UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
(PROFMAT)

As Diferentes Faces dos Números Complexos

por Douglas Monteiro Caetano

Orientador: Prof. Dr. Laerte Bemm

Maringá - PR
2018

DOUGLAS MONTEIRO CAETANO

As Diferentes Faces dos Números Complexos

Dissertação de mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Laerte Bemm

Maringá - PR

2018

Dados Internacionais de Catalogação-na-Publicação (CIP)

Caetano, Douglas Monteiro.
C131d As diferentes faces dos números completos / Douglas Monteiro Caetano.--- Maringá (PR), 2018.
77 f.

Orientador: Prof. Dr. Laerte Bemm.
Dissertação (mestrado) – Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento Matemática. Programa de Mestrado Profissional em Matemática, 2018.

1. Complexos. 2. Polinômios. 3. Matrizes. 4. Anéis. 5. Ângulos Entre Matrizes. I. Bemm, Laerte, orient. II. Universidade Estadual de Maringá, Centro de Ciências exatas, Departamento de Matemática. Programa de Mestrado Profissional em Matemática. III. Título.

CDD 515.93

Rosângela A. A. Silva – CRB 9ª/1810

DOUGLAS MONTEIRO CAETANO

AS DIFERENTES FACES DOS NÚMEROS COMPLEXOS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Laerte Bemm

Prof. Dr. Laerte Bemm
DMA/Universidade Estadual de Maringá (Orientador)

Thaísa R. Tamusiunas

Profa. Dra. Thaísa Raupp Tamusiunas
Universidade Federal do Rio Grande do Sul

Fernanda Hernandez

Profa. Dra. Fernanda Diniz de Melo Hernandez
DMA/Universidade Estadual de Maringá

Aprovada em: 29 de junho de 2018.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

Agradecimentos

Ao concluir este trabalho quero agradecer:

Ao meu orientador Prof. Dr. Laerte Bemm pela orientação, paciência, sabedoria, incentivo, cumplicidade, compreender minhas dificuldades de deslocamento e trabalho, por acreditar em mim e pelas ótimas ideias.

A minha irmã Adriana Monteiro Caetano Alves que me confortou em momentos difíceis com suas sábias palavras e sempre apoiou minhas decisões.

A toda a minha família pelo incentivo e compreensão pelas minhas ausências.

A todos meus amigos que compartilharam horas de alegrias, risadas, preocupações e que me ajudaram sem medir esforços em momentos de necessidades.

A todos que de alguma forma contribuíram para a conclusão desse projeto.

Resumo

Neste trabalho apresentamos um estudo sobre o conjunto dos números complexos, o conjunto dos polinômios, o conjunto das matrizes e anéis que fundamentam o tema deste trabalho, as diferentes faces dos números complexos. Mostraremos que o anel dos polinômios com coeficientes reais quocientado pelo ideal $\langle x^2 + 1 \rangle$ e um anel das matrizes de entradas reais de ordem dois se comportam algebricamente como o conjunto dos números complexos. Por fim mostraremos que é possível definir ângulo entre matrizes que estão no subconjunto de matrizes citado anteriormente.

Palavras chaves: Complexos, Polinômios, Matrizes, Anéis, Ângulos Entre Matrizes.

Abstract

In this work we present a study on the set of complex numbers, the set of polynomials, the set of matrices and rings that base the theme of this work, the different faces of the complex numbers. We will show that the ring of polynomials with real coefficients quotient by the ideal $\langle x^2 + 1 \rangle$ and a ring of the order two matrices with real entries behave algebraically as the set of complex numbers. Finally we show that it is possible to define angle between matrices that are in the subset of matrices quoted above.

Key Words: Complex, Polynomials, Matrices, Rings, Angle Between Matrices.

Lista de Figuras

Sumário

Introdução

O primeiro momento em que se percebeu que o conjunto dos números reais não eram mais suficientes e que começou a surgir ideias sobre o conjunto dos números complexos foi na Itália, no século XVI, por meio de uma disputa entre Cardano e Tartaglia pela resolução da equação do 3° grau.

No século $XVII$, René Descartes, com o domínio da geometria analítica estudou as equações algébricas e em uma passagem do *Discurso do Método*, Descartes escreveu: "Nem sempre as raízes verdadeiras (positivas) ou falsas (negativas) de uma equação são reais. Às vezes elas são *imaginárias*". Devido a isto, até hoje o número $\sqrt{-1}$ é chamado de número *imaginário* e este se consagrou juntamente com a expressão "número complexo". Já no século $XVIII$, Leonhard Euler contribui significativamente com o estudo dos números complexos. Ele propôs a notação de $\sqrt{-1}$ por i [5].

A história por trás dos conceitos matemáticos amplia a percepção de como a matemática está interligada. Tal percepção é de grande importância para alcançar o sucesso de ensino aprendizagem. Devido a isso nosso objetivo é apresentar como os elementos do conjunto dos números complexos podem ser estudado além da forma de par ordenado, forma algébrica ou forma polar. Lembramos que estas são as três formas apresentadas em livros do ensino médio. Nós mostraremos que o conjunto dos números complexos pode ser associado ao conjunto de polinômios e ao conjunto de matrizes. Para isto nosso trabalho será dividido em três capítulos.

O primeiro capítulo é dedicado em apresentar o conjunto dos números complexos, forma algébrica, forma polar e "forma geométrica" de um número complexo. Também definimos ângulo entre números complexos. Em seguida estudamos os polinômios com coeficientes reais e o conjunto das matrizes. Apresentamos as principais operações e propriedades destes.

Já no segundo capítulo nosso objetivo é fazer um estudo sobre anéis, operações e isomorfismo de anéis com o intuito de provar que o anel dos polinômios com coeficiente reais quocientado por um ideal e um subanel de matrizes 2×2 com entradas reais, se comportam algebricamente como o conjunto dos números complexos.

Por fim, no terceiro capítulo iremos fazer um estudo sobre espaços vetoriais e produto interno de espaços vetoriais para mostrar que é possível definir ângulo entre duas matrizes. Mostramos também que o isomorfismo entre o corpo dos complexos e um subanel das matrizes 2×2 com entradas reais preserva ângulo.

Capítulo 1

Números Complexos, Polinômios e Matrizes

Ao falarmos da relação que existe entre o conjunto dos números complexos com os conjuntos dos polinômios e das matrizes, é importante apresentarmos cada um com uma visão algébrica. Por isso, neste capítulo apresentaremos as principais definições, propriedades e teoremas necessários para o desenvolvimento deste trabalho. Maiores detalhes sobre estes assuntos podem ser encontrados em [2], [3] e [5].

1.1 O Conjunto Dos Números Complexos

Nesta seção abordaremos o conjunto dos números complexos. Inicialmente apresentamos um número complexo como um par ordenado do conjunto $\mathbb{R} \times \mathbb{R}$. Em seguida daremos ao conjunto $\mathbb{R} \times \mathbb{R}$ uma estrutura algébrica de adição, multiplicação e produto por escalar.

Definição 1.1. *Considere o conjunto $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, ou seja,*

$$\mathbb{C} = \{(x, y);\ x \in \mathbb{R} \text{ e } y \in \mathbb{R}\}.$$

Sejam (a, b) e (c, d) dois elemento de $\mathbb{C}$ e λ uma constante real. Definimos:

1 - ***Igualdade.***

Diremos que (a, b) *é igual a* (c, d) *se, e somente se,* $a = c$ *e* $b = d$*. Ou simbolicamente,*

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

2 - ***Adição.***

A adição é uma operação $+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ *que associa a cada* $((a, b), (c, d)) \in \mathbb{C} \times \mathbb{C}$ *o elemento*

$$(a, b) + (c, d) = (a + c, b + d)$$

chamado soma de (a,b) e (c,d). Assim a soma de dois pares ordenados de $\mathbb{C}$ *resulta em um par ordenado, cuja a primeira e a segunda posição são, respectivamente, a soma das primeiras e das segundas posições dos pares iniciais.*

3 - ***Multiplicação.***

A multiplicação em $\mathbb{C}$ *é uma operação* $\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ *que associa a cada par* $(a, b), (c, d) \in \mathbb{C}$ *um único elemento*

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

chamado produto. Assim o resultado da multiplicação de dois pares ordenados de $\mathbb{C}$ *será o par ordenado cuja primeira posição será a diferença entre o produto das primeiras posições com as segundas posições e a segunda posição será a soma dos produtos da primeira posições de cada elemento dado com a segunda posição dos mesmos. Na maioria das vezes* $(a, b) \cdot (c, d)$ *é escrito por* $(a, b)(c, d)$*.*

4 - ***Multiplicação por uma escalar.***

O produto de um par ordenado $(a, b) \in \mathbb{C}$ *por uma constante* $\lambda \in \mathbb{R}$ *é dado por*

$$\lambda \cdot (a, b) = (\lambda a, \lambda b),$$

ou seja, cada posição é multiplicada pela constante λ*.*

O conjunto $\mathbb{C}$ com as operações anteriores é chamado de conjunto dos números complexos.

Para facilitar a escrita, representaremos, respectivamente, o número $(0,0)$ e o número $(1,0)$ por 0 e 1. Ainda, para cada número $z=(a,b)\in\mathbb{C}$, definimos

$$z' = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right), \text{ se } z \neq 0.$$

Também, para cada $z=(a,b)\in\mathbb{C}$ definimos

$$-z = (-a,-b).$$

Mostremos que as operações de adição e multiplicação definidas satisfazem várias propriedades que serão importantes no capítulo seguinte.

Proposição 1.2. *As seguintes propriedades se verificam para quaisquer z, w, $t \in C$:*

1 - $z+(w+t)=(z+w)+t$.

2 - $0+z=z+0=z$.

3 - $z+(-z)=(-z)+z=0$.

4 - $z+w=w+z$.

5 - $z(wt)=(zw)t$.

6 - *i)* $z(w+t)=zw+zt$.

ii) $(z+w)t=zt+wt$.

7 - $1z=z$.

8 - $zw=wz$.

9 - $zw=0 \Longrightarrow z=0$ *ou* $w=0$.

10 - $zz'=1$, *se* $z\neq 0$.

Demonstração: Consideremos $z,w,t\in\mathbb{C}$, em que $z=(a,b)$, $w=(c,d)$ e $t=(e,f)$, então:

1 -

$$\begin{array}{lcll}
z+(w+t) & = & (a,b)+((c,d)+(e,f)) & = \\
(a,b)+(c+e,d+f) & = & (a+(c+e),b+(d+f)) & = \\
(a+c+e,b+d+f) & = & ((a+c)+e,(b+d)+f) & = \\
(a+c,b+d)+(e,f) & = & ((a,b)+(c,d))+(e,f) & = \\
(z+w)+t. & & &
\end{array}$$

2 -

$$0+z=(0,0)+(a,b)=(0+a,0+b)=z.$$

Analogamente, $z+0=z$.

3 -

$$z+(-z)=(a,b)+(-a,-b)=(a+(-a),b+(-b))=(0,0)=0.$$

Analogamente, $(-z)+z=0$.

4 -

$$\begin{array}{rclclcl}
z+w & = & (a,b)+(c,d) & = & (a+c,b+d) & = & (c+a,d+b) \\
 & = & (c,d)+(a,b) & = & w+z. & &
\end{array}$$

5 -

$$\begin{aligned}
z(wt) &= (a,b)\cdot((c,d)\cdot(e,f))=(a,b)\cdot(ce-df,cf+de) \\
&= (a\cdot(ce-df)-b\cdot(cf+de),a\cdot(cf+de)+b\cdot(ce-df)) \\
&= (ace-adf-bcf-bde,acf+ade+bce-bdf) \\
&= ((ac-bd)\cdot e-(ad+bc)\cdot f,(ad+bc)\cdot e+(ac-bd)\cdot f) \\
&= ((ac-bd)-(ad+bc),(ad+bc)+(ac-bd))\cdot(e,f) \\
&= ((a,b)\cdot(c,d))\cdot(e,f)=(zw)t.
\end{aligned}$$

6 - $i)$

$$\begin{aligned}
z(w+t) &= (a,b)\cdot((c,d)+(e,f))=(a,b)\cdot(c+e,d+f) \\
&= (a\cdot(c+e)-b\cdot(d+f),a\cdot(d+f)+b(c+e)) \\
&= (ac+ae-bd-bf,ad+af+bc+be) \\
&= ((ac-bd)+(ae-bf),(ad+bc)+(af+be)) \\
&= (ac-bd,ad+bc)+(ae-bf,af+be) \\
&= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)=zw+zt.
\end{aligned}$$

ii)

$$\begin{aligned}
(z+w)t &= ((a,b)+(c,d))\cdot(e,f) = (a+c,b+d)\cdot(e,f)\\
&= ((a+c)\cdot e-(b+d)\cdot f,(a+c)\cdot f+(b+d)\cdot e)\\
&= (ae+ce-bf-df,af+cf+be+de)\\
&= ((ae-bf)+(ce-df),(af+be)+(cf+de))\\
&= (ae-bf,af+be)+(ce-df,cf+de)\\
&= (a,b)\cdot(e,f)+(c,d)\cdot(e,f)
\end{aligned}$$

7 -

$$1z=(1,0)\cdot(a,b)=(1a-0b,1b+0a)=(a,b)=z.$$

8 -

$$zw=(a,b)\cdot(c,d)=(ac-bd,ad+bc)=(ca-db,cb+da)=(c,d)\cdot(a,b)=wz$$

9 -

$$zw=0\Longrightarrow z=0 \text{ ou } w=0$$

i) Se $z=0$ ou $w=0$, nada temos a provar.

ii) Suponhamos então, sem perda de generalidade, que $z\neq 0$. No caso em que $b\neq 0$ temos:

$$zw=0\Rightarrow(a,b)(c,d)=(0,0)\Rightarrow(ac-bd,ad+bc)=(0,0)\Rightarrow$$
$$\left\{\begin{array}{rcl} ac-bd &=& 0\\ ad+bc &=& 0\end{array}\right.\Longrightarrow\left\{\begin{array}{rcr} ac &=& bd\ \text{(A)}\\ ad &=& -bc\ \text{(B)}\end{array}\right..$$

Multiplicando a equação (B) por c resulta:

$$\left\{\begin{array}{rcr} ac &=& bd\ \text{(E)}\\ (ac)d &=& -bc^2\ \text{(F)}\end{array}\right..$$

Substituindo a equação (E) na equação (F) temos:

$$bd^2=-bc^2$$

Do fato de $b\neq 0$, segue que,

$$d^2=-c^2,$$

e como c, $d \in \mathbb{R}$, concluímos que $c = d = 0$, como queríamos demonstrar. No caso em que $a \neq 0$, o resultado segue analogamente.

10 - Seja $z \neq 0$. Então, $a^2 + b^2 \neq 0$ e temos

$$\begin{aligned} zz' &= (a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) \\ &= \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2} \right) \\ &= \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2} \right) = (1,0) = 1. \end{aligned}$$

Como zz' resulta em 1, chamamos z' de **inverso multiplicativo** de z. Devido a isso, escrevemos

$$z' = z^{-1},$$

ou também $\frac{1}{z}$ ou $1/z$.

Com as operações de adição e multiplicação em $\mathbb{C}$, definimos as operações de subtração e divisão. Dados z, $w \in \mathbb{C}$ definimos

$$z - w = z + (-w)$$

e

$$\frac{z}{w} = zw^{-1}, \text{ sempre que } w \neq 0.$$

A potenciação também é definida em $\mathbb{C}$. Dado $z \in \mathbb{C}$ e $n \in \mathbb{Z}, n \geq 0$, definimos:

$$z^0 = 1, \quad z^1 = z, \quad z^2 = zz \quad \text{e} \quad z^n = zz^{n-1}.$$

Agora que definimos as operações em $\mathbb{C}$, podemos identificar qualquer número real x com o número complexo $(x, 0)$

Note que vendo x, $y \in \mathbb{R}$, como elemento de $\mathbb{C}$, temos:

$$x + y = (x,0) + (y,0) = (x+y, 0+0) = (x+y, 0) = x + y \qquad \text{e}$$

$$x \cdot y = (x,0) \cdot (y,0) = (x \cdot y - 0 \cdot 0, x \cdot 0 + 0 \cdot y) = (x \cdot y - 0, 0+0) = (x \cdot y, 0) = x \cdot y.$$

Analisemos agora o que ocorre com a potência $(0,1)^2$. Temos que:

$$(0,1)^2 = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -1,$$

ou seja, há um número complexo que elevado ao quadrado resulta em -1. O número complexo $(0,1)$ é denotado por i e é chamado de **algarismo imaginário**. Logo, concluímos que

$$i^2 = -1. \tag{1.1}$$

Portanto, para qualquer número complexo $z = (a,b) \in \mathbb{C}$ temos que

$$z = (a,b) = (a,0) + (0,b) = a \cdot (1,0) + b \cdot (0,1) = a + bi$$

A expressão anterior de z é chamada **forma algébrica** de z, no qual definimos que:

a é a parte real de z e denotamos por $a = Re(z)$.

b é a parte imaginária de z e denotamos por $b = Im(z)$.

Todo $z = (a,b) \in \mathbb{C} = \mathbb{R} \times \mathbb{R}$, pode ser representado geometricamente no plano cartesiano, o qual chamamos, simplesmente, de **plano complexo**. Este plano possui dois eixos orientados e ortogonais, em que o eixo horizontal recebe o nome de **eixo real** e o eixo vertical recebe o nome de **eixo imaginário**. Chamamos de **origem**, e denotamos por **O**, o ponto de interseção destes eixos.

A representação do número complexo $a + bi$ é dado por uma flecha de origem em **O** e ponto final no ponto A de coordenadas (a,b).

Exemplo 1.3. *Para o número complexo $z = 5 - 7i$, temos:*

$$Re(z) = 5 \quad e \quad Im(z) = -7$$

e sua representação geométrica é:

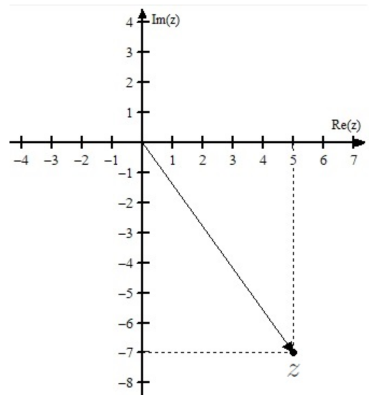


Figura 1.1: Exemplo 1.3.

Note que as operações de adição e multiplicação dos números complexos na forma algébrica são dadas por

$$\begin{aligned} z+w &= (a+bi)+(c+di) = a+bi+c+di = (a+c)+(b+d)i \\ &\text{e} \\ zw &= (a+bi)(c+di) = (ac+adi+bci+bdi^2) = (ac-bd)+(ad+cb)i. \end{aligned}$$

1.1.1 Conjugado

Considerando um número complexo $z = a + bi$, definimos como **conjugado de** z, e indicamos como $\overline{z}$, o número complexo que se obtém conservando a parte real e trocando-se o sinal da parte imaginária de z, ou seja, $\overline{z} = a - bi$.

