

# demonstrações erradas de teoremas falsos

Alexander Kahleul

8 de fevereiro de 2026

# Sumário

|          |   |           |
|----------|---|-----------|
| <b>I</b> | <b>Fundamentos</b>                          | <b>7</b>  |
| <b>1</b> | <b>Lógica Proposicional</b>                 | <b>8</b>  |
| <b>2</b> | <b>Teorias de Primeira Ordem</b>            | <b>13</b> |
| 2.1      | Linguagens de Primeira Ordem . . . . .      | 13        |
| 2.2      | Estruturas . . . . .                        | 16        |
| <b>3</b> | <b>O sistema ZFC</b>                        | <b>18</b> |
| 3.1      | Primeiros Axiomas . . . . .                 | 18        |
| 3.1.1    | O Axioma da Extensão . . . . .              | 18        |
| 3.1.2    | O Axioma do Vazio . . . . .                 | 19        |
| 3.1.3    | O Axioma do Par . . . . .                   | 20        |
| 3.1.4    | O Axioma da União . . . . .                 | 20        |
| 3.1.5    | O Axioma das Partes . . . . .               | 21        |
| 3.1.6    | O Esquema de Axiomas da Separação . . . . . | 22        |
| 3.1.7    | Propriedades Algébricas . . . . .           | 23        |
| 3.1.8    | O Axioma da Regularidade . . . . .          | 25        |
| 3.2      | Relações e Funções . . . . .                | 26        |
| 3.2.1    | Produto Cartesiano . . . . .                | 26        |
| 3.2.2    | Relações . . . . .                          | 27        |

|  |           |
|--|-----------|
| <i>SUMÁRIO</i>   | 3         |
| 3.2.3 Relações de Ordem . . . . .                        | 30        |
| 3.2.4 Relações de Equivalência . . . . .                 | 33        |
| 3.2.5 Funções . . . . .                                  | 35        |
| 3.2.6 Bijeções e Funções Inversas . . . . .              | 36        |
| 3.3 O Axioma do Infinito e os Números Naturais . . . . . | 41        |
| 3.3.1 O Teorema da Recursão . . . . .                    | 46        |
| 3.3.2 Aritmética dos Números Naturais . . . . .          | 49        |
| 3.4 O Axioma da Escolha . . . . .                        | 49        |
| <b>II Números Reais</b>                                  | <b>51</b> |
| <b>4 Números Reais como na Análise</b>                   | <b>52</b> |
| 4.1 Corpos . . . . .                                     | 52        |
| 4.2 Números Naturais . . . . .                           | 54        |
| 4.2.1 A Unicidade dos Números Naturais . . . . .         | 58        |
| 4.2.2 Definições recursivas . . . . .                    | 60        |
| 4.3 Conjuntos Finitos . . . . .                          | 61        |
| 4.3.1 Resultadinhos . . . . .                            | 62        |
| 4.4 Conjuntos Infinitos . . . . .                        | 63        |
| 4.5 Conjuntos Enumeráveis e Não-Enumeráveis . . . . .    | 64        |
| 4.6 Números Inteiros . . . . .                           | 65        |
| 4.6.1 Teoria Elementar dos Números . . . . .             | 65        |
| 4.7 Números Racionais . . . . .                          | 65        |
| 4.8 Números Reais . . . . .                              | 66        |
| <b>5 Números Reais como na Álgebra</b>                   | <b>69</b> |
| 5.1 Homomorfismos . . . . .                              | 73        |

|  |            |
|--|------------|
| <i>SUMÁRIO</i>   | 4          |
| <b>III Análise Real I</b>                                      | <b>74</b>  |
| <b>6 Sequências</b>  | <b>75</b>  |
| <b>7 Limites e Continuidade</b>                                | <b>78</b>  |
| 7.1 Topologia da Reta . . . . .                                | 78         |
| 7.2 Limites . . . . .  | 79         |
| 7.3 Continuidade . . . . .                                     | 83         |
| 7.4 Limites Infinitos . . . . .                                | 86         |
| 7.5 Limites e Sequências . . . . .                             | 88         |
| 7.6 Teoremas do Valor Intermediário e de Weierstrass . . . . . | 91         |
| 7.7 Algumas Funções Transcendentais . . . . .                  | 93         |
| 7.7.1 Trigonometria, parte I . . . . .                         | 93         |
| 7.7.2 Exponencial e Logaritmo . . . . .                        | 95         |
| <b>8 Derivadas</b>   | <b>101</b> |
| 8.1 Definições e Resultados Iniciais . . . . .                 | 101        |
| 8.2 Teoremas de Rolle, do Valor Médio e de Cauchy . . . . .    | 104        |
| 8.3 Gráficos de Funções . . . . .                              | 106        |
| 8.4 Regras de L'Hospital . . . . .                             | 108        |
| 8.5 Trigonometria, parte II . . . . .                          | 110        |
| 8.6 Polinômio de Taylor . . . . .                              | 111        |
| <b>9 Integrais</b>   | <b>112</b> |
| 9.1 A integral de Darboux . . . . .                            | 112        |
| 9.1.1 Estendendo a definição . . . . .                         | 116        |
| 9.2 Resultados . . . . .                                       | 117        |
| 9.3 O Teorema Fundamental do Cálculo . . . . .                 | 119        |

|   |            |
|---|------------|
| <i>SUMÁRIO</i>  | 5          |
| 9.4 A Integral de Riemann . . . . .                       | 122        |
| 9.5 Integrais Impróprias . . . . .                        | 123        |
| <b>10 Demonstrações</b>                                   | <b>124</b> |
| <b>IV Álgebra Linear</b>                                  | <b>130</b> |
| <b>11 Matrizes e Sistemas Lineares</b>                    | <b>131</b> |
| 11.1 Definições Iniciais e Operações Matriciais . . . . . | 131        |
| 11.2 Operações e Matrizes Elementares . . . . .           | 134        |
| 11.3 Eliminação Gaussiana e Decomposição LU . . . . .     | 136        |
| 11.4 Sistemas Lineares . . . . .                          | 136        |
| <b>12 Espaços Vetoriais</b>                               | <b>140</b> |
| 12.1 Espaços e Subespaços Vetoriais . . . . .             | 140        |
| 12.2 Combinações Lineares e Geradores . . . . .           | 144        |
| 12.3 Dependência e Independência Linear . . . . .         | 146        |
| 12.4 Base e Dimensão . . . . .                            | 148        |
| <b>13 Transformações Lineares</b>                         | <b>152</b> |
| 13.1 Matrizes . . . . .                                   | 153        |
| <b>14 Geometria Analítica</b>                             | <b>155</b> |
| <b>V Cálculo II</b>                                       | <b>159</b> |
| <b>15 Topologia do Espaço Euclidiano</b>                  | <b>160</b> |
| <b>16 Caminhos</b>  | <b>162</b> |

|  |            |
|--|------------|
| <i>SUMÁRIO</i>   | 6          |
| 16.1 Curvas . . . . .                                  | 166        |
| <b>17 Campos Escalares e Vetoriais</b>                 | <b>169</b> |
| <b>18 Integrais de Linha</b>                           | <b>172</b> |
| <b>VI Probabilidade</b>                                | <b>174</b> |
| <b>19 Combinatória Finita</b>                          | <b>175</b> |
| <b>20 Espaços de Probabilidade</b>                     | <b>177</b> |
| 20.1 Variáveis Aleatórias . . . . .                    | 181        |
| 20.1.1 Distribuições Discretas . . . . .               | 182        |
| 20.1.2 Distribuições Absolutamente Contínuas . . . . . | 183        |
| <b>VII Outros</b>                                      | <b>184</b> |
| <b>21 Shoenfield</b>                                   | <b>185</b> |
| <b>Bibliografia</b>                                    | <b>187</b> |

# **Parte I**

## **Fundamentos**

# Capítulo 1

## Lógica Proposicional

Seguimos [8].

