



Universidade de Brasília  
Departamento de Matemática

# Álgebra 1

Lineu Neto

1<sup>o</sup>/2004

## Sumário

<b>1</b>	<b>Noções de Lógica Simbólica</b>	<b>1</b>
	Relações entre Proposições . . . . .	5
	Lei da Álgebra das Proposições . . . . .	9
<b>2</b>	<b>Noções de Teoria dos Conjuntos</b>	<b>13</b>
	Leis da Álgebra de Conjuntos . . . . .	19
<b>3</b>	<b>Relações e Funções</b>	<b>23</b>
	Princípio da Boa Ordenação . . . . .	39
	Comentários Finais Sobre P.B.O. e Indução Matemática . . . . .	45
	Algumas Funções Importantes . . . . .	50
	Tópicos Importantes . . . . .	60
<b>4</b>	<b>Estruturas Algébricas</b>	<b>67</b>
	Principais Estruturas Algébricas . . . . .	68
	Propriedades de Uma Operação Binária . . . . .	71
	Tábua de Operação . . . . .	83
	Estruturas Algébricas Com Duas Operações Binárias . . . . .	89
	Exemplos de Anéis . . . . .	93
	Exemplos de Grupos . . . . .	116
<b>5</b>	<b>Homomorfismo Entre Estruturas Algébricas</b>	<b>125</b>
	Classificação de Homomorfismo . . . . .	125
<b>6</b>	<b>Polinômios</b>	<b>131</b>
	Polinômios $\times$ Funções Polinomiais . . . . .	134
	Divisibilidade e Raízes de Polinômios . . . . .	135
	Raízes de Polinômios . . . . .	139
	Curiosidades: (História da Matemática) . . . . .	141
	Comentários Finais Sobre Polinômios . . . . .	147
<b>7</b>	<b>Tópicos Especiais Sobre Anéis e Grupos</b>	<b>150</b>
	Subestrutura Algébrica . . . . .	150
	Anéis - Quociente . . . . .	160

<b>Exercícios Propostos</b>	<b>180</b>
Lógica & Conjuntos & Indução . . . . .	180
Relações & Funções . . . . .	184
Operações Binárias . . . . .	187
Homomorfismos & Polinômios . . . . .	189

# 1 Noções de Lógica Simbólica

**Definição 1.1 (Proposição Simples).** *Proposição (simples) é uma oração declarativa suscetível a um único valor lógico ( $V$  ou  $F$ ), sem ambigüidade.*

Exemplos de sentenças que não são proposições

- a)  $1 + 1$  (não é oração)
- b)  $\sqrt{2}$  é número racional? (não é afirmação)
- c)  $x + 1 = 0$  (não sabemos se tal sentença é  $V$  ou  $F$ , pois tal análise depende do valor atribuído à variável  $x$ )

**Definição 1.2 (Proposição Composta).** *Proposição composta é uma proposição obtida a partir de duas ou mais proposições simples, através do uso de modificadores e/ou conectivos.*

**Notações.**  $p, q, r$  - proposições simples  
 $P, Q, R$  - proposições compostas

**Observação.** Para determinar o valor lógico de uma proposição usamos um dispositivo prático chamado de *Tabela-Verdade*

- Modificador:  $\neg$  (ou  $\sim$ )  
(aplica-se a uma proposição). Lê-se: não  
 $p$  - proposição  
 $\neg p$  - negação de  $p$

*Tabela-Verdade da Negação*

$p$	$\neg p$
$V$	$F$
$F$	$V$

- Conectivos: (aplica-se a duas ou mais proposições)

1<sup>a</sup>)  $\vee$  (lê-se: “ou”)

**Observação.** Tal conectivo não tem caráter exclusivo.

$p, q$  - proposições

$p \vee q$  - disjunção de  $p$  e  $q$

*Tabela-Verdade da Disjunção*

$p$	$q$	$p \vee q$
$V$	$V$	$V$
$V$	$F$	$V$
$F$	$V$	$V$
$F$	$F$	$F$

2º)  $\wedge$  (lê-se: “e”)

$p, q$  - proposições

$p \wedge q$  - conjunção de  $p$  e  $q$

*Tabela-Verdade da Conjunção*

$p$	$q$	$p \wedge q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$F$
$F$	$F$	$F$

3º)  $\rightarrow$  (condicional simples)

$p, q$  - proposições

$p \rightarrow q$ :  $\begin{cases} \text{“se } p \text{ então } q” \text{ ou} \\ \text{“} p \text{ é condição suficiente para } q” \text{ ou} \\ \text{“} q \text{ é condição necessária para } p” \end{cases}$

*Tabela-Verdade da Condicional*

$p$	$q$	$p \rightarrow q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$V$
$F$	$F$	$V$

4º)  $\leftrightarrow$  (bicondicional)

$p, q$  - proposições

$p \leftrightarrow q$ :  $\begin{cases} \text{“} p \text{ se e somente se } q” \text{ ou} \\ \text{“} p \text{ é condição necessária e suficiente para } q” \text{ ou} \\ \text{“se } p \text{ então } q \text{ e reciprocamente”} \end{cases}$

*Tabela-Verdade da Bicondicional*

$p$	$q$	$p \leftrightarrow q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$F$
$F$	$F$	$V$

**Observação.**  $p \leftrightarrow q$  é  $V$  quando  $p$  e  $q$  têm o mesmo valor lógico (ou seja, ou ambas são verdadeiras ou ambas são falsas)

**Exercício:** Construa tabelas-verdade para as seguintes proposições:

- a)  $p \wedge (\neg p)$
- b)  $\neg(\neg p)$
- c)  $(p \rightarrow q) \leftrightarrow (\neg p) \vee q$
- d)  $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$  (muito importante)
- e)  $\neg(p \wedge q) \leftrightarrow (\neg p) \vee (\neg q)$
- f)  $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$

**Observação.** prioridade (de baixo pra cima):

$\leftrightarrow$   
 $\rightarrow$   
 $\wedge, \vee$   
 $\neg$

- a) (contradição)

$p$	$\neg p$	$p \wedge (\neg p)$
$V$	$F$	$F$
$F$	$V$	$F$

- b) 

$p$	$\neg p$	$\neg(\neg p)$
$V$	$F$	$V$
$F$	$V$	$F$

c) (tautologia)

$p$	$q$	$\neg p$	$p \rightarrow q$	$\neg p \vee q$	$(p \rightarrow q) \leftrightarrow (\neg p \vee q)$
$V$	$V$	$F$	$V$	$V$	$V$
$V$	$F$	$F$	$F$	$F$	$V$
$F$	$V$	$V$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$	$V$

d) (tautologia)

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$	$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
$V$	$V$	$F$	$F$	$V$	$V$	$V$
$V$	$F$	$F$	$V$	$F$	$F$	$V$
$F$	$V$	$V$	$F$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$	$V$	$V$

**Definição 1.3 (Tautologia).** Dizemos que uma proposição composta é uma Tautologia (ou proposição logicamente verdadeira) se o seu valor lógico é sempre  $V$ , independente dos valores lógicos das proposições simples que a constituem.

**Exemplos:** c, d (exercício anterior)

**Definição 1.4 (Contradição).** Dizemos que uma proposição composta é uma Contradição (ou proposição logicamente falsa) se o seu valor lógico é sempre  $F$ , independentemente dos valores lógicos das proposições simples que a constituem.

**Exemplo:** a (exercício anterior)

e) (tautologia)

$p$	$q$	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$(\neg p) \vee (\neg q)$	$\neg(p \wedge q) \leftrightarrow (\neg p) \vee (\neg q)$
$V$	$V$	$F$	$F$	$V$	$F$	$F$	$V$
$V$	$F$	$F$	$V$	$F$	$V$	$V$	$V$
$F$	$V$	$V$	$F$	$F$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$F$	$V$	$V$	$V$

f) (tautologia)

$p$	$q$	$r$	$q \vee r$	$p \wedge q$	$p \wedge r$	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
V	V	V	V	V	V	V	V	V
V	V	F	V	V	F	V	V	V
V	F	V	V	F	V	V	V	V
V	F	F	F	F	F	F	F	V
F	V	V	V	F	F	F	F	V
F	V	F	V	F	F	F	F	V
F	F	V	V	F	F	F	F	V
F	F	F	F	F	F	F	F	V

### Relações entre Proposições

**Definição 1.5 (Implicação Lógica).** *Sejam  $P$  e  $Q$  duas proposições (compostas). Dizemos que  $P$  implica em  $Q$ , simbolizado por  $P \Rightarrow Q$  se o condicional  $P \rightarrow Q$  é uma tautologia, isto é, se não ocorre de  $P$  ser  $V$  e  $Q$  ser  $F$ .*

**Observação.** Em matemática, a maioria dos *Teoremas* envolve uma implicação lógica do tipo:

$$\underbrace{\text{HIPÓTESE(S)}}_{\text{Teorema (proposição cuja veracidade depende de uma demonstração)}} \implies \text{TESE}$$

Teorema (proposição cuja veracidade depende de uma demonstração)

$$\begin{array}{ccc} \boxed{\text{Hipótese(s)}} & \longrightarrow & \boxed{\text{Tese}} \\ \text{(aquilo que temos)} & \text{argumento lógico} & \text{(conclusão, aquilo que)} \\ \text{como verdade)} & \text{(demonstração)} & \text{queremos demonstrar)} \end{array}$$

**Exemplo:**  $P : a$  é um número par;  $Q : a^2$  é um número par;  $P \Rightarrow Q$   
 $(P \rightarrow Q : \text{se } a \text{ é um número par, então } a^2 \text{ também o é})$

**Demonstração.**

H:  $a$  é um número par (isto é,  $a = 2k$ )

T:  $a^2$  é um número par (isto é,  $a^2 = 2l$ )

De fato:  $a^2 = (2k)^2 = 4k^2 = 2 \underbrace{(2k^2)}_l = 2l$

■



**Definição 1.6 (Equivalência de Proposição).** *Sejam  $P$  e  $Q$  proposições (compostas). Dizemos que  $P$  é equivalente a  $Q$ , simbolizado por  $P \Leftrightarrow Q$ , se o bicondicional  $P \leftrightarrow Q$  é uma tautologia, isto é, se  $P$  e  $Q$  têm a mesma tabela-verdade (mesmo valor lógico).*

**Observação.** Em matemática, certos teoremas envolvem uma equivalência de proposições. Neste caso:

$$\text{HIPÓTESE(S)} \iff \text{TESE}$$

**Exemplo:**  $P : a$  é um número par;  $Q : a^2$  é um número par;  $P \Leftrightarrow Q$   
 $P \leftrightarrow Q : a$  é um número par se, e somente se,  $a^2$  também o é.

**Demonstração.**

H:  $a$  é um número par

T:  $a^2$  é um número par

$(\Rightarrow) H \Rightarrow T$  (ok!)

$(\Leftarrow) T \Rightarrow H$

Vimos que  $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$  é uma tautologia. Assim,  $(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$  (contra-positiva, contra-recíproca)

Assim, mostrar que se  $a^2$  é par, então  $a$  é par é equivalente a mostrar que se  $a$  é ímpar, então  $a^2$  é ímpar.

De fato:  $(T \Rightarrow H) \Leftrightarrow (\neg H \Rightarrow \neg T)$

$a$  é ímpar:  $a = 2k + 1$

$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \underbrace{(2k^2 + 2k)}_l + 1 = 2l + 1 \Rightarrow a^2$  é ímpar ■

**Definição 1.7 (Sentença Aberta ou Função Proposicional).** *Uma sentença aberta é uma sentença que envolve uma ou mais variáveis.*

**Observação.** Uma sentença aberta NÃO é uma proposição, pois não sabemos definir o seu valor lógico, o qual depende da(s) variável(is) envolvida(s).

**Notação.**  $p(x)$  = sentença aberta que depende da variável  $x$ .

**Exemplo:**  $x + 1 = 0$

$$x := \underbrace{-1}_{cte} (V) \quad x := 1 (F)$$

Uma sentença aberta pode ser transformada numa proposição através de dois recursos:

i) atribuindo-se valores constantes à(s) variável(is) envolvida(s);

ii) usando quantificadores.

Dois quantificadores:

a) *Quantificador Universal*:  $\forall$  (lê-se: “para todo” ou “qualquer que seja”);

b) *Quantificador Existencial*:

–  $\exists$  (“existe” ou “existe pelo menos um”);

–  $\exists!$  (lê-se: “existe um único”);

–  $\nexists$  (lê-se: “não existe”).

**Notações.**  $(\forall x)(p(x))$ ;  $(\exists x)(p(x))$ ;  $(\exists! x)(p(x))$ ;  $(\nexists x)(p(x))$

**Exercício:** Considerando que todas as variáveis envolvidas são reais, use quantificadores para tornar proposições verdadeiras as seguintes sentenças abertas:

a)  $\sqrt{x^2} = x$ :  $(\exists x)(\sqrt{x^2}) \quad (x \geq 0)$

b)  $\sin(x+y) = \sin x \cos y + \sin y \cos x$ :  $(\forall x, y)(\sin(x+y) = \sin x \cos y + \sin y \cos x)$

c)  $\frac{x^2-1}{x-1} = x+1$ :  $(\exists x)\left(\frac{x^2-1}{x-1} = x+1\right) \quad (x \neq 1) \quad \text{ou} \quad (\forall x) \wedge (x \neq 1)$

d)  $|x| = -x$ :  $(\exists x)(|x| = -x) \quad (x \leq 0)$

e)  $x < x^2$ :  $(\exists x)(x < x^2) \quad (x < 0 \text{ ou } x > 1)$

f)  $x^2 + 1 = 0$ :  $(\nexists x)(x^2 + 1 = 0)$

Negação de Proposições e Sentenças Abertas Quantificadas:

1) Negação da negação:

$$\neg(\neg p) \Leftrightarrow p$$

2) Negação de conjunção: ( $e \leftrightarrow \text{ou}$ )

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$

**Exemplo:**  $p : a \neq 0, q : b \neq 0$

$$p \wedge q : a \neq 0 \text{ e } b \neq 0$$

$$\neg(p \wedge q) : a = 0 \text{ ou } b = 0$$

3) Negação de uma disjunção: ( $\text{ou} \leftrightarrow e$ )

$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

4) Negação de uma condicional:

$$\neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$$

**Exercício:** Verifique 4) de duas maneiras:

i) através da tabela-verdade;

$p$	$q$	$\neg q$	$p \rightarrow q$	$\neg(p \rightarrow q)$	$p \wedge \neg q$	$\neg(p \rightarrow q) \leftrightarrow p \wedge \neg q$
$V$	$V$	$F$	$V$	$F$	$F$	$V$
$V$	$F$	$V$	$F$	$V$	$V$	$V$
$F$	$V$	$F$	$V$	$F$	$F$	$V$
$F$	$F$	$V$	$V$	$F$	$F$	$V$

ii) usando o resultado anterior:  $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$  é uma tautologia

$$\begin{aligned} (p \rightarrow q) &\Leftrightarrow (\neg p \vee q) \\ \neg(p \rightarrow q) &\Leftrightarrow \neg(\neg p \vee q) \\ \neg(p \rightarrow q) &\Leftrightarrow p \wedge \neg q \end{aligned}$$

5) Negação de quantificadores: ( $\forall \leftrightarrow \exists$ )

$$\neg(\forall x)(p(x)) \Leftrightarrow (\exists x)(\neg p(x))$$

$$\neg(\exists x)(p(x)) \Leftrightarrow (\forall x)(\neg p(x))$$

**Exemplos:** (nos reais)

- a)  $(\forall x)(\sin^2 x + \cos^2 x = 1) \quad (V);$   
     negação:  $(\exists x)(\sin^2 x + \cos^2 x \neq 1) \quad (F)$
- b)  $(\exists x)(x^2 + 1 = 0) \quad (F)$   
     negação:  $(\forall x)(x^2 + 1 \neq 0) \quad (V)$

### Lei da Álgebra das Proposições

Qualquer proposição composta pode ser expressa apenas com os conectivos  $\wedge$  e  $\vee$  e com o modificador  $\neg$ . Em outras palavras, os conectivos  $\rightarrow$  e  $\leftrightarrow$  são “supérfluos”, pois podem ser escritos em termos de  $\wedge, \vee$  e  $\neg$ .

**Exemplo:**  $(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$

$$(p \leftrightarrow q) \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow (\neg p \vee q) \wedge (\neg q \vee p)$$

- $P$  = “coleção” de todas as proposições
- $p, q, r$  = proposições (“elementos de  $P$ ”)
- duas “operações” binárias:  $\wedge, \vee$
- uma “operação” unária:  $\neg$
- “Relação” de equivalência
- dois extremos universais:  $\begin{cases} v = \text{tautologia} \\ f = \text{contradição} \end{cases}$

$$P = P(\wedge, \vee, \neg, v, f) \quad (\text{Álgebra das Proposições})$$

**Teorema 1.8.**  $P$  satisfaz as seguintes equivalências:

$$I) \text{ (Leis Associativas) } \begin{cases} (p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r) \\ (p \vee q) \vee r \Leftrightarrow p \vee (q \vee r) \end{cases}$$

$$II) \text{ (Leis Comutativas) } \begin{cases} p \wedge q \Leftrightarrow q \wedge p \\ p \vee q \Leftrightarrow q \vee p \end{cases}$$

$$III) \text{ (Leis Idempotentes) } \begin{cases} p \wedge p \Leftrightarrow p \\ p \vee p \Leftrightarrow p \end{cases}$$

$$IV) \text{ (Leis de Absorção) } \begin{cases} p \wedge (p \vee q) \Leftrightarrow p \\ p \vee (p \wedge q) \Leftrightarrow p \end{cases}$$

$$V) \text{ (Leis Distributivas) } \begin{cases} p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r) \\ p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r) \end{cases}$$

$$VI) \text{ (Extremos Universais) } \begin{cases} p \wedge v \Leftrightarrow p \\ p \wedge f \Leftrightarrow f \\ p \vee v \Leftrightarrow v \\ p \vee f \Leftrightarrow p \end{cases}$$

$$VII) \text{ (Leis de Complementação) } \begin{cases} \neg(\neg p) \Leftrightarrow p \\ p \wedge \neg p \Leftrightarrow f \\ p \vee \neg p \Leftrightarrow v \end{cases}$$

$$VIII) \text{ (Leis de De Morgan) } \begin{cases} \neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q \\ \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q \end{cases}$$

### Demonstração.

IV)(tautologia)

$p$	$q$	$p \vee q$	$p \wedge (p \vee q)$	$p \wedge (p \vee q) \Leftrightarrow p$
$V$	$V$	$V$	$V$	$V$
$V$	$F$	$V$	$V$	$V$
$F$	$V$	$V$	$F$	$V$
$F$	$F$	$F$	$F$	$V$

I) (tautologia)

$p$	$q$	$r$	$p \wedge q$	$q \wedge r$	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$	$\wedge r \leftrightarrow p \wedge (q \wedge r)$
$V$	$V$	$V$	$V$	$V$	$V$	$V$	$V$
$V$	$V$	$F$	$V$	$F$	$F$	$F$	$V$
$V$	$F$	$V$	$F$	$F$	$F$	$F$	$V$
$V$	$F$	$F$	$F$	$F$	$F$	$F$	$V$
$F$	$V$	$V$	$F$	$V$	$F$	$F$	$V$
$F$	$V$	$F$	$F$	$F$	$F$	$F$	$V$
$F$	$F$	$V$	$F$	$F$	$F$	$F$	$V$
$F$	$F$	$F$	$F$	$F$	$F$	$F$	$V$

$$\text{VIII) } \neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$

$p$	$q$	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
$V$	$V$	$F$	$F$	$V$	$F$	$F$
$V$	$F$	$F$	$V$	$F$	$V$	$V$
$F$	$V$	$V$	$F$	$F$	$V$	$V$
$F$	$F$	$V$	$V$	$F$	$V$	$V$



**Observação.** Seja  $\mathcal{A}$  um “conjunto” munido de duas “operações” binárias  $(\wedge, \vee)$ , uma “operação” unária  $(\neg)$ , uma relação entre seus “elementos” e dois extremos universais  $(0, 1)$ . Dizemos que  $\mathcal{A} = \mathcal{A}(\wedge, \vee, \neg, 0, 1)$  é uma Álgebra de Boole (ou Álgebra Booleana) se  $\mathcal{A}$  satisfaz as propriedades (leis) I a VIII anteriores. Assim,  $P = P(\wedge, \vee, \neg, 0, 1)$  é uma Álgebra de Boole.

Vocabulário

- Definição
- Proposição
- Sentença aberta
- Teorema (Se hipóteses, então tese)
- Lema: “pequeno” Teorema (isto é, um Teorema auxiliar para demonstrar Teoremas mais complexos)
- Corolário: consequência de um Teorema
- Axioma (ou Postulado): proposição cuja veracidade é aceita sem demonstração (intuitivo)

**Exemplo:** (Geometria Plana)

Por um ponto fora de uma reta, passa uma única reta paralela à reta dada (5<sup>a</sup> Axioma de Euclides).



- Conceito Primitivo: base de qualquer teoria matemática (não se define)

**Exemplos:** ponto, reta, plano

**Objetivo:** “Demonstrar” Teoremas

Três técnicas básicas

a) Direta ( $H \Rightarrow T$ )

b) Indireta

b.1) contra-recíproco ( $\neg T \Rightarrow \neg H$ )

b.2) por absurdo: consiste em negar a tese (assumindo a hipótese verdadeira) e desenvolver um argumento lógico corrente que produza uma contradição da hipótese.

**Exemplo:** Teorema:  $\sqrt{2}$  é um número irracional.

**Demonstração.** T:  $\sqrt{2}$  é um número irracional

Suponha, por absurdo, que  $\sqrt{2}$  é racional, ou seja, que  $\sqrt{2} = a/b$ , onde  $a, b$  são números inteiros,  $b \neq 0$  e  $a$  e  $b$  não possuem fatores em comum (isto é,  $a/b$  é irredutível)

$$\sqrt{2} = \frac{a}{b} \Rightarrow (\sqrt{2})^2 = \frac{a^2}{b^2} \Rightarrow 2 = \frac{a^2}{b^2}$$

isto é,  $a^2 = 2b^2$  é um número par (\*)

Lembrando que, se  $a^2$  é par, então  $a$  é par. Logo,  $a = 2l$  (\*\*)

Substituindo (\*\*) em (\*), temos

$$(2l)^2 = 2b^2 \Rightarrow 4l^2 = 2b^2 \Rightarrow 2l^2 = b^2$$

isto é,  $b^2$  é par. Assim,  $b$  é par, isto é,  $b = 2m$  (\*\*\*)

**Conclusão:** De (\*\*) e (\*\*\*),  $a$  e  $b$  têm 2 como fator comum, o que contradiz nossa hipótese de a fração  $a/b$  ser irredutível.  $\sqrt{2}$  é irracional. ■

**Exercício:** (da 1ª Lista, pág. 180)

2) Considere as afirmações seguintes:

- Todo automóvel alemão é bom
- Se um automóvel é bom, então ele é caro
- Existem automóveis suecos bons
- Se não choveu, então todas as lojas estão abertas
- Se  $x < y$ , então  $z = 5$  ou  $z = 7$

Admitindo a veracidade dessas 5 afirmações e admitindo que existam automóveis franceses, alemães, suecos e coreanos, julgue os itens a seguir:

- a) (V) Se alguma loja está fechada, então choveu. (C-R)
- b) (V) Se um automóvel não é caro, então ele pode ser francês. (C-R)
- c) (V) Alguns automóveis suecos são caros.
- d) (F) Existem automóveis coreanos caros.
- e) (F) Um automóvel alemão pode não ser caro.
- f) (F) Se  $z \neq 5$  e  $z \neq 7$ , então  $x > y$ .

## 2 Noções de Teoria dos Conjuntos

Três conceitos primitivos

- Conjunto: qualquer coleção de objetos;
- Elemento: objeto que constitui um conjunto;
- Pertinência: relação entre conjunto e elemento.

**Notação.**

$A, B, C, \dots$  - conjuntos

$a, b, c, \dots$  - elementos

$x \in A$  (lê-se: “ $x$  pertence ao conjunto  $A$ ”)

$x \notin A$  (lê-se: “ $x$  não pertence a  $A$ ”)

**Definição 2.1 (Igualdade de Conjuntos).** *Dois conjuntos  $A$  e  $B$  são iguais se eles têm os mesmos elementos.*

**Notação.**  $A = B \Leftrightarrow (\forall x)((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A))$

**Exemplo:**  $A = \left\{ \frac{1}{3} \right\}, B = \left\{ \int_0^1 x^2 dx \right\}$   
 $A = B$

Caracterização de Conjuntos:



- i) Enumeração dos elementos do conjunto;
- ii) Através de uma propriedade (sentença aberta) específica dos elementos do conjunto;
- iii) Através de um dispositivo prático (Diagrama de Venn)

**Notação.**  $A = \{x \mid P(x)\}$

**Exemplo:**  $A = \{x \mid x \text{ é professor ou pesquisador de Álgebra do Departamento de Matemática}\}$

$B = \{y \mid y \text{ é a nacionalidade dos professores de Álgebra do Departamento de Matemática da UnB}\}$

$A = \{ \text{Pavel Zalesski, Pavel Shumyatsky, Alexei Krassilnikov, Rudolf Maier, Said Sidki, Salahoddin Shokranian, Nigel Pitt, Helder Matos, Marcus Vinícius, Hemar Godinho, Lineu Neto} \}$

$B = \{ \text{russo, alemão, árabe, iraniano, inglês, brasileiro} \}$

Alguns conjuntos notáveis:

- a) Universo: conjunto mais abrangente dentro de um certo contexto matemático;

**Notação.**  $E = \text{conjunto universo}$

Em C1, C2 e C3:  $E = \mathbb{R}$

Em VC:  $E = \mathbb{C}$

- b) Vazio: conjunto que não possui elementos;

**Notação.**  $\{ \}$  ou  $\emptyset$

- c) Unitário: conjunto que possui um único elemento.

**Exemplo:**  $A = \{x \mid x \text{ é um mês que possui apenas 28 ou 29 dias} \} = \{ \text{fevereiro} \}$

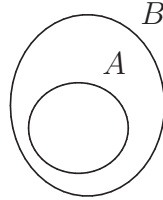
**Definição 2.2 (Inclusão).** *Sejam  $A$  e  $B$  conjuntos quaisquer. Dizemos que  $A$  é subconjunto de  $B$  (ou  $A$  é parte de  $B$  ou  $A$  está contido em  $B$  ou  $B$  contém  $A$ ) se todo elemento de  $A$  é também elemento de  $B$ .*

**Notação.**  $A \subseteq B$  (ou  $B \supseteq A$ )  $\Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$

**Negação:**  $A \not\subseteq B$  (ou  $B \not\supseteq A$ )  $\Leftrightarrow (\exists x)(x \in A \wedge x \notin B)$

Dizemos que  $A$  é um subconjunto próprio de  $B$  (ou  $A$  é parte própria de  $B$  ou  $B$  contém propriamente  $A$ ) se  $A \subseteq B$  e  $A \neq B$ .

Em termos de Diagrama de Venn:



**Notação.**  $A \subset B$

(ou  $A \subsetneq B$ )  $\Leftrightarrow (\forall x)(x \in A \rightarrow x \in B) \wedge (\exists x)(x \in B \wedge x \notin A)$

**Observações.** i)  $A = B \Leftrightarrow A \subseteq B$  e  $B \subseteq A$ ;

ii)  $A \subseteq A$ ;

iii)  $\emptyset \subseteq A$

De fato: suponha, por absurdo, que  $\emptyset \not\subseteq A$ . Assim,  $(\exists x)(x \in \emptyset \wedge x \notin A)$ . Mas, como  $\emptyset$  não possui elementos, isto é absurdo.

**Definição 2.3 (Conjunto das Partes de Um Conjunto).** *Dado um conjunto  $A$ , definimos o conjunto das partes de  $A$  como sendo o conjunto de todos os subconjuntos de  $A$ .*

**Notação.**  $P(A) = \{X \mid X \subseteq A\}$

**Observação.**  $X \in P(A) \Leftrightarrow X \subseteq A$

**Exemplos:**

a)  $A = \emptyset \Rightarrow P(A) = \{\emptyset\}$

b)  $A = \{a\} \Rightarrow P(A) = \{\emptyset, \{a\}\}$

c)  $A = \{a, b\} \Rightarrow P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

d)  $A = \{a, b, c\} \Rightarrow P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

**Observações.** a) Dado um conjunto  $A$ , definimos a cardinalidade de  $A$  como sendo o número de elementos de  $A$ .

**Notação.**  $|A|$  (ou  $n(A)$  ou  $\#A$ )

b) Se  $|A| = n$ , então  $|P(A)| = 2^n$

Conjuntos numéricos:

- $\mathbb{N} = \{1, 2, 3, 4, \dots\}$  (números naturais)  
convenção:  $0 \notin \mathbb{N}$
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  (números inteiros)
- $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \text{ e } b \neq 0\}$  (números racionais)
  - números com representação decimal finita:  $1/2 = 0.5$
  - números com representação decimal infinita periódica:  $1/3 = 0,333\dots$
- $\mathbb{R} = \mathbb{Q} \cup \{\text{números irracionais}\}$  (números reais)  
**Exemplos:**  $\sqrt{2} \cong 1,41$ ;  $\sqrt{3} \cong 1,73$ ;  $\pi \cong 3,14$ ;  $e \cong 2,71828$
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ e } i^2 = -1 \text{ ou } i = \sqrt{-1}\}$  (números complexos)

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Operações com Conjuntos ( $A, B \subseteq E$ )

A) União:  $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$

B) Intersecção:  $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$

C) Complementação:  $\mathbb{C}_E A = \{x \in E \mid x \notin A\}$

D) Diferença:  $A - B = \{x \mid x \in A \text{ e } x \notin B\}$  ou  $A \setminus B$

**Observações.** a) Se  $B \subseteq A$ , então podemos escrever  $A - B$  de uma maneira alternativa:

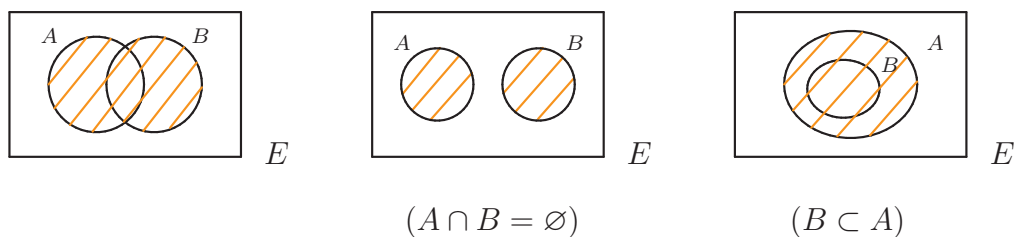
$$A - B = \underbrace{\mathbb{C}_A(B)}_{\text{complementar de } B \text{ em relação a } A} = \{x \mid x \in A \text{ e } x \notin B\}$$

b) Quando o conjunto universo  $E$  for explicitado (e não houver ambigüidade), vamos omiti-lo no símbolo do complementar. Assim,  $\mathbb{C}_E(A) = \mathbb{C}(A)$  ( $A \subseteq E$ ).

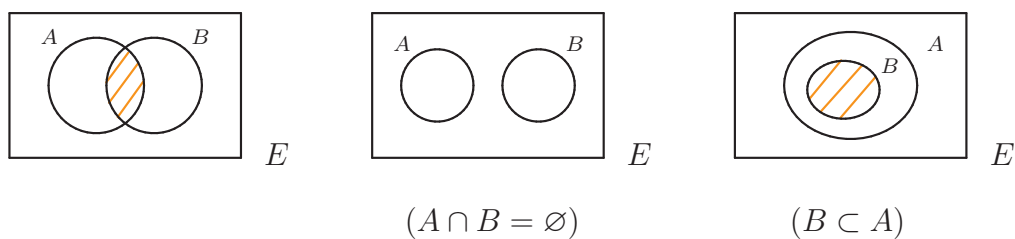
c) Se  $A \cap B = \emptyset$ , então  $A$  e  $B$  são ditos *conjuntos disjuntos*.

Em termos de Diagrama de Venn:

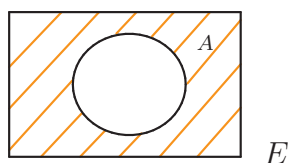
A) União:



B) Intersecção:



C) Complementação:



D) Diferença:

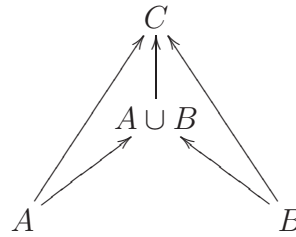


**Observações.** a)  $A \cup B$  é o “menor” conjunto que contém simultaneamente  $A$  e  $B$ , isto é:

a.1)  $A \subseteq A \cup B$  e  $B \subseteq A \cup B$ ;

a.2) Se  $A \subseteq C$  e  $B \subseteq C$ , então  $A \cup B \subseteq C$ .

**Notação.** (Reticulado)

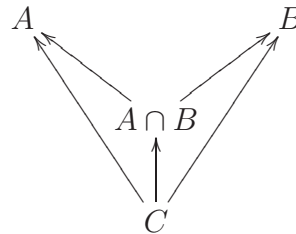


b)  $A \cap B$  é o “maior” conjunto que está contido simultaneamente em  $A$  e  $B$ , isto é:

b.1)  $A \cap B \subseteq A$  e  $A \cap B \subseteq B$ ;

b.2) Se  $C \subseteq A$  e  $C \subseteq B$ , então  $C \subseteq A \cap B$ .

**Notação.** (Reticulado)



**Exercícios:**

1) Sejam  $A, B \subseteq E$ . Mostre que se  $A \subseteq B$ , então  $\mathcal{C}_E(B) \subseteq \mathcal{C}_E(A)$ .

2) Sejam  $A, B \subseteq E$ . Mostre que:

a)  $\mathcal{C}_E(A \cup B) = \mathcal{C}_E(A) \cap \mathcal{C}_E(B)$  (1ª Lei de De Morgan)

b)  $\mathcal{C}_E(\mathcal{C}_E(A)) = A$

3) Sejam  $A, B, C, D \subseteq E$  tais que  $A \subseteq C$  e  $B \subseteq D$ . Mostre que:

a)  $A \cup B \subseteq C \cup D$

b)  $A \cap B \subseteq C \cap D$

4) Dê um contra-exemplo que refute a seguinte afirmação: se  $A \cup B = A \cup C$ , então  $B = C$ .

5) (Desafio) Mostre que se  $A \cup B = A \cup C$  e  $A \cap B = A \cap C$ , então  $B = C$

**Demonstração.** 1)

$$\begin{cases} \text{H: } A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B) & (*) \\ \text{T: } \mathbb{C}_E(B) \subseteq \mathbb{C}_E(A) \end{cases}$$

Queremos mostrar que dado  $x \in \mathbb{C}_E(B)$  qualquer, então  $x \in \mathbb{C}_E(A)$

$$x \in \mathbb{C}_E(B) \Rightarrow x \notin B \xrightarrow[(C-R)]{(*)} x \notin A \Rightarrow x \in \mathbb{C}_E(A)$$

Como  $x$  é arbitrário, então

$$(\forall x)(x \in \mathbb{C}_E(B) \rightarrow x \in \mathbb{C}_E(A)), \text{ isto é, } \mathbb{C}_E(B) \subseteq \mathbb{C}_E(A). \quad \blacksquare$$

**Demonstração.** 2) (se algum dos conjuntos envolvidos for  $\emptyset$ , não há nada a demonstrar)

a) Tome  $x \in \mathbb{C}_E(A \cup B)$

$$\begin{aligned} x \in \mathbb{C}_E(A \cup B) &\Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \text{ e } x \notin B \Leftrightarrow x \in \mathbb{C}_E(A) \text{ e } x \in \mathbb{C}_E(B) \\ &\Leftrightarrow x \in \mathbb{C}_E(A) \cap \mathbb{C}_E(B) \end{aligned}$$

b) Tome  $x \in \mathbb{C}_E(\mathbb{C}_E(A))$

$$x \in \mathbb{C}_E(\mathbb{C}_E(A)) \Leftrightarrow x \notin \mathbb{C}_E(A) \Leftrightarrow x \in A \quad \blacksquare$$

**Demonstração.** 3)

$$\begin{aligned} \text{H: } &\begin{cases} A \subseteq C & (*) \\ B \subseteq D & (**) \end{cases} \\ \text{T: } &\begin{cases} \text{a) } A \cup B \subseteq C \cup D \\ \text{b) } A \cap B \subseteq C \cap D \end{cases} \end{aligned}$$

$$\text{a) } x \in A \cup B \Rightarrow x \in A \text{ ou } x \in B \xrightarrow{(*)} x \in C \text{ ou } x \in D \Rightarrow x \in C \cup D$$

$$\text{b) } x \in A \cap B \Rightarrow x \in A \text{ e } x \in B \Rightarrow x \in C \text{ e } x \in D \Rightarrow x \in C \cap D \quad \blacksquare$$

### Leis da Álgebra de Conjuntos

- $E \neq \emptyset$  (conjunto universo)
- $A, B, C \subseteq E$  (isto é,  $A, B, C \in P(E)$ )
- duas “operações” binárias:  $\cup, \cap$
- uma “operação” unária:  $\mathbb{C}_E$

- dois extremos universais:  $\emptyset$  e  $E$

**Teorema 2.4.**  $(P(E), \cup, \cap, \complement_E, \emptyset, E)$  é uma Álgebra Booleana (ou Álgebra de Boole), isto é, satisfaz as seguintes leis:

- i) (associativas)  $\begin{cases} A \cup B(B \cup C) = (A \cup B) \cup C \\ A \cap B(B \cap C) = (A \cap B) \cap C \end{cases}$
- ii) (comutativas)  $\begin{cases} A \cup B = B \cup A \\ A \cap B = B \cap A \end{cases}$
- iii) (idempotentes)  $\begin{cases} A \cup A = A \\ A \cap A = A \end{cases}$
- iv) (absorção)  $\begin{cases} A \cup (A \cap B) = A \\ A \cap (A \cup B) = A \end{cases}$
- v) (distributivas)  $\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{cases}$
- vi) (extremos universais)  $\begin{cases} A \cup \emptyset = A \\ A \cap \emptyset = \emptyset \\ A \cup E = E \\ A \cap E = A \end{cases}$
- vii) (complementação)  $\begin{cases} A \cup \complement_E(A) = E \\ A \cap \complement_E(A) = \emptyset \\ \complement_E(\complement_E(A)) = A \end{cases}$
- viii) (de Morgan)  $\begin{cases} \complement_E(A \cup B) = \complement_E(A) \cap \complement_E(B) \\ \complement_E(A \cap B) = \complement_E(A) \cup \complement_E(B) \end{cases}$

Dois exemplos de Álgebras Booleanas

PROPOSIÇÕES	CONJUNTOS
$\vee$ (ou)	$\cup$
$\wedge$ (e)	$\cap$
$\neg$ (não)	$\complement_E$
$v$ (taut)	$E$ (universo)
$f$ (cont)	$\emptyset$
equivalência de proposições	igualdade de conjuntos

1<sup>a</sup> lista

6)  $A, B \subseteq E$

$$A \triangle B := (A - B) \cup (B - A)$$

ii) d) Tese:  $A \triangle B = (A \cup B) - (A \cap B)$  (igualdade de conjuntos)

**Demonstração.** Devemos mostrar a dupla inclusão:

I)  $A \triangle B \subseteq (A \cup B) - (A \cap B)$  e

II)  $(A \cup B) - (A \cap B) \subseteq A \triangle B$

I)  $A \triangle B \subseteq (A \cup B) - (A \cap B)$

Se  $A \triangle B = \emptyset$ , então não há nada a demonstrar. Se  $A \triangle B \neq \emptyset$ , então tome  $x \in A \triangle B$  (qualquer).

$$x \in A \triangle B \Rightarrow x \in (A - B) \cup (B - A)$$

$$\Rightarrow \begin{cases} x \in A - B \\ \text{ou} \\ x \in B - A \end{cases} \Rightarrow \begin{cases} x \in A \text{ e } x \notin B & (1) \\ \text{ou} \\ x \in B \text{ e } x \notin A & (2) \end{cases}$$

$$(1) \begin{cases} x \in A \\ \text{e} \\ x \notin B \end{cases} \xRightarrow{(*)} x \in A \cup B \text{ e } x \notin A \cap B \Rightarrow x \in (A \cup B) - (A \cap B)$$

$$(2) \begin{cases} x \in B \\ \text{e} \\ x \notin A \end{cases} \xRightarrow{(**)} x \in A \cup B \text{ e } x \notin A \cap B \Rightarrow x \in (A \cup B) - (A \cap B)$$

$$(*) A \subseteq A \cup B; A \cap B \subseteq B$$

$$(**) B \subseteq A \cup B; A \cap B \subseteq A$$

II)  $(A \cup B) - (A \cap B) \subseteq A \triangle B$

Se  $(A \cup B) - (A \cap B) = \emptyset$ , então não há nada a demonstrar.

Se  $(A \cup B) - (A \cap B) \neq \emptyset$ , então tome  $x \in (A \cup B) - (A \cap B)$  (qualquer).

$$x \in (A \cup B) - (A \cap B) \Rightarrow \begin{cases} x \in A \cup B \\ \text{e} \\ x \notin A \cap B \end{cases} \Rightarrow \begin{cases} x \in A \text{ ou } x \in B \\ \text{e} \\ x \notin A \text{ ou } x \notin B \end{cases}$$

$$\xRightarrow{\text{dist.}} \begin{cases} (x \in A \text{ ou } x \in B) \text{ e } (x \notin A) \\ \text{ou} \\ (x \in A \text{ ou } x \in B) \text{ e } (x \notin B) \end{cases}$$



$$\begin{aligned}
& \xRightarrow{\text{dist.}} \left\{ \begin{array}{l} (x \in A \text{ e } x \notin A) \text{ ou } (x \in B \text{ e } x \notin A) \\ \text{ou} \\ (x \in A \text{ e } x \notin B) \text{ ou } (x \in B \text{ e } x \notin B) \end{array} \right. \\
& \Rightarrow \left\{ \begin{array}{l} x \in B \text{ e } x \notin A \\ \text{ou} \\ x \in A \text{ e } x \notin B \end{array} \right. \Rightarrow x \in (A - B) \cup (B - A)
\end{aligned}$$

■

9)

$$(\Rightarrow) \left\{ \begin{array}{l} \text{H: } A \subseteq B \\ \text{T: } P(A) \subseteq P(B) \end{array} \right.$$

Queremos mostrar que  $P(A) \subseteq P(B)$ , isto é  $(\forall X)(X \in P(A) \rightarrow X \in P(B))$ . De fato:

Tome  $X \in P(A) \Rightarrow X \subseteq A \xRightarrow{A \subseteq B} X \subseteq B \Rightarrow X \in P(B)$ .

$$(\Leftarrow) \left\{ \begin{array}{l} \text{H: } P(A) \subseteq P(B) \\ \text{T: } A \subseteq B \end{array} \right.$$

Por hipótese,  $P(A) \subseteq P(B)$ , isto é,  $(\forall X)(X \in P(A)) \rightarrow (X \in P(B))$ . Em particular, tome  $X = A$ . Assim,  $A \in P(A)$  (pois  $A \subseteq A$ )  $\Rightarrow A \in P(B)$ , isto é  $A \subseteq B$ .

10)  $\emptyset \neq A, B \subseteq E$   
 $|A| < \infty; |B| < \infty$

Tese: a)  $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$

b)  $A \subseteq B \Rightarrow |B - A| = |B| - |A|$

c)  $|A \cup B| = |A| + |B| - |A \cap B|$

**Demonstração.**

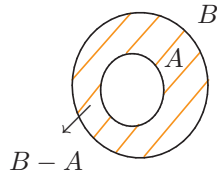
a)  $A = \{a_1, a_2, \dots, a_m\}$  ( $|A| = m \in \mathbb{N}$ )

$B = \{b_1, b_2, \dots, b_n\}$  ( $|B| = n \in \mathbb{N}$ )

Se  $A \cap B = \emptyset$ , então  $a_i \neq b_j, \forall 1 \leq i \leq m, \forall 1 \leq j \leq n$ . Então,  $A \cup B = \{a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n\}$ , isto é,  $|A \cup B| = m + n = |A| + |B|$ .

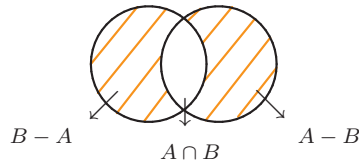
b) Observe que  $A \cap (B - A) = \emptyset$ .

Por a),  $|A \cup (B - A)| = |A| + |B - A| \Rightarrow |B - A| = |B| - |A|$ .



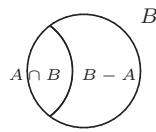
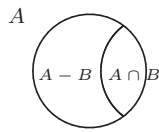
c) Usando a) (indução),

$$\underbrace{|(A - B) \cup (A \cap B) \cup (B - A)|}_{A \cup B} = \underbrace{|A - B|}_{\text{I}} + \underbrace{|A \cap B|}_{\text{II}} + \underbrace{|B - A|}_{\text{III}}$$



$$|A| \stackrel{\text{a)}}{=} |A - B| + |A \cap B| \Rightarrow |A - B| = |A| - |A \cap B| \quad (*)$$

$$|B| \stackrel{\text{a)}}{=} |A \cap B| + |B - A| \Rightarrow |B - A| = |B| - |A \cap B| \quad (**)$$



Substituindo (\*) em I e (\*\*) em III, temos

$$|A \cup B| = |A| - |A \cap B| + |A \cap B| + |B| - |A \cap B| = |A| + |B| - |A \cap B|$$

■

### 3 Relações e Funções

Conceito primitivo:

- par ordenado  $(a, b)$  (coordenada)

- igualdade de pares ordenados:

$$(a, b) = (c, d) \leftrightarrow \begin{cases} a = c & \text{e} \\ b = d \end{cases}$$

**Observação.** Não confundir conjunto com par ordenado.

*conjunto:* a ordem é irrelevante  $\{a, b\} = \{b, a\}$

*par ordenado:* a ordem é essencial  $(a, b) \neq (b, a)$  (se  $a \neq b$ )

**Definição 3.1 (Produto Cartesiano).** *Sejam  $A, B \neq \emptyset$ , Definimos o Produto Cartesiano de  $A$  por  $B$ , simbolizado por  $A \times B$ , como sendo o seguinte conjunto:*

$$A \times B \stackrel{\text{def}}{=} \{(x, y) \mid x \in A, y \in B\}$$

*Caso particular:*  $A = B$

$$A^2 = A \times A = \{(x, y) \mid x \in A, y \in A\}$$

**Observações.** a) Se  $|A| = m$  e  $|B| = n$ , então  $|A \times B| = m \cdot n$

b) Se  $A = \emptyset$  ou  $B = \emptyset$ , então  $A \times B = \emptyset$

c) Em geral,  $A \times B \neq B \times A$

**Exemplo:**  $A = \{1, 2, 3\}$ ,  $B = \{?, !\}$

$$A \times B = \{(1, ?), (1, !), (2, ?), (2, !), (3, ?), (3, !)\} \neq$$

$$B \times A = \{(? , 1), (? , 2), (? , 3), (! , 1), (! , 2), (! , 3)\}$$

d) Podemos generalizar produto cartesiano para  $n$  conjuntos ( $n \in \mathbb{N}$ )

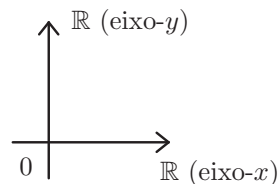
$$A_1, A_2, A_3, \dots, A_n \neq \emptyset$$

$$A_1 \times A_2 \times A_3 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) \mid x_i \in A_i, 1 \leq i \leq n\}$$

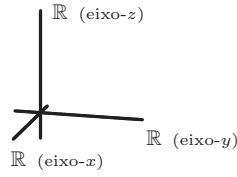
$$\text{Se } A_1 = A_2 = \dots = A_n = A, \text{ então } A^n = A \times A \times \dots \times A = \{(x_1, x_2, \dots, x_n) \mid x_i \in A, i = 1, \dots, n\}$$

**Exemplos:**

$$\text{a) } \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$



$$\text{b) } \mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$



**Definição 3.2 (Relação).** *Sejam  $A, B \neq \emptyset$ . Dizemos que  $R$  é uma relação (“binária”) de  $A$  em  $B$  se  $R$  é um subconjunto de  $A \times B$ .*

*Simbolicamente:  $R$  é relação de  $A$  em  $B \leftrightarrow R \subseteq A \times B$*

**Notações.** •  $a R b \Leftrightarrow (a, b) \in R$

(negação:  $a \nR b \Leftrightarrow (a, b) \notin R$ )

- $D(R)$  = domínio da relação  $R = \{x \in A \mid \exists y \in B, (x, y) \in R\} \subseteq A$   
(conjunto dos primeiros elementos dos pares ordenados de  $R$ )
- $Im(R)$  = imagem da relação  $R = \{y \in B \mid \exists x \in A, (x, y) \in R\} \subseteq B$   
(conjunto dos segundos elementos dos pares ordenados de  $R$ )

**Observações.** i) Uma relação pode ser representada de três maneiras:

- através de uma lei de formação que relacione elementos  $x \in A$  e  $y \in B$  (pares ordenados);
- através de Diagrama de Venn (se  $|A| < \infty$  e  $|B| < \infty$ ) (“diagramas de fecha”);
- no plano cartesiano;

- Se  $A = B$ , então uma relação  $R$  de  $A$  em  $B$  é dita relação sobre  $A$ .  
 $R$  é relação sobre  $A \Leftrightarrow R \subseteq A^2$

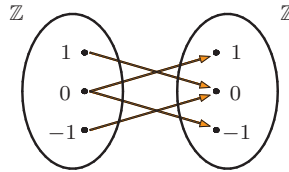
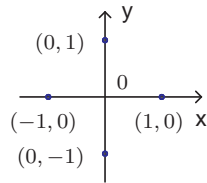
**Exemplos:**

- $A = \mathbb{Z}$   
 $R_1 = \{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = 1\} \subseteq \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$
- $A = \mathbb{R}$   
 $R_2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$
- $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{6, 7, 8\}$   
 $R_3 = \{(x, y) \in A \times B \mid x \text{ divide } y\}$

- d)  $A = \{a, b, c, d\}$ ,  $B = \{a, b, c\}$   
 $R_3 = \{(x, y) \in A \times B \mid x \text{ precede } y \text{ no alfabeto}\}$
- e)  $A = \mathbb{R}$   
 $R_5 = \{(x, y) \in \mathbb{R}^2 \mid x + y \leq 1\}$
- f)  $A = \{ \text{Cálculo 1, Cálculo 2, Cálculo 3} \}$ ,  
 $B = \{ \text{IAL, Cálculo Numérico, EDO, VC} \}$   
 $R_6 = \{(x, y) \in A \times B \mid x \text{ é pré-requisito direto de } y\}$

Em termos de gráficos e/ou diagramas de flechas, também temos as seguintes representações:

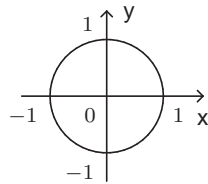
a)  $R_1 = \{(-1, 0), (1, 0), (0, 1), (0, -1)\}$



$$D(R_1) = \{-1, 0, 1\}$$

$$Im(R_1) = \{-1, 0, 1\}$$

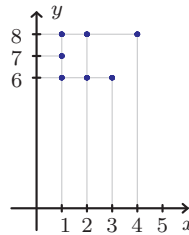
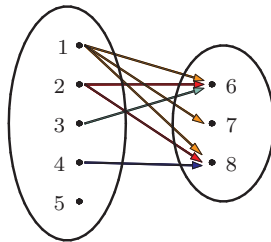
b) (círculo unitário)



$$D(R_2) = [-1, 1] = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$$

$$Im(R_2) = [-1, 1] = \{y \in \mathbb{R} \mid -1 \leq y \leq 1\}$$

c)  $R_3 = \{(1, 6), (1, 7), (1, 8), (2, 6), (2, 8), (3, 6), (4, 8)\}$

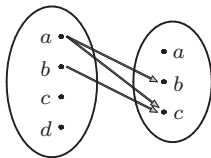


$$D(R_3) = \{1, 2, 3, 4\}$$

$$Im(R_3) = \{6, 7, 8\}$$

**Observação.** Sejam  $x, y \in \mathbb{Z}$ . Dizemos que “ $x$  divide  $y$ ” se existe  $z \in \mathbb{Z}$  tal que  $x \cdot z = y$ .