Exemplo 1.4. *Vamos obter os conjugados de alguns números complexos e suas representações geométricas.*

a) $z = 8 - 2i \Longrightarrow \overline{z} = 8 + 2i.$

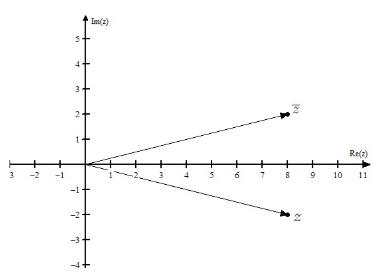


Figura 1.2: Exemplo 1.4 a).

b) $z = -3 + 4i \Longrightarrow \overline{z} = -3 - 4i.$

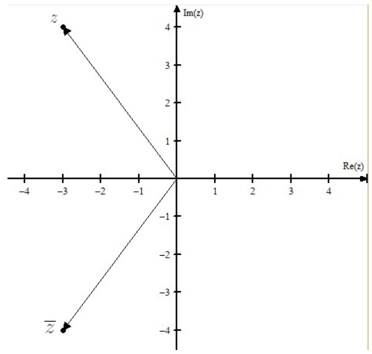


Figura 1.3: Exemplo 1.4 b).

c) $z = 5i \Longrightarrow \overline{z} = -5i.$

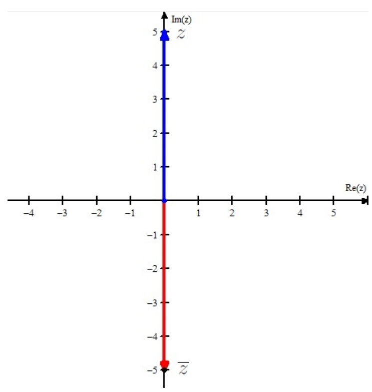


Figura 1.4: Exemplo 1.4 c).

Considerando z como uma flecha no plano complexo, $\overline{z}$ é obtido através da reflexão de z em relação ao eixo real.

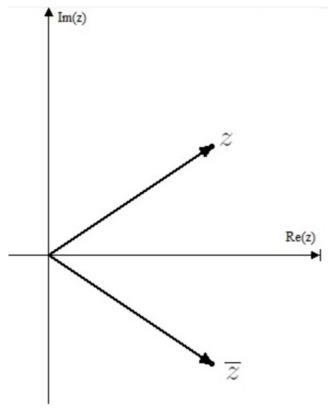


Figura 1.5: Representação de z e $\overline{z}$.

Proposição 1.5. *As seguintes propriedades se verificam para quaisquer z, $w \in \mathbb{C}$*

(a) $\overline{\overline{z}} = z$;

(b) $\overline{z \pm w} = \overline{z} \pm \overline{w}$;

(c) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

(d) $\overline{z/w} = \overline{z}/\overline{w}$, *se* $w \neq 0$;

(e) $z + \overline{z} = 2 \cdot Re(z)$ *e* $z - \overline{z} = 2i \cdot Im(z)$;

(f) $z \in \mathbb{R}$ *se e somente se* $\overline{z} = z$;

(g) z *é imaginário puro se e somente se* $\overline{z} = -z$.

Demonstração: Sejam $z = a + bi$, $w = c + di \in \mathbb{C}$.

(a) $\overline{\overline{z}} = z$.

De fato:

$\overline{\overline{z}} = \overline{\overline{a + bi}} = \overline{a - bi} = a + bi = z$

(b) $\overline{z \pm w} = \overline{z} \pm \overline{w}$.

Temos que:

$$
\begin{aligned}
\overline{z+w} &= \overline{(a+bi)+(c+di)} \\
&= \overline{(a+c)+(b+d)i} \\
&= (a+c)-(b+d)i \\
&= a-bi+c-di \\
&= \overline{z}+\overline{w}.
\end{aligned}
$$

e

$$
\begin{aligned}
\overline{z-w} &= \overline{(a+bi)-(c+di)} \\
&= \overline{(a-c)+(b-d)i} \\
&= (a-c)-(b-d)i \\
&= a-bi-(c+di) \\
&= \overline{z}-\overline{w}.
\end{aligned}
$$

(c) $\overline{z\cdot w}=\overline{z}\cdot\overline{w}$.

$$
\begin{aligned}
\overline{z\cdot w} &= \overline{(a+bi)\cdot(c+di)} \\
&= \overline{ac-bd+(ad+bc)i} \\
&= ac-bd-(ad+bc)i \\
&= ac+bdi^2-adi-bci \\
&= ac+bidi-adi-bci \\
&= a\cdot(c-di)-bi\cdot(c-di) \\
&= (a-bi)\cdot(c-di) \\
&= \overline{z}\cdot\overline{w}.
\end{aligned}
$$

(d) $\overline{z/w}=\overline{z}/\overline{w}$, se $w\neq 0$.

Seja $w\neq 0$, então:

$$
\begin{aligned}
\overline{z/w} &= \overline{zw^{-1}} \\
&= \overline{(a+bi)\cdot\left(\frac{c^2}{c^2+d^2}-\frac{d^2}{c^2+d^2}i\right)} \\
&= \overline{\left(a\cdot\frac{c^2}{c^2+d^2}-b\cdot\frac{d^2}{c^2+d^2}i^2\right)+\left(-a\cdot\frac{d^2}{c^2+d^2}+b\cdot\frac{c^2}{c^2+d^2}\right)i}
\end{aligned}
$$

$$= \left(a \cdot \frac{c^2}{c^2+d^2} + b \cdot \frac{d^2}{c^2+d^2}\right) - \left(-a \cdot \frac{d^2}{c^2+d^2} + b \cdot \frac{c^2}{c^2+d^2}\right) i$$

$$= \left(a \cdot \frac{c^2}{c^2+d^2} - (-b) \cdot \frac{d^2}{c^2+d^2}\right) + \left(a \cdot \frac{d^2}{c^2+d^2} - b \cdot \frac{c^2}{c^2+d^2}\right) i$$

$$= (a-bi) \cdot \left(\frac{c^2}{c^2+d^2} + \frac{d^2}{c^2+d^2} i\right)$$

$$= (\overline{z}) \left(\overline{w^{-1}}\right)$$

$$= \overline{z}/\overline{w}.$$

(e) $z + \overline{z} = 2 \cdot Re(z)$ e $z - \overline{z} = 2i \cdot Im(z)$.

$$\begin{aligned} z + \overline{z} &= a + bi + a - bi \\ &= (a+a) + (b-b)i \\ &= 2a \\ &= 2 \cdot Re(z). \end{aligned}$$

e

$$\begin{aligned} z - \overline{z} &= a + bi - (a - bi) \\ &= a + bi - a + bi \\ &= (a-a) + (b+b)i \\ &= 0 + 2bi \\ &= 2i \cdot Im(z). \end{aligned}$$

(f) $z \in \mathbb{R}$ se e somente se $\overline{z} = z$.

$\Rightarrow$) Se $z \in \mathbb{R}$ temos que $z = a + 0i$, com $a \in \mathbb{R}$. Assim:

$$z = a + 0i = a - 0i = \overline{z}.$$

$\Leftarrow$) Como $\overline{z} = z$, temos:

$$a + bi = a - bi.$$

Pela Definição 1.1, temos:

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

e da segunda equação concluímos que $b = 0$. Logo $z \in \mathbb{R}$.

(g) z é imaginário puro se e somente se $\overline{z} = -z$.

$\Rightarrow$) Se z é imaginário puro, temos que z é da forma $0 + bi$ para algum $b \in \mathbb{R}$. Assim:

$$\overline{z} = 0 - bi = -0 - bi = -z.$$

$\Leftarrow$) Como $\overline{z} = -z$, temos:

$$a - bi = -a - bi.$$

Pela Definição 1.1, segue que:

$$\begin{cases} a &= & -a \\ -b &= & -b \end{cases} \iff \begin{cases} 2a &= & 0 \Longrightarrow a = 0 \\ b &= & b \end{cases}.$$

Logo, temos que z é um número imaginário puro.

Definição 1.6. *O módulo de um número complexo $z = a + bi$ é definido por*

$$|z| = \sqrt{a^2 + b^2}.$$

Graficamente, o número real $|z|$ nos fornece a distância do ponto de coordenadas (a, b) no plano complexo até a origem. E ainda, $|z - w|$ é a distância entre os pontos do plano que representam z e w.

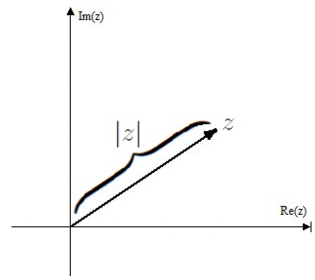


Figura 1.6: Representação gráfica do módulo de z.

Proposição 1.7. *As seguintes propriedades se verificam para quaisquer z, $w \in \mathbb{C}$:*

(a) $Re(z) \leq |Re(z)| \leq |z|$ *e* $Im(z) \leq |Im(z)| \leq |z|$;

(b) $|z|^2 = z\overline{z}$, $|\overline{z}| = |z|$ *e* $|zw| = |z||w|$;

(c) $|z/w| = |z|/|w|$, *se* $w \neq 0$;

(d) $|z+w| \leq |z| + |w|$ *(Desigualdade Triangular);*

(e) $|z+w| \geq ||z| - |w||$.

Demonstração: Sejam $z = a + bi$, $w = c + di \in \mathbb{C}$

(a) $Re(z) \leq |Re(z)| \leq |z|$ e $Im(z) \leq |Im(z)| \leq |z|$. Daí

$$Re(z) = a \leq |a| = |Re(z)| \Longrightarrow Re(z) \leq |Re(z)|$$

e

$$|Re(z)|^2 = |a|^2 = a^2 \leq a^2 + b^2 = |z|^2.$$

Disso, temos que $|Re(z)| \leq |z|$.

Portanto

$$Re(z) \leq |Re(z)| \leq |z|.$$

Analogamente, $Im(z) \leq |Im(z)| \leq |z|$.

(b) $|z|^2 = z\overline{z}$, $|\overline{z}| = |z|$ e $|zw| = |z||w|$.

Observe que

(1) $z\overline{z} = (a+bi)\cdot(a-bi) = a^2+b^2+abi-abi = a^2+b^2 = |z|^2$.

(2) $|\overline{z}| = |a-bi| = \sqrt{a^2+(-b)^2} = \sqrt{a^2+b^2} = |z|$.

(3)

$$
\begin{aligned}
|zw| &= |(a+bi)\cdot(c+di)| \\
&= |(ac-bd)+(ad+bc)i| \\
&= \sqrt{(ac-bd)^2+(ad+bc)^2} \\
&= \sqrt{(ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2} \\
&= \sqrt{a^2c^2+b^2d^2+a^2d^2+b^2c^2} \\
&= \sqrt{a^2(c^2+d^2)+b^2(c^2+d^2)} \\
&= \sqrt{(a^2+b^2)\cdot(c^2+d^2)} \\
&= \sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} \\
&= |z||w|.
\end{aligned}
$$

(c) $|z/w| = |z|/|w|$ se $w \neq 0$.

$$
\begin{aligned}
|z/w| &= |zw^{-1}| \\
&= \left|(a+bi)\cdot\left(\frac{c^2}{c^2+d^2} - \frac{-d^2}{c^2+d^2}i\right)\right| \\
&= \left|\left(a\frac{c^2}{c^2+d^2} + b\frac{d^2}{c^2+d^2}\right) + \left(a\frac{-d^2}{c^2+d^2} + b\frac{c^2}{c^2+d^2}\right)i\right| \\
&= \sqrt{\left(a\frac{c^2}{c^2+d^2} + b\frac{d^2}{c^2+d^2}\right)^2 + \left(a\frac{-d^2}{c^2+d^2} + b\frac{c^2}{c^2+d^2}\right)^2} \\
&= \sqrt{\frac{(ac^2+bd^2)^2+(a(-d^2)+bc^2)^2}{(c^2+d^2)^2}} \\
&= \sqrt{\frac{a^2c^4+2abc^2d^2+b^2d^4+a^2d^4-2abc^2d^2+b^2c^4}{(c^2+d^2)^2}}
\end{aligned}
$$

$$
\begin{aligned}
&= \sqrt{\frac{a^2c^4+b^2d^4+a^2d^4+b^2c^4}{(c^2+d^2)^2}} \\
&= \sqrt{\frac{c^4(a^2+b^2)+d^4(a^2+b^2)}{(c^2+d^2)^2}} \\
&= \sqrt{\frac{(a^2+b^2)\cdot(c^4+d^4)}{(c^2+d^2)^2}} \\
&= \sqrt{a^2+b^2}\cdot\sqrt{\frac{(c^2)^2+(d^2)^2}{(c^2+d^2)^2}} \\
&= \sqrt{a^2+b^2}\cdot\sqrt{\left(\frac{c^2}{c^2+d^2}\right)^2+\left(\frac{-d^2}{c^2+d^2}\right)^2} \\
&= |z||w|^{-1} \\
&= |z|/|w|.
\end{aligned}
$$

(d) $|z+w| \leq |z|+|w|$.

Inicialmente vamos verificar a validade da igualdade

$$|z+w|^2 = |z|^2 + 2Re(z\overline{w}) + |w|^2 \tag{1.2}$$

De fato, pelo item (b) desta proposição e a Proposição 1.5, temos que:

$$
\begin{aligned}
|z+w|^2 &= (z+w)\cdot\overline{(z+w)} \\
&= (z+w)\cdot(\overline{z}+\overline{w}) \\
&= z\overline{z}+z\overline{w}+w\overline{z}+w\overline{w} \\
&= z\overline{z}+z\overline{w}+\overline{z\overline{w}}+w\overline{w} \\
&= |z|^2+2Re(z\overline{w})+|w|^2.
\end{aligned}
$$

Pelos itens (a) e (b), temos

$$
\begin{aligned}
|z|^2+2Re(z\overline{w})+|w|^2 &\leq |z|^2+2|z\overline{w}|+|w|^2 \\
&= |z|^2+2|z||w|+|w|^2 \qquad (1.3)\\
&= (|z|+|w|)^2.
\end{aligned}
$$

Por (1.2) e (1.3), obtemos:

$$|z+w|^2 \leq (|z|+|w|)^2,$$

ou ainda,

$$|z+w| \leq |z|+|w|.$$

(e) $|z+w| \geq ||z|-|w||$.

Utilizando o item (d), temos que:

$$|z| = |z+w-w| \leq |z+w| + |-w| = |z+w| + |w|.$$

Logo

$$|z+w| \geq |z|-|w|.$$

Analogamente,

$$|w| = |w+z-z| \leq |z+w| + |-z| = |z+w| + |z|.$$

Portanto

$$|z+w| \geq |w|-|z|.$$

Pelo fato de que $||z|-|w|| = |z|-|w|$ se $|z| \geq |w|$ e $||z|-|w|| = |w|-|z|$ se $|w| \geq |z|$, podemos concluir que

$$|z+w| \geq ||z|-|w||.$$

Pela Proposição (1.7) (b) podemos verificar que se $z \neq 0$, então

$$|z|^2 = z\overline{z} \Longleftrightarrow \frac{1}{z} = \frac{\overline{z}}{|z|^2} \Longleftrightarrow z^{-1} = \frac{\overline{z}}{|z|^2}.$$

1.1.2 A forma polar

Seja $z = a+bi \in \mathbb{C}$, $z \neq 0$. Definimos o **argumento de** z, e denotamos por $arg(z)$, o ângulo θ formado pelo eixo real positivo com a flecha correspondente a z no sentido anti-horário.

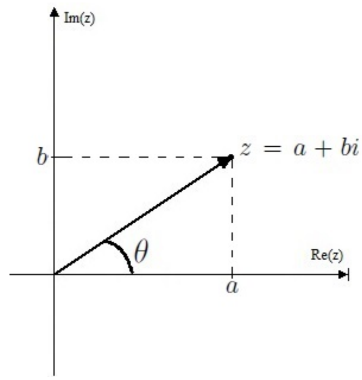


Figura 1.7: Representação do ângulo de z.

Se $z = a + bi$, então $a = |z| \cos\theta$ e $b = |z| \,\text{sen}\theta$ e daí temos que

$$z = |z|(\cos\theta + i\,\text{sen}\theta), \text{ com } \theta \in \mathbb{R}. \tag{1.4}$$

A Equação (1.4) é denominada uma **representação polar de** z. Como as funções $\cos\theta$ e $\text{sen}\theta$ são de período igual a $2k\pi$, para $k \in \mathbb{Z}$, temos que a Equação (1.4) continua sendo válida para $\theta + 2k\pi,\ k \in \mathbb{Z}$. Com isso, podemos afirmar que existem infinitos argumentos de z que satisfazem tal equação. Porém, no intervalo real $I = [\theta, \theta + 2\pi)$, existe um único argumento em I que satisfaz (1.4). Por conveniência, consideraremos $arg(z)$ no intervalo $[0, 2\pi)$.

Logo,

$$z = |z|(\cos arg(z) + i\,\text{sen}\, arg(z)) \tag{1.5}$$

é chamada a **forma polar de** z.

Para a demonstração da próxima proposição é importante relembrar que $\text{sen}(-\alpha) = -\,\text{sen}\,\alpha$ e $\cos(-\alpha) = \cos\alpha, \forall\alpha \in \mathbb{R}$.

