

# Resumo das aulas de discreta

Jair Donadelli

19 de abril de 2017

## Sumário

<b>1ª Semana — Lógica</b>	<b>5</b>
1.1 Operadores lógicos: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$	7
1.2 Tautologia e Contradição	9
1.3 Equivalência lógica	10
1.4 Implicação lógica	12
1.5 Predicados	13
1.6 Quantificadores	14
1.7 Distribuição de quantificadores	16
1.8 Negação de quantificadores	17
1.9 Múltiplos quantificadores	17
1.10 Regras de Inferência e Argumentos válidos	18
<b>2ª Semana — Demonstrações</b>	<b>24</b>

2.1	Prova direta de implicação . . . . .	25
2.2	Prova indireta de implicação . . . . .	27
2.3	Prova de equivalências . . . . .	30
2.4	Mais provas por contradição . . . . .	30
2.5	Prova por casos . . . . .	32
2.6	Provas existenciais . . . . .	33
<b>3<sup>a</sup></b>	<b>Semana — Indução</b>	<b>36</b>
3.1	Princípio da Boa Ordem (PBO) . . . . .	36
3.2	Princípios de indução . . . . .	37
3.3	Equivalência . . . . .	40
3.4	Provas por indução . . . . .	41
3.5	Definições recursivas . . . . .	44
<b>4<sup>a</sup></b>	<b>Semana — Avaliação</b>	<b>46</b>
4.1	Matutino . . . . .	46
4.2	Noturno . . . . .	47
<b>5<sup>a</sup></b>	<b>Semana — Conjuntos</b>	<b>50</b>
5.1	Abordagem intuitiva . . . . .	50
5.2	Provando proposições de conjuntos . . . . .	53
5.3	Operações sobre conjuntos . . . . .	53
5.4	Conjunto das partes . . . . .	56

5.5	Axiomática de ZFC . . . . .	57
5.6	Par ordenado e Produto cartesiano . . . . .	59
<b>6<sup>a</sup></b>	<b>Semana — Relações</b>	<b>62</b>
6.1	Composição e inversa . . . . .	62
6.2	Classificação de relações . . . . .	63
6.3	Relações de equivalência . . . . .	64
6.4	Relações de ordem . . . . .	67
<b>7<sup>a</sup></b>	<b>Semana — Contagem</b>	<b>71</b>
7.1	Bijeções . . . . .	71
7.2	Conjuntos finitos . . . . .	72
7.3	Conjuntos infinitos . . . . .	74
7.4	Conjuntos enumeráveis . . . . .	78
<b>8<sup>a</sup></b>	<b>Semana — Avaliação</b>	<b>80</b>
<b>9<sup>a</sup></b>	<b>Semana — Combinatória</b>	<b>82</b>
9.1	Arranjos . . . . .	86
9.2	Combinações . . . . .	91
9.3	Binômio de Newton . . . . .	95
<b>10<sup>a</sup></b>	<b>Semana — Funções geradoras</b>	<b>97</b>
10.1	Sobre convergência (opcional) . . . . .	100

10.2 Expansão de funções de geradoras . . . . .	104
---	-----

# 1 Elementos de lógica de 1ª ordem

Os lógicos contemporâneos

1. constroem *linguagens simbólicas*, rigorosas e livres de ambiguidades e de contexto, adequadas para lidar com a relação de consequência. As linguagens possuem duas dimensões relevantes:
  - a *sintática*: os símbolos da linguagem e as regras de combinação às quais estão sujeitos para a construção dos termos e fórmulas;
  - a *semântica* define precisamente o significado das fórmulas.
2. especificam os axiomas dentre as fórmulas bem formadas;
3. especificam as regras de inferência que independem da semântica.

E assim temos uma LÓGICA.

*Por que precisamos criar uma linguagem para formalizar as formas de raciocínio?*  
Para evitar os paradoxos e imprecisões da linguagem natural. Importante quando estudamos assuntos mais restritos, com menos complexidade, porém com maior exigência de rigor. A seguir daremos um esboço da lógica de primeira ordem, a qual tem poder expressivo suficiente para formalizar praticamente toda a matemática.

O que veremos a seguir são tópicos de lógica de predicados de primeira ordem apresentados de modo não formal.

**Definição 1.** Uma *proposição* é uma sentença que assume um de dois valores: *VERDADEIRO* ( $V$ ) ou *FALSO* ( $F$ ). O valor é chamado de *valor-verdade* ou *valor-lógico* da proposição.

Não é necessário sabermos se a sentença é verdadeira ou falsa.

Exemplos:

1. O time joga bem.
2. O time ganhou o campeonato.

3. O técnico é o culpado.
4. Os torcedores estão felizes.
5. O Sr. Temer está feliz.
6. A Sra. Temer não está feliz.
7. O suborno será pago.
8. As mercadorias são entregues.
9.  $1 + 1 = 2$ .
10.  $3 > 5$ .

Do ponto de vista da linguagem natural é bastante restritivo.

Mas, estamos mais interessado nos enunciados matemáticos

11. Uma sequência limitada é convergente
12. 27 é um quadrado perfeito
13. O conjunto vazio é único

onde sentenças interrogativas ou imperativas não são importantes. Não são proposições:

1.  $x^2$  é positivo.
2.  $x$  é a soma de quatro quadrados perfeitos.
3. essa frase é falsa.
4. vá estudar discreta.
5. hoje tem festa?

## 1.1 Operadores lógicos: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

Toda linguagem permite construir proposições mais complexas a partir de outras.

1. Os torcedores estão felizes **e** o técnico foi demitido.
2. Samuel virá para a festa **e** Maximiliano não virá, **ou** Samuel não virá para a festa **e** Maximiliano vai se divertir.
3. **Se** o time joga bem, **então** o time ganha o campeonato.
4. **Se** o time não joga bem, **então** o técnico é o culpado.
5. **Se** o time ganha o campeonato **então** os torcedores estão felizes.
6. O suborno será pago **se, e somente se**, as mercadorias são entregues.
7. 27 **não** é um quadrado perfeito.
8. O conjunto vazio **não** é único.
9. Os torcedores **não** estão felizes.

Uma proposição que não pode ser decomposta em proposições ligadas pelos *conectivos lógicos* “e”, “ou”, “se...então”, “se, e só se” é uma *proposição atômica*.

O valor lógico de uma proposição depende do valor lógico das proposições atômicas que a compõem, e da maneira como elas são combinadas pelos conectivos, de acordo com as regras abaixo. Sejam  $A$  e  $B$  proposições

**Definição 2.** A *negação* de  $A$  é a proposição  $\neg(A)$  cujo valor-verdade é

$A$	$\neg(A)$
$V$	$F$
$F$	$V$

**Definição 3.** A *disjunção* de  $A$  e  $B$  é a proposição  $A \vee B$  cujo valor-verdade é

$A$	$B$	$A \vee B$
$V$	$V$	$V$
$V$	$F$	$V$
$F$	$V$	$V$
$F$	$F$	$F$

**Definição 4.** A *conjunção* de  $A$  e  $B$  é a proposição  $A \wedge B$  cujo valor-verdade é

$A$	$B$	$A \wedge B$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$F$
$F$	$F$	$F$

	$A$	$B$	$A \rightarrow B$
	$V$	$V$	$V$
Definição 4. A <i>implicação</i> é a proposição $A \rightarrow B$ cujo valor-verdade é	$V$	$F$	$F$
	$F$	$V$	$V$
	$F$	$F$	$V$

**Exemplo:**

Se a lua é verde então o sol é quadrado,

é uma implicação verdadeira.

A implicação

- não pressupõe relação causa/efeito: se chove então o rio transborda.
- Não deve ser entendido como equivalência: Se não comer a refeição então não ganha a sobremesa.

A *recíproca* de  $A \rightarrow B$  é  $B \rightarrow A$ . Observe que há casos em que  $A \rightarrow B$  tem valor lógico diferente de  $B \rightarrow A$ .

A *contrapositiva* de  $A \rightarrow B$  é  $\neg(B) \rightarrow \neg(A)$ . Pode-se verificar que contrapositiva tem sempre o mesmo valor lógico que a proposição que a originou.

A implicação é um dos mais importantes conectivos da matemática, muitos teoremas são escritos na forma de implicações: se  $A$  (hipótese, premissa ou antecedente) é verdadeira, então  $B$  (tese, conclusão ou consequente) é verdadeira. Em português, a implicação pode ser expressa de muitas formas:

- se  $A$  então  $B$ .
- quando  $A$ , temos  $B$ .
- sempre que  $A$ , temos  $B$ .
- $B$  sempre que  $A$ .
- $B$  se  $A$ .



- $A$  é suficiente para  $B$ .
- $A$  é uma mais forte que  $B$ .
- se não  $B$ , então não  $A$ .
- se  $B$  não vale, então  $A$  não vale.
- não  $A$  se não  $B$ .
- $A$  é falsa sempre que  $B$  é falsa.
- $B$  é mais fraco que  $A$ .
- $B$  é necessário para  $A$ .

	$A$	$B$	$A \leftrightarrow B$
	$V$	$V$	$V$
	$V$	$F$	$F$
	$F$	$V$	$F$
	$F$	$F$	$V$

**Definição 5.** A *bicondicional* é a proposição  $A \leftrightarrow B$  cujo valor-verdade é

O conectivo lógico “se e somente se” também pode ser expresso de várias maneiras

- $A$  é condição necessária e suficiente para  $B$ .
- $A$  e  $B$  são equivalentes.
- se  $A$  então  $B$ , e se  $B$  então  $A$ .

As vezes usamos a abreviação “ $A$  sse  $B$ ”.

## 1.2 Tautologia e Contradição

**Definição 6.** Uma *tautologia* é uma proposição composta que é sempre verdadeira. Uma *contradição* é uma proposição composta que é sempre falsa.

Por exemplo  $A \vee \neg(A)$  e  $(A \rightarrow B) \leftrightarrow (\neg(A) \vee B)$  são tautologias e  $A \wedge \neg(A)$  é uma contradição.

Uma tautologia qualquer é denotada por **V** e uma contradição qualquer por **F**.

### 1.3 Equivalência lógica

**Definição 7.** Duas proposições  $A$  e  $B$  são *logicamente equivalentes* se assumem o mesmo valor-verdade. A notação é  $A \Leftrightarrow B$ .

$A \Leftrightarrow B$  é o mesmo que dizer que  $A \leftrightarrow B$  é tautologia.

Por exemplo  $(A \rightarrow B) \Leftrightarrow (\neg(A) \vee B)$  e  $(A \leftrightarrow B) \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$ .

**Teorema 1.** Sejam  $A, B, C$  proposições.

*1. Leis de identidade*

$$A \wedge \mathbf{V} \Leftrightarrow A \quad (1)$$

$$A \vee \mathbf{F} \Leftrightarrow A \quad (2)$$

*2. Leis de dominação*

$$A \vee \mathbf{V} \Leftrightarrow \mathbf{V} \quad (3)$$

$$A \wedge \mathbf{F} \Leftrightarrow \mathbf{F} \quad (4)$$

*3. Leis de idempotência*

$$A \wedge A \Leftrightarrow A \quad (5)$$

$$A \vee A \Leftrightarrow A \quad (6)$$

*4. Lei da dupla negação  $\neg(\neg(A)) \Leftrightarrow A$ .*

*5. Leis distributivas*

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C) \quad (7)$$

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \quad (8)$$

*6. Leis comutativas*

$$A \vee B \Leftrightarrow B \vee A \quad (9)$$

$$A \wedge B \Leftrightarrow B \wedge A \quad (10)$$

**7. Leis de associativas**

$$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C \quad (11)$$

$$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C \quad (12)$$

**8. Leis de De Morgan**

$$\neg(A \vee B) \Leftrightarrow \neg(A) \wedge \neg(B) \quad (13)$$

$$\neg(A \wedge B) \Leftrightarrow \neg(A) \vee \neg(B) \quad (14)$$

**9. Contrapositiva**  $A \rightarrow B \Leftrightarrow \neg(B) \rightarrow \neg(A)$ .

**10. Redução ao absurdo**  $A \rightarrow B \Leftrightarrow (A \wedge \neg(B)) \rightarrow \mathbf{F}$ .

**11. Leis de absorção**

$$A \vee (A \wedge B) \Leftrightarrow A \quad (15)$$

$$A \wedge (A \vee B) \Leftrightarrow A \quad (16)$$

**12. Leis de inversa**

$$A \vee \neg(A) \Leftrightarrow \mathbf{V} \quad (17)$$

$$A \wedge \neg(A) \Leftrightarrow \mathbf{F} \quad (18)$$

*Demonstração.* Exercício. □

**Exercício 1.** Verifique usando as leis acima que  $(A \vee B) \wedge \neg(\neg(A) \wedge B)$  é logicamente equivalente a  $A$ .

*Resolução.*

$$\begin{array}{ll} (A \vee B) \wedge \neg(\neg(A) \wedge B) & \text{motivo} \\ \Leftrightarrow (A \vee B) \wedge (\neg\neg(A) \vee \neg(B)) & \text{De Morgan} \\ \Leftrightarrow (A \vee B) \wedge (A \vee \neg(B)) & \text{dupla negação} \\ \Leftrightarrow (A \vee (B \wedge \neg(B))) & \text{distributiva} \\ \Leftrightarrow (A \vee \mathbf{F}) & \text{inversa} \\ \Leftrightarrow A & \text{identidade} \end{array}$$

□

**Exercício 2.** Verifique que  $\neg(A \rightarrow B) \Leftrightarrow A \wedge \neg(B)$ .

## 1.4 Implicação lógica

Sejam  $A$  e  $B$  proposições.

**Definição 8.** Dizemos que  $A$  *implica logicamente*  $B$  se  $A \rightarrow B$  é uma tautologia e escrevemos  $A \Rightarrow B$ . Nesse caso, dizemos também que  $B$  é uma *consequência lógica* de  $A$ .

Mais geralmente, sejam  $P_1, P_2, \dots, P_n$  e  $Q$  proposições. Dizemos que essas proposições  $P_1, P_2, \dots, P_n$  *implicam logicamente*  $Q$  se  $P_1 \wedge P_2 \wedge \dots \wedge P_n \rightarrow Q$  é uma tautologia e escrevemos  $P_1 \wedge P_2 \wedge \dots \wedge P_n \Rightarrow Q$ .

Por exemplo, se  $A \rightarrow B$  é verdadeira, sua conclusão  $B$  pode ser verdadeira ou falsa; mas se tanto a implicação quanto a hipótese  $A$  são verdadeiras, então a conclusão  $B$  deve ser verdadeira, isto é

$$A \wedge (A \rightarrow B) \Rightarrow B.$$

Notemos que se  $A \Leftrightarrow B$  então  $A \leftrightarrow B$  é tautologia, portanto,  $A \rightarrow B$  é tautologia e  $B \rightarrow A$  é tautologia, ou seja  $A \Rightarrow B$  e  $B \Rightarrow A$ . Reciprocamente, se  $A \Rightarrow B$  e  $B \Rightarrow A$  então  $A \rightarrow B$  é tautologia e  $B \rightarrow A$  é tautologia, ou seja,  $A \leftrightarrow B$  é tautologia, logo  $A \Leftrightarrow B$ .

**Exercício 3.** Considere as proposições

$A$  é “Mané estuda”

$B$  é “Mané joga futebol”

$C$  é “Mané passa em discreta”

Então  $A \rightarrow C$ ,  $\neg(B) \rightarrow A$ ,  $\neg(C)$  implicam logicamente  $B$ .

**Teorema 2.** Sejam  $A, B, C$  proposições arbitrárias.

1. **Lei da adição:**  $A \Rightarrow A \vee B$ .
2. **Lei da simplificação:**  $A \wedge B \Rightarrow A$ .
3. **Lei do modus ponens:**  $A \wedge (A \rightarrow B) \Rightarrow B$ .
4. **Lei do modus tollens:**  $(A \rightarrow B) \wedge \neg(B) \Rightarrow \neg(A)$ .

5. *Silogismo hipotético*:  $(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow A \rightarrow C$ .

6. *Silogismo disjuntivo*:  $(A \vee B) \wedge \neg(A) \Rightarrow B$ .

7. *Demonstração por absurdo*:  $A \rightarrow \mathbf{F} \Rightarrow \neg(A)$ .

*Demonstração.* Exercício.

□

No exercício 3

1.	$A \rightarrow C$	premissa
2.	$\neg C$	premissa
3.	$\neg(B) \rightarrow A$	premissa
4.	$\neg C \rightarrow \neg A$	contrapositiva de 1
5.	$\neg A$	Modus ponens de 2 e 4
6.	$\neg(A) \rightarrow \neg(\neg B)$	contrapositiva de 3
7.	$\neg(\neg B)$	modus ponens de 5 e 6
8.	$B$	dupla negação

A partir da linha 4, cada linha é consequência lógica das linhas anteriores, portanto,  $B$  é consequência lógica das premissas.

## 1.5 Predicados

**Definição 9.** Uma *sentença aberta* é uma sentença parametrizada por uma ou mais variáveis. Uma sentença aberta não tem valor lógico.

Por exemplo, são predicados

$$P(x): x \leq x^2.$$

$$Q(x, y): x \leq y^2.$$

O nome “predicado” vem da analogia com a gramática usual, onde  $x$  “faz o papel de sujeito” da afirmação. O símbolo  $x$  recebe o nome de *variável livre* do predicado  $P$ .

Pra nós, intuitivamente, cada variável está associada a um domínio não-vazio de onde empresta valores e sempre que substituirmos as variáveis de uma proposição aberta por valores do seu domínio, obtemos uma proposição fechada, que não depende de nenhuma variável e que portanto *pode ser tratada como uma proposição atômica do cálculo proposicional*.

Por exemplo,  $R(x, y) : x > y$  é uma proposição verdadeira se os valores de  $x$  e  $y$  forem 7 e 4 (i.e.,  $R(4, 7)$  é verdadeiro), mas é falsa se os valores forem 1 e 2 (i.e.,  $R(1, 2)$  é falso).

Usaremos letras minúsculas  $x, y, z, \dots$  para denotar variáveis, letras maiúsculas  $P, Q, R, \dots$  para os predicados as quais são seguidas por uma lista de variáveis entre parênteses para denotar que a proposição aberta depende dessas variáveis. Como em Funções, dado um predicado  $P(x_1, x_2, \dots, x_n)$ , usamos a notação  $P(v_1, v_2, \dots, v_n)$  para indicar a substituição da variável  $x_i$  valor  $v_i$ , para  $i = 1, 2, \dots, n$ . Supõe-se que todas as ocorrências da mesma variável na proposição são substituídas pelo mesmo valor.

Podemos combinar predicados, da mesma maneira que nós fizemos com as proposições, usando os operadores lógicos  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$  para formar predicados mais complexos.

A substituição de variáveis por valores do domínio não é a única maneira de transformar uma proposição aberta em uma proposição atômica. Outra maneira é a chamada *quantificação*. A quantificação permite expressar conceitos como “Todos os elementos de D” ou “alguns elementos de D”. O primeiro é chamado quantificação universal e segundo de quantificação existencial.

## 1.6 Quantificadores

**Definição 10.** A *quantificação universal* de  $P(x)$  é a proposição

para todo  $x$ ,  $P(x)$  também denotada por  $\forall x, P(x)$

que é verdadeira se  $P(x)$  é verdadeiro para toda instanciación de  $x$  com valores de um domínio  $D \neq \emptyset$ . Caso  $P(x)$  seja falsa para um ou mais valores atribuídos a  $x$  então a proposição para todo  $x \in D$ ,  $P(x)$  é falsa.

Por exemplo,

para todo  $x \in \mathbb{Z}$ ,  $x < x + 1$

é verdadeira enquanto que

para todo  $x \in \mathbb{N}$ ,  $x$  é primo

é falsa pois  $4 \in \mathbb{N}$  e 4 não é primo. Dizemos que 4 é um **contraexemplo** para  $\forall x \in \mathbb{N}$ ,  $x$  é primo.

As vezes quantificadores estão implícitos, por exemplo, no domínio dos reais a afirmação

*se um número é inteiro, então é racional*

é uma proposição implicitamente quantificada

$$\forall x \in \mathbb{R}, (x \in \mathbb{Z} \rightarrow x \in \mathbb{Q})$$

assim como  $\sin^2(x) + \cos^2(x) = 1$  expressa

$$\forall x \in \mathbb{R}, \sin^2(x) + \cos^2(x) = 1.$$

Se o domínio  $D$  é um conjunto finito, digamos  $D = \{v_1, v_2, \dots, v_n\}$ , então  $\forall x \in D$ ,  $P(x)$  equivale logicamente a  $P(v_1) \wedge P(v_2) \wedge \dots \wedge P(v_n)$ , i.e.,

$$(\forall x \in \{v_1, v_2, \dots, v_n\}, P(x)) \Leftrightarrow (P(v_1) \wedge P(v_2) \wedge \dots \wedge P(v_n)).$$

**Definição 11.** A **quantificação existencial** da proposição aberta  $P(x)$  é a proposição

existe  $x$ ,  $P(x)$  também denotada por  $\exists x, P(x)$

que é verdadeira se  $P(x)$  é verdadeiro para pelo menos uma instanciiação de  $x$  com valores de  $D \neq \emptyset$ . Caso  $P(x)$  seja falsa para todos os valores de  $D$  atribuídos a  $x$  então a proposição para todo  $x \in D$ ,  $P(x)$  é falsa.

Por exemplo,

$$\text{existe } x \in \mathbb{Z}, x = x + 1$$

é falsa enquanto que

$$\text{existe } x \in \mathbb{N}, x \text{ é primo}$$

é verdadeira.

Se o domínio  $D$  é um conjunto finito, digamos  $D = \{v_1, v_2, \dots, v_n\}$ , então  $\exists x \in D$ ,  $P(x)$  equivale logicamente a  $P(v_1) \vee P(v_2) \vee \dots \vee P(v_n)$ , i.e.,

$$(\exists x \in \{v_1, v_2, \dots, v_n\}, P(x)) \Leftrightarrow (P(v_1) \vee P(v_2) \vee \dots \vee P(v_n)).$$

<i>proposição</i>	<i>verdadeira</i>	<i>falsa</i>
para todo $x$ , $P(x)$	$P(a)$ é verdadeiro para todo $a$ no domínio	existe pelo menos um $a$ no domínio para o qual $P(a)$ é falso
existe $x$ , $P(x)$	existe pelo menos um $a$ no domínio para o qual $P(a)$ é verdadeiro	$P(a)$ é falso para todo $a$ no domínio

Defina os predicados  $P(x) : x \geq 0$ ,  $Q(x) : x^2 \geq 0$  e  $R(X) : x^2 > 3$ .

1. para todo  $x \in \mathbb{R}$ , se  $x \geq 0$  então  $x^2 \geq 0$ , ou

$$\forall x \in \mathbb{R} (P(x) \rightarrow Q(x))$$

é verdadeiro.

2. existe  $x \in \mathbb{R}$ , se  $x \geq 0$  então  $x^2 \geq 0$ , ou

$$\exists x \in \mathbb{R} (P(x) \rightarrow Q(x))$$

é verdadeiro.

Agora

$$\forall x \in \mathbb{R} (P(x) \rightarrow R(x))$$

é falso e para mostrar isso basta exibirmos um **contraexemplo**, um valor  $a$  do domínio ( $a \in \mathbb{R}$ ) para o qual  $P(a) \rightarrow R(a)$  é falso, como o 0.

**Definição 12.** As proposições abertas  $P(x)$  e  $Q(x)$  são **logicamente equivalentes** se  $P(a) \leftrightarrow Q(a)$  é tautologia para todo  $a \in D$ , e escrevemos  $\forall x (P(x) \Leftrightarrow Q(x))$ .

Se  $P(a) \rightarrow Q(a)$  é tautologia para todo  $a \in D$  então  $P(x)$  **implica logicamente**  $Q(x)$  e escrevemos  $\forall x (P(x) \Rightarrow Q(x))$ .

## 1.7 Distribuição de quantificadores

Sejam  $P(x)$  e  $Q(x)$  proposições abertas

1.  $\forall x (P(x) \wedge Q(x)) \Leftrightarrow (\forall x P(x)) \wedge (\forall x Q(x))$ .
2.  $\forall x (P(x) \vee Q(x)) \Leftrightarrow (\forall x P(x)) \vee (\forall x Q(x))$ .
3.  $\exists x (P(x) \vee Q(x)) \Leftrightarrow (\exists x P(x)) \vee (\exists x Q(x))$ .
4.  $\exists x (P(x) \wedge Q(x)) \Rightarrow (\exists x P(x)) \wedge (\exists x Q(x))$ .



## 1.8 Negação de quantificadores

$$\neg(\forall x, P(x)) \Leftrightarrow \exists x, \neg(P(x)).$$

$$\neg(\exists x, P(x)) \Leftrightarrow \forall x, \neg(P(x)).$$

## 1.9 Múltiplos quantificadores

Se uma proposição aberta menciona mais de uma variável, é preciso um quantificador para cada variável distinta para transformá-la numa proposição fechada.

Por exemplo, no domínio dos inteiros há oito maneiras de transformar a proposição aberta  $x + y = y + x$  em uma proposição fechada:

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}(x + y = y + x)$$

$$\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}(x + y = y + x)$$

$$\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}(x + y = y + x)$$

$$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}(x + y = y + x)$$

$$\forall y \in \mathbb{Z}, \forall x \in \mathbb{Z}(x + y = y + x)$$

$$\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}(x + y = y + x)$$

$$\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}(x + y = y + x)$$

$$\exists y \in \mathbb{Z}, \exists x \in \mathbb{Z}(x + y = y + x)$$

Em proposições com mais de uma variável *a ordem em que os quantificadores aparece é importante*. Por exemplo, se  $x$  e  $y$  são inteiros

$$\text{para todo } x \in \mathbb{Z}, \text{ existe } y \in \mathbb{Z}, (x + y = 0) \quad (19)$$

não é logicamente equivalente a

$$\text{existe } y \in \mathbb{Z}, \text{ para todo } x \in \mathbb{Z}, (x + y = 0) \quad (20)$$

pois (19) é verdadeiro enquanto que (20) é falso. Entretanto, em alguns casos vale a equivalência. Por exemplo, se  $x$  e  $y$  são números naturais

$$\text{para todo } x \in \mathbb{N}, \text{ existe } y \in \mathbb{N} \text{ tal que } x \text{ divide } y \quad (21)$$

é verdadeira, assim como

$$\text{existe } y \in \mathbb{N}, \text{ para todo } x \in \mathbb{N} \text{ tal que } x \text{ divide } y \quad (22)$$

pois todo  $x \in \mathbb{N}$  divide o 0.

Sempre podemos trocar a ordem de dois quantificadores do mesmo tipo

$$\begin{aligned} \forall x \forall y, P(x, y) &\Leftrightarrow \forall y \forall x, P(x, y) \\ \exists x \exists y, P(x, y) &\Leftrightarrow \exists y \exists x, P(x, y) \end{aligned}$$

## 1.10 Regras de Inferência e Argumentos válidos

As provas em matemática são *argumentos válidos* que estabelecem a verdade de sentenças.

Um **argumento** é uma seqüência  $P_1, P_2, \dots, P_n$  de proposições, ditas **premissas**, que terminam com uma conclusão  $Q$

$$\frac{\begin{array}{c} P_1 \\ P_2 \\ \vdots \\ P_n \end{array}}{\therefore Q}$$

O argumento é **válido** se, e só se,  $(P_1 \wedge P_2 \wedge \dots \wedge P_n) \Rightarrow Q$ .

**Regras de inferência** são modelos para construir argumentos válidos. Por exemplo,

$$\frac{\begin{array}{l} \text{Se você tem uma senha, então você pode fazer logon no facebook} \\ \text{Você tem uma senha} \end{array}}{\text{Portanto, você pode fazer logon no facebook}}$$

é um argumento válido porque se encaixa no modelo

$$\frac{P \rightarrow Q \quad P}{\therefore Q}$$

que é um argumento válido pelo teorema 2, essa regra de inferência é chamada *Modus Ponens*.

Notemos que cada caso do teorema 2 nos dá uma regra de inferência:

1. **Regra da Adição** Se  $P$  é uma premissa, podemos derivar  $P \vee Q$

$$\frac{P}{\therefore P \vee Q}$$

Por exemplo, “Ele estuda muito”, portanto “Ou ele estuda muito ou é um estudante muito ruim”.

