéis,

$$\frac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \simeq M_2(\mathbb{Z}_n).$$

Corolário 3.1 (2º Teorema do isomorfismo) *Sejam B um subanel de um anel A e I um ideal de A. Então,*

$$B/_{B \cap I} \simeq {}^{B+I}/_{I}$$

Demonstração: Notemos que dados $b_1 + i_1, b_2 + i_2 \in B + I$ com $b_1, b_2 \in B$ e $i_1, i_2 \in I$ temos que

$$(b_1 + i_1)(b_2 + i_2) = b_1b_2 + b_1i_2 + i_1b_2 + i_1i_2 \quad \in B + I$$

e

$$(b_1 + i_1) - (b_2 + i_2) = b_1 - b_2 + i_1 - i_2 \quad \in B + I.$$

Sendo assim, $B + I$ é um subanel de A e I um ideal de A se, $x, y \in I$ e $b + i \in B + I$, onde $b \in B,\ i \in I$, então

$$x - y \in I$$

e

$$(b + i)x = bx + ix \ \in I.$$

Portanto, I é um ideal de $B + I$. Agora, se $x, y \in B \cap I$, com isso, tanto x, y pertence ao subanel B do anel A e daí resulta que $x - y \in B$, quanto x, y pertence a I, donde segue que $x - y \in I$. Como $x - y \in B$ e $x - y \in I$, então

$$x - y \in B \cap I.$$

Sejam $a \in B$ e $x \in B \cap I$, temos que $x \in B$ e $x \in I$ o que implica que $ax \in B,$ e $ax \in I$, já que por hipótese I é um ideal. Consequentemente,

$$ax \in B \cap I.$$

Logo, $B \cap I$ é um ideal de B. Agora considere a função

$$\begin{aligned} f : B &\to {}^{B+I}/_{I} \\ x &\mapsto x + I = \bar{x} \end{aligned}$$

Dados $x, y \in B + I$, temos

$$f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y)$$

e

$$f(x \cdot y) = \overline{x \cdot y} = \bar{x} \cdot \bar{y} = f(x) \cdot f(y).$$

Com isso, f é um homomorfismo. Por outro lado, se $\bar{x} \in {}^{B+I}/_{I}$, então $\bar{x} = x + I$, com $x = b + a$, em que $b \in B$ e $a \in I$. Logo,

$$\begin{aligned} \bar{x} &= (b + a) + I \\ &= (b + I) + (a + I) \end{aligned}$$

$$= b + I,$$

pois $a + I = I$. Portanto $f(b) = \bar{x}$ e, assim, f é sobrejetiva. Assim, segue que

$$B/_{\ker(f)} \simeq B + I/_{I}.$$

Para finalizar, dado $x \in B$, então sendo I o zero do anel quociente $B + I/_{I}$, temos

$$x \in \ker(f) \Leftrightarrow f(x) = I \Leftrightarrow x + I = I,$$

ou seja,

$$x \in \ker(f) \Leftrightarrow x \in I \quad \text{e} \quad x \in B \Leftrightarrow x \in B \cap I.$$

Portanto, $\ker(f) = B \cap I$. Consequentemente,

$$B/_{B \cap I} \simeq B + I/_{I}.$$

Corolário 3.2 (3º Teorema do Isomorfismo) *Sejam $\mathcal{J}$ e I ideais de um anel A onde $\mathcal{J} \subset I$. Então,*

$$\frac{A/_{\mathcal{J}}}{I/_{\mathcal{J}}} \simeq A/_{I}.$$

Demonstração: Vamos definir a função:

$$\begin{aligned} f : A/_{\mathcal{J}} &\longrightarrow A/_{I} \\ a + \mathcal{J} &\longmapsto a + I \end{aligned}$$

observe que f é um homomorfismo sobrejetor, pois dado $a + I \in A/_{I}$ e sabendo que $\mathcal{J} \subset I$, então existe $a + \mathcal{J}$ tal que $f(a + \mathcal{J}) = a + I$. Agora, dados $a_1 + \mathcal{J}$, $a_2 + \mathcal{J}$, temos

$$\begin{aligned} f\big((a_1 + \mathcal{J}) + (a_2 + \mathcal{J})\big) &= (a_1 + a_2) + \mathcal{J} \\ &= (a_1 + a_2) + I \\ &= (a_1 + I) + (a_2 + I) \\ &= f(a_1 + \mathcal{J}) + f(a_2 + \mathcal{J}) \end{aligned}$$

e

$$f((a_1 + \mathcal{J}) \cdot (a_1 + \mathcal{J}) = (a_1 a_2) + \mathcal{J}$$

$$= (a_1 a_2) + I$$

$$= (a_1 + I) + (a_2 + I)$$

$$= f(a_1 + \mathcal{J}) \cdot f(a_1 + \mathcal{J})$$

logo, f é um homomorfismo. Para finalizar, seja

$$a + \mathcal{J} \in \ker(f) \Leftrightarrow f(a + \mathcal{J}) = a + I = I$$

pois, $a + I = \{a + x \ ; \ x \in I\} = \{0 + x \ ; \ x \in I\}$, com isso, $a \in I$.

Daí,

$$\ker(f) = \{a + \mathcal{J} \ ; a \in I\} = {}^{I}/_{\mathcal{J}}.$$

Portanto,

$$\frac{{}^{A}/_{\mathcal{J}}}{{}^{I}/_{\mathcal{J}}} \simeq {}^{A}/_{I}.$$

4. CONCLUSÃO

Esse Trabalho foi elaborado com o intuito de mostrar a importância do estudo da álgebra abstrata e sua vasta aplicação na matemática. Além disso, foi visto que álgebra pode facilmente manter relações com algumas áreas, como Teoria do Números e Análise por exemplo, a fim de esclarecer e fundamentar a natureza de diversas estruturas.

A álgebra é uma área onde a abstração é predominante, pensando nisso, este trabalho tem como finalidade explicar de maneira objetiva e descomplicada, o conceito da estrutura anel e a construção de seus mais importantes subconjuntos, tendo um propósito ainda maior, compreender o teorema fundamental dos homomorfismos de anéis, com o auxílio de exemplificações para facilitar ainda mais o entendimento dessa relevante área da matemática superior.

REFERÊNCIAS

[1] VIEIRA, Vanbemberg Lopes. Álgebra Abstrata Para Licenciatura. 2ª ed. EDUEPB. Campina Grande – PB 2015.

[2] DOMINGUES, H. H. Álgebra Moderna. 4ª .ed. — São Paulo: Atual Editora, 2003.

[3] MILIES, César P. Breve História da Álgebra Abstrata. Universidade de São Paulo. Disponível em: http://www.bienasbm.ufba.br/M18.pdf. (Acessado em 15/11/2022).

[4] MILIES, César P. Unidades em Anéis de Grupos. Instituto de matemática pura e aplicada. Rio de Janeiro, 1998. Disponível em: http://www.impa.br/opencms/pt/biblioteca/mono/Mon58. (Acessado em 15/11/2022).

[5] SOUSA, Francilene Almeida. Espectro primo: uma aplicação de ideais primos e maximais. Cuité: CES, 2015.

[6] AIRES, José Maria de Queiroz. Os teoremas dos isomorfismos para. 2013.

[7] GARCIA, A. Lequain, Y. Elementos de Algebra. 6 ed. Rio de Janeiro: IMPA, 2012.

[8] JANESCH, Oscar Ricardo Álgebra I / Oscar Ricardo Janesch, Inder Jeet Taneja. – 2. ed. rev. – Florianópolis: UFSC/EAD/CED/CFM, 2011.