Proposição 1.8. *Se $z \in \mathbb{C}$, $z \neq 0$, tem representação polar dado por $z = |z|(\cos\theta + i\,\text{sen}\theta)$, então*

$$z^{-1} = |z|^{-1}[cos(-\theta) + i\,\text{sen}(-\theta)]$$

Demonstração:

$$\begin{aligned}
z^{-1} &= \frac{1}{z} = \frac{1}{|z|(\cos\theta + i\,\text{sen}\theta)} \\
&= \frac{1}{|z|(\cos\theta + i\,\text{sen}\theta)} \cdot \frac{\cos\theta - i\,\text{sen}\theta}{\cos\theta - i\,\text{sen}\theta} \\
&= \frac{1}{|z|} \cdot \frac{\cos\theta - i\,\text{sen}\theta}{\cos^2\theta + \text{sen}^2\theta} \\
&= |z|^{-1} \cdot \frac{\cos\theta - i\,\text{sen}\theta}{1} \\
&= |z|^{-1}[\cos\theta - i\,\text{sen}\theta] \\
&= |z|^{-1}[\cos(-\theta) + i\,\text{sen}(-\theta)].
\end{aligned}$$

Proposição 1.9. *Sejam os números complexos $z \neq 0$ e $w \neq 0$, com suas respectivas representações polares:*

$$z = |z|(\cos\theta + i\,\text{sen}\theta) \quad e \quad w = |w|(\cos\omega + i\,\text{sen}\omega).$$

O produto de zw é dado por:

$$zw = |z||w|[\cos(\theta+\omega) + isen(\theta+\omega)].$$

Demonstração: De fato,

$$\begin{aligned}
zw &= |z|(\cos\theta + i\,\text{sen}\theta) \cdot |w|(\cos\omega + i\,\text{sen}\omega) \\
&= |z||w|(\cos\theta + i\,\text{sen}\theta)(\cos\omega + i\,\text{sen}\omega) \\
&= |z||w|[(\cos\theta\cos\omega - \text{sen}\theta\,\text{sen}\omega) + i(\cos\theta\,\text{sen}\omega + \text{sen}\theta\cos\omega)] \\
&= |z||w|[\cos(\theta+\omega) + isen(\theta+\omega)].
\end{aligned}$$

Corolário 1.10. *Se os números complexos $z \neq 0$ e $w \neq 0$, tem suas respectivas representações polares:*

$$z = |z|(\cos\theta + i\,\text{sen}\theta) \quad e \quad w = |w|(\cos\omega + i\,\text{sen}\omega),$$

então

$$\frac{z}{w} = \frac{|z|}{|w|}[\cos(\theta - \omega) + i\,\mathrm{sen}(\theta - \omega)]$$

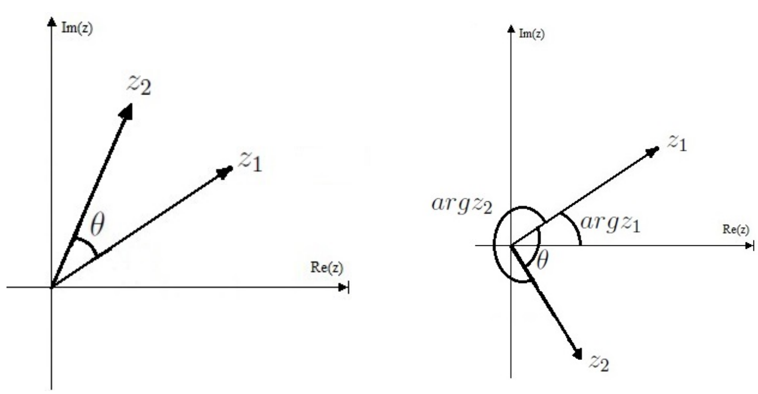
Demonstração: De fato,

$$\begin{aligned}
\frac{z}{w} &= \frac{|z|(\cos\theta + i\,\mathrm{sen}\theta)}{|w|(\cos\omega + i\,\mathrm{sen}\omega)} = \frac{|z|}{|w|} \cdot \frac{(\cos\theta + i\,\mathrm{sen}\theta)}{(\cos\omega + i\,\mathrm{sen}\omega)} \\
&= \frac{|z|}{|w|} \cdot \frac{(\cos\theta + i\,\mathrm{sen}\theta)}{(\cos\omega + i\,\mathrm{sen}\omega)} \cdot \frac{(\cos\omega - i\,\mathrm{sen}\omega)}{(\cos\omega - i\,\mathrm{sen}\omega)} \\
&= \frac{|z|}{|w|}\left[\frac{(\cos\theta\cos\omega + \mathrm{sen}\theta\,\mathrm{sen}\omega) + i(\mathrm{sen}\theta\cos\omega - \cos\theta\,\mathrm{sen}\omega)}{\cos^2\omega + \mathrm{sen}^2\omega}\right] \\
&= \frac{|z|}{|w|}[\cos(\theta - \omega) + i\,\mathrm{sen}(\theta - \omega)].
\end{aligned}$$

1.2 Ângulo Entre Números Complexos

Considere $z_1 = a + bi$, $z_2 = c + di$ dois números complexos e sejam A_1 de coordenadas (a, b) e A_2 de coordenadas (c, d).

Seja θ o ângulo entre A_1OA_2 cuja medida pertence a $[0, 180^o]$ ou $[0, \pi]$. O ângulo θ é definido como sendo o ângulo entre z_1 e z_2.



(a) $\theta = argz_2 - argz_1$ (b) $\theta = 2\pi - argz_2 + argz_1$

Figura 1.8: Possíveis ângulos entre números complexos.

1.3 Polinômios em uma Indeterminada

Esta seção tem como objetivo definir polinômios com coeficientes reais e suas operações de adição e multiplicação para a posterior demonstração de resultados importantes referentes a este trabalho.

Definição 1.11. *Sejam $\mathbb{R}$ o conjunto dos números reais. Cada soma formal finita do tipo $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, com $a_1, \ldots, a_n \in \mathbb{R}$, é chamado um polinômio na indeterminada x com coeficientes reais. Cada a_i é chamado coeficiente de $p(x)$. Se n é o maior natural tal que $a_n \neq 0$, n é chamado grau de $p(x)$, representado por $gr(p(x)) = n$. O coeficiente a_n é chamado coeficiente líder de $p(x)$. Quando o coeficiente líder é 1, o polinômio é dito mônico.*

O conjunto de todos os polinômios do tipo $a_0 + \cdots + a_nx^n$, com $a_i \in \mathbb{R}$, é denotado por $\mathbb{R}[x]$.

Definição 1.12. *Sejam $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{R}[x]$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in \mathbb{R}[x]$, com a_n, $b_n \neq 0$. Dizemos que $p(x)$ é igual a $q(x)$ se, e somente se, $a_0 = b_0, \;\; a_1 = b_1, \;\; \cdots, \;\; a_n = b_n$.*

Vamos definir uma operação de adição $+$ e uma operação de multiplicação $\cdot$ no conjunto $\mathbb{R}[x]$.

Definição 1.13. *Sejam $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{R}[x]$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in \mathbb{R}[x]$, com a_n, $b_m \neq 0$. Suponhamos $n \geq m$.*
Definimos a adição de $p(x)$ com $q(x)$ por

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n \in \mathbb{R}[x].$$

Definimos a multiplicação de $p(x)$ com $q(x)$ por

$$\begin{aligned} p(x) \cdot q(x) &= c_0 + c_1x + c_2x^2 + \cdots \in \mathbb{R}[x], \;\; \textit{em que} \\ c_k &= \sum_{k=i+j} a_ib_j = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0, \;\; k = 0, \ldots, n+m. \end{aligned}$$

Proposição 1.14. *Sejam $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in \mathbb{R}[x]$ tais que $a_n \neq 0$ e $b_m \neq 0$, isto é, $gr(p(x)) = n$ e $gr(q(x)) = m$. Então:*

(i) $gr(p(x)+q(x)) \leq max\{n,m\}$, *sempre que* $gr(p(x)+q(x)) \neq 0$.

(ii) $gr(p(x)q(x)) = m+n = gr(p(x)) + gr(q(x))$

Demonstração:

(i) Sem perda de generalidade, assuma que $n \geq m$. Assim,

$$\begin{aligned} 0 &\neq p(x)+q(x) \\ &= (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_m+b_m)x^m+\cdots+(a_n+b_n)x^n, \end{aligned}$$

onde acrescentamos coeficientes $b_j = 0$ para $j > m$, se for necessário. Se $a_n+b_n \neq 0$, então $gr(p(x)+q(x)) = n$, senão $gr(p(x)+q(x)) < n$. Portanto, $gr(p(x)+q(x)) \leq n = max\{n,m\}$

(ii) Como sabemos, $p(x)q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m}$, onde

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 \\ \vdots \\ c_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + \cdots + a_nb_m + a_{n+1}b_{m-1} + \cdots + a_{n+m-1}b_1 + a_{n+m}b_0 \end{cases}$$

Note que $c_{n+m} = a_nb_m$ e $a_nb_m \neq 0$. Logo, $gr(p(x)q(x)) = m+n = gr(p(x)) + gr(q(x))$

.

A seguir apresentamos duas definições e uma proposição que serão úteis em nosso trabalho.

Definição 1.15. *Seja* $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{R}[x]$. *Dizemos que um polinômios* $p(x)$ *é* ***nulo*** *quando todos os seus coeficientes são iguais a zero, ou seja,* $a_0 = a_1 = \cdots = a_n = 0$.

Definição 1.16. *Seja* $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{R}[x]$. *Chamamos de* ***oposto aditivo de*** $p(x)$ *o polinômio* $-p(x)$, *em que* $-p(x) = -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n$.

Proposição 1.17. *Para quaisquer* $p(x), q(x)$ *e* $r(x) \in \mathbb{R}[x]$, *temos que*

i) $p(x) + (q(x) + r(x)) = (p(x) + q(x)) + r(x)$;

ii) $p(x) + q(x) = q(x) + p(x)$;

iii) Existe $0 \in \mathbb{R}[x]$ *tal que,* $p(x) + 0 = 0 + p(x) = p(x)$;

iv) Existe o oposto aditivo de $p(x)$, *indicado por* $-p(x)$ *tal que* $p(x) + (-p(x)) = 0$;

v) $(p(x) \cdot q(x)) \cdot r(x) = p(x) \cdot (q(x) \cdot r(x))$;

vi) $p(x) \cdot (q(x) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x)$ *e*
$(q(x) + r(x)) \cdot p(x) = q(x) \cdot p(x) + r(x) \cdot p(x)$;

vii) $p(x) \cdot q(x) = q(x) \cdot p(x)$;

viii) $(k\,l)p(x) = k(l\,p(x))$, *para todos* $k, l \in \mathbb{R}$;

ix) $1 \cdot p(x) = p(x)$;

x) $k(p(x) + q(x)) = k\,p(x) + k\,q(x)$, *para todo* $k \in \mathbb{R}$;

xi) $(k + l)p(x) = k\,p(x) + l\,p(x)$, *para todos* $k, l \in \mathbb{R}$.

1.4 Matrizes

O objetivo desta seção é definirmos o conjunto das matrizes e suas operações para a posterior demonstração de resultados importantes referentes a este trabalho.

Iniciaremos falando de matrizes como um organização de informações, pois além de ordenar e simplificar problemas cotidianos também fornece novos métodos de resolução.

Definição 1.18. *Chamamos de* ***matriz*** *uma tabela de elementos dispostos em linhas e colunas.*

Por exemplo, ao anotarmos as médias bimestrais de um aluno na disciplinas de Matemática, Português e Ciências, podemos dispor em uma tabela.

	1° Bimestre	2° Bimestre	3° Bimestre	4° Bimestre
Matemática	5,0	4,5	6,2	5,9
Português	8,4	6,5	7,1	6,6
Ciência	9,0	7,8	6,8	8,6

Ao retirar os significados das linhas e colunas, temos o que se chama de matriz:

$$\begin{bmatrix} 5,0 & 4,5 & 6,2 & 5,9 \\ 8,4 & 6,5 & 7,1 & 6,6 \\ 9,0 & 7,8 & 6,8 & 8,6 \end{bmatrix}.$$

Para problemas com um número de variáveis e de observações muito grande, essa disposição ordenada dos dados em forma de matriz se torna indispensável.

Representamos uma matriz de m linhas e n colunas por

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \text{ em que cada } a_{ij} \in \mathbb{R}, \text{ com } 1 \leq i \leq m \text{ e } 1 \leq j \leq n.$$

O conjunto de todas as matrizes de m linhas e n colunas com entradas em valores reais é denotado por $\mathbb{M}_{m\times n}(\mathbb{R})$.

Utilizaremos letras maiúsculas para denotar matrizes, e quando quisermos especificar o número de linhas e colunas de uma matriz A escreveremos $A_{m\times n}$ em que m denota o número de linhas e n o número de colunas. Podemos utilizar parênteses para representar uma matriz. Por exemplo:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Também usamos a notação $A = [a_{ij}]_{m\times n}$ para indicar uma matriz de $\mathbb{M}_{m\times n}(\mathbb{R})$.

A próxima definição nos diz quando duas matrizes são iguais.

Definição 1.19. *Duas matrizes* $A_{m\times n} = [a_{ij}]_{m\times n}$ *e* $B_{r\times s} = [b_{ij}]_{r\times s}$ *são iguais,* $A = B$*, se elas têm o mesmo número de linhas* $(m = r)$ *e colunas* $(n = s)$*, e todos os seus elementos correspondentes são iguais* $(a_{ij} = b_{ij})$*.*

1.4.1 Alguns tipos especiais de matrizes

Entres as infinidades de matrizes que podemos escrever, existem as ditas especiais devido a sua frequente usabilidade. Aproveitamos esta seção para definir aquelas que serão utilizadas em nosso texto.

Consideremos a matriz $A_{m\times n}$ com entradas de números reais. Chamamos de:

Matriz quadrada aquela cujo número de linhas é igual ao número de colunas $(m = n)$.

Exemplo 1.20.

$$A_{3\times 3} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 2 & 3 & 5 \end{bmatrix}.$$

No caso de matrizes quadradas $A_{m\times m}$, costumamos dizer que A é uma matriz de ordem m.

Matriz nula aquela em que $a_{ij} = 0$, para todo i e j.

Exemplo 1.21.

$$A_{2\times 2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad B_{4\times 5} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Matriz identidade uma matriz quadrada em que $a_{ii} = 1$ e $a_{ij} = 0$, para $i \neq j$.

Exemplo 1.22.

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

1.4.2 Operações com matrizes

Quando trabalhamos com matrizes, pode ser necessário definirmos operações. Nesta seção definiremos algumas operações e propriedades que serão utilizadas em capítulos posteriores.

Definição 1.23. *A* ***adição*** *de duas matrizes de mesma ordem, $A_{m\times n} = [a_{ij}]$ e $B_{m\times n} = [b_{ij}]$, é uma matriz $m \times n$, que denotaremos $A + B$, cujos elementos são somas dos elementos correspondentes de A e B, isto é,*

$$A + B = [a_{ij} + b_{ij}].$$

Exemplo 1.24.

$$\begin{bmatrix} 1 & 3 & 5 \\ -1 & -3 & 5 \end{bmatrix} + \begin{bmatrix} 2 & 4 & 6 \\ 0 & 4 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 7 & 11 \\ -1 & 1 & 13 \end{bmatrix}.$$

Proposição 1.25. *Dadas as matrizes A, B e C de mesma ordem $m \times n$, temos:*

i) $A + B = B + A$.

ii) $A + (B + C) = (A + B) + C$.

iii) $A + 0 = A$, *em que* 0 *denota a matriz nula* $m \times n$.

Definição 1.26. *Seja $A = [a_{ij}]_{m\times n} \in \mathbb{M}_{m\times n}(\mathbb{R})$ e k um número real. Definimos a* ***multiplicação*** *de A por k como a matriz denotada por $k \cdot A$ e dada por*

$$k \cdot A = [ka_{ij}]_{m\times n}.$$

Exemplo 1.27.

$$-3 \cdot \begin{bmatrix} 1 & -3 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} -3 & 9 \\ 6 & -15 \end{bmatrix}.$$

Definição 1.28. *Dada uma matriz $A = [a_{ij}]_{m\times n}$, podemos obter uma outra matriz $A^t = [b_{ij}]_{n\times m}$, cujas linhas são as colunas de A, isto é, $b_{ij} = a_{ji}$. A^t é denominada* ***transposta*** *de A.*

Exemplo 1.29. *Se* $A = \begin{bmatrix} 2 & 0 \\ 3 & 1 \\ -5 & -7 \end{bmatrix}$, *então* $A^t = \begin{bmatrix} 2 & 3 & -5 \\ 0 & 1 & -7 \end{bmatrix}$.

Definição 1.30. *Sejam* $A = [a_{ij}]_{m\times n}$ *e* $B = [b_{rs}]_{n\times p}$. *Definimos a* ***multiplicação da matriz*** A ***pela matriz*** B *como* $AB = [c_{uv}]_{m\times p}$ *onde*

$$c_{uv} = \sum_{k=1}^{n} a_{uk}b_{kv} = a_{u1}b_{1v} + \cdots + a_{un}b_{nv}.$$

A matriz AB *é chamada matriz produto de* A *por* B.

Observações:

i) Só podemos efetuar o produto de duas matrizes $A_{m\times n}$ e $B_{l\times p}$ se o número de colunas da primeira for igual ao número de linhas da segunda, isto é, $n = l$. Além disso, a matriz resultado $C = AB$ será de ordem $m \times p$.

ii) O elemento c_{ij} (i-ésima linha e j-ésima coluna da matriz-produto) é obtido, multiplicando os elementos da i-ésima linha da primeira matriz pelos elementos correspondentes da j-ésima coluna da segunda matriz, e somando estes produtos.

Exemplo 1.31.

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}_{2\times 3} \cdot \begin{bmatrix} -1 & 2 \\ 0 & 1 \\ -3 & 1 \end{bmatrix}_{3\times 2} = \begin{bmatrix} 1\cdot(-1)+2\cdot 0+3\cdot(-3) & 1\cdot 2+2\cdot 1+3\cdot 1 \\ 4\cdot(-1)+5\cdot 0+6\cdot(-3) & 4\cdot 2+5\cdot 1+6\cdot 1 \end{bmatrix}_{2\times 2}$$
$$= \begin{bmatrix} -10 & 7 \\ -22 & 19 \end{bmatrix}_{2\times 2}.$$

Definição 1.32. *Seja uma matriz quadrada* $A = [a_{ij}]_m \in \mathbb{M}_m(\mathbb{R})$. *Definimos o* ***traço da matriz*** A, *denotando por* $tr(A)$, *como a soma dos elementos da diagonal principal, ou ainda,*

$$tr(A) = a_{11} + \cdots + a_{mm}.$$

Exemplo 1.33. *Para* $A = \begin{bmatrix} 1 & 3 \\ 5 & 13 \end{bmatrix}$, *o traço é dado por*

$$tr(A) = 1 + 13 = 14.$$

Proposição 1.34. *Considere as matrizes quadradas* $A = [a_{ij}]_m$ *e* $B = [b_{ij}]_m$, *e a matriz identidade* I_n, *temos que:*

i) $tr(A) = tr(A^t)$.

ii) $tr(I_n) = n$.

iii) $tr(kA) = k \cdot tr(A)$.

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

Demonstração: Omitiremos as demonstrações por não serem difíceis.

Capítulo 2

Anéis

Neste capítulo faremos uma fundamentação teórica para mostrar que um "subconjunto" dos polinômios de coeficientes reais e que um subconjunto das matrizes de entradas reais de ordem dois por dois se comportam algebricamente como o conjunto dos números complexos.

Para facilitar o entendimento deste capítulo é importante que o leitor tenha conhecimento sobre noções de conjuntos, tais como: subconjuntos, complementar, intersecção, união, etc.

Maiores detalhes podem ser encontrados em [1] e [6].

Consideremos os conjunto $A = \{1, 2, 3, 5\}$ e $B = \{2, 3, 5\}$. O produto cartesiano A com B é o conjunto

$$A \times B = \{(1, 2), (1, 3), (1, 5), (2, 2), (2, 3), (2, 5), (3, 2)(3, 3), (3, 5), (5, 2), (5, 3), (5, 5)\}.$$

Seja R o subconjunto de $A \times B$ formado pelos pares ordenados de números primos, isto é,

$$R = \{(2, 2), (2, 3), (2, 5), (3, 2), (3, 3), (3, 5), (5, 2), (5, 3), (5, 5)\}.$$

Podemos ver que para um par ordenado de $A \times B$ estar em R é necessário e suficiente que ele satisfaça a condição de que o primeiro e o segundo elementos do par ordenado sejam primos. Porém ao invés de dizer que um par ordenado (a, b) pertence a R, vamos dizer que a e b estão relacionados e vamos escrever aRb para indicar este fato (a está relacionado com b se, e somente se, a e b são primos).