### Definição 1.1.

- (a) O *alfabeto proposicional*  $\text{Alf}$  é uma coleção infinita de símbolos distintos, nenhum deles propriamente contido em outro, separados nas seguintes categorias:
  - i. Conectivos:  $\neg, \rightarrow$ .
  - ii. Parênteses:  $(, )$ .
  - iii. Variáveis proposicionais:  $p_1, p_2, p_3 \dots, p_i, \dots$
- (b) As *fórmulas* sobre  $\text{Alf}$  são definidas indutivamente pelas seguintes regras:
  - i. se  $\mathbf{p}$  é uma variável proposicional, então  $\mathbf{p}$  é uma fórmula.
  - ii. se  $\mathbf{A}$  e  $\mathbf{B}$  são fórmulas, então  $(\neg \mathbf{A})$  e  $(\mathbf{A} \rightarrow \mathbf{B})$  são fórmulas;
  - iii. todas as fórmulas são obtidas por um número finito de aplicações das regras acima.

O conjunto de todas as fórmulas é denotado por  $\text{Form}$ , enquanto o conjunto de todas as fórmulas atômicas é denotado por  $\text{Form}_{\text{At}}$

- (c) A *linguagem proposicional* é o par  $\mathcal{L} := (\text{Alf}, \text{Form})$

### Definição 1.2.

- (a) Um *sistema de dedução proposicional* é uma tripla  $(\mathcal{L}, \text{Ax}, \text{R})$ , onde  $\mathcal{L}$  é a linguagem proposicional,  $\text{Ax}$  é um conjunto de esquemas de axiomas e  $\text{R}$  é um conjunto de regras de inferência.
- (b) A Lógica Proposicional é o sistema  $\mathcal{L}_P := (\mathcal{L}, \Lambda, \text{MP})$ , onde  $\Lambda$  é um conjunto formado pelos esquemas de axiomas

$AX_1. (A \rightarrow (B \rightarrow A))$   
 $AX_2. ((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$   
 $AX_3. (((\neg B) \rightarrow (\neg A)) \rightarrow (((\neg B) \rightarrow A) \rightarrow B))$   
 e MP é a regra de inferência *Modus Ponens*, a saber,

$$MP := \{(\{A, (A \rightarrow B)\}, B) : A, B \in \text{Form}\}.$$

**Definição 1.3.** Sejam  $\Delta \subseteq \text{Form}$  e  $A \in \text{Form}$ .

(a) Uma *dedução* de  $A$  a partir de  $\Delta$  é uma sequência  $(A_1, \dots, A_n)$  tal que  $A_n \equiv A$  e, para cada  $k \in [n]$ , vale pelo menos uma das seguintes afirmações.

- (a)  $A_k \in \Lambda$ .
- (b)  $A_k \in \Delta$ .
- (c) Existem índices  $i, j < k$  tais que  $A_k$  é obtida de  $A_i$  e  $A_j$  via MP.

Isso é denotado por  $\Delta \vdash A$ .

(b) Dizemos que  $A$  é uma *consequência sintática* de  $\Delta$  se  $\Delta \vdash A$ .

(c) Dizemos que  $A$  é um *teorema* se  $\emptyset \vdash A$ . Isso é denotado por  $\vdash A$ .

**Proposição 1.4.**  $\vdash (A \rightarrow A)$ .

**Prova.** Pois tome:

- |  |            |
|--|------------|
| 1. $((A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)))$ | $AX_2$     |
| 2. $(A \rightarrow ((A \rightarrow A) \rightarrow A))$   | $AX_1$     |
| 3. $((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$   | $MP(1, 2)$ |
| 4. $(A \rightarrow (A \rightarrow A))$   | $AX_1$     |
| 5. $(A \rightarrow A)$   | $MP(4, 5)$ |

**Teorema 1.5** (da Dedução). Sejam  $\Delta \subseteq \text{Form}$  e  $A, B \in \text{Form}$ .

(a) Se  $\Delta \cup \{A\} \vdash B$ , então  $\Delta \vdash (A \rightarrow B)$ .

(b) Se  $\Delta \vdash (A \rightarrow B)$ , então  $\Delta \cup \{A\} \vdash B$ .

**Prova.**

(a) Façamos indução no número de fórmulas que ocorrem na dedução de  $B$  a partir de  $\Delta \cup \{A\}$ . Se  $(A_1)$  é uma dedução de  $B$ , então  $A_1 \equiv B$ .

- i. Se  $B \in \Lambda$ , então  $\Delta \vdash B$ , e como  $\Delta \vdash (B \rightarrow (A \rightarrow B))$ , temos, via MP, que  $\Delta \vdash (A \rightarrow B)$ .
- ii. Se  $B \in \Delta$ , então  $\Delta \vdash B$ , e como  $\Delta \vdash (B \rightarrow (A \rightarrow B))$ , temos, via MP, que  $\Delta \vdash (A \rightarrow B)$ .
- iii. Se  $B \equiv A$ , então de  $\Delta \vdash (A \rightarrow A)$  vem  $\Delta \vdash (A \rightarrow B)$ .

Agora, seja  $(A_1, \dots, A_n)$  uma dedução de  $B$  a partir de  $\Delta \cup \{A\}$  e suponha, por hipótese de indução, que o resultado vale para toda fórmula que pode ser deduzida a partir de  $\Delta \cup \{A\}$  por uma dedução com menos de  $n$  fórmulas. Se  $B \in \Lambda$ ,  $B \in \Delta$  ou  $B \equiv A$ , então podemos deduzir  $(A \rightarrow B)$  a partir de  $\Delta$  exatamente do mesmo modo que fizemos na base da indução. Suponha, então, que  $B$  é obtida de duas fórmulas de índices  $< n$  via MP. Essas duas fórmulas têm as formas  $C$  e  $(C \rightarrow B)$ , e como elas foram deduzidas de  $\Delta \cup \{A\}$  por menos de  $n$  fórmulas, temos que  $\Delta \vdash (A \rightarrow C)$  e  $\Delta \vdash (A \rightarrow (C \rightarrow B))$ . Com isso, podemos deduzir  $(A \rightarrow B)$  a partir de  $\Delta$  do seguinte modo.

$$\begin{array}{ll}
 \vdots & \vdots \\
 i. \quad \Delta \vdash (A \rightarrow C) & \\
 \vdots & \vdots \\
 j. \quad \Delta \vdash (A \rightarrow (C \rightarrow B)) & \\
 k. \quad \Delta \vdash ((A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))) & \text{Ax}_2 \\
 l. \quad \Delta \vdash ((A \rightarrow C) \rightarrow (A \rightarrow B)) & \text{MP}(j, k) \\
 m. \quad \Delta \vdash (A \rightarrow B) & \text{MP}(i, l)
 \end{array}$$

Assim, se  $\Delta \cup \{A\} \vdash B$ , então  $\Delta \vdash (A \rightarrow B)$ . ■

- (b) Como  $\Delta \vdash (A \rightarrow B)$  e  $\Delta \subseteq \Delta \cup \{A\}$ , temos  $\Delta \cup \{A\} \vdash (A \rightarrow B)$ . Daí, como  $\Delta \cup \{A\} \vdash A$ , temos que  $\Delta \cup \{A\} \vdash B$ . ■

### Proposição 1.6.

- (a)  $\{A \rightarrow B, B \rightarrow C\} \vdash A \rightarrow C$ .  
(b)  $\vdash A \leftrightarrow \neg\neg A$ .

### Definição 1.7.

- (a) Uma *valoração proposicional* é uma função  $\bar{v} : \text{Form}_{\text{At}} \rightarrow \{t, f\}$ .  
(b) Uma *valoração* é uma função  $v : \text{Form} \rightarrow \{t, f\}$  tal que
- i.  $v|_{\text{Form}_{\text{At}}} = \bar{v}$ ;
  - ii.  $v[(\neg A)] = f$  se, e somente se,  $v(A) = t$ ;
  - iii.  $v[(A \rightarrow B)] = f$  se, e somente se,  $v(A) = t$  e  $v(B) = f$ .

**Definição 1.8.** Uma fórmula  $A$  é *válida*, ou *tautológica*, se  $v(A) = t$  para toda valoração  $v$ . Isso é denotado por  $\models A$ .