2. **Regra da Simplificação** Se  $P \wedge Q$  é uma premissa, podemos derivar  $P$

$$\frac{P \wedge Q}{\therefore P}$$

Por exemplo, “Ele estuda muito” e “Ele é o melhor aluno da classe”, portanto “Ele é o melhor aluno da classe”.

3. ***Modus Ponens***

$$\frac{P \rightarrow Q \quad P}{\therefore Q}$$

4. ***Modus Tollens*** Se  $P \rightarrow Q$  e  $\neg Q$  são duas premissas, podemos usar o Modus Tollens para derivar  $\neg P$

$$\frac{P \rightarrow Q \quad \neg Q}{\therefore \neg P}$$

Por exemplo

Se você tem uma senha, então você pode fazer logon no facebook
Você não pode fazer logon no facebook
<hr style="width: 100%; border: 0.5px solid black;"/>
Portanto, você não tem uma senha

5. **Regra do silogismo hipotético** Se  $P \rightarrow Q$  e  $Q \rightarrow R$  são duas premissas, podemos usar o silogismo hipotético para derivar  $P \rightarrow R$

$$\frac{\begin{array}{l} P \rightarrow Q \\ Q \rightarrow R \end{array}}{\therefore P \rightarrow R}$$

Por exemplo, “Se chover, eu não vou para a escola” e “Se eu não for para a escola, não terei que fazer a lição de casa”, portanto, “Se chover, eu não precisarei fazer lição de casa”.

6. **Regra do silogismo disjuntivo** Se  $\neg P$  e  $P \vee Q$  são duas premissas, podemos usar o silogismo disjuntivo para derivar  $Q$

$$\frac{\begin{array}{l} P \vee Q \\ \neg P \end{array}}{\therefore Q}$$

Por exemplo, “O sorvete não é de baunilha” e “O sorvete é ou sabor baunilha ou sabor chocolate”, portanto, “O sorvete é chocolate aromatizado”.

7. **Regra da contradição** Se  $\neg P \rightarrow \mathbf{F}$  então deduzimos  $P$

$$\frac{\neg P \rightarrow \mathbf{F}}{\therefore P}$$

O seguinte é um argumento válido

$$\frac{\begin{array}{l} \neg(P) \rightarrow Q \\ Q \rightarrow S \\ P \rightarrow R \end{array}}{\therefore \neg R \rightarrow S}$$

*Resolução.* Vejamos

<i>passo</i>	<i>proposição</i>	<i>justificativa</i>
1.	$\neg P \rightarrow Q$	premissa
2.	$Q \rightarrow S$	premissa
3.	$P \rightarrow R$	premissa
4.	$\neg R \rightarrow \neg P$	contrapositiva de 3
5.	$\neg R \rightarrow Q$	Silogismo hipotético de 4 e 1
5.	$\neg R \rightarrow S$	Silogismo hipotético de 5 e 2

□

Atenção

$$\frac{\begin{array}{l} \text{se } \sqrt{2} > 3/2 \text{ então } 2 > 9/4 \\ \sqrt{2} > 3/2 \end{array}}{\therefore 2 > 9/4}$$

é um argumento válido!!!!!!

## Regras de inferência para quantificadores

8. **Instanciação universal.** Se para todo  $x$ ,  $P(x)$  então  $P(c)$  sempre que  $c$  é um elemento do domínio

$$\frac{\forall x, P(x)}{\therefore P(c)}$$

9. **Generalização universal.** Se  $P(c)$  para um elemento  $c$  **arbitrário** do domínio então para todo  $x$ ,  $P(x)$

$$\frac{P(c) \text{ para } c \text{ arbitrário}}{\therefore \forall x, P(x)}$$

10. **Instanciação existencial.** Se existe  $x$ ,  $P(x)$  então  $P(c)$  para algum elemento  $c$  do domínio

$$\frac{\exists x, P(x)}{\therefore P(c)}$$

11. **Generalização existencial.** Se  $P(c)$  para algum  $c$  específico, então existe  $x$ ,  $P(x)$

$$\frac{P(c) \text{ para algum } c \text{ específico}}{\therefore \exists x, P(x)}.$$

Atenção, consideremos a proposição aberta  $n^2 = n$ 

$$\frac{0^2 = 0}{\therefore \forall n \in \mathbb{N}, n^2 = n}$$

usando a generalização universal para  $c = 0$ !!! não é válido porque 0 não é um natural arbitrário.

Por exemplo, o seguinte argumento é válido

$$\frac{\begin{array}{l} \forall x(P(x) \rightarrow Q(x)) \\ \forall x(Q(x) \rightarrow R(x)) \end{array}}{\therefore \forall x(P(x) \rightarrow R(x))}$$

Vejamos

<i>passo</i>	<i>proposição</i>	<i>justificativa</i>
1.	$\forall x(P(x) \rightarrow Q(x))$	premissa
2.	$\forall x(Q(x) \rightarrow R(x))$	premissa
3.	$P(c) \rightarrow Q(c)$	instanciação universal de 1
4.	$Q(c) \rightarrow R(c)$	instanciação universal de 2
5.	$P(c) \rightarrow R(c)$	Silogismo hipotético de 3 e 4
6.	$\forall x(P(x) \rightarrow R(x))$	generalização universal.

A regra da conjunção:

$$\frac{\begin{array}{l} P \\ Q \end{array}}{\therefore P \wedge Q}$$

pode ser usada para mostrar que  $\exists x \in D, (P(x) \wedge Q(x)) \Rightarrow (\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$ . Vejamos

<i>passo</i>	<i>proposição</i>	<i>justificativa</i>
1.	$\exists x, (P(x) \wedge Q(x))$	premissa
2.	$P(c) \wedge Q(c)$	instanciação existencial de 1
3.	$P(c)$	simplificação de 2
4.	$Q(c)$	simplificação de 2
5.	$\exists x, P(x)$	generalização existencial de 3
6.	$\exists x, Q(x)$	generalização existencial de 4
7.	$(\exists x, P(x)) \wedge (\exists x, Q(x))$	conjunção.

No próximo exercício suponha que há um domínio associado sem se preocupar com o que de fato é tal conjunto (pode ser o conjunto de todos os animais conhecidos, por exemplo)

**Exercício 4** (Lewis Carrol). *Verifique se o seguinte argumento é válido:*

$$\frac{\begin{array}{l} \text{Todos os leões são selvagens.} \\ \text{Alguns leões não bebem café} \end{array}}{\text{Portanto, alguma criatura selvagem não bebe café.}}$$

*Solução.* Consideremos Matata um elemento do domínio.

<i>passo</i>	<i>proposição</i>	<i>justificativa</i>
1.	$\forall x, (L(x) \rightarrow S(x))$	premissa
2.	$\exists x, (L(x) \wedge \neg C(x))$	premissa
3.	$L(\text{Matata}) \wedge \neg C(\text{Matata})$	instanciação universal de 2
4.	$L(\text{Matata})$	simplificação de 3
5.	$\neg C(\text{Matata})$	simplificação de 3
6.	$(L(\text{Matata}) \rightarrow S(\text{Matata}))$	instanciação universal de 1
7.	$S(\text{Matata})$	Modus Ponens de 4 e 6
8.	$S(\text{Matata}) \wedge \neg C(\text{Matata})$	conjunção de 5 e 7
8.	$\exists x(S(x) \wedge \neg C(x))$	generalização existencial

□

**Exercício 5** (Modus Ponens Universal). *Verifique se o seguinte argumento que combina instanciação universal com Modus Ponens é válido:*

$$\frac{\begin{array}{l} \forall x(P(x) \rightarrow Q(x)) \\ P(a) \end{array}}{\therefore Q(a)}$$

**Exercício 6.** *Verifique a validade das seguintes regras de inferência:*

$$1. \text{ Resolução } \frac{\begin{array}{l} P \vee Q \\ \neg(P) \vee R \end{array}}{\therefore Q \vee R}$$

$$2. \text{ Prova por casos } \frac{\begin{array}{l} P \rightarrow Q \\ R \rightarrow Q \\ P \vee R \end{array}}{\therefore Q}$$

## 2 Técnicas de demonstração

Uma demonstração é um argumento válido que estabelece a veracidade de uma sentença matemática usando hipóteses do teorema, se houver, axiomas assumidos como verdadeiros, e teoremas previamente comprovados. Usando esses ingredientes e [regras de inferência](#), a demonstração estabelece a veracidade da afirmação provada. Passamos de provas formais, como visto na seção anterior, para as informais onde mais de uma regra de inferência pode ser usada em cada passo, os passos podem ser omitidos, e onde axiomas e regras de inferência utilizados não são explicitamente mencionadas.

**Definição 13.** Um *axioma* (ou *postulado*) são proposições que assumimos como verdadeiras.

Uma *conjetura* é uma proposição que está sendo proposta como uma sentença verdadeira. Se posteriormente demonstrada verdadeira, torna-se um teorema, entretanto pode ser falsa.

Um *teorema* é uma proposição que pode ser demonstrado ser verdadeira.

Uma *demonstração* é um argumento válido que estabelece a veracidade de um teorema. As proposições usadas em uma demonstração incluem axiomas, hipóteses (ou premissas) se houverem, teoremas previamente comprovados, regras de inferência, juntamente com a definição de termos.

Um *lema* é um “teorema auxiliar”, i.e., uma sentença verdadeira que é usada na demonstração de teoremas.

Um *proposição* é um teorema de menor importância.

**Observação:** *Lema* e *proposição* como definidos acima trata-se mais de uma convenção do que uma definição propriamente dita. Também *proposição* é usado em um sentido diferente do que usamos [até agora](#).

Um teorema pode ter muitas demonstrações diferentes. Quando não sabemos se uma sentença é verdadeira, nossa primeira atitude é encontrar uma demonstração que nos convença da veracidade. Para convencer outras pessoas, entretanto, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Começamos com algumas técnicas para construir demonstrações para implicações. Muitos teoremas afirmam propriedades para todos os elementos de um domínio sem



que o quantificado seja explicitamente mencionado

1. se 3 divide  $n$  então 9 divide  $n^2$ .
2. Se  $n$  é ímpar, então  $n^2$  é ímpar.
3. Se  $m$  é par e  $n$  é par, então  $m + n$  é par.

Essas sentenças significam, no domínio dos números naturais

1. Para todo  $n$ , se 3 divide  $n$  então 9 divide  $n^2$ .
2. Para todo  $n$ , se  $n$  é ímpar, então  $n^2$  é ímpar.
3. Para todo  $n$ , para todo  $m$ , se  $m$  é par e  $n$  é par, então  $m + n$  é par.

Em parte, esse comportamento é explicado pelo seguinte. Uma demonstração para a proposição  $\forall x(P(x) \rightarrow Q(x))$  tem os passos:

**passo 1** considere  $c$  arbitrário do domínio de  $x$

**passo 2** prove  $P(c) \rightarrow Q(c)$

**passo 3** conclua, por [generalização universal](#), que  $\forall x(P(x) \rightarrow Q(x))$ .

A parte principal é a implicação  $P(c) \rightarrow Q(c)$ , todo o trabalho de demonstrar “Para todo  $n$ , se 3 divide  $n$  então 9 divide  $n^2$ ” está concentrado na parte “se 3 divide  $n$  então 9 divide  $n^2$ ” para um  $n$  arbitrário.

Vamos ver esquemas para demonstrar uma implicação.

## 2.1 Prova direta de implicação

Nesse método, para demonstrar  $P \rightarrow Q$  assumimos  $P$  verdadeiro e usamos regras de inferência, definições, axiomas e equivalências lógicas para concluir que  $P$  é verdadeiro. Isso feito sabemos que  $P \rightarrow Q$  é verdadeiro o que estabelece o [passo 2](#) descrito acima.

Por exemplo, se  $n$  é um número natural arbitrário então a *implicação*

$$\text{se } 3 \text{ divide } n \text{ então } 9 \text{ divide } n^2 \quad (23)$$

é verdadeira.

**Definição 14.**  $3$  *divide*  $n$  se, e somente se,  $3q = n$  para algum  $q \in \mathbb{N}$ .

Que a implicação (23) é verdadeira:

- 1) Suponha que 3 divide  $n$  (premissa)
- 2) Se 3 divide  $n$ , então existe  $q \in \mathbb{N}$  tal que  $n = 3q$  (definição de divide)
- 3) Se  $n = 3q$ , então  $n^2 = 9q^2$  (propriedade aritmética)
- 4) Se  $n^2 = 9q^2$  então 9 divide  $n^2$  (definição de divide)
- 5) Se 3 divide  $n$ , então 9 divide  $n^2$  (silogismo hipotético com 2,3 e do resultado com 4)
- 6) 9 divide  $n^2$  (modus ponens com 1 e 5)

Como a variável  $n$  acima pode assumir qualquer valor natural, ou seja,  $n$  é um elemento genérico de  $\mathbb{N}$ , o que provamos de fato foi

**Teorema 3.** Para todo  $n \in \mathbb{N}$ , se 3 divide  $n$  então 9 divide  $n^2$ .

**Teorema 4.** Para todo  $n \in \mathbb{N}$ , se  $n$  é ímpar, então  $n^2$  é ímpar.

Em geral, quando escrevemos uma demonstração, não enumeramos nem justificamos os passos como foi feito no exemplo acima.

*Demonstração.* Seja  $n$  um número natural arbitrário. Vamos provar que se  $n$  é ímpar então  $n^2$  é ímpar.

Suponha  $n$  ímpar.

Se  $n$  é ímpar então existe  $k \in \mathbb{N}$  tal que  $n = 2k + 1$ .

Se  $n = 2k + 1$  então  $n^2 = (2k + 1)^2$ .

Se  $(2k + 1)^2 = 2(2k^2 + 2k) + 1$  então  $n^2 = 2(2k^2 + 2k) + 1$ .

Se  $n^2 = 2(2k^2 + 2k) + 1$  então  $n^2$  é ímpar.

Se  $n$  é ímpar então  $n^2$  é ímpar.

Portanto  $n^2$  é ímpar. □

**Teorema 5.** Para todo  $n \in \mathbb{N}$  e todo  $m \in \mathbb{N}$ , se  $m$  é par e  $n$  é par, então  $m + n$  é par.

Também, normalmente, pulamos passos elementares, mais fáceis e os passos ubíquos como a conclusão através da generalização universal. Ainda, é usual usarmos a mesma variável do enunciado para representar o elemento arbitrário do domínio.

*Demonstração.* Sejam  $m$  e  $n$  naturais arbitrários. Suponha que  $m$  e  $n$  são números pares, logo existem naturais  $k$  e  $\ell$  tais que  $m = 2k$  e  $n = 2\ell$ . Então,  $m + n = 2k + 2\ell = 2(k + \ell)$ , portanto,  $m + n$  é par.  $\square$

**Exercício 7.** *Escreva uma demonstração para: para todo  $x \in \mathbb{N}^*$  (os naturais menos o zero), para todo  $y \in \mathbb{N}$ , se  $x$  divide  $y$  então  $x^2$  divide  $y^2$ .*

*Solução.* Sejam  $n$  e  $m$  números naturais,  $n \neq 0$ .

Suponha que  $n|m$  e que  $n \neq 0$ .

Se  $n|m$  e  $n \neq 0$  então  $nq = m$  para algum  $q$ .

Se  $nq = m$  então  $n^2q^2 = m^2$ .

Portanto,  $n^2|m^2$ .

Usando a regra de generalização universal concluímos que para todo  $x \in \mathbb{N}^*$  (os naturais menos o zero), para todo  $y \in \mathbb{N}$ , se  $x$  divide  $y$  então  $x^2$  divide  $y^2$ .  $\square$

## 2.2 Prova indireta de implicação

Nesse tipo de prova, demonstramos que uma proposição logicamente equivalente a  $P \rightarrow Q$  é verdadeira, como a contrapositiva, por exemplo.

**Prova da contrapositiva:** Provamos que  $\neg(Q) \rightarrow \neg(P)$  é verdadeira donde concluímos que  $P \rightarrow Q$  é verdadeira pela [equivalência lógica da contrapositiva](#). Por exemplo, para um número natural  $n$  arbitrário, a implicação

$$n^2 \text{ par} \rightarrow n \text{ par} \tag{24}$$

é verdadeira (tente uma prova direta). Vamos provar a contrapositiva de (24)

$$n \text{ ímpar} \rightarrow n^2 \text{ ímpar}$$

1. Suponha  $n$  ímpar.
2. Se  $n$  é ímpar, então pelo teorema 4 acima  $n^2$  é ímpar.
3. Portanto,  $n^2$  é ímpar.

Esse argumento é a regra *Modus Ponens*, assim temos (24) verdadeira.

**Teorema 6.** *Se  $a$  e  $b$  são números inteiros positivos coprimos, então não são ambos par.*

Para facilitar a escrita definimos

$\text{mdc}(x, y)$  é o maior divisor comum dos naturais  $x, y$   
 $P(x)$  é o predicado  $x$  é par.

**Definição 15.**  $a$  e  $b$  inteiros positivos são **coprimos** se, e só se,  $\text{mdc}(a, b) = 1$ .

*Demonstração.* Sejam  $a$  e  $b$  números inteiros positivos arbitrários. Vamos demonstrar que se  $a$  e  $b$  são coprimos então não são ambos par pela contrapositiva. Vamos provar

$$(P(a) \text{ e } P(b)) \rightarrow \neg(\text{mdc}(a, b) = 1).$$

Suponha  $a$  par e  $b$  par. Então 2 divide  $a$  e 2 divide  $b$ , portanto,  $\text{mdc}(a, b) \geq 2$ . □

Um escrutínio da demonstração acima:

**passo 1** Sejam  $a$  e  $b$  números inteiros positivos arbitrários.

- |                |    |  |                           |
|----------------|----|--|---------------------------|
|                | 1) | $a$ é par e $b$ é par  | (premissa)                |
|                | 2) | Se $a$ é par e $b$ é par então $2 a$ e $2 b$                 | (definição de número par) |
| <b>passo 2</b> | 3) | se $2 a$ e $2 b$ então $\text{mdc}(a, b) \geq 2$             | (definição de mdc)        |
|                | 4) | se $\text{mdc}(a, b) \geq 2$ então $\text{mdc}(a, b) \neq 1$ | (silogismos)              |
|                | 5) | se $a$ é par e $b$ é par então $\text{mdc}(a, b) \neq 1$     | (silogismos)              |
|                | 6) | Portanto $\text{mdc}(a, b) \neq 1$ .                         | (modus ponens)            |

A implicação “se  $a$  e  $b$  são números inteiros positivos coprimos, então não são ambos par” é verdadeira.

**passo 3** Concluindo: *para todo  $a \in \mathbb{Z}^+$  e todo  $b \in \mathbb{Z}^+$ , se  $a$  e  $b$  são coprimos, então não são ambos par.*

**Prova por vacuidade:** A proposição  $P \rightarrow Q$  é verdadeira porque conseguimos provar que  $P$  é falso. Assim,  $\forall x \in D(P(x) \rightarrow Q(x))$  é verdadeiro porque para nenhum elemento do domínio  $D$  o predicado  $P$  é verdadeiro.

Por exemplo, considere o predicado  $P(n)$  : se  $n > 1$  então  $n^2 > n$ . A sentença  $P(0)$  é verdadeira por vacuidade.

Agora, para  $Q(n)$  : se  $n + \frac{1}{n} < 2$  então  $n^2 + \frac{1}{n^2} < 2$ . A sentença  $\forall n \in \mathbb{Z}^+, Q(n)$  é verdadeira por vacuidade.

**Teorema 7.** *Para todo  $x \in \mathbb{R}$ , se  $x^2 + 1 < 0$  então  $x^5 \geq 4$ .*

*Demonstração.* Seja  $x$  um real arbitrário. Sabemos que  $x^2 \geq 0$ , logo  $x^2 + 1 > 0$ . Portanto, se  $x^2 + 1 < 0$  então  $x^5 \geq 4$  por vacuidade.  $\square$

Notemos que a contrapositiva do teorema acima afirma que se  $x^5 < 4$  então  $x^2 + 1 \geq 0$ . Como a conclusão é sempre verdadeira a implicação também será, isto é,

$$\text{se } x^5 < 4 \text{ então } x^2 + 1 \geq 0$$

é verdadeiro porque  $x^2 + 1 \geq 0$  é verdadeiro. Esse argumento para uma implicação é chamado de **prova trivial**.

**Teorema 8.** Para qualquer conjunto  $A$ ,  $\emptyset \subseteq A$ .

*Demonstração.* Dado o conjunto  $A$ ,  $\emptyset \subseteq A$  se, e só se, para todo  $x$

$$x \notin A \rightarrow x \notin \emptyset$$

que vale trivialmente.  $\square$

**Prova por contradição:** Numa demonstração por contradição assumimos que a *negação* da proposição a ser provada é verdadeira e derivamos disso uma **contradição**, ou seja, uma proposição falsa. O argumento é válido pela **regra da inferência da contradição** que diz que da premissa  $\neg(R) \rightarrow \mathbf{F}$  concluímos  $R$ .

No caso em que  $R$  é da forma  $P \rightarrow Q$ , na demonstração por contradição provamos que  $\neg(P \rightarrow Q) \rightarrow \mathbf{F}$  é verdadeiro, porém  $\neg(P \rightarrow Q)$  é logicamente equivalente a  $P \wedge \neg(Q)$  assim a sentença a ser provada verdadeira é

$$P \wedge \neg(Q) \rightarrow \mathbf{F}$$

Vamos provar por contradição o teorema 6:  $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, ((\text{mdc}(a, b) = 1) \rightarrow \neg(P(a) \wedge P(b)))$ .

*Demonstração 1.* Sejam  $a$  e  $b$  números naturais arbitrários. Vamos demonstrar

$$(\text{mdc}(a, b) = 1) \wedge \neg(\neg(P(a) \wedge P(b))) \rightarrow \mathbf{F}.$$

ou, **pela dupla negação**,

$$(\text{mdc}(a, b) = 1) \wedge (P(a) \wedge P(b)) \rightarrow \mathbf{F}.$$

- |    |  |                              |
|----|--|------------------------------|
| 1) | $\text{mdc}(a, b) = 1.$                                | (premissa)                   |
| 2) | $P(a) \wedge P(b).$                                    | (premissa)                   |
| 3) | Se $P(a) \wedge P(b)$ então $\text{mdc}(a, b) \geq 2.$ | (da definição de mdc)        |
| 4) | $\text{mdc}(a, b) \geq 2.$                             | ( <i>modus ponens</i> )      |
| 5) | $\text{mdc}(a, b) = 1 \wedge \text{mdc}(a, b) \geq 2$  | ( <b>conjunção</b> de 1 e 4) |

A linha 5 é uma contradição.  $\square$

A demonstração foi escrita acima de maneira pouco ortodoxa para salientar os passos dedutivos. Abaixo escrevemos uma outra demonstração que, provavelmente, está mais próxima do modo que se apresenta em textos matemáticos.

*Demonstração 2.* Sejam  $a$  e  $b$  dois números naturais quaisquer. Suponhamos que  $a$  e  $b$  seja coprimos, isto é,  $\text{mdc}(a, b) = 1$ .

Se  $a$  é par e  $b$  é par então  $\text{mdc}(a, b) \geq 2$ , uma contradição. Portanto,  $a$  e  $b$  não são ambos números pares.  $\square$

## 2.3 Prova de equivalências

Para demonstrar uma sentença da forma  $P \leftrightarrow Q$  usamos que  $(P \leftrightarrow Q) \Leftrightarrow (P \leftarrow Q) \wedge (P \rightarrow Q)$  e, de fato provamos  $P \rightarrow Q$  e a sua recíproca  $Q \rightarrow P$ . Cada uma dessas duas implicações pode ser demonstrada com alguma das técnicas para demonstrar uma implicação.

**Teorema 9.** Para todo  $n \in \mathbb{N}$ ,  $n$  é ímpar se, e somente se,  $n^2$  é ímpar.

*Demonstração.* Seja  $n \in \mathbb{N}$  arbitrário. Vamos provar que  $n^2$  ímpar  $\leftrightarrow n$  ímpar.

$n^2$  ímpar  $\rightarrow n$  ímpar: Essa implicação pode ser provada na contrapositiva:  $n$  par  $\rightarrow n^2$  par. Suponha  $n$  par. Se  $n$  é par então  $n = 2k$  para algum  $k \in \mathbb{N}$ . Se  $n = 2k$  então  $n^2 = 4k^2$ . Se  $n^2 = 4k^2$  então  $n^2$  é par.

$n$  ímpar  $\rightarrow n^2$  ímpar: Essa implicação é o teorema 4.

Portanto a equivalência é verdadeira.  $\square$

## 2.4 Mais provas por contradição

Os próximos exemplos são de demonstrações por contradição mas os enunciados não envolvem implicação.

**Teorema 10.** Para todo  $d \in \mathbb{N}$  e  $e \in \mathbb{N}$

$$\text{mdc}\left(\frac{d}{\text{mdc}(d, e)}, \frac{e}{\text{mdc}(d, e)}\right) = 1.$$

*Demonstração.* Sejam  $d$  e  $e$  números naturais arbitrários e faça  $m = \text{mdc}(d, e)$ . Vamos provar

$$\text{mdc}\left(\frac{d}{m}, \frac{e}{m}\right) > 1 \rightarrow \mathbf{F}.$$

Suponha  $\text{mdc}(\frac{d}{m}, \frac{e}{m}) = k$ .

Suponha  $k > 1$ .

Se  $\text{mdc}(\frac{d}{m}, \frac{e}{m}) = k$  então  $k$  divide  $\frac{d}{m}$  e  $k$  divide  $\frac{e}{m}$ .

Se  $k$  divide  $\frac{d}{m}$  e  $k$  divide  $\frac{e}{m}$ , então  $k \cdot m$  divide  $d$  e  $k \cdot m$  divide  $e$ .

Portanto,  $k \cdot m$  divide  $d$  e  $k \cdot m$  divide  $e$ .

Se  $k > 1$  então  $k \cdot m > m$ .

Portanto  $k \cdot m > m$ .

$k \cdot m$  divide  $d$ ,  $k \cdot m$  divide  $e$  e  $k \cdot m > m$  é uma contradição pois  $m = \text{mdc}(d, e)$ .  $\square$

**Corolário 11.** *Todo número racional pode ser escrito como  $\frac{a}{b}$  com  $a$  e  $b$  coprimos.*

*Demonstração.* Seja  $q$  um racional arbitrário. Por definição, existem inteiros  $d$  e  $e$  tais que  $q = \frac{d}{e}$ .

Faça  $a = \frac{d}{\text{mdc}(d, e)}$  e  $b = \frac{e}{\text{mdc}(d, e)}$  que temos, pelo teorema anterior,  $\text{mdc}(a, b) = 1$ .

Claramente  $q = \frac{a}{b} = \frac{d}{e}$ .  $\square$

**Teorema 12.**  $\sqrt{2}$  é irracional.

*Demonstração.* Vamos provar que  $\sqrt{2}$  é irracional por contradição, isto é a, vamos provar que

$$\sqrt{2} \in \mathbb{Q} \rightarrow \mathbf{F}.$$

Suponha que  $\sqrt{2} \in \mathbb{Q}$ .

Se  $\sqrt{2} \in \mathbb{Q}$  então existem naturais positivos e coprimos  $a$  e  $b$  tais que  $\sqrt{2} = \frac{a}{b}$ .

Se  $\sqrt{2} = \frac{a}{b}$  então  $2 = a^2/b^2$ .

Se  $2 = a^2/b^2$  então  $a^2 = 2b^2$ .

Se  $a^2 = 2b^2$  então  $a^2$  é par.

Se  $a^2$  é par então  $a$  é par (contrapositiva do teorema 4).

Se  $a$  é par então existe  $k \in \mathbb{N}$ ,  $a = 2k$ .

Se  $a = 2k$  então  $2b^2 = 4k^2$ .

Se  $2b^2 = 4k^2$  então  $b^2 = 2k^2$ .

Se  $b^2 = 2k^2$  então  $b^2$  é par.

Se  $b^2$  é par então  $b$  é par.

Se  $a$  é par e  $b$  é par, então  $\text{mdc}(a, b) \geq 2$ , que é uma contradição.  $\square$

**Exercício 8.** *Prove que não há uma quantidade finita de números primos.*

## 2.5 Prova por casos

O argumento é baseado na equivalência lógica

$$((P_1 \vee P_2 \vee \cdots \vee P_n) \rightarrow Q) \Leftrightarrow ((P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge \cdots \wedge (P_n \rightarrow Q))$$

as implicações  $P_i \rightarrow Q$  são os casos. Essa equivalência justifica o argumento válido

$$\begin{array}{c} P_1 \rightarrow Q \\ P_2 \rightarrow Q \\ \vdots \\ P_n \rightarrow Q \\ \hline P_1 \vee P_2 \vee \cdots \vee P_n \\ \hline \therefore Q \end{array}$$

Por exemplo, podemos demonstrar em 3 casos que: *para todo inteiro  $n$ ,  $n^2 \geq n$ .*

1. **Caso**  $n = 0$ : se  $n = 0$  então  $n^2 \geq n$ .