Motivados por isto vamos formalizar a definição de relação.

Definição 2.1. *Sejam A e B dois conjuntos não vazios. Todo subconjunto $R \subset A \times B$ é chamado uma **relação** de A em B. Para um elemento qualquer $(a, b) \in R$, dizemos que a está **relacionado** com b e usamos a notação aRb.*

No caso em que $A = B$ dizemos que $R \subset A \times A$ é uma **relação** em A.

2.1 Conjunto Quociente

Nesta seção definiremos relações de equivalência, classe de equivalência e conjunto quociente. Este será de grande importância mais adiante.

Na definição a seguir, veremos quando uma relação é considerada relação de equivalência.

Definição 2.2. *Seja A um conjunto e R uma relação em A. Dizemos que R é uma relação de equivalência quando, para quaisquer a, b, $c \in A$, verifica-se:*

i) aRa (reflexiva).

ii) $aRb \Rightarrow bRa$ (simétrica).

iii) aRb, $bRc \Rightarrow aRc$ (transitiva).

Quando a relação R é de equivalência, utilizamos o símbolo $\sim$.

Exemplo 2.3. *A relação $\sim$ em $\mathbb{Z}$ (conjunto dos números inteiros) definida por*

$$x \sim y \Longleftrightarrow x^2 + 1 = y^2 + 1$$

é uma relação de equivalência em $\mathbb{Z}$.

Com efeito, quaisquer x, y, $z \in \mathbb{Z}$, temos:

i) $x \sim x$, pois $x^2 + 1 = x^2 + 1$.

ii) $x \sim y \Longrightarrow x^2 + 1 = y^2 + 1 \Longrightarrow y^2 + 1 = x^2 + 1 \Longrightarrow y \sim x.$

iii) $x \sim y$ *e* $y \sim z \Longrightarrow x^2+1 = y^2+1$ *e* $y^2+1 = z^2+1 \Longrightarrow x^2+1 = z^2+1 \Longrightarrow x \sim y.$

Portanto a relação $\sim$ *em* $\mathbb{Z}$ *é uma relação de equivalência em* $\mathbb{Z}$.

Definição 2.4. *Dados um conjunto* A *e uma relação de equivalência* $\sim$ *em* A*, o conjunto*

$$\bar{x} := \{a \in A; a \sim x\}$$

é denominado ***classe de equivalência*** *do elemento* x, $\forall x \in A$.

Proposição 2.5. *Seja* $\sim$ *uma relação de equivalência num conjunto não vazio* A.

i) *Toda classe de equivalência é não vazia.*

ii) *Duas classes de equivalências distintas são disjuntas.*

iii) *A união de todas as classes de equivalência é o próprio conjunto* A.

A demonstração encontra-se no livro [6], página 09.

Definição 2.6. *Seja* $\sim$ *uma relação de equivalência em um conjunto* A*. Chamamos de* ***conjunto quociente*** *de* A *pela relação de equivalência* $\sim$*, e denotamos por* $\dfrac{A}{\sim}$*, ao conjunto de todas as classes de equivalência relativamente a relação* $\sim$*. Assim*

$$\frac{A}{\sim} = \{\bar{x}; x \in A\}.$$

Exemplo 2.7. *Seja o conjunto* $A = \{0, 1, 2, 3\}$ *e consideremos a relação*

$$\sim = \{(0,0), (1,1), (2,2), (3,3), (0,2), (2,0), (1,3), (3,1)\}.$$

É fácil ver que $\sim$ *é uma relação de equivalência. As classes de equivalência são:*

$$\begin{array}{lllll}
\overline{0} & = & \{x \in A; x \sim 0\} & = & \{0,2\}. \\
\overline{1} & = & \{x \in A; x \sim 1\} & = & \{1,3\}. \\
\overline{2} & = & \{x \in A; x \sim 2\} & = & \{2,0\}. \\
\overline{3} & = & \{x \in A; x \sim 3\} & = & \{3,1\}.
\end{array}$$

Note que a classe $\overline{0}$ *possui os mesmos elementos que a classe* $\overline{2}$*. O mesmo ocorre com as classes* $\overline{1}$ *e* $\overline{3}$.

Logo,

$$\frac{A}{\sim} = \{\overline{0}, \overline{1}\} = \{\{0,2\}, \{1,3\}\}.$$

Exemplo 2.8. *Considere $A = \mathbb{Z}$ e a relação de equivalência $\sim$ dada por:*

$$\forall\ x, y \in \mathbb{Z},\ x \sim y \Leftrightarrow y - x = 4n,\ \textit{para algum } n \in \mathbb{Z},$$

ou seja,

$$x \sim y \Leftrightarrow y = 4n + x \textit{ para algum } n \in \mathbb{Z}.$$

Disso, temos que

$$\begin{aligned}
\overline{0} &= \{y \in \mathbb{Z}; 0 \sim y\} &&= \{y \in \mathbb{Z}; y = 4n + 0, n \in \mathbb{Z}\}\\
&= \{4n; n \in \mathbb{Z}\} &&= \{0, \pm 4, \pm 8, \pm 12, \ldots\}.\\
\overline{1} &= \{y \in \mathbb{Z}; 1 \sim y\} &&= \{y \in \mathbb{Z}; y = 4n + 1, n \in \mathbb{Z}\}\\
&= \{4n + 1; n \in \mathbb{Z}\} &&= \{\ldots, -11, -7, -3, 1, 5, 9, \ldots\}.\\
\overline{2} &= \{y \in \mathbb{Z}; 2 \sim y\} &&= \{y \in \mathbb{Z}; y = 4n + 2, n \in \mathbb{Z}\}\\
&= \{4n + 2; n \in \mathbb{Z}\} &&= \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\}.\\
\overline{3} &= \{y \in \mathbb{Z}; 3 \sim y\} &&= \{y \in \mathbb{Z}; y = 4n + 3, n \in \mathbb{Z}\}\\
&= \{4n + 3; n \in \mathbb{Z}\} &&= \{\ldots, -9, -5, -1, 3, 7, 11, \ldots\}.\\
\overline{4} &= \{y \in \mathbb{Z}; 4 \sim y\} &&= \{y \in \mathbb{Z}; y = 4n + 4, n \in \mathbb{Z}\}\\
&= \{4(n + 1); n \in \mathbb{Z}\}\\
&= \{0, \pm 4, \pm 8, \pm 12, \ldots\}\\
&= \overline{0}.
\end{aligned}$$

Observe que para qualquer $y \in \mathbb{Z}$, temos que $y = 4n$, $y = 4n + 1$, $y = 4n + 2$ ou $y = 4n + 3$. Logo, as distintas classes de equivalência podem ser representadas por $\overline{0}$, $\overline{1}$, $\overline{2}$ ou $\overline{3}$, e $\dfrac{\mathbb{Z}}{\sim} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

2.2 Anel

Nesta seção mostraremos as propriedades necessárias que um conjunto deve cumprir para ser chamado de anel. Definiremos também subanéis e ideais.

Definição 2.9. *Seja A um conjunto não vazio onde estão definidas duas operações, as quais chamaremos de adição e multiplicação em A e as denotaremos, respectivamente, por $+$ e $\cdot$.*

$$
\begin{aligned}
+ : A \times A &\to A \\
(a,b) &\mapsto a+b
\end{aligned}
\qquad\qquad
\begin{aligned}
\cdot : A \times A &\to A \\
(a,b) &\mapsto a \cdot b
\end{aligned}
$$

Dizemos que $(A, +, \cdot)$ *é um anel se as seguintes 6 propriedades são verificadas*

1 - *Associatividade da adição:*

$$\forall\ a, b, c \in A,\ (a+b)+c = a+(b+c).$$

2 - *Existência de elemento neutro para a adição:*

$$\exists\ 0 \in A \ \textit{tal que} \ \forall\ a \in A,\ a+0 = 0+a = a.$$

3 - *Existência de oposto aditivo:*

$\forall a \in A$, *existe um único* $y \in A$, *denotado por* $y = -a$, *tal que*

$$a + y = y + a = 0.$$

4 - *Comutatividade da adição:*

$$\forall\ a, b \in A,\ a+b = b+a.$$

5 - *Associatividade da multiplicação:*

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

6 - *Distributividade à esquerda e à direita:*

$\forall\ a, b, c \in A$,

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

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

A seguir apresentamos uma propriedade que decorre da definição de anel.

Proposição 2.10. *Seja* $(A, +, \cdot)$ *um anel e* $a, b \in A$. *Então, são satisfeitas:*

1 - $a0 = 0a = 0$.

2 - $a(-b) = (-a)b = -ab$.

3 - $(-a)(-b) = ab$.

Exemplo 2.11. *Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ com as operações usuais são anéis.*

Exemplo 2.12. *Como verificado na Proposição 1.2, o conjunto $\mathbb{C}$ dos números complexos é um anel.*

Exemplo 2.13. *Como visto no capítulo 1 o conjunto dos polinômios com coeficientes reais são exemplos de anéis.*

Exemplo 2.14. *É possível verificar, por meio de cálculos exaustivos, que o conjunto $\mathbb{M}_{n\times n}(\mathbb{R})$ das matrizes de ordem n, com entradas reais e as operações definidas no capítulo anterior, é um anel.*

Exemplo 2.15. *Considere o conjunto $F(\mathbb{R})$ de todas as funções $f : \mathbb{R} \to \mathbb{R}$, a adição de funções definida por*

$$(f + g)(x) = f(x) + g(x), \forall\ x \in \mathbb{R},$$

e a multiplicação dada por

$$(g \cdot f)(x) = g(f(x)), \forall\ x \in \mathbb{R}.$$

Então $(F(\mathbb{R}), +, \cdot)$ não é um anel.

Vamos mostrar que a propriedade 6, da distributividade, não é válida.

De fato, seja f, g, $h \in F(\mathbb{R})$, definidas por $f(x) = a \cdot x + b$, com a, $b \in \mathbb{R} - \{0\}$, $g(x) = a \cdot x^2$ e $h(x) = b \cdot x$. Então, $\forall\, x \in \mathbb{R}$

$f(g + h)(x) = f(g(x) + h(x)) = a \cdot (g(x) + h(x)) + b = a \cdot (g(x)) + a \cdot (h(x)) + b = a^2x^2 + abx \neq a \cdot (g(x)) + b + a \cdot (h(x)) + b = f(g(x)) + f(h(x)) = (fg)(x) + (fh)(x)$.

Exemplo 2.16. *Consideremos o conjunto $2\mathbb{Z} = \{p = 2k; k \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ dos número inteiros pares, com adição e multiplicação usuais. Vamos verificar se $(2\mathbb{Z}, +, \cdot)$ é um anel.*

De fato, para todo $a = 2k$, $b = 2k'$, $c = 2k'' \in 2\mathbb{Z}$, com k, k', $k'' \in \mathbb{Z}$ temos:

1 - *Associativa da adição:*

$$\begin{aligned}(a+b)+c &= (2k+2k')+2k'' &&= 2(k+k')+2k''\\ &= 2((k+k')+k'') &&= 2(k+k'+k'')\\ &= 2(k+(k'+k'')) &&= 2k+2(k'+k'')\\ &= 2k+(2k'+2k'') &&= a+(b+c).\end{aligned}$$

2 - *Existência de elemento neutro para a adição:*

$0 = 2\cdot 0 \in 2\mathbb{Z}$, *logo*

$$a+0 = 2k+0 = 0+2k = 2k = a.$$

3 - *Existência do oposto aditivo:*

Para todo $a \in 2\mathbb{Z}$ *temos:*

$$a+x=0 \Leftrightarrow 2k+x=0 \Leftrightarrow x=-2k \Leftrightarrow x=2(-k).$$

Como $-k \in \mathbb{Z}$ *concluímos que* $2(-k) \in 2\mathbb{Z}$, *e ainda,* $2(-k) = -2k = -(2k) = -a$. *Mostrando que existe um único elemento* $-a \in 2\mathbb{Z}$ *tal que*

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

4 - *Comutatividade da adição:*

$$a+b = 2k+2k' = 2(k+k') = 2(k'+k) = 2k'+2k = b+a.$$

5 - *Associatividade da multiplicação:*

$$(a\cdot b)\cdot c = (2k\cdot 2k')\cdot 2k'' = 2k\cdot 2k'\cdot 2k'' = 2k\cdot(2k'\cdot 2k'') = a\cdot(b\cdot c).$$

6 - *Distributividade à esquerda e à direita:*

$$\begin{aligned}a\cdot(b+c) &= 2k\cdot(2k'+2k'') &&= 2k\cdot(2\cdot(k'+k''))\\ &= 2\cdot 2(k\cdot(k'+k'')) &&= 2\cdot 2(kk'+kk'')\\ &= 2\cdot 2kk'+2\cdot 2kk'' &&= 2k\cdot 2k'+2k\cdot 2k''\\ &= a\cdot b+a\cdot c.\end{aligned}$$

$$
\begin{aligned}
(a+b)\cdot c &= (2k+2k')\cdot 2k'' &&= 2(k+k')\cdot 2k'' \\
&= 2\cdot 2\cdot((k+k')\cdot k'') &&= 2\cdot 2\cdot(kk''+k'k'') \\
&= 2\cdot 2kk''+2\cdot 2k'k'' &&= 2k\cdot 2k''+2k'\cdot 2k'' \\
&= a\cdot c+b\cdot c.
\end{aligned}
$$

Assim, concluímos que $(2\mathbb{Z},+,\cdot)$ *é um anel.*

Exemplo 2.17. *O conjunto* $I=\{\ldots,-5,-3,-1,1,3,5,\ldots\}$ *dos números inteiros ímpares, com adição e multiplicação usuais **não é um anel**, pois não satisfaz o item* 2 *da Definição de anel, ou seja,* $0\notin I$.

Exemplo 2.18. *O conjunto* $I\cup\{0\}=\{2k+1; k\in\mathbb{Z}\}\cup\{0\}=\{\cdots,-5,-3,-1,0,1,3,5,\cdots\}$ *com adição e multiplicação usuais **é um anel** ?*
Considere $a=2k+1$, $b=2k'+1$, $c=2k''+1\in I\cup\{0\}$, *com* k, k', $k''\in\mathbb{Z}$. *Verificaremos se as propriedades da Definição* 2.9 *estão satisfeitas.*

1 - *Associativa da adição:*

$$
\begin{aligned}
(a+b)+c &= (2k+1+2k'+1)+2k''+1 &&= 2k+1+2k'+1+2k''+1 \\
&= 2k+1+(2k'+1+2k''+1) &&= a+(b+c).
\end{aligned}
$$

2 - *Existência de elemento neutro para a adição:*

$\exists\ 0\in I\cup\{0\}\ \ tal\ que:$

$$a+0=2k+1+0=0+2k+1=2k+1=a.$$

3 - *Existência de inverso aditivo:*

para todo $a\in I\cup\{0\}$ *temos:*

$$a+x=0\Leftrightarrow 2k+1+x=0\Leftrightarrow x=-(2k+1)\Leftrightarrow x=2(-k)-1.$$

Como $-k\in\mathbb{Z}$ *concluímos que* $2(-k)-1\in I\cup\{0\}$, *e ainda,* $2(-k)-1=-2k-1=-(2k+1)=-a$. *Ou seja, existe um único elemento* $-a\in I\cup\{0\}$ *tal que*

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

4 - *Comutatividade da adição:*

$$a + b = 2k + 1 + 2k' + 1 = 2k' + 1 + 2k + 1 = b + a.$$

5 - *Associatividade da multiplicação:*

$$\begin{aligned} (a \cdot b) \cdot c &= ((2k+1) \cdot (2k'+1)) \cdot (2k''+1) &&= (2k+1) \cdot (2k'+1) \cdot (2k''+1) \\ &= (2k+1) \cdot ((2k'+1) \cdot (2k''+1)) &&= a \cdot (b \cdot c). \end{aligned}$$

6 - *Distributividade à esquerda e à direita:*

$$\begin{aligned} a \cdot (b + c) &= (2k+1) \cdot ((2k'+1) + (2k''+1)) \\ &= (2k+1) \cdot (2k'+1) + (2k+1) \cdot (2k''+1)) \\ &= a \cdot b + a \cdot c. \end{aligned}$$

$$\begin{aligned} (a + b) \cdot c &= ((2k+1) + (2k'+1)) \cdot (2k''+1) \\ &= (2k+1) \cdot (2k''+1) + (2k'+1) \cdot (2k''+1) \\ &= a \cdot c + b \cdot c. \end{aligned}$$

Embora $(I \cup \{0\}, +, \cdot)$ cumpra as propriedades de anel, temos que $(I \cup \{0\}, +, \cdot)$ não é fechado para a adição, pois para todo $k, k' \in \mathbb{Z}$ com $k \neq -(k'+1)$,

$$a + b = (2k+1) + (2k'+1) = 2k + 2k' + 2 = 2(k + k' + 1) \notin I \cup \{0\}.$$

*Portanto, concluímos que $(I \cup \{0\}, +, \cdot)$ **não é anel.***

Algo importante de se notar no Exemplo 2.16 é que nele não há o elemento neutro da multiplicação (neste caso o elemento 1). Notamos assim que $(A, +, \cdot)$ pode ser um anel sem a obrigatoriedade de ter o elemento neutro da multiplicação.

Definição 2.19. *O anel $(A, +, \cdot)$ é dito **anel com unidade** se:*

$$\exists\, u \in A, u \neq 0, \text{ tal que } x \cdot u = u \cdot x = x, \forall x \in A.$$

Notação: A unidade de um anel, quando existir, denotamos por 1_A ou apenas 1 quando não houver possibilidade de confusão. Vale ressaltar que no vasto campo da matemática nem sempre o elemento neutro da multiplicação é o número (inteiro, racional ou real) 1.

Vejamos alguns exemplos de anel com unidade:

Exemplo 2.20. *O conjunto* $\mathbb{M}_{2\times 2}(\mathbb{R})$ *das matrizes de ordem dois, com as operações definidas no capítulo* 1*, com entradas reais, é um anel com unidade, em que sua unidade é a matriz identidade* $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Exemplo 2.21. *Considere* $\mathbb{R}[x]$ *o anel dos polinômios com coeficientes em* $\mathbb{R}$*. Note que o número real* 1 *pode ser escrito como*

$$1 = 1 + 0x + \cdots + 0x^n = p(x).$$

Isto nos mostra que $1 = p(x) \in \mathbb{R}[x]$*. E portanto o anel* $\mathbb{R}[x]$ *é um anel com unidade.*

Exemplo 2.22. *Seja* $(A, +, \cdot)$ *um anel com unidade* 1*.*

Vamos definir duas novas operações no conjunto A*, usando as operações* $+$ *e* $\cdot$ *de* A*.*

$$a \oplus b = a + b + 1, \ \forall \ a, b \in A,$$
$$a \odot b = a \cdot b + a + b, \ \forall \ a, b \in A.$$

Então, $(A, \oplus, \odot)$ *é um anel.*

Vamos verificar se $(A, \oplus, \odot)$ *satisfaz as seis propriedades da Definição* 2.9*.*

Sejam $x,\ y,\ z \in A$*.*

1 - *Associatividade da adição.*

$(x \oplus y) \oplus z = (x+y+1) \oplus z = (x+y+1)+z+1 = x+y+1+z+1 = x+y+z+1+1 = x + (y + z + 1) + 1 = x + (y \oplus z) + 1 = x \oplus (y \oplus z)$.