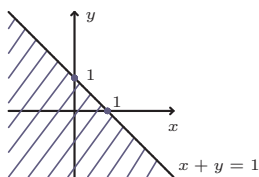
d)  $R_4 = \{(a, b), (a, c), (b, c)\}$



$$D(R_4) = \{a, b\}$$

$$Im(R_4) = \{b, c\}$$

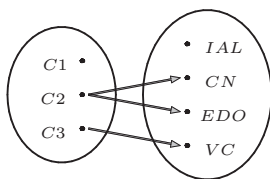
e) (semiplano inferior)



$$D(R_5) = \mathbb{R}$$

$$Im(R_5) = \mathbb{R}$$

f)  $R_6 = \{(C2, EDO), (C2, CN), (C3, VC)\}$



$$D(R_6) = \{C2, C3\}$$

$$Im(R_6) = \{EDO, CN, VC\}$$

**Definição 3.3 (Relação de Equivalência).** *Seja  $A \neq \emptyset$ . Seja  $R$  uma relação sobre  $A$  (isto é,  $R \subseteq A \times A$ ). Dizemos que  $R$  é uma Relação de Equivalência se  $R$  satisfaz as seguintes condições:*

(Reflexiva)(RE1)  $\forall a \in A, a R a$ ; (isto é,  $(a, a) \in R, \forall a \in A$ )

(Simétrica)(RE2)  $\forall a, b \in A, a R b \rightarrow b R a$ ; (isto é, se  $(a, b) \in R$ , então  $(b, a) \in R$ )

(Transitiva)(RE3)  $\forall a, b, c \in A, (a R b) \wedge (b R c) \rightarrow a R c$ . (isto é, se  $(a, b) \in R, (b, c) \in R$ , então  $(a, c) \in R$ )

**Exemplos:**

- 1)  $A = \{ \text{retas no plano} \}$   $r, s \in A$   
 $r R s \Leftrightarrow r \parallel s$  ( $r \cap s = \emptyset$  ou  $r = s$ )

**Afirmção.**  $R$  é relação de equivalência.

De fato:

(RE1)  $r R r$ , pois  $r = r$ ;

(RE2)  $r R s \rightarrow s R r$  ( $r \cap s = \emptyset \rightarrow s \cap r = \emptyset$ );

(RE3)  $r R s, s R t \rightarrow r R t$  ( $r \cap s = \emptyset \quad s \cap t = \emptyset \rightarrow r \cap t = \emptyset$ )

- 2)  $A = \{ \text{retas no plano} \} \quad r, s \in A$   
 $r R s \Leftrightarrow r \perp s \quad (r \cap s = \{p\})$

**Afirmação.**  $R$  não é relação de equivalência.

(RE1) FALHA, pois uma reta não é perpendicular a si mesma;

(RE2) é verdadeira, pois  $r \perp s \rightarrow s \perp r, \forall r, s \in A$ ;

(RE3) FALHA, pois  $r \perp s$  e  $s \perp t \nRightarrow r \perp t$

- 3)  $A = \{ \text{alunos de Álgebra 1 (turma A) - 1<sup>a</sup>/2004} \} \quad x, y \in A$   
 $x R y \Leftrightarrow x$  e  $y$  fazem o mesmo curso ( $\text{curso}(x) = \text{curso}(y)$ )

$R$  é relação de equivalência, pois:

(RE1)  $\forall x \in A, x R x$ ;

(RE2)  $\forall x, y \in A$ , se  $x R y$ , então  $y R x$ ;

(RE3)  $\forall x, y, z \in A$ , se  $x R y$  e  $y R z$ , então  $x R z$ .

- 4)  $E \neq \emptyset$

$A = P(E) = \{X \mid X \subseteq E\} \quad X, Y \in A$

$X R Y \Leftrightarrow X \subseteq Y$  (inclusão)

$R$  NÃO é relação de equivalência, pois

(RE1) é válida, pois  $X \subseteq X, \forall X \in A$ ;

(RE3) é válida, pois se  $X \subseteq Y$  e  $Y \subseteq Z$ , então  $X \subseteq Z, \forall X, Y, Z \in A$ ;

(RE2) FALHA, pois  $X \subseteq Y \nRightarrow Y \subseteq X$ .

**Exemplo:**  $E = \{1, 2, 3\}$

$X = \{1\} \subseteq E$  e  $Y = \{1, 2\} \subseteq E$

Temos que  $X \subseteq Y$ , mas  $Y \not\subseteq X$

- 5)  $A = \mathbb{Z}$

$x \in \mathbb{Z}$  é par se  $x = 2k, k \in \mathbb{Z}$

$x \in \mathbb{Z}$  é ímpar se  $x = 2k + 1, k \in \mathbb{Z}$

$x, y \in A$

$x R y \Leftrightarrow x - y = 2k, k \in \mathbb{Z}$  (isto é,  $x$  e  $y$  têm a mesma paridade)

$R$  é relação de equivalência, pois:

(RE1)  $\forall x \in A, x R x$ , pois  $x - x = 0 = 2 \cdot 0$

(RE2)  $\forall x, y \in A, \underbrace{x R y}_H \Rightarrow \underbrace{y R x}_T$ :

$$x R y \Rightarrow x - y = 2k \xrightarrow{\times(-1)} y - x = 2 \overbrace{(-k)}^{\in \mathbb{Z}} \Rightarrow y R x$$

(RE3)  $\forall x, y, z \in A, \underbrace{(x R y) \text{ e } (y R z)}_H \Rightarrow \underbrace{x R z}_T$ :

$$\left. \begin{array}{l} x R y \Rightarrow x - y = 2k \\ y R z \Rightarrow y - z = 2l \end{array} \right\} \Rightarrow x - y = 2 \underbrace{k+l}_{\in \mathbb{Z}} \Rightarrow x R z$$

Tal relação é chamada de Congruência Módulo 2 e é simbolizada por:  $x \equiv y \pmod{2}$  (lê-se:  $x$  é congruente a  $y$  módulo 2, isto é,  $x$  e  $y$  deixam o mesmo resto na divisão por 2) (dois restos possíveis  $\{0,1\}$ )

6) (Divisibilidade)

$$A = \mathbb{Z} \quad x, y \in \mathbb{Z}$$

Dizemos que “ $x$  divide  $y$ ” (ou “ $x$  é divisor de  $y$ ” ou “ $x$  é fator de  $y$ ” ou “ $y$  é múltiplo de  $x$ ” ou “ $y$  é divisível por  $x$ ”) se existe  $z \in A$  tal que  $x \cdot z = y$

Simbolicamente:

$$x \mid y^* \Leftrightarrow \exists z \in A, x \cdot z = y \quad *(\text{lê-se: } x \text{ divide } y)$$

Propriedades:

- a)  $1 \mid a, \forall a \in \mathbb{Z}$  (pois  $1 \cdot a = a$ );
- b)  $a \mid 0, \forall a \in \mathbb{Z}$  (pois  $a \cdot 0 = 0$ );  
(Em particular,  $0 \mid 0$ ) (é ind pois  $0 = 0x, \forall x \in A$ )
- c)  $a \mid a, \forall a \in \mathbb{Z}$  (pois  $a = a \cdot 1$ );
- d)  $a \mid b \text{ e } b \mid a \Rightarrow a = \pm b$ ;
- e)  $a \mid b \text{ e } c \mid d \Rightarrow ac \mid bd$ ;
- f)  $a \mid b \text{ e } b \mid c \Rightarrow a \mid c$ ; (transitiva)
- g)  $a \mid b \text{ e } a \mid c \Rightarrow a \mid bx + cy, \forall x, y \in A$ ;  
“ $a$  divide qualquer combinação linear inteira de  $b$  e  $c$ ”



$$x R y \Leftrightarrow x \mid y$$

$R$  não é relação de equivalência, pois:

(RE1) é verdadeira, pela propriedade c;

(RE3) é verdadeira, pela propriedade f;

(RE2) FALHA, pois  $a \mid b \not\Leftrightarrow b \mid a$ .

**Exemplo:**  $3 \mid 12$  (pois  $12 = 3 \cdot 4$ ), mas  $12 \nmid 3$ .

**Notações (para Relação de Equivalência).**  $A \neq \emptyset$  munido de uma relação de equivalência  $R$ .

- $R \leftrightarrow \sim$ ;  
 $(a R b \Leftrightarrow a \sim b)$
- $x \in A$   
 $A \supseteq \bar{x} \stackrel{\text{def}}{=} \{a \in A \mid a \sim x\}$   
 (classe de equivalência de  $x$  pela relação  $\sim$ )
- $A/\sim = \{\bar{x} \mid x \in A\}$   
 (conjunto quociente de  $A$  pela relação  $\sim$  ou conjunto de todas as classes de equivalência)

**Exemplos:** (Voltando aos exemplos anteriores)

1) (Paralelismo)

$$A = \{ \text{retas do plano} \} \quad r, s \in A$$

$$r \sim s \Leftrightarrow r \parallel s$$

$$\bar{r} = \{a \in A \mid a \sim r\} = \{a \in A \mid a \parallel r\} \text{ (feixe de retas paralelas a } r\text{)}$$

$$\bar{s} = \{a \in A \mid a \sim s\} = \{a \in A \mid a \parallel s\} \text{ (feixe de retas paralelas a } s\text{)}$$

(Tais conjuntos  $\bar{r}$  e  $\bar{s}$  representam direções do plano, horizontal e vertical, respectivamente)

$$A/\sim = \{\bar{a} \mid a \in A\} = \{ \text{direções do plano} \} = \{\rightarrow, \uparrow, \nearrow, \dots\}$$

3) (Disciplina de Álgebra 1)

$$A = \{ \text{alunos de Álgebra 1 (turma A) - 1}^{\text{o}}/2004 \} \quad x, y \in A$$

$$x \sim y \Leftrightarrow \text{curso}(x) = \text{curso}(y)$$

$\overline{\text{Jorge}} = \{a \in A \mid a \sim \text{Jorge}\} = \{a \in A \mid \text{curso}(a) = \text{MAT}\}$  (conjunto dos alunos de MAT desta disciplina representados por Jorge)

$$\overline{\text{Eduardo}} = \{a \in A \mid a \sim \text{Eduardo}\} = \{a \in A \mid \text{curso}(a) = \text{CIC}\}$$

$$\overline{\text{Renan}} = \{a \in A \mid a \sim \text{Renan}\} = \{a \in A \mid \text{curso}(a) = \text{curso}(\text{Renan}) = \text{ENE}\}$$

$$\overline{\text{Fernando}} = \{a \in A \mid a \sim \text{Fernando}\} = \{a \in A \mid \text{curso}(a) = \text{EST}\}$$

$$\overline{\text{Felipe}} = \{a \in A \mid a \sim \text{Felipe}\} = \{a \in A \mid \text{curso}(a) = \text{FIS}\}$$

$$A_{/\sim} = \{\bar{a} \mid a \in A\} = \{\overline{\text{Jorge}}, \overline{\text{Eduardo}}, \overline{\text{Renan}}, \overline{\text{Fernando}}, \overline{\text{Felipe}}\} \\ \{\text{MAT}, \text{CIC}, \text{ENE}, \text{EST}, \text{FIS}\}$$

A	$\overline{\text{Jorge}}$	$\overline{\text{Eduardo}}$	$\overline{\text{Renan}}$	$\overline{\text{Fernando}}$	$\overline{\text{Felipe}}$
	MAT	CIC	ENE	EST	FIS

(Partição de A)

**Observações.** a) As cinco classes acima são duas a duas disjuntas, isto é,  $\overline{X} \cap \overline{Y} = \emptyset$  (onde  $\overline{X} \neq \overline{Y}$ )

$$\text{b) } \overline{\text{Jorge}} \cup \overline{\text{Eduardo}} \cup \overline{\text{Renan}} \cup \overline{\text{Fernando}} \cup \overline{\text{Felipe}} = A$$

$$5) A = \mathbb{Z}$$

$$x \sim y \Leftrightarrow x - y = 2k, k \in \mathbb{Z}$$

$$\overline{0} = \{a \in A \mid a \sim 0\} = \{a \in \mathbb{Z} \mid a - 0 = 2k\} = \{a \in \mathbb{Z} \mid a = 2k\} = \{0, \pm 2, \pm 4, \pm 6, \dots\} \text{ (conjunto dos números pares)}$$

$$\overline{1} = \{a \in A \mid a \sim 1\} = \{a \in \mathbb{Z} \mid a - 1 = 2k\} = \{a \in \mathbb{Z} \mid a = 2k + 1\} = \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\} \text{ (conjunto dos números ímpares)}$$

$$A_{/\sim} = \{\overline{0}, \overline{1}\}$$

$$\begin{array}{|c|c|} \hline \overline{0} & \overline{1} \\ \hline \end{array} \quad A$$

**Observe que:** a)  $\overline{0} \cap \overline{1} = \emptyset$ ;

$$\text{b) } \overline{0} \cup \overline{1} = A$$

**Observações.** a)  $\overline{X} \neq \emptyset, \forall x \in A$ ; Isto se deve ao fato de uma relação de equivalência  $\sim$  satisfazer a propriedade reflexiva (RE1)  $\forall x \in A, x \sim x$ ; (ou seja,  $x \in \overline{X}$ )

b) Dois elementos são equivalentes se, e somente se, eles representam a mesma classe. (Isto é,  $\overline{X} = \overline{Y} \Leftrightarrow X \sim Y$ )

**Demonstração.**  $(\Rightarrow) \begin{cases} \text{H: } \overline{X} = \overline{Y} \\ \text{T: } x \sim y \end{cases}$

$$\overline{X} = \{a \in A \mid a \sim x\} = \{b \in A \mid b \sim y\} = \overline{Y}$$

$$x \in \overline{X} \text{ (pois } x \sim x) \Rightarrow x \in \overline{Y}, \text{ isto é, } x \sim y$$

$$\overline{X} = \overline{Y}$$

$$(\Leftarrow) \begin{cases} \text{H: } x \sim y \\ \text{T: } \overline{X} = \overline{Y} \end{cases} \text{ (igualdade de conjuntos)}$$

Queremos mostrar uma dupla inclusão:  $\overline{X} \subseteq \overline{Y}$  e  $\overline{Y} \subseteq \overline{X}$ .

Vamos mostrar apenas a 1ª inclusão (a 2ª é análoga, bastando trocar  $x$  por  $y$ ).

Tome  $a \in \overline{X}$  (arbitrário). Devemos mostrar que  $a \in \overline{Y}$

$$a \in \overline{X} \Rightarrow a \sim x \quad (\text{I})$$

$$\text{Por hipótese, } x \sim y \quad (\text{II})$$

De (I) e (II), segue que  $a \sim y$  (pela propriedade transitiva (RE3)). Assim,  $a \in \overline{Y}$ .

**Conclusão:**  $\overline{X} \subseteq \overline{Y}$  ■

**Definição 3.4 (Partição de Um Conjunto).** *Seja  $A \neq \emptyset$ . Seja  $B$  uma coleção não-vazia de subconjuntos de  $A$  (isto é,  $\emptyset \neq B \subseteq P(A)$ ). Dizemos que  $B$  é uma partição de  $A$  se:*

- i)  $\emptyset \notin B$ ; (isto é, todo elemento de  $B$  é não vazio)
- ii) Quaisquer dois elementos distintos de  $B$  são disjuntos (isto é,  $\forall B_1, B_2 \in B$ , se  $B_1 \neq B_2$ , então  $B_1 \cap B_2 = \emptyset$ )
- iii) A união de todos os elementos de  $B$  “reproduz” o conjunto original.  

$$\bigcup_{B_i \in B} B_i = A$$

**Teorema 3.5.** *Seja  $A \neq \emptyset$  munido de uma relação de equivalência  $\sim$ . Então, o conjunto quociente  $A/\sim = \{\overline{x} \mid x \in A\}$  é uma partição de  $A$ . (vide os três exemplos anteriores)*

**Demonstração.** Devemos verificar que  $A/\sim = B$  satisfaz as três condições de uma partição, a saber:

- i)  $\emptyset \notin A/\sim$ ;
- ii)  $\forall \overline{X}, \overline{Y} \in A/\sim$ , se  $\overline{X} \neq \overline{Y}$ , então  $\overline{X} \cap \overline{Y} = \emptyset$ ;

iii)  $\bigcup \overline{X} = A$ .

De fato:

- i) (ok!), pois  $\overline{X} \neq \emptyset$  (pois  $x \in \overline{X}$ );
- ii) Equivalentemente, pelo Contra-Recíproco (ou Contra-Positiva), vamos mostrar que se  $\overline{X} \cap \overline{Y} \neq \emptyset$ , então  $\overline{X} = \overline{Y}$ .

$$\text{Tome } a \in \overline{X} \cap \overline{Y} \Rightarrow \begin{cases} a \in \overline{X} \\ \text{e} \\ a \in \overline{Y} \end{cases} \Rightarrow \begin{cases} a \sim x \\ \text{e} \\ a \sim y \end{cases} \xRightarrow{\text{(RE2)}} \begin{cases} x \sim a \\ \text{e} \\ a \sim y \end{cases} \xRightarrow{\text{(RE3)}} \begin{cases} x \sim a \\ \text{e} \\ a \sim y \end{cases}$$

$$x \sim y \Rightarrow \overline{X} = \overline{Y}$$

iii) (igualdade de conjuntos)

I)  $\bigcup \overline{X} \subseteq A$ ;

De fato:  $\forall x \in A, \overline{X} \subseteq A \Rightarrow \bigcup \overline{X} \subseteq A$

II)  $A \subseteq \bigcup \overline{X}$ :

$\forall x \in A, x \in \overline{X} \subseteq \bigcup \overline{X} \Rightarrow x \in \bigcup \overline{X}$  ■

**Exemplo:** (exercício 1 da 2ª lista, pág. 184)

Determine todas as relações de equivalência sobre  $A = \{1, 2, 3\}$  e os respectivos conjuntos-quociente:

- $A = \{1\}$   
 $R = \{ (1,1) \}$  é a única relação de equivalência sobre  $A$   
 $\overline{1} = \{a \in A \mid a \sim 1\} = \{1\}$   
 $A_{/\sim} = \{\overline{1}\} = \{\{1\}\}$
- $A = \{1, 2\}$   
 $R_1 = \{ (1,1), (2,2) \}$  é uma relação de equivalência sobre  $A$   
 $R_2 = \{ (1,1), (2,2), (1,2), (2,1) \}$  é uma relação de equivalência  
Análise para  $R_1$ :  
 $\overline{1} = \{1\}$  e  $\overline{2} = \{2\}$   
 $A_{/R_1} = \{\overline{1}, \overline{2}\} = \{\{1\}, \{2\}\}$   
Análise para  $R_2$ :  
 $\overline{1} = \{1, 2\} = \overline{2}$   
 $A_{/R_2} = \{\overline{1}\}$

- $A = \{1, 2, 3\}$   
 $R_1 = \{(1, 1), (2, 2), (3, 3)\}$   
 $R_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$   
 $R_3 = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}$   
 $R_4 = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$   
 $R_5 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\} = A \times A$   
Análise para  $R_1$   
 $\bar{1} = \{1\}; \bar{2} = \{2\}; \bar{3} = \{3\}$   
 $A/R_1 = \{\bar{1}, \bar{2}, \bar{3}\} = \{\{1\}, \{2\}, \{3\}\}$   
Análise para  $R_2$   
 $\bar{1} = \{1, 2\} = \bar{2}; \bar{3} = \{3\}$   
 $A/R_2 = \{\bar{1}, \bar{3}\} = \{\{1, 2\}, \{3\}\}$   
Análise para  $R_5$   
 $\bar{1} = \bar{2} = \bar{3} = \{1, 2, 3\}$   
 $A/R_5 = \{I\} = \{\{1, 2, 3\}\}$   
Análise para  $R_3$ :  
 $\bar{2} = \{2\}; \bar{1} = \bar{3} = \{1, 3\}$   
 $A/R_3 = \{\bar{1}, \bar{2}\} = \{\{1, 3\}, \{2\}\}$   
Análise para  $R_4$ :  
 $\bar{1} = \{1\}; \bar{2} = \bar{3} = \{2, 3\}$   
 $A/R_4 = \{\bar{1}, \bar{2}\} = \{\{1\}, \{2, 3\}\}$

**Exercício:** Explique a razão pela qual as seguintes relações NÃO são de equivalência sobre  $A = \{1, 2, 3\}$

- $R^* = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$   
 não satisfaz a propriedade reflexiva para o 3 (RE1 falha)
- $R^{**} = \{(1, 1), (2, 2), (3, 3), (1, 2)\}$   
 não satisfaz a propriedade simétrica (falta  $(2, 1)$ ) (RE2 falha)
- $R^{***} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1)\}$   
 não satisfaz a propriedade transitiva (falta  $(2, 3)$  e  $(3, 2)$ ) (RE3 falha)

**Definição 3.6 (Relação de Ordem).** *Seja  $A \neq \emptyset$  munido de uma relação  $R$  (isto é,  $R \subseteq A \times A$ ). Dizemos que  $R$  é uma Relação de Ordem Parcial (ou que  $A$  é parcialmente ordenado por  $R$ ) se valem as seguintes condições:*

(RO1)  $\forall a \in A, a R a$  (isto é,  $(a, a) \in R$ ); (Reflexiva)

(RO2)  $\forall a, b \in A$ , se  $a R b$  e  $b R a$ , então  $a = b$ ; (Anti-Simétrica)

(RO3)  $\forall a, b, c \in A$ , se  $a R b$  e  $b R c$ , então  $a R c$ . (Transitiva)

**Observação.** Dizemos que  $R$  é uma relação de ordem total (ou que  $A$  é totalmente ordenado por  $R$ ) se, além de (RO1), (RO2) e (RO3), vale uma propriedade adicional:

(RO4)  $\forall a, b \in A$ , tem-se que ou  $a R b$  ou  $b R a$ ; (para  $a \neq b$ )  
(isto é, quaisquer dois elementos podem ser comparados)

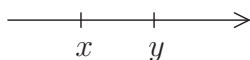
**Notação (para Relação de Ordem).**  $R \leftrightarrow \leq$  (lê-se: precede ou igual)

**Exemplos:**

1)  $A = \mathbb{N}$  (ou  $\mathbb{Z}$  ou  $\mathbb{Q}$  ou  $\mathbb{R}$ )

$x, y \in A$

$x \leq y \Leftrightarrow x - y \leq 0$  ( $\leq$  = ordem natural)



$\leq$  é relação de ordem total, pois

(RO1)  $x \leq x, \forall x \in A$ ;

(RO2)  $\forall x, y \in A, x \leq y$  e  $y \leq x \Rightarrow x = y$ ;

(RO3)  $\forall x, y, z \in A, x \leq y$  e  $y \leq z \Rightarrow x \leq z$ ;

(RO4)  $\forall x, y \in A, x \leq y$  ou  $y \leq x$

2)  $E \neq \emptyset$

$A = P(E) = \{X \mid X \subseteq E\}$

$X, Y \in A$

$X \leq Y \Leftrightarrow X \subseteq Y$  (lei de formação)

$\leq$  é uma relação de ordem parcial (em geral, não é total)

(RO1)  $\forall X \in A, X \subseteq X$ ;

(RO2)  $\forall X, Y \in A$ , se  $X \subseteq Y$  e  $Y \subseteq X$ , então  $X = Y$ ; (igualdade de conjuntos)

(RO3)  $\forall X, Y, Z \in A$ , se  $X \subseteq Y$  e  $Y \subseteq Z$ , então  $X \subseteq Z$

**Observações.** a) Em geral tal relação não é total.

**Exemplo:**  $E = \{1, 2\}$

$A = P(E) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

$X = \{1\}, Y = \{2\}$

Temos que  $X \not\subseteq Y$  e  $Y \not\subseteq X$ .

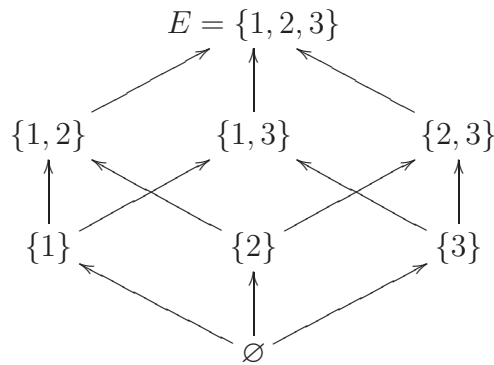
b) Se  $A$  é finito, então podemos representar graficamente uma relação de ordem através de um RETICULADO. (“Teoria dos Grafos”)

**Exemplo:**  $E = \{1, 2, 3\}$

$A = P(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

$X, Y \in A$

$X \leq Y \Leftrightarrow X \subseteq Y$  ( $\leq \leftrightarrow \subseteq$ )



**Observação.** Num reticulado é possível visualizar quando dois elementos não são comparáveis. Tais elementos devem estar no mesmo nível, de maneira que não haja aresta(s) ligando-os. No exemplo anterior,  $\{1\}$ ,  $\{2\}$ , e  $\{3\}$  estão no mesmo nível. Logo, não são comparáveis ( $\{1\} \not\subseteq \{2\}$  e  $\{2\} \not\subseteq \{1\}$ )

3)  $A = \mathbb{N}$

$x, y \in A$

$x \leq y \Leftrightarrow x \mid y$  (isto é,  $x \cdot z = y$ , para algum  $z \in A$ )

$\leq$  é uma relação de ordem parcial (não é total):

(RO1)  $\forall x \in A, x \mid x$  (pois  $x = 1 \cdot x$ );

(RO2)  $\forall x, y \in A$ , se  $\underbrace{x \mid y \text{ e } y \mid x}_{\text{H}}$ , então  $\underbrace{x = y}_{\text{T}}$ ;

De fato:

$x \mid y \Rightarrow x \cdot z_1 = y$  (I) ( $z_1 \in A$ )

$$y \mid x \Rightarrow y \cdot z_2 = x \quad (\text{II}) \quad (z_2 \in A)$$

(I)  $\rightarrow$  (II):

$$(x \cdot z_1) \cdot z_2 = x \Rightarrow z_1 \cdot z_2 = 1 \Rightarrow z_1 = 1 = z_2$$

Assim,  $x = y$ .

$$(\text{RO3}) \quad \forall x, y, z \in A, \text{ se } \underbrace{x \mid y \text{ e } y \mid z}_{\text{H}}, \text{ então } \underbrace{x \mid z}_{\text{T}}$$

$$x \mid y \Rightarrow x \cdot l = y \quad (\text{I}) \quad (l \in A)$$

$$y \mid z \Rightarrow y \cdot m = z \quad (\text{II}) \quad (m \in A)$$

(I)  $\rightarrow$  (II):

$$(x \cdot l) \cdot m = z \Rightarrow x \cdot \underbrace{(l \cdot m)}_{\in A} = z \Rightarrow x \mid z$$

Tal relação NÃO é total pois existem elementos em  $A$  que não são comparáveis.

**Exemplo:**  $x = 2, y = 3$

$$x \nmid y \text{ e } y \nmid x$$

**Exercícios:** 1) Usando a relação de divisibilidade, construa o reticulado correspondente ao conjunto  $A = \{x \in \mathbb{N} \mid x \text{ divide } 12\} = D_+(12)$

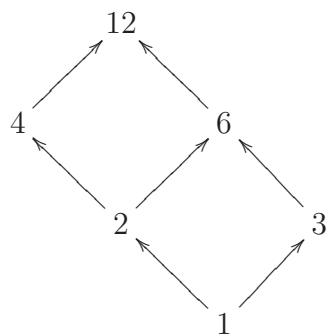
2) Mostre que a relação de divisibilidade em  $\mathbb{Z}$  não é relação de ordem (*Sugestão: verifique que (RO2) falha*).

**Resolução:**

$$1) \quad A = D_+(12) = \{1, 2, 3, 4, 6, 12\}$$

$$x, y \in A$$

$$x \leq y \Leftrightarrow x \mid y$$



$$2) \quad A = \mathbb{Z} \quad x, y \in A$$

$$x \leq y \Leftrightarrow x \mid y$$



(RO1)  $\forall x \in A, x \mid x$ ;  
 (RO2)  $\exists x, y \in A, x \mid y, y \mid x$  e  $x \neq y$   
 $x \mid y \Rightarrow y = x \cdot z_1 \quad (z_1 \in A) \quad (\text{I})$   
 $y \mid x \Rightarrow x = y \cdot z_2 \quad (z_2 \in A) \quad (\text{II})$   
 (II)  $\rightarrow$  (I):  
 $y = y \cdot z_2 \cdot z_1 \Rightarrow z_2 \cdot z_1 = 1 \Rightarrow z_1 = z_2 = \pm 1$   
 Então  $x = y$  ou  $x = -y$ , logo  $x$  pode ser diferente de  $y$ .

**Definição 3.7 (Elemento Mínimo e Elemento Máximo).** *Sejam  $E \neq \emptyset$  e  $\emptyset \neq A \subseteq E$  ( $A$  está ordenado por  $\leq$ ).*

*i) Dizemos que  $m$  é um elemento mínimo de  $A$  se:*

- a)  $m \in A$ ;*
- b)  $m$  é uma cota inferior de  $A$ , isto é,  $m \leq a, \forall a \in A$ .*

*ii) Dizemos que  $M$  é um elemento máximo de  $A$  se:*

- a)  $M \in A$ ;*
- b)  $M$  é uma cota superior de  $A$ , isto é,  $a \leq M, \forall a \in A$ .*

**Exemplos:**

- 1)  $A = \mathbb{N}$ ;  $\leq$  = ordem habitual  
 $A = \mathbb{N} = \{1, 2, 3, \dots\}$

- $A$  tem elemento mínimo ( $= 1$ ):  $1 = \min(A)$
- $A$  não tem elemento máximo (pois  $n < n + 1, \forall n \in A$ )

**Notação.**  $m = \min(A)$  e  $M = \max(A)$

- 2)  $E \neq \emptyset, A = P(E)$ ;  $\leq$  = inclusão  
 $A = \mathbb{N} = \{1, 2, 3, \dots\}$

- $A$  tem elemento mínimo:  $\emptyset = \min(A)$
- $A$  tem elemento máximo:  $E = \max(A)$

- 3)  $A = \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ ;  $\leq$  = ordem habitual

- $A$  não tem mínimo nem máximo (pois  $n - 1 < n < n + 1, \forall n \in A$ )

- 4)  $A = \{x \in \mathbb{Z} \mid x \leq 5\} = \{\dots, -1, 0, 1, 2, 3, 4, 5\}$ ;  $\leq$  = ordem habitual
- $A$  não tem mínimo, mas tem máximo:  $5 = \max(A)$
- 5)  $A = (0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ ;  $\leq$  = ordem habitual
- $A$  não tem elemento mínimo (embora seja limitado inferiormente)
- Observe que  $A$  possui infinitas cotas inferiores em  $E = \mathbb{R}$ :  $0, -1, -2, -3, \dots$ . Mas nenhum  $x_0 \in A$  é elemento mínimo (basta tomar  $x_1 = 1/2 x_0 < x_0$ ).
- $A$  não tem elemento máximo.

### P.B.O. (Princípio da Boa Ordenação)

- 1<sup>a</sup> versão: (para  $\mathbb{N}$ )  
 Todo subconjunto não-vazio de  $\mathbb{N}$  possui elemento mínimo (isto é,  $\forall \emptyset \neq A \subseteq \mathbb{N}, \exists \min(A)$ )
- 2<sup>a</sup> versão: (para  $\mathbb{Z}$ )  
 Todo subconjunto não-vazio e limitado inferiormente de  $\mathbb{Z}$  possui elemento mínimo.
- 3<sup>a</sup> versão: (caso geral)  
 Seja  $E \neq \emptyset$  munido de uma ordem total  $\leq$ .  $E$  é dito *bem ordenado* (ou  $\leq$  é uma *boa ordem*) se todo subconjunto não-vazio e limitado inferiormente de  $E$  possui elemento mínimo.

Princípio da Indução Matemática

### INDUÇÃO: PARTICULAR $\Rightarrow$ GERAL

**Observação.** Não confundir a indução matemática com a indução empírica (usada nas Ciências Naturais). A primeira delas é utilizada para demonstrar verdades matemáticas em conjuntos infinitos que possuem elemento mínimo. Tal indução baseia-se em lógica e não pode ser refutada (após demonstrada). A segunda delas é “mais fraca” pois tenta explicar os fenômenos naturais a partir de um número finito de observações (testadas experimentalmente), as quais podem ser invalidadas com o surgimento de uma nova teoria.

**Teorema 3.8 (Princípio de Indução Matemática - 1ª versão).** *Sejam  $n_0 \in \mathbb{Z}$  fixado e  $P(n)$  uma sentença aberta que depende de  $n$ , onde  $n \geq n_0$ . Suponha que  $P(n)$  satisfaça duas condições:*

i)  $P(n_0)$  é  $V$ ; (Base da Indução)

ii) Para todo  $n \geq n_0$ , se  $P(n)$  é  $V$ , então  $P(n+1)$  também o é. (Etapa da Indução)

Então,  $P(n)$  é  $V$ ,  $\forall n \geq n_0$

**Observação.** Na prática,  $P(n)$  é chamada de *Hipótese de Indução*. (fila infinita de dominós)

**Demonstração.** Defina  $A = \{n \in \mathbb{Z} \mid n \geq n_0 \text{ e } P(n) \text{ é } F\}$ . Queremos mostrar que  $A = \emptyset$ . Suponha, por absurdo, que  $A \neq \emptyset$ . Como  $\emptyset \neq A \subseteq \mathbb{Z}$  e é limitado inferiormente, então, pelo P.B.O. (2ª versão)  $\exists b = \min(A)$ , isto é,  $b \in A$  e  $b \leq n$ ,  $\forall n \in A$ .  $b$ : primeiro índice para o qual a sentença aberta é falsa. Como  $b \in A$ , segue que  $P(b)$  é  $F$ . (\*)

$$\begin{array}{c} n_0 \qquad \qquad b \\ | \qquad \qquad | \\ \hline \end{array}$$

Além disso,  $b \geq n_0$ . Por i),  $P(n_0)$  é  $V$ . Assim,  $b \in A \neq n_0 \notin A$  e, portanto,  $b > n_0$

$$\begin{aligned} b > n_0 &\Rightarrow b \geq n_0 + 1 \\ &\Rightarrow b - 1 \geq n_0 \end{aligned}$$

Como  $b - 1 < b$  e  $b$  é o primeiro índice para o qual  $P(n)$  é  $F$ , então  $P(b - 1)$  é  $V$ .

Por ii), se  $P(b - 1)$  é  $V$ , então  $P((b - 1) + 1) = P(b)$  é  $V$ . (\*\*)

Conclusão: de (\*) e (\*\*),  $P(b)$  é  $F$  e  $V$  (absurdo). Portanto,  $A = \emptyset$ . ■

**Exemplos:**

$$1) \underbrace{1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}}_{P(n) \quad (*)}, \quad \forall n \in \mathbb{N}. \quad n_0 = 1$$

i)  $P(1)$  é  $V$ :

$$1 = \frac{1(1+1)}{2} \quad (\text{ok!})$$

ii) Dado  $n \in \mathbb{N}$ , devemos mostrar que se  $P(n)$  é  $V$ , então  $P(n+1)$  também o é, ou seja, que

$$1 + 2 + \dots + (n+1) = \frac{(n+1)(n+2)}{2}$$

$$\begin{aligned} \text{De fato: } 1 + 2 + \dots + n + (n+1) &\stackrel{(*)}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \quad (\text{ok!}) \end{aligned}$$

Conclusão: de i) e ii), temos, pelo princípio de indução matemática que  $(*)$  é  $V$ ,  $\forall n \in \mathbb{N}$ .

2) Se  $f(x) = x^n$  ( $n \in \mathbb{Z}$ ), então  $f'(x) = nx^{n-1}$  ( $= P(n)$ )  $(*)$

1ª resolução: (sem indução)

$$f'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \rightarrow 0} \frac{(x+h)^n - x^n}{h} \stackrel{(\text{BN})}{=} nx^{n-1}$$

2ª resolução: (indução)

i)  $n_0 = 0$ ,  $P(0)$  é  $V$ :

$$\begin{aligned} f(x) &= x^0 = 1 \\ f'(x) &= 0 x^{0-1} = 0 \end{aligned}$$

ii) Dado  $n \geq 0$ , devemos mostrar que se  $(*)$  é  $V$  para  $n$ , então ela também é válida para  $n+1$ , isto é, se  $f(x) = x^{n+1}$ , então  $f'(x) = (n+1)x^n$ .

De fato:  $f(x) = x^{n+1} = x^n x$

Pela regra do produto para derivadas, temos

$$\begin{aligned} f'(x) &= (x^n x)' = (x^n)' x + x^n (x)' \stackrel{(*)}{=} (n x^{n-1}) x + x^n 1 \\ &= n x^n + x^n = (n+1) x^n \end{aligned}$$

Conclusão: de i) e ii), temos, pelo Princípio de Indução, que  $(*)$  é  $V$ ,  $\forall n \geq 0$ .

$$3) \text{ (Lista) } \underbrace{1 + x + x^2 + \dots + x^{n-1}}_{(*)} = \frac{(1 - x^n)}{1 - x}, \forall n \in \mathbb{N}, \forall x \in \mathbb{R}, x \neq 1$$

P.G.:  $a_1 = 1$  e  $q = x$

1ª resolução: (2ª grau e Cálculo 2)

$$\begin{aligned} S_n &= 1 + x + x^2 + \dots + x^{n-1} \quad (I) \\ x S_n &= x + x^2 + x^3 + \dots + x^n \quad (II) \end{aligned}$$

$$(I) - (II): S_n - x S_n = 1 - x^n$$

$$S_n(1 - x) = 1 - x^n \xrightarrow{x \neq 1} S_n = \frac{1 - x^n}{1 - x}$$

2ª resolução: (usando indução)

$$i) n = 1 \quad 1 = \frac{1 - x}{1 - x}$$

ii) Supondo que a hipótese de indução  $(*)$  é válida para  $n \geq 1$ , devemos mostrar a sua validade para  $n + 1$ , ou seja, que  $1 + x + \dots + x^n = (1 - x^{n+1})/(1 - x)$ .

De fato:

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

De i) e ii), temos, pelo Princípio de Indução, que  $(*)$  é válida  $\forall n \in \mathbb{N}$ .

4) (Exemplo onde a hipótese de indução não é fornecida) Problema: encontrar a soma dos  $n$  primeiros números ímpares naturais.

$n = 1$	$1$	$= 1$
$n = 2$	$1 + 3$	$= 4$
$n = 3$	$1 + 3 + 5$	$= 9$
$n = 4$	$1 + 3 + 5 + 7$	$= 16$
$n = 5$	$1 + 3 + 5 + 7 + 9$	$= 25$
$\vdots$		

$n$  genérico:  $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2 \quad (*)$   
 (hipótese de indução)

i)  $n = 1 : 1 = 1^2$  (ok!)

ii)  $P(n)$  é  $V \stackrel{?}{\Rightarrow} P(n+1)$  é  $V$ ;

$$P(n) : 1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2 \quad (*)$$

$$P(n+1) : 1 + 3 + 5 + 7 + \dots + (2n+1) = (n+1)^2 \quad (\text{a obter})$$

$$\text{De fato: } \overbrace{1 + 3 + 5 + 7 + \dots + (2n - 1)}^{(*)} + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2$$

De i) e ii),  $(*)$  é  $V, \forall n \in \mathbb{N}$ .

5) (Lista) (Desigualdade de Bernoulli)

$$(*) \quad (1 + x)^n \geq 1 + nx, \forall n \in \mathbb{N}, \forall x \in \mathbb{R}, x \geq -1$$

i)  $n = 1 : 1 + x \geq 1 + x$  (ok!)

ii)  $P(n)$  é  $V \stackrel{?}{\Rightarrow} P(n+1)$  é  $V$

$$P(n) : (1 + x)^n \geq 1 + nx \quad (V) \quad (*)$$

$$P(n+1) : (1 + x)^{n+1} \geq 1 + (n+1)x$$

Como  $x \geq -1$ , então  $x + 1 \geq 0$ . Logo, multiplicando  $(*)$  por  $x + 1$ , não alteramos o sentido da desigualdade:

$$(1 + x)^n \geq 1 + nx \xrightarrow{\times(x+1)} (1 + x)(1 + x)^n \geq (1 + x)(1 + nx) \Rightarrow (1 + x)^{n+1} \geq 1 + nx + x + nx^2 = 1 + (n+1)x + nx^2 \geq 1 + (n+1)x$$

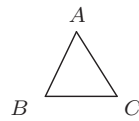
De i) e ii),  $(*)$  é  $V, \forall n \in \mathbb{N}$ .

6) (Lista) (Geometria Plana)

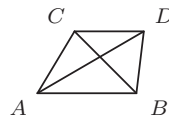
$$(*) \quad d_n = \frac{n(n-3)}{2}, \quad \forall n \in \mathbb{N}, \quad n \geq 3$$

$d_n$ : número de diagonais de um polígono convexo de  $n$  lados (diagonal: segmento de reta unindo vértices não adjacentes)

$$n = 3: 0 \text{ diagonais} \left( = \frac{3(3-3)}{2} \right)$$



$$n = 4: 2 \text{ diagonais} \left( = \frac{4(4-3)}{2} \right)$$



1ª resolução: (2ª grau)

$$\begin{aligned} C_{n,2} - n &= \binom{n}{2} - n = \frac{n!}{2!(n-2)!} - n = \frac{n(n-1)(n-2)!}{2(n-2)!} - n = \\ &= \frac{n(n-1)}{2} - n = \frac{n(n-1) - 2n}{2} = \frac{n^2 - 3n}{2} = \frac{n(n-3)}{2} \end{aligned}$$

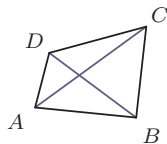
2ª resolução: (usando indução)

$$\text{i) } n = 3: 0 = \frac{3(3-3)}{2} = d_3 \quad (\text{ok!})$$

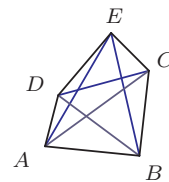
$$\text{ii) } P(n) \text{ é } V \Rightarrow P(n+1) \text{ é } V \quad (n \geq 3)$$

$$P(n): d_n = n(n-3)/2 \quad (V)$$

$$P(n+1): d_{n+1} = (n+1)(n-2)/2 \quad (\text{a obter})$$



$\overline{AC}, \overline{BD}$  = diagonais



$\overline{AC}, \overline{BD}, \overline{DC},$   
 $\overline{AE}, \overline{BE}$  = diagonais

Ao acrescentarmos mais um vértice, temos:

- i) as diagonais do polígono de  $n$  lados são preservados;
- ii) um dos lados do polígono original transforma-se numa diagonal;
- iii) pelo novo vértice, há  $n - 2$  novas diagonais.

Conclusão:

$$d_{n+1} = d_n + 1 + (n - 2) \stackrel{*}{=} \frac{n(n - 3)}{2} + (n - 1) = \frac{n(n - 3) + 2(n - 1)}{2} = \frac{n^2 - n - 2}{2} = \frac{(n + 1)(n - 2)}{2} \quad (\text{ok!})$$

De i) e ii),  $(*)$  é  $V$ ,  $\forall n \geq 3$ .

## 7) (Lista) (Conjuntos)

Se  $|A| = n$ , então  $|P(A)| = 2^n$  ( $n \in \mathbb{Z}_+$ )  $(*)$

i)  $n = 0$  :  $A = \emptyset$

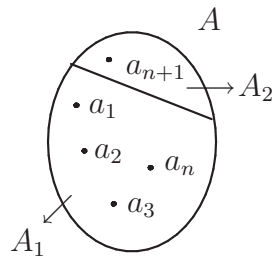
$$P(A) = \{\emptyset\}$$

$$|P(A)| = 1 = 2^0 \quad (\text{ok!})$$

ii)  $P(n)$  é  $V \stackrel{?}{\Rightarrow} P(n + 1)$  é  $V$  ( $n \geq 0$ )

$P(n)$ : se  $|A| = n$ , então  $|P(A)| = 2^n$  ( $V$ )

$P(n + 1)$ : se  $|A| = n + 1$ , então  $|P(A)| = 2^{n+1}$



$$\begin{cases} A = A_1 \cup A_2 = \{a_1, a_2, \dots, a_{n+1}\} \\ A_1 \cap A_2 = \emptyset \end{cases}$$

Seja  $B \subseteq A$ . Queremos mostrar que há  $2^{n+1}$  possibilidades para  $B$ . Observe que há dois casos a considerar:

1ª)  $a_{n+1} \notin B$ : nesse caso,  $B \subseteq A_1 = \{a_1, \dots, a_n\}$ . Por  $(*)$ , há  $2^n$  possibilidades para  $B$ ;

2ª)  $a_{n+1} \in B$ : nesse caso,  $B$  é obtido a partir dos subconjuntos de  $A_1$ , acrescentando-se  $a_{n+1}$ . Assim, há  $2^n$  possibilidades para  $B$ .

Conclusão: O número total de possibilidades é  $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

## Comentários Finais Sobre P.B.O. e Indução Matemática



1) As condições i) e ii) no princípio de indução (1<sup>a</sup> versão) são essências. Caso uma delas falhe, então não podemos aplicar a indução.

**Exemplo:** onde i) falha:

“Todo número natural coincide com o seu secessor”

$$(n = n + 1, \forall n \in \mathbb{N}) \quad (*)$$

Observe que ii) é válida, ou seja,  $P(n) \text{ é } V \Rightarrow P(n + 1) \text{ é } V \quad (n \in \mathbb{N})$

$$P(n) : n = n + 1 \quad (V)$$

$\Downarrow$

$$P(n + 1) : n + 1 = (n + 1) + 1 \quad (V)$$

Todavia, i) falha:  $P(1) \text{ é } F : 1 = 2 \quad (F)$

**Exemplo:** onde ii) falha

$$f(n) = n^2 - n + 41 \quad (n \in \mathbb{N})$$

**Afirmação.**  $f(n)$  é primo,  $\forall n \in \mathbb{N}$

**Definição 3.9 (Númeors Primos e Compostos).** *Seja  $n \in \mathbb{N}$*

a) *Dizemos que  $n$  é primo se:*

$$i) \quad n > 1;$$

$$ii) \quad n = a b \Rightarrow a = 1 \text{ ou } b = 1 \quad (a, b \in \mathbb{N})$$

$$D_+(n) = \{d \in \mathbb{N} \mid d \text{ divide } n\} = \{1, n\} \quad (\text{divisores triviais})$$

b) *Dizemos que  $n$  é composto se  $n$  não é primo, ou seja, se  $n$  possui divisores não-triviais ( $\neq 1, n$ )*

**Exemplos:** a) 2, 3, 5, 7, 11, 13, 17, 19, ... são primos

b) 4, 6, 8, 9, ... são compostos

Observe que i) é válida

$$n = 1 : f(1) = 1^2 - 1 + 41 = 41 \text{ é primo}$$

$$n = 2 : f(2) = 2^2 - 2 + 41 = 43 \text{ é primo}$$

$$n = 3 : f(3) = 3^2 - 3 + 41 = 47 \text{ é primo}$$

$\vdots$

$$n = 40 : f(40) = 40^2 - 40 + 41 = 1601 \text{ é primo}$$

Todavia, para  $n = 41$ ,  $f(n)$  é composto

$$f(41) = 41^2 - 41 + 41 = 41^2$$

$$D_+(41^2) = \{1, 41, 41^2\}$$

Assim, a condição ii) falha, pois  $f(40)$  é  $V$ , mas  $f(41)$  é  $F$ .

2) Há uma 2ª versão para o Princípio da Indução, cuja demonstração é similar a da 1ª versão.

**Teorema 3.10 (Princípio da Indução Matemática - 2ª versão).** *Sejam  $n_0 \in \mathbb{Z}$  (fixo) e  $P(n)$  uma sentença aberta que depende de  $n \in \mathbb{Z}$ , onde  $n \geq n_0$ . Suponha que  $P(n)$  satisfaça as seguintes condições:*

- i)  $P(n_0)$  é  $V$ ;
- ii) Dado  $m \in \mathbb{Z}$ ,  $m > n_0$ , se  $P(k)$  é  $V$  para todo  $n_0 \leq k < m$ , então  $P(m)$  é  $V$ .

Então,  $P(n)$  é  $V$ ,  $\forall n \geq n_0$ .

3) O elemento mínimo de um conjunto  $A$  parcialmente ordenado, quando existe, é único.

De fato: (unicidade)

Vamos mostrar que se  $m$  e  $m'$  são elementos mínimos de  $A$ , então  $m = m'$ .

$$\text{H: } \begin{cases} m = \min(A) \Rightarrow \begin{cases} \text{a) } m \in A \\ \text{b) } m \leq a, \forall a \in A \end{cases} \\ m' = \min(A) \Rightarrow \begin{cases} \text{a') } m' \in A \\ \text{b') } m' \leq a, \forall a \in A \end{cases} \end{cases}$$

T:  $m = m'$

De fato: de b) e a'),  $m \leq m'$   
de a) e b'),  $m' \leq m$

Por (RO2),  $m' = m$ .

**Definição 3.11 (Funções).** *Sejam  $A, B \neq \emptyset$ . Seja  $f$  uma relação de  $A$  em  $B$  (isto é,  $f \subseteq A \times B$ ). Dizemos que  $f$  é uma função (ou aplicação) de  $A$  em  $B$  se:*

- i)  $\forall x \in A, \exists y \in B \mid (x, y) \in f$ ;
- ii)  $\forall x \in A, \forall y, y' \in B$ , se  $(x, y) \in f$  e  $(x, y') \in f$ , então  $y = y'$ .

Em outras palavras: uma função  $f$  de  $A$  em  $B$  é uma Regra (ou correspondência) que associa a cada elemento  $x \in A$  um único elemento  $y \in B$ .

$$\begin{array}{ccccc} x \in A & \longrightarrow & \boxed{\text{FUNÇÃO}} & \longrightarrow & y \in B \\ & \text{entrada} & & & \text{saída} \end{array}$$

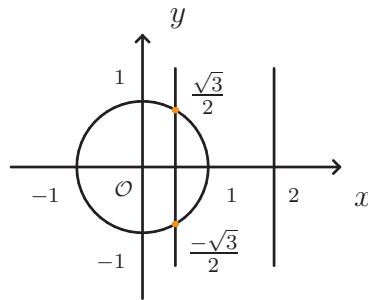
**Notação.**

$$\begin{aligned} f: A &\rightarrow B \\ x &\mapsto y = f(x) \end{aligned}$$

- $A$  = conjunto de partida = domínio de  $f$  ( $A = D(f)$ )
- $B$  = conjunto de chegada = contra-domínio de  $f$  ( $B = CD(f)$ )
- $x$  = variável independente
- $y$  = variável dependente
- $f: A \rightarrow B$  (“função de  $A$  em  $B$ ”)
- $f(x)$  = imagem de  $x$  por  $f$  ou valor de  $f$  em  $x$
- $Im(f)$  = imagem de  $f = \{y \in B \mid y = f(x), x \in A\} \subseteq B$
- Se  $A$  e  $B$  são conjuntos numéricos, então definimos o gráfico de  $f$  por:  
 $G(f) = \{(x, y) \in A \times B \mid y = f(x)\}$  (alguns autores identificam  $G(f)$  com  $f$ )

**Exemplos:** a)  $R_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$  é uma relação, mas não é função.

De fato:



i) falha, pois “sobram” elementos no domínio que não estão associados.

**Exemplo:**  $2 \in \mathbb{R}$  não está associado a nenhum outro elemento.

ii) falha, pois existem elementos no domínio com mais de uma imagem.

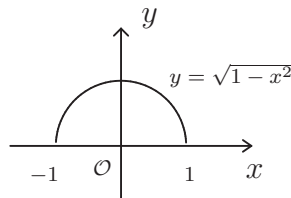
$\forall (x) \in (-1, 1)$ , existem duas imagens:  $\begin{cases} y = \sqrt{1-x^2} \\ y' = -\sqrt{1-x^2} \end{cases}$

**Exemplo:**  $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in R_1$  e  $\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \in R_1$

b)  $R_2 = \{(x, y) \in [-1, 1] \times \mathbb{R} \mid y = \sqrt{1-x^2}\}$  é função.