De fato, se  $n = 0$  então  $n^2 = 0^2 = 0 = n$ .

2. **Caso**  $n \geq 1$ : se  $n \geq 1$  então  $n^2 \geq n$ .

De fato, multiplicando os dois lados da desigualdade por  $n$ ,  $n^2 \geq n$ .

3. **Caso**  $n \leq -1$ : se  $n \leq -1$  então  $n^2 \geq n$ .

De fato, como  $n^2 \geq 0$  e  $0 \geq n$ , pois  $n$  é negativo, então  $n^2 \geq n$ .

portanto a proposição é verdadeira.  $\square$

**Teorema 13.** *Para todo  $n \in \mathbb{Z}$ ,  $n^2 + 3n + 5$  é ímpar.*

*Demonstração.* Seja  $n$  um inteiro arbitrário. Então  $n$  é divisível por 2 ou  $n$  não é divisível por 2.



Se  $n$  é divisível por 2 então  $n = 2k$  para algum inteiro  $k$  e

$$(2k)^2 + 3(2k) + 5 = 2(2k^2 + 3k + 2) + 1$$

que é ímpar

Se  $n$  não é divisível por 2 então  $n = 2k + 1$  para algum inteiro  $k$  e

$$(2k + 1)^2 + 3(2k + 1) + 5 = 2(2k^2 + 5k + 4) + 1.$$

□

**Teorema 14.** Para todo  $n \in \mathbb{Z}$ , se  $1 \leq n \leq 40$  então  $n^2 - n + 41$  é primo.

*Demonstração.* Defina  $f(n) = n^2 - n + 41$ .

$f(1) = 41$  é primo,  $f(2) = 43$  é primo,  $f(3) = 47$  é primo,  $f(4) = 53$  é primo,  $f(5) = 61$  é primo,  $f(6) = 71$  é primo,  $f(7) = 83$  é primo,  $f(8) = 97$  é primo,  $f(9) = 113$  é primo,  $f(10) = 131$  é primo,  $f(11) = 151$  é primo,  $f(12) = 173$  é primo,  $f(13) = 197$  é primo,  $f(14) = 223$  é primo,  $f(15) = 251$  é primo,  $f(16) = 281$  é primo,  $f(17) = 313$  é primo,  $f(18) = 347$  é primo,  $f(19) = 383$  é primo,  $f(20) = 421$  é primo,  $f(21) = 461$  é primo,  $f(22) = 503$  é primo,  $f(23) = 547$  é primo,  $f(24) = 593$  é primo,  $f(25) = 641$  é primo,  $f(26) = 691$  é primo,  $f(27) = 743$  é primo,  $f(28) = 797$  é primo,  $f(29) = 853$  é primo,  $f(30) = 911$  é primo,  $f(31) = 971$  é primo,  $f(32) = 1033$  é primo,  $f(33) = 1097$  é primo,  $f(34) = 1163$  é primo,  $f(35) = 1231$  é primo,  $f(36) = 1301$  é primo,  $f(37) = 1373$  é primo,  $f(38) = 1447$  é primo,  $f(39) = 1523$  é primo,  $f(40) = 1601$  é primo. □

É possível conferir a lista dos 1000 primeiros números primos [aqui](#).

**Exercício 9.** Para quaisquer  $a \in \mathbb{R}$  e  $b \in \mathbb{R}^*$ ,  $\left| \frac{a}{b} \right| = \frac{|a|}{|b|}$ .

## 2.6 Provas existenciais

Para demonstrar uma proposição da forma existe  $x$ ,  $P(x)$ , usualmente, adotamos as seguintes estratégias

**Prova construtiva:** exibimos um elemento  $c$  do universo tal que  $P(c)$  seja verdade,  
ou

**Prova não-constructiva:** ou inferimos indiretamente a existência desse objeto que torna  $P$  verdadeira, por exemplo, através de uma prova por contradição: assumimos que tal objeto não existe e derivamos uma contradição.

**Teorema 15.** *Existe um inteiro positivo  $n$  que pode ser escrito como a soma de dois cubos de duas maneiras diferentes.*

*Demonstração (constructiva).* Faça  $n = 1729$  e verifique que  $1729 = 10^3 + 9^3 = 12^3 + 1^3$ .  $\square$

**Teorema 16.** *Existem  $x, y$  irracionais tais que  $x^y \in \mathbb{Q}$ .*

*Demonstração (não-constructiva).* Vimos que  $\sqrt{2}$  é irracional.

Se  $\sqrt{2}^{\sqrt{2}}$  é racional então faça  $x = x = \sqrt{2}$ .

Se  $\sqrt{2}^{\sqrt{2}}$  é irracional então faça  $x = \sqrt{2}^{\sqrt{2}}$  e  $y = \sqrt{2}$  e temos

$$x^y = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$$

que é racional.  $\square$

Na demonstração acima usamos a regra de inferência de [prova por casos](#).

**Teorema 17.** *Existem subconjuntos de inteiros  $A \subset \mathbb{Z}$  e  $B \subset \mathbb{Z}$  tais que  $A \cap B = \emptyset$  e  $A \cup B = \mathbb{Z}$  e, ainda,  $A$  e  $B$  são infinitos.*

*Demonstração (constructiva).* Defina  $A = \{2k : k \in \mathbb{Z}\}$  e  $B = \{2k + 1 : k \in \mathbb{Z}\}$ . Nenhum desses conjuntos é finito (dê uma prova por contradição) e definem uma partição dos inteiros (prove).  $\square$

**Teorema 18.** *Se  $y \in \mathbb{Q}$  então existe  $x \in \mathbb{Z}$  tal que  $y < x$ .*

Esse enunciado está (implicitamente) dizendo que

$$\text{para todo } y \in \mathbb{Q}, \text{ existe } x \in \mathbb{Z}, y < x.$$

Então, consideramos um racional arbitrário  $q$  e provamos a sentença existencial existe  $x \in \mathbb{Z}, q < x$ .

*Demonstração (construtiva).* Seja  $\frac{p}{q}$  um racional arbitrário. Vamos exibir um inteiro  $n$  tal que  $\frac{p}{q} < n$ .

Faça  $n = |p| + 1$  e verifique que  $\frac{p}{q} \leq \left|\frac{p}{q}\right|$  e  $\left|\frac{p}{q}\right| < |p| + 1$ .  $\square$

**Teorema 19.** *O polinômio  $p(x) = x^3 + x - 1$  tem exatamente uma raiz real.*

*Demonstração (não-construtiva).* Pelo [Teorema do Valor Intermediário](#), para todo  $b \in [p(0), p(1)]$ , existe  $a \in [0, 1]$  tal que  $p(a) = b$ .

Como  $p(0) = -1$  e  $p(1) = 1$  temos  $0 \in [p(0), p(1)]$  assim fazendo  $b = 0$  concluímos que existe  $a \in [0, 1]$  tal que  $p(a) = 0$ .

Provamos que o polinômio  $p(x) = x^3 + x - 1$  tem uma raiz real usando o Teorema do Valor Intermediário. Agora, usando contradição e o [Teorema Valor Médio](#) vamos provar que a raiz é única.

Suponha que  $p(x)$  tem duas raízes e vamos deduzir uma contradição. Sejam  $r_1$  e  $r_2$  raízes distintas de  $p(x)$ , de modo que  $r_1 < r_2$ . Como  $p(x)$  é contínua em  $[r_1, r_2]$  e derivável em  $(r_1, r_2)$  então podemos usar o teorema do valor médio para concluir que existe um ponto  $c \in [r_1, r_2]$  tal que

$$p'(c) = \frac{p(r_2) - p(r_1)}{r_2 - r_1}$$

mas  $p(r_2) - p(r_1) = 0$ , portanto  $p'(c) = 0$  que é uma contradição pois o  $p'(x) = 3x^2 + 1 > 0$  qualquer que seja  $x$ .  $\square$

**Exercício 10.** *Prove que para qualquer natural  $n > 1$ , existe uma sequência formada por  $n$  números naturais consecutivos tal que nenhum deles é primo.*

*Solução.* Seja  $n$  um natural maior que 1 qualquer. A sequência  $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$  é formada por  $n$  números naturais consecutivos. Ainda,  $(n+1)! + j$  é divisível por  $j$  sempre que  $j \in \{2, 3, \dots, n+1\}$ .  $\square$

**Exercício 11.** *Prove que no domínio dos números reais a seguinte sentença é verdadeira:*

$$\forall \epsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, \left( |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} \right| < \epsilon \right).$$

## 3 O Princípio de Indução e provas por indução

### 3.1 Princípio da Boa Ordem (PBO)

**Definição 16.** *O natural  $m$  é **menor elemento** de um conjunto  $A \subset \mathbb{N}$  não vazio se, e só se,*

- (1)  $m \in A$  e
- (2)  $\forall x \in A, m \leq x$ .

**Princípio da Boa Ordem:** *Todo  $A \subset \mathbb{N}$  não-vazio tem um **menor elemento**.*

Esse fenômeno não ocorre nos conjuntos numéricos como  $\mathbb{Q}$  e  $\mathbb{R}$ . Por exemplo o intervalo  $(0, 1]$  em  $\mathbb{R}$  não tem menor elemento, enquanto que  $[0, 1]$  em  $\mathbb{R}$  tem menor elemento. Essa é uma das propriedades que caracterizam os números naturais, todo subconjunto tem menor elemento.

Esse princípio pode ser usado em demonstrações, usualmente provas por contradição: supomos que um  $A$  formado por contra-exemplos do que se quer provar é não vazio e derivamos uma contradição, concluindo que  $A$  é vazio.

**Teorema 20.** *Qualquer postagem que custe pelo menos oito reais pode ser feita com selos de 3 e 5 reais.*

*Demonstração.* Vamos chamar  $n \in \mathbb{N}$  de **postal** se  $n + 8$  pode ser um valor obtido a partir de selos de 3 e 5 reais. Por exemplo 0 é postal pois  $8 = 3 + 5$ , também 1 é postal pois  $9 = 3 \cdot 3 + 0 \cdot 5$  e 2 é postal pois  $10 = 0 \cdot 3 + 2 \cdot 5$ .

O teorema afirma que para todo  $n \in \mathbb{N}$ ,  $n$  é postal. Suponha que a afirmação do teorema é falsa. Seja  $A \subseteq \mathbb{N}$  o subconjunto dos naturais não-postais. Por hipótese  $A \neq \emptyset$ , portanto tem um menor elemento  $m$ . Pelas considerações acima sabemos que  $m \geq 3$ .

Se  $m \geq 3$  então  $m - 3 \in \mathbb{N}$  e é postal, existem naturais  $x$  e  $y$  tais que  $m - 3 = x \cdot 3 + y \cdot 5$ .

Se  $m - 3 = x \cdot 3 + y \cdot 5$  então  $m = (x + 1) \cdot 3 + y \cdot 5$ , uma contradição. □

**Exercício 12.** *Prove usando o PBO. Para todo inteiro  $n \geq 5$ , existem naturais  $a$  e  $b$  tais que  $n = 2a + 5b$ .*

(Solução)

**Teorema 21.** *Não existe um número natural entre 0 e 1.*

*Demonstração.* Suponha que a afirmação do teorema é falsa e seja  $A$  o conjunto dos naturais entre 0 e 1. Por hipótese  $A \neq \emptyset$  logo tem um menor elemento  $m$ ,  $0 < m < 1$ .

Se  $m < 1$  então  $m^2 < m$ , uma contradição pois  $m^2 \in \mathbb{N}$ . Portanto,  $A = \emptyset$ .  $\square$

**Teorema 22.** *Todo número natural tem um divisor primo.*

*Demonstração.* A prova dessa afirmação é por contradição, suponha que não é todo natural que admite um divisor primo e seja  $A$  o subconjunto desses naturais. Por hipótese  $A \neq \emptyset$ , portanto tem um menor elemento  $m$ .

Se  $m \in A$  então  $m$  não é primo, logo  $m = a \cdot b$  com  $1 < a, b < m$ . Todo divisor primo de  $a$  (e de  $b$ ) divide  $m$ , portanto  $a \in A$ , uma contradição ( $a$  é menor que o menor elemento de  $A$ ).  $\square$

**Exercício 13.**  $A \subseteq \mathbb{N}$  é dito limitado superiormente se existir um natural  $n$  tal que

$$\forall x \in A, x \leq n$$

e se  $n$  com a propriedade acima pertence a  $A$  ele é dito maior elemento de  $A$ .

Mostre que se  $A$  é limitado superiormente e não vazio então admite maior elemento.

## 3.2 Princípios de indução

**Teorema 23 (Princípio da Indução finita (PIF)).** *Seja  $X \subseteq \mathbb{N}$  tal que*

1.  $0 \in X$
2. para todo  $k \in \mathbb{N}$ ,  $k \in X \rightarrow k + 1 \in X$ .

Então  $X = \mathbb{N}$ .

*Demonstração.* Seja  $X$  um subconjunto dos naturais que satisfaz as hipóteses do teorema. Suponha que a conclusão do teorema seja falsa, ou seja, suponha que

$X \subsetneq \mathbb{N}$ . Então  $A = \mathbb{N} - X$  é não vazio e, pelo PBO, tomamos  $m$  o menor elemento de  $A$ .

De  $0 \in X$  temos  $m \geq 1$ , portanto  $m - 1$  é natural. Pela minimalidade de  $m$  temos que  $m - 1 \in X$ . Pela hipótese 2 do teorema, se  $m - 1 \in X$  então  $m \in X$ . Portanto  $m \in X$ , uma contradição.  $\square$

**Corolário 24 (Princípio da Indução finita (PIF)).** *Seja  $P(n)$  um predicado de números naturais. Se*

1.  $P(0)$  é verdadeiro, e
2. para todo  $k \geq 0$ ,  $P(k)$  implica  $P(k + 1)$  é verdadeiro,

*então  $P(n)$  é verdadeiro para todo natural  $n$ .*

*Demonstração.* Seja  $P$  um predicado com as hipóteses dadas. Faça  $X = \{k \in \mathbb{N} : P(k)\}$  e temos, da hipótese 1 que  $0 \in X$  e da hipótese 2, se  $k \in X$  então  $k + 1 \in X$ . Assim, estamos nas hipóteses do teorema 23 e podemos concluir que  $X = \mathbb{N}$ , ou seja,  $P(n)$  é verdadeiro para todo natural  $n$ .  $\square$

**Corolário 25 (Princípio da Indução finita generalizado (PIFg)).** *Sejam  $P(n)$  um predicado de números naturais e  $a \in \mathbb{N}$ . Se*

1.  $P(a)$  é verdadeiro, e
2. para todo  $k \geq a$ ,  $P(k)$  implica  $P(k + 1)$  é verdadeiro,

*então  $P(n)$  é verdadeiro para todo natural  $n \geq a$ .*

*Demonstração.* Como na demonstração anterior, agora faça  $X = \{k \in \mathbb{N} : P(k + a)\}$  e temos pelo teorema 23 que  $X = \mathbb{N}$ . Se  $P(n + a)$  é verdadeiro para todo  $n \geq 0$  então  $P(n)$  é verdadeiro para todo  $n \geq a$ .  $\square$

**Teorema 26 (Princípio da Indução finita completo (PIFc)).** *Seja  $X \subseteq \mathbb{N}$  tal que*

1.  $0 \in X$
2. para todo  $k \in \mathbb{N}$ ,  $\{0, 1, \dots, k\} \subset X \rightarrow k + 1 \in X$ .

Então  $X = \mathbb{N}$ .

*Demonstração.* Seja  $X \subseteq \mathbb{N}$  que satisfaz as hipóteses do teorema.

Defina o conjunto  $Y = \{n \in \mathbb{N} : \{0, 1, \dots, n\} \subseteq X\}$ .

Então  $0 \in Y$  pela condição 1 da hipótese do teorema.

Considere um natural arbitrário  $k$  e suponha que  $k \in Y$ . Se  $k \in Y$  então  $k+1 \in Y$  pela condição 2 da hipótese do teorema. Portanto, para todo  $k \in \mathbb{N}$ ,  $k \in Y \rightarrow k+1 \in Y$ .

Pelo PIF,  $Y = \mathbb{N}$  portanto  $X = \mathbb{N}$ . □

**Corolário 27 (Princípio da Indução finita completo (PIFc)).** *Seja  $P(n)$  um predicado de números naturais. Se*

1.  $P(0)$  é verdadeiro, e
2. para todo  $k \geq 0$ ,  $P(0)$  e  $P(1)$  e  $\dots$  e  $P(k)$  implica  $P(k+1)$  é verdadeiro,

então  $P(n)$  é verdadeiro para todo natural  $n \geq 0$ .

*Demonstração.* Exercício. □

**Corolário 28 (Princípio da Indução finita completo generalizado (PIFc<sub>g</sub>)).** *Sejam  $P(n)$  um predicado de números naturais e  $a \in \mathbb{N}$ . Se*

1.  $P(a)$  é verdadeiro, e
2. para todo  $k \geq a$ ,  $P(a)$  e  $P(a+1)$  e  $\dots$  e  $P(k)$  implica  $P(k+1)$  é verdadeiro,

então  $P(n)$  é verdadeiro para todo natural  $n \geq a$ .

*Demonstração.* Exercício. □

**Exercício 14.** *Seja  $a_i$  uma sequência (estritamente) crescente de números naturais. Verifique o seguinte Princípio de Indução Finita: Se  $P(n)$  é um predicado a respeito de  $n \in \mathbb{N}$  de modo que*

1.  $P(a_i)$  é verdadeiro para todo  $i \in \mathbb{N}$  e
2.  $P(j)$  verdadeiro implica  $P(j - 1)$  verdadeiro, para todo  $j > a_1$

então  $P(n)$  é verdadeiro para todo  $n \geq a_1$ .

Dissemos acima que o PBO é um dos princípios que caracterizam os número naturais. De fato PBO é *equivalente* ao PIF e o PIF é que é normalmente usado como um dos Axiomas de [Peano](#) que caracterizam os [Números Naturais](#).

### 3.3 Equivalência

Notemos que acima deduzimos PIFc de PIF e PIF de PBO. Esses princípios são, de fato, equivalentes, logo se assumimos qualquer um deles o outro pode ser provado. Para provar a equivalência vamos provar que PBO segue de PIFc e teremos

$$\text{PBO} \Rightarrow \text{PIF} \Rightarrow \text{PIFc} \Rightarrow \text{PBO}$$

*Demonstração de PIFc  $\Rightarrow$  PBO.* Seja  $A \subset \mathbb{N}$  não vazio. Vamos provar que  $A$  tem um menor elemento. A prova é por contradição, suponha que  $A$  não tem menor elemento.

Definimos

$$X := \{n \in \mathbb{N} : n \notin A\}$$

e vamos provar que: (i)  $0 \in X$ , e (ii) para todo  $k \in \mathbb{N}$ , se  $\{0, \dots, k\} \subset X$  então  $k + 1 \in X$ .

Se  $0 \notin X$  então  $0 \in A$ , portanto  $0$  é o menor elemento de  $A$ , contradição. Com isso provamos que  $0 \in X$ .

Seja  $k \geq 0$  arbitrário e suponha  $\{0, \dots, k\} \subset X$ . Se  $k + 1 \notin X$  então  $k + 1 \in A$ , portanto  $k + 1$  é o menor elemento de  $A$ , já que  $\{0, \dots, k\} \subset X$ , contradição. Portanto  $k + 1 \notin A$  e, generalizando universalmente, provamos para todo  $k \in \mathbb{N}$ , se  $\{0, \dots, k\} \subset X$  então  $k + 1 \in X$ .

Com (i) e (ii) podemos usar o PIFc para concluir que  $X = \mathbb{N}$ , ou seja  $A = \emptyset$ , uma contradição. Portanto,  $A$  tem menor elemento.  $\square$



### 3.4 Provas por indução

Indução matemática também é uma técnica de prova para proposições da forma para todo  $n \geq a$ ,  $P(n)$ . Numa prova por indução provamos  $P(a)$  (isto é, verificamos que a instanciiação da variável com  $a$  resulta numa sentença verdadeira) que é dito a **base da indução** e provamos  $\forall n \geq a (P(n) \rightarrow P(n+1))$  (usando as estratégias que já aprendemos para isso) que é dito o **passo da indução**.

**Exemplo:** Para todo  $n \in \mathbb{N}$ ,  $\sum_{i=0}^n i = n(n+1)/2$ .

**base:**  $\sum_{i=0}^0 i = 0(0+1)/2$

**passo:** Seja  $k \geq 0$  um natural arbitrário e suponha que  $\sum_{i=0}^k i = k(k+1)/2$ . Precisamos mostrar que  $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$ .

**Exemplo:** Para todo  $n \geq 5$ ,  $2^n > n^2$ .

**base:**  $2^5 > 5^2$ .

**passo:** Seja  $k \geq 5$  um natural arbitrário e suponha que  $2^k > k^2$ . Precisamos mostrar que  $2^{k+1} > (k+1)^2$ .

**A base é importante**, sem ela poderíamos pensar que sabemos provar

$$n(n+1) \text{ é ímpar para todo } n \geq 1$$

que obviamente não vale, pois conseguimos provar a implicação do passo da indução para essa sentença. Vamos provar que

$$\text{para todo } n \geq 1, n(n+1) \text{ ímpar} \rightarrow (n+1)(n+2) \text{ ímpar.}$$

Seja  $n > 1$  um natural e suponha que  $n(n+1)$  é ímpar. Então

$$(t+1)(t+2) = (t+1)t + (t+1)2$$

que é da forma ímpar + par, portanto ímpar.

**O passo é importante**, uma prova descuidada pode por tudo a perder. Por exemplo, seja  $P(t)$  a sentença

$$\text{para todo } a \in \mathbb{N}, \text{ para todo } b \in \mathbb{N}, (\max\{a, b\} = t \rightarrow a = b).$$

Se  $\max\{a, b\} = 0$  então  $a = b = 0$ , portanto a base é verdadeira.

Seja  $t \in \mathbb{N}$ , suponha que

para todo  $a$ , para todo  $b$ ,  $(\max\{a, b\} = t - 1 \rightarrow a = b)$

e vamos provar que para todo  $a$ , para todo  $b$ ,  $(\max\{a, b\} = t \rightarrow a = b)$ .

Se  $\max\{a, b\} = t$  então  $\max\{a - 1, b - 1\} = t - 1$ , portanto pela hipótese acima  $a - 1 = b - 1$ , logo  $a = b$ .

Claramente,  $P(t)$  é falso (determine um contraexemplo).

Qual é o problema da demonstração? ([Solução](#))

**Exemplo:** Para todo natural  $n \geq 2$ ,  $n$  é primo ou pode ser escrito como produto de primos.

Numa tentativa de prova usando o corolário 24 temos:

—a base é fácil,  $n = 2$  é primo;

—no passo temos que provar que se  $n$  é primo ou produto de primos então  $n + 1$  é primo ou produto de primos. Se  $n + 1$  é primo a implicação é verdadeira (vacuidade), se  $n + 1$  é composto então, por [definição de número composto](#)  $n + 1 = ab$  onde  $1 \leq a, b \leq n$  são números naturais. Se soubéssemos que  $a$  e  $b$  são primos ou produtos de primos então  $n + 1$  seria produto de primos, mas só o que sabemos é que  $n$  é produto de primos.

Esse problema pode ser contornado com o corolário 27. Se a hipótese vale para todo  $k \leq n$  então  $a$  é produto de primos,  $b$  é produto de primos, portanto  $a \cdot b$  é produto de primos:

Seja  $P(n)$  a sentença  $n$  é primo ou pode ser escrito como produto de primos.

**base:** 2 é primo, portanto  $P(2)$ .

**passo:** Seja  $k \geq 2$  um natural arbitrário e suponha

$$P(2) \wedge P(3) \wedge \cdots \wedge P(k) \tag{25}$$

Precisamos provar  $P(k + 1)$ . Em dois casos: (i) se  $k + 1$  é primo então  $P(k + 1)$ . (ii) se  $k + 1$  não é primo então  $k + 1 = ab$  com  $2 \leq a, b \leq k$ . Pela hipótese (25) valem  $P(a)$  e  $P(b)$  portanto  $ab$  é um produto de primos, portanto  $P(k + 1)$ . Pelo PIFc,  $P(n)$  para todo  $n \geq 2$ .

**Exemplo:** Se em  $2^n$  moedas 1 é falsa, mais leve, então é possível descobrir a moeda falsa em  $n$  pesagens numa balança de 2 pratos.

*Demonstração.* Se  $n = 0$  então a afirmação vale trivialmente, a única moeda é a falsa.

Seja  $k \geq 0$  um natural arbitrário e suponha que para  $2^j$  moedas sabemos encontrar a mais leve usando  $j$  pesagens, sempre que  $j \geq 0$  e  $j \leq k$ . Consideremos um conjunto com  $2^{k+1}$  moedas e dividimos as moedas em duas partes iguais de  $2^k$  moedas. Comparamos essas metades usando 1 pesagem e na metade mais leve achamos a moeda falsa com  $k$  pesagens, totalizando  $k + 1$  pesagens.

Portanto, pelo PIFc, se em  $2^n$  moedas 1 é mais leve, então é possível descobrir a moeda leve em  $n$  pesagens, para qualquer  $n \geq 0$ .  $\square$

**Outro exemplo de prova errada:** Seja  $P(n)$  a sentença: para todo  $n \in \mathbb{N}$ ,  $6n = 0$ .

*Demonstração.* Vamos provar  $P(n)$  por indução.

$P(0)$  é verdadeiro. Seja  $n$  um natural arbitrário e vamos provar que para todo  $n$ ,  $P(0) \wedge P(1) \wedge \dots \wedge P(n) \Rightarrow P(n+1)$ . Suponhamos  $P(0) \wedge P(1) \wedge \dots \wedge P(n)$ . Então

$$6(n+1) = 6 \cdot n + 6 \cdot 1 = 0 + 0 = 0$$

pois de  $P(n)$  temos  $6n = 0$  e de  $P(1)$  temos  $6 \cdot 1 = 0$ ; qual é o erro?  $\square$

**Teorema 29 (Princípio da casa dos pombos).** Se em  $n$  caixas ( $n \geq 1$ ) distribuímos mais de  $n$  objetos, então alguma caixa conterá mais de um objeto.

*Demonstração.* Provaremos usando indução no número de caixas  $n$ .

Se  $n = 1$  a afirmação é verdadeira pois, se há mais de um objeto, essa caixa terá mais de um objeto.

Seja  $k \geq 1$  arbitrário e suponha que se distribuímos mais de  $k$  objetos em  $k$  caixas, então alguma caixa conterá mais de um objeto.

Se  $m > k + 1$  objetos são distribuídos em  $k + 1$  caixas escolhemos uma das caixas. Se essa caixa escolhida tem mais de um objeto, a afirmação está provada. Senão, na caixa escolhida há no máximo um objeto. Isso significa que os pelo menos  $m - 1$  objetos restantes foram distribuídos nas outras  $k$  caixas, mas  $m - 1 > k$ , portanto por hipótese alguma caixa conterá mais de um objeto.  $\square$

**Exercício 15.** Sejam  $A_1, A_2, \dots, A_n$  conjuntos e  $n \geq 2$ . Suponha que para dois conjuntos quaisquer  $A_i$  e  $A_j$  vale que  $A_i \subseteq A_j$  ou  $A_j \subseteq A_i$ . Prove, por indução, um desses conjuntos é subconjunto de todos eles.

### 3.5 Definições recursivas

**Definição 17.** Quando a indução é usada para definir objetos chamamos de *definição recursiva*.

Conhecemos vários exemplos de definição recursiva

1. o fatorial:  $0! = 1$  e para todo  $n > 0$ ,  $n! = n \cdot (n-1)!$ ;
2. o somatório:  $\sum_{i=0}^0 x_i = x_0$  e para todo  $n \geq 0$ ,  $\sum_{i=0}^{n+1} x_i = (n+1) + \sum_{i=0}^n x_i$ ;
3. exponencial:  $a^0 = 1$  e para todo  $n > 0$ ,  $a^n = a^{n-1} \cdot a$ ;
4. sequência de Fibonacci:  $F_0 = 0$ ,  $F_1 = 1$  e  $F_n = F_{n-1} + F_{n-2}$  para todo  $n \geq 2$ .