2 - *Existência do elemento neutro.*

Queremos determinar $w \in A$ *tal que* $x \oplus w = x$*, ou seja,*

$$x + w + 1 = x.$$

Para que a igualdade anterior seja válida, devemos ter $w = -1$*. Pelo fato de* $(A, +, \cdot)$ *ser um anel com unidade, existe* $-1 \in A$*. Note que*

$$x \oplus (-1) = x + (-1) + 1 = x.$$

$$(-1) \oplus x = (-1) + x + 1 = x.$$

Portanto, -1 *é o elemento neutro da adição.*

3 - *Existência de oposto aditivo.*

Queremos determinar $t \in A$ *tal que* $x \oplus t$ *resulte no elemento neutro da soma, ou seja,* $x \oplus t = -1$*. Assim, queremos*

$$x + t + 1 = -1.$$

Para a igualdade anterior ser válida, devemos ter $t = -(x+2)$*, em que* $2 = 1+1$*. Como*

$$x \oplus (-(x+2)) = x + (-(x+2) + 1 = x - x - 2 + 1) = -1;$$

$$(-(x+2)) \oplus x = (-(x+2)) + x + 1 = -x - 2 + x + 1 = -1.$$

concluímos que o inverso aditivo de x *é* $-(x+2)$*.*

4 - *Comutatividade da adição.*

$$x \oplus y = x + y + 1 = y + x + 1 = y \oplus x.$$

5 - *Associatividade da multiplicação.*

$$x \odot y = x \cdot y + x + y = y \cdot x + y + x = y \odot x.$$

6 - *Distributividade à esquerda e à direita.*

Vamos verificar, primeiramente, a distributividade à esquerda.

$x \odot (y \oplus z) = x \cdot (y \oplus z) + x + (y \oplus z) = x(y+z+1) + x + (y+z+1) = x \cdot y + x \cdot z + x \cdot 1 + x + y + z + 1 = x \cdot y + x \cdot z + x + x + y + z + 1 = (x \cdot y + x + y) + (x \cdot z + x + z) + 1 = x \odot y + x \odot z + 1 = (x \odot y) \oplus (x \odot z)$.

Agora vamos verificar a distributividade à direita.

$(x \oplus y) \odot z = (x \oplus y) \cdot z + (x \oplus y) + z = (x+y+1) \cdot z + x + y + 1 + z = x \cdot z + y \cdot z + 1 \cdot z + x + y + 1 + z = x \cdot z + x + z + y \cdot z + y + z + 1 = (x \odot z) + (y \odot z) + 1 = (x \odot z) \oplus (y \odot z)$.

Como as seis propriedades são válidas, $(A, \oplus, \odot)$ *é um anel.*

Vale notar que $(A, \oplus, \odot)$ *possui unidade. Pela Proposição* 2.10 *temos*

$$\begin{aligned} x \odot 0 &= x \cdot 0 + 0 + x = x \\ &e \\ 0 \odot x &= 0 \cdot x + 0 + x = x. \end{aligned}$$

Portanto sua unidade é 0.

Definição 2.23. *Um anel* $(A, +, \cdot)$ *é dito* ***anel comutativo*** *se:*

$$\forall\ x, y \in A, x \cdot y = y \cdot x.$$

Exemplo 2.24. *O Anel do Exemplo* 2.16 *é comutativo, pois, para quaisquer* $a = 2k, b = 2k' \in 2\mathbb{Z}$, *com* $k, k' \in \mathbb{Z}$, *temos:*

$$\begin{aligned} a \cdot b &= 2k \cdot 2k' &&= 2 \cdot 2 \cdot k \cdot k' \\ &= 2 \cdot 2 \cdot k' \cdot k &&= 2k' \cdot 2k \\ &= b \cdot a. \end{aligned}$$

Exemplo 2.25. *O anel dos polinômios, como visto na Proposição* 1.17 *é um anel comutativo.*

O anel do Exemplo 2.20 não é um anel comutativo, pois para as matrizes $A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 3 \\ 3 & 5 \end{pmatrix}$ temos:

$$A \cdot B = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 6 & 13 \\ 0 & 3 \end{pmatrix}$$

e

$$B \cdot A = \begin{pmatrix} 0 & 3 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 8 & 6 \end{pmatrix}.$$

Assim $A \cdot B \neq B \cdot A$.

A seguir, definimos o que é um divisor de zero num anel comutativo.

Definição 2.26. *Seja* A *um anel comutativo. Um elemento* $a \in A$, $a \neq 0$ *é dito um* ***divisor de zero***, *se existe* $b \in A$, $b \neq 0$, *que satisfaz,* $a \cdot b = 0$.

Da definição acima dizemos que um anel comutativo **não possui divisores de zero** quando o produto de dois elementos de A é nulo, então um desses dois elementos será nulo. Ou seja,

$$a, b \in A \text{ e } a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

A próxima definição são para os anéis comutativo com unidade e não possui um divisor de zero.

Definição 2.27. *Se A é um* ***anel comutativo, com unidade*** *e* ***sem divisores de zero****, dizemos que A é um* ***domínio de integridade****.*

Exemplo 2.28. *Os números inteiros $\mathbb{Z}$ com as operações de adição e multiplicação usuais é um exemplo de domínio de integridade, pois é comutativo, possui a unidade 1 e para todos $a, b \in \mathbb{Z}$ temos que se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

Além do conjunto dos números inteiros, temos que os conjuntos dos **números racionais** $\mathbb{Q}$ e dos **números reais** $\mathbb{R}$ também são **domínios de integridade**, com as operações usuais de adição e multiplicação.

Definição 2.29. *Seja A um domínio de Integridade. Se para todo $a \in A$, $a \neq 0$ existe um $b \in A$ tal que $ab = 1$, dizemos que A é* ***corpo****.*

Exemplo 2.30. *O conjunto dos números racionais $\mathbb{Q}$ é um corpo, pois para todo $a \in \mathbb{Q}$, $a \neq 0$ temos que existe $\frac{1}{a} \in \mathbb{Q}$ tal que:*

$$a \cdot \frac{1}{a} = 1.$$

Além do conjunto dos números racionais $\mathbb{Q}$, temos que o conjunto dos número reais $\mathbb{R}$ também é um corpo.

Exemplo 2.31. *Como visto no capítulo 1, o conjunto dos números complexos $\mathbb{C}$ é um corpo.*

2.2.1 Subanéis

Definição 2.32. *Seja $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Se B é um anel com as operações de A, dizemos que B é um* ***subanel de*** *A, e denotamos por $B \leq A$.*

Exemplo 2.33. *O conjunto $\mathbb{Z}$ dos números inteiros e o conjunto $2\mathbb{Z}$ dos inteiros pares são anéis com as mesmas operações de adição e multiplicação de números inteiros, e ainda, $2\mathbb{Z}$ é um subconjunto de $\mathbb{Z}$. Portanto $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$.*

Como consequência da Definição 2.32, apresentamos uma proposição que facilita verificar se um subconjunto de um anel é um subanel.

Proposição 2.34. *Seja* $(A, +, \cdot)$ *um anel e seja* B *um subconjunto não vazio de* A. *Então,* B *é um subanel de* A *se, e somente se, as seguintes condições são verificadas:*

(i) B *é fechado para a diferença.*

$$x, y \in B \Rightarrow x - y \in B$$

(ii) B *é fechado para a multiplicação.*

$$x, y \in B \Rightarrow x \cdot y \in B$$

Demonstração: $(\Rightarrow)$ *Se* B *é um subanel então por definição temos a validade das condições (i) e (ii).*

$(\Leftarrow)$ *Por hipótese temos que* B *é não vazio. Suponhamos que as propriedades (i) e (ii) são satisfeitas.*

Dado $y \in B$, *da validade de (i), temos* $0 = y - y \in B$, *o que implica que* $-y = 0 - y \in B$. *Agora, dado* $x, y \in B$, *temos que* $x + y = x - (-y) \in B$, *isto é,* B *é fechado para a adição.*

De (ii) temos que B *é fechado para a multiplicação.*

Como B *é um subconjunto não vazio de* A, *possui o elemento neutro para a adição e é fechado para a multiplicação, temos que quaisquer elementos de* B *satisfazem as propriedade da Definição* 2.9.

Logo, pela Definição 2.32, B *é um subanel de* A.

Exemplo 2.35. *No conjunto dos números inteiros* $\mathbb{Z}$, *para qualquer* $m \in \mathbb{Z}$ *temos que* $m\mathbb{Z} = \{mk; k \in \mathbb{Z}\}$ ***é um subanel de*** $\mathbb{Z}$, *pois dados* $a = mp$, $b = mq \in m\mathbb{Z}$ *com* p, $q \in \mathbb{Z}$, *pela Proposição* 2.34 *temos:*

(i) $0 \in m\mathbb{Z}$, *pois* $0 = m \cdot 0$. *Isto mostra que* $m\mathbb{Z} \neq \varnothing$

(ii) $a - b = mp - mq = m(p - q) \in m\mathbb{Z}$, *pois* $(p - q) \in \mathbb{Z}$.

(iii) $a \cdot b = mp \cdot mq = m(mpq) \in m\mathbb{Z}$, *pois* $(mpq) \in \mathbb{Z}$.

Seja A um anel e $S \leq A$. Definimos:

$$\forall\ x, y \in A,\ x \sim y \Leftrightarrow y - x \in S.$$

É fácil a verificação de que $\sim$ é uma relação de equivalência em S.

Para todo $x \in A$, a classe de x é dada por

$$\begin{aligned} \overline{x} &= \{y \in A; y - x \in S\} \\ &= \{y \in A; y - x = s,\ \text{para algum } s \in S\} \\ &= \{y \in A; y = x + s,\ \text{para algum } s \in S\} \\ &= \{x + s; s \in S\} \\ &\coloneqq x + S. \end{aligned}$$

Seja o conjunto $\dfrac{A}{\sim} = \{x + S; x \in A\}$, e sejam $x, y \in A$. Definimos:

- $(x + S) + (y + S) = (x + y) + S$.
- $(x + S) \cdot (y + S) = (xy) + S$.

Nossa questão é: será que estas operações estão bem definidas a ponto de tornar $\dfrac{A}{\sim}$ um anel ?

Sejam x, x', y e y' elementos de A, tal que $x + S = x' + S$ e $y + S = y' + S$. Então $x - x' \in S$ e $y - y' \in S$. É fácil ver que $(x + y) + S = (x' + y') + S$.

Mas será que $(x+S) \cdot (y+S) = (x'+S) \cdot (y'+S)$? Ou seja, será que $xy+S = x'y'+S$?

Note que

$$xy + S = x'y' + S \Longleftrightarrow xy - x'y' \in S.$$

Mas, $xy - x'y' = xy + xy' - xy' + x'y' = x\underbrace{(y - y')}_{\in S} + \underbrace{(x - x')}_{\in S} y'$.

Embora $x - x'$, $y - y' \in S$, não há garantias de que

$$x(y - y') \in S \text{ e } (x - x')y' \in S. \tag{2.1}$$

Logo, não temos garantia de que

$$xy - x'y' \in S,$$

por isso, não há garantias de que

$$xy + S = x'y' + S.$$

Inspirados nisso, vamos definir uma nova classe de subanéis.

Definição 2.36. *Seja A um anel e seja I um subanel de A.*

(a) Dizemos que I é um ***ideal à esquerda*** *de A, se*

$$a \cdot x \in I, \ \forall a \in A, \ \forall x \in I.$$

(b) Dizemos que I é um ***ideal à direita*** *de A, se*

$$x \cdot a \in I, \ \forall a \in A, \ \forall x \in I.$$

(c) Dizemos que I é um ***ideal*** *de A se I é um ideal simultaneamente à direita e à esquerda de A.*

Notação: Se I é um ideal de A, escrevemos $I \lhd A$.

Após a Definição 2.36, percebemos que se S é um ideal de A teremos a validade de (2.1), e como consequência a validade da igualdade:

$$xy + S = x'y' + S.$$

Concluímos que as operações estão bem definidas em $\dfrac{A}{\sim}$ quando S é um ideal. Denotamos $\dfrac{A}{\sim}$ por $\dfrac{A}{S}$.

Como resultado do que vimos acima, temos a seguinte proposição:

Proposição 2.37. *Sejam A um anel, S um ideal de A.*

Se $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$ em $\dfrac{A}{S}$, então:

(a) $\overline{x} + \overline{y} = \overline{x + y} = \overline{x' + y'} = \overline{x'} + \overline{y'}$.

(b) $\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{x' \cdot y'} = \overline{x'} \cdot \overline{y'}$.

Teorema 2.38. *Seja A um anel e J um ideal de A. Se $\overline{x} = x + J$ e $A/J = \{\overline{x}; x \in A\}$, então:*

(a) $+ : A/J \times A/J \to A/J$ *e* $\cdot : A/J \times A/J \to A/J$

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

definem duas operações, denominadas adição e multiplicação, em A/J.

(b) $(A/J, +, \cdot)$ *é um anel, chamado anel quociente de A por J.*

(c) Se 1 *é a unidade de A então* $\overline{1}$ *é a unidade de A/J.*

(d) Se A é comutativo então A/J é comutativo.

Demonstração:

(a) Segue da Proposição 2.37.

(b) Para demonstrar que $(A/J, +, \cdot)$ é um anel, vamos verificar as 6 propriedades da Definição 2.9.

Considere, então, $\overline{x}$, $\overline{y}$, $\overline{z} \in A/J$.

1- Associatividade da adição.

$(\overline{x}+\overline{y})+\overline{z} = (\overline{x+y})+\overline{z} = \overline{(x+y)+z} = \overline{x+y+z} = \overline{x}+(\overline{y+z}) = \overline{x}+(\overline{y}+\overline{z})$.

2- Existência de elemento neutro para a adição.

Como $\overline{0} \in A/J$ temos que

$\overline{0} + \overline{x} = \overline{x} + \overline{0} = \overline{x}$ e portanto $\overline{0}$ é o elemento neutro para a adição.

3- Existência de inverso aditivo.

Do item anterior temos que

$$\overline{0} = (\overline{x - x}) = \overline{x + (-x)} = \overline{x} + \overline{(-x)} = \overline{(-x)} + \overline{x}.$$

4- Comutatividade da adição.

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}.$$

5- Associatividade da multiplicação.

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

6- Distributividade à esquerda e à direita.

i) $\overline{x}\cdot(\overline{y}+\overline{z}) = \overline{x}\cdot(\overline{y+z}) = \overline{x\cdot(y+z)} = \overline{x\cdot y + x\cdot z} = \overline{x\cdot y}+\overline{x\cdot z} = \overline{x}\cdot\overline{y}+\overline{x}\cdot\overline{z}$.

ii) $(\overline{x}+\overline{y})\cdot\overline{z} = (\overline{x+y})\cdot\overline{z} = \overline{(x+y)\cdot z} = \overline{x\cdot z + y\cdot z} = \overline{x\cdot z}+\overline{y\cdot z} = \overline{x}\cdot\overline{z}+\overline{y}\cdot\overline{z}$.

(c) Se $1 \in A$, então temos que $1\cdot x = x\cdot 1 = x$ para todo x em A, então,

$$\overline{1}\cdot\overline{x} = \overline{1\cdot x} = \overline{x}$$

e

$$\overline{x}\cdot\overline{1} = \overline{x\cdot 1} = \overline{x}.$$

(d) Se A é comutativo, temos que $x\cdot y = y\cdot x, \forall\, x, y \in A$, então, teremos

$$\overline{x}\cdot\overline{y} = \overline{y}\cdot\overline{x},\ \forall\, \overline{x}, \overline{y} \in A/J.$$

Exemplo 2.39. *Para todo anel A temos que $\{0\}$ e A são ideais de A. Estes ideais são chamado* ***ideais triviais*** *de A. Já os ideais não triviais de A são ditos* ***ideais próprios*** *de A.*

Exemplo 2.40. *No anel $\mathbb{M}_{2\times 2}(\mathbb{R})$, das matrizes de ordem 2 com entradas reais, considere o subanel*

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

Verifiquemos que I é um ideal à direita. De fato, se

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \in I,\ e\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$$

temos

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} aa_1 + cb_1 & a_1 b + b_1 d \\ 0 & 0 \end{pmatrix} \in I.$$

Logo I é um ideal à direita de $\mathbb{M}_{2\times 2}(\mathbb{R})$.

Note que I não é um ideal à esquerda, pois

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa_1 + b0 & ab_1 b + b0 \\ ca_1 + d0 & cb_1 + d0 \end{pmatrix} = \begin{pmatrix} aa_1 & ab_1 \\ ca_1 & cb_1 \end{pmatrix} \notin I,$$

sempre que $ca_1 \neq 0$ ou $cb_1 \neq 0$.

Exemplo 2.41. *No anel $\mathbb{Z}$, o anel dos inteiros, considere o subanel*

$$2\mathbb{Z} = \{2k; k \in \mathbb{Z}\}.$$

Verifiquemos que $2\mathbb{Z}$ é um ideal de de $\mathbb{Z}$. De fato, temos

(i) $2\mathbb{Z}$ é um ideal à direita de $\mathbb{Z}$, pois para todo $x \in \mathbb{Z}$ temos que

$$(2k)(x) = 2kx = 2(kx) \in 2\mathbb{Z}.$$

(ii) $2\mathbb{Z}$ é um ideal à esquerda de $\mathbb{Z}$, pois para todo $x \in \mathbb{Z}$ temos que

$$(x)(2k) = x2k = 2(kx) \in 2\mathbb{Z}.$$

Como queríamos verificar.

Sobre o exemplo anterior, é fácil ver que, para qualquer $a \in \mathbb{Z}$ temos que o subanel $a\mathbb{Z} = \{ak; k \in z\}$ é um ideal de $\mathbb{Z}$.

Exemplo 2.42. *Sejam $(A, +, \cdot)$ um anel e $a \in A$ o conjunto*

$$\langle a \rangle = \{r_1 a s_1 + \cdots + r_n a s_n; r_i, s_i \in A\}$$

é um ideal de A chamado um ideal principal gerado por a

Proposição 2.43. *Sejam I, J ideais de um anel A. Então os seguintes conjuntos são ideais*

$$I \cap J = \{x \in A; x \in I \;\text{ e }\; x \in J\},$$
$$I + J = \{x + y; x \in I \;\text{ e }\; y \in J\},$$
$$IJ = \{x_1 y_1 + \cdots + x_n y_n; x_i \in I \;\text{ e }\; y_i \in J\}, \;\; \textit{com } i \in \mathbb{N}.$$

2.2.2 Ideais maximais

Conforme vimos, se $I \lhd A$, então $\left(\dfrac{A}{I}, +, \cdot\right)$ é anel. Nesta seção veremos condições sobre I para que $\left(\dfrac{A}{I}, +, \cdot\right)$ seja corpo.