$f: [-1, 1] \rightarrow \mathbb{R}$

$x \mapsto y = f(x) = \sqrt{1-x^2}$



**Observações.** 1) Conhecido o gráfico de uma relação  $R$  de  $A$  em  $B$ , podemos verificar se a mesma é uma função. Isso ocorrerá se  $\forall x \in A$ , existir uma reta vertical interceptando o gráfico em um único ponto.

2) Conhecido o gráfico de uma função

$$\begin{aligned} f: A &\rightarrow B \\ x &\mapsto y \end{aligned}$$

obtemos  $D(f)$  e  $Im(f)$  através de projeções sobre os eixos coordenados

- $D(f) = A =$  projeção de  $G(f)$  sobre o eixo  $x$
- $Im(f) =$  projeção de  $G(f)$  sobre o eixo  $y$

No exemplo anterior:  $\begin{cases} D(f) = [-1, 1] \\ Im(f) = [0, 1] \end{cases}$

3) Em geral, trabalharemos com funções reais de uma variável real ( $A, B \subset \mathbb{R}$ ). Quando  $A$  não for explicitamente determinado, consideraremos o domínio como sendo o “maior” conjunto possível de valores para a variável independente  $x$ .

**Exemplo:** a)  $f(x) = \sqrt{1-x^2}$

$$D(f) = \{x \in \mathbb{R} \mid 1 - x^2 \geq 0\} = \{x \in \mathbb{R} \mid x^2 \leq 1\} = \{x \in \mathbb{R} \mid |x| \leq 1\} = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\} = [-1, 1]$$

Quando  $B$  não for explicitamente determinado, então  $B = \mathbb{R}$ .

>> Toda função é uma relação, mas nem toda relação é função.

**Definição 3.12 (Restrição e Prolongamento de Uma Função).** *Seja*

$$\begin{aligned} f: A &\rightarrow B \\ x &\mapsto y = f(x) \end{aligned}$$

*uma função. Seja  $A' \subseteq A$ . A função*

$$\begin{aligned} g: A' &\rightarrow B \\ x &\mapsto y = g(x) = f(x) \end{aligned}$$

*é dita uma RESTRIÇÃO de  $f$  a  $A'$  (Dizemos também que  $f$  é um PROLONGAMENTO de  $g$  a  $A$ ).*

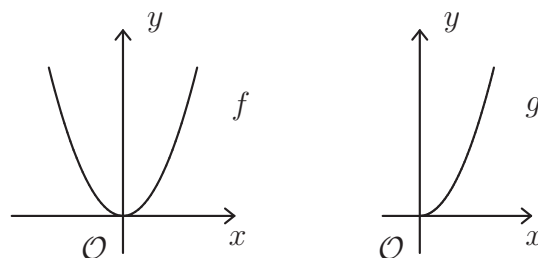
**Exemplo:**  $f: \mathbb{R} \rightarrow \mathbb{R}$  (prolongamento de  $g$ )

$$x \mapsto y = f(x) = x^2$$

$g: \mathbb{R}_+ \rightarrow \mathbb{R}$  (restrição de  $f$ )

$$x \mapsto y = g(x) = x^2$$

$$(\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\} \subseteq \mathbb{R})$$



**Notação.**  $g = f|_{A'}$  (lê-se:  $g$  é a restrição de  $f$  a  $A' \subseteq A$ )

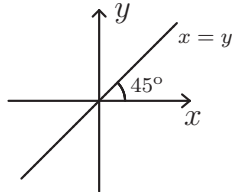
### Algumas Funções Importantes

A) (Função Identidade)

$$\begin{aligned} Id_A : A &\rightarrow A \\ x &\mapsto Id_A(x) = x \end{aligned}$$

Em particular, se  $A = \mathbb{R}$

$$\begin{aligned} Id_{\mathbb{R}} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto Id_{\mathbb{R}}(x) = x \end{aligned}$$



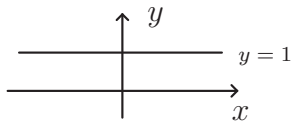
B) (Função Cte)

$$\begin{aligned} f : A &\rightarrow B \\ x &\mapsto y = f(x) = b \quad (\text{fixo}) \end{aligned}$$

$$Im(f) = \{b\}$$

Em particular, se  $A = B = \mathbb{R}$ :

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto f(x) = 1 \end{aligned}$$



C) (Seqüência de Números Reais) (Cálculo 2)

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{R} \\ n &\mapsto f(n) = a_n \end{aligned}$$

$$Im(f) = \{a_n \mid n \in \mathbb{N}\} = \{a_1, a_2, \dots\}$$

Na prática, identificamos uma seqüência com a coleção dos  $a_n$ 's dispostos numa certa ordem.

**Exemplo:** (seqüência cte)

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{R} \\ n &\mapsto f(n) = a_n = 1 \end{aligned}$$

$$\begin{aligned} \text{Im}(f) &= \{1, 1, 1, 1, \dots\} = \{1\} \\ &\neq \\ (a_n)_{n \in \mathbb{N}} &= (1, 1, 1, \dots, 1, \dots) \end{aligned}$$

**Definição 3.13 (Imagem Direta e Imagem Inversa).**

i) (*Imagem Direta*)

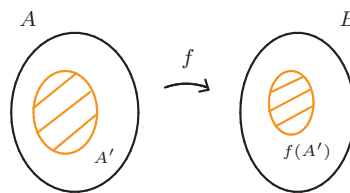
Sejam

$$\begin{aligned} f : A &\rightarrow B \\ x &\mapsto y = f(x) \end{aligned}$$

uma função e  $A' \subseteq A$ .

$$f(A') \stackrel{\text{def}}{=} \{f(x) \mid x \in A'\} \subseteq B$$

(*Imagem (Direta) de  $A'$  por  $f$* )

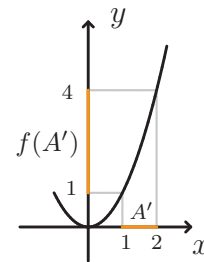


**Observação.** Se  $A' = A$ , então  $f(A') = \text{Im}(f)$

**Exemplo:**

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto y = f(x) = x^2 \end{aligned}$$

$$\begin{aligned} A &= \mathbb{R}, \quad A' = [1, 2] \\ f(A') &= f([1, 2]) = \{f(x) \mid x \in [1, 2]\} \\ &= \{x^2 \mid x \in [1, 2]\} = [1, 4] \end{aligned}$$



ii) (*Imagem Inversa*) (*não confundir com função inversa*)

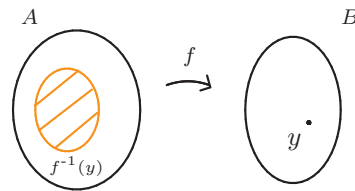
Sejam

$$\begin{aligned} f : A &\rightarrow B \\ x &\mapsto y = f(x) \end{aligned}$$

uma função e  $y \in B$ .

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in A \mid f(x) = y\} \subseteq A$$

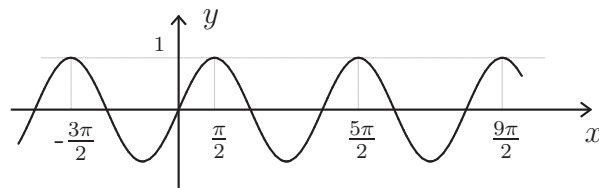
(Imagem Inversa ou pré-imagem de  $y$  por  $f$ )



**Exemplos:** a)  $f: \mathbb{R} \rightarrow \mathbb{R}$

$$x \mapsto y = f(x) = \sin x$$

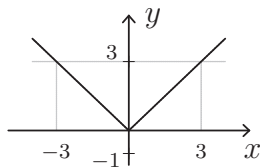
$$\begin{aligned} f^{-1}(1) &= \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid \sin x = 1\} \\ &= \{x \in \mathbb{R} \mid x = \pi/2 + 2k\pi, k \in \mathbb{Z}\} \end{aligned}$$



b)  $f: \mathbb{R} \rightarrow \mathbb{R}$

$$x \mapsto f(x) = |x|$$

$$\begin{aligned} f^{-1}(3) &= \{x \in \mathbb{R} \mid f(x) = 3\} = \{x \in \mathbb{R} \mid |x| = 3\} = \{-3, 3\} \\ f^{-1}(-1) &= \emptyset \end{aligned}$$



**Observações.** a) Se  $y \in B$  é tal que  $y \notin \text{Im}(f)$ , então  $f^{-1}(y) = \emptyset$ ;

b) Tal conceito pode ser generalizado para conjuntos



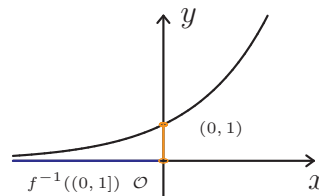
$$f: A \rightarrow B \quad ; \quad B' \subseteq B$$

$$x \mapsto y = f(x)$$

$$f^{-1}(B') \stackrel{\text{def}}{=} \{x \in A \mid f(x) \in B'\} \subseteq A$$

(Imagem inversa de  $B'$  por  $f$ )

**Exemplo:**  $f: \mathbb{R} \rightarrow \mathbb{R}$   
 $x \mapsto y = f(x) = e^x \quad (e \cong 2,71828)$   
 $Im(f) = (0, \infty) = \mathbb{R}_+^*$   
 $B' = (0, 1]$



$$\begin{aligned} f^{-1}(B') &= f^{-1}((0, 1]) = \{x \in \mathbb{R} \mid f(x) \in (0, 1]\} = (-\infty, 0] \\ &= \{x \in \mathbb{R} \mid x \leq 0\} \end{aligned}$$

**Definição 3.14 (Função Sobrejetora, Injetora e Bijetora).** *Seja*

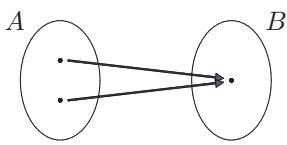
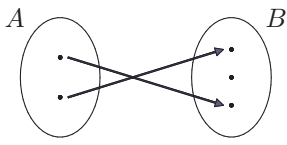
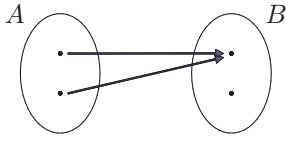
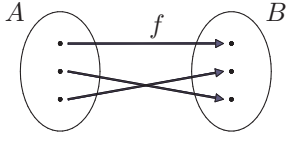
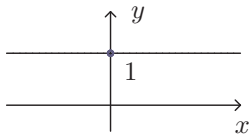
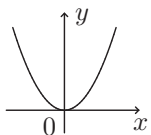
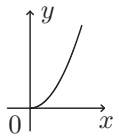
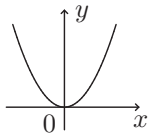
$$f: A \rightarrow B$$

$$x \mapsto y = f(x)$$

*uma função.*

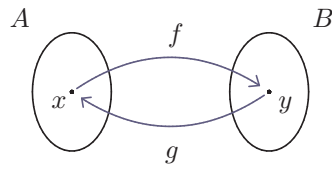
- i) (vide 1ª questão da 1ª lista)  $f$  é Injetora (ou Injetiva) se  $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$  (ou, pela contra-positiva,  $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ ).*
- ii)  $f$  é Sobrejetora (ou Sobrejetiva) se  $Im(f) = B$ , isto é,  $\forall y \in B, \exists x \in A \mid y = f(x)$ .*
- iii)  $f$  é Bijetora (ou Bijetiva ou Bijeção) se  $f$  é simultaneamente Injetora e Sobrejetora, isto é,  $\forall y \in B, \exists! x \in A \mid y = f(x)$ .*

**Exemplos:**

- 1)   $\left\{ \begin{array}{l} \text{é sobrejetora} \\ \text{não é injetora} \end{array} \right.$
- 2)   $\left\{ \begin{array}{l} \text{é injetora} \\ \text{não é sobrejetora} \end{array} \right.$
- 3)   $\left\{ \begin{array}{l} \text{não é injetora} \\ \text{não é sobrejetora} \end{array} \right.$
- 4)   $\left\{ \begin{array}{l} \text{é injetora} \\ \text{é sobrejetora} \end{array} \right. \Rightarrow \text{é bijetora}$
- 5)  $f : \mathbb{R} \rightarrow \mathbb{R}$   
 $x \mapsto f(x) = 1$    $\left\{ \begin{array}{l} \text{não é injetora} \\ \text{não é sobrejetora} \end{array} \right.$
- 6)  $f : \mathbb{R} \rightarrow \mathbb{R}$   
 $x \mapsto f(x) = x^2$    $\left\{ \begin{array}{l} \text{não é injetora} \\ \text{não é sobrejetora} \end{array} \right.$
- 7)  $f : \mathbb{R}_+ \rightarrow \mathbb{R}$   
 $x \mapsto f(x) = x^2$    $\left\{ \begin{array}{l} \text{é injetora} \\ \text{não é sobrejetora} \end{array} \right.$
- 8)  $f : \mathbb{R} \rightarrow \mathbb{R}_+$   
 $x \mapsto f(x) = x^2$    $\left\{ \begin{array}{l} \text{é sobrejetora} \\ \text{não é injetora} \end{array} \right.$



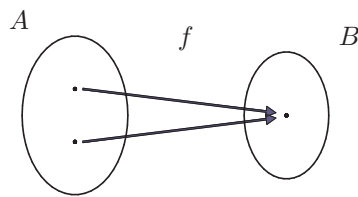




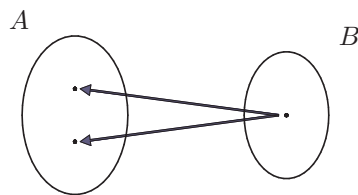
$$(g \circ f)(x) = g(f(x)) = g(y) = x$$

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

**Observação.** 1)

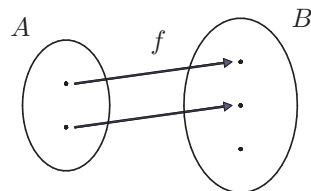


$\left\{ \begin{array}{l} \text{é sobrejetora} \\ \text{não é injetora} \end{array} \right.$

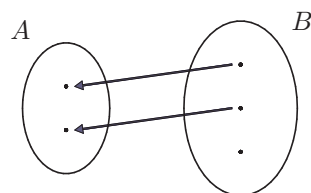


$\nexists g$  (função)

2)



$\left\{ \begin{array}{l} \text{é injetora} \\ \text{não é sobrejetora} \end{array} \right.$



não é função ( $\nexists g$ )

3)  $f : A \rightarrow B$   
 $x \mapsto y = f(x)$  é inversível  $\Leftrightarrow f$  é bijeção

Neste caso:

$$f^{-1} = g : B \rightarrow A$$

$$y \mapsto g(y) = x$$

onde  $x$  é o único elemento de  $A$  tal que  $f(x) = y$ .

Neste caso:

a)  $D(f) = Im(f^{-1});$

b)  $Im(f) = D(f^{-1});$

c)  $(x, y) \in f \Leftrightarrow (y, x) \in f^{-1}$

(Se  $A$  e  $B$  são conjuntos numéricos, então os gráficos de  $f$  e  $f^{-1}$  são simétricos em relação à reta  $y = x$ )

d)  $y = f(x) \Leftrightarrow x = f^{-1}(y)$

$$x \xrightleftharpoons[f^{-1}]{f} y$$

Para esboçar os gráficos de  $f$  e  $f^{-1}$  num mesmo sistema de eixos coordenados, trocamos  $x$  por  $y$  em  $f^{-1}$ . Assim,

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

$$\downarrow \text{mudança de variável}$$

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

**Exemplos:**

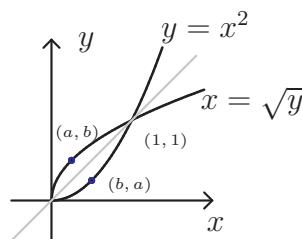
a)  $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+$  (bijetora)

$$x \mapsto f(x) = x^2$$

$\Rightarrow \exists f^{-1}$

$$y = f(x) = x^2 \Rightarrow x = \pm\sqrt{y} \xrightarrow{x \geq 0} x = f^{-1}(y) = \sqrt{y}$$

ou  $y = f^{-1}(x) = \sqrt{x}$



b)  $f : \mathbb{R} \rightarrow \mathbb{R}_+$  (bijeção)

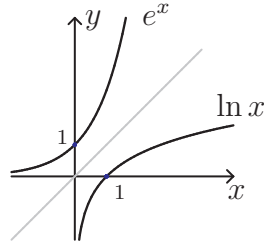
$$x \mapsto f(x) = e^x$$

$$x \neq y \Rightarrow e^x \neq e^y \quad inj$$

$$CD(f) = \mathbb{R}_+ = Im(f) \quad sob$$

$$\Rightarrow \exists f^{-1}$$

$$y = e^x \Rightarrow x = \ln y \text{ ou } y = \ln x$$



### Tópicos Importantes

A) Determinar o número de funções  $f : A \rightarrow B$ , onde  $A$  e  $B$  são finitos:

$$A = \{a_1, \dots, a_m\} \quad (|A| = m \in \mathbb{N})$$

$$B = \{b_1, \dots, b_n\} \quad (|B| = n \in \mathbb{N})$$

**Notação.**      •  $\mathcal{F}(A, B) = \{f : A \rightarrow B \mid f \text{ é função}\}$

$$\bullet \text{ } Inj(A, B) = \{f : A \rightarrow B \mid f \text{ é injetora}\}$$

$$\bullet \text{ } Sur(A, B) = \{f : A \rightarrow B \mid f \text{ é sobrejetora}\} \quad (\text{surjective})$$

$$\bullet \text{ } Bij(A, B) = \{f : A \rightarrow B \mid f \text{ é bijetora}\}$$

**Exemplos:**

a)  $A = \{0, 1\}; B = \{a, b\}$

Objetivo: obter pares ordenados do tipo  $(0, *)$  e  $(1, **)$ , onde  $*, ** \in \{a, b\} = B$

Assim, há  $2^2 = 4$  possibilidades para escolher os pares

$$f_1 : \begin{cases} 0 \mapsto a \\ 1 \mapsto a \end{cases} \quad f_1 = \{(0, a), (1, a)\}$$

$$f_2 : \begin{cases} 0 \mapsto b \\ 1 \mapsto b \end{cases} \quad f_2 = \{(0, b), (1, b)\}$$

$$f_3 : \begin{cases} 0 \mapsto a \\ 1 \mapsto b \end{cases} \quad f_3 = \{(0, a), (1, b)\}$$

$$f_4 : \begin{cases} 0 \mapsto b \\ 1 \mapsto a \end{cases} \quad f_4 = \{(0, b), (1, a)\}$$

$$|\mathcal{F}(A, B)| = 4$$

b)  $A = \{0, 1\}; B = \{a, b, c\}$

$$f: A \rightarrow B$$

$$0 \mapsto ? \quad (3 \text{ escolhas para } f(0))$$

$$1 \mapsto ?? \quad (3 \text{ escolhas para } f(1))$$

Há  $3^2 = 9$  possibilidades para escolher  $f(0)$  e  $f(1)$ .

$$f_1: \begin{cases} 0 \mapsto a \\ 1 \mapsto a \end{cases}$$

$$f_2: \begin{cases} 0 \mapsto b \\ 1 \mapsto b \end{cases}$$

$$f_3: \begin{cases} 0 \mapsto c \\ 1 \mapsto c \end{cases}$$

$$f_4: \begin{cases} 0 \mapsto a \\ 1 \mapsto b \end{cases}$$

$$f_5: \begin{cases} 0 \mapsto a \\ 1 \mapsto c \end{cases}$$

$$f_6: \begin{cases} 0 \mapsto b \\ 1 \mapsto a \end{cases}$$

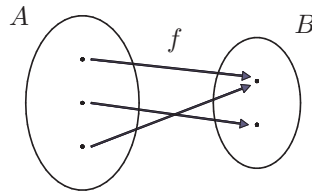
$$f_7: \begin{cases} 0 \mapsto b \\ 1 \mapsto c \end{cases}$$

$$f_8: \begin{cases} 0 \mapsto c \\ 1 \mapsto a \end{cases}$$

$$f_9: \begin{cases} 0 \mapsto c \\ 1 \mapsto b \end{cases}$$

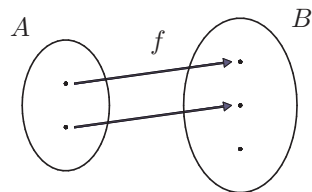
$$|\mathcal{F}(A, B)| = 3^2 = 9$$

c) Se  $|A| = m > n = |B|$ , então  $f: A \rightarrow B$  não é injetora. (Equivalentemente: se  $f$  é injetora, então  $m \leq n$ )



$$(Inj(A, B) = \emptyset)$$

d) Se  $|A| = m < n = |B|$ , então  $f: A \rightarrow B$  não é sobrejetora. (Equivalentemente: se  $f$  é sobrejetora, então  $m \geq n$ )



$$(Sur(A, B) = \emptyset)$$

e) Se  $f$  é bijeção,  $m = n$ .



**Observação.** Se  $f : A \rightarrow B$  é bijeção,  $|A| < \infty$  e  $|B| < \infty$ , podemos, sem perda de generalidade, considerar  $A = B$ .

$$\begin{array}{ccc} A = \{a_1, & \dots, & a_m\} \\ \downarrow & & \downarrow \\ B = \{b_1, & \dots, & b_n\} \end{array} \quad (a_m = a_n \text{ e } b_n = b_m)$$

Assim, uma bijeção  $f : A \rightarrow A$  é dita uma *permutação* de  $A$ .

**Notação.**

$$\text{Bij}(A, A) = S_A = \left\{ \begin{array}{l} f : A \rightarrow A \\ f \text{ é bijeção} \end{array} \right.$$

**Observação.**  $|A| = n \in \mathbb{N} \Rightarrow |S_A| = n!$

$$\begin{array}{l} A = \{a_1, \dots, a_n\} \\ \left\{ \begin{array}{ll} a_1 \mapsto n & \text{escolhas para } f(a_1) \\ a_2 \mapsto n-1 & \text{escolhas para } f(a_2) \\ \vdots & \vdots \\ a_n \mapsto 1 & \text{escolha para } f(a_n) \end{array} \right. \end{array}$$

**Exemplos:**

1)  $A = \{1, 2\}$  ( $|A| = 2$ )

$S_A = S_2 = \{f : A \rightarrow A \mid f \text{ é bijeção}\}$

$|S_A| = 2$

$$f_1 : \left\{ \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array} \right. \quad f_2 : \left\{ \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array} \right.$$

$$\text{ou} \quad f_1 : \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad f_2 : \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

2)  $A = \{1, 2, 3\}$  ( $|A| = 3$ )

$S_A = S_3 = \{f : A \rightarrow A \mid f \text{ é bijeção}\}$

$|S_A| = 3! = 6$

$$f_1 : \left\{ \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{array} \right. \quad \text{ou} \quad f_1 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$f_2 : \left\{ \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{array} \right. \quad \text{ou} \quad f_2 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f_3 : \left\{ \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{array} \right. \quad \text{ou} \quad f_3 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{aligned}
f_4 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} & \quad \text{ou} \quad f_4 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\
f_5 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} & \quad \text{ou} \quad f_5 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\
f_6 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases} & \quad \text{ou} \quad f_6 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\end{aligned}$$

**Notação.**  $A = \{1, 2, \dots, n\}$

$f : A \rightarrow A$  bijeção

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & & f(n) \end{pmatrix}, \text{ onde } f(i) \in A$$

B) Função Inversa

Vimos que  $f : A \rightarrow B$  é inversível (isto é,  $\exists g : B \rightarrow A \mid f \circ g = Id_B$  e  $g \circ f = Id_A$ )  $\Leftrightarrow f$  é bijeção.

Propriedades:

- i) A inversa é única e é denotada por  $f^{-1}$
- ii) A composição de duas bijeções é uma bijeção, isto é, se  $f : A \rightarrow B$  e  $g : B \rightarrow C$  são bijeções, então  $g \circ f : A \rightarrow C$  também o é. Neste caso,  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

De fato:

i) Suponha que  $g : B \rightarrow A$  e  $h : B \rightarrow A$  sejam inversas de  $f$ . Vamos mostrar que  $g = h$ .

$$\begin{cases} g \text{ é inversa de } f \Leftrightarrow g \circ f = Id_A \text{ e } f \circ g = Id_B \\ h \text{ é inversa de } f \Leftrightarrow h \circ f = Id_A \text{ e } f \circ h = Id_B \end{cases}$$

$$g = g \circ Id_B = g \circ (f \circ h) = (g \circ f) \circ h = Id_A \circ h = h$$

Assim,  $f \circ f^{-1} = Id_B$  e  $f^{-1} \circ f = Id_A$ . Além disso,  $(f^{-1})^{-1} = f$ .

ii) Vamos mostrar que a composta de duas funções sobrejetoras também é sobrejetora e a composta de duas funções injetoras também é injetora.

De fato:

$$1^a) \text{ H: } \begin{cases} f : A \rightarrow B & \text{sobrejetora} \\ g : B \rightarrow C & \text{sobrejetora} \end{cases}$$

T:  $\{g \circ f : A \rightarrow C \text{ é sobrejetora}\}$

$$\begin{array}{c}
 A \xrightarrow{f} B \xrightarrow{g} C \\
 \quad \searrow \quad \nearrow \\
 \quad \quad g \circ f \\
 x \longmapsto y \longmapsto z
 \end{array}$$

Queremos mostrar que dado  $z \in C$  (qualquer), existe  $x \in A$  tal que  $(g \circ f)(x) = z$ .

De fato: como  $g$  é sobrejetora, dado  $z \in C$ , existe  $y \in B$  tal que  $g(y) = z$ . Como  $f$  é sobrejetora, para tal  $y \in B$ , existe  $x \in A$  tal que  $f(x) = y$ . Assim,  $z = g(y) = g(f(x)) = (g \circ f)(x)$ .

$$2^{\circ}) \text{ H: } \begin{cases} f : A \rightarrow B & \text{é injetora} \\ g : B \rightarrow C & \text{é injetora} \end{cases}$$

T:  $\{g \circ f : A \rightarrow C \text{ é injetora}\}$

Queremos mostrar que  $\forall x, x' \in A, x \neq x' \Rightarrow (g \circ f)(x) \neq (g \circ f)(x')$ . Pela contrapositiva, isto é o mesmo que provar que  $(g \circ f)(x) = (g \circ f)(x') \Rightarrow x = x'$ .

$$(g \circ f)(x) = (g \circ f)(x') \Rightarrow g(f(x)) = g(f(x')) \xrightarrow{g \text{ é inj.}} f(x) = f(x') \xrightarrow{f \text{ é inj.}} x = x'$$

	Relação	Função
Domínio	está contido no conjunto de partida, primeiros elementos dos pares ordenados $(D(R) \subseteq A)$	igual ao conjunto de partida  $(D(f) = A)$

## 2ª lista

$$10) E \neq \emptyset; A = P(E) = \{X \mid X \subseteq E\}; \emptyset, X, Y \in A$$

$$X \sim Y \Leftrightarrow \text{existe } f : X \rightarrow Y \text{ bijeção}$$

Tese:  $\sim$  define uma relação de equivalência sobre  $A$ . (Neste caso, dizemos que  $X$  e  $Y$  são equipotentes, isto é,  $|X| = |Y|$ ).

**Demonstração.** Devemos verificar que  $\sim$  satisfaz as três propriedades de uma relação de equivalência:

(RE1) (reflexiva)  $X \sim X$

Devemos exibir uma bijeção  $f : X \rightarrow X$ . Tal bijeção (mais simples) é a Função Identidade:

$$\begin{aligned} Id_X : X &\rightarrow X \\ x &\mapsto Id_X(x) = x \end{aligned}$$

$Id_X$  é bijeção:

a)  $Id_X$  é injetora

$$(x, x' \in X) x \neq x' \Rightarrow Id_X(x) \neq Id_X(x')$$

b)  $Id_X$  é sobrejetora

$$CD(Id_X) = X = Im(Id_X)$$

(RE2) (simétrica)  $X \sim Y \stackrel{?}{\Rightarrow} Y \sim X$

$$\begin{aligned} X \sim Y &\Rightarrow \exists f : X \sim Y \text{ (bijeção)} (\Rightarrow \exists f^{-1}) \\ &\Rightarrow \exists f^{-1} : Y \rightarrow X \text{ inversa, a qual é uma bijeção} \\ &\Rightarrow Y \sim X \end{aligned}$$

$$f \circ f^{-1} = Id_Y \text{ e } f^{-1} \circ f = Id_X$$

(RE3) (transitiva)  $X \sim Y$  e  $Y \sim Z \stackrel{?}{\Rightarrow} X \sim Z$

$$\begin{aligned} X \sim Y &\Rightarrow \exists f : X \sim Y \text{ bijeção} \\ Y \sim Z &\Rightarrow \exists g : Y \sim Z \text{ bijeção} \\ &\Rightarrow \exists h : g \circ f : X \rightarrow Z \text{ bijeção} \Rightarrow X \sim Z \end{aligned}$$

(pois a composição de bijeções é uma bijeção) ■

11) (Aplicação do 10)  $|X| = |Y|$

a)  $X = \mathbb{N}; Y = \{y \in \mathbb{N} \mid y \text{ é par}\}$

$$Y \subseteq X$$

Para mostrar que  $|X| = |Y|$ , devemos exibir uma bijeção  $f : X \rightarrow Y$ .

Tese:

$$\begin{aligned} f : X &\rightarrow Y \\ n &\mapsto f(n) = 2n \end{aligned}$$

é bijeção.

De fato:

i)  $f$  é injetora

$$n, n' \in X$$

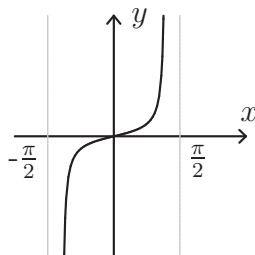
$$n \neq n' \Rightarrow f(n) \neq f(n')$$

$$n \neq n' \Rightarrow 2n \neq 2n'$$

ii)  $f$  é sobrejetora

$$CD(f) = Y = Im(f) = \{2n \mid n \in X\}$$

e)  $X = (-\pi/2, \pi/2); Y = \mathbb{R}$



$$\begin{aligned} f: X &\rightarrow Y \\ x &\mapsto y = \operatorname{tg} x \end{aligned}$$

$$\begin{aligned} f^{-1}: Y &\rightarrow X \\ x &\mapsto f^{-1}(x) = \operatorname{arc} \operatorname{tg} x \end{aligned}$$

8) Propriedades de divisibilidade

$$\text{iii) H: } \begin{cases} a \mid b \Rightarrow \exists m \in \mathbb{Z} \mid a \cdot m = b & (*) \\ c \mid d \Rightarrow \exists n \in \mathbb{Z} \mid c \cdot n = d & (**) \end{cases}$$

$$\text{T: } \{ac \mid bd\}$$

Queremos mostrar que  $\exists l \in \mathbb{Z} \mid (ac)l = bd$ . Multiplicando (\*) e (\*\*) termo a termo, temos  $(am)(cn) = bd$ . Assim, tome  $l = mn$ :

$$(ac)(mn) = (ac)l = bd$$

v)  $a \mid b$  e  $b \mid a \Leftrightarrow |a| = |b|$ ; (Se  $a, b \in \mathbb{N}$ , então  $a \mid b$  e  $b \mid a \Leftrightarrow a = b$ )

$$(\Rightarrow) \begin{cases} \text{H: } a \mid b \text{ e } b \mid a \\ \text{T: } |a| = |b| \text{ (ou } a = b \text{ ou } -b) \end{cases}$$

1º caso:  $a = 0$

$$0 \mid b \text{ e } b \mid 0 \Rightarrow b = 0$$

2º caso:  $a \neq 0$

$$a \mid b \Rightarrow \exists m \in \mathbb{Z} \mid a m = b \quad (1)$$

$$b \mid a \Rightarrow \exists n \in \mathbb{Z} \mid b n = a \quad (2)$$

$$(1) \rightarrow (2) : (a m) n = a \xrightarrow{a \neq 0} m n = 1$$

Se  $m = n = 1$ ,  $a = b$ . se  $m = n = -1$ ,  $a = -b$ .

( $\Leftarrow$ ) Idem

## 4 Estruturas Algébricas

Objetivo: estudar as principais estruturas algébricas e algumas aplicações à Geometria, Computação e Física.

**Definição 4.1 (Operação Binária ou Lei de Composição Interna).**

Seja  $A \neq \emptyset$ . Uma operação binária (ou lei de composição interna) sobre  $A$  é qualquer função de  $A \times A$  em  $A$ .

**Notação.**

$$* : A \times A \rightarrow A$$

$$(a, a') \mapsto a * a'$$

lê-se:  $a * a' =$  “ $a$  operado com  $a'$ ”

**Observações.** i) Como  $*$  é uma função, então  $\forall (a, a') \in A \times A$ ,  $\exists! a * a'$ .

Neste caso, dizemos que  $*$  está bem definida.

ii) Além disso, queremos que  $a * a' \in A$ ,  $\forall (a, a') \in A \times A$ . Neste caso, dizemos que  $A$  é fechado com relação à operação  $*$ .

**Exemplos:**

i)  $A = \mathbb{N}$  (ou  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ )

$* = +$  (adição)

$$\oplus : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(a, b) \mapsto \underbrace{a + b}_{\text{SOMA de } a \text{ e } b}$$

ii)  $A = \mathbb{N}$  (ou  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ )

$* = \cdot$  (multiplicação)

$$\odot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(a, b) \mapsto \underbrace{a \cdot b}_{\text{produto de } a \text{ por } b}$$

**Definição 4.2 (Estrutura Algébrica).** *Seja  $A \neq \emptyset$ . Dizemos que  $A$  é uma estrutura algébrica se  $A$  possui uma ou mais operações binárias bem definidas, satisfazendo determinadas propriedades.*

### Principais Estruturas Algébricas

- com uma operação:  $\left\{ \begin{array}{l} \text{semigrupos} \\ \text{monóides} \\ \text{grupos} \end{array} \right.$
- com duas operações:  $\left\{ \begin{array}{l} \text{anéis} \\ \text{domínios de integridade} \\ \text{corpos} \\ \text{espaços vetoriais} \\ \text{módulos} \end{array} \right.$
- com três operações:  $\{ \text{Álgebras} \}$

### Exemplos:

- 1)  $E \neq \emptyset$   
 $A = P(E) = \{X \mid X \subseteq E\}$   
 $*$  =  $\cup$  (união),  $\cap$  (intersecção)  
 $\cup: A \times A \rightarrow A$   
 $(X, Y) \mapsto X \cup Y$   
 $\cap: A \times A \rightarrow A$   
 $(X, Y) \mapsto X \cap Y$
- 2)  $A = \{ \text{proposições} \}$   
 $*$  =  $\wedge$  (conjunção),  $\vee$  (disjunção)  
 $\wedge: A \times A \rightarrow A$   
 $(p, q) \mapsto p \wedge q$   
 $\vee: A \times A \rightarrow A$   
 $(p, q) \mapsto p \vee q$
- 3)  $A = \mathcal{M}_{m \times n}(\mathbb{R}) = \{B = (a_{ij})_{m \times n} \mid a_{ij} \in \mathbb{R}\}$   
 $*$  =  $+$  (adição)  
 $+: \mathcal{M}_{m \times n}(\mathbb{R}) \times \mathcal{M}_{m \times n}(\mathbb{R}) \rightarrow \mathcal{M}_{m \times n}(\mathbb{R})$   
 $(B, C) \mapsto B + C$

onde  $B + C = (b_{ij} + c_{ij})$

caso particular:  $+: \mathcal{M}_{3 \times 2}(\mathbb{R}) \times \mathcal{M}_{3 \times 2}(\mathbb{R}) \rightarrow \mathcal{M}_{3 \times 2}(\mathbb{R})$

$$\left( \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}, \begin{pmatrix} -1 & 3 \\ 7 & -2 \\ 0 & 1 \end{pmatrix} \right) \mapsto \begin{pmatrix} 0 & 5 \\ 10 & 2 \\ 5 & 7 \end{pmatrix}$$

4)  $A = \mathcal{M}_{m \times n}(\mathbb{R}) = \{ \text{matrizes quadradas } n \times n \text{ com entradas reais} \}$

$$\begin{array}{lcl} * = \cdot & & \\ \cdot : \mathcal{M}_{n \times n}(\mathbb{R}) \times \mathcal{M}_{m \times n}(\mathbb{R}) & \rightarrow & \mathcal{M}_{m \times n}(\mathbb{R}) \\ B, C & \mapsto & BC \end{array}$$

onde  $BC = (d_{ij})$ ,  $d_{ij} = \sum_{k=1}^n b_{ik}c_{kj}$

caso particular:  $\cdot : \mathcal{M}_{2 \times 2}(\mathbb{R}) \times \mathcal{M}_{2 \times 2}(\mathbb{R}) \rightarrow \mathcal{M}_{2 \times 2}(\mathbb{R})$

$$\left( \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 3 \end{pmatrix} \right) \mapsto \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 1 & 12 \end{pmatrix}_{2 \times 2}$$

5)  $A = \mathbb{N}$

$*$  = potenciação

$$\begin{array}{lcl} * : \mathbb{N} \times \mathbb{N} & \rightarrow & \mathbb{N} \\ (a, b) & \mapsto & a * b = a^b (= \underbrace{a \cdot a \cdot \dots \cdot a}_{b \text{ fatores}}) \end{array}$$

6)  $A = \mathbb{Z}$  (ou  $\mathbb{Q}$  ou  $\mathbb{R}$ )

$*$  = potenciação

**Afirmção.**  $*$  NÃO é operação binária sobre  $A$

De fato:

- $(2, -1) \in \mathbb{Z} \times \mathbb{Z}$ , mas  $2^{-1} \notin \mathbb{Z}$  (isto é,  $\mathbb{Z}$  NÃO é fechado para a potenciação)
- $(2, 1/2) \in \mathbb{Q} \times \mathbb{Q}$ , mas  $2^{1/2} \notin \mathbb{Q}$  (isto é,  $\mathbb{Q}$  NÃO é fechado para a potenciação)
- $(-1, 1/2) \in \mathbb{R} \times \mathbb{R}$ , mas  $(-1)^{1/2} \notin \mathbb{R}$  (isto é,  $\mathbb{R}$  NÃO é fechado para a potenciação)

**Exercícios:** Verifique o fechamento (ou não) das seguintes operações em  $B$ .



- i)  $A = \mathbb{R}$ ,  $*$  = +  
 $B = \mathbb{R} - \mathbb{Q} \subseteq A$
- ii)  $A = \mathbb{R}$ ,  $*$  =  $\cdot$   
 $B = \mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\} \subseteq A$
- iii)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$ ,  $*$  =  $\cdot$   
 $B = \left\{ \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} ; \alpha \in \mathbb{R} \right\} \subseteq A$   
(matriz de rotação de  $\alpha$  rad no sentido anti-horário)
- iv)  $A = \mathbb{R}$ ,  $*$  = -  
 $B = \mathbb{N}$
- v)  $A = \mathbb{Z}$ ,  $*$  = +  
 $B_1 = \{x \in \mathbb{Z} \mid x \text{ é par}\} = \{x = 2k \mid k \in \mathbb{Z}\} \subseteq A$   
 $B_2 = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\} = \{x = 2k + 1 \mid k \in \mathbb{Z}\} \subseteq A$

### Resolução:

- i)  $A = \mathbb{R}$ ,  $*$  = +  
 $B = \mathbb{R} - \mathbb{Q} = \{\text{números irracionais}\} \subseteq A$

**Afirmção.**  $B$  NÃO é fechado com relação a operação de adição (isto é,  $*$  = + não é uma operação binária sobre  $B$ )

Contra-exemplo:

$x = \pi \in B$  e  $y = -\pi \in B$ , mas  $x + y = \pi + (-\pi) = 0 \notin B$   
(isto é,  $0 \in \mathbb{Q}$ )

- ii)  $A = \mathbb{R}$ ,  $*$  =  $\cdot$   
 $B = \mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}$  é FECHADO com relação à operação  $*$  =  $\cdot$ , pois  $\forall x, y > 0$ ,  $x \cdot y > 0$  ( $\forall x, y \in B$ ,  $x \cdot y \in B$ )
- iii)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$ ,  $*$  =  $\cdot$   
 $B = \left\{ \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$  é FECHADO com relação a operação  $*$  =  $\cdot$ , pois
- $$X = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \in B \quad \text{e} \quad Y = \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \in B$$

$$\begin{aligned}
\Rightarrow X \cdot Y &= \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \\
&= \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -\cos \alpha \sin \beta - \sin \alpha \cos \beta \\ \sin \alpha \cos \beta + \sin \beta \cos \alpha & -\sin \alpha \sin \beta + \cos \alpha \cos \beta \end{pmatrix} \\
&= \begin{pmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix} \in B
\end{aligned}$$

iv)  $A = \mathbb{R}$ ,  $*$  = -  
 $B = \mathbb{N} \subseteq A$  NÃO é fechado para  $*$  = -, pois  $x = 1 \in B$  e  $y = 2 \in B$ ,  
mas  $x - y = 1 - 2 = -1 \notin B$  ( $-1 \in \mathbb{Z}$ )

v)  $A = \mathbb{Z}$ ,  $*$  = +  
 $B_1 = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$  e  $B_2 = \{x \in \mathbb{Z} \mid x = 2k + 1, k \in \mathbb{Z}\}$   
 $B_1$  é FECHADO para  $*$  = +, pois:

$$\begin{cases} x_1 = 2k_1 \in B_1 \\ x_2 = 2k_2 \in B_1 \end{cases} \Rightarrow x_1 + x_2 = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k_3 \in B_1$$

$B_2$  NÃO é fechado para  $*$  = +, pois:

$$\begin{cases} x_1 = 2k_1 + 1 \in B_2 \\ x_2 = 2k_2 + 1 \in B_2 \end{cases}, \text{ mas } \begin{aligned} x_1 + x_2 &= (2k_1 + 1) + (2k_2 + 1) \\ &= 2(k_1 + k_2 + 1) = 2k_3 \notin B_2 \end{aligned}$$

### Propriedades de Uma Operação Binária

Seja  $A = \emptyset$  munido de uma operação binária  $*$ .

A) (Associatividade)

Dizemos que  $*$  é associativa se  $\forall x, y, z \in A$ ,

$$(x * y) * z = x * (y * z)$$

Neste caso, o uso de parênteses é facultativo

B) (Comutatividade)

Dizemos que  $*$  é comutativa se  $\forall x, y \in A$ ,

$$x * y = y * x$$

C) (Existência de Um Elemento Neutro)

Seja  $e \in A$ . Dizemos que

i)  $e$  é um elemento neutro à esquerda com relação à operação  $*$  se

$$e * x = x, \forall x \in A$$

ii)  $e$  é um elemento neutro à direita com relação à operação  $*$  se

$$x * e = x, \forall x \in A$$

iii)  $e$  é um elemento neutro (bilateral) com relação à operação  $*$  se ele é simultaneamente neutro à esquerda e à direita, ou seja,

$$e * x = x = x * e, \forall x \in A$$

### Exemplos:

i)  $A = \mathbb{N}$  (ou  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ )

$*$   $= +$  é associativa e comutativa

$$\begin{cases} (x + y) + z = x + (y + z) \\ x + y = y + x \end{cases} ; (\forall x, y, z \in A)$$

Se  $A = \mathbb{N}$ , então  $\nexists$  elemento neutro para  $*$   $= +$ . Se  $A = \mathbb{Z}$  (ou  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ) então  $e = 0$  é o elemento neutro para  $*$   $= +$ .

$$0 + x = x = x + 0, \forall x \in A$$

ii)  $A = \mathbb{N}$  (ou  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ )

$*$   $= \cdot$  é associativa e comutativa

$$\begin{cases} (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ x \cdot y = y \cdot x \end{cases} ; (\forall x, y, z \in A)$$

$e = 1$  é o elemento neutro para  $*$   $= \cdot$

$$1 \cdot x = x = x \cdot 1, \forall x \in A$$

iii)  $A = \{ \text{proposições} \}$

$*$   $= \vee$  (disjunção) é associativa e comutativa

$$\begin{cases} (p \vee q) \vee r = p \vee (q \vee r) \\ p \vee q = q \vee p \end{cases} ; (\forall p, q, r \in A)$$

$e = f$  (contradição) é o elemento neutro para  $*$   $= \vee$

$$p \vee f = p, \forall p \in A$$

$*' = \wedge$  (conjunção) é associativa e comutativa

$$\begin{cases} (p \wedge q) \wedge r = p \wedge (q \wedge r) \\ p \wedge q = q \wedge p \end{cases} ; (\forall p, q, r \in A)$$

$e = v$  (tautologia) é o elemento neutro para  $*' = \wedge$

$$p \wedge v = v \wedge p = p, \forall p \in A$$

iv)  $A = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é função}\}$

$* = +$

$$\begin{aligned} & \overbrace{f+g}^{\text{soma}} : \mathbb{R} \rightarrow \mathbb{R} \\ & x \mapsto (f+g)(x) = f(x) + g(x) \end{aligned}$$

$* = +$  é associativa, comutativa e possui  $e = 0$  (função constante identicamente nula) como elemento neutro

$$\begin{cases} (f+g)+h = f+(g+h) \\ f+g = g+f \end{cases}, \forall f, g, h \in A$$

$e \equiv 0$  (isto é,  $e(x) = 0, \forall x \in \mathbb{R}$ )

$$\begin{aligned} (g+0)(x) &= g(x) + 0(x) = g(x) + 0 = g(x) \quad \text{e} \\ (0+g)(x) &= 0(x) + g(x) = 0 + g(x) = g(x) \end{aligned}$$

$$\begin{aligned} & \overbrace{f \cdot g}^{\text{produto}} : \mathbb{R} \rightarrow \mathbb{R} \\ & x \mapsto (f \cdot g)(x) = f(x)g(x) \end{aligned}$$

$*' = \cdot$  é associativa, comutativa e possui  $e = 1$  (função constante 1) como elemento neutro

$$\begin{cases} (f \cdot g) \cdot h = f \cdot (g \cdot h) \\ f \cdot g = g \cdot f \end{cases}, \forall f, g, h \in A$$

$e \equiv 1$  (isto é,  $e(x) = 1, \forall x \in \mathbb{R}$ )

$$\begin{cases} (f \cdot e)(x) = f(x)e(x) = f(x) \cdot 1 = f(x) \\ (e \cdot f)(x) = e(x)f(x) = 1 \cdot f(x) = f(x) \end{cases}$$

### Exercícios:

1) Considere  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$ . Verifique que

- i)  $*$  =  $+$  é associativa, comutativa e possui

$$e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}_{2 \times 2}$$

(matriz identicamente nula) como elemento neutro para  $*$  =  $+$ .

- ii)  $*$  =  $\cdot$  é associativa, NÃO-comutativa e possui

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2 \times 2} = I_2$$

(matriz identidade de ordem 2) como elemento neutro para  $*$  =  $\cdot$ .

- 2) Julgue os itens a seguir ( $V$  ou  $F$ ), justificando.

- a) ( $V$ ) A subtração em  $\mathbb{Z}$  possui  $e = 0$  como elemento neutro à direita, mas não possui elemento neutro à esquerda.
- b) ( $V$ ) A potenciação em  $\mathbb{N}$  possui  $e = 1$  como elemento neutro à direita, mas não possui elemento neutro à esquerda.
- c) ( $F$ ) A subtração em  $\mathbb{Z}$  é associativa.
- d) ( $F$ ) A subtração em  $\mathbb{Z}$  é comutativa.
- e) ( $F$ ) A potenciação em  $\mathbb{N}$  é associativa.
- f) ( $F$ ) A potenciação em  $\mathbb{N}$  é comutativa.
- g) ( $V$ ) Sejam  $E \neq \emptyset$  e  $A = P(E)$ . Então,  $*$  =  $\cup$  é associativa, comutativa e possui  $e = \emptyset$  como elemento neutro para  $*$  =  $\cup$ .
- h) ( $V$ ) Sejam  $E \neq \emptyset$  e  $A = P(E)$ . Então,  $*$  =  $\cap$  é associativa, comutativa e possui  $e = E$  como elemento neutro para  $*$  =  $\cap$ .

- 3) Seja  $A \neq \emptyset$  munido de uma operação binária  $*$ . Mostre que se  $e \in A$  é um elemento neutro (bilateral), então ele é único.

- 4) Considere  $A = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é função}\}$

- a) Verifique que  $*$  =  $\circ$  (composição) é associativa
- b) Verifique que  $*$  =  $\circ$  NÃO é comutativa
- c) Qual é o elemento neutro  $e$  para tal operação  $*$  =  $\circ$ ?

1)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$

$$\begin{aligned}
\text{i)} \quad & \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left[ \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} \\
& = \begin{pmatrix} a+e+i & b+f+j \\ c+g+k & d+h+l \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
& = \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
& \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix} \\
& = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
& \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ c+0 & d+0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
& = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
\text{ii)} \quad & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[ \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix} \\
& = \begin{pmatrix} aei+afk+bgi+bhk & aej+af+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+dgj+dhl \end{pmatrix} \\
& = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
& \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \\
& \quad \neq \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea+fc & eb+fd \\ ga+hc & gb+hd \end{pmatrix} \\
& \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}
\end{aligned}$$

2) a)  $(V) \ z - 0 = z \neq -z = 0 - z, \forall z \in \mathbb{Z}^*$

b)  $(V)$  para  $n \in \mathbb{N}$ , temos  $n^1 = n$ , mas se  $a(\in \mathbb{N}) \neq 1$ , então  $a^n \neq n$

c)  $(F)$  contra-exemplo:  $(7 - 4) - 3 = 0 \neq 6 = 7 - (4 - 3)$

- d) ( $F$ ) contra-exemplo:  $2 - 1 = 1 \neq -1 = 1 - 2$
- e) ( $F$ ) Seja  $a, b, c \in \mathbb{N}$ , temos  $a^{(b^c)} \neq (a^b)^c = a^{bc}$ .  
 Contra-exemplo:  $2^{(3^4)} = 2^{81} \neq 2^{12} = (2^3)^4$
- f) ( $F$ ) para  $a, b \in \mathbb{N}$ , temos  $a^b \neq b^a$ .  
 Contra-exemplo:  $2^3 = 8 \neq 9 = 3^2$
- g) ( $V$ ) Para  $X, Y, Z \in A$ , temos
- $$\begin{cases} X \cup (Y \cup Z) = (X \cup Y) \cup Z \\ X \cup Y = Y \cup X \\ X \cup \emptyset = \emptyset \cup X = X \end{cases}$$
- h) ( $V$ ) Para  $X, Y, Z \in A$ , temos
- $$\begin{cases} X \cap (Y \cap Z) = (X \cap Y) \cap Z \\ X \cap Y = Y \cap X \\ X \cap E = E \cap X = X, \text{ pois } X \subseteq E \end{cases}$$

**Observação.** Se  $*$  é comutativa, então as noções de elemento neutro à esquerda, à direita e bilateral são equivalentes.

### 3) (Unicidade do Elemento Neutro)

$A \neq \emptyset$  munido de uma operação binária  $*$ .  $e (\in A)$  = elemento neutro bilateral (caso exista).

Tese:  $e$  é único

#### **Demonstração.**

H:  $e$  é neutro

T:  $e$  é único

Suponha que  $e$  e  $e'$  são dois elementos neutros. Vamos mostrar que  $e = e'$ .