### Lema 1.9.

- (a) Os axiomas de  $\mathcal{L}_P$  são válidos.

(b) Se  $\models A$  e  $\models (A \rightarrow B)$ , então  $\models B$ .

**Prova.**

(a) Suponha, por absurdo, que  $\not\models A \rightarrow (B \rightarrow A)$ . Isso só é possível se  $v[(B \rightarrow A)] = \text{f}$ , o que, por sua vez, só é possível se  $v(A) = \text{f}$ , o que contraria a hipótese. Logo,  $\models A \rightarrow (B \rightarrow A)$ . A prova de que os outros (esquemas de) axiomas são válidos segue analogamente. ■

(b) Suponha, por absurdo, que  $\not\models B$ . Logo, existe uma valoração  $v$  tal que  $v(B) = \text{f}$ . Para essa valoração, como  $\models A$ , temos  $v(A) = \text{t}$ , de modo que  $v[(A \rightarrow B)] = \text{f}$ , o que contraria a hipótese. Com isso,  $\models B$ . ■

**Teorema 1.10** (da Correção). Se  $\vdash A$ , então  $\models A$ .

**Prova.** Fazemos indução no número de fórmulas que ocorrem na dedução de  $A$ . Se  $(A_1)$  é a dedução de  $A$ , então  $A_1 \equiv A$  e  $A$  é um axioma, e como todos os axiomas são válidos (lema (1.9)), temos  $\models A$ . Agora, seja  $(A_1, \dots, A_n)$  a dedução de  $A$  e suponha, por hipótese de indução, que o resultado vale para toda fórmula que pode ser deduzida por uma dedução com menos de  $n$  fórmulas. Se  $A$  é um axioma, então  $\models A$ . Suponha, então, que  $A$  é obtida de duas fórmulas de índices  $< n$  via MP. Essas duas fórmulas têm as formas  $B$  e  $(B \rightarrow A)$ , e como elas foram deduzidas por menos de  $n$  fórmulas, temos que  $\models B$  e  $\models (B \rightarrow A)$ . Daí, como a regra MP conserva validade (lema (1.9)), temos que  $\models A$ . ■

**Lema 1.11** (Kalmár). Sejam  $A(p_1, \dots, p_n) \in \text{Form}$  e  $v : \text{Form} \rightarrow \{\text{t}, \text{f}\}$ . Se

$$p'_i := \begin{cases} p_i, & \text{se } v(p_i) = \text{t} \\ (\neg p_i), & \text{se } v(p_i) = \text{f} \end{cases} \quad \text{e} \quad A' := \begin{cases} A, & \text{se } v(A) = \text{t} \\ (\neg A), & \text{se } v(A) = \text{f} \end{cases},$$

então  $\{p'_1, \dots, p'_n\} \vdash A'$ .

**Prova.** Fazemos indução no número de conectivos que ocorrem em  $A$ .

**Teorema 1.12** (da Completude). Se  $\models A$ , então  $\vdash A$ .

**Prova.** Sejam  $p_1, \dots, p_n$  as variáveis proposicionais que ocorrem em  $A$ . Pelo lema (1.11), temos  $\{p'_1, \dots, p'_n\} \vdash A'$  para toda valoração  $v$ , e como  $\models A$ , temos  $A' \equiv A$ , de modo que  $\{p'_1, \dots, p'_n\} \vdash A$ . Agora, definindo

$$v_1(p_i) := \begin{cases} v(p_i), & \text{se } i < n \\ \text{t}, & \text{se } i = n \end{cases} \quad \text{e} \quad v_2(p_i) := \begin{cases} v(p_i), & \text{se } i < n \\ \text{f}, & \text{se } i = n \end{cases},$$

cada  $p'_i$ , para  $i < n$ , fica bem definido. Como  $v_2(p_n) = \text{f}$ , vem  $\{p'_1, \dots, p'_{n-1}, (\neg p_n)\} \vdash A$ , de modo que, pelo teorema da dedução (1.5), temos  $\{p'_1, \dots, p'_{n-1}\} \vdash ((\neg p_n) \rightarrow$

A). Analogamente, como  $v_1(p_n) = \mathbf{t}$ , então  $\{p'_1, \dots, p'_{n-1}\} \vdash (p_n \rightarrow \mathbf{A})$ . Assim:

1.  $\{p'_1, \dots, p'_{n-1}\} \vdash ((\neg p_n) \rightarrow \mathbf{A})$   $p.$
2.  $\{p'_1, \dots, p'_{n-1}\} \vdash (p_n \rightarrow \mathbf{A})$   $p.$
3.  $\{p'_1, \dots, p'_{n-1}\} \vdash (p_n \rightarrow \mathbf{A}) \rightarrow (((\neg p_n) \rightarrow \mathbf{A}) \rightarrow \mathbf{A})$  (1.6)
4.  $\{p'_1, \dots, p'_{n-1}\} \vdash (((\neg p_n) \rightarrow \mathbf{A}) \rightarrow \mathbf{A})$  MP(2, 3)
5.  $\{p'_1, \dots, p'_{n-1}\} \vdash \mathbf{A}$  MP(1, 4)

Com isso, eliminamos  $p_n$ . Repetindo esse processo (um número finito de vezes), eliminamos  $p_{n-1}, \dots, p_1$ , obtendo por fim  $\vdash \mathbf{A}$ . ■

**Corolário 1.13** (Adequação).  $\models \mathbf{A}$  se, e somente se,  $\vdash \mathbf{A}$ .

**Prova.** Segue dos teoremas da correção (1.10) e da completude (1.12). ■

coisas

**Definição 1.14.** Sejam  $\mathbf{A} \in \text{Form}$  e  $\Gamma \subseteq \text{Form}$ .

- (a) Um *modelo* de  $\mathbf{A}$  é uma valoração  $v$  tal que  $v(\mathbf{A}) = \mathbf{t}$ . Dizemos que  $v$  *satisfaz*  $\mathbf{A}$ . Isso é denotado por  $v \models \mathbf{A}$ .
- (b) Um *modelo* de  $\Gamma$  é uma valoração  $v$  tal que  $v \models \mathbf{B}$  para todo  $\mathbf{B} \in \Gamma$ .

**Definição 1.15.** Sejam  $\mathbf{A}, \mathbf{B} \in \text{Form}$  e  $\Gamma \subseteq \text{Form}$ .

- (a) Dizemos que  $\mathbf{B}$  é uma *consequência semântica* de  $\mathbf{A}$  se todo modelo de  $\mathbf{A}$  é também um modelo de  $\mathbf{B}$ . Isso é denotado por  $\{\mathbf{A}\} \models \mathbf{B}$ .
- (b) Dizemos que  $\mathbf{B}$  é uma *consequência semântica* de  $\Gamma$  se todo modelo de  $\Gamma$  é também um modelo de  $\mathbf{B}$ . Isso é denotado por  $\Gamma \models \mathbf{B}$ .