Definição 2.44. *Dizemos que I é um ideal maximal em A, e denotamos $I \lhd_{max} A$, se:*

(i) $I \neq A$, *isto é* $I \subsetneq A$;

(ii) Para todo ideal J de A, se I está contido em J, então $I = J$ ou $J = A$, ou simbolicamente,

$$\forall\ J \lhd A,\ I \subseteq J \Rightarrow \begin{cases} J = I \ ou \\ J = A. \end{cases}$$

No próximo teorema, veremos quais as condições para um anel ser um corpo. O segundo teorema nos dirá que um anel quocientado pelo seu ideal será corpo se, e somente se, este ideal é maximal.

Teorema 2.45. *Seja* $(\mathbb{K}, +, \cdot)$ *um anel comutativo com unidade* $1 \in \mathbb{K}$. *São equivalentes.*

(a) $\mathbb{K}$ *é um corpo.*

(b) $\{0\}$ *é um ideal maximal em* $\mathbb{K}$.

(c) os únicos ideais de $\mathbb{K}$ *são os triviais.*

Demonstração: $(a) \Rightarrow (b)$ Sejam $\mathbb{K}$ um corpo e J um ideal de $\mathbb{K}$, de tal forma que $\{0\} \subseteq J \subseteq \mathbb{K}$. Se $\{0\} = J$, não há o que provar. Suponha então que $\{0\} \neq J$. Então existe $a \in J$, com $a \neq 0$. Como $\mathbb{K}$ é um corpo, existe $b \in \mathbb{K}$ tal que $b \cdot a = 1$. Logo $1 \in J$, (pois J é um ideal e $1 = b \cdot a \in J$, $\forall a \neq 0 \in J$ e $\exists\ b \in \mathbb{K}$). Assim, para todo $k \in \mathbb{K}$, temos que $k \cdot 1 \in J$. Logo, para todo $k \in \mathbb{K}$, temos que $k \in J$ e portanto $J = \mathbb{K}$. Concluímos que $\{0\}$ é um ideal maximal em $\mathbb{K}$.

$(b) \Rightarrow (c)$ Se $\{0\}$ é um ideal maximal em $\mathbb{K}$, temos que para todo J ideal em $\mathbb{K}$, $\{0\} \subseteq J$, e assim J é o próprio conjunto $\{0\}$ ou J é o próprio $\mathbb{K}$ que são os ideais triviais. Logo, os únicos ideais de $\mathbb{K}$ são os triviais.

$(c) \Rightarrow (a)$ Seja $0 \neq a \in \mathbb{K}$. Por hipótese, $\langle a \rangle = \mathbb{K}$. Logo, $\exists\ b \in \mathbb{K}$ tal que $1 = ab = ba$. Portanto $\mathbb{K}$ é corpo.

Teorema 2.46. *Seja A um anel comutativo com unidade $1 \in A$ e seja J um ideal de A. Então, J é um ideal maximal se, e somente se, A/J é corpo.*

Demonstração

$\Rightarrow$) Para A/J ser um corpo, devemos mostrar que em A/J satisfaz a seguinte propriedade:

$$\forall\ \overline{0} \neq \overline{a} \in A/J,\ \exists\ \overline{b} \in A/J \text{ tal que } \overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = 1.$$

Suponhamos que J é um ideal maximal de A e seja $\overline{a} \in A/J$, $\overline{a} \neq 0$. Neste caso, $a \notin J$. Seja $L = A \cdot a$ um ideal principal de A gerado por a. Temos que $J + L = \{x + y;\ x \in J \text{ e } y \in L\}$ é um ideal contendo J. Como $a = 1 \cdot a \in L \subset J + L$ temos que $J + L$ é um ideal contendo J e ainda $J + L \neq J$.

Pela maximalidade de J segue que $A = J + L$, e daí temos, $1 \in J + L$, ou seja, existem $u \in J$, $v \in L$ tais que $1 = u + v$.

Como $v \in L = A \cdot a$, então $v = b \cdot a$ para algum $b \in A$ e como por hipótese $1 \notin J$, temos que $\overline{1} \in A/J$. Pela Proposição 2.37, segue que

$$\overline{1} = \overline{u + b \cdot a} = \overline{u} + \overline{b \cdot a} = \overline{0} + \overline{b} \cdot \overline{a} \in A/J.$$

Logo, $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b} = \overline{1}$, como queríamos demonstrar.

$\Leftarrow$) Suponha que $\overline{A} = A/J$ é um corpo. Então,

$$\overline{1} \in \overline{A} \Rightarrow J \neq A.$$

Se $M \neq J$ é um ideal de A e $J \subset M \subset A$, então teremos que existe $a \in M$, tal que $a \notin J$, ou seja, $\overline{a} \neq \overline{0}$, $\overline{a} \in \overline{A}$. Como $\overline{A}$ é corpo, $\exists\ \overline{b} \in \overline{A}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$; ou ainda

$$\exists\ u \in J \text{ tal que } a \cdot b - 1 = u.$$

Como $a \in M$ e M é um ideal, então $a \cdot b \in M$ e como $u \in J \subset M$ temos que $u \in M$. Logo, concluímos que $1 = a \cdot b - u \in M$, isto é $M = A$.

Portanto J é um ideal maximal.

2.3 Homomorfismo De Anéis

Nesta seção, A e A' denotarão anéis, a menos que mencionemos o contrário. Denotaremos, respectivamente por 0 e $0'$ os elementos neutros aditivos de A e A', bem como 1 e $1'$ as unidades de A e A', quando existirem. Adotaremos as operações $+$ e $\cdot$ para ambos os anéis.

Definição 2.47. *Uma função $f : A \to A'$ é um* ***homomorfismo*** *de A em A' se, para todo x, y em A, as seguintes condições estiverem satisfeitas:*

(i) $f(x+y) = f(x) + f(y)$.

(ii) $f(x \cdot y) = f(x) \cdot f(y)$.

Definição 2.48. *Se $f : A \to A'$ é um homomorfismo bijetivo dizemos que f é um* ***isomorfismo*** *de A sobre A'.*

Os homomorfismos $f : A \to A$ são chamados de **endomorfismos** de A, e os isomorfismos de A sobre si mesmo são chamados de **automorfismos** de A.

Observação: Se $f : A \to A'$ é um homomorfismo, então $f(0) = 0'$ e $\forall\, a \in A$, $f(-a) = -f(a)$.

De fato, pela hipótese temos, $f(0) = f(0+0) = f(0)+f(0)$. Então $f(0)-f(0) = f(0)$.

Logo,

$$f(0) = 0'.$$

E ainda,

$$f(0) = f(a-a) = f(a+(-a)) = f(a) + f(-a) \Leftrightarrow 0' - f(a) = f(-a).$$

Segue que,

$$f(-a) = -f(a).$$

Teorema 2.49. *Sejam A e A' anéis e $f : A \to A'$ um homomorfismo. Então:*

(1) $Im(f) = \{f(a); a \in A\}$ *é um subanel de A'.*

(2) $N(f) = \{a \in A; f(a) = 0'\}$ *é um ideal de A, e f é injetiva $\Leftrightarrow N(f) = \{0\}$.*

(3) *Os anéis $A/N(f)$ e $Im(f)$ são isomorfos.*

Demonstração:

(1) Para $Im(f)$ ser um subanel de A', $Im(f)$ deve satisfazer as condições da Proposição 2.34.

De fato, como f é um homomorfismo, temos que

(i) $0' = f(0) \in Im(f)$. Assim, $Im(f) \neq \varnothing$.

(ii) $f(a),\ f(b) \in Im(f) \Rightarrow f(a) - f(b) = f(a-b) \in Im(f)$.

(iii) $f(a),\ f(b) \in Im(f) \Rightarrow f(a) \cdot f(b) = f(a \cdot b) \in Im(f)$.

Portanto, $Im(f) \leq A'$.

(2) Primeiramente vamos mostrar que $N(f)$ é um ideal de A. De fato,

(i) Como f é um homomorfismo, temos que $f(0) = 0'$. Logo, $0 \in N(f)$.

(ii) Para quaisquer $a,\ b \in N(f)$ temos que

$$0' = 0' - 0' = f(a) - f(b) = f(a-b), \text{ assim } a - b \in N(f).$$

(iii) Para todo $x \in A$ e para todo $a \in N(f)$ temos

$$f(a \cdot x) = f(a) \cdot f(x) = 0' \cdot f(x) = 0'$$

e

$$f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0' = 0'.$$

Assim $a \cdot x \in N(f)$ e $x \cdot a \in N(f)$. Portanto $N(f)$ é um ideal de A.

Mostraremos agora que f é injetora $\Leftrightarrow N(f) = \{0\}$

$\Rightarrow$) Como f é um homomorfismo, temos que $f(0) = 0'$ e do fato de f ser injetiva temos que se $a \in N(f)$, então

$$f(a) = 0' = f(0) \Rightarrow a = 0.$$

Portanto $N(f) = \{0\}$.

$\Leftarrow$) Sejam x, $y \in A$ tais que $f(x) = f(y)$. Então,

$$0' = f(x) - f(y) = f(x - y).$$

Logo, $x - y \in N(f) = \{0\}$ e temos que $x = y$.

Portanto f é injetora.

(3) Queremos mostrar que existe um isomorfismo entre os anéis $A/N(f)$ e $Im(f)$. Para isto seja uma função $F : A/N(f) \rightarrow Im(f)$ definida por $F(\overline{x}) = f(x)$, $\forall\ \overline{x} \in A/N(f)$.

Primeiramente, vamos mostrar que F está bem definida e é bijetora.

(a) F está bem definida e é injetora.

De fato, para todos $\overline{x}$, $\overline{y} \in A/N(f)$ temos:

$$\begin{aligned} F(\overline{x}) = F(\overline{y}) &\Leftrightarrow f(x) = f(y) \\ &\Leftrightarrow f(x) - f(y) = 0 \\ &\Leftrightarrow f(x - y) = 0 \\ &\Leftrightarrow x - y \in N(f) \\ &\Leftrightarrow \overline{x} = \overline{y}. \end{aligned}$$

(b) F é sobrejetora.

De fato, dado $y = f(x) \in Im(f)$, $F(\overline{x}) = f(x) = y$.

(c) F é homomorfismo.

Queremos mostrar que para todos $\overline{x}$, $\overline{y} \in A/N(f)$, valem que

(i) $F(\overline{x} + \overline{y}) = F(\overline{x}) + F(\overline{y})$.

(ii) $F(\overline{x} \cdot \overline{y}) = F(\overline{x}) \cdot F(\overline{y})$.

De Fato,

(i) $F(\overline{x} + \overline{y}) = f(x + y) = f(x) + f(y) = F(\overline{x}) + F(\overline{y})$.

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

Portanto F é um homomorfismo.

Logo, pelos itens (a), (b) e (c) temos que F é um isomorfismo.

2.4 A Primeira Face Do Número Complexo

Nesta seção mostraremos que o anel $\mathbb{R}[x]$ dos polinômios quocientado pelo ideal $\langle x^2+1\rangle$ se comporta, algebricamente, como o conjunto $\mathbb{C}$ dos números complexos. Para isto, seja a função

$$\begin{aligned} \phi : \mathbb{R}[x] &\to \mathbb{C} \\ p(x) &\mapsto p(i) \end{aligned}, \tag{2.2}$$

ou seja, dado $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$,

$$\phi(p(x)) = a_n i^n + a_{n-1} i^{n-1} + \cdots + a_1 i + a_0.$$

Vamos verificar se a função ϕ é um homomorfismo. Para isto, sejam $p(x) = a_n x^n + \cdots + a_1 x + a_0$, com $a_n \neq 0$, e $q(x) = b_m x^m + \cdots + b_1 x + b_0$, com $b_m \neq 0$, polinômios quaisquer.

Suponhamos, sem perda de generalidade, que $n \geq m$.

i) Queremos mostrar que $\phi(p(x) + q(x)) = \phi(p(x)) + \phi(q(x))$.

De fato,

$$\begin{aligned} \phi(p(x)+q(x)) &= \phi((a_n x^n + \cdots + a_m x^m + \cdots + a_1 x + a_0) \\ &\quad +(b_m x^m + \cdots + b_1 x + b_0)) \\ &= \phi(a_n x^n + \cdots + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)) \\ &= a_n i^n + \cdots + (a_m + b_m) i^m + \cdots + (a_1 + b_1) i + (a_0 + b_0) \\ &= a_n i^n + \cdots + a_m i^m + b_m i^m + \cdots + a_1 i + b_1 i + a_0 + b_0 \\ &= (a_n i^n + \cdots + a_m i^m + \cdots + a_1 i + a_0) \\ &\quad +(b_m i^m + \cdots + b_1 i + b_0) \\ &= \phi((a_n x^n + \cdots + a_m x^m + \cdots + a_1 x + a_0)) \\ &\quad +\phi(b_m x^m + \cdots + b_1 x + b_0) \\ &= \phi(p(x)) + \phi(p(x)). \end{aligned}$$

ii) Queremos mostrar que $\phi(p(x) \cdot q(x)) = \phi(p(x)) \cdot \phi(p(x))$.

Inicialmente vamos calcular $p(x) \cdot q(x)$.

$$\begin{aligned}
p(x) \cdot q(x) &= (a_n x^n + \cdots + a_m x^m + \cdots + a_1 x + a_0) \cdot \\
&\quad (b_m x^m + \cdots + b_1 x + b_0) \\
&= a_n x^n \cdot (b_m x^m + \cdots + b_1 x + b_0) + \\
&\quad a_{n-1} x^{n-1} \cdot (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0) + \\
&\quad \cdots \\
&\quad + a_m x^m \cdot (b_m x^m + \cdots + b_1 x + b_0) + \\
&\quad \cdots \\
&\quad + a_1 x \cdot (b_m x^m + \cdots + b_1 x + b_0) + \\
&\quad a_0 \cdot (b_m x^m + \cdots + b_1 x + b_0) \\
&= a_n b_m \cdot x^{n+m} + \\
&\quad (a_n b_{m-1} + a_{n-1} b_m) \cdot x^{n+m-1} + \\
&\quad (a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m) \cdot x^{n+m-2} + \\
&\quad \cdots \\
&\quad + (a_n b_0 + a_{n-1} b_1 + a_{n-2} b_2 + \cdots + a_{n-m} b_m) \cdot x^n + \\
&\quad \cdots \\
&\quad + (a_m b_0 + a_{m-1} b_1 + a_{m-2} b_2 + \cdots + a_0 b_m) \cdot x^m + \\
&\quad \cdots \\
&\quad + (a_1 b_0 + a_0 b_1) \cdot x + \\
&\quad (a_0 b_0).
\end{aligned} \tag{2.3}$$

Ou seja, $p(x)q(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} (a_i b_j) x^k \right)$. Substituindo (2.3) em $\phi(p(x) \cdot q(x))$, temos

$$\begin{aligned}
\phi(p(x) \cdot q(x)) &= \phi(a_n b_m \cdot x^{n+m}) + \phi((a_n b_{m-1} + a_{n-1} b_m) \cdot x^{n+m-1}) + \\
&\quad \cdots \\
&\quad + \phi((a_n b_0 + a_{n-1} b_1 + a_{n-2} b_2 + \cdots + a_{n-m} b_m) \cdot x^n) + \\
&\quad \cdots
\end{aligned}$$

$$
\begin{aligned}
& +\phi((a_m b_0 + a_{m-1}b_1 + a_{m-2}b_2 + \cdots + a_0 b_m)\cdot x^m)+ \\
& \cdots \\
& \phi((a_1 b_0 + a_0 b_1)\cdot x) + \phi((a_0 b_0)) \\
= & +a_n b_m \cdot i^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)\cdot i^{n+m-1} + \\
& \cdots \\
& +(a_n b_0 + a_{n-1}b_1 + a_{n-2}b_2 + \cdots + a_{n-m}b_m)\cdot i^n + \\
& \cdots \\
& +(a_m b_0 + a_{m-1}b_1 + a_{m-2}b_2 + \cdots + a_0 b_m)\cdot i^m + \\
& \cdots \\
& +(a_1 b_0 + a_0 b_1)\cdot i + (a_0 b_0) \\
= & a_n i^n \cdot (b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) + \\
& a_{n-1} i^{n-1} \cdot (b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) + \\
& \cdots \\
& +a_m i^m \cdot (b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) + \\
& \cdots \\
& +a_1 i \cdot (b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) + \\
& a_0 \cdot (b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) \\
= & (a_n i^n + a_{n-1} i^{n-1} + \cdots + a_m i^m + a_{m-1} i^{m-1} \cdots + a_1 i + a_0)\cdot \\
& +(b_m i^m + b_{m-1} i^{m-1} + \cdots + b_1 i + b_0) \\
= & p(i)\cdot q(i) \\
= & \phi(p(x))\cdot\phi(q(x)).
\end{aligned}
$$

Mostramos, pelos itens (i) e (ii), que a função ϕ é um homomorfismo de anéis.

Verificaremos que ϕ é sobrejetora, ou seja, dado $(a+bi) \in \mathbb{C}$, existe $p(x) \in \mathbb{R}[x]$ tal que $\phi(p(x)) = a + bi$.

De fato considerando $p(x) = a + bx$, temos que

$$\phi(p(x)) = \phi(a+bx) = \phi(a) + \phi(bx) = a + bi.$$

Vamos analisar o núcleo de ϕ, ou seja, quem são os elementos $p(x) \in \mathbb{R}[x]$ tal que $\phi(p(x)) = 0$.

Considere $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n \in N(\phi)$. Então:

$$
\begin{aligned}
\phi(p(x)) = 0 &\iff \phi(a_0 + a_1x + a_2x^2 + \cdots a_nx^n) = 0 \\
&\iff a_0 + a_1i + a_2i^2 + \cdots a_ni^n = 0 \\
&\iff a_0 + a_1 \cdot i + a_2 \cdot (-1) + a_3 \cdot (-i) + a_4 \cdot 1 + a_5 \cdot i + \cdots = 0 \\
&\iff (a_0 - a_2 + a_4 - a_6 + a_8 - a_{10} + \cdots)+ \\
&\qquad (a_1 - a_3 + a_5 - a_7 + a_9 - a_{11} + \cdots) \cdot i = 0 + 0 \cdot i.
\end{aligned}
$$

Pela igualdade de números complexos, segue que

$$
\begin{cases}
a_0 - a_2 + a_4 - a_6 + a_8 - a_{10} + \cdots & = 0 \\
a_1 - a_3 + a_5 - a_7 + a_9 - a_{11} + \cdots & = 0
\end{cases},
$$

ou ainda,

$$
\begin{cases}
a_0 & = a_2 - a_4 + a_6 - a_8 + a_{10} + \cdots \qquad (A) \\
a_1 & = a_3 - a_5 + a_7 - a_9 + a_{11} + \cdots \qquad (B)
\end{cases}
$$

Substituindo (A) e (B) em $p(x)$, temos

$$
\begin{aligned}
p(x) &= (a_2 - a_4 + a_6 - a_8 + a_{10} + \cdots) + (a_3 - a_5 + a_7 - a_9 + a_{11} + \cdots)x+ \\
&\quad a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 + a_9x^9 + a_{10}x^{10} \\
&\quad +a_{11}x^{11} + \cdots + a_nx^n \\
&= a_2 \cdot (x^2+1) + a_3x \cdot (x^2+1) + a_4 \cdot (x^4-1) + a_5x \cdot (x^4-1)+ \\
&\quad a_6 \cdot (x^6+1) + a_7x \cdot (x^6+1) + a_8 \cdot (x^8-1) + a_9x \cdot (x^8-1)+ \\
&\quad a_{10} \cdot (x^{10}+1) + a_{11}x \cdot (x^{10}+1) + \cdots .
\end{aligned}
$$

Note que os fatores que aparecem são

$$
(x^2+1),\ (x^4-1),\ (x^6+1),\ (x^8-1),\ (x^{10}+1),\ \ldots\ ,
$$

que podem ser escritos como $(x^{4p+2}+1),\ p \in \mathbb{Z}_+$ ou $(x^{4q}-1),\ q \in \mathbb{Z}_+^*$.