(I)  $e (\in A)$  = elemento neutro  $\Leftrightarrow e * x = x * e = x, \forall x \in A$

(II)  $e' (\in A)$  = elemento neutro  $\Leftrightarrow e' * y = y * e' = y, \forall y \in A$

Em particular, tome  $x = e'$  em (I):

$$e * e' = e' * e = e'$$

Em particular, tome  $y = e$  em (II):

$$e' * e = e * e' = e$$

Logo,  $e' = e * e' = e$

■

4) (Importante)

$$A = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é função}\}$$

$*$  =  $\circ$  (composição)

$$\begin{aligned} \circ : \mathcal{F}(\mathbb{R}, \mathbb{R}) \times \mathcal{F}(\mathbb{R}, \mathbb{R}) &\rightarrow \mathcal{F}(\mathbb{R}, \mathbb{R}) \\ (g, f) &\mapsto g \circ f \end{aligned}$$

$$\mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R} \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } g \circ f$$

$$\mathbb{R} \xrightarrow{g} \mathbb{R} \xrightarrow{f} \mathbb{R} \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } f \circ g$$

a) Tese:  $*$  =  $\circ$  é associativa, isto é,  $\forall f, g, h \in A$ ,  $(h \circ g) \circ f = h \circ (g \circ f)$

**Demonstração.** Vamos mostrar que as funções  $h \circ g) \circ f$  e  $h \circ (g \circ f)$  são IGUAIS, ou seja:

i)  $D((h \circ g) \circ f) = D(h \circ (g \circ f))$

ii)  $CD((h \circ g) \circ f) = CD(h \circ (g \circ f))$

iii)  $\forall x \in \mathbb{R}$ ,  $[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x)$

$$\begin{array}{c} \mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R} \xrightarrow{h} \mathbb{R} \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } h \circ g \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } (h \circ g) \circ f \end{array}$$

$$\begin{array}{c} \mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R} \xrightarrow{h} \mathbb{R} \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } g \circ f \\ \text{curved arrow from } \mathbb{R} \text{ to } \mathbb{R} \text{ labeled } h \circ (g \circ f) \end{array}$$

Verificando iii)

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x)))$$

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x)))$$

■

b) Tese:  $*$  =  $\circ$  NÃO é comutativa

**Exemplo:**  $f(x) = \sin x$ ,  $g(x) = x^2$

$$(g \circ f)(x) = g(f(x)) = g(\sin x) = (\sin x)^2 = \sin^2 x$$

$$(f \circ g)(x) = f(g(x)) = f(x^2) = \sin x^2$$

c)  $e$  = Função Identidade

$$\begin{aligned} I_{\mathbb{R}} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto I_{\mathbb{R}}(x) = x \end{aligned}$$

$$f \circ I_{\mathbb{R}} = f \text{ e } I_{\mathbb{R}} \circ f = f$$

D) (Existência de Elemento Inversível)

Seja  $A \neq \emptyset$  com uma operação binária  $*$  e elemento neutro  $e$ . Dizemos que



i)  $x \in A$  é inversível à esquerda se existe  $x' \in A$  tal que

$$x' * x = e \quad (x' = \text{inverso à esquerda de } x)$$

ii)  $x \in A$  é inversível à direita se existe  $x' \in A$  tal que

$$x * x' = e \quad (x' = \text{inverso à direita de } x)$$

iii)  $x \in A$  é inversível se ele é simultaneamente inversível à esquerda e à direita, ou seja, se existe  $x' \in A$  tal que

$$x' * x = e = x * x' \quad (x' = \text{inverso de } x)$$

**Observações.** a) Se  $* = +$ , denotamos  $x'$  por  $-x$  (oposto, simétrico ou inverso aditivo)

b) Se  $* = \cdot$ , denotamos  $x'$  por  $x^{-1}$  (inverso multiplicativo de  $x$ )

c)  $\mathcal{U}_*(A) = \{x \in A \mid x \text{ é inversível com relação à operação } *\}$   
 $\mathcal{U}_*(A) \neq \emptyset$ , pois  $e \in \mathcal{U}_*(A)$ . De fato,  $e * e = e$ .

**Exemplos:**

i)  $A = \mathbb{N}$ ,  $* = +$  ( $0 \neq \mathbb{N}$ )  
 $\mathcal{U}_+(\mathbb{N}) = \emptyset$

ii)  $A = \mathbb{Z}_+ = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N} \cup \{0\}$ ,  $* = +$   
 $e = 0$   

$$\begin{cases} x \in A & (\text{dado}) \\ x' \in A & (\text{a obter}) \\ x + x' = 0 \end{cases}$$
  
 $\mathcal{U}_+(\mathbb{Z}_+) = \{0\}$  (pois  $0 + 0 = 0$ )

iii)  $A = \mathbb{Z}$ ,  $* = +$ ,  $e = 0$   
Sabemos que dado  $x \in \mathbb{Z}$ , existe  $-x \in \mathbb{Z}$  tal que  $x + (-x) = 0$   
 $\mathcal{U}_+(\mathbb{Z}) = \mathbb{Z}$

iv)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$   
 $* = \cdot$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \quad (\text{matriz identidade de ordem } 2)$$

$$X = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \quad (\text{NÃO é inversível com relação a operação } * = \cdot)$$

$$X' \cdot X = I_2$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} a + 3b = 1 \\ 2a + 6b = 0 \\ c + 3d = 0 \\ 2c + 6d = 1 \end{cases} \Rightarrow \begin{cases} a + 3b = 1 \\ 2a + 6b = 0 \end{cases} \text{ e } \begin{cases} c + 3d = 0 \\ 2c + 6d = 1 \end{cases}$$

$$\Rightarrow \begin{cases} a + 3b = 1 \\ a + 3b = 0 \end{cases} \text{ e } \begin{cases} c + 3d = 0 \\ c + 3d = 1/2 \end{cases}$$

Conclusão:  $\nexists X' = X^{-1}$

$$\mathcal{U}(\mathcal{M}_{2 \times 2}(\mathbb{R})) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$$

No exemplo anterior,  $\det X = 6 - 6 = 0$

v)  $A = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é função}\}, * = \circ, e = I_{\mathbb{R}}$

**Exemplo:**  $f(x) = x^3$  é inversível com relação à operação  $* = \circ$ :

$$\begin{aligned} y = f(x) &\Leftrightarrow x = f^{-1}(y) \\ y = x^3 &\Rightarrow x = \sqrt[3]{y} \text{ ou } y = \sqrt[3]{x} \end{aligned}$$

$g(x) = \sqrt[3]{x} = f^{-1}(x)$ , pois:

$$\begin{cases} g \circ f \stackrel{?}{=} I_{\mathbb{R}} \\ \text{e} \\ f \circ g = I_{\mathbb{R}} \end{cases}$$

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x \\ (f \circ g)(x) &= f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x \end{aligned}$$

$$\mathcal{U}_{\circ}(\mathcal{F}(\mathbb{R}, \mathbb{R})) = \text{Bij}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é bijeção}\}$$

vi)  $A = \mathbb{Q} \text{ (ou } \mathbb{R} \text{ ou } \mathbb{C}), * = \cdot, e = 1$

$$\begin{cases} x \in A & \text{(dado)} \\ x' \in A & \text{(a obter)} \\ x' \cdot x = 1 \end{cases}$$

$$\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} - \{0\}$$

**Exemplo:**  $x = a/b \in \mathbb{Q}^*$  ( $a, b \in \mathbb{Z}$ ,  $b \neq 0$  e  $a \neq 0$ )  
 $x^{-1} = b/a$  é o inverso de  $x$

vii)  $A = \mathbb{Z}$ ,  $*$  =  $\cdot$ ,  $e = 1$   
 $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$

**Observação.**  $x = 2$  é inversível em  $\mathbb{Q}$ , mas não o é em  $\mathbb{Z}$   
 $2x = 1$  NÃO tem solução em  $\mathbb{Z}$   
 $2x = 1$  TEM solução em  $\mathbb{Q}$  :  $x = 1/2$

E) (Lei do Cancelamento)  
 Seja  $A \neq \emptyset$  munido de uma operação binária  $*$ .

i)  $a \in A$  é regular à esquerda se

$$a * x = a * y \Rightarrow x = y, \forall x, y \in A \quad (\text{cancelamento à esquerda})$$

ii)  $a \in A$  é regular à direita se

$$x * a = y * a \Rightarrow x = y, \forall x, y \in A \quad (\text{cancelamento à direita})$$

iii)  $a \in A$  é regular se

$$\begin{cases} a * x = a * y \Rightarrow x = y \\ \text{e} \\ x * a = y * a \Rightarrow x = y \end{cases}, \forall x, y \in A$$

**Observações.** a) Se  $*$  é comutativa, tais noções de regular á esquerda e à direita são iguais;

b)  $\mathcal{R}_*(A) = \{x \in A \mid x \text{ é regular com relação a } *\}$

Observe que se  $e \in A$  é o elemento neutro, então  $e$  é regular:

$$\begin{cases} e * x = e * y \Rightarrow x = y \\ \text{e} \\ x * e = y * e \Rightarrow x = y \end{cases}, \forall x, y \in A$$

**Exemplos:** i)  $A = \mathbb{Z}$ ,  $*$  = +

$$\mathcal{R}_+(\mathbb{Z}) = \mathbb{Z}$$

Neste caso,  $\forall a \in \mathbb{Z}$ , vale

$$\begin{cases} a + x = a + y \Rightarrow x = y \\ \text{e} \\ x + a = y + a \Rightarrow x = y \end{cases}, \forall x, y \in \mathbb{Z}$$

ii)  $A = \mathbb{Q}$  (ou  $\mathbb{R}$ ,  $\mathbb{C}$ ),  $*$  =  $\cdot$

$$\mathcal{R}_\cdot(\mathbb{Q}) = \mathbb{Q}^*$$

Neste caso, se  $a \in \mathbb{Q}^*$ , então:

$$\begin{cases} a \cdot x = a \cdot y \stackrel{\cdot a}{\Rightarrow} x = y \\ \text{e} \\ x \cdot a = y \cdot a \stackrel{\cdot a}{\Rightarrow} x = y \end{cases}, \forall x, y \in \mathbb{Z}$$

0 não é regular, pois  $0 \cdot 1 = 0 \cdot 2$ , mas  $1 \neq 2$

**Exercícios:** (Teóricos)

1) Seja  $A \neq \emptyset$  munido de uma operação binária  $*$  associativa e com elemento neutro  $e$ . Mostre que se  $x \in A$  é inversível, então  $x'$  (inverso de  $x$ ) é único.

2) (1º exercício da 3ª lista)

Seja  $A \neq \emptyset$  munido de uma operação binária  $*$  associativa e com elemento neutro  $e$ . Considere  $\mathcal{U}_*(A) = \{x \in A \mid x \text{ é inversível}\}$  e  $\mathcal{R}_*(A) = \{x \in A \mid x \text{ é regular}\}$ . Verifique que:

a)  $\mathcal{U}_*(A) \neq \emptyset$ ;  $\mathcal{R}_*(A) \neq \emptyset$

b) Se  $x \in \mathcal{U}_*(A)$ , então  $x' \in \mathcal{U}_*(A)$ . Neste caso,  $(x')' = x$

c) Se  $x, y \in \mathcal{U}_*(A)$ , então  $x * y \in \mathcal{U}_*(A)$ . Neste caso,  $(x * y)' = y' * x'$

**Observação.** (Aplicando 2) b) e c) a dois contextos diferentes)

1ª) (matrizes)

$$A = \mathcal{M}_{n \times n}(\mathbb{R}), * = \cdot$$

$$\mathcal{U}_*(A) = \{ \text{matrizes com determinante} \neq 0 \}$$

b):  $(B^{-1})^{-1} = B$ ; (supondo  $B$  inversível)

c):  $(B \cdot C)^{-1} = C^{-1}B^{-1}$  (supondo que  $B$  e  $C$  são inversíveis)

2ª) (funções)

$$A = \mathcal{F}(\mathbb{R}, \mathbb{R}); * = \circ$$

$$\mathcal{U}_*(A) = \text{Bij}(\mathbb{R}, \mathbb{R})$$

$$\text{b): } (f^{-1})^{-1} = f; \text{ (supondo que } f \text{ seja inversível)}$$

$$\text{c): } (f \circ g)^{-1} = g^{-1} \circ f^{-1} \text{ (supondo que } f \text{ e } g \text{ têm inversa)}$$

**Resolução:**

1)

$$\text{H: } \begin{cases} e \\ * \text{ é associativa} \\ x = \text{ elemento inversível} \\ x' = \text{ inverso de } x \end{cases}$$

$$\text{T: } \{ x' \text{ é único}$$

**Demonstração.** Suponha que  $x'$  e  $x''$  sejam inversos de  $x$ :

$$\begin{cases} x' * x = e = x * x' & (1) \\ x'' * x = e = x * x'' & (2) \end{cases}$$

Vamos mostrar que  $x'' = x'$ . De fato:

$$x'' = x'' * e \stackrel{(1)}{=} x'' * (x * x') \stackrel{\text{assoc.}}{=} (x'' * x) * x' \stackrel{(2)}{=} e * x' = x' \quad \blacksquare$$

2) Tese:

$$\text{a) } \mathcal{U}_*(A) \neq \emptyset : e \in \mathcal{U}_*(A), \text{ pois } e * e = e$$

$$\mathcal{R}_*(A) \neq \emptyset : e \in \mathcal{R}_*(A)$$

$$\text{b) H: } x \in \mathcal{U}_*(A)$$

$$\text{T: } x' \in \mathcal{U}_*(A) \text{ e } (x')' = x$$

$$\textbf{Demonstração.} \quad x \in \mathcal{U}_*(A) \Rightarrow \exists x' \in A \mid x' * x = e = x * x'$$

$$\text{Dessa igualdade, segue que } x' \in \mathcal{U}_*(A) \text{ e } (x')' = x \quad \blacksquare$$

$$\text{c) H: } x, y \in \mathcal{U}_*(A)$$

$$\text{T: } x * y \in \mathcal{U}_*(A) \text{ e } (x * y)' = y' * x'$$

**Demonstração.** Como o inverso é único (quando existe), basta mostrar que:

$$(x * y) * (y' * x') = e \text{ e}$$

$$(y' * x') * (x * y) = e$$

De fato:

$$\begin{aligned}(x * y) * (y' * x') &= [x * (y * y')] * x' = [x * e] * x' = x * x' = e \\ (y' * x') * (x * y) &= [y' * (x' * x)] * y = [y' * e] * y = y' * y = e\end{aligned}\quad \blacksquare$$

### Tábua de Operação

$$A = \{a_1, a_2, \dots, a_n\}$$

$$* : A \times A \rightarrow A$$

$$(a_i, a_j) \mapsto a_i * a_j (= a_{ij})$$

A tábua da operação  $*$  é uma tabela  $n \times n$  cujos elementos são os “operados”  $a_i * a_j$ , onde  $i, j \in \{1, 2, \dots, n\}$

$*$	$a_1$	$a_2$	$a_3$	$\dots$	$a_i$	$\dots$	$a_j$	$\dots$	$a_n$	(linha fundamental)
$a_1$	$a_{11}$									
$a_2$		$a_{22}$								
$\vdots$										
$a_i$					$a_{ii}$		$a_i * a_j$			
$\vdots$										
$a_j$							$a_{jj}$			
$\vdots$										
$a_n$									$a_{nn}$	(diagonal principal)

↖ (coluna fundamental)

### Exemplos:

a)  $A = \{-1, 1\}$

$$* = \cdot$$

$\cdot$	$-1$	$1$
$-1$	$1$	$-1$
$1$	$-1$	$1$

b)  $E = \{a, b\}$

$$A = P(E) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$* = \cap$$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

$$\text{c) } E = \{1, 2\}$$

$$A = \text{Bij}(E, E) = \{f : E \rightarrow E \mid f \text{ é bijeção}\}$$

$$* = \circ$$

$$f_1 : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \end{cases} \quad (\text{Identidade})$$

$$f_2 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \end{cases}$$

$$f_1 \circ f_1 = f_1$$

$$f_1 \circ f_2 = f_2$$

$$f_2 \circ f_1 = f_2$$

$$f_2 \circ f_2 = f_1$$

$$\begin{array}{c|cc} \circ & f_1 & f_2 \\ \hline f_1 & f_1 & f_2 \\ f_2 & f_2 & f_1 \end{array}$$

Em notação matricial:

$$f_1 : \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad f_2 : \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$f_1 \circ f_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = f_2$$

$$f_2 \circ f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = f_1$$

**Observação.** A partir da tábua de operação, é possível verificar se a mesma é comutativa, se possui elemento(s) neutro(s), se possui elemento(s) inversível(is) e se possui elemento(s) regular(es).

I) Comutatividade:

$$a_i * a_j = a_j * a_i, \quad \forall a_i, a_j \in A$$

Neste caso,  $*$  é comutativa se a tábua da operação é simétrica em relação à diagonal principal, ou seja, os elementos em posições simétri-

cas em relação à diagonal principal são iguais.

$*$	$a_i$	$a_j$
$a_{11}$		
$\vdots$	$a_{22}$	
$a_i$	$a_{ii}$	$a_{ij}$
$\vdots$		
$a_j$	$a_{ji}$	$a_{jj}$
		$a_{nn}$

Nos exemplos anteriores,  $*$  é comutativa, pois:

a)	$\begin{array}{c cc} \cdot & -1 & 1 \\ \hline -1 & \textcolor{red}{1} & -1 \\ \hline 1 & -1 & \textcolor{red}{1} \end{array}$	b)	$\begin{array}{c cccc} \cap & \emptyset & \{a\} & \{b\} & \{a,b\} \\ \hline \emptyset & \textcolor{red}{\emptyset} & \textcolor{blue}{\emptyset} & \textcolor{green}{\emptyset} & \textcolor{orange}{\emptyset} \\ \{a\} & \textcolor{blue}{\emptyset} & \textcolor{red}{\{a\}} & \emptyset & \textcolor{green}{\{a\}} \\ \{b\} & \textcolor{green}{\emptyset} & \emptyset & \textcolor{red}{\{b\}} & \textcolor{blue}{\{b\}} \\ \{a,b\} & \textcolor{orange}{\emptyset} & \textcolor{green}{\{a\}} & \textcolor{blue}{\{b\}} & \textcolor{red}{\{a,b\}} \end{array}$
c)	$\begin{array}{c cc} \circ & f_1 & f_2 \\ \hline f_1 & \textcolor{red}{f_1} & f_2 \\ \hline f_2 & f_2 & \textcolor{red}{f_1} \end{array}$		

## II) Elemento Neutro

- $e \in A$  é elemento neutro à esquerda  $\Leftrightarrow e * a_i = a_i, \forall a_i \in A \Leftrightarrow$  na linha de  $e$  aparece uma cópia da linha fundamental;
- $e \in A$  é elemento neutro à direita  $\Leftrightarrow a_i * e = a_i, \forall a_i \in A \Leftrightarrow$  na coluna de  $e$  aparece uma cópia da coluna fundamental;
- $e \in A$  é elemento neutro  $\Leftrightarrow$  a linha e a coluna de  $e$  são cópias, respectivamente, da linha e da coluna fundamental.

Nos exemplos anteriores

- a)  $e = 1$ ;   b)  $e = \{a, b\} = E$ ;   c)  $e = f_1$

## III) Elemento Inverso

$e$  = elemento neutro

- $a_i \in A$  é inversível à esquerda  $\Leftrightarrow \exists a'_i \in A \mid a'_i * a_i = e \Leftrightarrow$  o elemento neutro  $e$  aparece na coluna de  $a_i$ ;



- $a_i \in A$  é inversível à direita  $\Leftrightarrow \exists a'_i \in A \mid a_i * a'_i = e \Leftrightarrow$  o elemento neutro  $e$  aparece na linha de  $a_i$ ;
- $a_i \in A$  é inversível  $\Leftrightarrow$  o elemento neutro  $e$  aparece na linha e na coluna de  $a_i$ .

Nos exemplos anteriores

$$\text{a) } \begin{cases} e = 1 \\ (-1)' = -1 \\ (1)' = 1 \end{cases} \quad \text{b) } \begin{cases} e = \{a, b\} \\ (\{a, b\})' = \{a, b\} \end{cases} \quad \text{c) } \begin{cases} e = f_1 \\ (f_1)' = f_1 \\ (f_2)' = f_2 \end{cases}$$

#### IV) Elementos Regulares

- $a \in A$  é regular à esquerda  $\Leftrightarrow a * x = a * y \Rightarrow x = y, \forall x, y \in A \xLeftrightarrow{\text{C-P}} (x \neq y \Rightarrow a * x \neq a * y, \forall x, y \in A) \Leftrightarrow$  todos os elementos da linha de  $a$  são distintos;
- $a \in A$  é regular à direita  $\Leftrightarrow x * a = y * a \Rightarrow x = y, \forall x, y \in A \xLeftrightarrow{\text{C-P}} (x \neq y \Rightarrow x * a \neq y * a, \forall x, y \in A) \Leftrightarrow$  todos os elementos da coluna de  $a$  são distintos;
- $a \in A$  é regular  $\Leftrightarrow$  todos os elementos da linha de  $a$  são distintos e todos os elementos da coluna de  $a$  são distintos.

**Exercícios:** Nas tábuas de operação abaixo, verifique a comutatividade e a existência de elementos neutros, inversíveis e regulares:

a) 

*	a	b	c
a	a	b	c
b	b	c	a
c	c	b	a

- \* NÃO é comutativa, pois  $c * b \neq b * c$
- elemento neutro :  $a$
- elementos inversíveis:  $a$  (bilateral)

$$(a' = a) \quad a * a = a$$

$$\underbrace{b}_{\text{inv à esq de } c} * \underbrace{c}_{\text{inv à dir de } b} = a$$

- elementos regulares:  $a$  (bilateral)
- $b$  - regular à esquerda, mas não à direita
- $c$  - não é regular à esquerda, mas é regular à direita.

b)

$*$	$a$	$b$	$c$
$a$	$a$	$b$	$c$
$b$	$c$	$a$	$b$
$c$	$b$	$a$	$c$

- $*$  não é comutativa, pois a tábua não é simétrica
- $\nexists$  elemento neutro bilateral.  $a$  = elemento neutro à esquerda
- elementos inversíveis:  $\nexists$
- elementos regulares:  $a$  é regular bilateralmente,  $b$  é regular à esquerda,  $c$  é regular à esquerda.

$*$	$e$	$a_1$	$a_2$	$a_3$	$a_4$
$e$	$e$	$a_1$	$a_2$	$a_3$	$a_4$
$a_1$	$a_1$	$a_2$	$a_3$	$a_4$	$e$
$a_2$	$a_2$	$a_3$	$a_4$	$a_1$	$a_2$
$a_3$	$a_3$	$a_4$	$a_1$	$a_2$	$a_1$
$a_4$	$a_4$	$e$	$a_3$	$a_4$	$a_2$

$*$	$e$	$a$	$b$	$c$	$d$
$e$	$e$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$d$	$e$	$c$
$b$	$b$	$c$	$c$	$b$	$b$
$c$	$c$	$d$	$e$	$a$	$b$
$d$	$d$	$e$	$b$	$d$	$b$

**Definição 4.3 (Semigrupo, Monóide, Grupo).** *Seja,  $A \neq \emptyset$  munido de uma operação binária*

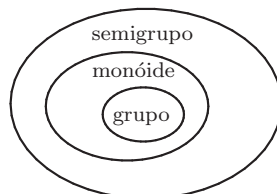
$$* : A \times A \rightarrow A$$

$$(a, a') \mapsto a * a'$$

*Um par  $(A, *)$  é dito uma Estrutura Algébrica com uma operação binária se  $*$  satisfaz determinadas propriedades*

- O par  $(A, *)$  é dito um Semigrupo se  $*$  é associativa;*
- O par  $(A, *)$  é dito um Monóide se  $*$  é associativa e possui elemento neutro (bilateral);*
- O par  $(A, *)$  é dito um Grupo se  $*$  é associativa, possui elemento neutro (bilateral) e todo elemento é inversível, isto é:*

- i)  $\forall a, b, c \in A, a * (b * c) = (a * b) * c;$
- ii)  $\exists e \in A \mid e * a = a = a * e, \forall a \in A;$
- iii)  $\forall a \in A, \exists a' \in A \mid a' * a = e = a * a'$



- Exemplos:** a)  $(\mathbb{N}, +)$  = semigrupo, mas não é monóide (pois  $e = 0 \notin \mathbb{N}$ ) ( $\nexists e$ )  
 b)  $(\mathbb{N}, \cdot)$  = monóide, mas não é um grupo (pois existem elementos não inversíveis) ( $e = 1$ )  
 c)  $(\mathbb{Z}, +)$  = grupo ( $e = 0, (x)' = -x$ )  
 d)  $(\mathbb{Z}, \cdot)$  = monóide, mas não é um grupo (apenas 1 e  $-1$  são inversíveis) ( $e = 1, (1)' = 1, (-1)' = (-1)$ )  
 e)  $(\mathbb{Q}^*, \cdot) = (\mathbb{R}^*, \cdot) = (\mathbb{C}^*, \cdot)$  = grupos ( $e = 1, (x)' = 1/x$ )

**Exercícios:** Verifique se o par  $(A, *)$  é um semigrupo, monóide ou grupo:

- a)  $(\mathbb{N}, \text{potenciação})$  = não é nenhuma das estruturas algébricas citadas
- b)  $(\mathbb{Z}, -)$  = não é nenhuma das estruturas algébricas citadas
- c)  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$  = monóide (mas não é grupo, pois apenas as funções bijetoras são inversíveis)
- d)  $(\mathcal{M}_{m \times n}(\mathbb{R}), +)$  = grupo (é associativa, tem o elemento neutro (matriz nula) e existe inverso)
- e)  $(\mathcal{M}_{n \times n}(\mathbb{R}), \cdot)$  = monóide (mas não é grupo pois nem toda matriz é inversível)
- f)  $(\{v, f\}, \wedge)$  = monóide (mas não é grupo pois  $f$  não é inversível)
- g)  $(P(\{a, b\}), \cup)$  = monóide (não é grupo, pois apenas  $\emptyset$  tem inverso)

**Resolução:**

- a) potenciação não é associativa, pois:  $(2^2)^3 = 2^6 \neq 2^8 = 2^{(2^3)}$
- b) – não é associativa, pois:

$$(2 - 2) - 3 = 0 - 3 = -3 \neq 3 = 2 - (-1) = 2 - (2 - 3)$$

f) é associativa, tem elemento neutro:  $e = v$

$\wedge$	$v$	$f$
$v$	$v$	$f$
$f$	$f$	$f$

g)  $e = \emptyset$

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

**Teorema 4.4.** *Sejam  $(A, *)$  um monóide e  $\mathcal{U}_*(A) = \{x \in A \mid x \text{ é inversível}\}$  ( $\subseteq A$ ). Então,  $(\mathcal{U}_*(A), *)$  é um grupo.*

**Demonstração.** Como  $\mathcal{U}_*(A) \subseteq A$  e  $*$  é associativa em  $A$ , então  $\mathcal{U}_*(A)$  “herda” esta propriedade.

Além disso,  $e$  (elemento neutro de  $A$ ) pertence a  $\mathcal{U}_*(A)$  (pois  $e * e = e$ ).

Por definição,  $\mathcal{U}_*(A)$  é a coleção de todos os elementos inversíveis. Assim,  $\forall a \in \mathcal{U}_*(A), \exists a' \in \mathcal{U}_*(A) \mid a * a' = e$ . ■

Lembre-se: (1ª questão da 3ª lista)

$$\begin{cases} (x')' = x; \\ (x * y)' = y' * x' \end{cases}$$

Voltando aos exemplos anteriores:

a)  $A = \mathcal{M}_{n \times n}(\mathbb{R}), * = \cdot$

$$\mathcal{U}_*(A) = GL(n, \mathbb{R}) = \{A = (a_{ij})_{n \times n} \in \mathcal{M}_{n \times n}(\mathbb{R}) \mid \det A \neq 0\}$$

(Tal grupo é chamado Grupo Linear Geral de grau  $n$  com entradas em  $\mathbb{R}$ )

b)  $A = \mathcal{F}(\mathbb{R}, \mathbb{R}), * = \circ$

$$\mathcal{U}_*(A) = S_{\mathbb{R}} = Bij(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é bijeção}\}$$

(Tal grupo é chamado Grupo Simétrico sobre  $\mathbb{R}$ )

### Estruturas Algébricas Com Duas Operações Binárias

Seja  $A \neq \emptyset$ , munido de duas operações binárias

$$\begin{aligned} \Delta : A \times A \rightarrow A & \quad \square : A \times A \rightarrow A \\ (a, a') \mapsto a \Delta a' & \quad \text{e} \quad (a, a') \mapsto a \square a' \end{aligned}$$

A tripla  $(A, \Delta, \square)$  é uma Estrutura Algébrica Com Duas Operações Binárias se  $\Delta$  e  $\square$  satisfaz certas propriedades.

**Definição 4.5 (Distributividade).**

- a) Dizemos que  $\Delta$  é distributiva à esquerda de  $\square$  se  $\forall x, y, z \in A$ ,  $x \Delta (y \square z) = (x \Delta y) \square (x \Delta z)$ ;
- b) Dizemos que  $\Delta$  é distributiva à direita de  $\square$  se  $\forall x, y, z \in A$ ,  $(y \square z) \Delta x = (y \Delta x) \square (z \Delta x)$ ;
- c) Dizemos que  $\Delta$  é distributiva com relação  $\square$  se  $\Delta$  é simultaneamente distributiva à esquerda e à direita de  $\square$ .

**Observação.** Se  $\Delta$  é comutativa, então as três noções anteriores são equivalentes.

**Exemplos:**

- a) (Apostila 1)

$$\begin{aligned} A &= \{ \text{proposições} \} \\ \Delta &= \wedge \text{ ("e")}, \square = \vee \text{ ("ou")} \quad (\text{comutativas}) \\ \forall p, q, r \in A, \quad p \wedge (q \vee r) &= (p \wedge q) \vee (p \wedge r) \\ \text{e} \quad p \vee (q \wedge r) &= (p \vee q) \wedge (p \vee r) \end{aligned}$$

- b) (Apostila 2)

$$\begin{aligned} E &\neq \emptyset \text{ (universo)} \\ A &= P(E) = \{X \mid X \subseteq E\} \\ \Delta &= \cap, \square = \cup \quad (\text{comutativas}) \\ \forall X, Y, Z \in A, \quad X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) \\ \text{e} \quad X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z) \end{aligned}$$

**Definição 4.6 (Anel, Domínio de Integridade e Corpo).** Seja  $A \neq \emptyset$  munido de duas operações binárias

$$\begin{aligned} + : A \times A \rightarrow A & \quad \cdot : A \times A \rightarrow A \\ (a, a') \mapsto a + a' & \quad \text{e} \quad (a, a') \mapsto a \cdot a' \end{aligned}$$

Dizemos que a tripla  $(A, +, \cdot)$  é um Anel se:

i)  $(A, +)$  é um grupo comutativo (também chamado grupo abeliano)

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

b) Existe  $0 \in A$  tal que  $0 + a = a = a + 0$

c) Para todo  $a \in A$ , existe  $a' = -a \in A$  tal que  $a + (-a) = 0$

d)  $a + b = b + a \quad (\forall a, b \in A)$

ii)  $(A, \cdot)$  é um semigrupo:

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

iii) Vale a distributividade à esquerda e à direita

$$\begin{cases} a \cdot (b + c) = ab + ac \\ e \\ (b + c) \cdot a = ba + ca \end{cases}$$

**Observações.** a) Se  $\cdot$  é comutativa, então  $(A, +, \cdot)$  é dito um Anel Comutativo.

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

b) Se  $A$  possui um elemento neutro para a operação  $\cdot$  ( $= 1$ ), então  $(A, +, \cdot)$  é dito um Anel Comutativo com Identidade. (identidade = elemento neutro para  $\cdot$ )

c)  $(A, +, \cdot)$  é dito um Domínio de Integridade se  $A$  é um anel comutativo com identidade  $1 \neq 0$  tal que  $\forall a, b \in A, a \neq 0 \text{ e } b \neq 0 \Rightarrow a \cdot b \neq 0$  (Pela contra-positiva, isto é equivalente a  $\forall a, b \in A, a \cdot b = 0 \Rightarrow a = 0$  ou  $b = 0$ )

d)  $(A, +, \cdot)$  é dito um Corpo se  $A$  é um anel comutativo com identidade  $1 \neq 0$  tal que todo elemento não-nulo é inversível para a operação  $\cdot$  :

$$\forall a \in A - \{0\}, \exists a^{-1} \in A \mid a \cdot a^{-1} = 1 = a^{-1} \cdot a$$

**Exemplos:**

a)  $(\mathbb{Z}, +, \cdot)$  = domínio de integridade, mas não é corpo.

Justificativa: não é corpo, pois apenas 1 e  $-1$  possuem inverso para a multiplicação (2 não tem inverso em  $\mathbb{Z}$ , pois  $2^{-1} = 1/2 \notin \mathbb{Z}$ )

b)  $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$  = corpos

- c)  $(\mathcal{M}_{n \times n}(\mathbb{R}), +, \cdot) = \text{anel}$ . Não-comutativo com identidade (logo, em particular, não é domínio de integridade) e, além disso, é possível que  $a \cdot b = 0$  com  $a \neq 0$  e  $b \neq 0$ .

Justificativa:  $n = 2$

$$- I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ é a identidade}$$

- não-comutativa:

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R}) \quad \text{e} \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$$

$$a \cdot b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$\neq$

$$b \cdot a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

-  $a \neq 0$  e  $b \neq 0$  tal que  $a \cdot b = 0$

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$$b = \begin{pmatrix} 3 & 4 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$$a \cdot b = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

- d)  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot) = \text{anel comutativo com identidade}$ , mas não é domínio de integridade, pois existem  $f, g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ , ambas não-nulas, tal que  $f \cdot g = 0$ .

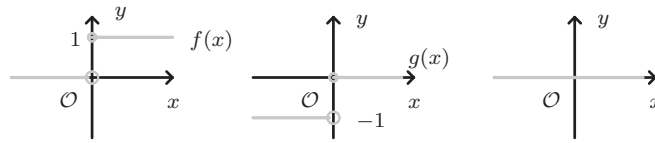
**Observação.**  $f \equiv 0 \Leftrightarrow f(x) = 0, \forall x \in \mathbb{R}$

$$f \neq 0 \Leftrightarrow \exists x \in \mathbb{R} \mid f(x) \neq 0$$

**Exemplo:**

$$f(x) = \begin{cases} 0, & \text{se } x < 0 \\ 1, & \text{se } x \geq 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} -1, & \text{se } x < 0 \\ 0, & \text{se } x \geq 0 \end{cases}$$

$$f(x) \cdot g(x) = \begin{cases} 0 \cdot (-1) = 0, & \text{se } x < 0 \\ 1 \cdot 0 = 0, & \text{se } x \geq 0 \end{cases}$$



**Teorema 4.7.** *Todo corpo é um domínio de integridade.*

**Observação.** Não vale a recíproca, ou seja, nem todo domínio de integridade é um corpo.

**Exemplo:**  $\mathbb{Z}$  é um domínio de integridade, mas NÃO é corpo (pois apenas os números 1 e  $-1$  são inversíveis para a multiplicação). (Isto é, a equação  $a \cdot x = 1$  só tem solução em  $\mathbb{Z}$  se  $a = 1$  ou  $-1$ )

**Demonstração.**

- $\left\{ \begin{array}{l} \text{H: } (A, +, \cdot) \text{ é um corpo} \\ \text{T: } (A, +, \cdot) \text{ é um domínio de integridade} \end{array} \right.$

Por hipótese,  $(A, +, \cdot)$  é um corpo, ou seja,  $A$  é um anel comutativo com identidade  $1 \neq 0$  tal que  $\forall a \in A, a \neq 0, \exists a^{-1} \in A \mid a \cdot a^{-1} = 1 = a^{-1} \cdot a$ . Queremos mostrar que  $(A, +, \cdot)$  é um domínio de integridade. Portanto, basta mostrar que  $\forall a, b \in A$ , se  $a \cdot b = 0$ , então  $a = 0$  ou  $b = 0$ .

- $\left\{ \begin{array}{l} \text{H: } a \cdot b = 0 \\ \text{T: } a = 0 \text{ ou } b = 0 \end{array} \right.$

Vamos mostrar que se  $a \neq 0$ , então  $b = 0$  (analogamente, se  $b \neq 0$  então  $a = 0$ ).

Por hipótese,  $a \cdot b = 0$  (\*), com  $a \neq 0$ . Como  $a \neq 0$  e  $(A, +, \cdot)$  é um corpo, então  $\exists a^{-1} \in A \mid a \cdot a^{-1} = 1 = a^{-1} \cdot a$ . Assim, multiplicando (\*) por  $a^{-1}$ :

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

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

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

Se  $b \neq 0$  então  $\exists b^{-1} \in A : b \cdot b^{-1} = 1 = b^{-1} \cdot b$ , assim

$$a \cdot b = 0$$

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

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

■

Alguns exemplos clássicos de anéis e grupos (aplicações à Física, Computação, Geometria, Variáveis Complexas, Álgebra Linear, etc)

## A) Anéis



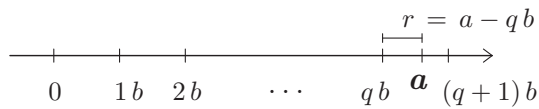
quatro exemplos: 
$$\begin{cases} \text{A.1) } \mathbb{Z} \\ \text{A.2) } \mathbb{Z}_n \text{ (anel dos inteiros módulo } n) \\ \text{A.3) } \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R} \\ \text{A.4) } \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C} \end{cases}$$

### A.1) O anel dos inteiros - $\mathbb{Z}$

- $(\mathbb{Z}, +, \cdot)$  = domínio de integridade;
- $\leq$  = ordem total;  
 $(x \leq y \Leftrightarrow x - y \leq 0, \forall x, y \in \mathbb{Z})$
- P.B.O.: (2ª versão)  
 Todo subconjunto não-vazio de  $\mathbb{Z}$ , limitado inferiormente, possui elemento mínimo, isto é,  $\forall A \subseteq \mathbb{Z}, A \neq \emptyset, \exists m = \min(A)$ , ou seja,  $m \in A$  e  $m \leq x, \forall x \in A$ . Logo, para tais conjuntos (“A”), vale o Princípio de Indução.

**Teorema 4.8 (Algoritmo da Divisão de Euclides).** *Sejam  $a, b \in \mathbb{Z}$ , com  $b > 0$ . Então, existem únicos  $q, r \in \mathbb{Z}$  tais que  $a = b + qr$ , onde  $0 \leq r < b$ . ( $a$  = dividendo,  $b$  = divisor,  $q$  = quociente,  $r$  = resto)*

Geometricamente: ( $a, b > 0$ )



**Demonstração.** I) Existência de  $q$  e  $r$ :

Defina  $A = \{a - bx \mid x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$ . Temos que  $A \subseteq \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ .

**Afirmação.**  $A \neq \emptyset$

De fato:

Tome  $x = -|a|$ . Então,

$$a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$$

Assim, tal número  $a - bx$ , para  $x = -|a|$ , pertence a  $A$ . Logo, pelo P.B.O.,  $\exists \min(A) = r$ .

Temos que:

a)  $r \in A \Rightarrow \exists x = q \in \mathbb{Z} \mid r = a - bx = a - bq$  (ou  $a = bq + r$ ). Além disso,  $r \geq 0$ .

b)  $r \leq y, \forall y \in A$ . Falta mostrar que  $r < b$ .

Suponha, por absurdo, que  $r \geq b$ . Considere o número  $y = a - b(q + 1)$ . Temos que

$$y = a - b(q + 1) = a - bq - b = r - b < r$$

Por outro lado,  $y = r - b \geq 0$ . Assim,  $y \in A$  com  $y < r$  (absurdo). (pois contradiz a minimalidade de  $r$ )

Conclusão:  $r < b$

II) Unicidade de  $q$  e  $r$ :

Vamos mostrar que se  $a = bq + r = bq' + r'$ , com  $q, q', r, r' \in \mathbb{Z}$  e  $0 \leq r, r' < b$ , então  $q = q'$  e  $r = r'$ .

$$bq + r = bq' + r' \Rightarrow bq - bq' = r' - r \Rightarrow b(q - q') = r' - r$$

Se mostrarmos que  $q = q'$ , segue que  $r' = r$ . Suponha, por absurdo, que  $q' \neq q$ . Assim,  $q' - q \neq 0$ . Então,

$$|q' - q| > 0 \Rightarrow |q' - q| \geq 1 \quad (1)$$

Por outro lado,

$$\begin{cases} 0 \leq r' < b \\ 0 \leq r < b \end{cases} \Rightarrow |r' - r| < b \quad (2)$$

Voltando à igualdade anterior:

$$|b||q - q'| = |b(q - q')| = |r' - r|$$

$$b \stackrel{(1)}{\leq} b|q - q'| = |r' - r| \stackrel{(2)}{<} b \quad (\text{absurdo})$$

Conclusão:  $q' = q$  ( $\Rightarrow r' = r$ ) ■

**Exercício:** Calcule  $q$  e  $r$  nos seguintes casos:

a)  $a = 102$ ;  $b = 7$

$$\begin{array}{r} 102 \quad | \underline{7} \\ 32 \quad 14 \\ 4 \end{array}$$

$$102 = 7 \cdot 14 + 4$$

b)  $a = -102$ ;  $b = 7$   
 $-102 = 7 \cdot 15 + 3$

**Corolário 4.9.** Dados  $a, b \in \mathbb{Z}$ , com  $b \neq 0$ , existem únicos  $q, r \in \mathbb{Z}$  tais que  $a = bq + r$ , onde  $0 \leq r < |b|$ .

**Demonstração.** Como  $b \neq 0$ , segue que  $|b| > 0$ . Pelo Teorema anterior, existem únicos  $q', r' \in \mathbb{Z}$  tais que  $a = |b|q' + r'$ , com  $0 \leq r' < |b|$ .

1ª caso:  $b > 0$ : neste caso,  $|b| = b$ . Assim, basta tomar  $q' = q$  e  $r' = r$  :  $a = bq + r$ , com  $0 \leq r < b$ .

2ª caso:  $b < 0$ : neste caso,  $|b| = -b$ . Assim, basta tomar  $q = -q'$  e  $r = r'$  :  $a = -bq' + r' = b(-q') + r'$ , com  $0 \leq r < -b$ . ■

**Exemplos:**  $102 = (-7)(\underline{-14}) + \underline{4}$   
 $-102 = (-7) \underline{15} + \underline{3}$

**Observação.** Se  $r = 0$ , então dizemos que a divisão é EXATA. Neste caso,  $a = bq$  e dizemos que “ $b$  divide  $a$ ” ou “ $b$  é divisor de  $a$ ” ou “ $b$  é fator de  $a$ ” ou “ $a$  é múltiplo de  $b$ ” ou “ $a$  é divisível por  $b$ ”.

**Notação.**  $b \mid a \Leftrightarrow \exists q \in \mathbb{Z} \mid bq = a$  ( $\Leftrightarrow q = a/b \in \mathbb{Z}$ )  
 negação:  $b \nmid a$

**Exemplos:**  $-3 \mid 12$  (pois  $(-3)(-4) = 12$ )  
 $-5 \mid -60$  (pois  $(-5)(12) = -60$ )  
 $-7 \nmid 20$  (pois  $-7x = 20$  não tem solução em  $\mathbb{Z}$ )

**Teorema 4.10 (Regras de Divisibilidade).**

- i)  $1 \mid a$ ;  $a \mid a$ ;  $a \mid 0$ ;
- ii)  $a \mid 1 \Leftrightarrow a = 1$  ou  $-1$ ;  $0 \mid b \Leftrightarrow b = 0$ ;
- iii)  $a \mid b$  e  $c \mid d \Rightarrow ac \mid bd$ ;
- iv)  $a \mid b$  e  $b \mid c \Rightarrow a \mid c$ ;
- v)  $a \mid b$  e  $b \mid a \Rightarrow a = b$  ou  $a = -b$ ;
- vi)  $a \mid b$  e  $b \neq 0 \Rightarrow |a| \leq |b|$ ;
- vii)  $a \mid b$  e  $a \mid c \Rightarrow a \mid bx + cy$ ,  $\forall x, y \in \mathbb{Z}$   
 Em particular,  $a \mid b + c$  ( $x = y = 1$ ) e  $a \mid b - c$  ( $x = 1$  e  $y = -1$ )

**Demonstração.**

$$\text{vi)} \begin{cases} \text{H: } a \mid b \text{ e } b \neq 0 \\ \text{T: } |a| \leq |b| \end{cases}$$

$$a \mid b \Rightarrow \exists q \in \mathbb{Z} \mid a q = b$$

Como  $b \neq 0$ , segue que  $a \neq 0$  e  $q \neq 0$ .

$$|a q| = |b| \\ |a| \leq |a| \underbrace{|q|}_{\geq 1} = |b|$$

$$\begin{aligned} \text{vii)} \begin{cases} \text{H: } a \mid b \text{ e } a \mid c \\ \text{T: } a \mid bx + cy \end{cases} \\ a \mid b \Rightarrow \exists m \in \mathbb{Z} \mid a m = b \quad (\times x) \\ a \mid c \Rightarrow \exists n \in \mathbb{Z} \mid a n = c \quad (\times y) \\ a m = b \xrightarrow{(\times x)} a m x = b x \quad \oplus \\ a n = c \xrightarrow{(\times y)} a n y = c y \\ \Rightarrow a m x + a n y = b x + c y \Rightarrow a \underbrace{(m x + n y)}_{q \in \mathbb{Z}} = b x + c y \Rightarrow a \mid b x + c y \end{aligned}$$

■

**Notações.**  $a \in \mathbb{Z}$

$$D(a) = \{ \text{divisores inteiros de } a \}$$

$$D_+(a) = \{ \text{divisores naturais de } a \}$$

$$M(a) = \{ \text{múltiplos inteiros de } a \} = a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$$

$$M_+(a) = \{ \text{múltiplos naturais de } a \}$$

**Exemplos:** a)  $D(1) = \{\pm 1\}$

$$\text{b) } D_+(1) = \{1\}$$

$$\text{c) } D(2) = \{\pm 1, \pm 2\}$$

$$\text{d) } D_+(2) = \{1, 2\}$$

$$\text{e) } D(4) = \{\pm 1, \pm 2, \pm 4\}$$

$$\text{f) } D_+(4) = \{1, 2, 4\}$$

$$\text{g) } D(0) = \mathbb{Z}$$

$$\text{h) } M(0) = \{0\}$$

$$\text{i) } M(2) = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \dots\} \quad (\text{números pares})$$

**Definição 4.11** (Máximo Divisor Comum e Mínimo Múltiplo Comum).

*M.D.C. (Máximo Divisor Comum)*

Sejam  $a, b \in \mathbb{Z}$ , não simultaneamente nulos. Definimos o M.D.C. de  $a$  e  $b$  como sendo o número natural  $d = \text{mdc}(a, b)$  satisfazendo as seguintes condições:

i)  $d \mid a$  e  $d \mid b$ ;

ii) Se  $c \in \mathbb{N}$  tal que  $c \mid a$  e  $c \mid b$ , então  $c \mid d$  ( $\Rightarrow |c| \leq |d| \Rightarrow c \leq d$ ).  
Em outras palavras,  $d = \max[D(a) \cap D(b)]$ .

*M.M.C. (Mínimo Múltiplo Comum)*

Sejam  $a, b \in \mathbb{Z}$ , ambos  $\neq 0$ . Definimos o M.M.C. de  $a$  e  $b$  como sendo o número natural  $m = \text{mmc}(a, b)$  satisfazendo as seguintes condições:

i)  $a \mid m$  e  $b \mid m$ ;

ii) Se  $c \in \mathbb{N}$  tal que  $a \mid c$  e  $b \mid c$ , então  $m \mid c$  ( $\Rightarrow |m| \leq |c| \Rightarrow m \leq c$ ).  
Em outras palavras,  $m = \min[M_+(a) \cap M_+(b)]$ .

**Exemplo:**  $a = 45 \Rightarrow D(45) = \{\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 45\}$

$b = 36 \Rightarrow D(36) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}$

$D(45) \cap D(36) = \{\pm 1, \pm 3, \pm 9\}$

$d = \text{mdc}(45, 36) = \max[D(45) \cap D(36)] = 9$

**Observação.** Se  $a = 0$  e  $b \neq 0$ , então  $\text{mdc}(a, b) = |b|$

**Exemplo:**  $a = 45 \Rightarrow M(45) = \{45k \mid k \in \mathbb{Z}\} = \{0, \pm 45, \pm 90, \pm 135, \pm 180, \pm 225, \dots\}$

$b = 36 \Rightarrow M(36) = \{36k \mid k \in \mathbb{Z}\} = \{0, \pm 36, \pm 72, \pm 108, \pm 144, \pm 180, \pm 216, \dots\}$

$M_+(45) = \{45, 90, 135, 180, 225, \dots\}$

$M_+(36) = \{36, 72, 108, 144, 180, 216, \dots\}$

$M_+(45) \cap M_+(36) = \{180, 360, 540, \dots\}$

$m = \min[M_+(45) \cap M_+(36)] = 180$

Se  $a = b = 0$ , então  $D(a) = D(b) = \mathbb{Z}$ ,  $D(a) \cap D(b) = \mathbb{Z}$ , não existe elemento máximo ( $\nexists$  mdc). Se  $a = 0$  ou  $b = 0$ ,  $M(0) = \{0\}$ ,  $M_+(0) = \emptyset$ , não existe elemento mínimo ( $\nexists$  mmc).

Alguns resultados importantes a respeito do M.D.C. e do M.M.C. (cujas demonstrações são vistas no curso de Teoria dos Números):

1) Sejam  $a, b \in \mathbb{Z}$ , não simultaneamente nulos. Seja  $d = \text{mdc}(a, b)$ . Então, existem  $x_0, y_0 \in \mathbb{Z}$  tais que  $d = ax_0 + by_0$ .

2) Sejam  $a, b \in \mathbb{Z}$ , ambos não-nulos. Seja  $d = \text{mdc}(a, b)$  e  $m = \text{mmc}(a, b)$ . Então,  $d \cdot m = |a \cdot b|$ .

**Exemplo:**  $a = 45, b = 36$

$$d = \text{mdc}(45, 36) = 9 \text{ e } m = \text{mmc}(45, 36) = 180$$

$$|a b| = a b = 45 \cdot 36 = 1620 = 9 \cdot 180 = d m$$

3) (Método das Divisões Sucessivas para o Cálculo do M.D.C.)

Sejam  $a, b \in \mathbb{Z}$ , com  $b \neq 0$ . Faça  $r_0 = |b|$ . Existem  $q_1, r_1 \in \mathbb{Z}$  com  $a = b q_1 + r_1$ , onde  $0 \leq r_1 < |b| = r_0$ .

Se  $r_1 = 0$ , então pare.

Se  $r_1 \neq 0$ , então existem  $q_2, r_2 \in \mathbb{Z}$  com  $r_0 = r_1 q_2 + r_2$ , onde  $0 \leq r_2 < r_1$ .

Se  $r_2 = 0$ , então pare.

Se  $r_2 \neq 0$ , então existem  $q_3, r_3 \in \mathbb{Z}$  com  $r_1 = r_2 q_3 + r_3$ , onde  $0 \leq r_3 < r_2$ .

$\vdots$

$$r_{k-2} = r_{k-1} q_k + r_k, \text{ onde } 0 \leq r_k < r_{k-1}$$

$\vdots$

Após um número finito de passos, existirá  $n \in \mathbb{N}$  tal que  $r_n \neq 0$  e  $r_{n+1} = 0$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, \text{ onde } 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1} q_n + r_n, \text{ onde } 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + \underbrace{0}_{r_{n+1}}$$

**Afirmção.**  $\text{mdc} = r_n$  (último resto não nulo)

$$\underbrace{r_0 > r_1 > r_2 > r_3 > \cdots > r_k > \cdots \geq 0}$$

seqüência decrescente de inteiros não negativos (limitada); tal seqüência converge para 0

**Exemplo:**  $d = \text{mdc}(45, 36) = 9$

$$\begin{array}{l} \text{restos} \rightarrow \begin{array}{c|c|c} & 9 & 0 \\ \hline 45 & 36 & 9 \\ \hline \end{array} \\ \text{quocientes} \rightarrow \begin{array}{c|c|c} & 1 & 4 \\ \hline & 1 & 4 \\ \hline \end{array} \end{array}$$

**Exercícios Seleccionados:**

1) Considere  $a = 180$  e  $b = 252$

a) Calcule  $d = \text{mdc}(a, b)$  pelo método das divisões sucessivas

b) Determine  $x_0, y_0 \in \mathbb{Z}$  tais que  $d = ax_0 + by_0$

c) Calcule  $m = \text{mmc}(a, b)$

2) Sejam  $a, b \in \mathbb{Z}$ , não simultaneamente nulos. Dizemos que  $a$  e  $b$  são *primos entre si* (ou relativamente primos ou co-primos) se  $d = \text{mdc}(a, b) = 1$ . Mostre que dois números consecutivos são primos entre si.

3) Sejam  $a, b, c \in \mathbb{Z}$  tais que  $a \mid bc$  e  $\text{mdc}(a, b) = 1$ . Mostre que  $a \mid c$ .