Definimos qualquer função com domínio  $\mathbb{N}$  recursivamente em duas etapas: na *base* especificamos o valor da função 0 e no *passo* damos uma regra para encontrar seu valor em um inteiro  $n$  em função de seus valores no inteiros menores que  $n$ . Tal definição é chamada de definição recursiva ou indutiva.

**Definição 18.** Uma função  $f : \mathbb{N} \rightarrow \mathbb{R}$  é o mesmo que uma *sequência*  $a_0, a_1, \dots$  com  $f(i) = a_i$ . Uma *recorrência* é uma sequência definida recursivamente.

As funções definidas recursivamente estão bem definidas. Isso significa que dado qualquer  $n$  podemos usar as duas partes da definição para encontrar o valor da função no ponto  $n$  de forma inequívoca.

**Exercício 16.** Use indução matemática para provar que uma função  $F$  definida pela especificação de  $F(0)$  e uma regra para obtenção de  $F(n+1)$  a partir de  $F(n)$  está bem definida.

**Exercício 17.** Use indução para provar que uma função  $F$  definida especificando  $F(0)$  e uma regra para obter  $F(n+1)$  dos valores  $F(k)$  para  $k = 0, 1, 2, \dots, n$  está bem definida.

**Exemplo:** uma progressão aritmética que começa em  $a \in \mathbb{R}$  e tem razão  $r \in \mathbb{R}$  é uma sequência  $a_0, a_1, \dots$  tal que

$$\begin{aligned} a_0 &= a \\ a_{n+1} &= a_n + r \text{ para todo } n \geq 0. \end{aligned}$$

Podemos provar por indução que para todo  $n$ ,  $a_n = nr + a$ . De fato, a base ( $n = 0$ ) é verdadeira,  $a_0 = 0r + a = a$  portanto confere com a definição. Seja  $k$  um natural arbitrário e suponha que  $a_k = kr + a$ . Vamos provar que  $a_{k+1} = (k+1)r + a$ .

$a_{k+1} = a_k + r$  por definição e  $a_k = kr + a$  por hipótese. Portanto,  $a_{k+1} = (k+1)r + a$ . Portanto, pelo PIF, para todo  $n$ ,  $a_n = nr + a$ .

**Exercício 18.** Uma progressão geométrica é uma sequência definida pela recorrência  $x_0 = a$  e  $x_n = x_{n-1} \cdot r$  para todo  $n > 0$  onde  $a$  e  $r$  são valores reais, chamados de termo inicial e razão da progressão. Prove usando indução que o termo geral de uma progressão geométrica é  $x_n = ar^n$  para todo  $n \geq 0$ .

**Teorema 30.** Defina  $X \subset \mathbb{N}$  por

1.  $1 \in X$
2. para todo  $a \in X$ ,  $a + 2 \in X$ .

Então  $X$  é o subconjunto dos naturais ímpares.

*Demonstração.* Para provar que  $X = \{2n + 1 : n \in \mathbb{N}\}$  provaremos duas inclusões  $X \subseteq \{2n + 1 : n \in \mathbb{N}\}$  e  $\{2n + 1 : n \in \mathbb{N}\} \subseteq X$ .

Para provar que  $X \subseteq \{2n + 1 : n \in \mathbb{N}\}$ , suponha existir um elemento de  $X$  que não está em  $\{2n + 1 : n \in \mathbb{N}\}$ . Seja  $m$  o menor deles, certamente  $m > 1$ . De  $m > 1$  temos  $m - 2 \in \mathbb{N}$  e da definição  $m - 2 \in X$ . De  $m$  mínimo,  $m - 2 \in \{2n + 1 : n \in \mathbb{N}\}$ , portanto  $m = 2(k + 1) + 1$ , contradição.

Para provar que  $\{2n + 1 : n \in \mathbb{N}\} \subseteq X$  vamos usar indução para provar que para todo  $n$ ,  $2n + 1 \in X$ . A base:  $2 \cdot 0 + 1 = 1 \in X$ . Seja  $k \in \mathbb{N}$  arbitrário e suponha que  $2k + 1 \in X$  é verdadeiro. Então  $2k + 1 + 2 \in X$ , pela hipótese 2 do teorema, ou seja,  $2(k + 1) + 1 \in X$ . Pelo PIF temos  $2n + 1 \in X$  para todo  $n$ .  $\square$

**Exercício 19.** Suponha que um casal de urubus começa a dar crias com dois anos de idade, e produz 6 crias (três casais) de urubuzinhos a cada ano. Suponha que um lixão começou a ser frequentado por 1 casal recém-nascido e que nenhum urubu é acrescentado ou eliminado do lixão. Escreva uma definição recursiva para o número de urubus que existem no ano  $n$ .

## 4 Aula de exercícios e Avaliação

### 4.1 Matutino

1. Suponha que o universo do discurso é composto por todas as pessoas. Considere os seguintes predicados:  $B(x)$  : “ $x$  é um bebê”;  $L(x)$  : “ $x$  é lógico”;  $M(x)$  : “ $x$  é capaz de domar um crocodilo”; e  $D(x)$  : “ $x$  é desprezado”.

Expresse em símbolos lógicos as sentenças

p1: Os bebês são ilógicos.

p2: Ninguém despreza quem pode domar um crocodilo.

p3: Pessoas ilógicas são desprezadas.

p4: Os bebês não podem domar crocodilos.

Essa sequência é um argumento válido com premissas p1,p2,p3 e conclusão p4? Justifique.

Escreva a negação de cada sentença simbólica.

2. Sejam  $P(x)$ ,  $Q(x)$  e  $R(x)$  as afirmações “ $x$  é a Professor”, “ $x$  é ignorante e “ $x$  é vazio”, respectivamente. O domínio é composto por todas as pessoas. Expresse em símbolos lógicos as sentenças

p1: Nenhum professor é ignorante.

p2: Todas as pessoas ignorantes são vazias.

p3: Nenhum professor é vazio.

Essa sequência é um argumento válido com premissas p1 e p2 e conclusão p3? Justifique.

Escreva a negação de cada sentença simbólica.

3. Expresse a sentença matemática usando predicados, quantificadores, conectivos lógicos e operadores aritméticos.

(a)  $m$  é um quadrado perfeito.

(b) O produto de dois números reais negativos é positivo.

4. Encontre um contra-exemplo, se possível, para a sentença com domínio nos inteiros

- (a)  $\forall x \forall y (x^2 = y^2 \rightarrow x = y)$
- (b)  $\exists y \forall x (xy = 1)$
- (c)  $\forall x \exists y (y^2 - x < 100)$

5. Dê uma demonstração detalhada para a seguinte afirmação. Se necessário, reescreva a afirmação de modo a torná-la precisa.

Se  $m$  e  $n$  são quadrados perfeitos então  $mn$  é quadrado perfeito.

Se  $n$  é quadrado perfeito então  $n - 2$  não é quadrado perfeito.

6. Prove usando indução que  $1^3 + 2^3 + \dots + n^3 = n^2(n+1)^2/4$ .

7. Prove usando indução que

$$\sum_{i=0}^n 9 \cdot 10^i = 10^{n+1} - 1$$

8. Os números de Fibonacci são dados pela definição recursiva:  $F(0) = 0$ ,  $F(1) = 1$  e para todo  $n \geq 2$ ,  $F(n) = F(n-1) + F(n-2)$ .

Prove usando indução que para todo  $n \geq 1$ ,  $\sum_{j=1}^n F(j) = F(n+2) - 1$ .

Prove usando indução que para todo  $n$ ,  $F(3n)$  é divisível por 2.

## 4.2 Noturno

1. Sejam  $P(x)$ ,  $Q(x)$  e  $R(x)$  as afirmações “ $x$  é uma explicação clara”, “ $x$  é satisfatório” e “ $x$  é uma desculpa”, respectivamente. Suponha que o domínio para  $x$  consiste de todos os textos em português. Expresse cada uma das declarações com símbolos lógicos

p1: Todas as explicações claras são satisfatórias.

p2: Algumas desculpas são insatisfatórias.

p3: Algumas desculpas não são explicações claras.

Essa sequência é um argumento válido com premissas p1 e p2 e conclusão p3? Justifique.

Escreva a negação de cada fórmula lógica.

2. Sejam  $P(x)$ ,  $Q(x)$ ,  $R(x)$  e  $S(x)$  as afirmações “ $x$  é um pato”, “ $x$  é uma de minhas aves”, “ $x$  é um oficial” e “ $x$  está disposto a uma dança”, respectivamente. Expresse cada uma das declarações com símbolos lógicos

- (a) Nenhum pato está disposto a uma dança.
- (b) Nenhum oficial indispôs-se a uma dança.
- (c) Todas as minhas aves são patos.
- (d) As minhas aves não são oficiais.

Essa sequência é um argumento válido com premissas p1,p2,p3 e conclusão p4? Justifique.

Escreva a negação de cada fórmula lógica.

3. Expresse a sentença matemática abaixo usando predicados, quantificadores, conectivos lógicos e operadores aritméticos.

- (a) Cada número real positivo tem exatamente duas raízes quadradas.
- (b) Um número real negativo não tem raiz quadrada que é um número real.

4. Encontre um contra-exemplo, se possível, para a sentença com domínio nos inteiros

- (a)  $\forall x \forall y (xy \geq x)$
- (b)  $\forall x \exists y (xy = 1)$
- (c)  $\forall x \forall y (x^2 = y^3)$
- (d) Cada inteiro positivo pode ser escrito como a soma dos quadrados de três inteiros.

5. Dê uma demonstração detalhada para a seguinte afirmação. Se necessário, reescreva a afirmação de modo a torná-la precisa.

se  $x$  é um real não nulo então  $x^2 + x^{-2} \geq 2$ .

6. Os números de Fibonacci são dados pela definição recursiva:  $F(0) = 0$ ,  $F(1) = 1$  e para todo  $n \geq 2$ ,  $F(n) = F(n-1) + F(n-2)$ .

Prove usando indução que para todo  $n$ ,  $F(5n)$  é divisível por 5.

Prove usando indução que para todo  $n$ ,  $\sum_{j=0}^{n-1} F(2j+1) = F(2n)$ .



7. O  $n$ -ésimo número harmônico é dado por  $H(n) = \sum_{i=1}^n \frac{1}{i}$ .

Dê uma definição recursiva para  $H(n)$ .

Prove usando indução que para todo  $n \geq 1$ ,  $\sum_{j=1}^n H(j) = (n+1)H(n) - n$ .

## 5 Teoria intuitiva de conjuntos

A teoria dos conjuntos é uma linguagem adequada para descrever e explicar as estruturas matemáticas; de fato é o fundamento dominante de toda a matemática; a ideia é que tudo pode ser descrito em termos de conjuntos. É possível desenvolver a teoria de conjuntos de maneira axiomática em lógica de primeira ordem, como foi feito por Ernest Zermelo e Abraham Fraenkel. A teoria de conjuntos de Zermelo–Fraenkel (ZF) é um dos vários sistemas axiomáticos propostos no início do século 20 para formular uma teoria de conjuntos livre de paradoxos como o. Acrescentando aos axiomas de ZF o historicamente controverso *axioma da escolha*, a teoria é chamada de *Teoria ZFC dos conjuntos* e é o tratamento axiomático mais comum da teoria dos conjuntos na matemática.

### 5.1 Abordagem intuitiva

*Conjunto* é informalmente entendido como uma *coleção de entidades*, essas entidades são chamadas de *elementos* ou *membros* do conjunto e eles mesmos podem ser conjuntos. Um elemento  $x$  *pertence* se  $x$  é um elemento de  $A$  o que é denotado por

$$x \in A$$

e escrevemos a negação como  $x \notin A$ .

Essa descrição de conjunto é circular pois usa o termo *coleção* que é sinônimo de conjunto. Não definimos conjunto e assumimos que todo têm alguma noção, mesmo que possivelmente errada, da concepção de conjuntos.

Convencionamos usar letras maiúsculas para conjuntos e minúsculas para elementos. Assim, um conjunto representado por uma letra minúscula deve ser entendido como um elemento de algum conjunto.

### Igualdade de conjuntos

*Dois conjuntos são iguais se, e somente se, têm os mesmos elementos.*

Ou seja, a única propriedade distintiva de um conjunto é sua lista de membros. Essa sentença é um axioma da teoria axiomática de conjuntos (o Axioma da Extensionalidade).

## Conjunto vazio

Há um (único) conjunto sem elementos, denotado por  $\emptyset$  e chamado de conjunto vazio.

## Especificação de conjuntos

Da igualdade de conjuntos podemos inferir que especificar todos os elementos de um conjunto é suficiente para defini-lo, podemos fazer isso de diversas formas.

Se um conjunto tem poucos elementos, podemos listá-los entre chaves “{ }” separados por vírgulas. Por exemplo, o conjunto dos algarismos primos é formado pelos números inteiros 2, 3, 5 e 7 e escrevemos  $\{2, 3, 5, 7\}$ . O conjunto dos algarismos indo-arábicos é  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ .

Quando os conjuntos têm muitos elementos não é viável escrever todos seus elementos e uma solução comum, mas que só usamos quando o contexto não dá margem a ambiguidade sobre seu significado, é o uso de reticências (...). Por exemplo, o conjunto dos naturais menores que 2.017 é descrito por  $\{0, 1, \dots, 2.016\}$ ; o conjunto das letras do alfabeto  $\{a, b, c, \dots, z\}$ ; o conjunto dos naturais pares  $\{0, 2, 4, 6, \dots\}$ . No geral é preciso muito cuidado e a recomendação é que essa solução deve ser evitada pois, por exemplo, o que é o conjunto  $\{3, 5, 7, \dots\}$ ?

**Exercício 20.** *Encontre duas respostas factíveis para a pergunta acima.*

Além de listar os elementos de um conjunto explicitamente, também podemos definir conjunto por *especificação* (também chamado de *compreensão*), onde damos uma regra de como gerar todos os seus elementos. Podemos especificar um conjunto através de uma ou mais propriedade de seus elementos e, nesse caso, usamos a notação como

$$A = \{x : P(x)\}$$

em que  $P$  é um predicado (fórmula da lógica de 1ª ordem). Assim,  $a \in A$  se, e só se,  $P(a)$  é verdadeiro. Por exemplo,  $\{x \in \mathbb{R} : x^2 \leq 2\} = [-\sqrt{2}, \sqrt{2}]$ . Por exemplo, o conjunto dos números primos é

$$\left\{x : x \in \mathbb{N} \wedge x > 1 \wedge \forall y \in \mathbb{N}, \forall z \in \mathbb{N}(yz = x \rightarrow y = 1 \vee z = 1)\right\}$$

Observamos que  $\{2, 3, 5, 7\}$  pode ser especificado como

$$\{x : x = 2 \vee x = 3 \vee x = 5 \vee x = 7\}.$$

Observamos também que os elementos de um conjunto podem, eles mesmos, serem conjuntos

$$X = \left\{ \{a\}, \{b\}, \{c\} \right\}$$

Observamos, ainda, que

$$\begin{aligned} \{1, 1, 1\} &= \{1\} \\ \{1, 2, 1, 1\} &= \{1, 2\} \\ \{1, 2, 3\} &= \{1, 3, 2\} \\ &= \{2, 3, 1\} \\ &= \{2, 1, 3\} \\ &= \dots \end{aligned}$$

são consequências do princípio de [extensionalidade](#) (igualdade de conjuntos).

## Paradoxo de Russel

O que é o conjunto

$$S = \{x : x \notin x\}?$$

## Inclusão de conjuntos

O conjunto  $A$  é *subconjunto* de um conjunto  $B$ , fato denotado por  $A \subseteq B$ , se todo elemento de  $A$  pertence a  $B$ , ou seja,

$$\forall x(x \in A \Rightarrow x \in B)$$

isto é  $x \in A \rightarrow x \in B$  é uma tautologia para todo  $x$ .

Se  $A$  não é subconjunto de  $B$  denotamos  $A \not\subseteq B$ ,

$$\begin{aligned} A \not\subseteq B &\Leftrightarrow \text{não } (\forall x(x \in A \Rightarrow x \in B)) \\ &\Leftrightarrow \exists x, \text{ não}(x \in A \Rightarrow x \in B) \\ &\Leftrightarrow \exists x(x \in A \text{ e } x \notin B) \end{aligned}$$

Observemos que

$$A = B \Leftrightarrow A \subseteq B \text{ e } B \subseteq A. \tag{26}$$

e, assim,  $A \neq B \Leftrightarrow A \not\subseteq B$  ou  $B \not\subseteq A$ .

**Teorema 31.** Para qualquer conjunto  $A$ ,  $\emptyset \subseteq A$ .

*Demonstração.* A implicação  $x \in \emptyset \rightarrow x \in A$  é tautologia para todo  $x$  pois  $x \in \emptyset$  é falso.  $\square$

Usaremos  $A \subsetneq B$  para expressar  $A \subset B$  e  $A \neq B$ .

## 5.2 Provando proposições de conjuntos

Há essencialmente três coisas provamos sobre conjuntos:

1. Dados  $x$  e  $S$ , prove que  $x \in S$ . Isto requer olhar a definição de  $S$  para ver se  $x$  satisfaz as propriedades que os elementos de  $S$  satisfazem.
2. Dados  $A$  e  $B$ , prove que  $A \subseteq B$ . Temos que mostrar que todo  $x$  em  $A$  também está em  $B$ . Assim, uma demonstração considera um elemento arbitrário  $x$  em  $A$  e mostra que ele também deve ser um elemento de  $B$ . Isto implicará usar as propriedades que definem  $A$  para mostrar que  $x$  satisfaz a definição de  $B$ .
3. Dados  $A$  e  $B$ , prove que  $A = B$ . Usualmente, fazemos isso mostrando  $A \subseteq B$  e  $B \subseteq A$  separadamente.

## 5.3 Operações sobre conjuntos

As operações sobre conjuntos definem novos conjuntos. A seguir descrevemos as operações mais usuais e suas propriedades.

**União:**  $A \cup B$  denota a união dos conjuntos  $A$  e  $B$  que é o conjunto dos elementos que pertencem a  $A$  ou a  $B$

$$A \cup B = \{x : x \in A \text{ ou } x \in B\} \quad (27)$$

**Intersecção:**  $A \cap B$  denota a intersecção dos conjuntos  $A$  e  $B$  que é o conjunto dos elementos que pertencem a  $A$  e a  $B$

$$A \cap B = \{x : x \in A \text{ e } x \in B\} \quad (28)$$

$A$  e  $B$  são *disjuntos* se  $A \cap B = \emptyset$ .

**Exercício 21.** Para quaisquer conjuntos  $A$  e  $B$

$$A \cap B \subset A \subset A \cup B.$$

**Diferença:**  $A \setminus B$  denota o conjunto dos elementos pertencem a  $A$  e não a  $B$

$$A \setminus B = \{x : x \in A \text{ e } x \notin B\}. \quad (29)$$

**Diferença simétrica:**  $A \triangle B$  denota o conjunto dos elementos que pertencem exclusivamente a  $A$  ou a  $B$ , não a ambos

$$A \triangle B = \{x : x \in A \cup B \text{ e } x \notin A \cap B\}. \quad (30)$$

## Propriedades das operações em conjuntos

Fica como exercício a verificação das seguintes propriedades.

### Leis de identidade

$$\begin{aligned} A \cap (C \setminus A) &= \emptyset \\ A \cup \emptyset &= A \\ A \cap \emptyset &= \emptyset \end{aligned}$$

### Leis de idempotência

$$\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}$$

### Leis distributivas

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}$$

### Leis comutativas

$$\begin{aligned} A \cap B &= B \cap A \\ A \cup B &= B \cup A \end{aligned}$$

### Leis associativas

$$\begin{aligned}A \cap (B \cap C) &= (A \cap B) \cap C \\ A \cup (B \cup C) &= (A \cup B) \cup C\end{aligned}$$

### Leis de De Morgan

$$\begin{aligned}C \setminus (A \cup B) &= (C \setminus A) \cap (C \setminus B) \\ C \setminus (A \cap B) &= (C \setminus A) \cup (C \setminus B)\end{aligned}$$

### Leis de absorção

$$\begin{aligned}A \cup (A \cap B) &= A \\ A \cap (A \cup B) &= A\end{aligned}$$

*Prova de uma das leis de De Morgan.* Sejam  $A$ ,  $B$  e  $C$  conjuntos e vamos provar que  $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ . Para provar essa igualdade, precisamos provar que (i)  $C \setminus (A \cup B) \subseteq (C \setminus A) \cap (C \setminus B)$  e que (ii)  $(C \setminus A) \cap (C \setminus B) \subseteq C \setminus (A \cup B)$ .

Para provar (i), seja  $x \in C \setminus (A \cup B)$

$x \in C \setminus (A \cup B) \Rightarrow$	$x \in C$ e $x \notin A \cup B$	por definição
$\Rightarrow$	$x \in C$ e não $(x \in A \cup B)$	por definição de $\notin$
$\Rightarrow$	$x \in C$ e não $(x \in A$ ou $x \in B)$	por definição de $\cup$
$\Rightarrow$	$x \in C$ e não $(x \in A)$ e não $(x \in B)$	por De Morgan (proposicional)
$\Rightarrow$	$x \in C$ e $x \notin A$ e $x \notin B$	por definição
$\Rightarrow$	$x \in C$ e $x \notin A$ e $x \in C$ e $x \notin B$	por definição
$\Rightarrow$	$x \in (C \setminus A) \cap (C \setminus B)$	por definição de $\cap$

Para provar (ii) basta notar que a recíproca de todas as implicações no argumento acima são verdadeiras.

Das duas inclusões segue a igualdade. □

### Complementos

Seja  $A$  um conjunto. O equivalente em teoria de conjuntos da negação lógica é  $\{x : x \notin A\}$ , que é conhecido como o complemento de  $A$ . Se permitimos complementos, estamos

necessariamente trabalhando dentro de um *Universo*, uma vez que o complemento do conjunto vazio deve conter *todos* os objetos possíveis.

Essa abordagem é possível quando trabalhamos dentro de um contexto onde o universo está entendido, por exemplo, os Inteiros formam o universo da Teoria Elementar de Números e os Reais formam o universo da Análise na reta. Mas, nós corremos o risco de se quisermos trabalhar com diferentes classes de objetos ao mesmo tempo. Contudo, um universo na Teoria dos Conjuntos é muito maior do que qualquer coisa que possamos usar e, mais que isso, é consequência dos axiomas que tal construção

*não é conjunto*

fazendo complementos não muito útil. A solução usual é usarmos a diferença de conjuntos com complementos relativos, como no enunciado das Leis de De Morgan acima.

**Exercício 22.** *Seja  $R$  um conjunto de conjuntos. Denote por  $\bigcup R$  a união dos elementos de  $R$ , isto é, se  $A = \{a, b, c\}$ , por exemplo, então  $\bigcup A = a \cup b \cup c$ .*

*Tome  $R = \left\{ \left\{ \{1\}, \{1, 2\} \right\}, \left\{ \{1\}, \{1, 3\} \right\}, \left\{ \{2\}, \{2, 3\} \right\} \right\}$*

*Escreva os conjuntos  $\bigcup R$  e  $\bigcup \bigcup R$ .*

## 5.4 Conjunto das partes

$2^A$  denota o conjunto formado por todos os subconjuntos de  $A$ , isto é,

$$B \in 2^A \Leftrightarrow B \subseteq A \quad (31)$$

*conjunto das partes de  $A$ .*

Algumas referências usam  $\mathcal{O}(A)$  ou  $\mathcal{P}(A)$ . Aqui usaremos  $2^A$  e  $\mathcal{O}(A)$  conforme a conveniência.

**Exercício 23.** *Descreva o conjunto das partes do conjunto vazio. Descreva o conjunto das partes do conjunto  $\{a\}$ .*



## 5.5 Axiomática de ZFC

A teoria dos conjuntos utilizada na matemática é definida por uma coleção de axiomas que nos permitem construir, essencialmente a partir do zero, um universo grande o suficiente para manter toda a matemática sem contradições aparentes, evitando os paradoxos que podem surgir na teoria intuitiva dos conjuntos.

Um dos problemas com a teoria dos conjuntos ingênuos é que a especificação irrestrita de conjuntos é muito forte, levando a contradições. Na teoria axiomática conjuntos a especificação é mais restritiva. Vamos descrever os axiomas da teoria ZFC abaixo, mas na prática você só precisa que pode construir conjuntos por (a) listando seus elementos, (b) tomando a união de outros conjuntos, (c) tomando o conjunto de todos os subconjuntos de um conjunto, ou (d) usando algum predicado para selecionar elementos ou subconjuntos de alguns conjuntos. Os pontos de partida para este processo são o conjunto vazio e o conjunto  $\mathbb{N}$  de todos os números naturais. Se você não consegue construir um conjunto desses princípios as chances são de que o seu objeto não é um conjunto.

Lembremos que na teoria axiomática tudo é conjunto, não há distinção entre elementos e conjuntos. A ideia é que podemos representar qualquer entidade como conjunto.

**Extensionalidade:** Quaisquer dois conjuntos com os mesmos elementos são iguais.

$$\forall a \forall b ((\forall x (x \in a \leftrightarrow x \in b)) \rightarrow a = b)$$

**Existência:** O conjunto vazio é um conjunto.

$$\exists a \forall x (x \notin a)$$

**Par:** Dados conjuntos  $y$  e  $z$ ,  $\{y, z\}$  é um conjunto.

$$\forall y \forall z \exists a \forall x (x \in a \leftrightarrow x = y \vee x = z)$$

**União:** Para qualquer  $A = \{x, y, z, \dots\}$  conjunto,  $\bigcup A = x \cup y \cup z \cup \dots$  é conjunto.

$$\forall z \exists a \forall x (x \in a \leftrightarrow \exists y (x \in y \wedge y \in z))$$

**Partes:** Para qualquer conjunto  $A$ , o conjunto  $\mathcal{P}(A) = \{B : B \subset A\}$  das partes de  $A$  existe.

$$\forall y \exists a \forall x (x \in a \leftrightarrow x \subseteq y)$$

**Especificação:** Dados um conjunto  $A$  e um predicado  $P$ , o conjunto  $\{x \in A : P(x)\}$  existe.

$$\forall y \exists a \forall x (x \in a \leftrightarrow x \in y \wedge P(x))$$

**Infinito:** Existe um conjunto que tem  $\emptyset$  como um membro e também tem  $x \cup \{x\}$  sempre que  $x$  é membro (isto dá uma codificação de  $\mathbb{N}$ ,  $\emptyset$  representa 0 e  $x \cup \{x\}$  representa  $x+1$ ). Efetivamente, define cada número natural como o conjunto de todos números menores, e.g.,  $0 = \emptyset$ ,  $1 = \{0\}$ ,  $2 = \{0, 1\}$ ,  $3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ .

$$\exists a (\emptyset \in a \wedge \forall x (x \in a \rightarrow x \cup \{x\} \in a))$$

Sem esse Axioma, só obtemos conjuntos finitos.

**Fundação:** Cada conjunto não vazio  $A$  tem um elemento  $B$  com  $A \cap B = \emptyset$ .

$$\forall a (a \neq \emptyset \rightarrow \exists b (b \in a \wedge a \cap b = \emptyset))$$

**Substituição:** Se  $A$  é um conjunto e  $R(x, y)$  é um predicado com a propriedade:  $\forall x \exists! y R(x, y)$ , então  $\{y : \exists x R(x, y)\}$  é um conjunto.

$$\forall x \exists! y R(x, y) \rightarrow \forall b \exists a \forall z (z \in a \leftrightarrow (\exists x \in b) R(x, z))$$

**Escolha:** Para qualquer conjunto formado de conjuntos não-vazios  $A$  existe uma função  $f$  que atribui para cada  $x$  em  $A$  algum  $f(x) \in x$ .

Notemos a forma diferente com que se escreve um conjunto por especificação, com respeito a teoria intuitiva. Agora não temos mais o paradoxo de Russell pois se

$$S = \{x \in A : x \notin x\}$$

então  $S \in S$  se e só se  $S \in A$  e  $S \notin S$  o que não é contraditório: se  $S \in S$  temos  $S \notin S$ , uma contradição, logo  $S \notin S$ ; agora, se  $S \in A$  temos uma contradição, logo  $S \notin A$ ; mas  $S \notin S \wedge S \notin A$  não é contradição. Como subproduto temos o fato já mencionado de que em teoria dos conjuntos *não há conjunto universo*.