Demonstraremos que $(x^{4p+2}+1)$ e $(x^{4q}-1)$, com $p \in \mathbb{Z}_+$ e $q \in \mathbb{Z}_+^*$, são múltiplos de (x^2+1).

1) $(x^{4p+2}+1)$ é múltiplo de (x^2+1) para todo $p \in \mathbb{Z}_+$.

De fato, por indução finita sobre $p \in \mathbb{Z}_+$, temos:

i) Para $p = 0$, resulta que $(x^{4 \cdot 0+2}+1) = (x^2+1) = 1 \cdot (x^2+1)$.

Assim, para $p = 0$, temos que $(x^{4p+2}+1)$ é múltiplo de (x^2+1)

ii) Suponha que para $p = k$ tenhamos $(x^{4k+2} + 1)$ múltiplo de $(x^2 + 1)$, ou seja,

$$(x^{4k+2} + 1) = (x^2 + 1) \cdot h(x),$$

para algum $h(x) \in \mathbb{R}[x]$.

iii) Vamos mostrar que para $p = (k + 1)$, $(x^{4(k+1)+2} + 1)$ é múltiplo de $(x^2 + 1)$.

De fato,

$$\begin{aligned} (x^{4(k+1)+2} + 1) &= (x^{4k+4+2} + 1) \\ &= x^4 \cdot x^{4k+2} + 1. \end{aligned}$$

Somando e subtraindo x^4, temos,

$$\begin{aligned} (x^{4(k+1)+2} + 1) &= x^4 \cdot x^{4k+2} + x^4 - x^4 + 1 \\ &= x^4 \cdot (x^{4k+2} + 1) - (x^4 - 1). \end{aligned}$$

Pelo item ii), segue que,

$$\begin{aligned} (x^{4(k+1)+2} + 1) &= x^4 \cdot (x^2 + 1) \cdot h(x) - (x^2 + 1) \cdot (x^2 - 1) \\ &= (x^2 + 1) \cdot (x^4 \cdot h(x) - (x^2 - 1)), \end{aligned}$$

com $(x^4 \cdot h(x) - (x^2 - 1)) \in \mathbb{R}[x]$.

Concluímos, pelos itens i), ii) e iii), que $(x^{4p+2} + 1)$ é múltiplo de $(x^2 + 1)$, para todo $p \in \mathbb{Z}_+$.

2) $(x^{4q} - 1)$ é múltiplo $(x^2 + 1)$, para todo $q \in \mathbb{Z}_+^*$.

Por indução finita com $q \in \mathbb{Z}_+^*$, temos:

i) Para $q = 1$, resulta que $x^{4\cdot 1} - 1 = x^4 - 1 = (x^2 + 1) \cdot (x^2 - 1)$.

Portanto, para $q = 1$, temos que $(x^{4q} - 1)$ é múltiplo $(x^2 + 1)$.

ii) Suponha que para $q = k$, tenhamos $(x^{4k} - 1)$ múltiplo de $(x^2 + 1)$, ou seja,

$$(x^{4k} - 1) = (x^2 + 1) \cdot g(x),$$

para algum $g(x) \in \mathbb{R}[x]$

iii) Vamos mostrar que para $q = (k+1)$, $(x^{4(k+1)} - 1)$ é múltiplo de (x^2+1).

De fato,

$$\begin{aligned}(x^{4(k+1)} - 1) &= (x^{4k+4} - 1)\\ &= x^{4k} \cdot x^4 - 1.\end{aligned}$$

Somando e subtraindo x^4, temos,

$$\begin{aligned}(x^{4(k+1)} - 1) &= x^{4k} \cdot x^4 - x^4 + x^4 - 1\\ &= x^4 \cdot (x^{4k} - 1) + (x^4 - 1).\end{aligned}$$

Pelo item ii), segue que,

$$\begin{aligned}(x^{4(k+1)} - 1) &= x^4 \cdot (x^2+1) \cdot g(x) + (x^2+1) \cdot (x^2-1)\\ &= (x^2+1) \cdot (x^4 \cdot g(x) + (x^2-1)),\end{aligned}$$

com $(x^4 \cdot g(x) + (x^2-1)) \in \mathbb{R}[x]$.

Pelos itens i), ii) e iii), concluímos que $x^{4q} - 1$ é múltiplo de (x^2+1), para todo $q \in \mathbb{Z}_+^*$.

Assim, podemos afirmar que

$$\begin{aligned}p(x) \;=\; & a_2 \cdot (x^2+1) + a_3 x \cdot (x^2+1) + a_4 \cdot (x^4-1) + a_5 x \cdot (x^4-1) +\\ & a_6 \cdot (x^6+1) + a_7 x \cdot (x^6+1) + a_8 \cdot (x^8-1) + a_9 x \cdot (x^8-1) +\\ & a_{10} \cdot (x^{10}+1) + a_{11} x \cdot (x^{10}+1) + \cdots .\end{aligned}$$

pode ser escrito como $p(x) = (x^2+1) \cdot f(x)$ para algum $f(x) \in \mathbb{R}[x]$.

Portanto o núcleo da função ϕ é formado por todos os polinômios múltiplos de x^2+1, isto é,

$$N(\phi) = \{(x^2+1) \cdot h(x);\; h(x) \in \mathbb{R}[x]\},$$

ou simplesmente, $N(\phi) = \langle x^2+1 \rangle$.

Como a função ϕ é um homomorfismo, pelo Teorema 2.49, item (3), concluímos que $\dfrac{\mathbb{R}[x]}{N(\phi)}$ e $Im(\phi) = \mathbb{C}$ são isomorfos, ou seja,

$$\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong \mathbb{C}.$$

Mostrando que o conjunto $\dfrac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$ se comporta, algebricamente, como o conjunto $\mathbb{C}$ dos números complexos.

2.5 A Segunda Face Do Número Complexo

Nesta seção mostraremos uma outra face do conjunto dos números complexos. Provaremos que existe um subanel no anel $\mathbb{M}_{2\times 2}(\mathbb{R})$ das matrizes de ordem 2 que se comporta algebricamente como o conjunto dos números complexos.

Exemplo 2.50. *Considere o anel* $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R} \right\}$ *e a função*

$$\begin{array}{rccl} \Psi : & S & \to \mathbb{C} \\ & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} & \mapsto a + bi \end{array}. \tag{2.4}$$

Sejam as matrizes $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in S$. *Verificaremos se* Ψ *é um homomorfismo.*

i) Mostraremos que $\Psi(A + C) = \Psi(A) + \Psi(C)$

De fato,

$$\begin{aligned} \Psi(A + C) &= \Psi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) \\ &= \Psi\left(\begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix}\right) \\ &= (a + c) + (b + d)i \\ &= a + c + bi + di \\ &= a + bi + c + di \\ &= (a + bi) + d + bi \\ &= \Psi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + \Psi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) \\ &= \Psi(A) + \Psi(C) \end{aligned}$$

ii) Mostraremos que $\Psi(A \cdot C) = \Psi(A) \cdot \Psi(C)$.

De fato,

$$\begin{aligned}
\Psi(A \cdot C) &= \Psi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) \\
&= \Psi\left(\begin{pmatrix} ac + b(-d) & ad + bc \\ (-b)c + a(-d) & (-b)d + ac \end{pmatrix}\right) \\
&= \Psi\left(\begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}\right) \\
&= \Psi\left(\begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}\right) \\
&= (ac - bd) + (ad + bc)i \\
&= ac - bd + adi + bci \\
&= ac + bdi^2 + adi + bci \\
&= ac + bidi + adi + cbi \\
&= a(c + di) + bi(c + di) \\
&= (a + bi)(c + di) \\
&= \Psi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) \cdot \Psi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) \\
&= \Psi(A) \cdot \Psi(C)
\end{aligned}$$

Por i) e ii), concluímos que a função Ψ *é um homomorfismo.*

A seguir, mostraremos que a função Ψ *é bijetiva.*

Injetividade: *Para mostrar que* Ψ *é injetiva, utilizaremos o Teorema* 2.49*, item* (2)*. Primeiramente, verificaremos que* $N(\Psi) = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$. *Para isto considere a matriz*

$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in N(\Psi)$. *Então,*

$$\Psi(A) = 0 \Leftrightarrow \Psi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = 0 \Leftrightarrow$$

$$a + bi = 0 \Leftrightarrow a + bi = 0 + 0i$$

pela igualdade de número complexos, temos que

$$\begin{cases} a = 0 \\ b = 0 \end{cases}.$$

Concluímos que qualquer matriz do núcleo de Ψ *é nula. Garantindo, pelo Teorema* 2.49*, que* Ψ *é injetiva.*

Sobrejetividade: *Queremos mostrar que para qualquer* $a + bi \in \mathbb{C}$ *existe* $A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in S$ *com* $x, y \in \mathbb{R}$*, tal que* $\Psi(A) = a + bi$.

De fato, temos que

$$\begin{array}{rccc} & \Psi(A) & = & a + bi \\ \Longleftrightarrow & \Psi\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\right) & = & a + bi \\ \Longleftrightarrow & x + yi & = & a + bi, \end{array}$$

pela igualdade de números complexos, obtemos,

$$\begin{cases} x = a \\ y = b \end{cases}, \ x, y, a, b \in \mathbb{R}$$

Logo, para qualquer $a + bi \in \mathbb{C}$*, existe uma matriz* $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in S$ *tal que*

$$\Psi(A) = a + bi.$$

Como a função Ψ *é um homomorfismo bijetivo, pela Definição* 2.48*, concluímos que a função* Ψ *é um isomorfismo.*

Como acabamos de ver, no Exemplo 2.50 temos que a função Ψ é um isomorfismo, e devido a isto podemos então afirmar que existe a função inversa

$$\begin{aligned} \Psi^{-1}: \quad \mathbb{C} \quad &\to S \\ a+bi \quad &\mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \end{aligned} \tag{2.5}$$

ou seja, dado $a+bi \in \mathbb{C}$, temos que

$$\Psi^{-1}(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Motivados pelo isomorfismo da função Ψ e pelo fato de podermos definir ângulo entre números complexo, vamos verificar que é possível formar ângulos com duas matrizes A e B do conjunto S.

Capítulo 3

Ângulos Entre Matrizes

Neste capítulo mostraremos que é possível encontrar ângulo entre duas matrizes que estão no conjunto $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in \mathbb{R} \right\}$ definido no capítulo anterior. Como base, iniciaremos definindo espaço vetorial e produto interno num espaço vetorial.

Maiores detalhes podem ser encontrado em [3], [4] e [8].

Definição 3.1. *Um conjunto não vazio V é um **espaço vetorial sobre um corpo** $\mathbb{K}$ (ou um $\mathbb{K}-$espaço vetorial) se em seus elementos, denominados vetores, estiverem definidas duas operações:*

- *A cada par u, v de vetores de V corresponde um vetor $u + v \in V$, chamado de adição de u e v, de modo que:*

  1 - $u + v = v + u$, $\forall\ u, v \in V$.

  2 - $(u + v) + w = u + (v + w)$.

  3 - *existe em V um vetor, denominado **vetor nulo** e denotado por 0, tal que $0 + v = v$, $\forall\ v \in V$.*

  4 - *a cada vetor $v \in V$ exista um vetor em V, denotado por $-v$ tal que $v + (-v) = 0$.*

- *A cada par $\alpha \in \mathbb{K}$ e $v \in V$, corresponde um vetor $\alpha \cdot v \in V$ denominado **produto por escalar** de α por v de modo que:*

5 - $(\alpha\beta) \cdot v = \alpha(\beta \cdot v)$, $\forall\ \alpha, \beta \in \mathbb{K}$ e $\forall\ v \in V$.

6 - $1 \cdot v = v$, $\forall\ v \in V$ *(onde* 1 *é o elemento identidade de* $\mathbb{K}$*).*

Além disso, vamos impor que as operações dadas se distribuam, isto é, que valham as seguintes propriedades

7 - $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$, $\forall\ \alpha \in \mathbb{K}$ e $\forall\ u, v \in V$.

8 - $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$, $\forall\ \alpha, \beta \in \mathbb{K}$ e $\forall\ v \in V$.

Exemplo 3.2. *Para quaisquer* $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{R}^n$ *e* $\alpha \in \mathbb{R}$, *definimos*

$$\begin{aligned} \textit{Adição}: &\quad (a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n); \\ \textit{Produto por escalar}: &\quad \alpha \cdot (a_1, \dots, a_n) = (\alpha \cdot a_1, \dots, \alpha \cdot a_n). \end{aligned}$$

O conjunto $\mathbb{R}^n$ *é espaço vetorial sobre o corpo* $\mathbb{R}$. *Vejamos.*

1 - *Dados* $u, v \in \mathbb{R}^n$, *com* $u = (a_1, \dots, a_n)$, $a_1, \dots, a_n \in \mathbb{R}$ *e* $v = (b_1, \dots, b_n)$, $b_1, \dots, b_n \in \mathbb{R}$, *temos*

$$u+v = (a_1, \dots, a_n)+(b_1, \dots, b_n) = (a_1+b_1, \dots, a_n+b_n) = (b_1+a_1, \dots, b_n+a_n) = v+u.$$

2 - $u, v, w \in \mathbb{R}^n$, *com* $u = (a_1, \dots, a_n)$, $a_1, \dots, a_n \in \mathbb{R}$, $v = (b_1, \dots, b_n)$, $b_1, \dots, b_n \in \mathbb{R}$ *e* $w = (c_1, \dots, c_n)$, $c_1, \dots, c_n \in \mathbb{R}$, *temos*

$$\begin{aligned} (u + v) + w &= ((a_1, \dots, a_n) + (b_1, \dots, b_n)) + (c_1, \dots, c_n) \\ &= (a_1 + b_1, \dots, a_n + b_n) + (c_1, \dots, c_n) \\ &= ((a_1 + b_1) + c_1, \dots, (a_n + b_n) + c_n) \\ &= (a_1 + b_1 + c_1, \dots, a_n + b_n + c_n) \\ &= (a_1 + (b_1 + c_1), \dots, a_n + (b_n + c_n)) \\ &= (a_1, \dots, a_n) + ((b_1 + c_1), \dots, (b_n + c_n)) \\ &= (a_1, \dots, a_n) + ((b_1, \dots, b_n) + (c_1, \dots, c_n)) \\ &= v + (u + w). \end{aligned}$$

3 - *Existe em* $\mathbb{R}^n$ *o vetor* $0 = (0, \dots, 0)$, *tal que*

$$0 + u = (0, \dots, 0) + (a_1, \dots, a_n) = (0 + a_1, \dots, 0 + a_n) = (a_1, \dots, a_n) = v,$$

$\forall\ u = (a_1, \dots, a_n) \in \mathbb{R}^n$.

4 - *A cada vetor* $u = (a_1, \ldots, a_n) \in \mathbb{R}^n$ *existe um vetor* $-u = (-a_1, \ldots, -a_n) \in \mathbb{R}^n$*, tal que*

$$\begin{aligned} u + (-u) &= (a_1, \ldots, a_n) + (-(a_1, \ldots, a_n)) &&= (a_1, \ldots, a_n) + (-a_1, \ldots, -a_n) \\ &= (a_1 - a_1, \ldots, a_n - a_n) &&= (0, \ldots, 0) \\ &= 0. \end{aligned}$$

5 - *Sejam* $\alpha, \beta \in \mathbb{R}$ *e* $u = (a_1, \ldots, a_n) \in \mathbb{R}^n$*. Então*

$$\begin{aligned} (\alpha\beta) \cdot u &= (\alpha\beta) \cdot (a_1, \ldots, a_n) &&= ((\alpha\beta)a_1, \ldots, (\alpha\beta)a_n) \\ &= (\alpha\beta a_1, \ldots, \alpha\beta a_n) &&= \alpha(\beta a_1, \ldots, \beta a_n) \\ &= \alpha(\beta(a_1, \ldots, a_n)) &&= \alpha(\beta \cdot u) \end{aligned}$$

6 - *Para qualquer* $u = (a_1, \ldots, a_n) \in \mathbb{R}^n$ *e* $1 \in \mathbb{R}$*, temos*

$$1 \cdot u = 1 \cdot (a_1, \ldots, a_n) = (1 \cdot a_1, \ldots, 1 \cdot a_n) = (a_1, \ldots, a_n) = v$$

7 - *Para todo* $\alpha \in \mathbb{R}$ *e quaisquer* $u = (a_1, \ldots, a_n), v = (b_1, \ldots, b_n) \in \mathbb{R}^n$*, temos*

$$\begin{aligned} \alpha \cdot (u + v) &= \alpha \cdot (a_1 + b_1, \ldots, a_n + b_n) = (\alpha(a_1 + b_1), \ldots, \alpha(a_n + b_n)) \\ &= (\alpha a_1 + \alpha b_1, \ldots, \alpha a_n + \alpha b_n) = (\alpha a_1, \ldots, \alpha a_n) + (\alpha b_1, \ldots, \alpha b_n) \\ &= \alpha \cdot (a_1, \ldots, a_n) + \alpha \cdot (b_1, \ldots, b_n) = \alpha \cdot u + \alpha \cdot v. \end{aligned}$$

8 - *Para todos* $\alpha, \beta \in \mathbb{R}$ *e para todo* $u = (a_1, \ldots, a_n) \in \mathbb{R}^n$*, obtemos*

$$\begin{aligned} (\alpha + \beta) \cdot u &= (\alpha + \beta) \cdot (a_1, \ldots, a_n) = ((\alpha + \beta)a_1, \ldots, (\alpha + \beta)a_n) \\ &= (\alpha a_1 + \beta a_1, \ldots, \alpha a_n + \beta a_n) = (\alpha a_1, \ldots, \alpha a_n) + (\beta a_1, \ldots, \beta a_n) \\ &= \alpha \cdot (a_1, \ldots, a_n) + \beta \cdot (a_1, \ldots, a_n) = \alpha \cdot u + \beta \cdot u. \end{aligned}$$

Exemplo 3.3. *O conjunto* $\mathbb{M}(\mathbb{R})_{n \times n}$ *das matrizes* $n \times n$ *com coeficientes em* $\mathbb{R}$ *é um* $\mathbb{R}$*-espaço vetorial com as operações de adição de matrizes (Definição* 1.23*) e multiplicação por escalares (Definição* 1.26*).*

Exemplo 3.4. *O conjunto de polinômios*

$$P(\mathbb{R}) = \{p(x) = a_n x^n + \cdots + a_1 x + a_0; a_i \in \mathbb{R} \text{ e } n \in \mathbb{N}\}$$

é um $\mathbb{R}$*-espaço vetorial com as operações usuais de adição de polinômios e multiplicação por escalar definidas na Proposição* 1.17.