### Resolução:

1) a)

$$\begin{array}{c|c|c|c|c} & 180 & 72 & 36 & 0 \\ \hline 180 & 252 & 180 & 72 & 36 \\ \hline & 0 & 1 & 2 & 2 \end{array} \Rightarrow d = \text{mdc}(180, 252) = 36$$

b)  $252 = 180 \cdot 1 + 72$

$$180 = 72 \cdot 2 + 36$$

$$72 = 36 \cdot 2 + 0$$

$$36 = 180 - 72 \cdot 2 = 180 - (252 - 180 \cdot 1) \cdot 2 = 3 \cdot 180 + (-2) \cdot 252$$

$$x_0 = 3, y_0 = -2$$

c)  $m = \text{mmc}(180, 252)$

$$a = 180, b = 252, d = \text{mdc}(180, 252) = 36$$

Segue que  $a \cdot b = d \cdot m$ , isto é

$$m = \frac{a \cdot b}{d} = \frac{252 \cdot 180}{36} = 1260$$

2) H:  $n, n + 1$  são dois números consecutivos

$$T: d = \text{mdc}(n, n + 1) = 1$$

**Demonstração.** De fato:

$$d = \text{mdc}(n, n + 1) \Rightarrow \begin{cases} d \mid n \\ d \mid n + 1 \end{cases} \text{ e}$$

$$\stackrel{\text{vii)}}{\Rightarrow} d \mid (n + 1) - n = 1 \stackrel{\text{ii)}}{\Rightarrow} d = 1 \text{ ou } -1 \stackrel{d \geq 0}{\Rightarrow} d = 1$$

■

3)

$$H: \begin{cases} a \mid bc \\ \text{mdc}(a, b) = 1 \end{cases}$$

$$T: a \mid c$$

**Demonstração.**  $a \mid bc \Rightarrow \exists m \in \mathbb{Z} \mid am = bc \quad (*)$

$$\text{mdc}(a, b) = 1 \Rightarrow \exists x_0, y_0 \in \mathbb{Z} \mid ax_0 + by_0 = 1 \quad (**)$$

Queremos mostrar que  $a \mid c$ , ou seja,  $\exists l \in \mathbb{Z} \mid al = c$

Multiplicando  $(**)$  por  $c$ :

$$c(ax_0 + by_0) = c \cdot 1 \Rightarrow cax_0 + cby_0 = c \xrightarrow{(*)} cax_0 + amy_0 = c$$

$$\Rightarrow a \underbrace{(cx_0 + my_0)}_{l \in \mathbb{Z}} = c \Rightarrow a \mid c$$

■

#### Definição 4.12 (Número Primo e Número Composto).

- 1ª versão: (em  $\mathbb{N}$ )

Dizemos que  $n \in \mathbb{N}$  é primo se:

$$i) \ n > 1;$$

$$ii) \ D_+(n) = \{1, n\}$$

(equivalentemente: se  $n = a \cdot b$ , com  $a, b \in \mathbb{N}$ , então ou  $a = 1$  ou  $b = 1$ )

Dizemos que  $n \in \mathbb{N}$  é composto se ele não é primo, ou seja,  $n > 1$  e é possível escrever  $n = a \cdot b$ , com  $1 < a, b < n$  ( $a, b \in \mathbb{N}$ ).

- 2ª versão: (em  $\mathbb{Z}$ )

Dizemos que  $n \in \mathbb{Z}$  é primo se:

$$i) \ n \neq 1 \text{ e } n \neq -1;$$

$$ii) \ D(n) = \{-1, 1, n, -n\}$$

Dizemos que  $n \in \mathbb{Z}$  é composto se ele não é primo, isto é, se  $n \neq \pm 1$  e  $|D(n)| > 4$ .

Vamos nos restringir apenas ao caso natural.



**Observação.** 1 e  $n$  são ditos divisores triviais de  $n$

**Exemplos:** a) 2, 3, 5, 7, 11, 13, 17, 19, 23, ... são primos

b) 4 é composto (pois  $D_+(4) = \{1, 2, 4\}$ )

6 é composto (pois  $D_+(6) = \{1, 2, 3, 6\}$ )

**Notação.**  $\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ é primo}\}$

### Exercícios Selecionados:

- 1) a) Sejam  $p \in \mathbb{P}$  e  $a, b \in \mathbb{N}$ . Mostre que se  $p \mid a \cdot b$ , então  $p \mid a$  ou  $p \mid b$ .  
b) Através de um contra-exemplo, verifique que a) é falso se o número for composto.
- 2) Seja  $n \in \mathbb{N}$ ,  $n > 1$ . Mostre que existe  $p \in \mathbb{P}$  tal que  $p \mid n$  (isto é, todo número natural  $> 1$  tem um primo que o divide).

**Observação.** De 2), segue o Teorema Fundamental da Aritmética:

Seja  $n \in \mathbb{N}$ ,  $n > 1$

- a) Existem  $p_1, p_2, \dots, p_r \in \mathbb{P}$  (não necessariamente distintos:  $p_1 \leq p_2 \leq \dots \leq p_r$ ) tais que  $n = p_1 \dots p_r$
- b) Tal decomposição é única, ou seja, se  $n = p_1 \dots p_r = q_1 \dots q_s$ , com  $p_1, \dots, p_r \in \mathbb{P}$  ( $p_1 \leq p_2 \leq \dots \leq p_r$ ) e  $q_1, \dots, q_s \in \mathbb{P}$  ( $q_1 \leq q_2 \leq \dots \leq q_s$ ), então  $r = s$  e  $p_1 = q_1, p_2 = q_2, \dots, p_r = q_s$ .

### Resolução:

- 1) a) **Demonstração.**

$$\text{H: } \begin{cases} p \in \mathbb{P} \\ p \mid a \cdot b \end{cases}$$

$$\text{T: } p \mid a \text{ ou } p \mid b$$

Queremos mostrar que se  $p \mid a \cdot b$ , então  $p \mid a$  ou  $p \mid b$ . Vamos mostrar que se  $p \nmid a$ , então  $p \mid b$ . (analogamente, se  $p \nmid b$ , então  $p \mid a$ )

De fato:  $p \mid a \cdot b$  e  $p \nmid a$ .

**Afirmção.**  $\text{mdc}(p, a) = 1$

$$d = \text{mdc}(p, a) \Rightarrow \begin{cases} d \mid a \\ \text{e} \\ d \mid p \end{cases}$$

Como  $d \mid p$  e  $p \in \mathbb{P}$ , então  $d = 1$  ou  $p$ . Temos que  $d \neq p$ , pois, do contrário, teríamos que  $(d =)p \mid a$  (o que contradiz a nossa suposição inicial). Assim,  $d = 1$ . Portanto,

$$\begin{cases} p \mid a \cdot b \\ \text{mdc}(p, a) = 1 \end{cases} \Rightarrow p \mid b \quad \blacksquare$$

b) contra-exemplo:  $6 \notin \mathbb{P}$

$$6 = 2 \cdot 3$$

$$6 \mid 6 = 2 \cdot 3, \text{ mas } 6 \nmid 2 \text{ e } 6 \nmid 3$$

2) H:  $n > 1$  ( $n \in \mathbb{N}$ )

T:  $\exists p \in \mathbb{P} \mid p \text{ divide } n$

**Demonstração.**  $A = \{ \text{divisores naturais de } n, \text{ maiores do que } 1 \}$   
 $= \{ t \in \mathbb{N} \mid t > 1 \text{ e } t \mid n \}$

$A \neq \emptyset$  (pois  $n \in A$ );  $A \subseteq \mathbb{N}$

$\xRightarrow{\text{P.B.O.}} \exists p = \min(A)$

**Afirmção.**  $p \in \mathbb{P}$

De fato: Como  $p \in A$ , segue que  $p > 1$ .  $p$  não pode ser composto pois, do contrário, chegaríamos ao seguinte absurdo:

$$p = a \cdot b, \text{ com } 1 < a, b < p = \min(A)$$

$$\begin{cases} a \mid p \\ p \mid n \end{cases} \xRightarrow{(\text{trans})} a \mid n$$

$a \mid n$  e  $a > 1 \Rightarrow a \in A$  (absurdo), pois  $a < p = \min(A)$

Conclusão:  $p \in \mathbb{P}$  ■

**Teorema 4.13 (de Euclides).**  $\mathbb{P}$  é infinito

**Demonstração.**  $\mathbb{P} = \{x \in \mathbb{N} \mid x \text{ é primo}\} = \{2, 3, 5, 7, \dots\}$

Suponha, por absurdo, que  $\mathbb{P}$  fosse finito.  $\mathbb{P} = \{p_1, p_2, \dots, p_r\}$

Considere  $N = p_1 p_2 \dots p_r + 1 > 1$ . Pelo exercício 2), existe  $p \in \mathbb{P} \mid p \mid N$ .

Como  $\mathbb{P}$  é finito, então  $p = p_k$ , onde  $1 \leq k \leq r$ .

$$\begin{cases} p_k \mid N = p_1 p_2 \dots p_k \dots p_r + 1 & (*) \\ p_k \mid p_1 p_2 \dots p_k \dots p_r & (**) \end{cases}$$

Em particular,  $p_k \mid (*) - (**) = N - p_1 p_2 \dots p_k \dots p_r$   
 $p_k \mid (*) - (**) = (p_1 p_2 \dots p_k \dots p_r + 1) - (p_1 p_2 \dots p_k \dots p_r) = 1 \Rightarrow p_k = 1$   
 ou  $-1$   
 $\xRightarrow{p_k \in \mathbb{N}} p_k = 1$  (absurdo), pois  $p_k \in \mathbb{P}$  (logo, não pode ser 1)  
 Conclusão:  $\mathbb{P}$  é infinito. ■

## A.2) O anel dos inteiros módulo $n$ - $\mathbb{Z}_n$

**Definição 4.14 (Congruência módulo  $n$ ).** *Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ ,  $n > 1$ . Dizemos que  $a$  e  $b$  são congruentes módulo  $n$  se  $n \mid a - b$ .*

**Notação.**  $a \equiv b \pmod{n}$  (lê-se:  $a$  é congruente a  $b$  módulo  $n$ )  
 $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$ , ou seja, existe  $k \in \mathbb{Z} \mid nk = a - b$

**Exemplo prático:** Relógio digital (congruência módulo 12)

$$15 \equiv \underbrace{3}_{\text{resto da divisão de 15 por 12}} \pmod{12}, \text{ pois } 12 \mid 15 - 3$$

resto da divisão de 15 por 12

$$21 \equiv 9 \pmod{12}, \text{ pois } 12 \mid 21 - 9$$

**Observação.** A negação de  $a \equiv b \pmod{n}$  é  $a \not\equiv b \pmod{n}$

**Teorema 4.15.** *A congruência módulo  $n$  define uma relação de equivalência sobre  $\mathbb{Z}$ .*

**Demonstração.** De fato:

(RE1) Reflexiva:  $a \equiv a \pmod{n}$  pois  $n \mid a - a = 0$  ( $n \cdot 0 = 0$ )

(RE2) Simétrica:  $\overbrace{a \equiv b \pmod{n}}^H \Rightarrow \overbrace{b \equiv a \pmod{n}}^T$

$a \equiv b \pmod{n} \Rightarrow n \mid a - b \Rightarrow nk = a - b$ , para algum  $k \in \mathbb{Z} \Rightarrow \overbrace{(-k)}^{l \in \mathbb{Z}} n = b - a \Rightarrow n \mid b - a$ , isto é,  $b \equiv a \pmod{n}$

(RE3) Transitiva:  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

$$a \equiv b \pmod{n} \Rightarrow n \mid a - b \Rightarrow nk_1 = a - b \quad (k_1 \in \mathbb{Z}) \quad (1)$$

$$b \equiv c \pmod{n} \Rightarrow n \mid b - c \Rightarrow nk_2 = b - c \quad (k_2 \in \mathbb{Z}) \quad (2)$$

$$(1) + (2): nk_1 + nk_2 = a - c \Rightarrow n(k_1 + k_2) = a - c \Rightarrow nk_3 = a - c \\ \Rightarrow a \equiv c \pmod{n} \quad \blacksquare$$

**Exercícios Seleccionados:**

- 1) Verifique as seguintes propriedades de congruências:  $a \equiv b \pmod{n}$ ,  
 $c \equiv d \pmod{n}$
- a)  $a + c \equiv b + d \pmod{n}$   
b)  $a \cdot c \equiv b \cdot d \pmod{n}$   
c)  $a^k \equiv b^k \pmod{n}$ ,  $\forall k \in \mathbb{N}$
- 2) Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ ,  $n > 1$ . Então,  $a \equiv b \pmod{n} \Leftrightarrow a$  e  $b$  deixam o mesmo resto na divisão por  $n$ .
- 3) Sejam  $a \in \mathbb{Z}$  e  $n \in \mathbb{N}$ ,  $n > 1$ . Então, existe um único  $r \in \mathbb{Z}$ , com  $0 \leq r \leq n - 1$  tal que  $a \equiv r \pmod{n}$ .

### Resolução:

- 1) H:  $a \equiv b \pmod{n} \Rightarrow n \mid a - b \Rightarrow nk_1 = a - b \quad (k_1 \in \mathbb{Z}) \quad (*)$   
 $c \equiv d \pmod{n} \Rightarrow n \mid c - d \Rightarrow nk_2 = c - d \quad (k_2 \in \mathbb{Z}) \quad (**)$
- a) T:  $a + c \equiv b + d \pmod{n}$   
Queremos mostrar que  $n \mid (a + c) - (b + d)$ . De fato:
- $$\left. \begin{array}{l} n \mid a - b \\ \text{e} \\ n \mid c - d \end{array} \right\} \Rightarrow n \mid (a - b) + (c - d) (= (a + c) - (b + d))$$
- b) T:  $ac \equiv bd \pmod{n}$   
Queremos mostrar que  $n \mid ac - bd$ , ou seja,  $nk_3 = ac - bd$  para algum  $k_3 \in \mathbb{Z}$ . De fato:
- $$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) \stackrel{(*)}{=} \stackrel{(**)}{=} ank_2 + dnk_1 = n \underbrace{(ak_2 + dk_1)}_{k_3 \in \mathbb{Z}} \Rightarrow n \mid ac - bd$$
- c) H:  $a \equiv b \pmod{n} \Rightarrow n \mid a - b \Rightarrow nq_1 = a - b \quad (1)$   
T:  $a^k \equiv b^k \pmod{n} \Rightarrow n \mid a^k - b^k \Rightarrow nq_2 = a^k - b^k \quad (2)$
- i)  $k_0 = 2$  :
- $$nq_1 = a - b \xrightarrow{\times(a+b)} n \underbrace{q_1(a+b)}_{q_2} = (a - b)(a + b) = (a^2 - b^2) \Rightarrow$$
- $$n \mid a^2 - b^2 \Rightarrow a^2 \equiv b^2 \pmod{n}$$

ii) Supondo que  $a^m \equiv b^m \pmod{n}$  seja válido para todo  $m$ , tal que  $2 \leq m < k$ , temos que mostrar que  $a^k \equiv b^k \pmod{n}$  é verdadeiro.

$$\text{Temos que } a^{k-1} \equiv b^{k-1} \pmod{n} \Rightarrow nq_3 = a^{k-1} - b^{k-1} \quad (3)$$

Então,

$$\begin{aligned} a^k - b^k &= a^k - a b^{k-1} + a b^{k-1} - b^k \\ &= a(a^{k-1} - b^{k-1}) + b^{k-1}(a - b) \\ &\stackrel{(3) \text{ e } (1)}{=} a n q_3 + b^{k-1} n q_1 \\ &= n \underbrace{(a q_3 + b^{k-1} q_1)}_{q_4} \end{aligned}$$

$$\Rightarrow n \mid a^k - b^k \Rightarrow a^k \equiv b^k \pmod{n}, \forall k \in \mathbb{Z}$$

2)  $a \equiv b \pmod{n} \Leftrightarrow a$  e  $b$  deixam o mesmo resto na divisão por  $n$ .

**Demonstração.**  $(\Leftarrow)$  H:  $\begin{cases} a = n q_1 + r \\ b = n q_2 + r \end{cases}$

T:  $a \equiv b \pmod{n}$

$$a - b = (n q_1 + r) - (n q_2 + r) = n q_1 - n q_2 = n(q_1 - q_2) = n q_3$$

$$\Rightarrow n \mid a - b \Rightarrow a \equiv b \pmod{n}$$

$$(\Rightarrow) \text{ H: } a \equiv b \pmod{n} \Rightarrow \bar{a} = \bar{b} \text{ em } \mathbb{Z}_n$$

$$\text{T: } r_1 = r_2, \text{ onde } \begin{cases} r_1 = a - n q_1 \\ r_2 = b - n q_2 \end{cases}, \quad 0 \leq r_1, r_2 < n$$

Vamos supor que  $r_1 \neq r_2$ . Então  $0 < |r_1 - r_2| < n$ . Temos

$$\begin{aligned} \bar{a} = \bar{b} &\Rightarrow \overline{n q_1 + r_1} = \overline{n q_2 + r_2} \\ &\Rightarrow \overline{n q_1} + \overline{r_1} = \overline{n q_2} + \overline{r_2} \Rightarrow \overline{n q_1} + \overline{r_1} = \overline{n q_2} + \overline{r_2} \\ &\Rightarrow \overline{0 q_1} + \overline{r_1} = \overline{0 q_2} + \overline{r_2} \Rightarrow \overline{0} + \overline{r_1} = \overline{0} + \overline{r_2} \\ &\Rightarrow \overline{r_1} = \overline{r_2} \Rightarrow r_1 \equiv r_2 \pmod{n} \\ &\Rightarrow n \mid r_1 - r_2 \Rightarrow n k = r_1 - r_2 \end{aligned}$$

$$n \stackrel{(*)}{\leq} |n||k| = |n k| = |r_1 - r_2| < n \quad (\text{absurdo})$$

$$(*) \quad n > 0 \text{ e } |k| > 0$$

Então  $r_1 = r_2$ . ■

3) H:  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ ,  $n > 1$

T: existe um único  $r \in \mathbb{Z}$ , com  $0 \leq r \leq n-1$ , tal que  $a \equiv r \pmod{n}$

**Demonstração.** Como  $n \in \mathbb{N}$ , podemos dividir  $a$  por  $n$ . Pelo Algoritmo da Divisão de Euclides, existem únicos  $q, r \in \mathbb{Z}$  tais que  $a = nq + r$ , com  $0 \leq r < n \Leftrightarrow 0 \leq r \leq n-1$

$$a = nq + r \Rightarrow a - r = nq \Rightarrow n \mid a - r \Rightarrow a \equiv r \pmod{n} \quad \blacksquare$$

**Observação.** Na divisão por  $n$ , há  $n$  restos possíveis:  $0, 1, 2, \dots, n-1$ .

Objetivo: “Operar” (adicionar e multiplicar) com tais congruências.

**Notação.**  $a \in \mathbb{Z}$

- $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$   
(classe de equivalência de  $a$  pela congruência módulo  $n$  ou classe de resíduo de  $a$  módulo  $n$ )

$$\bar{a} = \{x \in \mathbb{Z} \mid n \mid x - a\} = \{x \in \mathbb{Z} \mid nk = x - a, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x = a + nk, k \in \mathbb{Z}\}$$

- $\mathbb{Z}/\sim = \mathbb{Z}/\equiv \pmod{n} = \mathbb{Z}_n = \{\bar{a} \mid a \in \mathbb{Z}\}$   
(conjunto dos inteiros módulo  $n$ )

Pelo exercício 3, tal conjunto  $\mathbb{Z}_n$  é finito, a saber:  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$  (classes dos resíduos, ou restos, na divisão por  $n$ )

**Observações.** a)  $\bar{a}$  ( $a$  é dito um representante da classe)

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{n}$$

b)  $\mathbb{Z}_n$  é uma partição de  $\mathbb{Z}$

- $\bar{a} \neq \emptyset$
- $\bar{a} \neq \bar{b} \Rightarrow \bar{a} \cap \bar{b} = \emptyset$
- $\bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$

**Exemplos:**

a)  $n = 2$

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

$$\bar{0} = \{x = 0 + 2k = 2k, k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \dots, \pm 2k, \dots\} \quad (\text{pares})$$

$$\bar{1} = \{x = 1 + 2k, k \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\} \quad (\text{ímpares})$$

$\bar{0}$	$\bar{1}$	$\mathbb{Z}$
$\parallel$	$\parallel$	
$\{2k\}$	$\{2k + 1\}$	

b)  $n = 3 \quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$$\bar{0} = \{3k, k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$$

$$\bar{1} = \{3k + 1, k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, \dots\}$$

$$\bar{2} = \{3k + 2, k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\mathbb{Z}$
-----------	-----------	-----------	--------------

### Operações Binárias Módulo $n$

- Adição:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$(\bar{x}, \bar{y}) \mapsto \bar{x} + \bar{y} \stackrel{\text{def}}{=} \overline{x + y}$$

- Multiplicação:

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$(\bar{x}, \bar{y}) \mapsto \bar{x} \cdot \bar{y} \stackrel{\text{def}}{=} \overline{x \cdot y}$$

**Teorema 4.16.** a) As operações de “+” e “ $\cdot$ ” acima estão bem definidas, ou seja, independem da escolha dos representantes das classes;

b)  $(\mathbb{Z}_n, +, \cdot)$  é um anel comutativo com identidade (anel dos inteiros módulo  $n$ );

c)  $(\mathbb{Z}_n, +, \cdot)$  é um domínio de integridade  $\Leftrightarrow n = p \in \mathbb{P}$ ;

d) Se  $n = p \in \mathbb{P}$ , então  $(\mathbb{Z}_p, +, \cdot)$  é um corpo.

**Demonstração.**

$$\begin{aligned} \text{a)} \quad \overline{x} + \overline{y} &= \overline{x + y} \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y} \end{aligned}$$

Para que tais operações sejam válidas, elas não devem depender da escolha dos representantes  $x$  e  $y$  das classes envolvidas. Isto é, se  $x' \equiv x \pmod{n}$  (isto é,  $\overline{x'} = \overline{x}$ ) e  $y' \equiv y \pmod{n}$  (isto é,  $\overline{y'} = \overline{y}$ ), então  $\overline{x' + y'} = \overline{x + y}$  e  $\overline{x' \cdot y'} = \overline{x \cdot y}$ .

Tal resultado segue do exercício 1 (página 105) (propriedades de congruência)

$$\begin{aligned} \begin{cases} x' \equiv x \pmod{n} \\ y' \equiv y \pmod{n} \end{cases} &\Rightarrow \begin{cases} x' + y' \equiv x + y \pmod{n} \\ x' \cdot y' \equiv x \cdot y \pmod{n} \end{cases} \\ \Rightarrow \begin{cases} \overline{x' + y'} = \overline{x + y} \\ \overline{x' \cdot y'} = \overline{x \cdot y} \end{cases} \end{aligned}$$

b) Tese:  $(\mathbb{Z}_+, +, \cdot)$  é um anel comutativo com identidade.  
De fato:

i)  $(\mathbb{Z}_+, +)$  é um grupo abeliano:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c});$$

$$\overline{a} + \overline{0} = \overline{a} = \overline{0} + \overline{a};$$

$$\overline{a} + (\overline{-a}) = \overline{0} = (\overline{-a}) + \overline{a};$$

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}$$

ii)  $(\mathbb{Z}_+, \cdot)$  é um semigrupo  $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ ;

iii) Valem as leis distributivas

$$\begin{cases} \overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \\ \text{e} \\ (\overline{b} + \overline{c}) \cdot \overline{a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a} \end{cases}$$

iv)  $\cdot$  é comutativo  $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ ;

v)  $\cdot$  possui  $\overline{1}$  como elemento neutro:  $\overline{a} \cdot \overline{1} = \overline{a} = \overline{1} \cdot \overline{a}$

c)  $(\mathbb{Z}_n, +, \cdot)$  é DI  $\Leftrightarrow n = p \in \mathbb{P}$

( $\Leftarrow$ ) H:  $n = p \in \mathbb{P}$

T:  $(\mathbb{Z}_n, +, \cdot)$  é DI

Queremos mostrar que  $(\mathbb{Z}_n, +, \cdot)$  é um Domínio de Integridade, isto é, anel comutativo com identidade tal que

$$\overline{a} \cdot \overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0} \quad (\overline{a}, \overline{b} \in \mathbb{Z}_n)$$



Falta mostrar que se  $\bar{a} \cdot \bar{b} = \bar{0}$ , então  $\bar{a} = \bar{0}$  ou  $\bar{b} = \bar{0}$

(\*) Lembre-se:  $p \in \mathbb{P}$ ,  $p \mid a \cdot b \Rightarrow p \mid a$  ou  $p \mid b$

$\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \overline{a \cdot b} = \bar{0} \Rightarrow a \cdot b \equiv 0 \pmod{p} \Rightarrow p \mid a \cdot b - 0 = a \cdot b$

$$\stackrel{(*)}{\Rightarrow} \left\{ \begin{array}{l} p \mid a \\ \text{ou} \\ p \mid b \end{array} \right. \Rightarrow \left\{ \begin{array}{l} p \mid a - 0 \\ \text{ou} \\ p \mid b - 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} a \equiv 0 \pmod{p} \\ \text{ou} \\ b \equiv 0 \pmod{p} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \bar{a} = \bar{0} \\ \text{ou} \\ \bar{b} = \bar{0} \end{array} \right.$$

( $\Rightarrow$ ) H:  $(\mathbb{Z}_+, +, \cdot)$  é DI

T:  $n \in \mathbb{P}$

pela contra-positiva,  $(H \Rightarrow T) \Leftrightarrow (\neg T \Rightarrow \neg H)$

$\neg T$ :  $n \notin \mathbb{P}$ , ou seja,  $n$  é composto:  $n = a \cdot b$ , com  $1 < a, b < n$ .

$n = a \cdot b \Rightarrow \bar{n} = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = \bar{0}$ , onde  $\bar{a} \neq \bar{0}$  e  $\bar{b} \neq \bar{0}$ , pois como

$$\left\{ \begin{array}{l} a < n, \text{ então } n \nmid a - 0 \quad (a \not\equiv 0 \pmod{n}) \\ b < n, \text{ então } n \nmid b - 0 \quad (b \not\equiv 0 \pmod{n}) \end{array} \right.$$

d) Tese:  $n = p \in \mathbb{P} \Rightarrow (\mathbb{Z}_p, +, \cdot)$  é corpo

Queremos mostrar que  $(\mathbb{Z}_p, +, \cdot)$  é corpo, ou seja, anel comutativo com identidade tal que todo elemento  $\neq 0$  possui inverso multiplicativo:

$$\forall \bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}, \exists (\bar{a})^{-1} \in \mathbb{Z}_p \mid \bar{a} (\bar{a})^{-1} = \bar{1}$$

Falta mostrar que dado  $\bar{a} \in \mathbb{Z}_p$ ,  $\bar{a} \neq \bar{0}$ ,  $\exists (\bar{a})^{-1} \in \mathbb{Z}_p \mid \bar{a} (\bar{a})^{-1} = \bar{1}$

De fato:

(\*) Lembre-se:  $p \in \mathbb{P}$ ;  $a \in \mathbb{Z}$

$p \nmid a \Rightarrow \text{mdc}(p, a) = 1$

Tome  $\bar{a} \in \mathbb{Z}_p$ , com  $\bar{a} \neq \bar{0}$ . Isto equivale a dizer que  $a \not\equiv 0 \pmod{p}$ , ou seja,  $p \nmid a - 0 = a$ . Por (\*),  $\text{mdc}(p, a) = 1$ . Logo, existem  $x_0, y_0 \in \mathbb{Z}$ :  $px_0 + ay_0 = 1$ .

Tomando a classe de equivalência

$$\begin{aligned} \overline{px_0 + ay_0} = \bar{1} &\Rightarrow \overline{px_0} + \overline{ay_0} = \bar{1} \Rightarrow \bar{p} \bar{x_0} + \bar{a} \bar{y_0} = \bar{1} \\ &\Rightarrow \bar{0} \bar{x_0} + \bar{a} \bar{y_0} = \bar{1} \Rightarrow \bar{0} + \bar{a} \bar{y_0} = \bar{1} \Rightarrow \bar{a} \underbrace{\bar{y_0}}_{(\bar{a})^{-1}} = \bar{1} \end{aligned}$$

■

**Exemplos:** (Construção das tábuas de adição e multiplicação para  $\mathbb{Z}_n$ )

- $n = 2$ :  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ , onde  $\bar{0} = \{2k \mid k \in \mathbb{Z}\}$  (pares) e  $\bar{1} = \{1 + 2k \mid k \in \mathbb{Z}\}$  (ímpares)

$$\begin{array}{c|c|c}
+ & \overline{0} & \overline{1} \\
\hline
\overline{0} & \overline{0} & \overline{1} \\
\hline
\overline{1} & \overline{1} & \overline{0}
\end{array}
\qquad
\begin{array}{c|c|c}
\cdot & \overline{0} & \overline{1} \\
\hline
\overline{0} & \overline{0} & \overline{0} \\
\hline
\overline{1} & \overline{0} & \overline{1}
\end{array}$$

- $n = 3$ :  $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ , onde

$$\begin{cases}
\overline{0} = \{3k \mid k \in \mathbb{Z}\} \\
\overline{1} = \{1 + 3k \mid k \in \mathbb{Z}\} \\
\overline{2} = \{2 + 3k \mid k \in \mathbb{Z}\}
\end{cases}$$

$$\begin{array}{c|c|c|c}
+ & \overline{0} & \overline{1} & \overline{2} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} \\
\hline
\overline{1} & \overline{1} & \overline{2} & \overline{0} \\
\hline
\overline{2} & \overline{2} & \overline{0} & \overline{1}
\end{array}
\qquad
\begin{array}{c|c|c|c}
\cdot & \overline{0} & \overline{1} & \overline{2} \\
\hline
\overline{0} & \overline{0} & \overline{0} & \overline{0} \\
\hline
\overline{1} & \overline{0} & \overline{1} & \overline{2} \\
\hline
\overline{2} & \overline{0} & \overline{2} & \overline{1}
\end{array}$$

- $n = 4$ :  $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ , onde

$$\begin{cases}
\overline{0} = \{4k \mid k \in \mathbb{Z}\} \\
\overline{1} = \{1 + 4k \mid k \in \mathbb{Z}\} \\
\overline{2} = \{2 + 4k \mid k \in \mathbb{Z}\} \\
\overline{3} = \{3 + 4k \mid k \in \mathbb{Z}\}
\end{cases}$$

$$\begin{array}{c|c|c|c|c}
+ & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\
\hline
\overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\
\hline
\overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2}
\end{array}
\qquad
\begin{array}{c|c|c|c|c}
\cdot & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\
\hline
\overline{1} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\overline{2} & \overline{0} & \overline{2} & \overline{0} & \overline{2} \\
\hline
\overline{3} & \overline{0} & \overline{3} & \overline{2} & \overline{1}
\end{array}$$

- $n = 5$ :  $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ , onde

$$\begin{cases}
\overline{0} = \{5k \mid k \in \mathbb{Z}\} \\
\overline{1} = \{1 + 5k \mid k \in \mathbb{Z}\} \\
\overline{2} = \{2 + 5k \mid k \in \mathbb{Z}\} \\
\overline{3} = \{3 + 5k \mid k \in \mathbb{Z}\} \\
\overline{4} = \{4 + 5k \mid k \in \mathbb{Z}\}
\end{cases}$$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

- $n = 6$  :  $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ , onde

$$\begin{cases} \overline{0} = \{6k \mid k \in \mathbb{Z}\} \\ \overline{1} = \{1 + 6k \mid k \in \mathbb{Z}\} \\ \overline{2} = \{2 + 6k \mid k \in \mathbb{Z}\} \\ \overline{3} = \{3 + 6k \mid k \in \mathbb{Z}\} \\ \overline{4} = \{4 + 6k \mid k \in \mathbb{Z}\} \\ \overline{5} = \{5 + 6k \mid k \in \mathbb{Z}\} \end{cases}$$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

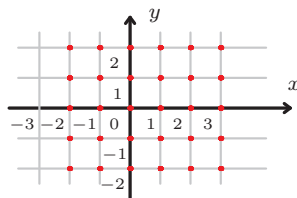
**Exercício:**  $\mathbb{Z}_6$  é DI? Justifique através de um exemplo.

Não, pois 6 é composto. Exemplo:  $\overline{2} \neq \overline{0}$  (pois  $6 \nmid 2 - 0$ ),  $\overline{3} \neq \overline{0}$  (pois  $6 \nmid 3 - 0$ ), mas  $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$

**A.3)**  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z} \text{ e } i^2 = -1\} \subset \mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$   
 ( $i$  = unidade imaginária)

Graficamente:  $\mathbb{C} \leftrightarrow \mathbb{R}^2$  (plano bidimensional)

$\mathbb{Z}[i] \leftrightarrow \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}$



- Adição:

$$x = a + bi \in \mathbb{Z}[i]$$

$$y = c + di \in \mathbb{Z}[i]$$

$$\begin{array}{ccccc} x + y = & (a + bi) & + & (c + di) & \stackrel{\text{def}}{=} & (a + c) + (b + d)i \\ & \parallel & & \parallel & & \parallel \\ & (a, b) & & (c, d) & & (a + c, b + d) \end{array}$$

- Multiplicação:

$$x \cdot y = (a + bi) \cdot (c + di) = (ac - bd) + (da + bc)i$$

$(\mathbb{Z}[i], +, \cdot)$  é um anel comutativo com identidade

$$0 + 0i, 1 = 1 + 0i, -(a + bi) = (-a) + (-b)i$$

### Exercícios:

- 1) Mostre que  $(\mathbb{Z}[i], +, \cdot)$  é um domínio de integridade.
- 2) Mostre que  $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$  (portanto,  $\mathbb{Z}[i]$  não é corpo)

**Observação.** O anel  $(\mathbb{Z}[i], +, \cdot)$  é dito o anel dos inteiros gaussianos.

### Resolução:

- 1) Falta mostrar que se  $(a + bi) \cdot (x + yi) = 0 (= 0 + 0i)$  então  $a + bi = 0$  ou  $x + yi = 0$

De fato:

Suponha que  $a + bi \neq 0$ , isto é,  $a \neq 0$  ou  $b \neq 0$  (analogamente,  $x + yi \neq 0$ ). Vamos mostrar que  $x + yi = 0$ .

$$(a + bi)(x + yi) = 0 = 0 + 0i \Leftrightarrow \begin{cases} ax - by = 0 \\ ay + bx = 0 \end{cases} \Leftrightarrow \begin{cases} ax - by = 0 \\ bx + ay = 0 \end{cases} \quad (*)$$

(\*) é um Sistema Linear Homogêneo com duas equações a duas incógnitas:  $x, y$ .

Em notação matricial:

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

$$\det A = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 > 0 \ (\neq 0)$$

(pois  $(a, b) \neq (0, 0)$ )

$\Rightarrow (*)$  é um SPD, isto é, tem solução única, a saber: trivial  $(0, 0)$ .

2) Tese:  $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

Queremos resolver a seguinte equação:

$$\underbrace{(a + bi)}_{\text{(dado)}} \underbrace{(x + yi)}_{\text{(a obter)}} = 1 = 1 + 0i$$

Como queremos que o produto seja 1, então  $a + bi \neq 0$  e  $x + yi \neq 0$

$$(a + bi)(x + yi) = 1 = 1 + 0i \Leftrightarrow \begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases} \Leftrightarrow \begin{cases} ax - by = 1 \\ bx + ay = 0 \end{cases}$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Regra de Cramer

$$x = \frac{\begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{a}{a^2 + b^2} \quad y = \frac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{-b}{a^2 + b^2}$$

Assim,

$$x + yi = (a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in \mathbb{Z}[i]$$

Como  $\frac{a}{a^2 + b^2} \in \mathbb{Z}$  e  $\frac{-b}{a^2 + b^2} \in \mathbb{Z}$ , devemos impor que  $a^2 + b^2 = 1$ .

$$a^2 + b^2 = 1 \text{ tem solução em } \mathbb{Z} \Leftrightarrow \begin{cases} a^2 = 1 \\ \text{e} \\ b^2 = 0 \end{cases} \text{ ou } \begin{cases} a^2 = 0 \\ \text{e} \\ b^2 = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} a = \pm 1 \\ \text{e} \\ b = 0 \end{cases} \text{ ou } \begin{cases} a = 0 \\ \text{e} \\ b = \pm 1 \end{cases}$$

Assim,  $(1, 0), (-1, 0), (0, 1)$  e  $(0, -1)$  são as únicas soluções em  $\mathbb{Z}$ .

**A.4)**  $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$

• Adição:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

- Multiplicação:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

**Exercício:** Mostre que  $(\mathbb{Z}[\sqrt{2}], +, \cdot)$  é um domínio de integridade.

$(\mathbb{Z}[\sqrt{2}], +, \cdot)$  é DI, ou seja, é um anel comutativo com identidade  $1 \neq 0$ , tal que, se  $a + b\sqrt{2} \neq 0$  e  $c + d\sqrt{2} \neq 0$ , então  $(a + b\sqrt{2})(c + d\sqrt{2}) \neq 0$ .

De fato:

- i)  $(\mathbb{Z}[\sqrt{2}], +)$  é um grupo abeliano:
  - $(a + b\sqrt{2}) + [(c + d\sqrt{2}) + (e + f\sqrt{2})] = [(a + b\sqrt{2}) + (c + d\sqrt{2})] + (e + f\sqrt{2})$
  - $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (0 + 0\sqrt{2}) + (a + b\sqrt{2}) = a + b\sqrt{2}$
  - $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = (-a - b\sqrt{2}) + (a + b\sqrt{2}) = 0 + 0\sqrt{2}$
  - $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$
- ii)  $(\mathbb{Z}[\sqrt{2}], \cdot)$  é um semigrupo:
  - $(a + b\sqrt{2})[(c + d\sqrt{2})(e + f\sqrt{2})] = [(a + b\sqrt{2})(c + d\sqrt{2})](e + f\sqrt{2})$
- iii) vale a distributividade à esquerda e à direita
  - $(a + b\sqrt{2})[(c + d\sqrt{2}) + (e + f\sqrt{2})] = [(c + d\sqrt{2}) + (e + f\sqrt{2})](a + b\sqrt{2}) = (a + b\sqrt{2})(c + d\sqrt{2}) + (a + b\sqrt{2})(e + f\sqrt{2})$
- iv) “ $\cdot$ ” é comutativa
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (c + d\sqrt{2})(a + b\sqrt{2})$
- v)  $\mathbb{Z}[\sqrt{2}]$  possui elemento neutro para a “ $\cdot$ ”
  - $(a + b\sqrt{2})(1 + 0\sqrt{2}) = (1 + 0\sqrt{2})(a + b\sqrt{2}) = a + b\sqrt{2}$
- vi) Se  $(a + b\sqrt{2}) \neq 0$  e  $(c + d\sqrt{2}) \neq 0$ , então  $(a + b\sqrt{2})(c + d\sqrt{2}) \neq 0$  ou, pela contra-recíproca,  $(a + b\sqrt{2})(c + d\sqrt{2}) = 0 \Rightarrow (a + b\sqrt{2}) = 0$  ou  $(c + d\sqrt{2}) = 0$ . Seja  $(a + b\sqrt{2})(c + d\sqrt{2}) = 0$ .

– Suponha que  $(a + b\sqrt{2}) \neq 0$ , vamos mostrar que  $(c + d\sqrt{2}) = 0$ .

Temos

$$(ac + 2bd) + (ad + bc)\sqrt{2} = 0 \Rightarrow \begin{cases} ac + 2bd = 0 \\ bc + ad = 0 \end{cases}$$

em notação matricial:

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad (\text{SLH})$$

$$\det \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = a^2 - 2b^2$$

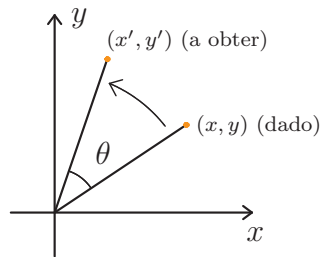
$$a^2 - 2b^2 = 0 \Rightarrow a^2 = 2b^2 \Rightarrow |a| = \sqrt{2}|b|$$

mas  $a, b \in \mathbb{Z}$ , então  $a^2 - 2b^2 \neq 0$ . Daí, temos um SPD, só a solução trivial satisfaz o sistema, então  $c + d\sqrt{2} = 0 + 0\sqrt{2} = 0$

– Analogamente, se  $(c + d\sqrt{2}) \neq 0$ , então  $(a + b\sqrt{2}) = 0$ .

## B) Grupos

### B.1) Grupos de Rotações no Plano $\mathbb{R}^2$



(Rotação de  $(x, y)$  ao redor da origem de  $\theta$  rad no sentido anti-horário)

Em IAL (ou AL):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \underbrace{\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}}_{\text{matriz de rotação em } \mathbb{R}} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\left( \text{Em } \mathbb{R}^3 : \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$

$G = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$  é um grupo com relação à operação de multiplicação de matrizes.

- $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (\theta = 0 \text{ ou } 2\pi)$

- fato:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \text{ se } ad - bc \neq 0$$

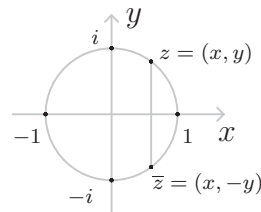
$$\det \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} = \cos^2 \theta + \sin^2 \theta = 1 \neq 0$$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}^{-1} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = A^T$$

( $A^{-1} = A^T$  matrizes ortogonais)

## B.2) Grupos & Variáveis Complexas

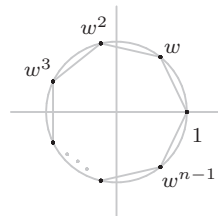
- $G = \{z \in \mathbb{C} \mid |z| = 1\}$  é um grupo com relação à operação de multiplicação em  $\mathbb{C}$ . (círculo unitário)



$$z = \cos \theta + i \sin \theta = e^{i\theta}$$

$$\left( z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2} = \bar{z} \right)$$

- $G = \{z \in \mathbb{C} \mid z^n = 1\} = \{1, w, w^2, \dots, w^{n-1}\}$ , onde  $w = \cos(2\pi/n) + i \sin(2\pi/n)$ , é um grupo com relação à multiplicação em  $\mathbb{C}$ . (raízes  $n$ -ésimas da unidade)



## B.3) Grupos & Química & Física Quântica (Grupo das Simetrias)

Motivação: Química/ Física: (simetrias de uma molécula ou de um cristal)

**Exemplo:**  $\text{NH}_3$  (amônia) (molécula)

$\text{CH}_4$  (metano) (molécula)

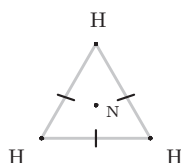


NaCl (cloreto de sódio) (cristal)

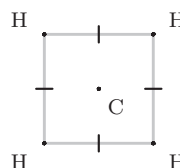
Simetria de uma molécula: movimento em  $\mathbb{R}^3$  que “preserve” a molécula, ou seja, movimento que leve um átomo num átomo do mesmo elemento e preserve as valências.

Simetria de um cristal: movimento em  $\mathbb{R}^3$  que “preserve” o cristal (preservar ligações químicas e propriedades dos elementos)

NH<sub>3</sub>



CH<sub>4</sub>



Em  $\mathbb{R}^2$

Isometria em  $\mathbb{R}^2$ :

$$T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$v \mapsto T(v)$$

bijeção que preserva a distância  $d(T(v_1), T(v_2)) = d(v_1, v_2)$

Em AL: as isometrias em  $\mathbb{R}^2$  são

- Rotação em torno de pontos (linear)
- Reflexões em torno de eixos (linear)
- Translações (não é linear)

Seja  $X \subseteq \mathbb{R}^2$  (por exemplo, um polígono regular) limitado. Uma simetria de  $X$  é uma isometria que leva  $X$  em  $X$ . Neste caso, as únicas simetrias de  $X$  são rotações e reflexões.

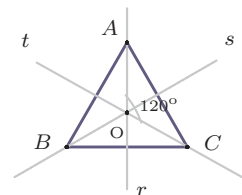
### Grupos Diedrais - $D_n$ :

Grupos das simetrias de um polígono regular de  $n$  lados em  $\mathbb{R}^2$ :

$n = 3$  :  $D_3$  = grupo diedral das simetrias de um triângulo equilátero. (com relação à composição)

$O$  = baricentro (origem fixa)  
(encontro das medianas)

Há seis simetrias para o triângulo equilátero:



- $\rho_{\frac{2\pi}{3}}$ : rotação em torno de  $O$  no sentido anti-horário de  $2\pi/3$ ;
- $\rho_{\frac{4\pi}{3}}$ : rotação em torno de  $O$  no sentido anti-horário de  $4\pi/3$ ;
- $\rho_{2\pi}$ : rotação em torno de  $O$  no sentido anti-horário de  $2\pi$ ;
- $\tau_r$ : reflexão em torno da reta  $r$  passando por  $A$  e  $O$ ;
- $\tau_s$ : reflexão em torno da reta  $s$  passando por  $B$  e  $O$ ;
- $\tau_t$ : reflexão em torno da reta  $t$  passando por  $C$  e  $O$

$$D_3 = \{\rho_{\frac{2\pi}{3}}, \rho_{\frac{4\pi}{3}}, \rho_{2\pi}, \tau_r, \tau_s, \tau_t\}$$

$$\rho_{\frac{2\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_{\frac{4\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \rho_{2\pi} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = Id$$

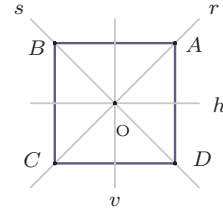
$$\tau_r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(vide 3<sup>a</sup> lista)

$$\begin{cases} \text{rotação} \circ \text{rotação} = \text{rotação} \\ \text{rotação} \circ \text{reflexão} = \text{reflexão} \\ \text{reflexão} \circ \text{reflexão} = \text{rotação} \end{cases}$$

$n = 4$ : (quadrado)

$O$  = centro de gravidade  
(fixo)



Oito simetrias:

- $\rho_{\frac{\pi}{2}}$ : rotação de  $\pi/2$  rad no sentido anti-horário em torno de  $O$ ;
- $\rho_{\pi}$ : rotação de  $\pi$  rad no sentido anti-horário em torno de  $O$ ;
- $\rho_{\frac{3\pi}{2}}$ : rotação de  $3\pi/2$  rad no sentido anti-horário em torno de  $O$ ;
- $\rho_{2\pi} = Id$ : rotação de  $2\pi$  rad no sentido anti-horário em torno de  $O$ ;
- $\tau_r$ : reflexão em torno da reta  $r$ ;
- $\tau_s$ : reflexão em torno da reta  $s$ ;

- $\tau_t$ : reflexão em torno da reta horizontal  $h$ ;
- $\tau_v$ : reflexão em torno da reta vertical  $v$

$$D_4 = \{I, \rho_{\frac{\pi}{2}}, \rho_{\pi}, \rho_{\frac{3\pi}{2}}, \tau_r, \tau_s, \tau_h, \tau_v\}$$

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \rho_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\rho_{\pi} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \rho_{\frac{3\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau_r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \tau_s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\tau_h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \tau_v = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

**Observação.** (Álgebra 2) Pode-se mostrar que o grupo  $D_n$  ( $n \geq 3$ ) é constituído de  $2n$  elementos, a saber:

- $n$  rotações em torno do centro  $O$ :  $2k\pi/n$ ,  $k = 1, \dots, n$
- $n$  reflexões
  - $n$  ímpar: reflexão em torno de retas unindo vértices ao ponto médio do lado oposto
  - $n$  par: reflexão em torno de retas unindo vértices opostos e reflexão em torno de retas unindo pontos médios de lados opostos

#### B.4) Grupos & Física

- Física Nuclear: representação de grupos para classificar partículas elementares (quarks, anti-quarks, mésons, ...)
- $\left\{ \begin{array}{l} \text{interação fraca} \\ \text{interação forte} \\ \text{interação eletromagnética} \end{array} \right.$
- Mecânica Clássica & Relatividade: simetrias que preservem propriedades físicas e mudanças de coordenadas

– (Mecânica Clássica): Grupo de Newton - Galileu

$$\begin{cases} x' = x - vt \\ t' = t \end{cases}$$

– (Relatividade): Grupo de Lorentz

$$\begin{cases} x' = \frac{x - vt}{\sqrt{1 - \left(\frac{v}{c}\right)^2}} \\ t' = \frac{t - \left(\frac{v}{c^2}\right)x}{\sqrt{1 - \left(\frac{v}{c}\right)^2}} \end{cases}$$

( $c$  = velocidade da luz)

### Correção: (lista 3)

9) Lembre-se:  $X \neq \emptyset$

$$\text{Sim}(X) = \text{Bij}(X, X) = \{f : X \rightarrow X \mid f \text{ é bijeção}\}$$

$$* = \circ$$

(Grupo Simétrico sobre  $X$ )

Caso particular:  $X = \{1, 2, \dots, n\}$

$$S_n = \{f : X \rightarrow X \mid f \text{ é bijeção}\}$$

$$- |S_n| = n!$$

$$- X = \{1, 2, 3\}$$

( $n = 3$ ) :  $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ , onde

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e = Id_x \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

( $S_3, \circ$ ) NÃO é abeliano, isto é,  $\circ$  não é comutativa.

### Exemplo:

$$f_2 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3$$

$$f_5 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_4$$

Conclusão:  $f_2 \circ f_5 \neq f_5 \circ f_2$

2) d)  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  (múltiplos de  $n$ )  $n \in \mathbb{N}$

$n = 1 : \mathbb{Z}$

$n = 2 : 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$  (pares)

–  $n\mathbb{Z}$  é fechado para  $+$

$x = nk_1 \in n\mathbb{Z}$  ( $k_1 \in \mathbb{Z}$ ) e  $y = nk_2 \in n\mathbb{Z}$  ( $k_2 \in \mathbb{Z}$ )

$x + y = nk_1 + nk_2 = n \underbrace{(k_1 + k_2)}_{k_3} \in n\mathbb{Z}$

–  $n\mathbb{Z}$  é fechado para  $\cdot$

$x \cdot y = (nk_1) \cdot (nk_2) = n \underbrace{(k_1 nk_2)}_{k_3} \in n\mathbb{Z}$

3)  $A = P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$* = \cap$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

–  $* = \cap$  é comutativa pois a tábua é simétrica em relação à diagonal principal

–  $e = \{a, b\}$  (conjunto universo)

– elementos inversíveis (simetrizáveis):  $\{a, b\}' = \{a, b\}$

– elementos regulares:  $\{a, b\}$

### Exercícios Seleccionados:

1) a) Calcule o mdc ( $d$ ) de  $a = 3887$  e  $b = 637$  usando o método das divisões sucessivas.

b) Determine  $x_0, y_0 \in \mathbb{Z}$  tais que  $d = ax_0 + by_0$

2) Sejam  $A$  um domínio de integridade e  $a, b, c \in A$ . Mostre que se  $ab = ac$  e  $a \neq 0$ , então  $b = c$  (lei do cancelamento)

3) Mostre que  $\sqrt{p}$  é irracional, onde  $p \in \mathbb{P}$ . (Sugestão:  $p \in \mathbb{P}$  e  $p \mid a \cdot b \Rightarrow p \mid a$  ou  $p \mid b$ )

4) Explique o motivo pelo qual

- a)  $\mathbb{Z}$  NÃO é corpo  $(\mathbb{Z}, +, \cdot)$
- b)  $(\mathbb{Z}_6, +, \cdot)$  não é domínio de integridade
- c)  $(\mathbb{N}, +)$  não é monóide
- d)  $(\mathbb{Z}, -)$  não é semigrupo
- e)  $(\mathcal{M}_{2 \times 2}(\mathbb{R}), +, \cdot)$  NÃO é domínio de integridade

**Resolução:**

1) a)

$$\begin{array}{r|rrrr}
 \text{restos} \rightarrow & 65 & 52 & 13 & 0 \\
 \hline
 & 3887 & 637 & 65 & 52 & 13 \\
 \hline
 \text{quocientes} \rightarrow & 6 & 9 & 1 & 4
 \end{array}$$

$$d = \text{mdc}(a, b) = 13$$

b)  $x_0, y_0 \in \mathbb{Z} = ?$

$$13 = 3887x_0 + 637y_0$$

$$3887 = 637 \cdot 6 + 65$$

$$637 = 65 \cdot 9 + 52$$

$$65 = 52 \cdot 1 + 13$$

$$52 = 13 \cdot 4 + 0$$

$$\begin{aligned}
 13 &= 65 - 52 \cdot 1 = 65 - (637 - 65 \cdot 9) \cdot 1 = 65 \cdot 10 - 637 \cdot 1 \\
 &= (3887 - 637 \cdot 6) \cdot 10 - 637 \cdot 1 = 3887 \cdot 10 - 637 \cdot 61 \\
 &= 3887 \cdot 10 + 637 \cdot (-61)
 \end{aligned}$$

2)  $A = \text{DI}$  (anel comutativo com identidade tal que  $a \cdot b = 0 \Rightarrow a = 0$  ou  $b = 0, \forall a, b \in A$ )

$$\text{H: } \begin{cases} ab = ac \\ a \neq 0 \end{cases}$$

$$\text{T: } b = c$$

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

$$\stackrel{A = \text{DI}}{\implies} a = 0 \text{ ou } b - c = 0$$

Como  $a \neq 0$ , segue que  $b - c = 0 \Rightarrow b = c$  ■

- 3) H:  $p \in \mathbb{P}$   
 T:  $\sqrt{p}$  é irracional

**Demonstração.** Suponha, por absurdo, que  $\sqrt{p} \in \mathbb{Q}$ . Assim,  $\exists a, b \in \mathbb{Z}$ , com  $b \neq 0$  tal que  $\sqrt{p} = a/b$ . Sem perda de generalidade,  $a, b \in \mathbb{N}$  e  $a/b$  é uma fração irredutível, isto é,  $\text{mdc}(a, b) = 1$ .

$$\sqrt{p} = \frac{a}{b} \Rightarrow p = \frac{a^2}{b^2} \Rightarrow \underbrace{a^2 = p \cdot b^2}_{(*)} \Rightarrow p \mid a^2 = a \cdot a \Rightarrow p \mid a$$

$$p \mid a \Rightarrow \underbrace{a = p \cdot m}_{(**)} \text{ para algum } m \in \mathbb{N}$$

Substituindo (\*\*) em (\*)

$$(pm)^2 = pb^2 \Rightarrow p^2 m^2 = pb \stackrel{(p \neq 0)}{\Rightarrow} pm^2 = b^2 \Rightarrow p \mid b^2 = b \cdot b \Rightarrow p \mid b$$

Conclusão:  $a$  e  $b$  têm  $p$  como fator comum o que contradiz o fato de  $\text{mdc}(a, b) = 1$ .  $\sqrt{p} \notin \mathbb{Q}$ . ■

- 4) a) Pois apenas 1 e  $-1$  têm inverso multiplicativo ( $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$ )

b)  $6 \notin \mathbb{P}$  ( $6 = 2 \cdot 3$ )  
 $\bar{2} \neq 0$  e  $\bar{3} \neq 0$ , mas  $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

c)  $\nexists$  elemento neutro ( $0 \notin \mathbb{N}$ )

d)  $-$  não é associativa

**Exemplo:**  $(1-2)-3 = -1-3 = -4 \neq 2 = 1-(-1) = 1-(2-3)$

e)  $\cdot$  não é comutativa

**Exemplo:**

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

Existem matrizes não-nulas cujo produto é a matriz nula.