**Teorema 1.16.** Se  $\Gamma \vdash \mathbf{A}$ , então  $\Gamma \models \mathbf{A}$ .

**Prova.** O caso  $\Gamma = \emptyset$  é simplesmente o teorema da correção (1.10). Suponha, então, que  $\Gamma \neq \emptyset$ . Se  $\mathbf{C}_1, \dots, \mathbf{C}_n$  são as fórmulas de  $\Gamma$  que aparecem na dedução de  $\mathbf{A}$ , então  $\{\mathbf{C}_1, \dots, \mathbf{C}_n\} \vdash \mathbf{A}$ , de modo que, por sucessivas aplicações do teorema da dedução (1.5), temos  $\vdash \mathbf{C}_1 \rightarrow \dots \rightarrow \mathbf{C}_n \rightarrow \mathbf{A}$ . Com isso, para toda valoração  $v$  tal que  $v(\mathbf{C}_i) = \mathbf{t}$  para todo  $i \in [n]$ , temos  $v(\mathbf{A}) = \mathbf{t}$ . Como  $\{\mathbf{C}_1, \dots, \mathbf{C}_n\} \subseteq \Gamma$ , temos  $v \models \mathbf{A}$  para toda valoração  $v$  tal que  $v \models \Gamma$ , isto é,  $\Gamma \models \mathbf{A}$ . ■

# Capítulo 2

## Teorias de Primeira Ordem

### 2.1 Linguagens de Primeira Ordem

**Definição 2.1** (Linguagens de Primeira Ordem).

- (a) Um *alfabeto* é uma coleção infinita de símbolos distintos, nenhum deles propriamente contido em outro, separados nas seguintes categorias:
- i. Conectivos:  $\vee, \neg$ .
  - ii. Quantificador universal:  $\forall$ .
  - iii. Parênteses:  $(, )$ .
  - iv. Variáveis, uma para cada inteiro positivo  $n$ :  $v_1, v_2, \dots, v_n, \dots$ .
  - v. Símbolos de função: para cada inteiro positivo  $n$ , uma coleção de símbolos de função  $n$ -ários.
  - vi. Símbolos de predicado: para cada inteiro positivo  $n$ , uma coleção de símbolos de predicado  $n$ -ários.
  - vii. Símbolo predicado binário de igualdade:  $=$ .
  - viii. Símbolos de constantes: uma coleção de símbolos.
- (b) Os *termos* correspondentes a um alfabeto são definidos do seguinte modo:
- i. as variáveis são termos;
  - ii. as constantes são termos;
  - iii. se  $t_1, t_2, \dots, t_n$  são termos e  $f$  é um símbolo de função  $n$ -ário, então  $f(t_1, t_2, \dots, t_n)$  é um termo;
  - iv. todos os termos têm uma das formas acima.
- (c) As *fórmulas* correspondentes a um alfabeto são definidas do seguinte modo:

- i. se  $t_1$  e  $t_2$  são termos, então  $(t_1, t_2)$  é uma fórmula;
- ii. se  $t_1, t_2, \dots, t_n$  são termos e  $R$  é um símbolo de predicado  $n$ -ário, então  $R(t_1, t_2, \dots, t_n)$  é uma fórmula;
- iii. se  $\alpha$  e  $\beta$  são fórmulas, então  $(\neg\alpha)$  e  $(\alpha \vee \beta)$  são fórmulas;
- iv. se  $x$  é uma variável e  $\alpha$  é uma fórmula, então  $(\forall x)(\alpha)$  é uma fórmula;
- v. todas as fórmulas têm uma das formas acima.

As fórmulas como definidas nos itens i. e ii. são ditas *atômicas*. A fórmula  $\alpha$  que aparece no item iv. é chamada de *escopo* do quantificador  $\forall$ .

- (d) Uma *linguagem de primeira ordem*  $\mathcal{L}$  consiste num alfabeto como descrito no item (a) e termos ( $\mathcal{L}$ -termos) e fórmulas ( $\mathcal{L}$ -fórmulas) como descritos nos itens (b) e (c).
- (e) Para especificar uma linguagem de primeira ordem  $\mathcal{L}$ , basta especificar quais são suas constantes, seus símbolos de função e seus símbolos de predicado:

$$\mathcal{L} \text{ é } \{c_1, c_2, \dots, f_1^{a(f_1)}, f_2^{a(f_2)}, \dots, R_1^{a(R_1)}, R_2^{a(R_2)}, \dots\},$$

onde cada  $c_i$  é um símbolo de constante, cada  $f_i^{a(f_i)}$  é um símbolo de função de aridade  $a(f_i)$  e cada  $R_i^{a(R_i)}$  é um símbolo de predicado de aridade  $a(R_i)$ .

**Teorema 2.2** (Legibilidade única). Seja  $\mathcal{L}$  uma linguagem de primeira ordem.

- (a) Todo termo tem uma, e exatamente uma, das formas i.-iii. da definição de termo.
- (b) Toda fórmula tem uma, e exatamente uma, das formas i.-iv. da definição de fórmula.

**Prova.** Ver [21], página 16, ou ainda, [16], página 18.

**Definição 2.3** (Subtermos e subfórmulas). Sejam  $t$  um  $\mathcal{L}$ -termo e  $\varphi$  uma  $\mathcal{L}$ -fórmula.

- (a) Um *subtermo* de  $t$  é um  $\mathcal{L}$ -termo definido recursivamente do seguinte modo:
  - i. se  $t$  é uma variável ou uma constante, então  $t$  é o único subtermo de si mesmo;
  - ii. se  $t$  é da forma  $ft_1t_2 \dots t_n$ , onde  $f$  é um símbolo funcional  $n$ -ário e  $t_1, t_2, \dots, t_n$  são  $\mathcal{L}$ -termos, então os subtermos de  $t$  são  $t$  e os subtermos de  $t_1, t_2, \dots, t_n$ .
- (b) Uma *subfórmula* de  $\varphi$  é uma  $\mathcal{L}$ -fórmula definida recursivamente do seguinte modo:
  - i. se  $\varphi$  é atômica, então  $\varphi$  é a única subfórmula de si mesma;

- ii. se  $\varphi$  é da forma  $(\neg\alpha)$  ou da forma  $(\forall x)(\alpha)$ , então as subfórmulas de  $\varphi$  são  $\varphi$  e as subfórmulas de  $\alpha$ ;
- iii. se  $\varphi$  é da forma  $(\alpha \vee \beta)$ , então as subfórmulas de  $\varphi$  são  $\varphi$  e as subfórmulas de  $\alpha$  e de  $\beta$ .

**Definição 2.4.** Sejam  $\mathcal{L}$  uma linguagem de primeira ordem,  $x$  uma variável e  $\varphi$  uma fórmula.

- (a) (Variáveis livres) Dizemos que  $x$  é *livre* em  $\varphi$  se
- i.  $\varphi$  é atômica e  $x$  ocorre em (é um símbolo)  $\varphi$ ; ou
  - ii.  $\varphi$  é da forma  $(\neg\alpha)$  e  $x$  é livre na fórmula  $\alpha$ ; ou
  - iii.  $\varphi$  é da forma  $(\alpha \vee \beta)$  e  $x$  é livre em pelo menos uma das fórmulas  $\alpha$  ou  $\beta$ ; ou
  - iv.  $\varphi$  é da forma  $(\forall y)(\alpha)$ , com  $x$  diferente de  $y$  e livre na fórmula  $\alpha$ .
- Equivalentemente, podemos dizer que uma ocorrência de  $x$  é livre em  $\varphi$  se  $x$  não ocorre no escopo de uma subfórmula  $(\forall x)(\alpha)$  de  $\varphi$ .
- (b) (Variáveis ligadas) Dizemos que  $x$  é *ligada* em  $\varphi$  se não for livre em  $\varphi$ .
- (c) (Sentenças) Uma *sentença* de  $\mathcal{L}$ , ou uma  $\mathcal{L}$ -*sentença*, é uma  $\mathcal{L}$ -fórmula que não possui variáveis livres.

**Definição 2.5** (Substituição). Sejam  $\mathcal{L}$  uma linguagem de primeira ordem,  $t$  um termo e  $x$  uma variável.