Exemplo 3.5. *O conjunto* $\mathbb{C}$ *dos números complexos é um* $\mathbb{R}-$*espaço vetorial com as operações de adição e multiplicação por escalar definidas na Proposição* 1.2.

3.1 Produto Interno De Espaços Vetoriais

Nesta seção apresentamos o produto interno de espaços vetoriais para a posterior definição de ângulos entre vetores.

Definição 3.6. *Seja* V *um espaço vetorial sobre* $\mathbb{R}$. *Um produto interno sobre* V *é uma função que a cada par de vetores,* v_1 *e* v_2, *associa um número real, denotado* $\langle v_1, v_2 \rangle$, *satisfazendo as propriedades:*

i) $\langle v, v \rangle \geq 0$ *para todo vetor* v *e* $\langle v, v \rangle = 0$ *se, e somente se* $v = 0$

ii) $\langle \alpha v_1, v_2 \rangle = \alpha \langle v_1, v_2 \rangle$ *para todo* $\alpha \in \mathbb{R}$ *e todos* $v_1, v_2 \in V$.

iii) $\langle v_1 + v_2, v_3 \rangle = \langle v_1, v_3 \rangle + \langle v_2, v_3 \rangle$, *para quaisquer* $v_1, v_2 \in V$.

iv) $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle$ *para quaisquer* $v_1, v_2 \in V$.

Exemplo 3.7. *O produto interno usual de vetores do espaço* $\mathbb{R}^n$, *para* $v = (a_1, \ldots, a_n)$ *e* $w = (b_1, \ldots, b_n)$ *é dado por*

$$\langle v, w \rangle = a_1 b_1 + \cdots + a_n b_n.$$

Exemplo 3.8. *O produto interno usual de vetores do espaço* $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, *para* $z = a + bi$, $w = c + di \in \mathbb{C}$ *é dado por*

$$\langle z, w \rangle = ac + bd.$$

Definição 3.9. *Seja* V *um espaço vetorial com produto interno* $\langle \ , \ \rangle$. *Definimos a* ***norma*** *(ou comprimento) de um vetor* v *em relação a este produto interno por* $||v|| = \sqrt{\langle v, v \rangle}$. *Se* $||v|| = 1$, *isto é,* $\langle v, v \rangle = 1$, v *é chamado vetor* ***unitário***. *Dizemos também, neste caso, que* v *está* ***normalizado***.

Proposição 3.10. *Seja V um espaço vetorial com produto interno. Para quaisquer v, w em V e $\alpha \in \mathbb{R}$.*

i) $||v|| \geq 0$ *e* $||v|| = 0$ *se, e somente se* $v = 0$.

ii) $||\alpha v|| = |\alpha| \; ||v||$.

iii) $|\langle v, w\rangle| \leq ||v|| \; ||w||$. *(Desigualdade de Schwarz)*

iv) $||v + w|| \leq ||v|| + ||w||$. *(Desigualdade triangular)*

Demonstração: Consideremos V um espaço vetorial com produto interno $\langle \; , \; \rangle$.

$i)$ Seja $v \in V$. Pela Definição 3.9 temos que para qualquer $v \in V$, $||v|| = \sqrt{\langle v, v\rangle}$. Pela Definição 3.6 $i)$, temos,

$$\langle v, v\rangle \geq 0 \Leftrightarrow \sqrt{\langle v, v\rangle} \geq \sqrt{0} \Leftrightarrow ||v|| \geq 0.$$

Ainda,

$$||v|| = 0 \Leftrightarrow \sqrt{\langle v, v\rangle} = 0 \Leftrightarrow \langle v, v\rangle = 0 \Leftrightarrow v = 0.$$

$ii)$ Sejam $\alpha \in \mathbb{R}$ e $v \in V$. Então, pelas Definições 3.6 e 3.9,

$$\begin{aligned} ||\alpha v|| &= \sqrt{\langle \alpha v, \alpha v\rangle} \quad = \sqrt{\alpha \langle \; v, \alpha v\rangle} \\ &= \sqrt{\alpha \langle \; \alpha v, v\rangle} \;\; = \sqrt{\alpha \alpha \langle v, v\rangle} \\ &= \sqrt{\alpha^2 \langle v, v\rangle} \quad = \sqrt{\alpha^2}\sqrt{\langle v, v\rangle} \\ &= |\alpha| \; ||v||. \end{aligned}$$

$iii)$ Sejam v, $w \in V$.

Se $v = 0$ ou $w = 0$, vale a igualdade $|\langle v, w\rangle| = ||v|| \; ||w|| = 0$.

Suponhamos, então, $v \neq 0$ e $w \neq 0$. Para qualquer $\alpha \in \mathbb{R}$, temos que

$$\langle \alpha v + w, \alpha v + w\rangle \geq 0.$$

Pelas propriedades da Definição 3.6 e pelos itens $i)$ e $ii)$ desta Proposição, temos que:

$$\begin{aligned} \langle \alpha v, \alpha v + w\rangle + \langle w, \alpha v + w\rangle &= \langle \alpha v + w, \alpha v\rangle + \langle \alpha v + w, w\rangle \\ &= \langle \alpha v, \alpha v\rangle + \langle w, \alpha v\rangle + \langle \alpha v, w\rangle + \langle w, w\rangle \\ &= \alpha^2 \langle v, v\rangle + 2\alpha \langle v, w\rangle + \langle w, w\rangle \geq 0. \end{aligned}$$

Temos então um trinômio do segundo grau que deve ser positivo para qualquer valor de α. Como o coeficiente $\langle v, v\rangle$ de α^2 é sempre positivo, o discriminante Δ deve ser negativo. Assim

$$\Delta = 4\langle v, w\rangle^2 - 4\,\langle v, v\rangle\,\langle w, w\rangle \leq 0.$$

Isto é $4\langle v, w\rangle^2 - 4||v||^2\;||w||^2 \leq 0$, o que implica que

$$\langle v, w\rangle^2 \leq ||v||^2\;||w||^2,$$

ou ainda,

$$|\langle v, w\rangle| \leq ||v||\;||w||.$$

iv) Sejam $v, w \in V$. Pelas Definições 3.6, 3.9 e por esta Proposição *iii*), temos que

$$\begin{aligned}
||v+w||^2 &= \left(\sqrt{\langle v+w, v+w\rangle}\right)^2 \\
&= \langle v+w, v+w\rangle \\
&= ||v||^2 + 2\,\langle v, w\rangle + ||w||^2 \\
&\leq ||v||^2 + 2|\,\langle v, w\rangle\,| + ||w||^2 \\
&\leq ||v||^2 + 2||v||\;||w|| + ||w||^2 \\
&= (||v|| + ||w||)^2.
\end{aligned}$$

Extraindo as raízes quadradas de ambos os lados da desigualdade, temos

$$||v+w|| \leq ||v|| + ||w||.$$

3.2 Ângulo Entre Dois Vetores

Nesta seção definiremos ângulos entre dois vetores para, na próxima seção, mostrar que é existe ângulo entre matrizes.

Consideremos dois vetores u e v não nulos de um espaço vetorial V com produto interno $\langle\, ,\, \rangle$. Calculando a Desigualdade de Schwarz nos dos vetores u e v temos que

$$|\,\langle u, v\rangle\,| \leq ||u||\;||v||.$$

Dividindo ambos os lados por $||u||\ ||v||$ obtemos $\dfrac{|\langle v,w\rangle|}{||v||\ ||w||} \leq 1$, ou seja,

$$\left|\frac{\langle v,w\rangle}{||v||\ ||w||}\right| \leq 1,$$

isto nos diz que

$$-1 \leq \frac{\langle v,w\rangle}{||v||\ ||w||} \leq 1.$$

Como a função $\cos : [0,\pi] \longrightarrow [-1,1]$ é bijetora, existe um único $\theta \in [0,\pi]$ tal que

$$\cos\theta = \frac{\langle v,w\rangle}{||v||\ ||w||}.$$

Este ângulo θ é dito o ângulo entre os vetores u e v.

Exemplo 3.11. *Considere o produto interno usual no $\mathbb{R}^2$. O ângulo entre os vetores $u = (-2,-2)$ e $v = (0,2)$ é dado por*

$$\begin{aligned}
\cos\theta &= \frac{\langle v,w\rangle}{||v||\ ||w||} &&= \frac{(-2\cdot 0 + (-2)\cdot(-2))}{\sqrt{(-2)^2+(-2)^2}\cdot\sqrt{0^2+(-2)^2}} \\
&= \frac{0+4}{\sqrt{4+4}\cdot\sqrt{4}} &&= \frac{4}{\sqrt{8}\cdot 2} \\
&= \frac{4}{2\cdot\sqrt{2}\cdot 2} &&= \frac{4}{4\cdot\sqrt{2}} \\
&= \frac{1}{\sqrt{2}} &&= \frac{\sqrt{2}}{2}.
\end{aligned}$$

Então,

$$\theta = \arccos\frac{\sqrt{2}}{2} = \frac{\pi}{4}.$$

3.3 Ângulo Entre Duas Matrizes

Como visto no Exemplo 3.3, o conjunto $\mathbb{M}_{n\times n}(\mathbb{R})$ das matrizes $n\times n$ é um espaço vetorial. Assim temos que o conjunto $\mathbb{M}_{2\times 2}(\mathbb{R})$ das matrizes quadradas de ordem 2 também é um espaço vetorial.

Pela seção anterior, apresentamos que é possível definir ângulo entre dois vetores não nulos em um espaço vetorial munido de um produto interno. Motivados por isso e pelo isomorfismo algébrico entre $\mathbb{C}$ e $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R} \right\}$ queremos definir um produto interno entre duas matrizes quadradas não nulas de ordem 2. Em seguida queremos verificar se o isomorfismo Ψ definido no Exemplo 2.50 preserva ângulos.

Definição 3.12. *Sejam A, $B \in \mathbb{M}_{2\times 2}(\mathbb{R})$, com $A \neq 0$ e $B \neq 0$. Definimos o produto interno de A por B,*

$$\langle A, B \rangle = tr(A^t \cdot B).$$

Assim, se $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, então

$$\begin{aligned} \langle A, B \rangle &= tr(A^t \cdot B) \\ &= tr\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \\ &= tr\left(\begin{pmatrix} ae + cg & af + ch \\ be + dg & bf + dh \end{pmatrix} \right) \\ &= ae + cg + bf + dh. \end{aligned}$$

Em particular, $\langle A, A \rangle = a^2 + c^2 + b^2 + d^2$.

Vamos verificar se $\langle A, B \rangle = tr(A^t \cdot B)$ é um produto interno. Para isto vamos mostrar que $\langle A, B \rangle = tr(A^t \cdot B)$ satisfaz a Definição 3.6.

De fato,

i) Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$ temos que:

$$\langle A, A \rangle = a^2 + b^2 + c^2 + d^2.$$

Como a^2, b^2, c^2, d^2 são não negativos, segue que $\langle A, A \rangle \geq 0$. E $\langle A, A \rangle = 0$ se, e somante se, $a = 0,\ b = 0,\ c = 0$ e $d = 0$

$ii)$ Sejam $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$. Para mostrarmos a validade da Definição 3.6 $ii)$ utilizaremos a Proposição 1.34 $iii)$. Assim,

$$\begin{aligned}
\langle \alpha A, B\rangle &= \left\langle \alpha \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right\rangle \\
&= \left\langle \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right\rangle \\
&= tr\left(\begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}^t \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \\
&= tr\left(\begin{pmatrix} \alpha a & \alpha c \\ \alpha b & \alpha d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \\
&= tr\left(\alpha \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \\
&= \alpha \cdot tr\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \\
&= \alpha \cdot \langle A, B\rangle .
\end{aligned}$$

$iii)$ Sejam $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ e $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$. Então,

$$\langle A + B, C\rangle = \left\langle \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \begin{pmatrix} x & y \\ z & w \end{pmatrix} \right\rangle$$

$$= \left\langle \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}, \begin{pmatrix} x & y \\ z & w \end{pmatrix} \right\rangle$$

$$= tr\left(\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}^t \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right)$$

$$= tr\left(\begin{pmatrix} a+e & c+g \\ b+f & d+h \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right)$$

$$= tr\left(\begin{pmatrix} (a+e)x+(c+g)z & (a+e)y+(c+g)w \\ (b+f)x+(d+h)z & (b+f)y+(d+h)w \end{pmatrix}\right)$$

$$= tr\left(\begin{pmatrix} ax+ex+cz+gz & ay+ey+cw+gw \\ bx+fx+dz+hz & by+fy+dw+hw \end{pmatrix}\right)$$

$$= (ax+ex+cz+gz)+(by+fy+dw+hw)$$

$$= (ax+cz)+(ex+gz)+(by+dw)+(fy+hw).$$

Por outro lado temos que,

$$\langle A, C\rangle + \langle B, C\rangle = tr\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right) + tr\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}^t \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right)$$

$$= tr\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right) + tr\left(\begin{pmatrix} e & g \\ f & h \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right)$$

$$= tr\left(\begin{pmatrix} ax+cz & ay+cw \\ bx+dz & by+dw \end{pmatrix}\right) + tr\left(\begin{pmatrix} ex+gy & ez+gw \\ fx+hz & fz+hw \end{pmatrix}\right)$$

$$= (ax+cz)+(ex+gz)+(by+dw)+(fy+hw).$$

Como $\langle A+B, C\rangle = (ax+cz)+(ex+gz)+(by+dw)+(fy+hw) = \langle A, C\rangle + \langle B, C\rangle$, concluímos que $\langle A+B, C\rangle = \langle A, C\rangle + \langle B, C\rangle$.

$iv)$ Sejam $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathbb{M}_{2\times 2}(\mathbb{R})$

$$\begin{aligned} \langle A, B\rangle &= tr(A^t \cdot B) \\ &= tr\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \\ &= tr\left(\begin{pmatrix} ae+cg & af+ch \\ be+dg & bf+dh \end{pmatrix}\right) \\ &= (ae+cg)+(bf+dh). \end{aligned}$$

Agora, calculando $\langle B, A\rangle$, temos

$$\begin{aligned} \langle B, A\rangle &= tr(B^t \cdot A) \\ &= tr\left(\begin{pmatrix} e & g \\ f & h \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \\ &= tr\left(\begin{pmatrix} ea+gc & eb+gd \\ fa+hc & fb+hd \end{pmatrix}\right) \\ &= (ea+gc)+(fb+hd) \\ &= (ae+cg)+(bf+dh). \end{aligned}$$

Resultando que $\langle A, B\rangle = (ae+cg)+(bf+dh) = \langle B, A\rangle$.

Mostrando que $\langle A, B\rangle = tr(A^t \cdot B)$ está bem definida. Daí, temos a norma de $A \in \mathbb{M}_{2\times 2}(\mathbb{R})$ dada por

$$||A|| = \sqrt{tr(A^t \cdot A)} = \sqrt{\langle A, A\rangle}.$$

Considerando o conjunto $S = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R}\right\} \subseteq \mathbb{M}_{2\times 2}(\mathbb{R})$, e para todo $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in S$, temos

$$\langle A, A\rangle = (a^2+b^2)+(a^2+b^2) = 2\cdot(a^2+b^2).$$

Assim

$$||A|| = \sqrt{tr(A^t \cdot A)} = \sqrt{2 \cdot (a^2 + b^2)} = \sqrt{2} \cdot ||\Psi(A)||.$$

Portando,

$$||A|| = \sqrt{2} \cdot ||\Psi(A)||.$$

Além disso, para qualquer $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in S$, temos

$$\langle A, B \rangle = ac + (-b)(-d) + bd + ac = 2(ac + bd) = 2Re(\Psi(A \cdot B)).$$

O ângulo $\theta_{A,B}$ entre as matrizes A e B é definida como sendo

$$\begin{aligned} \cos\theta_{A,B} &= \frac{\langle A, B \rangle}{||A|| \cdot ||B||} \\ &= \frac{2(ac + bd)}{\sqrt{2} \cdot \sqrt{a^2 + b^2} \cdot \sqrt{2}\sqrt{c^2 + d^2}} \\ &= \frac{ac + bd}{\sqrt{a^2 + b^2}\sqrt{c^2 + d^2}}. \end{aligned}$$

Por outro lado , se $z_1 = \Psi(A) = a + bi$ e $z_2 = \Psi(B) = c + di$, sabemos que

$$\langle z_1, z_2 \rangle = ac + bd$$

e o ângulo θ_{z_1,z_2} entre z_1 e z_2 é tal que

$$\cos\theta_{z_1,z_2} = \frac{\langle z_1, z_2 \rangle}{||z_1|| \cdot ||z_2||} = \frac{ac + bd}{\sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2}} = \cos\theta_{A,B}.$$

Logo, o ângulo entre $A, B \in \mathbb{M}_{2\times 2}(\mathbb{R})$ e $\Psi(A), \Psi(B) \in \mathbb{C}$ coincidem. Mostrando que Ψ é mais que um isomorfismo algébrico, Ψ é também um isomorfismo geométrico.

Referências Bibliográficas

[1] BARROS, C. J. B. & SANTANA, A. J., *Estruturas Algébricas: Com Ênfase em Elementos da Teoria de Lie*. Maringá: Eduem, 2011.

[2] BEMM, L., *O "x"da Questão do Polinômio*. Disponível em: <http://files.laertebemm.webnode.com/200000059-8eb759082c/polinomios%20 semat.pdf> Acesso em 20 de maio de 2018.

[3] BOLDRINI, J. L.; COSTA, S. I. R.; FIGUEIREDO, V. L. & WETZLER, H. G *Álgebra Linear I*. São Paulo: Harper & Row do Brasil, 3ª ed., 1986.

[4] COELHO, F. U. & LOURENÇO, M. L., *Um Curso de Álgebra Linear*. São Paulo: Editora da Universidade de São Paulo, 2ª ed., 2007.

[5] FERNANDES, C. S. & BERNARDES, N. C. J., *Introdução às Funções de uma Variável Complexa*. Rio de Janeiro: SBM, 2ª ed., 2008.

[6] GONÇALVES, A.; *Introdução à Álgebra*. Projeto Euclides, IMPA-CNPq, 5ª ed., 2001.

[7] GILBERTO G. GARBI, *O Romance das Equações Algébricas*. São Paulo: Editora Livraria da Física, 3ª ed., 2009

[8] STEINBRUCH, A. & WINTERLE, P., *Introdução à Álgebra Linear*. São Paulo: Pearson Education do Brasil, 1997.