**Exemplo:**

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

## 5 Homomorfismo Entre Estruturas Algébricas

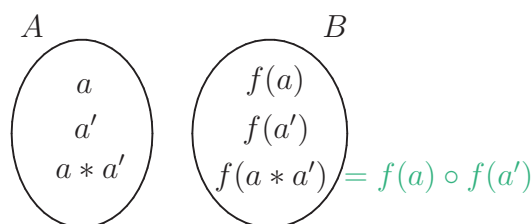
Motivação: Dados  $A$  e  $B$  duas estruturas algébricas do mesmo tipo, queremos definir uma função  $f : A \rightarrow B$  que “preserve” as operações de cada conjunto.

**Definição 5.1 (Homomorfismo Entre Duas Estruturas Algébricas).**

i) (uma operação binária)

Sejam  $(A, *)$  e  $(B, \circ)$  duas estruturas algébricas com uma operação binária. Dizemos que uma função  $f : A \rightarrow B$  é um homomorfismo se  $f$  “preserva” as operações “ $*$ ” e “ $\circ$ ”, ou seja,

$$\forall a, a' \in A, f(a * a') = f(a) \circ f(a')$$



ii) (duas operações binárias)

Sejam  $(A, *, \square)$  e  $(B, \circ, \triangle)$  duas estruturas algébricas com duas operações binárias. Dizemos que uma função  $f : A \rightarrow B$  é um homomorfismo se  $f$  “preserva” as primeiras operações “ $*$ ” e “ $\circ$ ” e também as segundas operações “ $\square$ ” e “ $\triangle$ ” de  $A$  e  $B$ , ou seja,

$$\forall a, a' \in A, f(a * a') = f(a) \circ f(a')$$

e

$$f(a \square a') = f(a) \triangle f(a')$$

### Classificação de Homomorfismo

Seja  $f : A \rightarrow B$  um homomorfismo

a) Se  $f$  é sobrejetora, então  $f$  é dito um *Epimorfismo*;



- b) Se  $f$  é injetora, então  $f$  é dito um *Monomorfismo*;
- c) Se  $f$  é bijeção, então  $f$  é dito um *Isomorfismo*. Neste caso,  $A$  e  $B$  são ditos *isomorfos*.

**Notação.**  $A \cong B$  (lê-se:  $A$  é isomorfo a  $B$ )

Casos particulares

- d) Se  $A = B$ , então  $f$  é dito um *Endomorfismo*
- e) Se  $A = B$  e  $f$  é uma bijeção, então  $f$  é dito um *Automorfismo* (= Endomorfismo Bijetor = Isomorfismo de um conjunto em si mesmo).

**Exemplos:**

- a)  $E = \{a, b\}$   
 $A = B = P(E) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$   
 $*$  =  $\cap$  (operação em  $A$ )  
 $\circ$  =  $\cup$  (operação em  $B$ )  
 $f: A \rightarrow B = A$   
 $X \mapsto f(X) = \mathbb{C}_E(X) = E - X$   
 $f(\emptyset) = \mathbb{C}_E \emptyset = E - \emptyset = E = \{a, b\}$   
 $f(\{a\}) = \mathbb{C}_E \{a\} = E - \{a\} = \{b\}$   
 $f(\{b\}) = \mathbb{C}_E \{b\} = E - \{b\} = \{a\}$   
 $f(E) = \mathbb{C}_E E = E - E = \emptyset$   
 $\left. \begin{array}{l} \bullet f \text{ é injetora} \\ \bullet f \text{ é sobrejetora} \end{array} \right\} \Rightarrow f \text{ é bijeção}$

**Afirmção.**  $f$  é um homomorfismo (entre monóides).

De fato:

$$\begin{aligned} X, Y &\in A \text{ (quaisquer)} \\ f(X * Y) &= f(X) \circ f(Y) \\ f(X \cap Y) &= \mathbb{C}_E(X \cap Y) = \mathbb{C}_E(X) \cup \mathbb{C}_E(Y) = f(X) \cup f(Y) \end{aligned}$$

Conclusão:  $f$  é isomorfismo (na verdade, como  $A = B$ , é automorfismo).

- b)  $A = \mathbb{R}$ ,  $*$  = + (grupo abeliano)  
 $B = \mathbb{R}_+^* = (0, \infty)$ ,  $\circ$  =  $\cdot$  (grupo abeliano)

$$f: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \cdot)$$

$$x \mapsto f(x) = e^x$$

**Afirmação.**  $f$  é um isomorfismo (de grupos)

De fato:

- $f$  é bijeção, pois

$$f^{-1}: (\mathbb{R}_+^*, \cdot) \rightarrow (\mathbb{R}, +)$$

$$x \mapsto f^{-1}(x) = \ln x$$

é a inversa de  $f$ .

- $f$  é homomorfismo:  $x, x' \in \mathbb{R}$   
 $f(x * x') = f(x) \circ f(x')$   
 $f(x + x') = e^{x+x'} = e^x \cdot e^{x'} = f(x) \cdot f(x')$

Analogamente,  $f^{-1}$  é um homomorfismo:

$$f^{-1}(y \cdot y') = \ln(y \cdot y') = \ln y + \ln y' = f^{-1}(y) + f^{-1}(y')$$

Assim,  $(\mathbb{R}, +) \cong (\mathbb{R}_+^*, \cdot)$

- c)  $A = \text{GL}(n, \mathbb{R}) =$  grupo linear geral de dimensão (grau)  $n$  com entradas em  $\mathbb{R} = \{A = (a_{ij}) \in \mathcal{M}_{n \times n}(\mathbb{R}) \mid A \text{ é inversível}\} = \mathcal{U}(\mathcal{M}_{n \times n}(\mathbb{R}))$   
 $*$  =  $\cdot$

(grupo não abeliano)

$$B = \mathbb{R}^* = \mathbb{R} - \{0\} \quad (\text{grupo abeliano})$$

$\circ$  =  $\cdot$

$$f: A \rightarrow B$$

$$X \mapsto f(X) = \det X$$

**Afirmação.**  $f$  é um epimorfismo (de grupos).

- $f$  é um homomorfismo:  
 $X, Y \in A$   
 $f(X \cdot Y) = \det(X \cdot Y) = \det X \cdot \det Y = f(X) \cdot f(Y)$

- $f$  é sobrejetora:

Dado  $\lambda \in B$ , existe  $X \in A$  tal que  $f(X) = \lambda$

$$X = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}_{n \times n} \quad (\text{matriz diagonal})$$

$$\det X = \lambda \cdot \underbrace{1 \cdot 1 \dots 1}_{n-1 \text{ vezes}} = \lambda$$

**Observação.**  $f$  não é injetora, pois matrizes distintas podem ter o mesmo determinante.

**Exemplo:**

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

$$Y = \begin{pmatrix} -1 & & & \\ & -1 & & 0 \\ 0 & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \Rightarrow \det Y = 1$$

$$X \neq Y, \text{ mas } \det X = 1 = \det Y$$

**Exercícios:**

1) Verifique em cada caso que  $f$  é um homomorfismo e classifique-o:

a)  $(A, +, \cdot)$  - anel

$$\begin{aligned} f: A &\rightarrow A \\ x &\mapsto f(x) = x \end{aligned}$$

(aplicação identidade)

b)  $A = \mathbb{Z}$

$$B = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\} \quad (n \in \mathbb{N}, n > 1)$$

(anéis)

$$\begin{aligned} f : A &\rightarrow B \\ x &\mapsto f(x) = \bar{x} \end{aligned}$$

- c)  $A = \mathbb{Z}$ ,  $*$  = +  
 $B = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ ,  $\circ$  = +  
(grupos abelianos)

$$\begin{aligned} f : A &\rightarrow B \\ x &\mapsto f(x) = 2x \end{aligned}$$

- d)  $(A, +, \cdot) = \text{anel}$

$$\begin{aligned} f : A &\rightarrow B = A \\ x &\mapsto f(x) = 0 \end{aligned}$$

(aplicação nula)

- 2) Verifique se

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z} \\ x &\mapsto f(x) = -x \end{aligned}$$

é um homomorfismo de anéis.

**Resolução:**

- 1) a)  $\begin{cases} f(x + x') = x + x' = f(x) + f(x') \\ f(x \cdot x') = x \cdot x' = f(x) \cdot f(x') \end{cases}$   
 $\Rightarrow f$  é homomorfismo  
•  $f$  é bijeção  
isomorfismo (na verdade, automorfismo)
- b)  $\begin{cases} f(x + x') = \overline{x + x'} = \bar{x} + \bar{x}' = f(x) + f(x') \\ f(x \cdot x') = \overline{x \cdot x'} = \bar{x} \cdot \bar{x}' = f(x) \cdot f(x') \end{cases}$   
 $\Rightarrow f$  é homomorfismo  
•  $f$  é sobrejetora:  $CD(f) = \mathbb{Z}_n$

$$Im(f) = \{f(x) \mid x \in A\} = \{\bar{x} \mid x \in \mathbb{Z}\} = \mathbb{Z}_n$$

Conclusão:  $f$  é um epimorfismo (chamado de projeção canônica)

**Observação.**  $f$  não é injetora, pois elementos distintos podem ter a mesma imagem.

**Exemplo:**  $n = 2$

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

$$2 \neq 4, \text{ mas } f(2) = \bar{2} = \bar{0} = \bar{4} = f(4)$$

- c) •  $f(x + x') = 2(x + x') = 2x + 2x' = f(x) + f(x')$   
 $\Rightarrow f$  é homomorfismo de grupo  
•  $f$  é sobrejetora, pois  $Im(f) = \{2x \mid x \in A\} = B = CD(f)$   
•  $f$  é injetora, pois  $\underbrace{x \neq x'}_{\in A} \Rightarrow \underbrace{f(x)}_{\in B} = 2x \neq 2x' = \underbrace{f(x')}_{\in B}$

Assim,  $f$  é bijeção. Logo,  $f$  é isomorfismo ( $\mathbb{Z} \cong 2\mathbb{Z}$ )

- d) •  $f(x + x') = 0 = 0 + 0 = f(x) + f(x')$   
•  $f(x \cdot x') = 0 = 0 \cdot 0 = f(x) \cdot f(x')$

Se  $A \neq \{0\}$ , então  $f$  não é sobrejetora. Além disso,  $f$  não é injetora.

2) a)  $f(x + x') = -(x + x') = -x - x' = (-x) + (-x') = f(x) + f(x')$   
(1ª operação é “preservada”)

b)  $f(x \cdot x') = -(x \cdot x')$   
 $\neq$   
 $f(x) \cdot f(x') = (-x) \cdot (-x') = x \cdot x'$   
(2ª operação NÃO é “preservada”)

Conclusão:  $f$  NÃO é homomorfismo de anéis.

**Observação.** (Álgebra Linear)

$A = V$  = espaço vetorial sobre um corpo  $K$

$+$  (adição de vetores);  $\cdot$  (multiplicação por escalar)

$B = W$  = espaço vetorial sobre um corpo  $K$

$$T: V \rightarrow W$$
$$v \mapsto w = T(v)$$

é uma Transformação Linear se  $T$  “preserva” as operações “+” e “.”, ou seja, se  $T$  é um homomorfismo entre espaços vetoriais

$$\begin{cases} T(v + v') = T(v) + T(v'); (\forall v, v' \in V) \\ T(\alpha v) = \alpha T(v); (\alpha \in K, v \in V) \end{cases}$$

## 6 Polinômios

**Definição 6.1 (Polinômio com Coeficientes num Anel  $A$ ).** *Seja  $A$  um anel comutativo com identidade. Definimos um polinômio na indeterminada  $X$  com coeficientes em  $A$  como sendo uma soma infinita do seguinte tipo:*

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n + 0X^{n+1} + 0X^{n+2} + \dots + 0X^k + \dots$$

(onde  $\exists n \in \mathbb{Z}_+ \mid a_j = 0, \text{ se } j \geq n$ )

*Por convenção, representamos apenas a parte “finita” do polinômio (sem as infinitas parcelas de 0’s).*

**Notações.**  $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$

- $a_i$ ’s  $\in A, 0 \leq i \leq n$ : coeficientes do polinômio  $f(X)$  (constantes);
- $X$ : indeterminada ou “variável” (pode assumir qualquer valor, NÃO necessariamente em  $A$ );
- $a_iX^i$  = monômio de polinômio  $f(X)$ ;
- $A[X] = \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n \mid a_i$ ’s  $\in A (0 \leq i \leq n), n \in \mathbb{Z}_+\}$  (lê-se: conjunto dos polinômios na indeterminada  $X$  com coeficientes no anel  $A$ )

**Observações.** a) Definimos o polinômio identicamente nulo como sendo aquele cujos coeficientes são todos nulos:

$$f(X) = 0 + 0X + 0X^2 + \dots = 0 \quad (a_j$$
’s  $= 0, \forall j \in \mathbb{Z}_+)$

b) Dois polinômios  $f(X)$  e  $g(X)$  são iguais se os respectivos coeficientes são iguais, isto é:

$$f(X) = a_0 + a_1X + \dots + a_nX^n (+ \dots)$$

$$g(X) = b_0 + b_1X + \dots + b_mX^m (+ \dots)$$

$$f(X) = g(X) \Leftrightarrow a_j = b_j, \forall j \in \mathbb{Z}_+$$

c) (Grau de Polinômio)

Seja  $f(X) \in A[X] - \{0\}$ . Então,  $f(X) = a_0 + a_1X + \dots + a_nX^n$ , com  $a_n \neq 0$  e  $a_j = 0$ , se  $j \geq n + 1$ . Definimos o grau de  $f(X)$  como sendo  $\text{gr}(f) = n \in \mathbb{Z}_+$ . NÃO se define grau para o polinômio identicamente nulo.

- Exemplos:** a)  $f(X) = a$  ( $a \neq 0$ )  
 $\text{gr}(f) = 0$  (polinômio constante)  
 b)  $f(X) = b + aX^1$  ( $a \neq 0$ )  
 $\text{gr}(f) = 1$  (polinômio do 1º grau)  
 c)  $f(X) = c + bX + aX^2$  ( $a \neq 0$ )  
 $\text{gr}(f) = 2$  (polinômio do 2º grau)

**Afirmção.** Sejam  $f(X), g(X) \in A[X] - \{0\}$ . Então,  $\text{gr}(\underbrace{f+g}_{\neq 0}) \leq \max\{\text{gr}(f), \text{gr}(g)\}$ .

Em  $A[X]$  vamos definir duas operações

$$f(X) = a_0 + a_1X + \dots + a_nX^n, \text{ com } a_n \neq 0 \quad (\text{gr}(f) = n)$$

$$g(X) = b_0 + b_1X + \dots + b_mX^m, \text{ com } b_m \neq 0 \quad (\text{gr}(g) = m)$$

- Adição:

$$f(X) + g(X) = \underbrace{\sum_{i=0}^k (a_i + b_i)X^i}_{\in A[X]} = (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_k + b_k)X^k,$$

$$\text{onde } k \leq \max\{n, m\}$$

- Multiplicação:

$$f(X) \cdot g(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \dots + (a_0b_k + a_1b_{k-1} + \dots + a_{k-1}b_0)X^k + \dots + a_nb_mX^{n+m} = \sum_{k=0}^{n+m} c_k X^k,$$

$$\text{onde } c_k = \sum_{i=0}^k a_i b_{k-i}$$

Conclusão: Como  $A$  é anel comutativo com identidade, segue que

$$A[X] = \{a_0 + a_1X + \dots + a_nX^n \mid a_i \text{'s} \in A \ (0 \leq i \leq n), \ n \in \mathbb{Z}_+\}$$

é também um anel comutativo com identidade chamado de Anel de Polinômios na Indeterminada  $X$  com Coeficientes em  $A$ .

$$\begin{cases} 0 = \text{polinômio nulo (elemento neutro de } +) \\ 1 = 1 + 0X + \dots \text{ (elemento neutro de } \cdot) \end{cases}$$

Voltando à afirmação anterior  $\text{gr}(f + g) \leq \max\{n, m\}$

De fato:

Suponha que  $n > m$  (se  $n < m$ , o raciocínio é similar). Então,  $\max\{n, m\} = n$ .

$$f(X) = a_0 + a_1X + \dots + a_mX^m + a_{m+1}X^{m+1} + \dots + a_nX^n, \text{ com } a_n \neq 0$$

$$g(X) = b_0 + b_1X + \dots + b_mX^m (+0X^{m+1} + \dots + 0X^n), \text{ com } b_m \neq 0$$

Assim,

$$f(X) + g(X) = (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_m + b_m)X^m + a_{m+1}X^{m+1} + \dots + a_nX^n$$

$$\Rightarrow \text{gr}(f + g) = n = \max\{n, m\}$$

Se  $n = m$  e  $b_n = -a_n$ , então  $\text{gr}(f + g) < n = \max\{n, m\}$

$$f(X) = a_0 + a_1X + \dots + a_nX^n$$

$$g(X) = b_0 + b_1X + \dots + b_nX^n = b_0 + b_1X + \dots + (-a_n)X^n$$

**Teorema 6.2.** *Seja  $A$  um domínio de integridade. Então:*

a) *Se  $f(X), g(X) \in A[X] - \{0\}$ , então  $\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g)$ ;*

b) *Se  $A$  é domínio de integridade, então  $A[X]$  também o é.*

**Observação.** É essencial que  $A$  seja domínio de integridade.

**Exemplo:**  $A = \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  (não é DI, pois  $4 \notin \mathbb{P}$ )

$$f(x) = g(x) = \bar{2}x + \bar{1} \in \mathbb{Z}_4[x]$$

$$\text{gr}(f) = \text{gr}(g) = 1$$

$$f(x) \cdot g(x) = (\bar{2}x + \bar{1})(\bar{2}x + \bar{1}) = (\bar{2}x + \bar{1})^2 = \bar{4}x^2 + \bar{4}x + \bar{1} = \bar{0}x^2 + \bar{0}x + \bar{1}$$

(constante)

$$\text{gr}(f \cdot g) = 0 \neq 2 = \text{gr}(f) + \text{gr}(g)$$

**Demonstração.**

a)  $f(X) = a_0 + a_1X + \dots + a_nX^n$ , onde  $a_n \neq 0$  e  $a_j = 0, j \geq n + 1$   
( $\text{gr}(f) = n$ )

$g(X) = b_0 + b_1X + \dots + b_mX^m$ , onde  $b_m \neq 0$  e  $b_j = 0, j \geq m + 1$   
( $\text{gr}(g) = m$ )

$$f(X) \cdot g(X) = c_0 + c_1X + c_2X^2 + \dots + c_kX^k + \dots, \text{ onde}$$



$$\begin{cases} c_0 = a_0 b_0 \\ c_1 = a_0 b_1 + a_1 b_0 \\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \\ \vdots \\ c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_i b_{k-i} + \dots + a_k b_0 \\ \vdots \end{cases}$$

**Afirmação.**  $\begin{cases} (1) c_{n+m} \neq 0 \\ (2) c_{n+m+j} = 0, j \geq 1 \end{cases}$

$$(1) c_{n+m} = (a_0 b_{n+m} + a_1 b_{n+m-1} + \dots + a_{n-1} b_{m+1}) + (a_n b_m + a_{n+1} b_{m-1} + \dots + a_{n+m} b_0) = a_n b_m$$

Como  $A$  é DI, temos que se  $a_n \neq 0$  e  $b_m \neq 0$ , então  $a_n b_m \neq 0$ . Assim,  $c_{n+m} = a_n b_m \neq 0$ .

(2) Exercício

De (1) e (2), segue que  $\text{gr}(f \cdot g) = n + m = \text{gr}(f) + \text{gr}(g)$

b) Segue trivialmente de a) pois acabamos de mostrar que se  $f(X) \neq 0$  e  $g(X) \neq 0$ , então  $f(X) \cdot g(X) \neq 0$ . ■

### Polinômios $\times$ Funções Polinomiais

Sejam  $A$  um anel comutativo com identidade e  $f(X) = a_0 + a_1 X + \dots + a_n X^n \in A[X]$ . Definimos a função polinomial associada (ou induzida) ao polinômio  $f$  como sendo

$$\begin{aligned} \hat{f}: A &\rightarrow A \\ u &\mapsto \hat{f}(u) = f(u) = \underbrace{a_0 + a_1 u + \dots + a_n u^n}_{\in A} \end{aligned}$$

$$\begin{cases} X = \text{indeterminada} \\ u = \text{variável (restrito a } A) \end{cases}$$

**Observação.** Polinômios diferentes podem induzir a mesma função polinomial.

**Exemplo:**  $A = \mathbb{Z}_2\{\bar{0}, \bar{1}\}$

$$f(x) = x^2 + x \in \mathbb{Z}_2[x] \quad \text{e} \quad g(x) = 0 \in \mathbb{Z}_2[x]$$

Observe que  $f(x) \neq g(x)$ . Todavia,  $\hat{f}(u) = \hat{g}(u)$ ,  $\forall u \in A = \mathbb{Z}_2$  (isto é, as funções polinomiais induzidas são iguais).

$$\begin{aligned}\hat{f}: \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \\ u &\mapsto \hat{f}(u) = f(u) = u^2 + u\end{aligned}$$

$$\begin{aligned}u = \bar{0}: \hat{f}(\bar{0}) &= \bar{0}^2 + \bar{0} = \bar{0} \\ u = \bar{1}: \hat{f}(\bar{1}) &= \bar{1}^2 + \bar{1} = \bar{1} + \bar{1} = \bar{0}\end{aligned}$$

$$\begin{aligned}\hat{g}: \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \\ u &\mapsto \hat{g}(u) = g(u) = \bar{0}, \forall u \in \mathbb{Z}_2\end{aligned}$$

### Divisibilidade e Raízes de Polinômios

$$\begin{aligned}\text{Problema: } f(X) &= a_0 + a_1X + \dots + a_nX^n \in A[X] \\ g(X) &= b_0 + b_1X + \dots + b_mX^m \in A[X] - \{0\}\end{aligned}$$

$$\begin{aligned}a_nX^n + \dots + a_0 &= \begin{array}{c} f(X) \\ r(X) \end{array} \begin{array}{c} \underline{\phantom{f(X)} g(X)} \\ q(X) \end{array} = b_mX^m + \dots + b_0 \\ &= (a_n/b_m)X^{n-m} + \dots\end{aligned}$$

Solução: a partir de agora,  $A = K = \text{corpo } (\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, p \in \mathbb{P})$

**Teorema 6.3 (Algoritmo de Euclides para Divisão de Polinômios).**

Sejam  $f(X), g(X) \in K[X]$ , onde  $K$  é corpo e  $g(X) \neq 0$ . Então,  $\exists!$   $q(X), r(X) \in K[X]$  tais que

$$f(X) = g(X) \cdot q(X) + r(X)$$

onde  $r(X) = 0$  ou  $\text{gr}(r) < \text{gr}(g)$

**Observação.** Se  $r(X) = 0$ , então a divisão é exata. Neste caso,  $f(X) = g(X) \cdot q(X)$

**Notação.**  $g(X) \mid f(X)$  (lê-se: “ $g(X)$  divide  $f(X)$ ” ou “ $g(X)$  é divisor (fator) de  $f(X)$ ” ou “ $f(X)$  é múltiplo de  $g(X)$ ” ou “ $f(X)$  é divisível por  $g(X)$ ”).

**Demonstração.**

I) Existência:

1<sup>a</sup> caso:  $f(X) = 0$

$$\begin{array}{c|c} 0 & g(X) \\ \hline ? & ? \end{array}$$

Tome  $q(X) = 0$  e  $r(X) = f(X) = 0$

$$f(X) = 0 = \underbrace{0}_{q(X)} \cdot g(X) + \underbrace{0}_{r(X)}$$

2ª caso:  $f(X) \neq 0$  e  $\text{gr}(f) < \text{gr}(g)$

Neste caso,

$$f(X) = \underbrace{0}_{q(X)} \cdot g(X) + \underbrace{f(X)}_{r(X)}$$

3ª caso:  $f(X) \neq 0$  e  $\text{gr}(f) \geq \text{gr}(g)$

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X],$$

com  $a_n \neq 0$  ( $\text{gr}(f) = n$ )

$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0 \in K[X] - \{0\},$$

com  $b_m \neq 0$  ( $\text{gr}(g) = m$ )

Por hipótese,  $n \geq m$ .

(\*) Lembre-se: (Princípio da Indução - 2ª versão)

$P(n)$  = sentença aberta que depende de  $n$ , onde  $n \geq n_0$  ( $n_0 \in \mathbb{Z}$  fixo)

Suponha que:

i)  $P(n_0)$  é V;

ii) Dado  $m \in \mathbb{Z}$ , com  $n_0 \leq m < n$ , se  $P(m)$  é V, então  $P(n)$  é V.

Então,  $P(n)$  é V,  $\forall n \geq n_0$ .

Vamos usar indução sobre  $n = \text{gr}(f)$

i)  $n = 0$  ( $= n_0$ ):  $f(X) = a_0 \neq 0$

Como  $n \geq m \geq 0$ , segue que  $m = 0$ , isto é,  $g(X) = b_0 \neq 0$  ( $\Rightarrow \exists b_0^{-1} \in K$ ). Assim,  $f(X) = (a_0/b_0) g(X) + 0$

- ii) Suponha que para todo polinômio de grau menor que  $n$  seja válido o teorema, ou seja, conseguimos dividi-lo por  $g(X)$  para obter  $q(X)$  e  $r(X)$ . Queremos mostrar que o mesmo é válido para  $f$ .

$$\frac{a_n X^n + \dots + a_1 X + a_0}{f_1(X)} \quad \left| \frac{b_m X^m + \dots + b_1 X + b_0}{(a_n/b_m)X^{n-m}} \right.$$

Defina  $f_1(X) = f(X) - g(X) (a_n/b_m)X^{n-m}$

(ou  $f(X) = g(X) (a_n/b_m)X^{n-m} + f_1(X)$ )

Observe que

$$f_1(X) = (a_n X^n + a_{n-1} X^{n-1} + \dots + a_0) - (b_m X^m + \dots + b_1 X + b_0) (a_n/b_m)X^{n-m}$$

Logo,  $\text{gr}(f_1(X)) < n = \text{gr}(f)$

Por (\*), segue que existem  $q_1(X)$  e  $r_1(X)$  tais que

$$f_1(X) = g(X) \cdot q_1(X) + r_1(X),$$

onde  $r_1(X) = 0$  ou  $\text{gr}(r_1(X)) < \text{gr}(g(X))$ . Assim,

$$\begin{aligned} f(X) &= g(X) (a_n/b_m)X^{n-m} + f_1(X) \\ &= g(X) (a_n/b_m)X^{n-m} + (g(X) \cdot q_1(X) + r_1(X)) \\ &= g(X)[(a_n/b_m)X^{n-m} + q_1(X)] + r_1(X) \end{aligned}$$

Faça  $q(X) = (a_n/b_m)X^{n-m} + q_1(X)$  e  $r(X) = r_1(X)$

## II) Unicidade

Suponha que  $\exists q_1(X), q_2(X), r_1(X), r_2(X) \in K[X]$  tal que  $f(X) = g(X) \cdot q_1(X) + r_1(X)$  e  $f(X) = g(X) \cdot q_2(X) + r_2(X)$ , com

$$\begin{cases} r_1(X) = 0 & \text{ou} & \text{gr}(r_1) < \text{gr}(g) \\ r_2(X) = 0 & \text{ou} & \text{gr}(r_2) < \text{gr}(g) \end{cases}$$

$$\text{Tese: } \begin{cases} q_1(X) = q_2(X) \\ r_1(X) = r_2(X) \end{cases} \text{ e}$$

De fato:

$$g(X) \cdot q_1(X) + r_1(X) = g(X) \cdot q_2(X) + r_2(X)$$

$$g(X)[q_1(X) - q_2(X)] = r_2(X) - r_1(X) \quad (**)$$

Basta mostrar que  $q_1(X) = q_2(X)$  ( $\Rightarrow r_2(X) = r_1(X)$ ). Suponha, por absurdo, que  $q_1(X) \neq q_2(X)$ . Assim,  $q_1(X) - q_2(X) \neq 0$  ( $\Rightarrow \text{gr}(q_1 - q_2)$  está bem definido). Tomando grau em (\*\*):

$$\underbrace{\text{gr}(g(X)) + \text{gr}(q_1(X) - q_2(X))}_{\text{gr}(g(X))} \leq \underbrace{\text{gr}(r_2(X) - r_1(X))}_{\leq \max\{\text{gr}(r_1), \text{gr}(r_2)\} < \text{gr}(g)}$$

Assim,  $q_1(X) = q_2(X)$  e, portanto,  $r_1(X) = r_2(X)$ . ■

**Exercícios:** Obtenha  $q(X)$  e  $r(X)$  em cada caso:

- a)  $f(x) = 3x^5 + 4x^3 + 2x + 5$ ,  $g(x) = 2x^3 - 3x^2 + 7$  em  $\mathbb{Q}[x]$  (ou  $\mathbb{R}[x]$ );
- b)  $f(x) = -x^6 + 12x^4 + 8x^3 - 4x + 10$ ,  $g(x) = x^2 - 3$  em  $\mathbb{Z}[x]$
- c)  $\begin{cases} f(x) = \overline{4}x^5 + \overline{3}x^3 - \overline{4}x^2 - \overline{2}x + \overline{3} \\ g(x) = \overline{3}x^2 - \overline{1}x - \overline{2} \end{cases}$  em  $\mathbb{Z}_7[x]$ ,  
onde  $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

### Correção dos Exercícios:

**Observação.** Se o anel de coeficientes  $A$  não for um corpo (como em b), ainda sim é possível dividir  $f(x)$  por  $g(X)$ , desde que  $b_m$  (coeficiente da maior potência de  $g(x)$ ) tenha inverso multiplicativo em  $A$ .

a)

$$\begin{array}{r} 3x^5 + 0x^4 + 4x^3 + 0x^2 + 2x + 5 \quad | \quad 2x^3 - 3x^2 + 7 \\ \underline{-3x^5 + \frac{9}{2}x^4 - \frac{21}{2}x^2} \quad \frac{3}{2}x^2 + \frac{9}{4}x + \frac{43}{8} \\ \frac{9}{2}x^4 + 4x^3 - \frac{21}{2}x^2 + 2x + 5 \\ \underline{-\frac{9}{2}x^4 + \frac{27}{4}x^3 - \frac{63}{4}x} \\ \frac{43}{4}x^3 - \frac{21}{2}x^2 - \frac{55}{4}x + 5 \\ \underline{-\frac{43}{4}x^3 + \frac{129}{8}x^2 - \frac{301}{8}} \\ \frac{45}{8}x^2 - \frac{55}{4}x - \frac{261}{8} \end{array}$$

$$\begin{cases} q(x) = (3/2)x^2 + (9/4)x + (43/8) \\ r(x) = (45/8)x^2 - (55/4)x - (261/8) \end{cases}$$

b)

$$\begin{array}{r}
-x^6 + 12x^4 + 8x^3 - 4x + 10 \quad \Big| \quad 1x^2 - 3 \\
\underline{x^6 - 3x^4} \phantom{+ 8x^3 - 4x + 10} \\
9x^4 + 8x^3 - 4x + 10 \\
\underline{-9x^4 + 27x^2} \\
8x^3 + 27x^2 - 4x + 10 \\
\underline{-8x^3 + 24x} \\
27x^2 + 20x + 10 \\
\underline{-27x^2 + 81} \\
20x + 91
\end{array}$$

$$\begin{cases} q(x) = -x^4 + 9x^2 + 8x + 27 \\ r(x) = 20x + 91 \end{cases}$$

c)

**Observação.** i)  $7 \in \mathbb{P} \Rightarrow \mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$  é corpo  $\Rightarrow \forall \bar{a} \in \mathbb{Z}_7; \bar{a} \neq \bar{0}, \exists \bar{b} \in \mathbb{Z}_7 \mid \bar{a} \cdot \bar{b} = \bar{1}$

ii)  $\overline{k} = \overline{n+k}, \forall k \in \mathbb{Z}$  (em  $\mathbb{Z}_n$ ), pois  $n+k \equiv k \pmod{n}$

**Exemplo:** Em  $\mathbb{Z}_7$  :  $-\bar{4} = \overline{-4+7} = \bar{3}$  (pois  $-4 \equiv 3 \pmod{7}$ )

$$\begin{array}{r}
4x^5 + \bar{0}x^4 + \bar{3}x^3 - \bar{4}x^2 - \bar{2}x + \bar{3} \quad \Big| \quad \bar{3}x^2 - \bar{1}x - \bar{2} \\
\underline{-\bar{18}x^5 + \bar{6}x^4 + \bar{12}x^3} \phantom{- \bar{4}x^2 - \bar{2}x + \bar{3}} \\
-\bar{14}x^5 + \bar{6}x^4 + \bar{15}x^3 - \bar{4}x^2 - \bar{2}x + \bar{3} \\
\underline{-\bar{6}x^4 + \bar{2}x^3 + \bar{4}x^2} \\
\bar{17}x^3 - \bar{2}x + \bar{3} \\
\underline{-\bar{3}x^3 + \bar{1}x^2 + \bar{2}x} \\
\bar{14}x^3 + x^2 + \bar{3} \\
\underline{-\bar{15}x^2 + \bar{5}x + \bar{10}} \\
-\bar{14}x^2 + \bar{5}x + \bar{13}
\end{array}$$

$$\begin{cases} q(x) = \bar{6}x^3 + \bar{2}x^2 + \bar{1}x + \bar{5} \\ r(x) = \bar{5}x + \bar{6} \end{cases}$$

## Raízes de Polinômios

**Definição 6.4 (Raiz de Um Polinômio).** *Sejam  $K$  um corpo e  $f(x) \in K[x] - \{0\}$ . Seja  $\alpha \in K$ .  $\alpha$  é raiz de  $f(x)$  em  $K$  se  $f(\alpha) = 0 \in K$ .*

Obter uma raiz em  $K$  para  $f(x)$  significa resolver a equação polinomial  $f(x) = 0$  em  $K$ .

Três problemas básicos:

- 1ª) Existência de soluções;
- 2ª) Contagem do número de soluções;
- 3ª) Métodos de resolução de equações polinomiais
  - Geométricos;
  - Algébricos;
  - Numéricos;
  - Analíticos

Tais problemas dependem de  $K$ .

**Exemplos:**

- 1)  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ 
  - $K = \mathbb{Q}$ :  $f(x) = 0$  NÃO tem solução em  $K$  (isto é,  $f$  não possui raiz em  $K$ )
  - 0 soluções (pois  $\pm\sqrt{2} \notin K$ )
  - $K = \mathbb{R}$  (ou  $\mathbb{C}$ ):  $f(x) = 0$  tem 2 soluções em  $K$ :  $\pm\sqrt{2} \in K$
- 2)  $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ 
  - $K = \mathbb{Q}$  (ou  $\mathbb{R}$ ):  $f(x) = 0$  NÃO tem solução em  $K$
  - 0 soluções
  - De fato: Se  $\alpha \in K$  fosse raiz de  $f(x)$ , então  $\alpha^2 + 1 = 0$ . Assim,

$$\underbrace{\alpha^2}_{\geq 0} = \underbrace{-1}_{< 0} \quad (\text{absurdo})$$

- $K = \mathbb{C}$ :  $f(x) = 0$  tem 2 soluções em  $K$ :  $\pm i$

- 3)  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$
- $K = \mathbb{Q} : f(x) = 0$  NÃO tem solução em  $K$   
0 soluções
  - $K = \mathbb{R} : f(x) = 0$  tem 1 solução:  $\sqrt[3]{2}$
  - $K = \mathbb{C} : f(x) = 0$  tem 3 soluções:  $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ , onde  $w = \cos(2\pi/3) + i \sin(2\pi/3)$

### Curiosidades: (História da Matemática)

- $\cong 1800$  a.C.: Os babilônios já sabiam resolver determinadas equações práticas de 2<sup>a</sup> grau.

**Exemplo:** Obter dois números  $x, y \in \mathbb{R}$  tais que são conhecidos

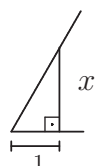
$$\begin{cases} S = x + y \\ P = xy \end{cases}$$

$$(x^2 - Sx + P = 0)$$

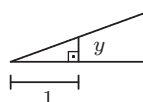
- Civilização grega: Os gregos já sabiam resolver, por métodos geométricos, certas equações do 2<sup>a</sup> e 3<sup>a</sup> graus.

Três Problemas “Clássicos”: (geometria)  
(Construção com Régua e Compasso)

1<sup>a</sup>) Trissecção do Ângulo:



$x =$  “abertura”  
do ângulo 1



$y =$  “abertura”  
do ângulo 2

Problema: Dado  $x$ , é possível com régua e compasso obter  $y$  tal que  $\text{ângulo } 1 = 3 \cdot \text{ângulo } 2$ ? NÃO

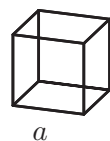
2<sup>a</sup>) Duplicação do Cubo:

Problema: Dado  $a$  (aresta do cubo 1), é possível com régua e compasso obter  $b$  (aresta do cubo 2) tal que  $V_2 = 2 \cdot V_1$ ? NÃO

3<sup>a</sup>) Quadratura do Círculo:

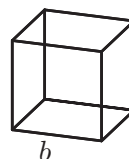
Problema: Dado  $r$ , é possível com régua e compasso obter  $l$  tal que  $A_{\square} = A_{\circ}$ ? NÃO





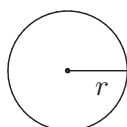
$$V_1 = a^3$$

(dado)



$$V_2 = b^3 = 2a^3$$

(a obter)



(dado)



(a obter)

- Início da Era Cristã: Os árabes hindus aperfeiçoaram os métodos antigos e obtiveram uma fórmula para obter as raízes de  $f(x) = ax^2 + bx + c$  ( $a \neq 0$ )

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

(Fórmula de Bháskara) ( $K = \mathbb{C}$ )

- Séc. XV/XVI: quatro matemáticos italianos (Scipione Del Ferro, Tartaglia, Cardano, Ludovico Ferrari) se interessaram pela resolução de  $ax^3 + bx^2 + cx + d = 0$  ( $a \neq 0$ )

$$ax^3 + bx^2 + cx + d = 0 \xleftrightarrow{\text{mud. var.}} x^3 + px + q = 0$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

(Fórmula de Cardano)

- Séc. XVII: Existe uma fórmula (semelhante à de Bháskara e à de Cardano) para resolver

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \quad (a \neq 0)$$

- 1824: Abel provou que se  $n = 5$ , então não existe fórmula para resolver

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0 \quad (a \neq 0)$$

- 1832: Évariste Galois (1811 - 1832) determinou condições necessárias e suficientes para que uma equação polinomial  $f(x) = 0$  (onde  $\text{gr}(f) \geq 5$ ) tenha solução por meio de radicais (Teoria de Galois).

**Teorema 6.5 (Teorema do Resto).** *Sejam  $K$  um corpo e  $f(x) \in K[x]$ . Considere  $g(x) = x - \alpha$ , onde  $\alpha \in K$ . Então o resto da divisão de  $f(x)$  por  $g(x)$  é  $f(\alpha)$ .*

**Corolário 6.6 (Teorema de D’Alembert).** *Nas condições anteriores,  $\alpha$  é raiz de  $f(x) \Leftrightarrow g(x) \mid f(x)$ .*

**Observação.** Tais resultados constituem a base do Algoritmo de Briott-Ruffini para dividir  $f(x)$  por  $g(x)$ .

**Demonstração.** (Teorema 6.5)

Como  $g(x) = x - \alpha \neq 0$ , então podemos dividir  $f(x)$  por  $g(x)$  usando o Algoritmo de Euclides:

$$f(x) = (x - \alpha)q(x) + r(x),$$

onde  $r(x) = 0$  ou  $\text{gr}(r) < \text{gr}(g) = 1$  (isto é, em qualquer caso,  $r(x) = c \in K$  (constante)). Assim,  $f(x) = (x - \alpha)q(x) + c$ . Substituindo  $x$  por  $\alpha$ , temos

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + c \Rightarrow r(x) = c = f(\alpha) \quad \blacksquare$$

**Demonstração.** (Corolário 6.6)

$\alpha$  é raiz de

$$\begin{aligned} f(x) &\Leftrightarrow f(\alpha) = 0 \\ &\stackrel{\text{Teo}}{\Leftrightarrow} r(x) = 0 \Leftrightarrow f(x) = (x - \alpha)q(x) \\ &\Leftrightarrow (g(x) =) x - \alpha \mid f(x) \end{aligned} \quad \blacksquare$$

**Exemplo:**  $K = \mathbb{R}$

$$f(x) = x^2 - 5x + 6$$

$$f(2) = 2^2 - 5 \cdot 2 + 6 = 0 \Rightarrow 2 \text{ é raiz de } f \Rightarrow x - 2 \mid f(x)$$

$$f(3) = 3^2 - 5 \cdot 3 + 6 = 0 \Rightarrow 3 \text{ é raiz de } f \Rightarrow x - 3 \mid f(x)$$

**Teorema 6.7 (Contagem do Número de Raízes de Um Polinômio Sobre Um Corpo).** *Sejam  $K$  um corpo e  $f(x) \in K[x] - \{0\}$ . Sejam  $n = \text{gr}(f)$  e  $N$  o número de raízes de  $f$  em  $K$ . Então,  $N \leq n$ , isto é, o número de raízes de  $f$  em  $K$  (na verdade, em qualquer corpo  $L$ , tal que  $L \supseteq K$ ) é no máximo o grau do polinômio.*

### Demonstração.

1<sup>a</sup> caso: Se  $f(x)$  não possui raiz, então não há nada a demonstrar.  
 $\{N = 0 \leq n = \text{gr}(f)\}$

2<sup>a</sup> caso: Seja  $\alpha$  raiz de  $f(x)$  em  $K$ . Neste caso, pelo Teorema de D'Allembert,

$$f(x) = (x - \alpha)q(x) \quad (*)$$

onde  $\text{gr}(q) = n - 1$ . A idéia é usar indução sobre  $n$ , supondo que o resultado que queremos mostrar seja válido para polinômios de grau  $< n$ .

i)  $n = 0$ . Neste caso,  $f(x) = c \neq 0$  (constante). Assim,  $N = 0 = n$ .

(Podemos supor agora que  $f$  tem raiz)

ii) Se vale para grau  $< n$ , então vale para  $n$ . Seja  $\beta \in K$  uma outra raiz de  $f(x)$  em  $K$ . Substituindo  $\beta$  em  $(*)$ , temos

$$f(\beta) = \underbrace{(\beta - \alpha)}_{\in K} \underbrace{q(\beta)}_{\in K} = 0 \xRightarrow{\text{corpo}} \beta - \alpha = 0 \quad \text{ou} \quad q(\beta) = 0$$

$$\Rightarrow \beta = \alpha \quad \text{ou} \quad \beta \text{ é raiz de } q(x)$$

Como  $\text{gr}(q) = n - 1 < n = \text{gr}(f)$ , segue da hipótese de indução que  $q(x)$  tem no máximo  $n - 1$  raízes em  $K$ . Logo,  $f(x)$  tem no máximo  $n$  raízes em  $K$ . ■

**Observação.** É essencial que  $K$  seja um corpo para que tal teorema valha.

**Exemplo:**  $f(x) = \overline{1}x^2 + \overline{1}x \in \mathbb{Z}_6[x]$ , onde  $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ . Como  $6 \notin \mathbb{P}$ , então  $\mathbb{Z}_6$  não é corpo.

$$n = \text{gr}(f) = 2$$

$$N = ?$$

$$x = \overline{0} : f(\overline{0}) = \overline{0} \Rightarrow \overline{0} \text{ é raiz}$$

$$x = \overline{1} : f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{2} \neq \overline{0}$$

$$x = \overline{2} : f(\overline{2}) = \overline{2}^2 + \overline{2} = \overline{6} = \overline{0} \Rightarrow \overline{2} \text{ é raiz}$$

$$x = \overline{3} : f(\overline{3}) = \overline{3}^2 + \overline{3} = \overline{12} = \overline{0} \Rightarrow \overline{3} \text{ é raiz}$$

$$x = \overline{4} : f(\overline{4}) = \overline{4}^2 + \overline{4} = \overline{20} = \overline{2} \neq \overline{0}$$

$$x = \overline{5} : f(\overline{5}) = \overline{5}^2 + \overline{5} = \overline{30} = \overline{0} \Rightarrow \overline{5} \text{ é raiz}$$

Logo,  $N = 4 > n = 2$

Pergunta: Tal exemplo contraria o Teorema?

Não, pois  $\mathbb{Z}_6$  não é corpo.

**Exercícios Selecionados:** (lista 4)

- 7) Seja  $K$  um corpo (isto é,  $K = \mathbb{Q}$  ou  $\mathbb{R}$  ou  $\mathbb{C}$  ou  $\mathbb{Z}_p$ ,  $p \in \mathbb{P}$ ). Dize-mos que  $K$  é algebricamente fechado se todo polinômio, não-constante, com coeficientes em  $K$ , admite pelo menos uma raiz em  $K$  (isto é,  $\forall f(x) \in K[x]$ ,  $\text{gr}(f) \geq 1$ ,  $\exists \alpha \in K \mid f(\alpha) = 0$ ). Mostre que  $K = \mathbb{R}$  não é algebricamente fechado.

**Exemplo:**  $f(x) = x^2 + 1 \in \mathbb{R}[x]$ ,  $\text{gr}(f) = 2$

$\nexists \alpha \in \mathbb{R} \mid f(\alpha) = 0$ , pois  $\alpha^2 + 1 = 0 \Rightarrow \alpha^2 = -1$  (absurdo)

**Observação.**  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$  é algebricamente fechado. Este resultado é chamado de Teorema Fundamental da Álgebra, demonstrado pela primeira vez por Karl Friedrich Gauss (1777 - 1855) em sua Tese de Doutorado em 1796 (aos 19 anos).

- 10) a) Mostre que o polinômio  $f(x) = x^2$  possui infinitas raízes no anel  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$ .
- b) Comente o fato do polinômio  $f$  acima ter um número de raízes maior que o grau.
- a)  $f(X) = 1 X^2 \in \mathcal{M}_{2 \times 2}(\mathbb{R})[X]$   
 $f(X) = I_2 X^2$ , onde

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in A, \text{ onde } c \in \mathbb{R}$$

$$f(\alpha) = \alpha^2 = \alpha \cdot \alpha = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$\Rightarrow \alpha$  é raiz de  $f(X)$  em  $A$ .

Como  $c \in \mathbb{R}$  (arbitrário), então há infinitas escolhas para  $\alpha$ , isto é,  $f$  tem infinitas raízes em  $A$ .

- b) Como  $A$  não é DI, então  $A$  não é corpo. Logo, o Teorema a respeito do número de raízes não é contrariado.

- 20) a) Sejam  $A = \mathbb{Z}_2\{\bar{0}, \bar{1}\}$  e  $f(x) = \bar{1} + x + x^3 \in \mathbb{Z}_2[x]$ . Determine  $g(x) \in \mathbb{Z}_2[x]$ ,  $g(x) \neq f(x)$ , tal que  $\hat{g} = \hat{f}$ .
- b) Sejam  $A = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ ,  $f(x) = x$ ,  $g(x) = x^3$ ,  $h(x) = x + 5x^3 + x^9 \in \mathbb{Z}_3[x]$ . Mostre que  $\hat{f} = \hat{g} = \hat{h}$ .

Lembre-se: (Polinômios *vs* Função Polinomial)

- Polinômio sobre um anel  $A$ :

$$\begin{cases} f(x) = a_n x^n + \dots + a_1 x + a_0 \in A[x] \\ a_i \text{'s} \in A \\ x = \text{indeterminada} \end{cases}$$

- Função polinomial (induzida por  $f$ )

$$\begin{aligned} \hat{f} : A &\rightarrow A \\ u &\mapsto \hat{f}(u) := f(u) = a_n u^n + \dots + a_1 u + a_0 \in A \end{aligned}$$

- 20) a)  $f(x) = \bar{1} + x + x^3 \in \mathbb{Z}_2[x]$

$$\begin{aligned} \hat{f} : \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \\ u &\mapsto \hat{f}(u) = f(u) = \bar{1} + u + u^3 \end{aligned}$$

$$u = \bar{0} : \hat{f}(\bar{0}) = f(\bar{0}) = \bar{1} + \bar{0} + \bar{0}^3 = \bar{1}$$

$$u = \bar{1} : \hat{f}(\bar{1}) = f(\bar{1}) = \bar{1} + \bar{1} + \bar{1}^3 = \bar{3} = \bar{1}$$

Assim,  $\hat{f}$  é a função constante 1, pois  $\forall u \in \mathbb{Z}_2$ ,  $\hat{f}(u) = \bar{1}$ . É natural definir  $g(x) = \bar{1}$  (polinômio constante 1). Neste caso,

$$\begin{aligned} \hat{g} : \mathbb{Z}_2 &\rightarrow \mathbb{Z}_2 \\ u &\mapsto \hat{g}(u) = g(u) = \bar{1} \end{aligned}$$

Logo,  $\forall u \in \mathbb{Z}_2$ ,  $\hat{g}(u) = g(u) = \bar{1} = \hat{f}(u)$ .

Conclusão:  $f(x) \neq g(x)$  (polinômios diferentes), mas  $\hat{f} = \hat{g}$  (funções polinomiais iguais).