- (a) Seja  $u$  um termo. O termo  $u_t^x$ , que resulta da substituição de todas as ocorrências de  $x$  em  $u$  por  $t$ , é definido recursivamente do seguinte modo:
- i. se  $u$  é uma variável diferente de  $x$ , então  $u_t^x$  é  $u$ ;
  - ii. se  $u$  é a variável  $x$ , então  $u_t^x$  é  $t$ ;
  - iii. se  $u$  é uma constante, então  $u_t^x$  é  $u$ ;
  - iv. se  $u$  é da forma  $ft_1 \dots t_n$ , então  $u_t^x$  é  $ft_1^x \dots t_n^x$ .
- (b) Seja  $\varphi$  uma fórmula. A fórmula  $\varphi_t^x$ , que resulta da substituição de todas as ocorrências de  $x$  em  $\varphi$  por  $t$ , é definida recursivamente do seguinte modo:
- i. se  $\varphi$  é da forma  $(t_1 = t_2)$ , então  $\varphi_t^x$  é  $(t_1^x = t_2^x)$ ;
  - ii. se  $\varphi$  é da forma  $Rt_1 \dots t_n$ , então  $\varphi_t^x$  é  $Rt_1^x \dots t_n^x$ ;
  - iii. se  $\varphi$  é da forma  $(\neg\alpha)$ , então  $\varphi_t^x$  é  $(\neg\alpha_t^x)$ ;
  - iv. se  $\varphi$  é da forma  $(\alpha \vee \beta)$ , então  $\varphi_t^x$  é  $(\alpha_t^x \vee \beta_t^x)$ ;
  - v. se  $\varphi$  é da forma  $(\forall y)(\alpha)$ , então  $\varphi_t^x$  é

$$\begin{cases} \varphi, & \text{se } y \text{ é } x; \text{ ou} \\ (\forall y)(\alpha_t^x), & \text{caso contrário.} \end{cases}$$

**Definição 2.6** (Substituibilidade). Sejam  $\mathcal{L}$  uma linguagem de primeira ordem,  $\varphi$  uma fórmula,  $t$  um termo e  $x$  uma variável. Dizemos que  $x$  é *substituível* por  $t$  em  $\varphi$  se

- i.  $\varphi$  é atômica; ou
- ii.  $\varphi$  é da forma  $(\neg\alpha)$  e  $x$  é substituível por  $t$  em  $\alpha$ ;
- iii.  $\varphi$  é da forma  $(\alpha \vee \beta)$  e  $x$  é substituível por  $t$  em  $\alpha$  e em  $\beta$ ;
- iv.  $\varphi$  é da forma  $(\forall y)(\alpha)$  e, exclusivamente, ou  $x$  é ligada em  $\varphi$ , ou  $y$  não ocorre em  $t$  e  $x$  é substituível por  $t$  em  $\alpha$ .

## 2.2 Estruturas

**Definição 2.7.** Seja  $\mathcal{L}$  uma linguagem de primeira ordem. Uma  $\mathcal{L}$ -*estrutura*  $\mathfrak{A}$  consiste num conjunto  $A$ , chamado de *universo* de  $\mathfrak{A}$ , tal que

- i. para cada símbolo de constante  $c$  de  $\mathcal{L}$ , há um elemento  $c^{\mathfrak{A}}$  em  $A$ ;
- ii. para cada símbolo de função  $n$ -ário  $f$  de  $\mathcal{L}$ , há uma função  $f^{\mathfrak{A}} : A^n \rightarrow A$ ;
- iii. para cada símbolo de relação  $n$ -ário  $R$  de  $\mathcal{L}$ , há uma relação  $R^{\mathfrak{A}}$  em  $A$  (isto é,  $R^{\mathfrak{A}} \subseteq A^n$ ).

**Definição 2.8.** Seja  $\mathfrak{A}$  uma  $\mathcal{L}$ -estrutura de universo  $A$ .

- (a) Uma *valoração* é qualquer função  $s : \text{Vars} \rightarrow A$ .
- (b) Sejam  $s$  uma valoração,  $x$  uma variável e  $a$  um elemento de  $A$ . Uma  *$x$ -modificação de  $s$*  é definida como

$$s[x|a](v) := \begin{cases} s(v) & \text{se } v \text{ é uma variável diferente de } x \\ a & \text{se } v \text{ é a variável } x \end{cases}.$$

- (c) Seja  $s : \text{Vars} \rightarrow A$  uma valoração. Uma *valoração de termos gerada por  $s$*  é uma função  $\bar{s} : \text{Term} \rightarrow A$  definida recursivamente do seguinte modo:
  - i. se  $t$  é uma variável, então  $\bar{s}(t) = s(t)$ ;
  - ii. se  $t$  é um símbolo de constante  $c$ , então  $\bar{s}(t) = c^{\mathfrak{A}}$ ;
  - iii. se  $t$  é da forma  $ft_1 \dots t_n$ , onde  $f$  é um símbolo funcional  $n$ -ário e  $t_1, \dots, t_n$  são termos, então  $\bar{s}(t) = f^{\mathfrak{A}}(\bar{s}(t_1), \dots, \bar{s}(t_n))$ .
- (d) Sejam  $\varphi$  uma  $\mathcal{L}$ -fórmula e  $s : \text{Vars} \rightarrow A$  uma valoração. Dizemos que  $\mathfrak{A}$  *satisfaz  $\varphi$  com relação a  $s$* , denotando isso por  $\mathfrak{A} \models \varphi[s]$ , se

- i.  $\varphi$  é da forma  $= t_1 t_2$  e  $\bar{s}(t_1)$  coincide com  $\bar{s}(t_2)$ ; ou
- ii.  $\varphi$  é da forma  $Rt_1 \dots t_n$  e  $(\bar{s}(t_1), \dots, \bar{s}(t_n))$  é um elemento de  $R^{\mathfrak{A}}$ ; ou
- iii.  $\varphi$  é da forma  $(\neg\alpha)$  e  $\mathfrak{A} \not\models \alpha[s]$ ; ou
- iv.  $\varphi$  é da forma  $(\alpha \vee \beta)$  e  $\mathfrak{A} \models \alpha[s]$  ou  $\mathfrak{A} \models \beta[s]$ ; ou
- v.  $\varphi$  é da forma  $(\forall x)(\alpha)$  e  $\mathfrak{A} \models \alpha[s[x|a]]$  para cada elemento  $a$  de  $A$ .

Se  $\Gamma$  é um conjunto de  $\mathcal{L}$ -fórmulas, dizemos que  $\mathfrak{A}$  satisfaz  $\Gamma$  com relação a  $s$ , escrevendo  $\mathfrak{A} \models \Gamma[s]$ , se  $\mathfrak{A} \models \gamma[s]$  para cada fórmula  $\gamma$  em  $\Gamma$ .

**Teorema 2.9.** Seja  $\mathfrak{A}$  uma  $\mathcal{L}$ -estrutura.

- (a) Se  $s_1$  e  $s_2$  são valorações tais que  $s_1(v) = s_2(v)$  para toda variável  $v$  que ocorre num termo  $t$ , então  $\bar{s}_1(t) = \bar{s}_2(t)$ .
- (b) Se  $s_1$  e  $s_2$  são valorações tais que  $s_1(v) = s_2(v)$  para toda variável livre  $v$  que ocorre na fórmula  $\varphi$ , então  $\mathfrak{A} \models \varphi[s_1]$  se, e somente se,  $\mathfrak{A} \models \varphi[s_2]$ .
- (c) Se  $\psi$  é uma sentença, então ou  $\mathfrak{A} \models \psi[s]$  para todas as valorações  $s$ , ou  $\mathfrak{A} \not\models \psi[s]$  para nenhuma valoração  $s$ .

**Prova.** Ver [16], seção 1.7.

**Definição 2.10.** Seja  $\mathfrak{A}$  uma  $\mathcal{L}$ -estrutura.

- (a) Seja  $\varphi$  uma fórmula. Diremos que  $\mathfrak{A}$  é um *modelo* de  $\varphi$ , denotando isso por  $\mathfrak{A} \models \varphi$ , se  $\mathfrak{A} \models \varphi[s]$  para toda função de atribuição de variável  $s$ .
- (b) Seja  $\Phi$  um conjunto de fórmulas. Diremos que  $\mathfrak{A}$  *modela*  $\Phi$ , denotando isso por  $\mathfrak{A} \models \Phi$ , se  $\mathfrak{A} \models \varphi$  para cada fórmula  $\varphi$  de  $\Phi$ .

# Capítulo 3

## O sistema ZFC

A linguagem (de primeira ordem) da teoria dos conjuntos, denotada por  $\mathcal{L}_{ST}$ , consiste em somente um símbolo de predicado binário dito de *pertencimento*  $\in$ . A seguir apresentamos os axiomas de ZFC que constituem a teoria de primeira ordem da teoria dos conjuntos. Na primeira seção apresentamos e discutimos os axiomas básicos, deixando os axiomas do infinito (que garante a existência do conjunto dos números naturais  $\omega$ ), da escolha (que tem muitas equivalências) e da substituição (fundamental para a teoria dos ordinais), os mais importantes, e mais complicados, para serem tratados nas próximas seções.