**Teorema.**  $\neg \exists y \forall x (x \in y)$ .

De fato, se existisse então tomaríamos-o por  $A$  no argumento acima o que daria uma contradição pois  $S \notin A$ .

## 5.6 Par ordenado e Produto cartesiano

Sejam  $a \in A$  e  $b \in B$ . Pelo axioma do Par  $\{a, b\}$  é conjunto e por Extensionalidade  $\{a, b\} = \{b, a\}$ .

Por *par ordenado* entendemos um par de elementos de modo que a ordem em que tais elementos se apresentam importam e, usualmente, denotamos-o por  $(a, b)$ , de modo que  $(a, b) \neq (b, a)$  exceto quando  $a = b$ . Também, denotamos por  $A \times B$  o conjunto de todos os tais pares  $(a, b)$  com  $a \in A$  e  $b \in B$ , isto é,

$$A \times B = \{(a, b) : a \in A \text{ e } b \in B\}$$

chamado de *produto cartesiano* de  $A$  com  $B$ .

Agora, nessa seção, vamos justificar essas definições na teoria dos conjuntos.

A definição mais simples de par ordenado em termos de conjunto como foi dada pelo matemático polonês Kazimierz Kuratowski

$$(a, b) = \{\{a\}, \{a, b\}\}. \quad (32)$$

Notemos que se  $a \in A$  e  $b \in B$  então  $\{a\} = \{a, a\}$  e  $\{a, b\}$  são conjuntos pelo axioma do Par, o qual também nos dá que  $\{\{a\}, \{a, b\}\}$  é conjunto.

Ainda  $\{a\} \in \mathcal{P}(A \cup B)$  e  $\{a, b\} \in \mathcal{P}(A \cup B)$ , portanto  $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$ , ou seja,  $\{\{a\}, \{a, b\}\} = (a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$ , portanto, existe o conjunto cujos elementos são todos os pares  $(a, b)$  com  $a \in A$  e  $b \in B$ , é o conjunto dada pela especificação

$$\left\{ z \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists x \exists y (x \in A \wedge y \in B \wedge z = (x, y)) \right\}$$

sempre que  $A$  e  $B$  são ambos não vazios.

**Exercício.** Construa a partir dos axiomas o conjunto  $A \cup B$ , dados os conjuntos  $A$  e  $B$ .

Agora, precisamos mostrar que a definição (32) faz o que promete, isto é

**Teorema 32.** Se  $(a, b) = (x, y)$  então  $a = x$  e  $b = y$ .

Para provar o teorema usaremos o seguinte resultado auxiliar

**Lema 33.** Se  $\{a, x\} = \{a, y\}$  então  $x = y$ .

*Demonstração.* Exercício

□

*Demonstração do teorema.* A prova do teorema é por casos, em 2 deles: (1)  $a = b$  e (2)  $a \neq b$ .

Suponha que  $(a, b) = (x, y)$ , isto é,  $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$

Caso 1. Se  $a = b$  então  $(a, b) = \{\{a\}\}$ .

Se  $(a, b) = (x, y)$  então  $\{\{x\}, \{x, y\}\}$  só tem um elemento e esse elemento é  $\{a\}$ , ou seja,  $\{x\} = \{x, y\}$  e  $\{x\} = \{a\}$ . Portanto  $x = y$  e  $x = a$ , ou seja  $\{\{a\}\} = \{\{x\}, \{x, y\}\}$ , portanto,  $\{x\} = \{x, y\}$  e  $\{x, y\} = \{a\}$ , logo  $a = x = y = b$ .

Caso 2.  $a \neq b$ .

Se  $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$  então  $\{x\} \in \{\{a\}, \{a, b\}\}$ .

Se  $\{x\} \in \{\{a\}, \{a, b\}\}$  então  $\{x\} = \{a\}$  ou  $\{x\} = \{a, b\}$ . Se  $a \neq b$  então  $\{x\} = \{a\}$ .

Se  $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$  e  $\{x\} = \{a\}$  então  $\{x, y\} = \{a, b\}$ , pelo lema acima. Se  $\{x\} = \{a\}$  então  $x = a$ .

Se  $\{x, y\} = \{a, b\}$  e  $x = a$ , então  $y = b$ , pelo lema acima.

Portanto  $x = a$  e  $y = b$ .

□

Como no produto cartesiano os pares são ordenados, temos que  $A \times B \neq B \times A$  (exceto quando  $A = B$  ou  $A = \emptyset$  ou  $B = \emptyset$ ).

Podemos definir recursivamente o produto cartesiano de mais de dois conjuntos. De um modo geral, se  $A_1, A_2, \dots, A_n$  são conjuntos não vazios

$$\prod_{i=1}^n A_i = \begin{cases} A_1 & \text{se } n = 1 \\ (\prod_{i=1}^{n-1} A_i) \times A_n & \text{se } n > 1 \end{cases}$$

Definimos  $(a_1, a_2, \dots, a_n) = (a_1)$  se  $n = 1$  e  $(a_1, a_2, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$  se  $n > 1$  então

$$\prod_{i=1}^n A_i = A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_i \in A_i (\forall i)\}.$$

No caso em que os conjuntos  $A_1, A_2, \dots, A_n$  são iguais a  $A$  denotamos por  $A^n$  o produto cartesiano  $\prod_{i=1}^n A_i$ .

Há uma definição para o produto cartesiano de uma quantidade infinita de conjuntos não vazios e provar que esse produto cartesiano resulta num conjunto não vazio depende do axioma da Escolha.

## Relações e funções

Uma *relação* é um subconjunto de um produto cartesiano. Se  $R \subseteq A \times B$  então  $A$  é chamado de domínio e  $B$  de contradomínio da relação.

Usualmente, ao invés de escrevermos  $(x, y) \in R$  escrevemos  $x R y$ , por exemplo,  $3 < 4$  ao invés de  $(3, 4) \in <$ . Por exemplo, se  $A$  é um conjunto então  $R = \{(x, B) \in A \times 2^A : x \in B\}$  é uma relação e  $x R B$  é o mesmo que  $x \in B$ .

O *domínio* e a *imagem* de  $R$  são os conjuntos

$$\begin{aligned}\text{dom}(R) &= \{x \in A : \exists y \in B, x R y\} \\ \text{im}(R) &= \{y \in B : \exists x \in A, x R y\}\end{aligned}$$

Uma relação  $R \subseteq A \times B$  é uma *função* se para cada  $x \in A$  existe um único  $y \in B$  tal que  $(x, y) \in R$ , nesse caso escrevemos  $R : A \rightarrow B$ , o único  $y$  tal que  $(x, y) \in R$  é denotado por  $R(x)$  é dito *o valor que a função assume em x*.

O conjunto de todas as função de  $A$  em  $B$  é um subconjunto de  $\mathcal{P}(A \times B)$  denotado por  $B^A$ .

**Exercício 24.** Verifique a partir dos axiomas de ZFC que  $B^A$  é conjunto.

## 6 Relações

Se  $A_1, A_2, \dots, A_n$  são conjuntos não vazios, um subconjunto  $R \subseteq \prod_{i=1}^n A_i$  é uma *relação  $n$ -ária*. No caso de dois conjuntos, digamos  $A$  e  $B$ , temos uma *relação binária de  $A$  para  $B$*  ou, simplesmente, dizemos *relação*. Uma *relação binária  $R$  sobre  $A$*  é uma relação binária de  $A$  para  $A$ .

**Notação:** Escrevemos  $a R b$  com o significado de  $(a, b) \in R$ . Escrevemos  $a \not R b$  com o significado de  $(a, b) \notin R$ .

São exemplos de relações (binárias)

1.  $< \subset \mathbb{N} \times \mathbb{N}$  é uma relação binária e  $(2, 3) \in <$ , mas usamos  $2 < 3$ .
2.  $| \subset \mathbb{Z}^+ \times \mathbb{Z}^+$  é uma relação binária e  $(2, 4) \in |$ , mas usamos  $2|4$ .
3.  $\subseteq \subset 2^{\mathbb{N}} \times 2^{\mathbb{N}}$  é uma relação binária e  $(\{1, 2\}, \{1, 2, 3\}) \in \subseteq$ , mas usamos  $\{1, 2\} \subseteq \{1, 2, 3\}$ .

### 6.1 Composição e inversa

Assim como as funções, as relações podem ser *compostas*. Dadas as relações  $R \subseteq A \times B$  e  $S \subseteq B \times C$  definimos

$$(S \circ R) \subset A \times C$$

pela regra  $(x, z) \in (S \circ R)$  se, e somente se, existe  $y \in B$  tal que  $(x, y) \in R$  e  $(y, z) \in S$ . Em notação *infixa*

$$x (S \circ R) z \Leftrightarrow \exists y (x R y \wedge y S z)$$

Não é difícil ver que a composição ordinária de funções é um caso especial de composição de relação.

Por exemplo, considere as relações

$$\begin{aligned} R &= \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\} \\ S &= \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\} \end{aligned}$$

A composição delas é

$$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$$

As relações também têm *inversa*

$$x R^{-1} y \Leftrightarrow y R x.$$

Ao contrário das funções, toda relação tem uma inversa.

Por exemplo, tome  $A = \{1, 2, 3\}$  e

$$R = \{(1, 2), (1, 3), (2, 3)\}$$

A relação inversa é

$$R^{-1} = \{(2, 1), (3, 1), (3, 2)\}.$$

Ademais

$$R^{-1} \circ R = \{(1, 1), (1, 2), (2, 2), (2, 1)\}$$

$$R \circ R^{-1} = \{(2, 2), (2, 3), (3, 3), (3, 2)\}$$

**Exercício 25.** Qual é inversa da relação  $<$  sobre  $\mathbb{N}$ ?

**Notação:** Para uma relação genérica, usamos símbolos como  $\sim$ ,  $\equiv$ ,  $\simeq$ ,  $\approx$  ao invés de  $R$ .

## 6.2 Classificação de relações

Uma relação binária  $\sim$  sobre um conjunto  $A$  pode ou não ter uma das seguintes propriedades:

**reflexiva** para todo  $a \in A$ ,  $a \sim a$ ;

**irreflexiva** para todo  $a \in A$ ,  $a \not\sim a$ ;

**simétrica** para todo  $a \in A$ , para todo  $b \in A$ , se  $a \sim b$  então  $b \sim a$ ;

**antissimétrica** para todo  $a \in A$ , para todo  $b \in A$ , se  $a \sim b$  e  $b \sim a$  então  $b = a$ ;

**transitiva** para todo  $a \in A$ , para todo  $b \in A$ , para todo  $c \in A$ , se  $a \sim b$  e  $b \sim c$  então  $a \sim c$ .

Por exemplo, em  $\mathbb{R}$  a relação  $x \sim y$  se, e só se,  $|x - y| < 1$  é reflexiva, simétrica e transitiva.

Uma relação pode ser simétrica e antissimétrica ao mesmo tempo, ou pode não ser nem simétrica nem antissimétrica. Uma relação pode ser nem reflexiva e nem irreflexiva porém, se o conjunto  $A$  não é vazio, uma relação não pode ser ao mesmo tempo reflexiva e irreflexiva sobre  $A$ .

Por exemplo, as relações sobre  $A = \{1, 2, 3, 4\}$

1.  $R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 1), (4, 4)\}$  é reflexiva.
2.  $R_2 = \{(1, 1), (1, 2), (2, 1)\}$  é simétrica.
3.  $R_3 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 1), (1, 4), (4, 4)\}$  é reflexiva e simétrica.
4.  $R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$  é irreflexiva, antissimétrica e transitiva.
5.  $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$  é reflexiva, antissimétrica e transitiva.
6.  $R_6 = (3, 4)$  é irreflexiva, antissimétrica e transitiva.

**Exercício 26.** *A seguir, considere  $A = \{1, 2, 3, 4\}$  e  $B = \{1, 2, 3\}$  e classifique, quanto as propriedades acima, as relações*

1.  $R_1 = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$ .
2.  $R_2 = \{(1, 1), (2, 2), (3, 3)\}$ .
3.  $R_3 = \{(1, 1), (2, 2), (3, 3), (2, 3)\}$ .
4.  $R_4 = \{(1, 1), (2, 3), (3, 3)\}$ .
5.  $R_5 = \{(1, 2), (2, 3), (3, 1)\}$ .

### 6.3 Relações de equivalência

Uma relação é de equivalência se for reflexiva, simétrica e transitiva.

São exemplos de relações de equivalência

1.  $=$  é uma relação de equivalência em  $\mathbb{N}$ .



2.  $\leq$  não é uma relação de equivalência em  $\mathbb{N}$ .
3. Se  $T$  e  $S$  são triângulos no plano e  $T \cong S$  se os triângulos são semelhantes, então  $\cong$  é relação de equivalência sobre o conjunto de todos os triângulos no plano.
4. Semelhança de matriz é uma relação de equivalência sobre o conjuntos de todas as matrizes quadradas de ordem  $n$  de números reais.
5.  $\cong \pmod{3}$  é a relação dada pelos pares de inteiros que deixam o mesmo resto quando divididos por 3, é de equivalência.
6.  $\subset$  não é relação de equivalência sobre o conjunto das partes de  $A$ .

## Partição de um conjunto

O conjunto  $\mathcal{A}$  é uma *partição* do conjunto  $A$  se seus elementos são subconjuntos não-vazio de  $A$ , disjuntos dois-a-dois e a união deles é  $A$ , isto é,

- (a) para todo  $B \in \mathcal{A}$ ,  $B \neq \emptyset$  e  $B \subseteq A$ ;
- (b) para todos  $B, C \in \mathcal{A}$ ,  $B \neq C \Rightarrow B \cap C = \emptyset$ ;
- (c)  $\bigcup \mathcal{A} = A$ .

Por exemplo, sejam  $R_0, R_1$  e  $R_2$  subconjuntos de  $\mathbb{Z}$  definidos por

$$R_i = \{n \in \mathbb{Z} : n \text{ dividido por } 3 \text{ deixa resto } i\}$$

$\{R_0, R_1, R_2\}$  é uma partição de  $\mathbb{Z}$ .

**Teorema 34.** *Se  $\mathcal{A}$  é uma partição do conjunto  $A$ , então a relação binária  $\sim$  sobre  $A$  dada por  $a \sim b$  se, e só se, existe  $B \in \mathcal{A}$  tal que  $\{a, b\} \subseteq B$  é uma relação de equivalência.*

*Demonstração.* Sejam  $A, \mathcal{A}$  e  $\sim$  como dados no enunciado.

A relação  $\sim$  é reflexiva pois para todo  $a \in A$  existe um  $B \in \mathcal{A}$  tal que  $a \in B$  pelo item (c) da definição de partição.

A relação  $\sim$  é simétrica pois para todos  $a, b \in A$  se existe um  $B$  tal que  $\{a, b\} \subseteq B$  então  $\{b, a\} \subseteq B$ .

A relação  $\sim$  é transitiva pois para todos  $a, b, c \in A$  se existe um  $B$  tal que  $\{a, b\} \subseteq B$  e existe um  $C$  tal que  $\{b, c\} \subseteq C$  então, como  $b \in B \cap C$ , temos  $B = C$  pelo item (b) da definição de partição.  $\square$

No exemplo acima  $\{R_0, R_1, R_2\}$  é a partição de  $\mathbb{Z}$  dada pelas restas da divisão por 3. Definimos  $\sim$  sobre  $\mathbb{Z}$  por

$$a \sim b \text{ se existe } i \in \{0, 1, 2\} \text{ tal que } a, b \in R_i$$

isto é,  $a$  e  $b$  estão na relação se deixam o mesmo resto quando divididos por 3.

## Classes de equivalência

Seja  $\sim$  uma relação de equivalência sobre o conjunto  $A \neq \emptyset$  e  $a \in A$

$$[a]_{\sim} = \{b \in A : b \sim a\}$$

é o subconjunto de  $A$  formado por todos os elementos equivalentes a  $a$ , chamado de *classe de equivalência* de  $a$ . O elemento dentro dos colchetes é chamado de *representante* da classe.

Por transitividade, qualquer elemento da classe pode ser seu representante. Seja  $b \in A$  com  $b \sim a$ . Para todo  $c \in [a]_{\sim}$  vale  $c \sim a$ , portanto,  $c \sim b$ , logo  $c \in [b]_{\sim}$ . Reciprocamente, se  $c \in [b]_{\sim}$  então  $c \in [a]_{\sim}$ , por argumento análogo. Assim  $[a]_{\sim} = [b]_{\sim}$ . Também, se  $[a]_{\sim} = [b]_{\sim}$  então de  $a \in [a]_{\sim}$  temos  $a \in [b]_{\sim}$ , portanto  $a \sim b$ . Com isso provamos

$$a \sim b \Leftrightarrow [a]_{\sim} = [b]_{\sim}. \quad (33)$$

O que podemos dizer no caso  $[a]_{\sim} \neq [b]_{\sim}$ ? Imediatamente, por (33) que  $a \not\sim b$ . Para qualquer  $c \in A$ , se  $c \sim a$  então  $b \not\sim c$ , caso contrário teríamos uma contradição pela transitividade, de modo que  $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ .

Concluindo, dos parágrafos precedentes temos que para as classes de equivalência vale um dos casos: para quaisquer  $a, b \in A$

1.  $[a]_{\sim} = [b]_{\sim}$ , ou
2.  $[a]_{\sim} \cap [b]_{\sim} = \emptyset$ .

O conjunto quociente de  $A$  pela relação de equivalência  $\sim$  é o conjunto das classes de equivalência da relação

$$A/\sim = \{[a]_{\sim} : a \in A\}. \quad (34)$$

Já provamos, no teorema 34, que uma partição do conjunto não vazio  $A$  define uma relação de equivalência. A recíproca também vale, uma relação de equivalência sobre  $A$  define uma partição desse conjunto.

**Teorema 35.** *Se  $\sim$  é uma relação de equivalência sobre o conjunto  $A \neq \emptyset$  então  $A/\sim$  é uma partição de  $A$ .*

*Demonstração.* Exercício. □

Por exemplo, no caso de exemplo dos restos de divisão por 3

$$\begin{aligned} R_0 = [0] &= \{\dots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \dots\} \\ R_1 = [1] &= \{\dots, -8, -5, -2, 1, 4, 7, 10, 13, 16, \dots\} \\ R_2 = [2] &= \{\dots, -7, -4, -1, 2, 5, 8, 11, 14, 17, \dots\} \end{aligned}$$

Observemos que  $[0] = [3] = [6]$ .

## 6.4 Relações de ordem

Uma relação  $\preccurlyeq$  sobre um conjunto  $A$  é uma *relação de ordem* se essa for

- reflexiva,
- antissimétrica e
- transitiva.

**Exemplo:**  $\subseteq$  é uma relação de ordem sobre  $2^{\mathbb{Z}}$  e  $\leq$  é uma relação de ordem sobre  $\mathbb{Z}$ .

Há uma diferença importante entre as duas relações de ordem do exemplo anterior, na primeira,  $\subseteq$ , pode haver elementos **incomparáveis**, por exemplo, os conjuntos  $\{1, 2\}$  e  $\{2, 3\}$  são incomparáveis

$$\{1, 2\} \not\subseteq \{2, 3\} \text{ e } \{2, 3\} \not\subseteq \{1, 2\}$$

enquanto que quaisquer dois números inteiros  $x$  e  $y$  são **comparáveis**

$$x \leq y \text{ ou } y \leq x.$$

Se em  $A$  há elementos incomparáveis sob a relação de ordem  $\preceq$  então

$(A, \preceq)$  é uma ordem parcial

ou,  $A$  é conjunto parcialmente ordenado por  $\preceq$  Caso contrário

$(A, \preceq)$  é uma ordem total

ou,  $A$  é conjunto totalmente ordenado por  $\preceq$ .

**Exemplo:**  $(2^A, \subseteq)$ ,  $(\mathbb{Z}, \leq)$  e  $(\mathbb{Z}^+, |)$  são ordens parciais, somente  $(\mathbb{Z}, \leq)$  é total.

## Máximos e mínimos

**Definição 19.** Em  $(A, \preceq)$  temos que  $x \in A$  é um elemento *minimal* se, e só se, para todo  $y \in A$ ,  $y \preceq x$  implica que  $y = x$ .

Em  $(A, \preceq)$  temos que  $x \in A$  é um elemento *maximal* de  $A$  se para todo  $y$ ,  $x \preceq y$  implica que  $y = x$ .

Um conjunto parcialmente ordenado pode ter qualquer número de elementos minimais: os números inteiros não têm mínimo, os naturais têm um mínimo e um conjunto com  $k$  elementos nenhum dos quais são comparáveis entre si tem  $k$  mínimos. As afirmações análogas para maximal também valem.

**Exemplo:** Sejam  $A = \{1, 2, 3, 4, 5, 6\}$  e tomemos em  $A$  a relação de ordem  $\preceq$  dada por  $\{(1, 3), (2, 3), (1, 4), (2, 4), (3, 4), (5, 6), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$ . O número  $2 \in A$ , por exemplo, é um elemento *minimal* de  $(A, \preceq)$ , pois não existe nenhum par  $(a, 2)$ ,  $a \neq 2$ , na relação. Os elementos minimais  $(A, \preceq)$  são 1, 2 e 5.

**Exemplo:** Tomemos  $A = \mathbb{N} \setminus \{0, 1\}$  e  $|$  a relação “divide”. O número 21 não é minimal pois, por exemplo,  $(3, 21) \in |$  e  $3 \neq 21$ . O número 17 é minimal pois não existe nenhum par  $(a, 17)$  com  $a \neq 17$  em  $|$  (a única possibilidade seria o 1 que não está no conjunto). Note que os elementos minimais de  $(A, \preceq)$  são os números primos.

Quando  $A$  é um conjunto de conjuntos e a relação de ordem é  $\subseteq$ , um elemento minimal de  $(A, \subseteq)$  é um conjunto que não contém propriamente nenhum outro elemento de

A. Por exemplo, se  $A = \{\{2\}, \{1, 2\}, \{1, 3\}, \{1, 2, 4\}, \{3, 4, 5\}\}$  então  $\{1, 2, 4\}$  não é minimal (contém propriamente  $\{1, 2\} \in A$ ). São os elementos minimais  $\{2\}$ ,  $\{1, 3\}$  e  $\{3, 4, 5\}$ . O elemento  $\{2\}$  não é maximal (por que?). Os elementos maximais de são  $\{1, 3\}$ ,  $\{1, 2, 4\}$  e  $\{3, 4, 5\}$ .

**Definição 20.** Se um elemento  $x \in A$  satisfaz  $x \preceq y$  para todo  $y \in A$ , então  $x$  é um *mínimo* de  $A$ .

Se um elemento  $x \in A$  satisfaz  $y \preceq x$  para todo  $y \in A$ , então  $x$  é um *máximo* de  $A$ .

Um conjunto parcialmente ordenado tem no máximo um mínimo. Por exemplo, 0 nos naturais é mínimo. Também pode não ter um mínimo como os inteiros negativos ou pode não ter mínimo porque tem mais de um elemento minimal. As afirmações análogas para máximo também valem.

**Exemplo:** Seja  $A = \{2, 4, 6, 8\}$  e seja  $R$  a relação  $\leq$  (menor ou igual) sobre  $\mathbb{Z}$ . O inteiro 2 é um mínimo de  $(A, R)$ . Por outro lado, se  $A$  é o conjunto dos inteiros pares então  $(A, R)$  não tem mínimo.

**Exemplo:** O elemento  $\{2, 4\}$  de  $\{\{1, 2, 4\}, \{2, 4\}, \{2, 3, 4\}, \{2, 4, 5\}, \{2, 3, 4, 6\}\}$ , com a relação de inclusão, é mínimo

**Exemplo:** Exemplo da diferença entre um elemento maximal e um elemento máximo: considere o conjunto  $\mathcal{P}$  de todos os subconjuntos de  $\mathbb{N}$  com no máximo três elementos e ordenados por inclusão  $\subseteq$ . Então  $\{0, 1, 2\}$  é um elemento maximal de  $(\mathcal{P}, \subseteq)$  pois ninguém de  $\mathcal{P}$  o contém e  $\{0, 1, 2\}$  não é máximo porque não contém o elemento  $\{3\}$  de  $\mathcal{P}$ .

**Exercício 27.** Determine os elementos maximais/minimais/máximo/mínimo em  $(\mathbb{Z}^+, |)$ .

**Exercício 28.** Prove que se  $(A, \preceq)$  tem máximo então ele é único.

**Exercício 29.** Prove que todo elemento máximo de uma ordem é maximal.

## Boa ordem

$(A, \preceq)$  é uma *boa ordem* se  $\preceq$  é uma ordem total e todo subconjunto não vazio de  $A$  tem mínimo.

A propriedade útil da Boa-ordem é que ela permite provas por indução, como nos naturais.

**Notação:**  $a \prec b$  significa  $a \preccurlyeq b$  e  $a \neq b$ .

**Teorema 36 (Princípio da Indução para conjuntos bem-ordenados).** *Seja  $(A, \preccurlyeq)$  bem-ordenado e  $P$  um predicado sobre  $A$ . Se para todo  $y \in A$*

*$P(x)$  verdadeiro para todo  $x \in A$  com  $x \prec y$  implica que  $P(y)$  é verdadeiro*

*então  $P(a)$  é verdadeiro para todo  $a \in A$ .*

Em resumo

$$\forall y \in A \left( \left( \forall x \in A (x \prec y \Rightarrow P(x)) \right) \Rightarrow P(y) \right) \Rightarrow \forall a \in A, P(a) \quad (35)$$

*Demonstração.* A prova é por contradição. Sejam  $(A, \preccurlyeq)$  uma boa ordem e  $P$  um predicado sobre  $A$ .

Suponha que para todo  $y \in A$  vale que

$$\left( \forall x \in A (x \prec y \Rightarrow P(x)) \right) \Rightarrow P(y) \quad (36)$$

e assumamos que existe  $a \in A$  tal que  $P(a)$  não é verdadeiro.

Defina

$$S = \{a \in A : \text{não } P(a)\} \quad (37)$$

que, por hipótese é não vazio. Seja  $m$  o menor elemento de  $S$  com respeito a ordem  $\preccurlyeq$ . Então, para todo  $x \prec m$  vale  $P(x)$ . Por (36),  $P(m)$  é verdadeiro, uma contradição.  $\square$

Na axiomática de ZF o seguinte resultado é *equivalente* ao axioma da escolha.

**Teorema 37.** *Para todo conjunto  $A$  não vazio, existe uma ordem total  $\preccurlyeq$  tal que  $(A, \preccurlyeq)$  é boa-ordem.*

## 7 Princípios de contagem: bijeção e cardinalidade

Uma característica importante dos números naturais é que eles respondem a pergunta *quantos elementos tem esse conjunto?* Ou seja, os naturais constituem o modelo matemático que torna possível o processo de contagem.

Contagem é o processo de criar uma bijeção entre um conjunto que queremos contar e algum conjunto cujo tamanho já sabemos. O tamanho de um conjunto é chamado de cardinalidade. Geralmente, não fornecemos uma bijeção explícita para calcular o tamanho de um conjunto, mas sim nos baseamos em princípios de contagem derivados dos processos de construção de conjuntos. O ramo da matemática que estuda conjuntos construídos pela combinação de outros conjuntos é chamado de **Combinatória** e a subárea que estuda os métodos de contagem é chamada de Combinatória Enumerativa.

Cardinalidade é um conceito da Teoria dos Conjuntos que estende para qualquer conjunto a noção quantidade de elementos de um conjunto, a qual é intuitivamente clara no caso de conjuntos finitos: a cardinalidade de um conjunto finito é o número (natural) de elementos no conjunto. Os números cardinais transfinitos descrevem os tamanhos de conjuntos infinitos. Na verdade, a ideia de cardinalidade torna-se bastante sutil quando os conjuntos são infinitos. Há uma sequência transfinita de números cardinais:

$$0, 1, 2, 3, \dots, n, \dots; \aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots, \aleph_{\omega^2}, \dots, \aleph_{\omega^\omega}, \dots, \aleph_\alpha, \dots$$

Os índices dos números *alef* ( $\aleph$ ) são **números ordinais**.

### 7.1 Bijeções

Para contar os elementos de um conjunto é necessário usar a noção de correspondência biunívoca, ou bijeção, ou função bijetiva. Dois conjuntos têm a mesma cardinalidade se, e somente se, há uma correspondência um-para-um (bijeção) entre os elementos dos dois conjuntos.

**Definição 21.** Uma função  $f : X \rightarrow Y$  é **injetiva** quando  $\forall x, x' \in X (x \neq x' \Rightarrow f(x) \neq f(x'))$ .