- b) **Demonstração.** Observe que  $f \neq g \neq h$ . Queremos mostrar que as funções polinomiais induzidas são iguais, isto é,  $\hat{f} = \hat{g} = \hat{h}$ .

$$\begin{aligned} \hat{f} : \mathbb{Z}_3 &\rightarrow \mathbb{Z}_3 \\ u &\mapsto \hat{f}(u) = f(u) = \bar{1}u \end{aligned}$$

$$\begin{aligned} \hat{g} : \mathbb{Z}_3 &\rightarrow \mathbb{Z}_3 \\ u &\mapsto \hat{g}(u) = g(u) = \bar{1}u^3 \end{aligned}$$

$$\begin{aligned}
\hat{h} : \mathbb{Z}_3 &\rightarrow \mathbb{Z}_3 \\
u &\mapsto \hat{h}(u) = h(u) = \overline{1}u + \overline{5}u^3 + \overline{1}u^9 \\
u = \overline{0}: \\
\hat{f}(\overline{0}) &= f(\overline{0}) = \overline{0} \\
\hat{g}(\overline{0}) &= g(\overline{0}) = \overline{0}^3 = \overline{0} \\
\hat{h}(\overline{0}) &= h(\overline{0}) = \overline{0} + \overline{5} \overline{0}^3 + \overline{0}^9 = \overline{0} \\
u = \overline{1}: \\
\hat{f}(\overline{1}) &= f(\overline{1}) = \overline{1} \\
\hat{g}(\overline{1}) &= g(\overline{1}) = \overline{1}^3 = \overline{1} \\
\hat{h}(\overline{1}) &= h(\overline{1}) = \overline{1} + \overline{5} \overline{1}^3 + \overline{1}^9 = \overline{7} = \overline{1} \\
u = \overline{2}: \\
\hat{f}(\overline{2}) &= f(\overline{2}) = \overline{2} \\
\hat{g}(\overline{2}) &= g(\overline{2}) = \overline{2}^3 = \overline{8} = \overline{2} \\
\hat{h}(\overline{2}) &= h(\overline{2}) = \overline{2} + \overline{5} \overline{2}^3 + \overline{2}^9 = \overline{2} + \overline{40} + \overline{512} = \overline{554} = \overline{2} \quad \blacksquare
\end{aligned}$$

- 3) Seja  $A$  um domínio de integridade. Determine  $\mathcal{U}(A[x]) = \{f(x) \in A[x] \mid f(x) \text{ é inversível para a multiplicação}\}$ .

Fatos:

•  $A$  - DI  $\Rightarrow A[x]$  = anel de polinômios na indeterminada  $x$  com coeficientes em  $A$  - DI. Em particular,  $\text{gr}(f(x) \cdot g(x)) = \text{gr}(f(x)) + \text{gr}(g(x))$ .

$f(x) \in A[x]$  (Observe que  $f \neq 0$  e  $g \neq 0$ )

$f(x) \in \mathcal{U}(A[x]) \Leftrightarrow \exists g(x) \in A[x] \mid f(x) \cdot g(x) = 1$

Tomando o grau em ambos os lados, temos:

$$f \cdot g = 1$$

$$\text{gr}(f \cdot g) = \text{gr}(1)$$

$$\begin{array}{ccc}
& \text{gr}(f) = 0 & f = a_0 \in A^* = A - \{0\} \\
\text{gr}(f) + \text{gr}(g) = 0 \Leftrightarrow & \text{e} & \Leftrightarrow \text{e} \\
& \text{gr}(g) = 0 & g = b_0 \in A^* = A - \{0\}
\end{array}$$

Assim,  $a_0 \cdot b_0 = 1$ , isto é,  $f \in \mathcal{U}(A)$ . Assim,  $\mathcal{U}(A[x]) = \mathcal{U}(A)$ .

**Exemplos:** i)  $\mathcal{U}(\mathbb{Z}[x]) = \mathcal{U}(\mathbb{Z}) = \{\pm 1\}$

ii)  $\mathcal{U}^*(\mathbb{R}[x]) = \mathcal{U}(\mathbb{R}) = \mathbb{R}^* = \mathbb{R} - \{0\}$

### Comentários Finais Sobre Polinômios

1) É possível definir polinômios via seqüências infinitas. Seja  $A$  um anel comutativo com identidade.

- (seqüência de elementos de  $A$ )

$$\begin{aligned} f: \mathbb{Z}_+ &\rightarrow A \\ n &\mapsto f(n) = a_n \end{aligned}$$

Identificamos

$$f = (a_n)_{n \in \mathbb{Z}_+} = (a_0, a_1, a_2, \dots, a_n, \dots)$$

- $f$  é dita seqüência quase nula em  $A$  se  $\exists N \in \mathbb{Z}_+ \mid a_j = 0, j > N$ .

**Exemplos:**  $0 = (0, 0, 0, \dots, 0, \dots)$  (seqüência nula) ( $N = 0$ )

$1 = (1, 0, 0, \dots, 0, \dots)$  ( $N = 1$ )

$f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$  (seqüência nula) ( $N = n + 1$ )

- Operações com seqüências quase nulas em  $A$ :

$$f = (a_0, a_1, \dots, a_n, 0, \dots, 0, \dots)$$

$$g = (b_0, b_1, \dots, b_m, 0, \dots, 0, \dots)$$

$$- \text{igualdade: } f = g \Leftrightarrow a_i = b_i, \forall i$$

$$- \text{adição: } f + g = (c_0, c_1, c_2, c_3, \dots, 0, \dots, 0, \dots), \text{ onde } c_i = a_i + b_i, \forall i$$

$$- \text{multiplicação: } f \cdot g = (d_0, d_1, d_2, \dots, 0, 0, \dots), \text{ onde}$$

$$d_0 = a_0 b_0$$

$$d_1 = a_0 b_1 + a_1 b_0$$

$$d_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

- Identificação:

$$- a \in A \text{ (constante)}$$

$$a = (a, 0, 0, 0, \dots)$$

$$- x \text{ (indeterminada)}$$

$$x = (0, 1, 0, 0, \dots)$$

$$a \cdot x = (a, 0, 0, \dots) \cdot (0, 1, 0, \dots) = (0, a, 0, \dots, 0, \dots)$$

$$x^2 = x \cdot x = (0, 1, 0, \dots) \cdot (0, 1, 0, \dots) = (0, 0, 1, 0, \dots)$$

$$\vdots$$

(indução)

$$x^n = (\underbrace{0, 0, \dots, 0}_{n \text{ posições de } 0\text{'s}}, 1, 0, \dots)$$

$n$  posições de 0's

Assim, para uma seqüência  $f = (a_0, a_1, a_2, \dots, a_n, 0, \dots)$  genérica, temos:

$$f = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, a_2, \dots) + (0, 0, 0, a_3, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

2) Se  $K$  é um corpo, então  $K[x]$  possui propriedades similares a  $\mathbb{Z}$ :  
Semelhanças:

- A) Algoritmo de Euclides: Dados  $f(x), g(x) \in K[x]$ , com  $g(x) \neq 0$ , existem únicos  $q(x), r(x) \in K[x]$  tal que  $f(x) = g(x) \cdot q(x) + r(x)$  onde  $r(x) = 0$  ou  $\text{gr}(r) < \text{gr}(g)$ .
- B) Polinômios Irredutíveis: (análogo dos números primos)  
 $f(x) \in K[x]$  é irredutível se:
- i)  $\text{gr}(f) \geq 1$ ;
  - ii) Se  $f(x) = g(x) \cdot h(x)$  com  $g(x), h(x) \in K[x]$ , então  $g(x) = \text{cte}$  ( $\text{gr}(g) = 0$ ) ou  $h(x) = \text{cte}$  ( $\text{gr}(h) = 0$ )

**Exemplos:**

- a)  $f(x) = x^2 - 5x + 6 \in \mathbb{R}[x]$  é redutível em  $\mathbb{R}$ , pois:  
 $f(x) = (x - 2)(x - 3)$  ( $\text{gr}(g) = 1 = \text{gr}(h)$ )
- b)  $f(x) = x^2 + 1 \in \mathbb{R}[x]$   
 $f$  é irredutível sobre  $\mathbb{R}$ , mas  $f$  é redutível sobre  $\mathbb{C}$ , pois  
 $f(x) = (x + i)(x - i)$
- c)  $f(x) = x^2 - 2 \in \mathbb{R}[x]$   
 $f$  é irredutível sobre  $\mathbb{Q}$ , mas  $f$  é redutível sobre  $\mathbb{R}$ , pois  
 $f(x) = (x - \sqrt{2})(x + \sqrt{2})$
- C) Métodos das divisões sucessivas para o cálculo do MDC:  
 $f(x), g(x) \in K[x]$  (não simultaneamente nulos)  
 $d = \text{mdc}(f(x), g(x)) = \text{último polinômio não-nulo (na divisão de } f \text{ por } g)$
- D) Fatoração única para polinômios (análogo ao Teorema Fundamental da Álgebra)  
 Todo polinômio  $f(x) \in K[x]$ , de  $\text{gr}(f) \geq 1$ , pode ser escrito, de forma única, como produto de polinômios irredutíveis (a menos de constantes).

**Exemplo:**  $f(x) = 3x^3 - 3x \in \mathbb{R}[x]$   
 $f(x) = 3x^2 - 3x = 3x(x^2 - 1) = 3x(x + 1)(x - 1)$

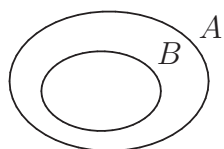


## 7 Tópicos Especiais Sobre Anéis e Grupos

**Observação.** Tais tópicos serão estudados com mais detalhe nos cursos de Álgebra 2 e 3).

Motivação: Comportamento de subconjunto de um anel e de um grupo com relação às operações do conjunto. Vamos introduzir a noção de subestrutura algébrica.

### Subestrutura Algébrica



$A$  - estrutura algébrica com uma (semigrupo, monóide, *grupo*) ou duas (*anel*, domínio de integridade, corpo) operações;

$$B \subseteq A$$

Dizemos que  $B$  é uma subestrutura algébrica de  $A$  se  $B$  satisfaz as seguintes condições:

- a)  $B \neq \emptyset$ ;
- b)  $B$  é *fechado* com relação à(s) operação(ões) de  $A$ ;
- c)  $B$ , com relação à(s) operação(ões) de  $A$ , é também uma estrutura algébrica do mesmo tipo de  $A$ .

### Exemplos:

- a)  $A = \mathbb{C}$  (corpo);  $B_1 = \mathbb{Q}$  (corpo);  $B_2 = \mathbb{R}$  (corpo)

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

$B_1$  é subcorpo de  $B_2$

$B_1$  é subcorpo de  $A$

$B_2$  é subcorpo de  $A$

- b)  $A = P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$$* = \cup$$

$(A, *)$  - monóide

$$B = \{\emptyset, \{a, b\}\} \subseteq A$$

$\cup$	$\emptyset$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

$e = \emptyset$

Assim,  $B$  é um submonóide de  $A$ .

A partir de agora, vamos nos restringir ao estudo de anéis e grupos.

### I) Anéis

**Definição 7.1 (Subanel).** *Seja  $(A, +, \cdot)$  um anel. Seja  $B \subseteq A$ .  $B$  é dito um subanel de  $A$  se:*

- a)  $B \neq \emptyset$ ;
- b)  $\forall x, y \in B, x + y \in B \text{ e } x \cdot y \in B$ ;
- c)  $B$  é um anel com relação às operações de  $A$ .

**Teorema 7.2 (Critério para Determinar Subanéis).** *Seja  $A$  um anel.  $B \subseteq A$  é um subanel de  $A$  se, e somente se, valem as seguintes condições:*

- i)  $0 \in B$ ; (elemento neutro para  $+$  em  $A$ )
  - ii)  $\forall x, y \in B, x - y \in B$ ; ( $B$  é fechado para  $-$ )
  - iii)  $\forall x, y \in B, x \cdot y \in B$ . ( $B$  é fechado para  $\cdot$ )
- (Isto é, a), b) e c) são equivalentes a i), ii), iii))

#### Demonstração.

$$(\Rightarrow) \begin{cases} \text{H: a), b), c)} \\ \text{T: i), ii), iii)} \end{cases}$$

Não há nada a demonstrar neste caso.

$$(\Leftarrow) \begin{cases} \text{H: i), ii), iii)} \\ \text{T: a), b), c)} \end{cases}$$

- Por i),  $0 \in B$ . Logo,  $B \neq \emptyset$  (isto é, vale a)).
- Vamos mostrar que se  $x, y \in B$ , então  $x + y \in B$ . (primeira parte de b)).

De fato:

Seja  $y \in B$ . Por i),  $0 \in B$ . Assim, segue de ii),  $0 - y = -y \in B$  (isto é, se  $y \in B$ , então  $-y \in B$ ).

Considere agora  $x \in B$  e  $-y \in B$ . Por ii), segue que  $x - (-y) \in B$ .

- A segunda parte de b) (fechamento para  $\cdot$ ) é equivalente a iii) (logo, não há nada a demonstrar).

• Como  $A$  é anel e  $B \subseteq A$ , então  $B$  “herda” as propriedades associativa, comutativa e distributiva de  $A$ . Então,  $B$  é subanel de  $A$ . ■

**Exercícios:** Verifique em cada caso que  $B$  é subanel de  $A$ :

a)  $A = \mathbb{Z}$

$$B = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \quad (n \in \mathbb{N})$$

b)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

$$B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

c)  $A = \mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$

$$B = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \text{ (anel dos inteiros gaussianos)}$$

d)  $A = \mathbb{R}$

$$B = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

e) (Cálculo 1)

$$A = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é função}\}$$

$$B = \mathcal{P}(\mathbb{R}, \mathbb{R}) = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p \text{ é função polinomial}\}$$

$$C = \mathcal{C}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é contínua}\}$$

$$D = \mathcal{D}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ é derivável}\}$$

$$B \subseteq D \subseteq C \subseteq A$$

**Resolução:**

a) i)  $0 \in B$ , pois  $0 = n \cdot 0$

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

$$x = nk_1, \quad k_1 \in \mathbb{Z} \quad \text{e} \quad y = nk_2, \quad k_2 \in \mathbb{Z}$$

$$x - y = nk_1 - nk_2 = n \underbrace{(k_1 - k_2)}_{= k_3} \in B$$

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

$$x \cdot y = (nk_1)(nk_2) = n \underbrace{(k_1 nk_2)}_{= k_3} \in B$$

b) i)  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \in B$ , pois basta tomar  $a = 0$

$$\text{ii)} \quad X = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in B \quad \text{e} \quad Y = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in B$$

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

$$\text{iii)} \quad X \cdot Y = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in B$$

$$\text{c)} \quad \text{i)} \quad 0 \in B, \text{ pois } 0 + 0i \in B$$

$$\text{ii)} \quad x = a + bi \in B \quad \text{e} \quad y = c + di \in B$$

$$x - y = (a + bi) - (c + di) = \underbrace{(a - c)}_{\in \mathbb{Z}} + \underbrace{(b - d)}_{\in \mathbb{Z}} i \in B$$

$$\text{iii)} \quad x \cdot y = (a + bi)(c + di) = \underbrace{(ac - bd)}_{\in \mathbb{Z}} + \underbrace{(ad + bc)}_{\in \mathbb{Z}} i \in B$$

$$\text{d)} \quad \text{i)} \quad 0 \in B, \text{ pois } 0 + 0\sqrt{2} \in B$$

$$\text{ii)} \quad x = a + b\sqrt{2} \in B \quad \text{e} \quad y = c + d\sqrt{2} \in B$$

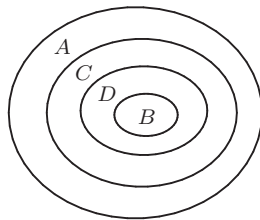
$$x - y = (a + b\sqrt{2}) - (c + d\sqrt{2}) = \underbrace{(a - c)}_{\in \mathbb{Z}} + \underbrace{(b - d)}_{\in \mathbb{Z}} \sqrt{2} \in B$$

$$\text{iii)} \quad x \cdot y = (a + b\sqrt{2})(c + d\sqrt{2}) = \underbrace{(ac + 2bd)}_{\in \mathbb{Z}} + \underbrace{(ad + bc)}_{\in \mathbb{Z}} \sqrt{2} \in B$$

$$\text{e)} \quad \text{i)} \quad 0 \in B \quad (\text{função constante})$$

ii) A diferença entre funções polinomiais (respectivamente, contínuas, deriváveis) também é polinomial (respectivamente, contínua, derivável)

iii) O produto de duas funções polinomiais (respectivamente, contínuas, deriváveis) é também polinomial (respectivamente, contínua, derivável)



**Exemplos:**  $h(x) = \begin{cases} 1, & \text{se } x > 0 \\ 0, & \text{se } x = 0 \\ -1, & \text{se } x < 0 \end{cases} \in A$

$g(x) = |x| \in C$

$f(x) = \text{sen } x \in D$

### Exercícios:

- 1) Mostre que se  $B_1$  e  $B_2$  são subanéis de  $A$ , então  $B_1 \cap B_2$  também o é.
- 2) Vimos que se  $A$  é um anel e  $B \subseteq A$  é um subanel, então  $B$  “herda” as propriedades de  $A$ . Porém, se  $A$  é anel com identidade  $1 \neq 0$ , então  $B$  não necessariamente possui a mesma identidade.
  - a) Verifique que  $A = \mathbb{Z}$  e  $B = 2\mathbb{Z}$  satisfazem a observação acima.
  - b) Considere  $A = \mathcal{M}_{2 \times 2}(\mathbb{R})$  e  $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ .

Verifique que  $B$  possui identidade  $1'$ , mas  $1' \neq 1$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A \quad \text{e} \quad 1' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in B$$

**Resolução:**

- 1) H:  $B_1$  e  $B_2$  são subanéis de  $A$   
T:  $B_1 \cap B_2$  é subanel de  $A$
- i)  $0 \in B_1 \cap B_2$ , pois  $0 \in B_1$  e  $0 \in B_2$  (por hipótese)
- ii) 
$$\left\{ \begin{array}{l} x \in B_1 \cap B_2 \Rightarrow x \in B_1 \text{ e } x \in B_2 \\ y \in B_1 \cap B_2 \Rightarrow y \in B_1 \text{ e } y \in B_2 \\ \Rightarrow x - y \in B_1 \cap B_2 \end{array} \right. \Rightarrow \begin{array}{l} x - y \in B_1 \\ x - y \in B_2 \end{array}$$
- iii)  $x \cdot y \in B_1$  e  $x \cdot y \in B_2 \Rightarrow x \cdot y \in B_1 \cap B_2$
- 2) a)  $A = \mathbb{Z}$  e  $B = 2\mathbb{Z}$   
 $(A, +, \cdot)$  é um anel comutativo com identidade  $1 \neq 0$   
 $B$  é subanel de  $A$ , mas  $1 \notin B$ , pois  $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$

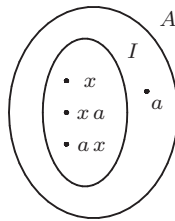
$$\begin{aligned}
\text{b) } A &= \mathcal{M}_{2 \times 2}(\mathbb{R}) \text{ e } B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\} \\
1_A &= I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} &\in A \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} &\in B; \quad 1_B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in B \\
\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \\
&\Leftrightarrow ab = a \Leftrightarrow b = 1 \\
&\Rightarrow 1_B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_A
\end{aligned}$$

**Definição 7.3 (Ideal de um Anel).** *Seja  $A$  um anel. Seja  $I \subseteq A$ . Dizemos que  $I$  é um ideal de  $A$  se:*

i)  $I$  é subanel de  $A$ , ou seja

$$\begin{cases} 0 \in I; \\ x - y \in I \text{ } (x, y \in I); \\ x \cdot y \in I \text{ } (x, y \in I) \end{cases}$$

ii)  $\forall a \in A, \forall x \in I$ , então  $a \cdot x \in I$  e  $x \cdot a \in I$



**Observação.** Se  $A$  é comutativo, então  $a \cdot x = x \cdot a$ . Neste caso, a condição ii) transforma-se em:

ii')  $\forall a \in A, \forall x \in I, a \cdot x = x \cdot a \in I$

A partir de agora,  $A$  será sempre um anel comutativo (exceto em alguns exemplos particulares)

**Exemplos:**

a)  $A = \mathbb{Z}$

$$I = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \text{ (múltiplos de } n \in \mathbb{N})$$

$I$  é ideal de  $A$ , pois

i)  $I$  é subanel de  $A$  (veja página 152)

ii) Tome  $a \in \mathbb{Z}$  e  $x \in I$ . Então,

$$ax = xa = a(nk) = n \underbrace{(ak)}_{l \in \mathbb{Z}} \in I$$

b)  $A = \mathcal{M}_{2 \times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

$$I = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \mid \alpha, \beta, \gamma \in \mathbb{R} \right\} \subseteq A$$

$I$  é subanel de  $A$ , mas não é ideal de  $A$ , pois:

$$(I) \ 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$$

$$(II) \ X = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \in I \text{ e } Y = \begin{pmatrix} \lambda & \epsilon \\ 0 & \phi \end{pmatrix} \in I$$

$$\Rightarrow X - Y = \begin{pmatrix} \alpha - \lambda & \beta - \epsilon \\ 0 & \gamma - \phi \end{pmatrix} \in I$$

$$(III) \ X \cdot Y = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} \lambda & \epsilon \\ 0 & \phi \end{pmatrix} = \begin{pmatrix} \alpha\lambda & \alpha\epsilon + \beta\phi \\ 0 & \gamma\phi \end{pmatrix} \in I$$

De (I), (II) e (III), segue que  $I$  é subanel de  $A$ .

$$(IV) \text{ Tome } X = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \text{ e } a = \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix} \in A$$

$$\text{Então, } xa = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix} = \begin{pmatrix} 16 & 19 \\ 18 & 21 \end{pmatrix} \notin I$$

Logo,  $I$  não é ideal de  $A$ .

c)  $A = \mathbb{R}$ ,  $I = \mathbb{Q} \subseteq A$

$I$  é subanel de  $A$ , mas não é ideal de  $A$  (por exemplo: tome  $x = 1/2 \in I$  e  $a = \pi \in A$ . Então,  $xa \notin I$ ).

d)  $A$  - anel comutativo (genérico)

A)  $\{0\}$  e  $A$  são Ideais Triviais de  $A$ .

(Se  $I$  é ideal de  $A$  não-trivial, então  $I$  é dito ideal próprio de  $A$ )

$$\{0\} \subsetneq I \subsetneq A$$

B)  $x_1, x_2, \dots, x_n \in A$  (fixos)

$I = \{a_1x_1 + a_2x_2 + \dots + a_nx_n \mid a_i \text{'s} \in A, 1 \leq i \leq n\}$  é um ideal de  $A$  chamado de ideal gerado por  $x_1, \dots, x_n$

**Notação.**  $I = (x_1, x_2, \dots, x_n)$  ou  $\langle x_1, x_2, \dots, x_n \rangle$

De fato:

•  $0 \in I$ , pois  $0 = 0x_1 + 0x_2 + \dots + 0x_n$

•  $\begin{cases} \alpha = a_1x_1 + \dots + a_nx_n \in I \\ \beta = b_1x_1 + \dots + b_nx_n \in I \end{cases}$

$\alpha - \beta = (a_1 - b_1)x_1 + \dots + (a_n - b_n)x_n \in I$

•  $\alpha \cdot \beta \in I$  (exercício)

$$\begin{aligned} \alpha \cdot \beta &= (a_1x_1 + \dots + a_nx_n)(b_1x_1 + \dots + b_nx_n) = (a_1x_1 + \dots + a_nx_n)b_1x_1 + (a_1x_1 + \dots + a_nx_n)b_2x_2 + \dots + (a_1x_1 + \dots + a_nx_n)b_nx_n = \\ &= \underbrace{(a_1b_1x_1 + \dots + a_nb_1x_n)}_{\in A} x_1 + \underbrace{(a_1b_2x_1 + \dots + a_nb_2x_n)}_{\in A} x_2 + \dots + \\ &= \underbrace{(a_1b_nx_1 + \dots + a_nb_nx_n)}_{\in A} x_n \in I \end{aligned}$$

Tome  $\alpha \in I$  e  $y \in A$ . Então,  $\alpha \cdot y = y \cdot \alpha = y(a_1x_1 + \dots + a_nx_n) = \underbrace{(ya_1)}_{\in A} x_1 + \dots + \underbrace{(ya_n)}_{\in A} x_n \in I$ .

Caso particular: (um gerador apenas)

Neste caso,  $I = (x_1) = \{ax_1 \mid a \in A\}$  (ideal principal gerado por  $x_1$ )

C) (Operações com Ideais)

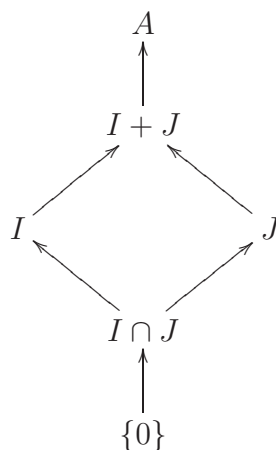
$I, J$  - ideais de  $A$

$I \cap J \stackrel{\text{def}}{=} \{x \in A \mid x \in I \text{ e } x \in J\}$  (intersecção de ideais)

$I + J \stackrel{\text{def}}{=} \{x + y \mid x \in I \text{ e } y \in J\}$  (adição de ideais)



**Afirmação.**  $I \cap J$  e  $I + J$  são ideais de  $A$



De fato:

Vamos verificar que  $I \cap J$  é ideal de  $A$  (o outro caso fica como exercício)

•  $0 \in I \cap J$ , pois  $0 \in I$  e  $0 \in J$

•  $x, y \in I \cap J \Rightarrow x - y \in I \cap J$

$$\begin{cases} x \in I \cap J \Rightarrow x \in I \text{ e } x \in J \\ y \in I \cap J \Rightarrow y \in I \text{ e } y \in J \end{cases} \Rightarrow x - y \in I \text{ e } x - y \in J$$

$\Rightarrow x - y \in I \cap J$

•  $x, y \in I \cap J \Rightarrow x \cdot y \in I \cap J$

$$\begin{cases} x \in I \cap J \Rightarrow x \in I \text{ e } x \in J \\ y \in I \cap J \Rightarrow y \in I \text{ e } y \in J \end{cases} \Rightarrow x \cdot y \in I \text{ e } x \cdot y \in J$$

$\Rightarrow x \cdot y \in I \cap J$

•  $x \in I \cap J : a \in A \Rightarrow xa = ax \in I \cap J$

$x \in I \cap J \Rightarrow x \in I \text{ e } x \in J$

$a \in A$

Como  $I$  é ideal, então  $ax \in I$ . Como  $J$  é ideal, então,  $ax \in J$ . Segue que  $ax \in I \cap J$ .

$I + J$  é ideal de  $A$

•  $0 \in I + J$ , pois  $0 = \underbrace{0}_{\in I} + \underbrace{0}_{\in J} \in I + J$

•  $a, b \in I + J \Rightarrow a = x_1 + y_1$  e  $b = x_2 + y_2$

$$\begin{aligned}
a - b &= (x_1 + y_1) - (x_2 + y_2) = \underbrace{(x_1 - x_2)}_{= x_3 \in I} + \underbrace{(y_1 - y_2)}_{= y_3 \in J} \in I + J \\
\bullet \quad a \cdot b &= (x_1 + y_1) \cdot (x_2 + y_2) = \underbrace{x_1 x_2}_{\in I} + \underbrace{x_1 y_2}_{\in I \cap J} + \underbrace{x_2 y_1}_{\in I \cap J} + \underbrace{y_1 y_2}_{\in J} = \\
& x_3 + y_3 \in I + J \\
\bullet \quad c \in A \text{ e } (x + y) &\in I + J \\
c(x + y) &= \underbrace{cx}_{\in I} + \underbrace{cy}_{\in J} \in I + J \\
(x + y)c &= \underbrace{xc}_{\in I} + \underbrace{yc}_{\in J} \in I + J
\end{aligned}$$

### Exercícios:

1)  $A = \mathbb{Z}$

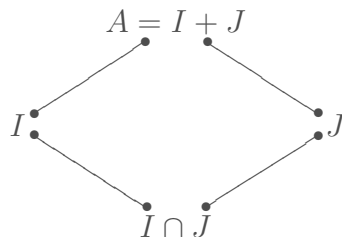
$$I = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \dots\} = \{2x \mid x \in \mathbb{Z}\}$$

$$J = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \dots\} = \{3x \mid x \in \mathbb{Z}\}$$

$$I \cap J = ? \quad I + J = ?$$

$$I \cap J = (\text{mmc}(2, 3)) = (6) = 6\mathbb{Z}$$

$$I + J = (\text{mdc}(2, 3)) = (1) = \mathbb{Z}$$



2) Verifique que a união de ideais, em geral, não é um ideal.

**Exemplo:**  $A = \mathbb{Z}$

$$I = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$$

$$J = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$$

$I \cup J$  não é ideal, pois

$$x = 2 \in I \subseteq I \cup J \text{ e } y = 3 \in J \subseteq I \cup J$$

$$y - x = 3 - 2 = 1 \notin I \cup J \quad (\text{não vale o fechamento pra “-”})$$

3) Mostre que todo ideal de  $\mathbb{Z}$  é principal, ou seja, se  $I$  é ideal de  $\mathbb{Z}$ , então

$$I = (n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \text{ onde } n \in \mathbb{Z}_+.$$

**Demonstração.** Seja  $I$  um ideal de  $\mathbb{Z}$ . Se  $I = \{0\}$ , então não há nada a demonstrar, pois  $I = 0\mathbb{Z} = \{0k \mid k \in \mathbb{Z}\} = \{0\}$ .

Podemos supor que  $I \neq \{0\}$ . Então,  $\exists x \in I - \{0\}$ . Como  $I$  é ideal, segue que  $-x \in I$ . Assim,  $I$  contém elementos positivos e negativos.

Considere  $S = I \cap \mathbb{N} = \{a \in I \mid a > 0\} \subseteq \mathbb{N}$ ,  $S \neq \emptyset \xrightarrow{\text{PBO}} \exists n = \min(S)$ , ou seja,  $n \in S$  e  $n \leq a$ ,  $\forall a \in S$ .

**Afirmção.**  $I = (n) = n\mathbb{Z}$  (igualdade de conjuntos)

(A)  $n\mathbb{Z} \subseteq I$

Segue do fato de  $n\mathbb{Z}$  ser ideal de  $\mathbb{Z}$

$$\left. \begin{array}{l} n \in I \\ k \in \mathbb{Z} \end{array} \right\} \Rightarrow nk \in I \Rightarrow n\mathbb{Z} \subseteq I$$

(B)  $I \subseteq n\mathbb{Z}$

Tome  $a \in I$ . Queremos mostrar que  $a \in n\mathbb{Z}$

$a \in I$ ;  $n > 0$

Podemos dividir  $a$  por  $n$  usando o Algoritmo de Euclides:  $a = kn + r$ , onde  $0 \leq r < n$ . Observe que  $r = a - kn \in I$ .

**Afirmção.**  $r = 0$  ( $\Rightarrow a = kn$ )

Se  $r \neq 0$ , então  $r \in I$ ,  $r > 0 \Rightarrow r \in S = I \cap \mathbb{N}$ , o que é absurdo, pois  $r < n = \min(S)$ . ■

## Anéis - Quociente

Motivação: Generalizar a noção de congruência para números inteiros.

Lembre-se:  $A = \mathbb{Z}$

$x, y \in \mathbb{Z}$ ,  $n \in \mathbb{N}$

$x \equiv y \pmod{n} \Leftrightarrow n \mid x - y$ , ou seja,  $x - y = nk$ , para algum  $k \in \mathbb{Z}$ .

Generalizando:

Sejam  $A$  um anel comutativo com identidade e  $I$  um ideal de  $A$ . Sejam  $x, y \in A$ . Dizemos que “ $x$  é congruente a  $y$  módulo  $I$ ” se  $x - y \in I$ .

**Notação.**  $x \equiv y \pmod{I} \Leftrightarrow x - y \in I$  (\*)

**Observações.** i) A congruência em  $\mathbb{Z}$  é um caso particular da congruência acima, pois:

$$A = \mathbb{Z}, I = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \quad (n \in \mathbb{N})$$

Neste caso, dados  $x, y \in \mathbb{Z}$ ,

$$\begin{aligned} x \equiv y \pmod{I} &\Leftrightarrow x - y \in I = n\mathbb{Z} \\ &\Leftrightarrow x - y = nk, \text{ para algum } k \in \mathbb{Z} \\ &\Leftrightarrow n \mid x - y \Leftrightarrow x \equiv y \pmod{n} \end{aligned}$$

ii) (\*) define uma relação de equivalência sobre  $A$ , pois:

$$(RE1) \text{ (Reflexiva)} \quad x \equiv x \pmod{I}, \forall x \in A$$

$$\text{De fato: } x - x = 0 \in I$$

$$(RE2) \text{ (Simétrica)} \quad x \equiv y \pmod{I} \Rightarrow y \equiv x \pmod{I}$$

$$\text{De fato: } x \equiv y \pmod{I} \Rightarrow x - y \in I \Rightarrow -(x - y) \in I \Rightarrow y - x \in I \Rightarrow y \equiv x \pmod{I}$$

$$(RE3) \text{ (Transitiva)} \quad x \equiv y \pmod{I} \text{ e } y \equiv z \pmod{I} \Rightarrow x \equiv z \pmod{I}$$

$$\text{De fato: } x \equiv y \pmod{I} \Rightarrow x - y \in I \quad (A)$$

$$\text{e } y \equiv z \pmod{I} \Rightarrow y - z \in I \quad (B)$$

(A) + (B): Como  $I$  é ideal, segue que

$$(x - y) + (y - z) \in I \Rightarrow x - z \in I \Rightarrow x \equiv z \pmod{I}$$

iii) Usando a congruência (\*) é possível construir um novo anel análogo ao anel dos inteiros módulo  $n$ .  $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$

- $A$  - anel (comutativo com identidade)
- $\equiv \pmod{I}$
- $\overline{x} = \{y \in A \mid y \equiv x \pmod{I}\} = \{y \in A \mid y - x = z \in I\} = \{y \in A \mid y = x + z, \text{ com } z \in I\} = X + I = \{x + z \mid z \in I\}$   
(classe de equivalência de  $x$  módulo  $I$ )
- $A/I = A/\equiv = \{\overline{x} \mid x \in A\}$   
(conjunto das classes de equivalência)

Observe que  $A/I$  é uma partição de  $A$ , ou seja,

a)  $\bar{x} \neq \emptyset, \forall x \in A;$

b)  $\bar{x} \neq \bar{y} \Rightarrow \bar{x} \cap \bar{y} = \emptyset$

c)  $\bigcup_{x \in A} \bar{x} = A$

- Em  $A/I$ , podemos definir duas operações binárias (“+” e “.”) a partir das seguintes propriedades

$$\text{Se } \begin{cases} x \equiv x' \pmod{I} \\ y \equiv y' \pmod{I} \end{cases}, \text{ então } \begin{cases} x + y \equiv x' + y' \pmod{I} \\ x \cdot y \equiv x' \cdot y' \pmod{I} \end{cases}$$

$$\text{Analogamente: Se } \begin{cases} \bar{x} = \overline{x'} \\ \bar{y} = \overline{y'} \end{cases}, \text{ então } \begin{cases} \overline{x + y} = \overline{x' + y'} \\ \overline{x \cdot y} = \overline{x' \cdot y'} \end{cases}$$

Desta maneira, podemos definir adição e multiplicação da seguinte maneira:

$$\begin{aligned} + : A/I \times A/I &\rightarrow A/I \\ (\bar{x}, \bar{y}) &\mapsto \bar{x} + \bar{y} \stackrel{\text{def}}{=} \overline{x + y} \end{aligned}$$

(independe da escolha dos representantes)

$$\begin{aligned} \cdot : A/I \times A/I &\rightarrow A/I \\ (\bar{x}, \bar{y}) &\mapsto \bar{x} \cdot \bar{y} \stackrel{\text{def}}{=} \overline{x \cdot y} \end{aligned}$$

(independe da escolha dos representantes)

Assim,  $(A/I, +, \cdot)$  é um anel comutativo com identidade  $\bar{1}$ , chamado de anel quociente de  $A$  pelo ideal  $I$

$$\begin{cases} \bar{0} = \text{elemento neutro para } + \\ \bar{1} = \text{elemento neutro para } \cdot \end{cases}$$

### Exercícios Seleccionados:

1) Mostre que se  $K$  é um corpo, então os únicos ideais de  $K$  são os triviais:  $\{0\}$  e  $K$ .

2) Sejam  $A$  e  $B$  anéis. Seja  $f : A \rightarrow B$  um homomorfismo, ou seja,

$$\begin{cases} f(a + a') = f(a) + f(a') \\ f(a \cdot a') = f(a) \cdot f(a') \end{cases}, \forall a, a' \in A$$

Mostre que

- a)  $f(0_A) = 0_B$ ;
- b)  $f(-a) = -f(a)$ ;
- c) Se  $A$  e  $B$  são domínios de integridade então ou  $f$  é a função constante 0 ou  $f(1_A) = 1_B$

3) Sejam  $A$  e  $B$  anéis e

$$\begin{aligned} f : A &\rightarrow B \\ a &\mapsto f(a) \end{aligned}$$

um homomorfismo. Definimos

- $\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\} \subseteq A$  (núcleo de  $f$ )
- $\text{Im}(f) = \{f(a) \mid a \in A\} \subseteq B$  (imagem de  $f$ )

Mostre que

- a)  $\text{Im}(f)$  é um subanel de  $B$ ;
- b)  $\text{Ker}(f)$  é um ideal de  $A$ ;
- c)  $f$  é injetiva  $\Leftrightarrow \text{Ker}(f) = \{0_A\}$  (núcleo trivial)

**Resolução:**

- 1) H:  $\begin{cases} K - \text{corpo} \\ I - \text{ideal de } K \end{cases}$

T:  $I = \{0\}$  ou  $I = K$

**Demonstração.** Vamos supor que  $I \neq \{0\}$ . Queremos mostrar que  $I = K$ .

Se  $I \neq \{0\}$ , então existe  $a \in I$ , com  $a \neq 0$ . Como  $K$  é corpo, então existe  $b \in K$  tal que  $a \cdot b = 1$ . Observe que

$$\begin{cases} a \in I \\ b \in K \end{cases} \Rightarrow a \cdot b = 1 \in I$$

Assim, segue que se  $x \in K$ , então  $x \in I$ , ou seja,  $K \subseteq I$ . Como  $I \subseteq K$ , segue que  $I = K$ . ■

- 2) a) H:  $f : A \rightarrow B$  (homomorfismo)  
T:  $f(0_A) = 0_B$

**Demonstração.**  $0_A + 0_A = 0_A$

$$\begin{aligned} f(0_A + 0_A) &= f(0_A) \Rightarrow f(0_A) + f(0_A) = f(0_A) = f(0_A) = f(0_A) + 0_B \Rightarrow \\ [f(0_A) + f(0_A)] + (-f(0_A)) &= [f(0_A) + 0_B] + (-f(0_A)) \Rightarrow f(0_A) + \\ 0_B &= 0_B + 0_B \Rightarrow f(0_A) = 0_B \quad \blacksquare \end{aligned}$$

b) T:  $f(-a) = -f(a)$

**Demonstração.**  $a + (-a) = 0_A$

$$\begin{aligned} f(a + (-a)) &= f(0_A) \Rightarrow f(a) + f(-a) = 0_B \Rightarrow [f(a) + f(-a)] + \\ (-f(a)) &= 0_B + (-f(a)) \Rightarrow f(-a) = -f(a) \quad \blacksquare \end{aligned}$$

c) H:  $A$  e  $B$  são DI

T:  $f \equiv 0$  (função identidade nula) ou  $f(1_A) = 1_B$

**Demonstração.** Vamos supor que  $f \not\equiv 0$  e concluir que  $f(1_A) = 1_B$ .

De fato:

$$1_A \cdot 1_A = 1_A$$

$$\begin{aligned} f(1_A \cdot 1_A) &= f(1_A) \Rightarrow f(1_A)f(1_A) = f(1_A) \Rightarrow f(1_A)f(1_A) - \\ f(1_A) &= 0_B \Rightarrow f(1_A)[f(1_A) - 1_B] = 0_B \end{aligned}$$

$$\Rightarrow f(1_A) = 0_B \quad \text{ou} \quad f(1_A) = 1_B$$

Se ocorre o segundo caso, então (ok!). Se ocorre o primeiro, então,  
 $\forall x \in A,$

$$f(x) = f(x \cdot 1_A) = f(x) \cdot f(1_A) = 0_B \quad \blacksquare$$

### 3) Demonstração.

a) Devemos mostrar que:

i)  $0_B \in \text{Im}(f)$

ii)  $b_1, b_2 \in \text{Im}(f) \Rightarrow b_1 - b_2 \in \text{Im}(f)$

iii)  $b_1, b_2 \in \text{Im}(f) \Rightarrow b_1 \cdot b_2 \in \text{Im}(f)$

De fato:

i) Pelo exercício 2 (a),  $0_B = f(0_A)$

ii)  $b_1 \in \text{Im}(f) \Rightarrow b_1 = f(a_1), a_1 \in A; \quad b_2 \in \text{Im}(f) \Rightarrow b_2 = f(a_2), a_2 \in A$

Como  $f$  é homomorfismo, então

$$\begin{aligned} f(a_1 - a_2) &= f(a_1 + (-a_2)) = f(a_1) + f(-a_2) = f(a_1) - f(a_2) = \\ b_1 - b_2 &\in \text{Im}(f) \end{aligned}$$

$$\text{iii)} \quad f(a_1 \cdot a_2) = f(a_1)f(a_2) = b_1 \cdot b_2 \in \text{Im}(f)$$

b) Devemos mostrar que:

$$\text{i)} \quad 0_A \in \text{Ker}(f)$$

$$\text{ii)} \quad a_1, a_2 \in \text{Ker}(f) \Rightarrow a_1 - a_2 \in \text{Ker}(f)$$

$$\text{iii)} \quad a_1, a_2 \in \text{Ker}(f) \Rightarrow a_1 \cdot a_2 \in \text{Ker}(f)$$

$$\text{iv)} \quad a \in \text{Ker}(f), x \in A \Rightarrow ax \in \text{Ker}(f) \quad \text{e} \quad xa \in \text{Ker}(f)$$

De fato:

$$\text{i)} \quad \text{Pelo exercício 2 (a), } f(0_A) = 0_B \Rightarrow 0_A \in \text{Ker}(f)$$

$$\text{ii)} \quad a_1 \in \text{Ker}(f) \Rightarrow f(a_1) = 0_B; \quad a_2 \in \text{Ker}(f) \Rightarrow f(a_2) = 0_B$$

Como  $f$  é homomorfismo,

$$f(a_1 - a_2) = f(a_1) - f(a_2) = 0_B - 0_B = 0_B \Rightarrow a_1 - a_2 \in \text{Ker}(f)$$

$$\text{iii)} \quad a_1, a_2 \in \text{Ker}(f) \Rightarrow a_1 - a_2 \in \text{Ker}(f)$$

$$a_1 \in \text{Ker}(f) \Rightarrow f(a_1) = 0$$

$$a_2 \in \text{Ker}(f) \Rightarrow f(a_2) = 0$$

$$f(a_1 - a_2) \stackrel{(*)}{=} f(a_1) + f(-a_2) \stackrel{(*)}{=} f(a_1) - f(a_2) = 0 + 0 = 0$$

$$\Rightarrow a_1 - a_2 \in \text{Ker}(f)$$

$$\text{iv)} \quad a \in \text{Ker}(f), x \in A \Rightarrow a \cdot x \in \text{Ker}(f) \quad \text{e} \quad x \cdot a \in \text{Ker}(f)$$

$$a \in \text{Ker}(f) \Rightarrow f(a) = 0$$

$$f(a \cdot x) \stackrel{(*)}{=} f(a) \cdot f(x) = 0 \cdot f(x) = 0$$

$$\Rightarrow a \cdot x \in \text{Ker}(f)$$

$$f(x \cdot a) \stackrel{(*)}{=} f(x) \cdot f(a) = f(x) \cdot 0 = 0$$

$$x \cdot a \in \text{Ker}(f)$$

(\*) :  $f$  é homomorfismo

$$\text{c)} \quad (\Rightarrow) \begin{cases} \text{H: } f \text{ é injetiva} \\ \text{T: } \text{Ker}(f) = \{0_A\} \end{cases}$$

Por hipótese,  $f$  é injetiva, ou seja, elementos distintos têm imagens distintas. Assim, se  $a \in A$  é tal que  $a \neq 0_A$ , então  $f(a) \neq f(0_A) = 0_B$ . Portanto,  $\forall a \neq 0_A, a \notin \text{Ker}(f) \Rightarrow \text{Ker}(f) = \{0_A\}$ .

$$(\Leftarrow) \begin{cases} \text{H: } \text{Ker}(f) = \{0_A\} \\ \text{T: } f \text{ é injetora} \end{cases}$$

Queremos mostrar que se  $f(a) = f(a')$ , então  $a = a'$ .

De fato:  $f(a) = f(a') \Rightarrow f(a) - f(a') = 0_B \Rightarrow f(a - a') = 0_B \Rightarrow a - a' \in \text{Ker}(f) = \{0_A\} \Rightarrow a - a' = 0_A$ , isto é,  $a = a' + 0_A = a'$ . ■



**Teorema 7.4 (Primeiro Teorema do Homomorfismo de Anéis).** *Seja  $f : A \rightarrow B$  um homomorfismo de anéis. Então:*

- a)  $Im(f)$  é um subanel de  $B$ ;
- b)  $Ker(f)$  é um ideal de  $A$ ;
- c) O anel quociente  $A_{/Ker(f)}$  é isomorfo a  $Im(f)$ , isto é,  $A_{/Ker(f)} \cong Im(f)$

**Demonstração.** Falta apenas demonstrar c).

Queremos mostrar que existe uma função  $\psi : A_{/Ker(f)} \rightarrow Im(f)$  tal que:

i)  $\psi$  é bijeção;

ii)  $\psi$  é homomorfismo.

$$f : A \rightarrow B \quad (\text{dada})$$

$$x \mapsto y = f(x)$$

$$\pi : A \rightarrow A_{/Ker(f)} \quad (\text{auxiliar})$$

$$x \mapsto \pi(x) = \bar{x}$$

$$\psi : A_{/Ker(f)} \rightarrow Im(f) \quad (\text{a obter})$$

$$\bar{x} \mapsto \psi(\bar{x}) := f(x)$$

i)  $\psi$  é bijeção:

•  $\psi$  é sobrejetora:  $CD(\psi) = Im(f)$

$$Im(\psi) = \{\psi(\bar{x}) \mid \bar{x} \in A_{/Ker(f)}\} = \{f(x) \mid x \in A\} = Im(f)$$

•  $\psi$  é injetiva:  $\psi(\bar{x}) = \psi(\bar{y}) \Rightarrow \bar{x} = \bar{y}$

De fato:

$$\psi(\bar{x}) = \psi(\bar{y}) \Rightarrow f(x) = f(y) \Rightarrow f(x) - f(y) = 0_B \Rightarrow f(x - y) = 0_B \Rightarrow x - y \in Ker(f) = I \Rightarrow x \equiv y \pmod{I} \Rightarrow \bar{x} = \bar{y}$$

ii)  $\psi$  é homomorfismo:

$$\bullet \psi(\bar{x} + \bar{y}) = \psi(\bar{x}) + \psi(\bar{y})$$

$$\bullet \psi(\bar{x} \cdot \bar{y}) = \psi(\bar{x}) \cdot \psi(\bar{y})$$

De fato:

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

$$\bullet \psi(\bar{x} \cdot \bar{y}) = \psi(\overline{x \cdot y}) = f(x \cdot y) = f(x) \cdot f(y) = \psi(\bar{x}) \cdot \psi(\bar{y}) \quad \blacksquare$$

## II) Grupos

**Definição 7.5 (Grupo).** Seja  $G \neq \emptyset$  munido de uma operação binária  $*$ . Dizemos que o par  $(G, *)$  é um Grupo (ou que  $G$  é um grupo) se:

- a)  $*$  é associativa:  $(a * b) * c = a * (b * c), \forall a, b, c \in G$
- b)  $*$  possui um elemento neutro  $e$ :  $e * a = a * e (\forall a \in G)$
- c)  $\forall a \in G, \exists a' \in G \mid a * a' = e \text{ e } a' * a = e$

**Observação.** Se vale também a propriedade

- d)  $\forall a, b \in G, a * b = b * a$ ,  
então  $G$  é dito grupo abeliano (ou comutativo).