### 3.1 Primeiros Axiomas

#### 3.1.1 O Axioma da Extensão

**Axioma 3.1** (da Extensão). Dois conjuntos são iguais se, e somente se, eles têm os mesmos elementos.

$$\boxed{\forall x \forall y ((x = y) \leftrightarrow \forall z ((z \in x) \leftrightarrow (z \in y)))}$$

**Definição 3.2** (Inclusão). Um conjunto  $x$  está *contido* num conjunto  $y$ , ou é um *subconjunto* de  $y$ , se todo elemento de  $x$  é um elemento de  $y$ :

$$(x \subseteq y) \stackrel{\text{def}}{\leftrightarrow} \forall z ((z \in x) \rightarrow (z \in y)).$$

**Observação 3.3.** De maneira análoga podemos definir  $\subsetneq$ ,  $\not\subseteq$ ,  $\supseteq$ , etc. Além disso, com a definição de  $\subseteq$ , o axioma da extensão pode ser enunciado assim:

$$\forall x \forall y ((x = y) \leftrightarrow ((x \subseteq y) \wedge (y \subseteq x))).$$

**Proposição 3.4.** <sup>1</sup>

- (a)  $\forall x(x \subseteq x)$ .
- (b)  $\forall x \forall y((x \subseteq y) \wedge (y \subseteq x) \rightarrow (x = y))$ .
- (c)  $\forall x \forall y \forall z(((x \subseteq y) \wedge (y \subseteq z)) \rightarrow (x \subseteq z))$ .

**Prova.** ■**3.1.2 O Axioma do Vazio****Definição 3.5.** Um conjunto  $x$  é *vazio* se  $\forall y(y \notin x)$ .**Axioma 3.6** (do Vazio). Existe um conjunto vazio.

$$\boxed{\exists x \forall y(y \notin x)}$$

Onde  $(y \notin x) \stackrel{\text{def}}{\leftrightarrow} (\neg(y \in x))$ .**Proposição 3.7.** Quaisquer dois conjuntos vazios são iguais.

$$\forall x_1 \forall x_2((\forall y(y \notin x_1) \wedge \forall y(y \notin x_2)) \rightarrow (x_1 = x_2)).$$

**Prova.** Se  $x_1 \neq x_2$ , então ou existe  $z \in x_1$  tal que  $z \notin x_2$ , ou existe  $z \in x_2$  tal que  $z \notin x_1$ . Em ambos os casos,  $x_1$  e  $x_2$  não são vazios, uma contradição. Logo  $x_1 = x_2$ . ■**Observação 3.8.** O axioma do vazio (3.6), junto com a proposição (3.7), nos permite estabelecer que existe um único conjunto vazio:

$$\exists x(\forall y(y \notin x) \wedge \forall z(\forall y(y \notin z) \rightarrow (z = x))).$$

Podemos então falar *do* conjunto vazio (em vez de *de um*). Ele é denotado por  $\emptyset$ .**Proposição 3.9.** O conjunto vazio está contido em qualquer conjunto.

$$\forall x(\emptyset \subseteq x)$$

**Prova.** Suponha que existe  $x$  tal que  $\emptyset \not\subseteq x$ . Então existe  $y \in \emptyset$  tal que  $y \notin x$ , uma contradição pois  $\forall y(y \notin \emptyset)$ . Logo  $\forall x(\emptyset \subseteq x)$ . ■**Prova.** Pela definição de  $\subseteq$ , precisamos provar que  $\forall x(\forall y((y \in \emptyset) \rightarrow (y \in x)))$ . Como a fórmula  $y \in \emptyset$  é sempre falsa,  $(y \in \emptyset) \rightarrow (y \in x)$  é sempre verdadeira,<sup>1</sup>Conforme a definição (3.45), isso significa que a relação  $\subseteq$  é uma relação de ordem parcial.

donde  $\forall y((y \in \emptyset) \rightarrow (y \in x))$  é sempre verdadeira, donde  $\forall x(\forall y((y \in \emptyset) \rightarrow (y \in x)))$  é sempre verdadeira. Isto prova que a fórmula  $\forall x(\emptyset \subseteq x)$  é sempre verdadeira. ■

### 3.1.3 O Axioma do Par

**Axioma 3.10** (do Par). Para quaisquer conjuntos  $x$  e  $y$ , existe um conjunto cujos elementos são  $x$  e  $y$ .

$$\boxed{\forall x \forall y \exists z \forall w ((w \in z) \leftrightarrow ((w = x) \vee (w = y)))}$$

**Proposição 3.11.** O conjunto  $z$  do axioma do par é único. Notação:  $z := \{x, y\}$ .

**Prova.** Pelo axioma do par,  $z$  é tal que

$$\forall w ((w \in z) \leftrightarrow ((w = x) \vee (w = y))).$$

Se  $z'$  é tal que

$$\forall w ((w \in z') \leftrightarrow ((w = x) \vee (w = y))),$$

então  $\forall w ((w \in z') \leftrightarrow (w \in z))$ , de modo que  $z' = z$  pelo axioma da extensão. ■

**Proposição 3.12.**  $\forall x \forall y ((x \in y) \leftrightarrow \{x\} \subseteq y)$ .

### 3.1.4 O Axioma da União

**Axioma 3.13** (da União). Para todo conjunto  $x$  existe o conjunto de todos os conjuntos que pertencem a algum elemento de  $x$ .

$$\boxed{\forall x \exists y \forall z ((z \in y) \leftrightarrow \exists w ((z \in w) \wedge (w \in x)))}$$

**Proposição 3.14.** O conjunto  $y$  do axioma da união é único. Notação:  $y := \bigcup x$ .

**Prova.** Pelo axioma da união,  $y$  é tal que

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

Se  $y'$  é tal que

$$\forall z ((z \in y') \leftrightarrow \exists w ((z \in w) \wedge (w \in x))),$$

então  $\forall z ((z \in y') \leftrightarrow (z \in y))$ , donde  $y' = y$  pelo axioma da extensão. ■

**Teorema 3.15.** Para quaisquer conjuntos  $x$  e  $y$ , existe o conjunto dos conjuntos que pertencem a  $x$  ou a  $y$ .

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

Ademais, esse conjunto é único, sendo denotado por  $x \cup y$ .

**Prova.** Provemos que  $z := \bigcup \{x, y\}$ , que existe pelos axiomas do par e da união, funciona. De fato, para todo  $w$ , temos  $w \in z$  se, e somente se, existe  $u \in \{x, y\}$  tal que  $w \in u$ . Mas  $u \in \{x, y\}$  se, e somente se,  $u = x$  ou  $u = y$ , de modo que  $w \in x$  ou  $w \in y$ , como queríamos. A unicidade de  $z$  segue do axioma da extensão, de modo que podemos denotar  $x \cup y := z$ . ■

**Prova.** Uma prova alternativa é a seguinte. Precisamos provar que

$$\forall w \left( \left( w \in \bigcup \{x, y\} \right) \leftrightarrow ((w \in x) \vee (w \in y)) \right). \quad (\diamond)$$

Pelos axiomas do par e da união, temos

$$\begin{aligned} w \in \bigcup \{x, y\} &\leftrightarrow \exists u ((u \in \{x, y\}) \wedge (w \in u)) \\ &\leftrightarrow \exists u (((u = x) \vee (u = y)) \wedge (w \in u)) \\ &\leftrightarrow \exists u (((u = x) \wedge (w \in u)) \vee ((u = y) \wedge (w \in u))) \\ &\leftrightarrow \exists u ((w \in x) \vee (w \in y)) \\ &\leftrightarrow (w \in x) \vee (w \in y). \end{aligned}$$

Com isso, temos  $\diamond$ , como queríamos. ■

### 3.1.5 O Axioma das Partes

**Axioma 3.16** (das Partes). Para todo conjunto  $x$ , existe o conjunto dos subconjuntos de  $x$ .

$$\boxed{\forall x \exists y \forall z ((z \in y) \leftrightarrow (z \subseteq x))}$$

**Proposição 3.17.** O conjunto  $y$  do axioma das partes é único. Notação:  $y := \mathcal{P}(x)$ .

**Prova.** Pelo axioma das partes, o conjunto  $y$  cumpre  $\forall z ((z \in y) \leftrightarrow (z \subseteq x))$ . Se  $y'$  cumpre  $\forall z ((z \in y') \leftrightarrow (z \subseteq x))$ , então  $\forall z ((z \in y') \leftrightarrow (z \in y))$ , de modo que  $y' = y$  pelo axioma da extensão. ■

### 3.1.6 O Esquema de Axiomas da Separação

**Axioma 3.18** (da Separação). Para cada fórmula  $P$  em que  $z$  não ocorre livre, a fórmula

$$\boxed{\forall y \exists z \forall x ((x \in z) \leftrightarrow ((x \in y) \wedge P))}$$

é um axioma.