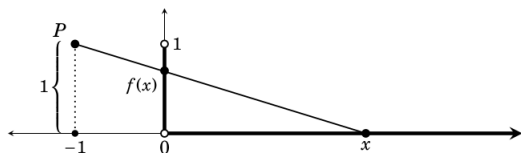
Uma função  $f : X \rightarrow Y$  é **sobrejetiva** quando  $\forall y \in Y \exists x \in X (f(x) = y)$ .

Uma função  $f : X \rightarrow Y$  é **bijetiva** quando for injetiva e sobrejetiva, isto é, quando  $\forall y \in Y \exists! x \in X (f(x) = y)$ .

**Definição 22.** A cardinalidade de  $A$  é denotada por  $|A|$ . Dois conjuntos têm a mesma cardinalidade,  $|A| = |B|$  se, e somente se, existe uma bijeção  $f : A \rightarrow B$ .

Escrevemos  $|A| \leq |B|$  para abreviar que existe  $f : A \rightarrow B$  injetiva.

**Exercício 30.** Verifique que  $f : \mathbb{R}^+ \rightarrow (0, 1)$ , dada por  $f(x) = \frac{x}{x+1}$  é bijetiva. A função  $f$  tem a seguinte interpretação gráfica



Para cada  $x \in (0, +\infty)$  o valor  $f(x)$  é dado pela intersecção da reta que passa por  $x$  e por  $P = (-1, 1)$  com o eixo  $y$ . Usando semelhança de triângulos temos

$$\frac{1}{x+1} = \frac{f(x)}{x}$$

donde tiramos a expressão para  $f(x)$ .

**Exercício 31.** Verifique que  $g : \mathbb{R} \rightarrow \mathbb{R}^+$ , dada por  $g(x) = 2^x$  é bijetiva.

**Exercício 32.** Prove que se  $g : A \rightarrow B$  e  $f : B \rightarrow C$  são bijeções então a função composta  $f \circ g : A \rightarrow C$  é bijeção.

## 7.2 Conjuntos finitos

Definimos  $I_n = \{1, 2, \dots, n\}$  para todo natural  $n \geq 1$ .

**Definição 23.** A cardinalidade do vazio é 0,  $|\emptyset| = 0$ .

Se  $A \neq \emptyset$  então  $|A| = n$  se existe uma bijeção  $f : I_n \rightarrow A$ .

**Definição 24.**  $A$  é **finito** se  $|A| = n$  para algum  $n \in \mathbb{N}$ .

Uma tal bijeção  $f : I_n \rightarrow A$  é chamada de **enumeração** ou **contagem** dos elementos de  $A$ . Desse modo,  $A = \{f(1), f(2), \dots, f(n)\}$  e dizemos que  $A$  tem  $n$  elementos.

**Exercício 33.** Se  $A \neq \emptyset$  é conjunto e  $f : I_n \rightarrow A$  e  $g : I_m \rightarrow A$  são bijeções então  $m = n$ .



Note que a relação de ordem entre cardinais, definição 22, no caso finito concorda com a representação conjuntista de número natural que apresentamos na ocasião dos [Axiomas de ZFC](#):  $1 = \{\emptyset\}$ ,  $2 = \{0, 1\}$ ,  $\dots$ ,  $n = \{0, 1, \dots, n-1\}$  ... Assim  $3 \leq 4$  pois existe  $f : \{0, 1, 2\} \rightarrow \{0, 1, 2, 3\}$  injetiva, a saber  $f(n) = n$ .

**Teorema 38 (princípio aditivo).** *Se  $A$  e  $B$  são conjuntos finitos e disjuntos, então  $|A \cup B| = |A| + |B|$ .*

*Demonstração.* Sejam  $A$  e  $B$  conjuntos disjuntos com cardinalidade  $n$  e  $m$ , respectivamente. Se pelo menos um deles for vazio então o teorema vale como pode ser verificado facilmente.

Vamos supor  $m, n > 0$  e vamos mostrar uma bijeção  $h : I_{n+m} \rightarrow A \cup B$ .

Se  $f : I_n \rightarrow A$  e  $g : I_m \rightarrow B$  são bijeções então definimos  $h$  por

$$h(x) = \begin{cases} f(x) & \text{se } 1 \leq x \leq n \\ g(x - n) & \text{se } n + 1 \leq x \leq n + m. \end{cases}$$

$h$  é sobrejetora: se  $y \in A \cup B$ , então  $y \in A$  ou  $y \in B$ , mas não em ambos já que são disjuntos. Se  $y \in A$  então  $f(x) = y$  para algum  $x \in \{1 \dots, n\}$ , portanto  $h(x) = y$ . Se  $y \in B$  então  $g(x) = y$  para algum  $x \in \{1 \dots, m\}$ , portanto,  $h(x + n) = g(x)$ . Ainda,  $h$  é injetora: como  $A$  e  $B$  são disjuntos, se  $h(x) = h(y)$  então  $f(x) = f(y)$  ou  $g(x) = g(y)$ , em ambos os casos  $x = y$ .  $\square$

**Exercício 34.** *Prove usando indução em  $n$  que se  $A_1, \dots, A_n$  são conjuntos dois-a-dois disjuntos então*

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

**Teorema 39 (princípio multiplicativo).** *Se  $A$  e  $B$  são conjuntos finitos não vazios, então  $|A \times B| = |A| \cdot |B|$ .*

*Demonstração.* Seja  $n = |A|$  e  $A = \{f(1), f(2), \dots, f(n)\}$  para alguma enumeração  $f$  de  $A$ . Definimos os conjuntos dois-a-dois disjuntos

$$E_i = \{(f(i), b) \in A \times B : b \in B\}$$

de modo que  $|E_i| = |B|$ , para todo  $i$ , pela bijeção  $g_i((f(i), b)) = b$ .

Assim,  $\{E_1, \dots, E_n\}$  é uma partição de  $A \times B$  (verifique) e

$$|A \times B| = \left| \bigcup_{i=1}^n E_i \right| = \sum_{i=1}^n |B| = |A| |B| \quad (38)$$

onde a segunda igualdade segue do exercício 34.  $\square$

**Exercício 35.** Prove o teorema acima exibindo uma bijeção entre  $I_{|A||B|}$  e  $A \times B$ .

**Exercício 36.**  $|\{0, 1\}^n| = 2^n$  (prove usando indução em  $n$  uma generalização do princípio multiplicativo e use-a para provar a igualdade proposta).

**Teorema 40.** Todo conjunto  $A$  de cardinalidade  $n \in \mathbb{N}$  tem  $2^n$  subconjuntos distintos, isto é,

$$|2^A| = 2^{|A|}.$$

*Demonstração.* Seja  $A$  um conjunto de cardinalidade  $n$ . Se  $n = 0$  então  $A = \emptyset$  é o único subconjunto dele mesmo e  $2^0 = 1$ .

Se  $n \geq 1$  então existe uma bijeção  $f : I_n \rightarrow A$ . Como  $A = \{f(1), f(2), f(3), \dots, f(n)\}$ , cada subconjunto  $B \subset A$  corresponde a uma, e só uma, sequência  $\mathbf{b}(B) = (b_1, b_2, \dots, b_n) \in \{0, 1\}^n$  dada por

$$b_i = 1 \Leftrightarrow f(i) \in B$$

para cada  $i \in \{1, 2, \dots, n\}$ , ou seja

$$\begin{aligned} \mathbf{b} : 2^A &\rightarrow \{0, 1\}^n \\ B &\mapsto \mathbf{b}(B) \end{aligned}$$

assim definida é bijetiva (verifique), de modo que  $|2^A| = |\{0, 1\}^n|$ , portanto  $|2^A| = 2^n$ .  $\square$

## 7.3 Conjuntos infinitos

**Definição 25.**  $A$  é *infinito* não é finito.

O conjunto dos naturais não é finito. De fato, se houvesse uma bijeção  $f : I_n \rightarrow \mathbb{N}$  então tomaríamos o número natural  $m = f(1) + f(2) + \dots + f(n)$  de modo que  $m$  pertenceria à imagem de  $f$  contradizendo que  $m > f(i)$  para todo  $i \in \{1, \dots, n\}$ .

No caso de conjuntos infinitos não se pode falar em quantidade de elementos e, além disso, dizer simplesmente que são infinitos elementos não diz muita coisa desde que Cantor nos mostrou a possibilidade de vários “tamanhos” de infinito, como veremos a seguir.

**Definição 26.**  $\aleph_0 = |\mathbb{N}|$  é o menor cardinal infinito.

**Teorema 41 (Teorema de Cantor).** Para todo conjunto  $A$ ,  $|A| < |2^A|$ .

*Demonstração.* Se  $A$  é finito então  $|A| < 2^{|A|}$ . Seja  $A$  um conjunto infinito e vamos mostrar que  $|A| \leq |2^A|$  e que  $|A| \neq |2^A|$ . A função

$$\begin{aligned} f : A &\rightarrow 2^A \\ a &\rightarrow \{a\} \end{aligned}$$

é injetiva, portanto  $|A| \leq |2^A|$ .

Para mostrar que  $|A| \neq |2^A|$  provaremos (por contradição) que não há sobrejeção  $g : A \rightarrow 2^A$ .

Suponhamos que  $g : A \rightarrow 2^A$  é sobrejetiva. Definimos

$$B = \{a \in A : a \notin g(a)\}.$$

$B \subset A$  e  $g$  sobrejetiva implica que  $B = g(b)$  para algum  $b$ .

Se  $b \in B$  então  $b \notin g(b) = B$ , pela definição do conjunto  $B$ . Também, se  $b \notin B$  então  $b \in g(b) = B$ , ou seja,  $b \notin B \Leftrightarrow b \in B$ , uma contradição.  $\square$

Em particular, temos

$$|\mathbb{N}| < |2^{\mathbb{N}}| < |2^{2^{\mathbb{N}}}| < \dots$$

**A hipótese do contínuo:** Por quase um século após a descoberta de Cantor de que há diferentes infinitos muitos matemáticos atacaram o problema de descobrir se existe um conjunto  $A$  tal que  $|\mathbb{N}| < |A| < |2^{\mathbb{N}}|$ . Suspeitava-se que tal conjunto não existiria e a proposição que *não existe tal  $A$*  é conhecida como [hipótese do contínuo](#). Gödel, nos anos 1930, provou que a negação da hipótese do contínuo não pode ser provada a partir dos axiomas ZFC. Em 1964, Paul Cohen descobriu que nenhuma prova pode deduzir a hipótese do contínuo a partir dos axiomas de ZFC. Tomados em conjunto, os resultados de Gödel e Cohen significa que dos axiomas padrão da Teoria dos Conjuntos não se pode decidir se a hipótese do contínuo é verdadeira ou falsa; nenhum conflito lógico surge a partir da afirmação ou negação da hipótese do contínuo. Dizemos que a hipótese do contínuo é independente de ZFC. Assumindo a hipótese do contínuo

$$\begin{aligned} \aleph_0 &= |\mathbb{N}| \\ \aleph_{\alpha+1} &= |2^{\aleph_\alpha}| \end{aligned}$$

O seguinte resultado é bastante famoso, ele é altamente não trivial no caso de conjuntos infinitos. A utilidade deste resultado vem do fato que, em geral, estabelecer uma bijeção que comprove  $|A| = |B|$  pode ser muito difícil enquanto que estabelecer funções injetivas que comprovem  $|A| \leq |B|$  e  $|B| \leq |A|$  é mais fácil.

**Teorema 42 (Teorema de Cantor–Bernstein–Schröder).** Se  $|A| \leq |B|$  e  $|B| \leq |A|$  então  $|A| = |B|$ .

Uma demonstração será dada adiante.

## Alguns exemplos importantes

1.  $|\mathbb{N}| = |\mathbb{Z}|$ ;

Para mostrar que  $|\mathbb{N}| = |\mathbb{Z}|$  definimos a função  $f : \mathbb{Z} \rightarrow \mathbb{N}$  dada por

$$f(z) = \begin{cases} 2z, & \text{se } z \geq 0 \\ 2(-z) - 1, & \text{se } z < 0. \end{cases}$$

Dado  $n \in \mathbb{N}$ , se  $n$  é par então  $n = 2z$  para algum  $z \in \mathbb{N}$ , portanto  $f(z) = n$ ; senão  $n$  é ímpar,  $n = 2z - 1$  para algum  $z \in \mathbb{Z}^+$ , portanto  $f(-z) = 2(-(-z)) - 1 = n$ . Assim  $f$  é sobrejetora. Agora, se  $f(z_1) = f(z_2)$  então  $2z_1 = 2z_2$  ou  $2(-z_1) - 1 = 2(-z_2) - 1$  e em ambos os casos  $z_1 = z_2$ . Portanto a função é bijetora.  $\square$

2.  $|\mathbb{N}| = |\mathbb{Q}|$ ;

Claramente há uma função injetiva  $f : \mathbb{N} \rightarrow \mathbb{Q}$  pois  $\mathbb{N} \subset \mathbb{Q}$ , logo  $|\mathbb{N}| \leq |\mathbb{Q}|$ . Para mostrar que  $|\mathbb{Q}| \leq |\mathbb{N}|$  consideremos os racionais não-nulo dados pelas frações da forma

$$\frac{p}{q}, \quad p \in \mathbb{Z} \text{ e } q \in \mathbb{N}, \quad \text{mdc}(p, q) = 1$$

agora, definimos  $g : \mathbb{Q} \rightarrow \mathbb{N}$  por  $g(0) = 0$  e

$$g\left(\frac{p}{q}\right) = \begin{cases} 2^p 3^q, & \text{se } p > 0 \\ 5^p 3^q, & \text{se } p < 0 \end{cases}$$

que é injetiva (verifique). É possível exibir um bijeção entre  $\mathbb{Q}$  e  $\mathbb{N}$  mas isso também é bastante trabalhoso.  $\square$

3.  $|\mathbb{R}| = |(0, 1)|$ ;

Dos exercícios 30 e 31 temos as bijeções  $f : \mathbb{R}^+ \rightarrow (0, 1)$ , dada por  $f(x) = \frac{x}{x+1}$ , e  $g : \mathbb{R} \rightarrow \mathbb{R}^+$ , dada por  $g(x) = 2^x$ , que estabelecem que  $|\mathbb{R}| = |(0, 1)|$  pois  $f \circ g : \mathbb{R} \rightarrow (0, 1)$  também é bijeção.  $\square$

4.  $|\mathbb{N}| < |\mathbb{R}|$ ;

Neste exemplo temos a famosa demonstração de Cantor por diagonalização. Como  $\mathbb{N} \subset \mathbb{R}$ , temos  $|\mathbb{N}| \leq |\mathbb{R}|$  logo precisamos mostrar que  $|\mathbb{N}| \neq |\mathbb{R}|$ . Para tal, mostraremos que  $|\mathbb{N}| \neq |(0, 1)|$ .

Suponha que exista  $f : \mathbb{N} \rightarrow (0, 1)$  bijetiva. Se existe tal  $f$  então podemos enumerar (todos) os elementos do intervalo

$$\begin{aligned} f(0) &= 0, \textcolor{blue}{d}_{0,0} d_{0,1} d_{0,2} d_{0,3} d_{0,4} \dots d_{0,n} \dots \\ f(1) &= 0, d_{1,0} \textcolor{blue}{d}_{1,1} d_{1,2} d_{1,3} d_{1,4} \dots d_{1,n} \dots \\ f(2) &= 0, d_{2,0} d_{2,1} \textcolor{blue}{d}_{2,2} d_{2,3} d_{2,4} \dots d_{2,n} \dots \\ &\vdots \\ f(n) &= 0, d_{n,0} d_{n,1} d_{n,2} d_{n,3} d_{n,4} \dots \textcolor{blue}{d}_{n,n} \dots \\ &\vdots \end{aligned}$$

com  $d_{i,j} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . Consideremos o número real

$$\alpha = 0, d_0 d_1 d_2 d_3 \dots d_n \dots \text{ com } d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \setminus \{0, 9, d_{i,i}\} \ (\forall i \in \mathbb{N}).$$

Esse número  $\alpha$  pertence ao intervalo  $(0, 1)$  pois  $d_i \neq 0$ , logo  $\alpha$  é diferente de  $0 = 0,00000\dots$ , e  $d_i \neq 9$  logo  $\alpha$  é diferente de  $1 = 0,9999\dots$ . Ademais,  $\alpha \neq f(i)$  pois  $d_i \neq d_{i,i}$  para todo  $n \in \mathbb{N}$ , uma contradição. Portanto, não existe  $f : \mathbb{N} \rightarrow (0, 1)$  bijetiva, tampouco  $f : \mathbb{N} \rightarrow \mathbb{R}$  bijetiva.  $\square$

5.  $|\mathbb{R}^2| = |\mathbb{R}|$ ;

Aqui é suficiente basta mostrarmos que  $|(0, 1) \times (0, 1)| \leq |(0, 1)|$  pois, claramente, temos  $|(0, 1)| \leq |(0, 1) \times (0, 1)|$  pela injetiva  $f(x) = (x, 1)$  para todo  $x$ .

Um ponto no quadrado  $(0, 1) \times (0, 1)$  é da forma  $(x, y)$  com  $x = 0, a_1 a_2 a_3 \dots$  e  $y = 0, b_1 b_2 b_3 \dots$  e uma função injetiva sobre  $(0, 1)$  é dada quando mapeamos tal ponto em  $0, a_1 b_1 a_2 b_2 a_3 b_3 \dots$  de  $(0, 1)$ .  $\square$

6.  $|2^{\mathbb{N}}| = |\mathbb{R}|$ .

Que  $|2^{\mathbb{N}}| \leq |(0, 1)|$ : um subconjunto  $B \subseteq \mathbb{N}$  pode ser representado por uma sequência binária infinita  $b_0 b_1 b_2 \dots$  em que  $b_i = 1 \Leftrightarrow i \in B$ , para todo  $i \in \mathbb{N}$ . Essa sequência é mapeada na representação binária  $0, b_0 b_1 b_2 \dots$  de um número real do intervalo  $(0, 1)$ ; tal função é injetora (verifique).

Que  $|(0, 1)| \leq |2^{\mathbb{N}}|$ : defina  $f(0, d_1 d_2 d_3, \dots) = \{10d_1, 10^2 d_2, 10^3 d_3, \dots\}$  e verifique que  $f$  é injetiva.  $\square$

Sob a hipótese do contínuo  $\aleph_1 = |\mathbb{R}|$ .

## 7.4 Conjuntos enumeráveis

O conjunto  $A$  é dito *enumerável* se é finito ou se tem a mesma cardinalidade de  $\mathbb{N}$ , isto é  $|A| = |\mathbb{N}|$  de modo que  $A = \{f(1), f(2), \dots\}$ .  $\mathbb{N}$ ,  $\mathbb{Z}$  e  $\mathbb{Q}$  são enumeráveis.  $\mathbb{R}$  não é enumerável.

Uma dúvida que pode surgir nesse momento é saber se vale a lei de tricotomia para cardinalidades, ou seja, para quaisquer  $A$  e  $B$ , ou  $|A| < |B|$ , ou  $|A| = |B|$ , ou  $|B| < |A|$ . De fato, vale tal lei se assumirmos que vale o axioma da escolha. Nesse caso, vale que para qualquer conjunto  $A$

1. se  $|A| < |\mathbb{N}|$  então  $A$  é finito e enumerável;
2. se  $|A| = |\mathbb{N}|$  então  $A$  é infinito e enumerável;
3. se  $|A| > |\mathbb{N}|$  então  $A$  é infinito e não enumerável.

**Demonstração do Teorema de Cantor–Bernstein–Schröder (opcional):** Antes de demonstrar o teorema vamos adotar a seguinte convenção notacional:  $\overline{A}^X = X \setminus A$ .

*Demonstração.* Sejam  $A$  e  $B$  conjuntos tais que  $|A| \leq |B|$  e  $|B| \leq |A|$  e vamos mostrar que  $|A| = |B|$ . Sejam  $f : A \rightarrow B$  e  $g : B \rightarrow A$  funções injetivas, que existem por hipótese. Vamos mostrar que existe uma bijeção  $h : A \rightarrow B$ .

Definimos, para todo  $X \subset A$

$$F(X) = A \setminus g(B \setminus f(X)) = A \setminus g\left(\overline{f(X)}^B\right) = \overline{g\left(\overline{f(X)}^B\right)}^A$$

onde  $f(X)$  é o subconjunto de  $B$  formado pela imagem dos elementos de  $X$ . Vamos mostrar que existe  $A_0 \subset A$  tal que  $F(A_0) = A_0$ . Primeiro, notemos que para uma

sequência qualquer  $(A_i : i \geq 1)$  de subconjuntos de  $A$  temos

$$\begin{aligned}
F\left(\bigcap_{i \geq 1} A_i\right) &= \overline{g\left(\overline{f\left(\bigcap_{i \geq 1} A_i\right)^B}\right)^A} && \text{por definição} \\
&= \overline{g\left(\overline{\bigcap_{i \geq 1} f(A_i)^B}\right)^A} && \text{pois } f \text{ é injetiva} \\
&= \overline{g\left(\bigcup_{i \geq 1} \overline{f(A_i)^B}\right)^A} && \text{por De Morgan} \\
&= \bigcup_{i \geq 1} \overline{g\left(\overline{f(A_i)^B}\right)^A} && \text{pois } g \text{ é injetiva} \\
&= \bigcap_{i \geq 1} \overline{g\left(\overline{f(A_i)^B}\right)^A} && \text{por De Morgan} \\
&= \bigcap_{i \geq 1} F(A_i) && \text{por definição de } F.
\end{aligned}$$

Tomemos

$$A_0 = A \cap F(A) \cap F^2(A) \cap F^3(A) \cap \dots$$

onde  $F^n(A) = F(F^{n-1}(A))$  donde temos

$$F(A_0) = F\left(A \cap F(A) \cap F^2(A) \cap F^3(A) \cap \dots\right) = F(A) \cap F(F(A)) \cap F(F^2(A)) \cap F(F^3(A)) \cap \dots$$

logo  $F(A_0) = F(A) \cap F^2(A) \cap F^3(A) \cap F^4(A) \cap \dots = A_0$  pois  $A \supset F(A) \supset F^2(A) \supset \dots$ .

Desse modo  $h : A \rightarrow B$  dado por

$$h(x) = \begin{cases} f(x), & \text{se } x \in A_0 \\ g^{-1}(x), & \text{caso contrário, isto é } x \in g\left(\overline{f(A_0)^B}\right) \end{cases} \quad (39)$$

é uma bijeção. Que é sobrejetiva: seja  $y \in B$ . Se  $y \in f(A_0)$ , então  $y = f(x)$  para  $x \in A_0$ , portanto  $y = h(x)$ ; senão,  $y \notin f(A_0)$ , ou seja  $y \in \overline{f(A_0)^B}$ , logo  $g(y) \notin A_0$  logo  $h(g(y)) = g^{-1}(g(y)) = y$ , portanto  $h$  é sobrejetora. Que é injetiva: sejam  $x, y \in A$  com  $x \neq y$ . A demonstração segue em três casos; (i) se  $x, y \in A_0$  então  $h(x) = f(x) \neq f(y) = h(y)$ ; (ii) se  $x \in A_0$ , então  $h(x) = f(x) \in f(A_0)$ , e se  $y \notin A_0$ , ou seja  $y \in g\left(\overline{f(A_0)^B}\right)$ , então  $h(y) = g^{-1}(y) \in g^{-1}\left(g\left(\overline{f(A_0)^B}\right)\right) = \overline{f(A_0)^B}$ , portanto  $h(x) \neq h(y)$ ; (iii) se  $x, y \notin A_0$  então  $h(x) = g^{-1}(x) \neq g^{-1}(y) = h(y)$ . Em todos os casos  $h(x) \neq h(y)$ , logo  $h$  é injetora.  $\square$

## 8 Aula de exercícios e avaliação

1. Prove ou dê contraexemplo: Para todos  $A$ ,  $B$  e  $C$  conjuntos,  $A \subseteq B$  se, e somente se,  $C \setminus B \subseteq C \setminus A$ .
2. Prove ou dê contraexemplo: Para todo  $R_1$  e todo  $R_2$ , se  $R_1$  e  $R_2$  são relações de equivalência sobre um conjunto  $A$  então  $R_1 \cap R_2$  é uma relação de equivalência sobre  $A$ .
3. Defina *conjunto infinito* e prove usando indução que  $A$  é infinito se, e somente se,  $|A| \geq n$  para todo  $n \in \mathbb{N}$ .
4. Prove usando indução em  $n$  que se  $A_1, \dots, A_n$  são conjuntos dois-a-dois disjuntos então

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

5. Sejam  $A_1, A_2, \dots, A_n$  conjuntos finitos e não vazios. Prove usando indução que

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$$

6. Seja  $A$  um conjunto totalmente ordenado pela relação de ordem  $\prec$  e seja  $B$  um conjunto totalmente ordenado pela relação de ordem  $\leq$ . Uma função  $f : A \rightarrow B$  é **crescente** sse

$$\text{para todos } x \text{ e } y \text{ pertencentes a } A, x \prec y \Rightarrow f(x) \triangleleft f(y).$$

Uma função crescente de  $A$  em  $B$  é injetiva? Justifique (dê uma prova ou um contraexemplo).

7. Prove o princípio multiplicativo exibindo uma bijeção entre  $\{1, 2, \dots, |A| \cdot |B|\}$  e  $A \times B$ .
8. Sejam  $A$  um conjunto não vazio,  $\mathfrak{P}$  o conjunto de todas as partições de  $A$  e  $\mathfrak{R}$  o conjunto de todas as relações de equivalência sobre  $A$ .  
Prove que  $f : \mathfrak{R} \rightarrow \mathfrak{P}$  dada por  $f(R) = \{[a]_R : a \in A\}$  para todo  $R \in \mathfrak{R}$  é uma função bijetiva.
9. Prove que se uma ordem parcial  $(A, \preceq)$  tem elemento máximo então ele é único.
10. Prove que se uma ordem parcial  $(A, \preceq)$  tem elemento mínimo então ele é único.
11. Considere  $(\mathbb{Z}^-, \preceq)$  com  $a \preceq b$  se, e somente se,  $|b| \leq |a|$ .

$(\mathbb{Z}^-, \preceq)$  é uma ordem parcial?

$(\mathbb{Z}^-, \preceq)$  é uma ordem total?

$(\mathbb{Z}^-, \preceq)$  é uma boa-ordem?

Justifique as respostas.



12. Considere a relação  $\preccurlyeq$  sobre  $\mathbb{Z}^-$  definida por  $a \preccurlyeq b$  se, e somente se,  $|b| \leq |a|$ .  
 $(\mathbb{Z}^-, \preccurlyeq)$  é uma boa-ordem? Justifique a resposta.
13. Prove que uma relação  $R$  sobre  $A$  é antissimétrica se e somente se  $R \cap R^{-1} \subseteq \{(a, a) : a \in A\}$ .
14. **(Bônus)** Prove que todo conjunto infinito contém um subconjunto infinito enumerável.

## 9 Princípios de contagem: combinatória

Uma interpretação para o **princípio aditivo** é: suponha que o evento  $E$  pode ocorrer  $n$  maneiras e o evento  $F$  de  $m$  maneiras distintas das outras  $n$ . Então, o número de maneiras de ocorrer o evento “ $E$  ou  $F$ ” é  $n + m$ . No caso geral, se  $A_1, \dots, A_n$  são conjuntos dois-a-dois disjuntos então

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

Por exemplo, há quantas possibilidades de escolher um inteiro entre 1 e 16 que é múltiplo de 3 ou de 7? Devemos determinar a cardinalidade do conjunto de inteiros entre 1 e 16 que são múltiplos de 3 ou múltiplos de 7, tais conjuntos são disjuntos pois  $\text{mmc}(3, 7) = 21$ . Os múltiplos de 3 são cinco, os múltiplos de 7 são dois, portanto, os múltiplos de ambos são  $5 + 2 = 7$ . O evento *múltiplo de 3 ou múltiplo de 7* ocorre de 7 modos distintos.