Convenção: A partir de agora, vamos adotar uma notação multiplicativa para um grupo  $(G, *)$ .

notação abstrata	notação multiplicativa
$*$	$\cdot$
$e$	$1$
$a'$	$a^{-1}$

Com esta notação, podemos definir potências inteiras de  $a \in G$

$$\begin{aligned}
 a^0 &:= 1 \\
 a^1 &:= a \\
 a^2 &:= a \cdot a \\
 &\vdots \\
 a^n &= \underbrace{a \cdot a \cdot a \dots a}_{n \text{ vezes}} = a^{n-1} \cdot a \quad (n \in \mathbb{N}) \\
 a^{-n} &= (a^n)^{-1} \quad (n \in \mathbb{N})
 \end{aligned}$$

**Propriedades:** (Lei de Expoentes)

$$\begin{cases} a^m \cdot a^n = a^{m+n} = a^n \cdot a^m \\ (a^m)^n = a^{m \cdot n} \end{cases}, \quad (m, n \in \mathbb{Z})$$

$$\text{Lembre-se: } \begin{cases} (a^{-1})^{-1} = a \\ (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \end{cases}$$

**Exercício:** (Desafio)

Seja  $(G, \cdot)$  um grupo. Mostre que se  $x^2 = 1, \forall x \in G$ , então  $G$  é abeliano.

$$\text{Sugestão: usar } \begin{cases} (x^{-1})^{-1} = x \\ (xy)^{-1} = y^{-1}x^{-1} \end{cases}$$

$x, y \in G \Rightarrow x \cdot y \in G$  e  $(x \cdot y)^{-1} \in G$ , pois  $(G, \cdot)$  é grupo.  
 Como  $x^2 = x \cdot x = 1$ ,  $\forall x \in G$ , temos  $x^{-1} = x$ ,  $\forall x \in G$ . Então,

$$x \cdot y = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$$

mas,  $y^{-1} = y$  e  $x^{-1} = x$ , daí

$$x \cdot y = y \cdot x, \quad \forall x, y \in G$$

**Observação.** Quando  $G$  é abeliano, é costume denotar  $*$  por  $+$ . Neste caso:

notação abstrata	notação aditiva
$*$	$+$
$e$	$0$
$a'$	$-a$

Com esta notação, podemos definir múltiplos inteiros de  $a \in G$

$$0 \cdot a := 0$$

$$1 \cdot a := a$$

$$-1 \cdot a := -a$$

$$n \cdot a := \underbrace{a + a + a + \dots + a}_{n \text{ parcelas}} \quad (n \in \mathbb{N})$$

$$-n \cdot a := -\underbrace{[a + a + a + \dots + a]}_{n \cdot a} \quad (n \in \mathbb{N})$$

**Propriedade:**  $na + ma = (n + m)a \quad (m, n \in \mathbb{Z})$

**Definição 7.6 (Ordem de Um Grupo).** *Seja  $(G, \cdot)$  um grupo. Definimos a ordem de  $G$  como sendo a cardinalidade de  $G$ .*

**Notação.**  $\circ(G) = |G|$  (lê-se: “ordem de  $G$ ”)

**Observação.** Se  $|G| < \infty$ , então  $G$  é dito grupo finito. Caso contrário,  $G$  é dito grupo infinito.

**Exemplos:** a)  $(\mathbb{Z}, +)$  = grupo infinito (abeliano)

b)  $(\mathbb{Z}_n, +)$  = grupo finito ( $|\mathbb{Z}_n| = n$ ) (abeliano)

c)  $(S_n, \circ)$  = grupo finito ( $|S_n| = n!$ ) (não-abeliano)

d)  $(\mathbb{R}^+, \cdot)$  = grupo infinito (abeliano) ( $|\mathbb{R}| = \infty$ )

**Definição 7.7 (Subgrupo).** *Sejam  $(G, \cdot)$  um grupo e  $H \subseteq G$ . Dizemos que  $H$  é um subgrupo de  $G$  se:*

- a)  $H \neq \emptyset$  (isto é,  $1 \in H$ );
- b)  $\forall h_1, h_2 \in H, h_1 \cdot h_2 \in H$ ;
- c)  $(H, \cdot)$  é também um grupo

**Exemplos:**

- a)  $\forall$  grupo  $(G, \cdot)$ ,  $\{1\}$  e  $G$  são subgrupos (subgrupos triviais)
- b)  $G = \text{GL}_n(\mathbb{R}) = \{A = (a_{ij})_{n \times n} \mid a_{ij} \text{'s} \in \mathbb{R} \text{ e } \det A \neq 0\}$   
 (grupo linear geral de grau  $n$ );  $\cdot = \cdot$   
 $\det(A^{-1}) = 1/\det A$  e  $\det(AB) = \det A \cdot \det B$   
 $H = \{A \in \text{GL}_n(\mathbb{R}) \mid \det A = 1\} = \text{SL}_n(\mathbb{R}) \subseteq G$   
 (grupo linear especial de grau  $n$ )  
 $H$  é subgrupo de  $G$  ( $H \leq G$ )

**Notação.**  $H \leq G$  (lê-se:  $H$  é subgrupo de  $G$ )

- c)  $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ ,  $\cdot = +$   
 $H = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq G$

**Afirmção.**  $H \leq G$

$$e = \bar{0} \in H$$

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

(vale o fechamento)

$$(\bar{0})' = \bar{0}, (\bar{2})' = \bar{4} (= -\bar{2}), (\bar{4})' = \bar{2} (= -\bar{4})$$

- d)  $G = S_3 = \{f : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \mid f \text{ é bijeção}\}$   
 $= \{f_1, f_2, f_3, f_4, f_5, f_6\}$ , onde

$$f_1 = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$H_1 = \{f_1\} \leq G \quad (\text{trivial})$$

$$H_2 = \{f_1, f_2\} \leq G$$

$$H_3 = \{f_1, f_3\} \leq G$$

$$H_4 = \{f_1, f_4\} \leq G$$

$$H_5 = \{f_1, f_5, f_6\} \leq G$$

$$H_6 = S_3 \leq G \quad (\text{trivial})$$

$$H_5 \leq G$$

De fato:

$$\bullet f_1 \in H_5$$

$$\begin{array}{c|ccc} \circ & f_1 & f_5 & f_6 \\ \hline f_1 & f_1 & f_5 & f_6 \\ f_5 & f_5 & f_6 & f_1 \\ f_6 & f_6 & f_1 & f_5 \end{array}$$

$$f_5 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$$

$$f_5 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_6 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_6 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$$

(vale o fechamento)

$$(f_1)^{-1} = f_1, (f_5)^{-1} = f_6, (f_6)^{-1} = f_5$$

$$\bullet H_2 = \{f_1, f_2\}$$

$$\begin{array}{c|cc} \circ & f_1 & f_2 \\ \hline f_1 & f_1 & f_2 \\ f_2 & f_2 & f_1 \end{array}$$

$$f_2 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$\left\{ \begin{array}{l} f_1 \in H_2 \\ \text{vale o fechamento} \\ (f_1)^{-1} = f_1, (f_2)^{-1} = f_2 \end{array} \right. \Rightarrow H_2 \leq G$$

- $H_3 = \{f_1, f_3\}$

$$\begin{array}{c|cc} \circ & f_1 & f_3 \\ \hline f_1 & f_1 & f_3 \\ f_3 & f_3 & f_1 \end{array}$$

$$f_3 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$\left\{ \begin{array}{l} f_1 \in H_3 \\ \text{vale o fechamento} \\ (f_1)^{-1} = f_1, (f_3)^{-1} = f_3 \end{array} \right. \Rightarrow H_3 \leq G$$

- $H_4 = \{f_1, f_4\}$

$$\begin{array}{c|cc} \circ & f_1 & f_4 \\ \hline f_1 & f_1 & f_4 \\ f_4 & f_4 & f_1 \end{array}$$

$$f_4 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$\left\{ \begin{array}{l} f_1 \in H_4 \\ \text{vale o fechamento} \\ (f_1)^{-1} = f_1, (f_4)^{-1} = f_4 \end{array} \right. \Rightarrow H_4 \leq G$$

e) (Subgrupo Cíclico)

$(G, \cdot)$  - grupo,  $a \in G$

$$H = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle \leq G$$

(subgrupo cíclico gerado por  $a$ )

**Observação.** Se  $\langle a \rangle = G$ , isto é,  $\forall g \in G, g = a^k$ , para algum  $k \in \mathbb{Z}$ , então  $G$  é dito grupo cíclico gerado por  $a$ .

**Afirmação.**  $H \leq G$

De fato:

- $e = a^0 \quad (k = 0) \in H$

- $\left\{ \begin{array}{l} h_1 = a^{k_1} \in H \\ h_2 = a^{k_2} \in H \end{array} \right. \Rightarrow h_1 \cdot h_2 = a^{k_1} a^{k_2} = a^{k_1+k_2} \in H$

- $(H, \cdot)$  é um grupo
 
$$\left\{ \begin{array}{l} - \text{ associativa} \\ - \text{ elemento neutro} \\ - (a^k)^{-1} = a^{-k} \in H \end{array} \right.$$

Caso particular: subgrupo cíclico com dois elementos

$$G = \mathbb{R}^*; a = -1$$

$$* = \cdot$$

$$H = \{-1, 1\} = \langle -1 \rangle = \{(-1)^n \mid n \in \mathbb{Z}\} \subset G$$

$$\begin{array}{c|cc} \cdot & -1 & 1 \\ \hline -1 & 1 & -1 \\ 1 & -1 & 1 \end{array}$$

**Exercício:** Sejam  $(G, \cdot)$  um grupo e  $H \leq G$ . Dados  $x, y \in G$ , defina:

$$x \equiv y \pmod{H} \Leftrightarrow x^{-1}y \in H$$

Mostre que  $\equiv$  define uma relação de equivalência sobre  $G$ .

**Resolução:**

(RE 1) (Reflexiva)

$$x \equiv x \pmod{H} \text{ (ok!)}, \text{ pois } x^{-1}x = 1 \in H$$

(RE 2) (Simetria)

$$x \equiv y \pmod{H} \Rightarrow y \equiv x \pmod{H}$$

$$\text{De fato: } x \equiv y \pmod{H} \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H$$

$$(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \Rightarrow y \equiv x \pmod{H}$$

(RE 3) (Transitividade)

$$x \equiv y \pmod{H} \Rightarrow x^{-1}y \in H$$

$$y \equiv z \pmod{H} \Rightarrow y^{-1}z \in H$$

$$\text{Como } H \leq G, (x^{-1}y)(y^{-1}z) \in H$$

$$(x^{-1}y)(y^{-1}z) = x^{-1}(yy^{-1})z = (x^{-1}1)z = x^{-1}z \Rightarrow x \equiv z \pmod{H}$$

**Teorema 7.8 (Teorema de Lagrange).** (Tal Teorema relaciona as cardinalidades de  $H$  e  $G$ , onde  $H \leq G$  e  $|G| < \infty$ )

Seja  $(G, \cdot)$  um grupo finito. Seja  $H \leq G$ . Então,  $|H|$  divide  $|G|$ .

**Exemplo:**  $G = S_3$ ;  $* = \circ$

$$|G| = 3! = 6$$

$$H_1 = \{f_1\} \Rightarrow |H_1| = 1 \mid 6$$

$$H_2 = \{f_1, f_2\} \Rightarrow |H_2| = 2 \mid 6$$

$$H_3 = \{f_1, f_3\} \Rightarrow |H_3| = 2 \mid 6$$

$$H_4 = \{f_1, f_4\} \Rightarrow |H_4| = 2 \mid 6$$

$$H_5 = \{f_1, f_5, f_6\} \Rightarrow |H_5| = 3 \mid 6$$

$$H_6 = S_3 \Rightarrow |H_6| = 6 \mid 6$$

### Correção da Lista 4

2) a) Tese:  $f$  é monomorfismo de anéis

$$f: \mathbb{C} \rightarrow \mathcal{M}_{2 \times 2}(\mathbb{R})$$

$$a + bi \mapsto f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

#### Demonstração.

I)  $f$  é homomorfismo (preserva “+” e “.”)

$$z_1 = a + bi \in \mathbb{C} \Rightarrow f(z_1) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$$

$$z_2 = c + di \in \mathbb{C} \Rightarrow f(z_2) = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{R})$$

$$z_1 + z_2 = (a + c) + (b + d)i \in \mathbb{C}$$

$$f(z_1 + z_2) = \begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$$

$$= f(z_1) + f(z_2)$$

$$z_1 \cdot z_2 = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

$$f(z_1 \cdot z_2) = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix}$$

II

$$f(z_1) \cdot f(z_2) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \quad \text{II) } f \text{ é injetiva:}$$

$$\begin{aligned} \text{Ker}(f) &= \{z \in \mathbb{C} \mid f(z) = 0\} \\ &= \left\{ a + bi \in \mathbb{C} \mid \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ &= \{0 + 0i\} = \{0\} \Rightarrow f \text{ é injetora} \end{aligned}$$

■



11)  $f(x) = x^2 - x \in A[x]$ , onde  $A$  é DI

Tese: As únicas raízes de  $f$  em  $A$  são 0 e 1.

**Demonstração.**  $\alpha \in A$  é raiz de  $f$  se  $f(\alpha) = 0$

$$f(\alpha) = 0 \Rightarrow \alpha^2 - \alpha = 0 \Rightarrow \alpha(\alpha - 1) = 0 \Rightarrow \alpha = 0 \text{ ou } \alpha - 1 = 0 \Rightarrow \alpha = 0 \text{ ou } \alpha = 1 \quad \blacksquare$$

**Teorema de Lagrange (7.8).** Sejam  $(G, \cdot)$  um grupo finito e  $H \leq G$ . Então,  $|H|$  divide  $|G|$  (isto é,  $|G| = n|H|$ , com  $n \in \mathbb{N}$ ).

**Demonstração.** (do Teorema 7.8)

Pelo exercício da página 172, dados  $x, y \in G$ ,  $x \equiv y \pmod{H} \Leftrightarrow x^{-1}y \in H$  define uma relação de equivalência sobre  $G$ . Assim, podemos obter  $\bar{x}$  (classe de equivalência de  $x$ ), a saber:

$$\begin{aligned} \bar{x} &= \{y \in G \mid x \equiv y \pmod{H}\} = \{y \in G \mid x^{-1}y = h \in H\} \\ &= \{y \in G \mid y = xh, h \in H\} \stackrel{\text{def}}{=} xH = \{xh \mid h \in H\} \end{aligned}$$

( $xH$  é a classe lateral à esquerda de  $H$  determinada por  $x$ )

**Observações.** a) Poderíamos também ter definido uma outra relação de equivalência:

$$x \equiv y \pmod{H} \Leftrightarrow xy^{-1} \in H$$

Neste caso,  $\bar{x} = Hx$  (classe lateral à direita de  $H$  determinada por  $x$ )

b) Como  $G$  é finito, segue que há um número finito de classes laterais à esquerda, a saber:  $x_1H, x_2H, \dots, x_nH$ . Tais classes constituem uma partição de  $G$ , ou seja:

$$\text{i) } x_iH \neq \emptyset, \forall i \in \{1, \dots, n\};$$

$$\text{ii) } x_iH \neq x_jH \Rightarrow x_iH \cap x_jH = \emptyset, (i \neq j);$$

$$\text{iii) } G = x_1H \cup x_2H \cup \dots \cup x_nH$$

c) Todas as classes laterais à esquerda têm o mesmo número de elementos.

De fato:

$$\begin{aligned} f: H &\rightarrow xH \\ h &\mapsto f(h) = xh \end{aligned}$$

é uma bijeção. Logo,  $|xH| = |H|, \forall x \in G$ .

Conclusão:

$$|G| = |x_1H| + |x_2H| + \dots + |x_nH| = |H| + |H| + \dots + |H| = nH$$

( $n$  = índice de  $H$  em  $G$  = número de distintas classes à esquerda) ■

### Exercícios:

1) Fatore os seguintes polinômios como produto de fatores irredutíveis em  $\mathbb{R}[x]$ :

a)  $f(x) = x^3 + x^2 + x + 1$

b)  $f(x) = x^3 + 1$

c)  $f(x) = x^3 - 1$

d)  $f(x) = x^3 - x$

e)  $f(x) = x^3 + x$

f)  $f(x) = x^4 + 1$

g)  $f(x) = x^6 - 1$

2) (Multiplicidade de uma Raiz)

$K$  = corpo (por exemplo:  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  ou  $\mathbb{Z}_p$ )

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x], \quad a_n \neq 0$$

$\alpha \in K$  - raiz de  $f(x)$  (isto é,  $f(\alpha) = 0$ )

$m \in \mathbb{N}$

nomenclatura:  $\begin{cases} \bullet a_n = \text{coeficiente dominante (líder)} \\ \bullet \text{Se } a_n = 1, \text{ então } f \text{ é dito mônico} \end{cases}$

Dizemos que  $\alpha$  é raiz de multiplicidade  $m$  se  $f(x) = (x - \alpha)^m \cdot g(x)$ , onde  $g(x) \in K[x]$  e  $g(\alpha) \neq 0$ .

(Lembre-se: (Teorema do resto + Teorema de D'Allembert)

Mostre que  $\alpha$  é raiz simples  $\Leftrightarrow f(\alpha) = 0$  e  $f'(\alpha) \neq 0$ . Eq:  $\alpha$  é raiz de multiplicidade  $m \geq 2 \Leftrightarrow f(\alpha) = 0$  e  $f'(\alpha) = 0$ . (Na verdade:  $f(\alpha) = f'(\alpha) = \dots = f^{(m-1)}(\alpha) = 0$  e  $f^{(m)}(\alpha) \neq 0$ )

### Observação.

$m = 1$  :  $\alpha$  é raiz simples

$$f(x) = (x - \alpha)g(x)$$

$$\begin{aligned}
m = 2 : \alpha \text{ é raiz dupla} \\
f(x) = (x - \alpha)g(x) \\
\vdots
\end{aligned}$$

### Resolução:

- a) Lembre-se: Todo polinômio  $f(x) \in K[x]$  não-constante (isto é,  $\text{gr}(f) \geq 1$ ) pode ser decomposto como um produto de fatores irredutíveis. Tal decomposição é única, a menos de constantes.
- b) Em  $\mathbb{C}$  (T.F.A.), os únicos polinômios irredutíveis são os lineares:  $ax + b$ , com  $a \neq 0$ .
- c) Em  $\mathbb{R}$ , os únicos polinômios irredutíveis são os lineares ( $ax + b$ , com  $a \neq 0$ ) e os quadráticos com  $\Delta < 0$  ( $ax^2 + bx + c$ , com  $a \neq 0$  e  $\Delta = b^2 - 4ac < 0$ )
- d) Se  $\alpha \in \mathbb{C}$  é raiz de  $f(x) \in \mathbb{R}[x]$  então  $\bar{\alpha} \in \mathbb{C}$  também o é

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - \underbrace{(\alpha + \bar{\alpha})}_{2 \operatorname{Re}(\alpha) \in \mathbb{R}} x + \underbrace{\alpha \bar{\alpha}}_{|\alpha|^2 \in \mathbb{R}}$$

- 1) a)  $f(x) = x^3 + x^2 + x + 1 = x^2(x + 1) + (x + 1) = (x + 1) \underbrace{(x^2 + 1)}_{\Delta = -4 < 0}$
- b)  $f(x) = x^3 + 1 \stackrel{(1)}{=} (x + 1) \underbrace{(x^2 - x + 1)}_{\Delta = -3 < 0}$
- c)  $f(x) = x^3 - 1 \stackrel{(2)}{=} (x - 1)(x^2 + x + 1)$
- d)  $f(x) = x^3 - x = x(x^2 - 1) \stackrel{(3)}{=} x(x + 1)(x - 1)$
- e)  $f(x) = x^3 + x = x \underbrace{(x^2 + 1)}_{\Delta = -4 < 0}$
- f)  $f(x) = x^4 + 1 = [(x^2)^2 + 2x^2 \cdot 1 + 1^2] - 2x^2 \cdot 1 = (x^2 + 1)^2 - \underbrace{2x^2}_{(\sqrt{2}x)^2} \stackrel{(3)}{=} (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x) = \underbrace{(x^2 + \sqrt{2}x + 1)}_{\Delta = -2 < 0} \underbrace{(x^2 - \sqrt{2}x + 1)}_{\Delta = -2 < 0}$

$$\begin{aligned}
\text{g)} \quad f(x) &= x^6 - 1 \stackrel{(3)}{=} (x^3 - 1)(x^3 + 1) \\
&\stackrel{(2) \text{ e } (1)}{=} (x - 1) \underbrace{(x^2 + x + 1)}_{\Delta = -3 < 0} (x + 1) \underbrace{(x^2 - x + 1)}_{\Delta = -3 < 0} \\
(1) \quad (a^3 + b^3) &= (a + b)(a^2 - ab + b^2) \\
(2) \quad (a^3 - b^3) &= (a - b)(a^2 + ab + b^2) \\
(3) \quad (a^2 - b^2) &= (a + b)(a - b)
\end{aligned}$$

2) (Multiplicidade)

**Exemplos:**

$$\begin{aligned}
\text{a)} \quad f(x) &= ax + b \in \mathbb{R}[x], \quad a \neq 0 \\
f(x) = 0 &\Rightarrow ax + b = 0 \Rightarrow x = -b/a \\
f(x) &= ax + b = a \left( x + \frac{b}{a} \right) = a \left( x - \left( -\frac{b}{a} \right) \right)^1 \\
x = -b/a &\text{ é raiz simples} \\
f'(x) &= a \neq 0 \text{ (em particular, } f'(-b/a) \neq 0)
\end{aligned}$$

$$\begin{aligned}
\text{b)} \quad f(x) &= ax^2 + bx + c \in \mathbb{R}[x], \text{ com } a \neq 0 \\
f(x) = 0 &\Rightarrow ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \\
\begin{cases} \Delta > 0 : x_1, x_2 \in \mathbb{R}; x_1 \neq x_2 \\ \Delta = 0 : x_1, x_2 \in \mathbb{R}; x_1 = x_2 \\ \Delta < 0 : x_1, x_2 \in \mathbb{C}; (x_2 = \overline{x_1}) \end{cases}
\end{aligned}$$

Observe que se  $\Delta = 0$ , então  $\lambda = (-b/2a)$  é uma raiz dupla ( $m = 2$ ). Assim,  $f(x) = a(x - x_1)(x - x_2) = a(x - \lambda)^2$  ( $\lambda = x_1 = x_2$ )

$$f'(x) = 2ax + b$$

$$f''(x) = 2a \neq 0 \text{ (pois } a \neq 0)$$

Observe que

$$\begin{cases} f(\lambda) = 0 \\ f'(\lambda) = 0 \\ f''(\lambda) \neq 0 \end{cases}$$

$$\text{c)} \quad f(x) = x^3 \in \mathbb{R}[x]$$

$$x^3 = (x - 0)^3$$

$x = 0$  é raiz tripla ( $m = 3$ )

$$f(x) = x^3 \quad f''(x) = 6x$$

$$f'(x) = 3x^2 \quad f'''(x) = 6 \neq 0$$

Observe que  $f(0) = f'(0) = f''(0) = 0$  e  $f'''(0) \neq 0$ .

3) (Pendente - veja página 159)

$A = \mathbb{Z}$  (anel dos inteiros)

$a, b \in \mathbb{N}$

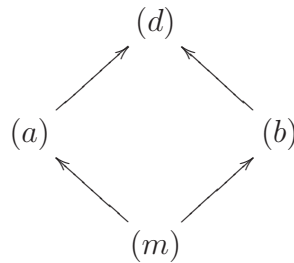
$I = (a) = a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \dots\}$

$J = (b) = b\mathbb{Z} = \{by \mid y \in \mathbb{Z}\} = \{0, \pm b, \pm 2b, \dots\}$

$I + J = (d) = d\mathbb{Z} = \{0, \pm d, \pm 2d, \dots\}$

$I \cap J = (m) = m\mathbb{Z} = \{0, \pm m, \pm 2m, \dots\}$

**Teorema 7.9.**  $d = \text{mdc}(a, b)$  e  $m = \text{mmc}(a, b)$



**Exemplo:**  $a = 2$ ,  $b = 3$

$I = (2) = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \dots\}$

$J = (3) = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \pm 15, \pm 18, \dots\}$

$I + J = (\text{mdc}(3, 2)) = (1) = 1\mathbb{Z} = \mathbb{Z}$

$I \cap J = (\text{mmc}(2, 3)) = (6) = 6\mathbb{Z} = \{0, \pm 6, \pm 12, \pm 18, \dots\}$

**Definição 7.10 (Ordem de Um Elemento de Um Grupo).** *Sejam  $(G, \cdot)$  um grupo e  $a \in G$ . Dizemos que  $a$  tem ordem (ou período) finita se  $\exists n \in \mathbb{N} \mid a^n = 1$ . O mínimo valor de  $n$  é chamado de ordem (ou período) de  $a$ .*

**Notação.**  $\circ(a) = \min\{n \in \mathbb{N} \mid a^n = 1\}$

**Observação.** Caso não exista tal  $n \in \mathbb{N}$ , dizemos que  $a$  tem ordem infinita.

4) Calcule  $\circ(a)$  nos seguintes casos:

a)  $G = \{\pm 1\}$ ,  $\ast = \cdot$

$a = 1 \Rightarrow \circ(1)$

$a = -1 \Rightarrow \circ(-1)$

- b)  $G = S_3; * = \circ$   
 $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow \circ \left( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right)$
- c)  $G = \mathbb{Z}_6; * = +$   
 $a = \bar{2} \Rightarrow \circ(\bar{2})$   
 $a = \bar{3} \Rightarrow \circ(\bar{3})$
- d)  $G = \mathbb{C}^*; * = \cdot$   
 $a = i \Rightarrow \circ(i)$

**Resolução:**

- a)  $e = 1; a^n = 1$   
 $\circ(1) = 1$ , pois  $1^1 = 1$   
 $\circ(-1) = 2$ , pois  $(-1)^2 = 1$
- b)  $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$   
 $a^n = e$  (compor  $a$   $n$  vezes)  
 $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq e$   
 $a^2 = a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq e$   
 $a^3 = a^2 \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$   
 $\Rightarrow \circ(a) = 3$
- c)  $e = \bar{0}; * = +$   
 $na = 0$   
 $a = \bar{2}$   
 $1 \cdot \bar{2} = \bar{2} \neq \bar{0}$   
 $2 \cdot \bar{2} = \bar{2} + \bar{2} = \bar{4} \neq \bar{0}$   
 $3 \cdot \bar{2} = \bar{2} + \bar{2} + \bar{2} = \bar{6} = \bar{0}$   
 $\circ(\bar{2}) = 3$   
 $a = \bar{3}$

$$1 \cdot \overline{3} = \overline{3} \neq \overline{0}$$

$$2 \cdot \overline{3} = \overline{3} + \overline{3} = \overline{6} = \overline{0}$$

$$\circ(\overline{3}) = 2$$

$$\text{d) } e = 1; a^n = 1$$

$$a = i$$

$$a^1 = i \neq 1$$

$$a^2 = -1 \neq 1$$

$$a^3 = -i \neq 1$$

$$a^4 = 1$$

$$\circ(a) = 4$$

## Exercícios Propostos

### Lógica & Conjuntos & Indução

(1ª Lista de Exercícios)

- 1) João e Ricardo estudam em colégios diferentes, porém estudam juntos em casa. Por coincidência, no dia em que João teve aula sobre função injetora, Ricardo também a teve. No caderno de João estava escrito: “Uma função é injetora quando  $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ ”. Já no caderno de Ricardo estava escrito: “Uma função é injetora quando  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ ”.

Assim, começou uma discussão:

- Seu professor errou - disse João.
- Foi o seu quem errou, pois o meu não erra - respondeu Ricardo.

Com base no texto acima, qual é a sua conclusão? Justifique.

- 2) Considere as afirmações seguintes:

- Todo automóvel alemão é bom
- Se um automóvel é bom, então ele é caro

- Existem automóveis suecos bons
- Se não choveu, então todas as lojas estão abertas
- Se  $x < y$ , então  $z = 5$  ou  $z = 7$

Admitindo a veracidade dessas 5 afirmações e admitindo que existam automóveis franceses, alemães, suecos e coreanos, julgue os itens a seguir:

- ☐ Se alguma loja está fechada, então choveu.
  - ☐ Se um automóvel não é caro, então ele pode ser francês.
  - ☐ Alguns automóveis suecos são caros.
  - ☐ Existem automóveis coreanos caros.
  - ☐ Um automóvel alemão pode não ser caro.
  - ☐ Se  $z \neq 5$  e  $z \neq 7$ , então  $x > y$ .
- 3) (PAS - UnB) Em matemática, as manipulações algébricas são fundamentais e devem ser feitas com bastante cautela, a fim de que sejam evitadas operações incorretas. Na seqüência de igualdades abaixo, numeradas de I a VII, considere  $x$  e  $y$  números reais não-nulos.

I)  $x = y$

II)  $xy = y^2$

III)  $x^2 - xy = x^2 - y^2$

IV)  $x(x - y) = (x + y)(x - y)$

V)  $x = x + y$

VI)  $x = 2x$

VII)  $1 = 2$

Com base nessas informações e admitindo I como verdadeira, julgue os itens abaixo:

- ☐ II é consequência de I.
- ☐ Os processos de fatoração usados em III para se obter IV valem apenas para  $x > 0$ .



c) ( ) É correta a obtenção de V a partir de IV.

d) ( ) É correta a obtenção de VII a partir de VI.

4) Sendo  $A = \{0, 1, 2, \{2\}, \{1, 2\}\}$ ,  $B = \{2\}$ ,  $C = \{\emptyset, 2\}$  e  $D = \{ \}$ , julgue os itens abaixo:

a) ( )  $0 \in A$       f) ( )  $\{1, 2\} \subseteq A$       l) ( )  $B \in C$

b) ( )  $2 \in A$       g) ( )  $\emptyset \subseteq C$       m) ( )  $D \in C$

c) ( )  $B \in A$       h) ( )  $D \subseteq C$       n) ( )  $B \subseteq C$

d) ( )  $B \subseteq A$       i) ( )  $1 \in A$       o) ( )  $D \subseteq B$

e) ( )  $\emptyset \in C$       j) ( )  $\emptyset \in A$       p) ( )  $\{1, 2\} \in A$

5) (UnB) Sejam  $A, B, C$  e  $D$  conjuntos tais que  $(A \cup B) \cap (C \cup D) = \emptyset$ . Observe a tabela abaixo e julgue os itens a seguir:

Conjunto	nº de elementos
$(A - B) \cup (C - D)$	12
$C$	11
$(A \cap B) \cup (C \cap D)$	10
$A \cap B$	4
$A \cup B$	17
$(C - D) \cup (D - C)$	13

a) ( )  $|C - D| = 5$

b) ( )  $|D - C| = 9$

c) ( )  $|C \cup D| = 19$

d) ( )  $|(A - B) \cup (B - A)| = 13$

e) ( )  $|B - A| = 5$

6) Sejam  $A, B \subseteq E$ . Definimos a *diferença simétrica* entre  $A$  e  $B$ , denotado por  $A \triangle B$ , por:

$$A \triangle B := (A - B) \cup (B - A)$$

i) Represente  $A \triangle B$  por meio de Diagramas de Venn.

ii) Mostre que:

- a)  $A \Delta A = \emptyset$ ;
- b)  $A \Delta \emptyset = A$ ;
- c)  $A \Delta B = B \Delta A$ ;
- d)  $A \Delta B = (A \cup B) - (A \cap B)$

7) Determine os seguintes conjuntos:

$$\begin{cases} \mathbb{Z}_+ = \text{conjunto dos inteiros não-negativos} \\ \mathbb{Z}_- = \text{conjunto dos inteiros não-positivos} \end{cases}$$

- a)  $\mathbb{Z}_+ - \mathbb{Z}_- =$
- b)  $\mathbb{Z}_+ \cap \mathbb{Z}_- =$
- c)  $\mathbb{Z}_+ \cup \mathbb{Z}_- =$
- d)  $\mathbb{C}_{\mathbb{R}}(\mathbb{Q}) =$
- e)  $\mathbb{Z} - \mathbb{N} =$
- f)  $\mathbb{C}_{\mathbb{C}}(\mathbb{R}) =$

8) Usando o Princípio de Indução, mostre que:

- a)  $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$ ;
- b)  $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \forall n \in \mathbb{N}$ ;
- c)  $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}, \forall n \in \mathbb{N}$ ;
- d)  $1 + x + x^2 + \cdots + x^{n-1} = \frac{1-x^n}{1-x}, \forall n \in \mathbb{N}, \forall x \in \mathbb{R}, x \neq 1$ ;
- e)  $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}, \forall n \in \mathbb{N}$ ;
- f)  $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}, \forall n \in \mathbb{N}$ ;
- g)  $(1+x)^n \geq 1+nx, \forall n \in \mathbb{N}, \forall x \in \mathbb{R}, x \geq -1$ ;  
(Desigualdade de Bernoulli)
- h)  $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}), \forall n \in \mathbb{N}, n \geq 2$ ;

- i)  $S_n = (n - 2) \cdot 180^\circ$ ,  $\forall n \in \mathbb{N}$ ,  $n \geq 3$ ;  
( $S_n$  = soma das medidas dos ângulos internos de um polígono convexo de  $n$  lados)
  - j)  $d_n = \frac{n(n - 3)}{2}$ ,  $\forall n \in \mathbb{N}$ ,  $n \geq 3$ ;  
( $d_n$  = número de diagonais de um polígono convexo de  $n$  lados)
  - l)  $n! > 2^n$ ,  $\forall n \in \mathbb{N}$ ,  $n \geq 4$ ;
  - m) Se  $A$  é um conjunto finito com  $n$  elementos, então  $A$  possui  $2^n$  subconjuntos. (Equivalente: se  $|A| = n$ , então  $|P(A)| = 2^n$ )
- 9) Sejam  $A, B \subseteq E$ . Mostre que  $A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$ .
- 10) Sejam  $A, B \subseteq E$  tais que  $|A| < \infty$  e  $|B| < \infty$ . Mostre que:
- a) Se  $A \cap B = \emptyset$ , então  $|A \cup B| = |A| + |B|$ ;
  - b) Se  $A \subseteq B$ , então  $|B - A| = |B| - |A|$ ;
  - c)  $|A \cup B| = |A| + |B| - |A \cap B|$

## Relações & Funções

(2ª Lista de Exercícios)

- 1) Determinar todas as relações de equivalência  $R$  sobre o conjunto  $A = \{1, 2, 3\}$  e os respectivos conjuntos-quociente  $A/R$ .
- 2) Dar exemplos de relações  $R$  sobre o conjunto  $A = \{1, 2, 3\}$  tais que:
  - a)  $R$  satisfaz (RE1), (RE2) e (RE3);
  - b)  $R$  satisfaz (RE1), mas não satisfaz (RE2) e nem (RE3);
  - c)  $R$  satisfaz (RE2), mas não satisfaz (RE1) e nem (RE3);
  - d)  $R$  satisfaz (RE3), mas não satisfaz (RE1) e nem (RE2);
  - e)  $R$  satisfaz (RE1) e (RE2), mas não satisfaz (RE3);
  - f)  $R$  satisfaz (RE1) e (RE3), mas não satisfaz (RE2);
  - g)  $R$  satisfaz (RE2) e (RE3), mas não satisfaz (RE1);

Conclusão: são independentes entre si.

3) Explícite a relação dada por  $R = \{(x, y) \in \mathbb{R} \times \mathbb{Z} \mid 9x^2 + 4y^2 = 36\}$ , determinado  $D(R)$  e  $Im(R)$ .

4) Seja  $A = \mathbb{Z} \times \mathbb{Z}^*$  ( $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ ). Para  $(a, b), (c, d) \in A$ , defina:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Mostre que  $\sim$  define uma relação de equivalência sobre  $A$ .

5) Sejam  $A = \mathbb{Z}$  e  $n \in \mathbb{N}$  (fixado). Para  $x, y \in A$ , defina:

$$x \sim y \Leftrightarrow n \mid x - y$$

Mostre que  $\sim$  define uma relação de equivalência sobre  $A$ , chamada de *congruência módulo  $n$*  e denotada por  $x \equiv y \pmod{n}$  (lê-se: “ $x$  é congruente a  $y$ ” (módulo  $n$ )).

6) Sabendo que  $A = \{1, 2, 3\}$  e  $B = \{\square, \triangle\}$ , determine  $\mathcal{F}(A, B)$ ,  $\mathcal{F}(B, A)$ ,  $Sur(A, B)$ ,  $Inv(A, B)$ ,  $S_A = Bij(A, A)$  e  $S_B = Bij(B, B)$ .

7) Mostre que se  $|A| = m$  e  $|B| = n$ , com  $m, n \in \mathbb{N}$ , então  $|\mathcal{F}(A, B)| = n^m$ .

8) Sejam  $A = \mathbb{Z}$  e  $a, b, c \in A$ . Verifique as seguintes propriedades de divisibilidade em  $A$ :

i)  $1 \mid a; a \mid 0; a \mid a;$

ii)  $a \mid b$  e  $b \mid c \Rightarrow a \mid c;$

iii)  $a \mid b$  e  $c \mid d \Rightarrow ac \mid bd;$

iv)  $a \mid b$  e  $a \mid c \Rightarrow a \mid bx + cy, \forall x, y \in A;$

v)  $a \mid b$  e  $b \mid a \Leftrightarrow |a| = |b|;$

vi)  $a \mid b$  e  $b \neq 0 \Rightarrow |a| \leq |b|;$

vii)  $a \mid 1 \Leftrightarrow a = \pm 1; 0 \mid b \Leftrightarrow b = 0;$

Usando i, ii e v, conclua que a relação de divisibilidade em  $A = \mathbb{Z}$  satisfaz as propriedades reflexiva e transitiva, mas não a anti-simétrica. (Portanto, não é uma relação de ordem parcial sobre  $\mathbb{Z}$ .)

9) Seja  $A = \{1, 2, \dots, n\}$ . Denotamos por  $S_A = Bij(A, A) = S_n = \{\sigma : A \rightarrow A \mid \sigma \text{ é bijeção}\}$ . Um elemento  $\sigma \in S_A$  é dito uma *permutação* de  $A$ . Mostre que  $|S_A| = n!$ .

10) Sejam  $E \neq \emptyset$  e  $A = P(E)$ . Para  $\emptyset \neq X, Y \in A$ , defina:

$$X \sim Y \Leftrightarrow \exists f : X \rightarrow Y \text{ bijeção}$$

Mostre que  $\sim$  define uma relação de equivalência sobre  $A$ . (Neste caso, dizemos que  $X$  e  $Y$  são *equipotentes*, ou seja,  $|X| = |Y|$ .)

11) Mostre que  $X$  e  $Y$  são equipotentes nos seguintes casos:

- a)  $X = \mathbb{N}$ ,  $Y = \{y \in \mathbb{N} \mid y \text{ é par}\}$ ;
- b)  $X = \mathbb{Z}$ ;  $Y = \mathbb{N}$ ;
- c)  $X = (0, 1)$ ;  $Y = (a, b)$ ;
- d)  $X = \mathbb{R}$ ;  $Y = \mathbb{R}_+^* = \{y \in \mathbb{R} \mid y > 0\}$
- e)  $X = (-\pi/2, \pi/2)$ ;  $Y = \mathbb{R}$

*Sugestão:*

a) Verifique que

$$\begin{aligned} f : X &\rightarrow Y \\ n &\mapsto f(n) = 2n \end{aligned}$$

é uma bijeção.

b) Verifique que

$$\begin{aligned} f : X &\rightarrow Y \\ n &\mapsto f(n) = \begin{cases} 2n, & \text{se } n > 0 \\ -2n + 1, & \text{se } n \leq 0 \end{cases} \end{aligned}$$

é uma bijeção.

c) Verifique que

$$\begin{aligned} f : X &\rightarrow Y \\ x &\mapsto f(x) = (b - a)x + a \end{aligned}$$

é uma bijeção.

d) e e): Lembre-se de duas funções estudadas em Cálculo 1.

- 12) Seja  $A = \mathbb{N} \times \mathbb{N}$ , onde  $\mathbb{N}$  está munido de sua ordem natural  $\leq$ . Para  $(a, b), (c, d) \in A$ , defina:

$$(a, b) R (c, d) \Leftrightarrow a < c \text{ ou } a = c \text{ e } b \leq d$$

(ordem lexicográfica). Mostre que  $R$  define uma relação de ordem total sobre  $A$ .

- 13) Seja  $f : A \rightarrow B$  uma função, onde  $A, B \neq \emptyset$ . Para  $x, x' \in A$ , defina:

$$x \sim x' \Leftrightarrow f(x) = f(x')$$

Verifique que  $\sim$  define uma relação de equivalência sobre  $A$  ( $\sim$  é a *relação de equivalência induzida* por  $f$ ).

## Operações Binárias

(3ª Lista de Exercícios)

- 1) Seja  $A \neq \emptyset$  munido de uma operação binária  $*$  associativa e com elemento neutro  $e$ . Considere  $\mathcal{U}_*(A) = \{x \in A \mid x \text{ é inversível}\}$  e  $\mathcal{R}_*(A) = \{x \in A \mid x \text{ é regular}\}$ . Verifique que:

- $\mathcal{U}_*(A) \neq \emptyset$  e  $\mathcal{R}_*(A) \neq \emptyset$ ;
- Se  $x \in \mathcal{U}_*(A)$ , então  $x' \in \mathcal{U}_*(A)$ . Neste caso,  $(x')' = x$ ;
- Se  $x, y \in \mathcal{U}_*(A)$ , então  $x * y \in \mathcal{U}_*(A)$ . Neste caso,  $(x * y)' = y' * x'$ ;
- $\mathcal{U}_*(A) \subseteq \mathcal{R}_*(A)$ .

- 2) Diga quais dos seguintes subconjuntos de  $\mathbb{Z}$  são fechados para as operações de adição e de multiplicação:

- $\mathbb{Z}_- = \{x \in \mathbb{Z} \mid x \leq 0\}$
- $P = \{x \in \mathbb{Z} \mid x \text{ é par}\}$
- $I = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$
- $n\mathbb{Z} = \{x \in \mathbb{Z} \mid x = nk, k \in \mathbb{Z}\}$  (conjunto dos múltiplos de  $n$ ,  $n \in \mathbb{N}$ )

- 3) Considere  $A = P(\{a, b\})$  munido de uma operação  $*$ , onde  $X * Y = X \cap Y$ . Verifique, usando a tabela de operação, se  $*$  é comutativa, se existe elemento neutro e quais são os elementos simetrizáveis.

- 4) Determine o número de operações binárias que se pode construir sobre um conjunto finito  $A$  com  $n$  elementos ( $n \in \mathbb{N}$ ).
- 5) Construa a tabela de uma operação  $*$  sobre  $A = \{a, b, c, d\}$  de modo que  $*$  seja comutativa,  $a$  seja elemento neutro,  $\mathcal{U}_*(A) = A$ ,  $\mathcal{R}_*(A) = A$  e  $b * c = a$ .
- 6) Construa a tabela de uma operação  $*$  sobre  $A = \{e, a, b, c\}$  de modo que  $*$  seja comutativa,  $e$  seja elemento neutro,  $x * a = a$  ( $\forall x \in A$ ) e  $\mathcal{R}_*(A) = A - \{a\}$ .
- 7) Considere  $A = \mathbb{Z}$  e  $*$   $= \div$ . Explique de duas maneiras distintas a razão pela qual  $*$  não é uma operação binária sobre  $A$ .
- 8) Considere  $A = \mathbb{R}$  munido de uma operação binária  $*$ , onde  $x * y = y$ ,  $\forall x, y \in A$ . Verifique se  $*$  é associativa, comutativa e se possui elemento neutro à esquerda, à direita e bilateral.
- 9) Considere  $E = \{1, 2, 3\}$  e  $A = S_3 = \{f : E \rightarrow E \mid f \text{ é bijeção}\}$ . Construa a tabela de  $A$  com relação à operação de composição de funções, verificando se a mesma é comutativa, se existe elemento neutro, quais elementos são inversíveis e quais são regulares.
- 10) Determine todos os elementos neutros à esquerda no conjunto

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

para a operação de multiplicação.

- 11) Sejam  $A \neq \emptyset$  munido de uma operação binária  $*$  e  $a \in A$ . Considere

$$\begin{array}{ll} \lambda_a : A \rightarrow A & \text{e} \quad \xi_a : A \rightarrow A \\ x \mapsto \lambda_a(x) = a * x & x \mapsto \xi_a(x) = x * a \end{array}$$

Verifique que:

- a)  $a$  é regular à esquerda  $\Leftrightarrow \lambda_a$  é injetora;
- b)  $a$  é regular à direita  $\Leftrightarrow \xi_a$  é injetora.

## Homomorfismos & Polinômios

(4ª Lista de Exercícios)

- 1) Para  $n, k \in \mathbb{Z}_+$ , com  $n \geq k \geq 0$ , definimos o coeficiente binomial  $\binom{n}{k}$  por  $n!/k!(n-k)!$ , onde

$$n! = \begin{cases} n \cdot (n-1) \cdot \dots \cdot 3 \cdot 2 \cdot 1 & , \text{ se } n \in \mathbb{N}; \\ 1 & , \text{ se } n = 0 \end{cases}$$

- a) Demonstre, usando a definição de coeficiente binomial, a Relação de Stiffel:

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \quad (n, k \in \mathbb{Z}_+; \ n \geq k \geq 1)$$

- b) Seja  $A$  um anel comutativo com identidade. Usando a) e indução sobre  $n$ , mostre que é válido o desenvolvimento binomial em  $A$ :

$$(a+b)^n = \begin{cases} \sum_{k=0}^n \binom{n}{k} a^k \cdot b^{n-k} \\ \text{ou} \\ \sum_{k=0}^n \binom{n}{k} a^{n-k} \cdot b^k \end{cases}, \quad \forall a, b \in A, \quad \forall n \in \mathbb{N}$$

- 2) Mostre que:

- a)  $f$  é um monomorfismo de anéis

$$\begin{aligned} f: \quad \mathbb{C} &\rightarrow \mathcal{M}_{2 \times 2}(\mathbb{R}) \\ a+bi &\mapsto f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{aligned}$$

- b)  $g$  é um automorfismo de anéis

$$\begin{aligned} g: \quad \mathbb{C} &\rightarrow \mathbb{C} \\ a+bi &\mapsto g(a+bi) = a-bi \end{aligned}$$

- c)  $h$  não é um homomorfismo de anéis

$$\begin{aligned} h: \quad \mathcal{M}_{2 \times 2}(\mathbb{R}) &\rightarrow \mathcal{M}_{2 \times 2}(\mathbb{R}) \\ \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_A &\mapsto h\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \underbrace{\begin{pmatrix} a & c \\ b & a \end{pmatrix}}_{\text{transposta de } A} \end{aligned}$$



- 3) Seja  $A$  um domínio de integridade. Determine  $\mathcal{U}(A[X])$ .
- 4) Calcule o quociente e o resto da divisão de  $f(X)$  por  $g(X)$  para os seguintes pares de polinômios:
- i)  $f(X) = 3X^5 + 4X^3 + 2X + 5$ ;  $g(X) = 2X^3 - 3X^2 + 7$  em  $\mathbb{Q}[X]$ ;
  - ii)  $f(X) = -X^6 + 12X^4 + 8X^3 - 4X + 10$ ;  $g(X) = X^3 - 3$  em  $\mathbb{Z}[X]$ ;
  - iii)  $f(X) = \bar{4}X^5 + \bar{3}X^3 - \bar{4}X^2 - \bar{2}X + \bar{3}$ ;  $g(X) = \bar{3}X^2 - \bar{1}X - \bar{2}$  em  $\mathbb{Z}_7[X]$ .
- 5) Seja  $f(X) = a_nX^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$ , onde  $\text{gr}(f) = n \geq 1$ .
- a) Mostre que se  $r/s \in \mathbb{Q}$  é raiz de  $f(X)$ , com  $\text{mdc}(r, s) = 1$ , então  $r \mid a_0$  e  $s \mid a_n$ .
  - b) Conclua que se  $r/s \in \mathbb{Q}$  é raiz de  $f(X)$ , com  $\text{mdc}(r, s) = 1$ , e  $a_n \in \mathcal{U}(\mathbb{Z})$ , então tal raiz é inteira.
- 6) Seja  $A$  um domínio de integridade e considere  $f(X) = a_nX^n + \dots + a_2X^2 + a_1X + a_0 \in A[X]$ . Definimos a “derivada formal” de  $f(X)$  por:

$$f'(X) := na_nX^{n-1} + \dots + 2a_2X + a_1 \in A[X]$$

Mostre que: (Regras de Derivação)

- a)  $(a \cdot f)' = a \cdot f'$ ;
- b)  $(f + g)' = f' + g'$ ;
- c)  $(f \cdot g)' = f' \cdot g + f \cdot g'$ ;
- d)  $(f^n)' = nf^{n-1} \cdot f'$ .

$(n \in \mathbb{N}; f, g \in A[X]; a \in A)$

- 7) Seja  $K$  um corpo.  $K$  é dito “algebricamente fechado” se  $\forall f(X) \in K[X]$ , com  $\text{gr}(f) \geq 1$ ,  $\exists \alpha \in K \mid f(\alpha) = 0$ . Mostre que  $\mathbb{R}$  não é algebricamente fechado.
- 8) a) Mostre que o polinômio  $f(X) = X^2 - \bar{1}$  possui quatro raízes no anel  $\mathbb{Z}_{15}$ .

- b) Comente o fato do polinômio  $f$  acima ter um número de raízes maior que o grau.
- 9) Sejam  $K$  um corpo infinito e  $f(X), g(X) \in K[X]$ . Mostre que  $f = g \Leftrightarrow \hat{f} = \hat{g}$  (isto é, dois polinômios com coeficientes num corpo infinito são iguais se, e somente se, eles induzem a mesma função polinomial).
- 10) a) Mostre que o polinômio  $f(X) = X^2$  possui infinitas raízes no anel  $\mathcal{M}_{2 \times 2}(\mathbb{R})$ .
- b) Comente o fato do polinômio  $f$  acima ter um número de raízes maior que o grau.
- 11) Considere  $f(X) = X^2 - X \in A[X]$ , onde  $A$  é um domínio de integridade. Mostre que as únicas raízes de  $f$  em  $A$  são 0 e 1.
- 12) Mostre que todo polinômio sobre  $\mathbb{R}$  de grau ímpar possui pelo menos uma raiz real.
- 13) Sejam  $K = \mathbb{C}$  e  $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$ , onde  $\text{gr}(f) = n \geq 1$ . Mostre que  $f$  pode ser fatorada da seguinte maneira:
- $$f(X) = a_n (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n),$$
- onde  $\alpha_1, \dots, \alpha_n \in K$  são as raízes de  $f(X)$  (não necessariamente distintas).
- 14) Calcule a soma e o produto de  $f(X) = \overline{2}X^3 + \overline{4}X^2 + \overline{3}X + 3$  e  $g(X) = \overline{3}X^4 + \overline{2}X + \overline{4}$  sobre  $\mathbb{Z}_5$  e sobre  $\mathbb{Z}_7$ .
- 15) Calcule  $q(x)$  e  $r(x)$  tais que  $f(x) = g(x)q(x) + r(x)$ , onde  $r(x) = 0$  ou  $\text{gr}(r) < \text{gr}(g)$ :
- a)  $f(x) = x^5 - x^3 + 3x - 5$ ;  $g(x) = x^2 + 7 \in \mathbb{Q}[x]$
- b)  $f(x) = x^5 - x^3 + 3x - 5$ ;  $g(x) = x - 2 \in \mathbb{Q}[x]$
- c)  $f(x) = x^5 - x^3 + \overline{3}x - \overline{5}$ ;  $g(x) = \overline{1}x + \overline{2} \in \mathbb{Z}_5[x]$
- d)  $f(x) = x^5 - x^3 + \overline{3}x - \overline{5}$ ;  $g(x) = x^3 + x - \overline{1} \in \mathbb{Z}_3[x]$

- 16) Seja  $K$  um corpo, onde  $K \subseteq \mathbb{C}$ . Sejam  $f(X) \in K[X] - \{0\}$ , com  $\text{gr}(f) = n \geq 1$ , e  $\alpha \in \mathbb{C}$  uma raiz de  $f(X)$ . Então:

$$\alpha \text{ é raiz simples de } f(X) \Leftrightarrow f(\alpha) = 0 \text{ e } f'(\alpha) \neq 0$$

(Equivalentemente:  $\alpha$  é raiz de  $f(X)$  de multiplicidade  $\geq 2 \Leftrightarrow f(\alpha) = 0$  e  $f'(\alpha) = 0$ )

- 17) Liste todos os polinômios de grau  $\leq 3$  em  $\mathbb{Z}_2[X]$  e todos os de grau  $\leq 2$  em  $\mathbb{Z}_3[X]$  (incluindo o polinômio identicamente nulo).
- 18) Sejam  $(G, \cdot)$  um grupo e  $g \in G$ . Defina

$$\begin{aligned} \psi_g : G &\rightarrow G \\ x &\mapsto \psi_g(x) = g^{-1}xg \end{aligned}$$

Mostre que  $\psi_g$  é um automorfismo de  $G$ .

- 19) Calcule o MDC em  $\mathbb{Q}[X]$  entre os seguintes polinômios:

- a)  $f(x) = x^4 + x^3 + 2x^2 + x + 1$ ;  $g(x) = x^3 + 4x^2 + 4x + 3$   
b)  $f(x) = 4x^5 + 7x^3 + 2x^2 + 1$ ;  $g(x) = 3x^3 + x + 1$   
c)  $f(x) = x^4 + x^3 + 2x^2 + 3x + 1$ ;  $g(x) = x^4 + x^3 - 2x^2 - x + 1$

- 20) a) Sejam  $A = \mathbb{Z}_2$  e  $f(X) = \bar{1} + X + X^3 \in \mathbb{Z}_2[X]$ . Determine  $g(X) \in \mathbb{Z}_2[X]$ ,  $g(X) \neq f(X)$ , tal que  $\hat{g} = \hat{f}$ .
- b) Sejam  $A = \mathbb{Z}_3$  e  $f(X) = X$ ,  $g(X) = X^3$ ,  $h(X) = X + 5X^3 + X^9 \in \mathbb{Z}_3[X]$ . Mostre que  $\hat{f} = \hat{g} = \hat{h}$ .

- 21) Verifique em cada caso se  $f$  é um homomorfismo de grupos:

- a)  $f : (\mathbb{Z}, +) \rightarrow (\mathbb{C}^*, \cdot)$   
 $n \mapsto f(n) = i^n$
- b)  $f : (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}_+^*, \cdot)$   
 $z \mapsto f(z) = |z|$
- c)  $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$   
 $n \mapsto f(n) = kn \quad (k \in \mathbb{Z} \text{ dado})$
- d)  $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$   
 $x \mapsto f(x) = x + 1$

$$\begin{array}{lcl} \text{e)} & f : (\mathbb{C}^*, \cdot) & \rightarrow (\mathbb{C}^*, \cdot) \\ & z & \mapsto f(z) = \bar{z} \end{array}$$

22) Verifique em cada caso se  $f$  é um homomorfismo de anéis:

$$\begin{array}{lcl} \text{a)} & f : \mathbb{C} & \rightarrow \mathbb{C} \\ & (a + bi) & \mapsto f(a + bi) = a - bi \end{array}$$

$$\begin{array}{lcl} \text{b)} & f : \mathbb{Z} & \rightarrow \mathbb{Z} \\ & x & \mapsto f(x) = x + 1 \end{array}$$

$$\begin{array}{lcl} \text{c)} & f : \mathbb{Z} & \rightarrow \mathbb{Z} \\ & x & \mapsto f(x) = 2x \end{array}$$

$$\begin{array}{lcl} \text{d)} & f : \mathbb{Z} & \rightarrow \mathbb{Z}_n \\ & x & \mapsto f(x) = \bar{x} \end{array}$$

$$\begin{array}{lcl} \text{e)} & f : \mathbb{Z} & \rightarrow \mathbb{Z} \\ & x & \mapsto f(x) = -x \end{array}$$