**Observação 3.19.** O conjunto  $y$  é o “universo” da discussão. O axioma da separação também é chamado de axioma da compreensão ou axioma da especificação.

**Proposição 3.20.** O conjunto  $z$  do axioma da separação (3.18) é único. Notação:  $z := \{x \in y : P(x)\}$ .

**Prova.** Segue do axioma da extensão. ■

**Teorema 3.21** (Paradoxo de Russell). Não existe o conjunto de todos os conjuntos.

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

**Prova.** Suponha que  $\exists x \forall y (y \in x)$ . Pelo axioma da separação com universo  $x$  e a fórmula  $y \notin y$ , existe  $z$  tal que  $\forall y ((y \in z) \leftrightarrow ((y \in x) \wedge (y \notin y)))$  (note que  $z$  não ocorre livre em  $y \notin y$ ). Como  $\forall y (y \in x)$ , temos  $\forall y ((y \in z) \leftrightarrow (y \notin y))$ . Particularmente para  $y = z$ , temos  $((z \in z) \leftrightarrow (z \notin z))$ , uma contradição. Logo  $\forall x \exists y (y \notin x)$ . ■

**Teorema 3.22.** Para todo conjunto  $x \neq \emptyset$  existe o conjunto de todos os conjuntos que pertencem simultaneamente a todos os elementos de  $x$ .

$$\forall x ((x \neq \emptyset) \rightarrow \exists y \forall z ((z \in y) \leftrightarrow \forall w ((w \in x) \rightarrow (z \in w))))$$

Ademais, esse conjunto é único, sendo denotado por  $\bigcap x$ .

**Prova.** Precisamos provar que existe  $y$  tal que

$$\forall z ((z \in y) \leftrightarrow \forall w ((w \in x) \rightarrow (z \in w))). \quad (\diamond)$$

Observe inicialmente que o axioma da separação pode ser escrito como

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

onde  $P$  é uma fórmula em que  $y$  não ocorre livre. Agora, como  $x \neq \emptyset$ , tome  $v \in x$ . Pelo axioma da separação com universo  $v$  e a fórmula  $\forall w ((w \in x) \rightarrow (z \in w))$ , onde  $y$  não ocorre livre, existe  $y$  tal que

$$\forall z ((z \in y) \leftrightarrow ((z \in v) \wedge (\forall w ((w \in x) \rightarrow (z \in w))))),$$

isto é, existe

$$y := \{z \in v : \forall w((w \in x) \rightarrow (z \in w))\}.$$

Afirmamos que vale ( $\diamond$ ) nesse  $y$ . De fato,

- por um lado ( $\Rightarrow$ ), se  $z \in y$ , então trivialmente  $\forall w((w \in x) \rightarrow (z \in w))$ ;
- por outro lado ( $\Leftarrow$ ), se  $z$  é tal que  $\forall w((w \in x) \rightarrow (z \in w))$ , então, particularmente para  $w = v$ , temos  $v \in x \rightarrow z \in v$ , e como  $v \in x$ , temos  $z \in v$ . Como  $z \in v$  e  $\forall w((w \in x) \rightarrow (z \in w))$ , temos que  $z \in y$ .

Logo, existe  $y$  tal que  $\diamond$ . A unicidade de  $y$  segue do axioma da extensão, de modo que podemos denotar  $\bigcap x := y$ . ■

**Definição 3.23.** Sejam  $x$  e  $y$  conjuntos.

(a) A *interseção* entre  $x$  e  $y$  é definida como

$$x \cap y := \{z \in x : z \in y\}.$$

Dizemos que  $x$  e  $y$  são *disjuntos* se  $x \cap y = \emptyset$ .

(b) A *diferença* entre  $x$  e  $y$  é definida como

$$x \setminus y := \{z \in x : z \notin y\}.$$

Dizemos que  $x \setminus y$  é o *complementar* de  $y$  relativo a  $x$  se  $y \subseteq x$ . Nesse caso, denotamos  $x \setminus y$  por  $y^C$ .

(c) A *diferença simétrica* entre  $x$  e  $y$  é definida como

$$x \Delta y := \{z \in x \cup y : z \notin x \cap y\}.$$

**Observação 3.24.** As definições (3.23) se dão pelo axioma da separação. Vejamos como isso é feito, por exemplo, na definição de  $x \cap y$ . Sendo  $x$  o universo, o axioma da separação é a fórmula  $\forall x \exists w \forall z((z \in w) \leftrightarrow ((z \in x) \wedge P))$ , onde  $P$  é uma fórmula em que  $w$  não ocorre livre. Se  $P$  é a fórmula  $z \in y$ , então existe  $w$  que cumpre  $\forall z((z \in w) \leftrightarrow (z \in x) \wedge (z \in y))$ , isto é,  $w = \{z \in x : z \in y\}$ . Denotamos esse  $w$  por  $x \cap y$ .

### 3.1.7 Propriedades Algébricas

**Proposição 3.25** (Propriedades da União).

- (a)  $\forall x(x \cup x = x)$ .
- (b)  $\forall x(x \cup \emptyset = x)$ .

- (c)  $\forall x \forall y (x \cup y = y \cup x)$ .
- (d)  $\forall x \forall y \forall z (x \cup (y \cup z) = (x \cup y) \cup z)$ .
- (e)  $\forall x \forall y (x \cup y = y \leftrightarrow x \subseteq y)$ .
- (f)  $\forall x \forall y ((x \subseteq x \cup y) \wedge (y \subseteq x \cup y))$ .
- (g)  $\forall x \forall y \forall z (x \subseteq y \rightarrow x \cup z \subseteq y \cup z)$ .
- (h)  $\forall x \forall y (x \subseteq y \rightarrow \bigcup x \subseteq \bigcup y)$ .

**Prova.** Trivial. ■

**Proposição 3.26** (Propriedades da Interseção).

- (a)  $\forall x (x \cap x = x)$ .
- (b)  $\forall x (x \cap \emptyset = \emptyset)$ .
- (c)  $\forall x \forall y (x \cap y = y \cap x)$ .
- (d)  $\forall x \forall y \forall z (x \cap (y \cap z) = (x \cap y) \cap z)$ .
- (e)  $\forall x \forall y (x \cap y = x \leftrightarrow x \subseteq y)$ .
- (f)  $\forall x \forall y ((x \cap y \subseteq x) \wedge (x \cap y \subseteq y))$ .
- (g)  $\forall x \forall y \forall z (x \subseteq y \rightarrow x \cap z \subseteq y \cap z)$ .
- (h)  $\forall x \forall y (x \subseteq y \wedge x \neq \emptyset \rightarrow \bigcap y \subseteq \bigcap x)$ .

**Prova.** Trivial. ■

**Proposição 3.27** (Distributividade).

- (a)  $\forall x \forall y \forall z (x \cap (y \cup z) = (x \cap y) \cup (x \cap z))$ .
- (b)  $\forall x \forall y \forall z (x \cup (y \cap z) = (x \cup y) \cap (x \cup z))$ .