**Teorema 43 (Princípio de Inclusão–Exclusão).** *Se  $E$  e  $F$  são conjuntos finitos (não necessariamente disjuntos) então*

$$|E \cup F| = |E| + |F| - |E \cap F|. \quad (40)$$

*Demonstração.* Sejam  $E$  e  $F$  conjuntos finitos. Podemos escrever  $E \cup F$  como a seguinte união de subconjuntos *disjuntos* (verifique)

$$E \cup F = (E \setminus F) \cup (F \setminus E) \cup (E \cap F)$$

portanto, pelo princípio aditivo

$$|E \cup F| = |E \setminus F| + |F \setminus E| + |E \cap F|. \quad (41)$$

Também podemos escrever  $E$  como uma união disjunta (verifique)

$$E = (E \setminus F) \cup (E \cap F)$$

portanto  $|E| = |E \setminus F| + |E \cap F|$  donde deduzimos

$$|E \setminus F| = |E| - |E \cap F| \quad (42)$$

Analogamente,

$$|F \setminus E| = |F| - |E \cap F| \quad (43)$$

Finalmente, substituindo (42) e (43) em (41)  $|E \cup F| = |E| + |F| - |E \cap F|$ .  $\square$

Por exemplo, o número de possíveis resultados que são múltiplo de 2 ou de 3 no lançamento de uma dado é dado por: os múltiplos de 2 definem o subconjunto  $E = \{2, 4, 6\}$ , os múltiplos de 3 definem o subconjunto  $F = \{3, 6\}$ , portanto,

$$|E \cup F| = |E| + |F| - |E \cap F| = 4. \quad (44)$$

**Exercício 37.** Prove que se  $A$ ,  $B$  e  $C$  são conjuntos finitos então

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|. \quad (45)$$

**Exemplo:** Em uma academia de arte, há 43 estudantes que tomam aula de cerâmica, 57 estudantes que fazem pintura e 29 estudantes que tomam aula de escultura. Há 10 alunos em cerâmica e pintura, 5 em pintura e escultura, 5 em cerâmica e escultura e 2 tendo todos os três cursos. Quantos alunos estão fazendo pelo menos um curso na academia de arte? Vamos indicar por  $C$ ,  $P$  e  $E$  os conjuntos de alunos que fazem cerâmica, pintura e escultura, respectivamente. Queremos calcular  $|C \cup P \cup E|$ . Aplicamos inclusão-exclusão:  $|C \cup P \cup E| = |C| + |P| + |E| - |C \cap P| - |P \cap E| - |C \cap E| + |C \cap P \cap E| = 111$ .

**Exercício 38.** De quantas maneiras podemos escolher um número em  $\{1, 2, \dots, 100\}$  que não é divisível por 2, 3 ou 5?

**Teorema 44 (Princípio da Casa dos Pombos).** Sejam  $E$  e  $F$  conjuntos finitos não vazios. Se existe função  $f : E \rightarrow F$  injetiva então  $|E| \leq |F|$ .

Antes de demonstrar esse resultado definimos a **imagem inversa** de  $y \in F$  pela função  $f$  como o conjunto

$$f^{-1}(y) = \{x \in E : f(x) = y\}$$

e notemos que se  $f$  for sobrejetiva então  $f^{-1}(y) \neq \emptyset$  para todo  $y \in F$ , e se  $f$  for injetiva então  $|f^{-1}(y)| \leq 1$  para todo  $y \in F$ .

*Demonstração.* Sejam  $E$  e  $F \neq \emptyset$  conjuntos finitos. Suponha que  $f : E \rightarrow F$  seja uma função injetiva.

Se  $F$  é finito, então existe  $h : I_m \rightarrow F$  para algum  $m \in \mathbb{N}$ , de modo que

$$F = \{h(1), h(2), \dots, h(m)\}.$$

Se  $f : E \rightarrow F$  é função então  $E$  é a união

$$E = f^{-1}(h(1)) \cup f^{-1}(h(2)) \cup \dots \cup f^{-1}(h(m))$$

de conjuntos disjuntos dois-a-dois. Ademais, se  $f$  injetiva então  $|f^{-1}(h(i))| \leq 1$  para todo  $i \in \{1, 2, \dots, m\}$ . Pelo princípio aditivo

$$|E| = |f^{-1}(h(1))| + |f^{-1}(h(2))| + \dots + |f^{-1}(h(m))|$$

Pela injetividade

$$|f^{-1}(h(1))| + |f^{-1}(h(2))| + \dots + |f^{-1}(h(m))| \leq m$$

portanto  $|E| \leq |F|$ . □

**Corolário 45.** *Sejam  $E$  e  $F$  conjuntos finitos não vazios. Se  $|F| < |E|$  então para toda  $f : E \rightarrow F$  existe  $y \in F$  tal que*

$$|f^{-1}(y)| \geq \frac{|E|}{|F|}.$$

*Demonstração.* Seguindo a demonstração do teorema, se não existe tal  $y$  então

$$|E| = |f^{-1}(h(1))| + |f^{-1}(h(2))| + \dots + |f^{-1}(h(m))| < |F| \frac{|E|}{|F|}$$

que é uma contradição. □

**Exemplo:** Dado  $n \in \mathbb{N}$ , existem números inteiros positivos  $a$  e  $b$ , com um  $a \neq b$ , tal que  $n^a - n^b$  é divisível por 10. Considere os seguintes 11 números

$$n^1 \quad n^2 \quad n^3 \quad n^4 \quad n^5 \quad n^6 \quad n^7 \quad n^8 \quad n^9 \quad n^{10} \quad n^{11}$$

como há 10 possibilidades para o algarismo da unidade, a saber  $\{0, 1, 2, \dots, 9\}$ , dois desses números, digamos  $n^a$  e  $n^b$  com  $a \neq b$ , termina com o mesmo algarismo de modo que  $n^a - n^b$  é divisível por 10.

**Exercício 39.** *Se cinco pontos são distribuídos num quadrada de lado 1 então há dois deles cuja distância é no máximo  $\sqrt{2}/2$ .*

**Exemplo:** Em qualquer escolha de mais que  $n$  números do conjunto  $\{1, 2, \dots, 2n\}$  um dos escolhidos será múltiplo de um outro escolhido. Se  $r \in \{1, 2, \dots, 2n\}$  então, pelo [teorema fundamental da aritmética](#), esse número pode ser escrito de forma única como  $r = 2^a t$  com  $a, t$  naturais e  $t$  ímpar. Se  $t$  é ímpar, então  $t \in \{1, 3, 5, 7, \dots, 2n-1\}$ . Então, em mais que  $n$  números dois deles terão o mesmo divisor ímpar, digamos  $r = 2^a t$  e  $s = r = 2^b t$ . O maior deles é múltiplo do menor.

**Exercício 40.** *Em qualquer escolha de mais que  $n$  números do conjunto  $\{1, 2, \dots, 2n\}$  haverão dois deles primos entre si.*

Uma interpretação para o **princípio multiplicativo** é: se um evento pode ser descrito em duas etapas de modo que há  $n$  desfechos possíveis para a 1ª etapa e há  $m$  desfechos possíveis para a 2ª etapa, então o número de possíveis desfechos para o evento é  $n \cdot m$ .

De um modo geral, se  $E_1, \dots, E_r$  representam  $r$  etapas de evento composto, então o números de modos distintos de realizar o evento é

$$\left| \prod_{i=1}^r E_i \right| = |E_1| \cdot |E_2| \cdots |E_r| \quad (46)$$

que pode ser demonstrado usando princípio da indução.

**Exercício 41.** *Uma placa de carro é uma sequência de 3 letras seguidas por 4 dígitos. Qual é a quantidade de placas distintas que podemos obter?*

*Esboço de solução.*  $E_i = \{A, B, \dots, Z\}$  para  $i = 1, 2, 3$ .

$E_i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  para  $i = 4, 5, 6, 7$ .

$$\left| \prod_{i=1}^8 E_i \right| = 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 26^3 10^4 = 175.760.000. \quad \square$$

**Exemplo:** Cada posição da memória (célula de memória) de um computador tem um endereço que é uma sequência binária. As arquiteturas com processadores 32-bits tem capacidade para endereçamento de  $2^{32} = 4.294.967.296$  posições de memória, aproximadamente 4 Gigabytes. As arquiteturas com processadores 64-bits tem capacidade para endereçamento de

$$2^{64} = 18.446.744.073.709.551.616$$

posições de memória, aproximadamente 16 Exabytes (16 milhões de Terabytes). Suponhamos que um dispositivo de 1 Gigabyte ocupe um dispositivo de dimensões  $1 \text{ mm} \times 1 \text{ mm} \times 1 \text{ mm}$ . Para guardar 16 Exabytes precisaríamos de uma quarto de dimensões  $2,5 \text{ m} \times 2,5 \text{ m} \times 2,5 \text{ m}$ .

A seguir destacamos alguns casos particulares do princípio multiplicativo. Essencialmente são dois tipos de listas: *arranjos* e *combinações*. Nos arranjos a ordem dos elementos importa e nas combinações a ordem não importa.

## 9.1 Arranjos

Quantas palavras (sequências) de 3 letras *distintas* do alfabeto latino podem ser formadas? Como o alfabeto tem 26 letras, pelo princípio multiplicativo são  $26 \cdot 25 \cdot 24$  palavras.

**Definição 27.** Um *arranjo simples* de  $r$  elementos tomados de um conjunto  $A$  de  $n$  elementos ( $r \leq n$ ) é uma sequência  $(a_1, a_2, \dots, a_r)$  de elementos não repetidos de  $A$ . A quantidade de arranjos simples de  $r$  elementos tomados de um conjunto de  $n$  elementos ( $r \leq n$ ) é o número  $(n)_r$  dado por

$$(n)_r = n(n-1)(n-2) \cdots (n-r+1) \quad (47)$$

Quando é permitido repetição dizemos *arranjo com repetição* que é um caso particular do Princípio Multiplicativo com todos os conjuntos iguais. A quantidade de arranjos com repetição de  $r$  elementos tomados de um conjunto de  $n$  elementos é o número  $n^r$ .

Por *arranjo* nos referimos a arranjo simples. Alguns textos usam a notação  $A(n, r)$  para  $(n)_r$ .

**Exemplo:** De quantas maneiras podemos escolher um inteiro entre 000 e 999 (inclusive e com 3 dígitos) com todos os dígitos distintos? O conjunto tem 1.000 elementos e a quantidade deles sem dígitos repetidos é  $(10)_3 = 10 \cdot 9 \cdot 8 = 720$ .

**Paradoxo do aniversário:** Com que probabilidade ocorre que num grupo com 25 pessoas 2 ou mais pessoas façam aniversário no mesmo dia? O aniversário de 25 pessoas pode ocorrer de  $365^{25}$  modos diferentes. O aniversário de 25 pessoas sem que nenhum deles coincida pode ocorrer de  $(365)_{25}$  modos diferentes. Portanto, há  $365^{25} - (365)_{25}$  possibilidades diferentes para o aniversário de 25 pessoas com pelo menos duas aniversariando no mesmo dia; a probabilidade desse evento é

$$\frac{365^{25} - (365)_{25}}{365^{25}} = 1 - \frac{(365)_{25}}{365^{25}} > 0,56.$$

Com 55 pessoas a probabilidade é maior que 98%.

**Exercício 42.** Sejam  $A$  e  $B$  conjuntos finitos com  $|A| \leq |B|$ . Há quantas funções injetivas de  $A$  em  $B$ ? E quantas são as funções de  $A$  em  $B$ ?

## Permutação

**Exemplo:** De quantas maneiras diferentes 8 alunos podem se sentar numa sala com 8 cadeiras? O primeiro aluno tem 8 opções, o segundo tem 7, o terceiro tem 6, o quarto tem 5, o quinto tem 4, o sexto tem 3, o sétimo tem 2 e para o oitavo resta 1 opção. Logo há  $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40320$  maneiras dos 8 alunos sentarem nas 8 cadeiras.

O caso de arranjo simples com  $r = n$  é uma *permutação*. Quantas palavras com letras *distintas* podem ser formadas com as letras  $a, b$  e  $c$ ? Pelo princípio multiplicativo são  $3 \cdot 2 \cdot 1 = 6$  palavras.

**Definição 28.** Uma *permutação* de elementos de um conjunto  $A$  é uma sequência de elementos de  $A$ . O número de permutações dos elementos de um conjunto de  $n \geq 0$  elementos é

$$\begin{aligned} 0! &= 1 \\ n! &= n(n-1)! \text{ se } n \geq 1. \end{aligned}$$

**Exemplo:** O número de permutações possíveis com as letras  $a, b, c, d$  e  $e$  é  $5! = 120$ . O número de permutações possíveis com as letras  $a, b, c, d, e$  e  $f$  é  $6! = 720$ .

**Exemplo:** A quantidade de permutações que podem ser formadas com as letras da palavra *livros* é  $6! = 720$ . A quantidade de permutações que podem ser formadas com as letras da palavra *teclado* é  $7! = 5.040$ . A quantidade de permutações que podem ser formadas com as letras da palavra *discreta* é  $8! = 40.320$ . A quantidade de permutações que podem ser formadas com as letras da palavra *universal* é  $9! = 362.880$ . A quantidade de permutações que podem ser formadas com as letras da palavra *pernambuco* é  $10! = 3.628.800$ . A quantidade de permutações que podem ser formadas com as letras da palavra *seminublado* é  $11! = 39.916.800$ . A quantidade de permutações que podem ser formadas com as letras da palavra *configuravel* é  $12! = 479.001.600$ .

Perceba que o fatorial cresce bastante rápido com  $n$ :

- 11! é mais que a quantidade de segundos que passam em 1 ano.
- 12! é mais que a quantidade de segundos que passam em 12 anos.
- 13! é mais que a quantidade de segundos que passam em 100 anos.

Notemos que

$$(n)_r = \frac{n!}{(n-r)!}. \quad (48)$$

## Permutação com repetição

**Exercício 43.** Qual é o número de permutações distintas com as letras da palavra *ana*?

*Solução.* São  $3!$  permutações de 3 símbolos, mas há permutações que dão origem a mesma sequência. As seis permutações de **ana** são:

**ana**      **ana**      **aan**      **aan**      **naa**      **naa**

em cada duas permutações a palavra é a mesma, só muda a ordem da letra repetida, portanto são

$$\frac{3!}{2!} = 3$$

permutações distintas. □

**Exercício 44.** Qual é o número de permutações distintas com as letras da palavra *bala*?

*Solução.* da mesma maneira, das  $4!$  permutações as  $2!$  permutações que troca a ordem da letra igual e deixam as outras letras na mesma posição da sequência geram a mesma palavra, portanto são

$$\frac{4!}{2!} = 12$$

permutações distintas. □

**Exercício 45.** Qual é o número de permutações distintas com as letras da palavra *banana*?

*Solução.* São  $6!$  permutações de 6 símbolos. Mas agora há permutações que diferem apenas na ordem das letras *a* ou das letras *n* e dão origem a mesma sequência, por exemplo:

**banana**      **banana**      **banana**      **banana**



são permutações diferentes que determinam a mesma sequência. As  $3!$  permutações das letras  $a$  são indistinguíveis, assim como as  $2!$  da letras  $n$ , portanto, há

$$\frac{6!}{3!2!} = 60$$

permutações distintas. □

**Exercício 46.** *Um sinal é composto por nove bandeiras alinhadas. Quantos sinais diferentes é possível formar quando há disponíveis 4 bandeiras brancas, três bandeiras vermelhas e duas bandeiras azuis? Bandeiras da mesma cor são idênticas.*

*Esboço de solução.*  $\frac{9!}{4!3!2!} = 1.260$ . □

**Definição 29.** *No caso de permutações com repetição de objetos, se são  $n$  objetos no total, com  $r$  tipos de objetos distintos e  $k_i$  objetos do tipo  $i$  ( $1 \leq i \leq r$ ,  $n = k_1 + \dots + k_r$ ) então temos  $n!$  permutações donde descontamos as  $k_i!$  permutações de objetos do mesmo tipo resultando*

$$\binom{n}{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! k_2! \dots k_r!} \quad (49)$$

**Mão de bridge:** Numa mão de Bridge as 52 cartas de um baralho embaralhado são divididas igualmente entre 4 jogadores. O número de modos distintos com que isso é feito pode ser calculado da seguinte forma: uma distribuição de cartas corresponde a uma sequência de 52 objetos, os 13 primeiros objetos da sequência são as cartas do primeiro jogador, os 13 seguintes do segundo jogador, os próximos 13 do terceiro e os 13 últimos objetos da sequência são as cartas do quarto jogador. Há  $52!$  sequências distintas de cartas. Entretanto, dessas  $52!$  temos que, para cada jogador,  $13!$  permutações correspondem a mesma sequência de cartas em sua mão, portanto, são

$$\binom{52}{13, 13, 13, 13} = 53.644.737.765.488.792.839.237.440.000$$

modos distintos de distribuir as cartas, ou mãos diferentes de início de jogo.

**Exercício 47.** *Se numa mão de Bridge as 52 cartas de um baralho são divididas igualmente e aleatoriamente entre 4 jogadores. Com que probabilidade cada jogador recebe um ás?*

*Solução.* Os 4 ases podem ser distribuídos de  $4!$  modos distintos entregando um para cada jogador. As 48 cartas restantes são distribuídas pelos jogadores de  $\binom{48}{12, 12, 12, 12}$

maneiras distintas. Pelo princípio multiplicativo são  $4! \binom{48}{12,12,12,12}$  modos distintos de os jogadores receberem um ás cada. Portanto a probabilidade é

$$\frac{4! \binom{48}{12,12,12,12}}{\binom{52}{13,13,13,13}}$$

que vale aproximadamente 0,0044. □

**Exercício 48.** *Quantos são as permutações das letras da palavra MATEMÁTICA?*

## Permutação circular

De quantos modos 5 crianças podem formar uma roda de ciranda? As rodas *abcde*, *eabcd* e *deabc*, por exemplo, são iguais pois importa apenas a posição relativa entre as crianças. Assim cada roda pode ser girada de cinco maneiras e a resposta correta é  $5!/5 = 4! = 24$

**Definição 30.** *O número de permutações circulares de  $n$  objetos distintos, se consideramos equivalentes disposições que possam coincidir por rotação, é igual a*

$$(PC)_n = \frac{n!}{n}$$

## Aproximação de Stirling

Duas sequências de números  $a_n$  e  $b_n$  são *assintoticamente iguais* e escrevemos  $a_n \sim b_n$ , se

$$\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = 1.$$

Frequentemente, é muito útil quando trabalhamos com fatoriais a seguinte igualdade assintótica conhecida como fórmula de Stirling

$$n! \sim n^n e^{-n} \sqrt{2\pi n} \tag{50}$$

$n$	$n!$	stirling
1	1	0.922137
2	2	1.919004
3	6	5.83621
7	5040	4980.396
10	3628800	3598696
20	$2.432902e + 18$	$2.422787e + 18$
50	$3.041409e + 64$	$3.036345e + 64$
75	$2.480914e + 109$	$2.478159e + 109$
100	$9.332622e + 157$	$9.324848e + 157$
142	$2.695364e + 245$	$2.693783e + 245$

## 9.2 Combinações

Tomemos um arranjo de  $r$  elementos escolhidos de um conjunto com  $n$  elementos. A quantidade de arranjos que têm os mesmos  $r$  elementos é  $r!$  pois a única diferença entre eles é a ordem com que se apresentam os  $r$  elementos. Por exemplo, se selecionamos sequencialmente e sem reposição 3 cartas de um baralho então temos  $52 \cdot 51 \cdot 50$  arranjos distintos, um dos quais é  $(\heartsuit K, \clubsuit 5, \diamond Q)$ . Agora, se selecionamos três cartas de uma só vez as  $3!$  permutações de  $(\heartsuit K, \clubsuit 5, \diamond Q)$  correspondem a mesma seleção. A quantidade de seleções distintas é

$$\frac{52 \cdot 51 \cdots 50}{3!} = \frac{52!}{49!3!}.$$

**Exercício 49.** *Seja  $A$  um conjunto com  $n$  elementos. Dado  $k$ ,  $0 \leq k \leq n$ , quantos subconjuntos de cardinalidade  $k$  estão contidos em  $A$ ?*

*Solução.* Denote por  $S(k, n)$  a quantidade de subconjuntos de cardinalidade  $k$  estão contidos em  $A$ .

Um único subconjunto de tamanho  $k$  determina  $k!$  arranjos de  $k$  elementos de  $A$ . Subconjuntos distintos determinam arranjos distintos, portanto,  $S(k, n) \cdot k! = (n)_k$ , ou seja

$$S(k, n) = \frac{(n)_k}{k!}$$

Usando (48)

$$S(k, n) = \frac{n!}{k!(n-k)!}$$

□

**Definição 31.** Uma *combinação* de  $r$  elementos escolhidos de um conjunto  $A$  com  $n$  elementos é simplesmente um subconjunto com  $r$  elementos de  $A$ . A quantidade de subconjuntos de  $A$  com  $r$  elementos, para  $0 \leq r \leq n$ , é o *coeficiente binomial*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Convencionamos que  $\binom{a}{b} = 0$  se  $a < b$ .

**Exemplo (Mega-Sena):** O jogo de apostas consiste em acertar 6 dezenas escolhidas dentre 60. O número de possíveis resultados distinto para a Mega-Sena é  $\binom{60}{6} = 50.063.860$ . Se uma aposta em seis números demorar 1 segundo para ser registrada, então registrar 50.063.860 demoraria um ano e meio, aproximadamente. A probabilidade de acertar os seis números é

$$\frac{1}{\binom{60}{6}} = \frac{1}{50.063.860} \approx 2 \times 10^{-8}.$$

A chance<sup>1</sup> de morrer por raio no Brasil em 2010 era  $0,8 \times 10^{-6}$  (40 vezes maior).

**Exemplo:** Numa população com  $n$  elementos,  $n_1$  são azuis e  $n_2 = n - n_1$  são verdes. De quantas maneiras podemos escolher  $k$  elementos com  $r$  deles azuis? ( $0 \leq r \leq \min\{n_1, k\}$ ) O número de maneiras de escolher  $k - r$  verdes é  $\binom{n_2}{k-r}$ . O número de maneiras de escolher  $r$  azuis é  $\binom{n_1}{r}$ . Pelo Princípio Multiplicativo, o número de maneiras de escolher  $r$  azuis e  $k - r$  verdes é  $\binom{n_2}{k-r} \binom{n_1}{r}$ .

**Exercício 50.** Prove que a seguinte identidade

$$i \binom{n}{i} = n \binom{n-1}{i-1}. \quad (51)$$


**Exercício 51.** Três bolas são retiradas aleatoriamente de uma caixa com 6 bolas brancas e 5 bolas pretas. Com que probabilidade a escolha resulta em 1 branca e 2 pretas?

*Solução.* No total são 13 bolas das quais escolhemos 3. O número de possíveis resultados é  $\binom{13}{3}$ . “6 bolas brancas e 5 bolas pretas” ocorre de  $\binom{6}{1} \binom{5}{2}$  modos diferentes, pelo exercício anterior. Portanto a probabilidade é  $\frac{\binom{6}{1} \binom{5}{2}}{\binom{13}{3}}$ .  $\square$

---

<sup>1</sup>esse número é uma média no sentido de que considera que todos têm a mesma chance de ser atingido, o que não é real. [[http://www2.uol.com.br/sciam/reportagens/os\\_numeros\\_surpreendentes\\_de\\_mortes\\_por\\_raios\\_no\\_brasil.html](http://www2.uol.com.br/sciam/reportagens/os_numeros_surpreendentes_de_mortes_por_raios_no_brasil.html)]

## Combinação com repetição

Se escolhemos uma peça de dominó ao acaso, com que probabilidade obtemos  ?

As peças de dominós são formadas por dois números tomados dos números de 0 a 6 podendo haver repetição. Os dominós com pares de números diferentes são  $\binom{7}{2} = 21$ , mais os 7 pares repetidos resultam em 28 peças de dominós, portanto, são 28 combinações de 2 objetos tomados dentre 7 com repetição. Essa estratégia de contagem não é facilmente generalizável, o leitor pode tentar contar o número de peças de dominós de 5 pontas com 16 possíveis números diferentes, o resultado deverá ser 15.504.

A resposta para o caso geral: dentre  $n$  objetos, queremos selecionar  $r$  podendo haver repetição e sem considerar ordem. Isso pode ser feito de

$$\binom{n+r-1}{r} \quad (52)$$

maneiras diferentes. No caso dos dominós, por exemplo, são 7 números dos quais selecionamos 2, podendo repetir número

$$\binom{7+2-1}{2} = \binom{8}{2} = \frac{8!}{6!2!} = 36.$$

Uma maneira de modelar combinação com repetição para deduzir equação (52) é escrever uma equação com uma indeterminada para cada um dos  $n$  objetos,  $x_1, x_2, \dots, x_n$ . A variável  $x_i$  indica quantas vezes o  $i$ -ésimo objeto será selecionado, portanto  $x_1 + x_2 + \dots + x_n = r$ . Assim, o número combinações com repetição é a quantidade de soluções inteiras de

$$x_1 + x_2 + x_3 + \dots + x_n = r \text{ com } x_i \in \{0, 1, 2, \dots\} \text{ para todo } i. \quad (53)$$

## Soluções inteiras de equações lineares

Vamos começar com um caso simples, estudaremos o número de soluções de

$$x_1 + x_2 + x_3 = 6 \text{ com } x_i \in \{1, 2, \dots\} \text{ para todo } i. \quad (54)$$

Escrevemos

$$1 + 1 + 1 + 1 + 1 + 1 = 6 \quad (55)$$

e uma solução da equação (54) corresponde a escolha de 2 operadores + dentre os 5 escritos na equação acima; por exemplo, se usamos  $\oplus$  para representar as escolhas

$$\underbrace{1+1}_{x_1} \oplus \underbrace{1+1+1}_{x_2} \oplus \underbrace{1}_{x_3} = 6 \quad (56)$$

corresponde a  $x_1 = 2$ ,  $x_2 = 3$  e  $x_3 = 1$ , e

$$\underbrace{1+1}_{x_1} \oplus \underbrace{1+1}_{x_2} \oplus \underbrace{1+1}_{x_3} = 6 \quad (57)$$

corresponde a  $x_1 = 2$ ,  $x_2 = 2$  e  $x_3 = 2$ . Portanto essa equação tem  $\binom{5}{2}$  soluções em  $\mathbb{Z}^+$ .

Agora, estudaremos o número de soluções de

$$x_1 + x_2 + x_3 = 6 \text{ com } x_i \in \{0, 1, 2, \dots\} \text{ para todo } i. \quad (58)$$

Notemos que uma solução  $(x_1, x_2, x_3) = (x, y, z)$  inteira e *positiva* da equação  $x_1 + x_2 + x_3 = 6 + 3$  determina uma única solução inteira e *não-negativa*  $(x-1, y-1, z-1)$  da equação  $x_1 + x_2 + x_3 = 6$  e vice-versa, ou seja, as equações

$$\begin{aligned} x_1 + x_2 + x_3 &= 6 + 3 & \text{com } x_i \in \{1, 2, 3, \dots\} & \text{ para todo } i. \\ x_1 + x_2 + x_3 &= 6 & \text{com } x_i \in \{0, 1, 2, 3, \dots\} & \text{ para todo } i. \end{aligned}$$

têm o mesmo número de soluções.

De volta ao problema que gerou essa discussão: o número de maneiras de selecionar  $r$  objetos, podendo haver repetição, dentre  $n$  objetos é igual ao número de soluções inteiras da equação (53), que é o mesmo número de soluções inteiras de

$$x_1 + x_2 + x_3 + \dots + x_n = n + r \text{ com } x_i \in \{1, 2, \dots\} \text{ para todo } i. \quad (59)$$

consideramos  $1 + 1 + 1 + \dots + 1 = n + r$  e dos  $n + r - 1$  operadores + escolhemos  $n - 1$ , ou seja, são  $\binom{n+r-1}{n-1}$  soluções inteiras. Finalmente, a equação (52) segue do seguinte exercício

**Exercício 52.** *Verifique que vale*

$$\binom{n+r-1}{r} = \binom{n+r-1}{n-1} \quad (60)$$

para todo  $n$  e todo  $r$  para os quais os coeficientes binomiais estão definidos.

A quantidade de maneiras diferentes de selecionarmos  $r$  elementos de um conjunto de  $n$  elementos é,

	com repetição	sem repetição
com ordem	$n^r$	$\binom{n}{r}_r$
sem ordem	$\binom{n+r-1}{r}$	$\binom{n}{r}$

### 9.3 Binômio de Newton

Se  $A$  é um conjunto com  $n$  elementos então a quantidade de subconjuntos de  $A$  de cardinalidade  $r$  é o número de maneiras distintas que podemos selecionar  $r$  elementos dentre os  $n$  do conjunto, isto é, são  $\binom{n}{r}$  subconjuntos, como há  $2^n$  subconjuntos de  $A$  concluímos que

$$\sum_{r=0}^n \binom{n}{r} = 2^n \quad (61)$$

Esse fato é consequência, também, de um resultado mais geral conhecido como Teorema Binomial.

**Teorema 46** (Teorema Binomial). *Para todo  $n > 0$ , vale*

$$(x + y)^n = \sum_{r=0}^n \binom{n}{r} x^r y^{n-r}.$$

Fazendo  $x = y = 1$  temos a equação (61).

Veamos como o produto se desenvolve para valores pequenos de  $n$

$$\begin{aligned} (x + y)(x + y) &= (x + y)x + (x + y)y \\ &= xx + yx + xy + yy \\ (x + y)(x + y)(x + y) &= (x + y)(xx + yx + xy + yy) \\ &= (x + y)xx + (x + y)yx + (x + y)xy + (x + y)yy \\ &= xxx + yxx + xyx + yyx + xxy + yxy + xyy + yyy \\ (x + y)(x + y)(x + y)(x + y) &= (x + y)(xxx + yxx + xyx + yyx + xxy + yxy + xyy + yyy) \\ &= xxxx + xyxx + xxyx + xyxy + xxxy + xyxy + xxyy + xyyy \\ &\quad + yxxx + yyxx + yxyx + yyxy + yxxy + yyxy + yxyy + yyyy \end{aligned}$$

Assim,  $(x + y)^n =$

$$(x + y)(x + y) \cdots (x + y) \quad (62)$$

com  $n$  ocorrências de  $(x + y)$ . Desenvolvendo o produto temos uma soma em que cada termo é da forma  $x^r y^{n-r}$ , para  $0 \leq r \leq n$ . Para cada  $r$  o coeficiente de  $x^r y^{n-r}$  é o número de maneiras de escolher o  $x$  de  $r$  fatores da equação (62) (para o  $y$ , dos  $n - r$  fatores restantes). O número de maneiras de escolher  $r$  fatores dentre  $n$  é  $\binom{n}{r}$ , portanto

$$(x + y)^n = \sum_{r=0}^n \binom{n}{r} x^r y^{n-r}. \quad (63)$$

## Coeficiente multinomial

De volta ao exemplo [mão de bridge](#), se dividimos a tarefa de distribuir as cartas em 4 etapas, cada etapa seleciona 13 cartas para um jogador, então pelo princípio multiplicativo o número de maneiras distintas de distribuir as cartas no jogo de bridge é

$$\binom{52}{13} \binom{52-13}{13} \binom{52-13-13}{13} \binom{52-13-13-13}{13} = \binom{52}{13, 13, 13, 13} \quad (64)$$

Com raciocínio análogo ao feito para o Teorema Binomial,

$$(x + y + z)^n = \sum_{r_1+r_2+r_3=n} \binom{n}{r_1, r_2, r_3} x^{r_1} y^{r_2} z^{r_3}. \quad (65)$$

e, de modo geral,

**Teorema 47** (Teorema Multinomial). *Para todo  $n > 0$ , vale*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{r_1+r_2+\cdots+r_k=n} \binom{n}{r_1, r_2, \dots, r_k} x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}.$$

de modo que  $\binom{n}{r_1, r_2, \dots, r_k}$  é conhecido como **coeficiente multinomial**.



## 10 Funções geradoras

*De quantas maneiras distintas podemos lançar uma dado quatro vezes de modo que os resultados somam 14?*

O resultado do primeiro lançamento é representado por um polinômio

$$x^1 + x^2 + x^3 + x^4 + x^5 + x^6 \quad (66)$$

O símbolo  $x$  aqui é chamado de *indeterminada*, o que significa que não é uma variável que assume valores, seu único papel é codificar uma enumeração, neste papel ele contém duas informações: (1) as potências de  $x$  representam as diferentes faces dos dados; (2) os coeficientes das potências de  $x$  mostram o número de ocorrências de cada face. Se o dado fosse defeituoso com faces 1,2,2,2,5,5 então o polinômio seria

$$x^1 + 3x^2 + 2x^5$$

Se o segundo lançamento é codificado pelo mesmo polinômio, então o produto

$$(x^1 + x^2 + x^3 + x^4 + x^5 + x^6)(x^1 + x^2 + x^3 + x^4 + x^5 + x^6) = \\ x^{12} + 2x^{11} + 3x^{10} + 4x^9 + 5x^8 + 6x^7 + 5x^6 + 4x^5 + 3x^4 + 2x^3 + x^2$$

e nesse polinômio  $ax^k$  significa que há  $a$  maneiras de obtermos a soma  $k$  (pela maneira que multiplicamos polinômio). Por exemplo, só há uma maneira de obtermos 12, é como  $6 + 6$ , há 0 modos de obtermos soma 0 ou soma maior que 12, há 3 maneiras de obter soma 4 (a saber  $1 + 3$ ,  $2 + 2$  e  $3 + 1$ ).

Para responder a pergunta inicial, precisamos conhecer o coeficiente de  $x^{14}$  em

$$(x^1 + x^2 + x^3 + x^4 + x^5 + x^6)^4$$

que expandido é o polinômio

$$x^{24} + 4x^{23} + 10x^{22} + 20x^{21} + 35x^{20} + 56x^{19} + 80x^{18} + 104x^{17} + 125x^{16} + 140x^{15} + 146x^{14} + \\ 140x^{13} + 125x^{12} + 104x^{11} + 80x^{10} + 56x^9 + 35x^8 + 20x^7 + 10x^6 + 4x^5 + x^4$$

portanto há 146 maneiras diferentes de obter a soma 14.

**Exercício 53.** *Um pai generoso deseja dividir R\$20,00 entre seus três filhos de modo que cada um receba pelo menos R\$5,00 e ninguém receba mais que R\$10,00 e a quantia do filho mais velho é par. Quantas maneiras existem de fazer isso?*

*Solução.* Procuramos pelo coeficiente de  $x^{20}$  no polinômio

$$(x^6 + x^8 + x^{10})(x^5 + x^6 + x^7 + x^8 + x^9 + x^{10})^2 = \\ x^{30} + 2x^{29} + 4x^{28} + 6x^{27} + 9x^{26} + 12x^{25} + 13x^{24} + 14x^{23} + 13x^{22} + 12x^{21} + \\ 9x^{20} + 6x^{19} + 4x^{18} + 2x^{17} + x^{16}$$

portanto são 9 maneiras.  $\square$

**Exercício 54.** Quantas soluções inteiras tem  $x_1 + x_2 + x_3 = 11$  com  $x_1 \in \{1, 2, 3\}$  e  $x_2, x_3 \in \{4, 5\}$ ?

*Solução.* O coeficiente de  $x^{11}$  em  $(x^1 + x^2 + x^3)(x^4 + x^5)(x^4 + x^5)$ .  $\square$

**Exercício 55.** Imagine um país no qual há apenas três moedas: uma moeda de 1 centavo, uma moeda de 2 centavos e uma moeda de 4 centavos. De quantas maneiras podemos “trocar” 100 centavos?

*Solução.* Precisamos resolver a equação  $a + 2b + 4c = 100$  para números inteiros não-negativos  $a, b, c$ . Fazemos isso encontrando o coeficiente de  $x^{100}$  no “polinômio”

$$P(x) = \underbrace{(1 + x + x^2 + \cdots)}_{\text{quantas moedas de 1}} \cdot \underbrace{(1 + x^2 + x^4 + \cdots)}_{\text{quantas moedas de 2}} \cdot \underbrace{(1 + x^4 + x^8 + \cdots)}_{\text{quantas moedas de 4}}$$

Podemos multiplicar os termos e com alguma perseverança eventualmente encontramos o coeficiente de  $x^{100}$ . Mas agora precisamos buscar um modo mais inteligente para isso.  $\square$

## Funções geradoras

**Definição 32.** Se  $a_0, a_1, a_2, \dots$  é uma sequência de números a *função geradora (ordinária)* dessa sequência é a *série de potências*

$$A(x) = \sum_{n \geq 0} a_n x^n \quad (67)$$

O coeficiente  $a_n$  é denotado por

$$[x^n]A(x)$$

Por exemplo,

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n \quad (68)$$

é função geradora da sequência  $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}, 0, 0, \dots$

$$\frac{1-x^{n+1}}{1-x} = 1+x+x^2+\cdots+x^n \quad (69)$$

é função geradora da sequência  $1, 1, \dots, 1, 0, 0, 0 \dots$  ( $n+1$  ocorrências de 1); se considerarmos  $|x| < 1$  e tomarmos o limite quando  $n \rightarrow \infty$  em (69) obtemos

$$\frac{1}{1-x} = 1+x+x^2+x^3+\cdots \quad (70)$$

é função geradora da sequência constante  $1, 1, 1, \dots$ . Também, sabemos que, por exemplo,

$$e^x = 1 + \frac{x}{1} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \quad (71)$$

é função geradora da sequência  $(1/n! : n \in \mathbb{N})$  e

$$\frac{1}{\sqrt{1-4x}} = \sum_{n \geq 0} \binom{2n}{n} x^n \quad (72)$$

é função geradora da sequência  $(\binom{2n}{n} : n \in \mathbb{N})$  e

$$\ln\left(\frac{1}{1-x}\right) = \sum_{n \geq 1} \frac{1}{n} x^n \quad (73)$$

é função geradora da sequência  $(\frac{1}{n} : n \in \mathbb{N}^*)$

$$\text{sen}(x) = \sum_{n \geq 0} (-1)^n \frac{1}{(2n+1)!} x^{2n+1} \quad (74)$$

é função geradora da sequência  $1, \frac{-1}{3!}, \frac{1}{5!}, \frac{-1}{7!}, \dots$ , e

$$\cos(x) = \sum_{n \geq 0} (-1)^n \frac{1}{(2n)!} x^{2n} \quad (75)$$

é função geradora da sequência  $1, \frac{-1}{2!}, \frac{1}{4!}, \frac{-1}{6!}, \dots$

Em nossas aplicações (contagem) os coeficientes da série (67) são inteiros, porém todas as propriedades discutidas são válidas para números complexos. Ademais,  $A(x)$  em (67) só é uma função para os valores de  $x$  em que a série converge.

## 10.1 Sobre convergência (opcional)

$A(x) = \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots$  é uma *série de potências formal*, isto é, é um elemento de uma estrutura algébrica chamada *anel das séries formais*, onde podemos somar e multiplicar séries formais. Ainda, foi dito que tal série *não* é uma função, como a notação  $A(x) = \dots$  pode sugerir. Também foi dito que as vezes tal série é uma função! Como é isso então?

Considere a seguinte soma de  $n$  termos (que é uma soma de P.G.)

$$\mathcal{S}_n = 1 + \frac{1}{2} + \frac{1}{4} + \dots + \frac{1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}}.$$

Recorde-se da definição de limite vista em Cálculo e

$$\lim_{n \rightarrow \infty} \mathcal{S}_n = 2.$$

Uma soma com infinitas parcelas, como em  $1 + \frac{1}{2} + \frac{1}{4} + \dots$  não faz sentido se levarmos em conta a definição usual de soma. Essa soma é chamada de *série* e é definida usando limite: Dada uma sequência  $(a_n)_{n \in \mathbb{N}}$  formamos a sequência  $(S_n)_{n \in \mathbb{N}}$

$$S_n = a_0 + a_1 + \dots + a_{n-1},$$

e dessa forma

$$\sum_{n \geq 0} a_n = \lim_{n \rightarrow \infty} S_n.$$

Quando o limite acima existe então dizemos que a série  $\sum_{n \geq 0} a_n$  é *convergente*, caso contrário, isto é, se o limite não existe, então a série é dita *divergente*. Por exemplo,

$$1 + \frac{1}{2} + \frac{1}{4} + \dots = \sum_{n \geq 0} \left(\frac{1}{2}\right)^n \text{ é convergente,}$$
$$1 + \frac{1}{2} + \frac{1}{3} + \dots = \sum_{n \geq 0} \frac{1}{n} \text{ é divergente.}$$

As séries de funções mais importantes são as do tipo

$$\sum_{n \geq 0} a_n (x - c)^n$$

chamadas *série de potências em torno do ponto  $c$* .

Fazendo a transformação de variáveis  $y = x - c$ , o caso geral das séries de potências se reduz ao estudo das séries para  $c = 0$ , ou seja em torno do 0,

$$\sum_{n \geq 0} a_n x^n.$$

Um dos principais resultados sobre convergência de séries de potências é o seguinte:

**Teorema 48.** *A série de potências  $\sum_{n \geq 0} a_n x^n$  ou converge apenas para  $x = 0$  ou existe um número real  $r > 0$  tal que  $\sum_{n \geq 0} a_n x^n$  converge absolutamente<sup>a</sup> no intervalo  $(-r, +r)$  da reta e diverge fora do intervalo  $[-r, +r]$ , e nos pontos  $+r$  e  $-r$  a série pode divergir ou convergir.*

A série de Taylor da função (analítica)  $f$  em torno de  $c \in I$  é a série de potências

$$\sum_{n \geq 0} \frac{f^{(n)}(c)}{n!} x^n,$$

e pode acontecer de: (1) a série divergir, ou (2) a série convergir para  $f(c + x)$ , ou (3) a série convergir para algum outro número.

Na maioria das funções que estudamos no curso de Cálculo acontece o segundo fato, felizmente. Aí temos, por exemplo, as seguintes séries de Taylor em torno do 0:

$$\begin{aligned} \frac{1}{1-x} &= \sum_{n \geq 0} x^n, \text{ se } |x| < 1 \\ \log \frac{1}{1-x} &= \sum_{n \geq 1} \frac{x^n}{n}, \text{ se } |x| < 1 \\ e^x &= \sum_{n \geq 0} \frac{x^n}{n!}, \text{ para todo } x \\ \text{sen}(x) &= \sum_{n \geq 0} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \text{ para todo } x \\ \text{cos}(x) &= \sum_{n \geq 0} (-1)^n \frac{x^{2n}}{(2n)!}, \text{ para todo } x \end{aligned}$$

e, agora, são *igualdades entre funções* e não definição de objetos formais. *Você sabe como a sua calculadora científica calcula o valor do seno de um número?*

---

<sup>a</sup>absolutamente significa que  $\sum_{n \geq 0} |a_n x^n|$  converge, o que implica que  $\sum_{n \geq 0} a_n x^n$  converge. A recíproca não é verdadeira.

Não nos preocuparemos com questões de convergência, embora seja relevante para aplicar ferramentas do cálculo, e podemos tratar a série *simbolicamente*, como uma

[série formal de potências](#), que nos permite ignorar problemas de convergência e manipular séries de potências formais do mesmo modo como fazemos com polinômios.

Notemos que se  $A(x)$  é função geradora de  $a_0, a_1, \dots$  então para qualquer número  $c$  a função  $A(cx)$  é função geradora de  $a_0, a_1c, a_2c^2, a_3c^3, \dots$ . Por exemplo

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \dots \quad (76)$$

é função geradora da sequência  $1, -1, 1, -1, 1, \dots$  pois de (70)

$$\frac{1}{1+x} = \frac{1}{1-(-x)} = 1 + (-x) + (-x)^2 + (-x)^3 + \dots = 1 - x + x^2 - x^3 + \dots$$

$\frac{1}{1-2x}$  é função geradora da sequência  $1, 2, 4, 8, 16, \dots$  pois de (70)

$$\frac{1}{1-(2x)} = 1 + (2x) + (2x)^2 + (2x)^3 + \dots$$

Sejam  $A(x) = \sum_{n \geq 0} a_n x^n$  e  $B(x) = \sum_{n \geq 0} b_n x^n$  funções geradoras, definimos:

deslocamento a direita	$xA(x) = \sum_{n \geq 1} a_{n-1} x^n$
deslocamento a esquerda	$\frac{A(x) - a_0}{x} = \sum_{n \geq 0} a_{n+1} x^n$
diferenciação	$A'(x) = \sum_{n \geq 0} (n+1) a_{n+1} x^n$
integração	$\int_0^x A(t) dt = \sum_{n \geq 1} \frac{a_{n-1}}{n} x^n$
adição	$A(x) + B(x) = \sum_{n \geq 0} (a_n + b_n) x^n$
convolução (produto)	$A(x)B(x) = \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) x^n$
somas parciais	$\frac{A(x)}{1-x} = \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} a_k \right) x^n$

Por exemplo, se  $a_0, a_1, \dots$  tem função geradora  $f(x)$  então  $x^k f(x)$  é função geradora de  $0, 0, \dots, 0, a_0, a_1, \dots$  com  $k$  ocorrências de 0 no início da sequência. Em particular,  $0, 0, 0, 1, 1, 1, \dots$  tem função geradora  $\frac{x^3}{1-x}$ .

Usando adição e os exemplos dados acima

$$\frac{1}{1-x} + \frac{1}{1+x} = \frac{2}{1-x^2} \quad (77)$$

é função geradora da sequência  $2, 0, 2, 0, 2, \dots$

**Fibonacci:** A sequência de Fibonacci  $F_0, F_1, F_2, \dots$  dada por  $F_0 = 0, F_1 = 1$  e  $F_n = F_{n-1} + F_{n-2}$  para todo  $n \geq 2$ , ou seja,

$$0, F_0 + 1, F_1 + F_0, F_2 + F_1, F_3 + F_2$$

é obtida da soma das três sequências

$$\begin{aligned} &0, 1, 0, 0, 0, 0, \dots \\ &0, F_0, F_1, F_2, F_3, \dots \\ &0, 0, F_0, F_1, F_2, F_3, \dots \end{aligned}$$

cuja função geradora são, respectivamente,  $x$ ,  $xF(x)$  e  $x^2F(x)$ , onde  $F(x)$  é a função geradora da sequência de Fibonacci. Logo

$$F(x) = \frac{x}{1 - x - x^2}$$

## Teorema binomial estendido

**Definição 33.** Vamos definir  $(x)_k$  para qualquer  $x \in \mathbb{R}$  por

$$(x)_k = x(x-1)(x-2) \cdots (x-k+1)$$

de modo que o *coeficiente binomial estendido* fica definido por

$$\binom{x}{k} = \begin{cases} \frac{(x)_k}{k!} & \text{se } k > 0 \\ 1 & \text{se } k = 0 \end{cases}.$$

Por exemplo,  $\binom{-2}{3} = -4$  e  $\binom{1/2}{3} = 1/16$  e para todo  $n \in \mathbb{N}$ ,  $\binom{n}{k} = 0$  se  $n < k$ .

Notemos que se  $x \in \mathbb{Z}^+$  então

$$\begin{aligned} \binom{-x}{k} &= \frac{-x(-x-1)(-x-2) \cdots (-x-k+1)}{k!} \\ &= \frac{(-1)^k x(x+1)(x+2) \cdots (x+k-1)}{k!} \\ &= \frac{(-1)^k (x+k-1)!}{(x-1)! k!} = (-1)^k \binom{n+k-1}{k} \end{aligned}$$

**Teorema 49** (Teorema binomial estendido). *Para todo  $x \in (-1, 1)$  e todo real  $u$*

$$(1+x)^u = \sum_{n \geq 0} \binom{u}{n} x^n.$$

*Demonstração.* Omitimos, decorre da série da Maclaurin para  $(1+x)^u$ . □

Com a definição e teorema acima temos para  $k \in \mathbb{N}$

$$(1+x)^{-k} = \sum_{n \geq 0} \binom{-k}{n} x^n = \sum_{n \geq 0} (-1)^n \binom{k+n-1}{k-1} x^n$$

e

$$(1-x)^{-k} = \sum_{n \geq 0} \binom{-k}{n} (-x)^n = \sum_{n \geq 0} \binom{k+n-1}{k-1} x^n$$

## 10.2 Expansão de funções de geradoras

Dada uma *forma funcional* para uma função geradora, gostaríamos de um mecanismo para encontrar a sequência associada. Esse processo é chamado de *expandir* a função geradora. Muitas funções são facilmente manipuladas a partir do teorema de Taylor

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \dots = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!}x^n$$

de modo que

$$[x^n]f(x) = \frac{1}{n!}f^{(n)}(0)$$

sempre que diferenciação for possível.

Também, obtemos coeficientes por manipulações algébricas envolvendo as identidades básicas que já são conhecidas e transformações dadas nas tabelas acima. Por exemplo

$$[x^n] \frac{c}{1-bx} = cb^n \tag{78}$$

para quaisquer constantes  $b$  e  $c$ , pois de (70) temos

$$\frac{c}{1-bx} = c \sum_{n \geq 0} (bx)^n.$$



**Exemplo:** Considere o problemas dos dados enunciado no início dessa seção: *De quantas maneiras distintas podemos lançar uma dado quatro vezes de modo que os resultados somam 14?* A função geradora é

$$\begin{aligned} D(x) &= (x + x^2 + x^3 + x^4 + x^5 + x^6)^4 \\ &= x^4(1 + x^2 + x^3 + x^4 + x^5)^4 \\ &= x^4 \left( \frac{1 - x^6}{1 - x} \right)^4 \\ &= x^4 (1 - x^6)^4 (1 - x)^{-4} \end{aligned}$$

de modo que  $[x^{14}]D(x) = [x^{10}](1 - x^6)^4(1 - x)^{-4}$ . Ainda,

$$(1 - x^6)^4 = \sum_{j \geq 0} \binom{4}{j} (-x^6)^j = 1 - 4x^6 + 6x^{12} - 4x^{18} + x^{24}$$

$$(1 - x)^{-4} = \sum_{j \geq 0} \binom{4 + j - 1}{j} x^j = \sum_{j \geq 0} \binom{3 + j}{j} x^j$$

Agora,  $[x^{10}](1 - x^6)^4(1 - x)^{-4}$  pode ser obtido de  $[x^0](1 - x^6)^4 = 1$  e  $[x^{10}](1 - x)^{-4} = \binom{13}{10} = 286$  e ser obtido de  $[x^6](1 - x^6)^4 = -4$  e  $[x^4](1 - x)^{-4} = \binom{7}{4} = 35$ , logo temos  $286 - 140 = 146$  modos distintos.

**Exemplo:** Determine o coeficiente de  $[x^{15}](x^2 + x^3 + x^4 + \dots)^4$ .

Notemos que

$$\begin{aligned} [x^{15}](x^2 + x^3 + x^4 + \dots)^4 &= [x^{15}](x^2(1 + x + x^3 + \dots))^4 \\ &= [x^{15}] \left( \frac{x^2}{1 - x} \right)^4 = [x^{15}] \left( \frac{x^8}{(1 - x)^4} \right) = [x^7] \left( \frac{1}{(1 - x)^4} \right) \end{aligned}$$

e

$$\frac{1}{(1 - x)^4} = \sum_{r \geq 0} \binom{-4}{r} (-x)^r = \sum_{r \geq 0} \binom{4 + r - 1}{r} x^r$$

portanto  $[x^{15}](x^2 + x^3 + x^4 + \dots)^4 = \binom{4+7-1}{7}$ .

**Exemplo:** Quantos subconjuntos de  $\{1, 2, \dots, 15\}$  formado de 4 elementos não consecutivos existem? Se  $\{a, b, c, d\}$  é um tal subconjunto de modo que

$$1 \leq a < b < c < d \leq 15$$

então

$$\underbrace{(15 - d)}_{x_1} + \underbrace{(d - c)}_{x_2} + \underbrace{(c - b)}_{x_3} + \underbrace{(b - a)}_{x_4} + \underbrace{(a - 1)}_{x_5} = 14$$

portanto, queremos o número de soluções inteiras de

$$x_1 + x_2 + x_3 + x_4 + x_5 = 15$$

com  $x_1, x_5 \geq 0$  e  $x_2, x_3, x_4 \geq 2$ , o qual é o coeficiente

$$[x^{14}](1+x+x^2+\dots)^2(x^2+x^3+x^4+\dots)^3 = [x^{14}]x^6(1-x)^{-5} = [x^8](1-x)^{-5} = \binom{5+8-1}{8} = 495.$$

**Exercício 56.** De quantos modos podemos comprar  $n$  frutas de modo que (1) o número de maçãs é par, (2) o número de bananas é múltiplo de 5, (3) no máximo 4 laranjas, e (4) no máximo uma pêra.

*Solução.*

$$f(x) = \frac{1}{1-x^2} \cdot \frac{1}{1-x^5} \cdot \frac{1-x^5}{1-x} \cdot (1+x)$$

$$[x^n]f(x) = n+1. \quad \square$$

No caso de funções racionais podemos usar a [técnica da frações parciais](#), por exemplo

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\varphi x)(1-\bar{\varphi} x)}$$

onde  $\varphi = (1+\sqrt{5})/2$  e onde  $\bar{\varphi} = (1-\sqrt{5})/2$  são as raízes de  $1-x-x^2$ . Fazendo

$$\frac{x}{(1-\varphi x)(1-\bar{\varphi} x)} = \frac{A}{1-\varphi x} + \frac{B}{1-\bar{\varphi} x}$$

temos  $A = 1/\sqrt{5}$  e  $B = 11/\sqrt{5}$  de modo que

$$\frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}} \frac{1}{1-\varphi x} - \frac{1}{\sqrt{5}} \frac{1}{1-\bar{\varphi} x}$$

Agora

$$\frac{1}{\sqrt{5}} \frac{1}{1-\varphi x} = \frac{1}{\sqrt{5}} \sum_{n \geq 0} (\varphi x)^n$$

e

$$\frac{1}{\sqrt{5}} \frac{1}{1-\bar{\varphi} x} = \frac{1}{\sqrt{5}} \sum_{n \geq 0} (\bar{\varphi} x)^n$$

portanto  $\frac{x}{1-x-x^2} = \sum_{n \geq 0} \frac{1}{\sqrt{5}} (\varphi^n - \bar{\varphi}^n) x^n$  de modo que

$$[x^n] \frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}} (\varphi^n - \bar{\varphi}^n) \quad (79)$$

**Exemplo:** Determina o coeficiente de  $x^n$  na série de potências de

$$\frac{1}{x^3 - 7x^2 + 16x - 12}$$

Primeiro, temos que

$$x^3 - 7x^2 + 16x - 12 = (x - 3)(x - 2)^2$$

portanto devemos determinar constantes  $A, B, C$  tais que

$$\frac{1}{x^3 - 7x^2 + 16x - 12} = \frac{A}{x - 3} + \frac{B}{x - 2} + \frac{C}{(x - 2)^2}$$

e temos que  $A = 1$  e  $B = C = -1$ , logo

$$\frac{1}{x^3 - 7x^2 + 16x - 12} = \frac{1}{x - 3} - \frac{1}{x - 2} - \frac{1}{(x - 2)^2}$$

Agora, reescrevemos cada fração para cairmos no caso  $\frac{1}{1-ax}$

$$\begin{aligned}\frac{1}{x - 3} &= \frac{1}{-3(1 - x/3)} = -\frac{1}{3} \frac{1}{1 - x/3} \\ \frac{1}{x - 2} &= \frac{1}{-2(1 - x/2)} = -\frac{1}{2} \frac{1}{1 - x/2}\end{aligned}$$

e no caso  $\frac{1}{(1-ax)^2}$

$$\frac{1}{(x - 2)^2} = \frac{-1}{4} \frac{1}{(1 - x/2)^2}$$

logo

$$\begin{aligned}\frac{1}{x^3 - 7x^2 + 16x - 12} &= -\frac{1}{3} \frac{1}{(1 - \frac{x}{3})} + \frac{1}{2} \frac{1}{(1 - \frac{x}{2})} + \frac{1}{4} \frac{1}{(1 - x/2)^2} \\ &= -\frac{1}{3} \sum_{n \geq 0} \left(\frac{x}{3}\right)^n + \frac{1}{2} \sum_{n \geq 0} \left(\frac{x}{2}\right)^n + \frac{1}{4} \sum_{n \geq 0} \binom{-2}{n} \left(\frac{-x}{2}\right)^n \\ &= \sum_{n \geq 0} \left( \left(\frac{1}{2}\right)^{n+1} - \left(\frac{1}{3}\right)^{n+1} + \frac{1}{4}(-1)^n \binom{-2}{n} \right) x^n \\ &= \sum_{n \geq 0} \left( \left(\frac{1}{2}\right)^{n+1} - \left(\frac{1}{3}\right)^{n+1} + \frac{1}{4}(-1)^n \binom{n+3}{n} \right) x^n\end{aligned}$$

portanto

$$[x^n] \frac{1}{x^3 - 7x^2 + 16x - 12} = \frac{1}{2^{n+1}} - \frac{1}{3^{n+1}} + \frac{(n+3)(n+2)(n+1)}{24}.$$