**Prova.** Trivial. ■

**Proposição 3.28** (Propriedades da Diferença).

- (a) (Imediatas).
  - i.  $\forall x (x \setminus \emptyset = x)$ ;
  - ii.  $\forall x (x \setminus x = \emptyset)$ ;
  - iii.  $\forall x (\emptyset \setminus x = \emptyset)$ .
- (b)
  - i.  $\forall x \forall y (x \setminus y = x \leftrightarrow x \cap y = \emptyset)$ ;
  - ii.  $\forall x \forall y (x \setminus y = \emptyset \leftrightarrow x \subseteq y)$ .
- (c) (Leis de De Morgan).

- i.  $\forall x \forall y \forall z (x \setminus (y \cup z) = (x \setminus y) \cap (x \setminus z));$
- ii.  $\forall x \forall y \forall z (x \setminus (y \cap z) = (x \setminus y) \cup (x \setminus z)).$
- (d)  $\forall x \forall y \forall z (x \setminus (y \setminus z) = (x \setminus y) \cup (x \cap z)).$
- (e) (Diferenças entre interseções).
  - i.  $\forall x \forall y \forall z (x \cap (y \setminus z) = (x \cap y) \setminus (x \cap z));$
  - ii.  $\forall x \forall y \forall z ((x \setminus y) \cap z = (x \cap z) \setminus y).$
- (f) (Monotonocidade da diferença).
  - i.  $\forall x \forall y \forall z (x \subseteq y \rightarrow x \setminus z \subseteq y \setminus z).$
  - ii.  $\forall x \forall y \forall z (y \subseteq z \rightarrow x \setminus z \subseteq x \setminus y).$

**Prova.** Trivial. ■

**Proposição 3.29** (Propriedades do Complemento Relativo).

- (a)  $\forall x \forall y (y \subseteq x \rightarrow (y^C)^C = y).$
- (b)  $\forall x \forall y (y \subseteq x \rightarrow (y \cup y^C = x) \wedge (y \cap y^C = \emptyset)).$
- (c)  $\forall x \forall y \forall z (z \subseteq y \subseteq x \rightarrow y^C \subseteq z^C).$
- (d)  $\forall x \forall y \forall z (y \subseteq x \wedge z \subseteq x \rightarrow y \setminus z = y \cap z^C).$
- (e) (Leis de De Morgan para complementos).
  - i.  $\forall x \forall y \forall z (y \subseteq x \wedge z \subseteq x \rightarrow (y \cup z)^C = y^C \cap z^C).$
  - ii.  $\forall x \forall y \forall z (y \subseteq x \wedge z \subseteq x \rightarrow (y \cap z)^C = y^C \cup z^C).$

**Prova.** Trivial. ■

**Proposição 3.30.**

- (a)  $\forall x \forall y \forall z (((x \in y) \wedge (y \in z)) \rightarrow ((x \in \bigcup z) \wedge (y \subseteq \bigcup z))).$

**Proposição 3.31.**  $\forall A (\bigcup \mathcal{P}(A) = A).$

### 3.1.8 O Axioma da Regularidade

**Axioma 3.32** (da Regularidade). Para todo conjunto  $x \neq \emptyset$  existe  $y \in x$  tal que  $x \cap y = \emptyset$ .

$$\boxed{\forall x ((x \neq \emptyset) \rightarrow \exists y ((y \in x) \wedge (x \cap y = \emptyset)))}$$

**Proposição 3.33.** Não existem conjuntos  $x$  e  $y$  tais que  $x \in y$  e  $y \in x$ .

$$\neg(\exists x \exists y ((x \in y) \wedge (y \in x)))$$

**Prova.** Basta provar que  $\forall x \forall y ((x \notin y) \vee (y \notin x))$ . Pelo axioma do par, tome  $z := \{x, y\}$ . Como  $z \neq \emptyset$ , pelo axioma da regularidade existe  $w \in z$  tal que  $w \cap z = \emptyset$ . Se  $w = x$ , então  $y \notin x$ , porque se fosse  $y \in x$  teríamos  $x \cap z = \{y\} \neq \emptyset$ , uma contradição. Analogamente, se  $w = y$ , então  $x \notin y$ . ■

**Corolário 3.34.** Não existe  $x$  tal que  $x \in x$ .

$$\forall x (x \notin x)$$

**Prova.** Segue do teorema anterior com  $y = x$ . ■

## 3.2 Relações e Funções

### 3.2.1 Produto Cartesiano

**Definição 3.35** (Par ordenado). Sejam  $a$  e  $b$  conjuntos. O *par ordenado*  $(a, b)$  é definido como o conjunto  $\{\{a\}, \{a, b\}\}$ , isto é,

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

**Proposição 3.36.** Dois pares ordenados  $(a, b)$  e  $(c, d)$  são iguais se, e somente se,  $a = c$  e  $b = d$ .

$$\forall a \forall b \forall c \forall d ((a, b) = (c, d)) \leftrightarrow ((a = c) \wedge (b = d))$$

**Prova.** Ver [5], teorema 4.2, página 95. Ver [7], teorema 4.2, página 50. ■

**Teorema 3.37.** Para quaisquer conjuntos  $A$  e  $B$  existe o conjunto de todos os pares ordenados  $(a, b)$  tais que  $a \in A$  e  $b \in B$ .

$$\forall A \forall B \exists C \forall x (x \in C \leftrightarrow \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b)))$$

Ademais, esse conjunto é único, sendo denotado por  $A \times B$ .

**Prova.** Pelos axiomas da união e das partes, considere o conjunto  $\mathcal{P}(\mathcal{P}(A \cup B))$ ; pelo axioma da separação, considere o conjunto

$$C := \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b))\}.$$

Afirmamos que  $C$  cumpre as condições do enunciado. Se  $x \in C$ , então pela definição de  $C$  existem  $a \in A$  e  $b \in B$  tais que  $x = (a, b)$ . Provemos então que se

existem  $a \in A$  e  $b \in B$  tais que  $x = (a, b)$ , então  $x \in C$ . Para isso, basta provar que  $x \in \mathcal{P}(\mathcal{P}(A \cup B))$ . Qualquer que seja o par ordenado  $(a, b)$ , onde  $a \in A$  e  $b \in B$ ,

$$\begin{aligned} (a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) &\leftrightarrow \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B)) \\ &\leftrightarrow \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B) \\ &\leftrightarrow \{a\} \in \mathcal{P}(A \cup B) \wedge \{a, b\} \in \mathcal{P}(A \cup B) \\ &\leftrightarrow \{a\} \subseteq (A \cup B) \wedge \{a, b\} \subseteq (A \cup B), \end{aligned}$$

o que sabemos ser verdade. A unicidade de  $C$  segue do axioma da extensão, de modo que podemos denotar  $A \times B := C$ . ■

**Definição 3.38.** O *produto cartesiano* dos conjuntos  $A$  e  $B$  é definido como  $A \times B$ .

### 3.2.2 Relações

**Definição 3.39.**

- (a) Uma *relação binária*, ou simplesmente uma *relação*, é um conjunto de pares ordenados.
- (b) Um símbolo de predicado para “ $R$  é relação”, onde  $R$  ocorre livre, é

$$\text{Rel}(R) \stackrel{\text{def}}{\leftrightarrow} \forall x (x \in R \rightarrow \exists a \exists b (x = (a, b))).$$

Denotamos  $(a, b) \in R$  por  $aRb$ .

- (c) Dizemos que  $R$  é uma relação de  $A$  em  $B$  se  $R \subseteq A \times B$ . Dizemos que  $R$  é uma relação em  $A$  se  $R \subseteq A \times A$ .

**Teorema 3.40.** Um conjunto  $R$  é uma relação se, e somente se, existem conjuntos  $A$  e  $B$  tais que  $R \subseteq A \times B$ .

$$\forall R (\text{Rel}(R) \leftrightarrow \exists A \exists B (R \subseteq A \times B))$$

**Prova.** ( $\Rightarrow$ ) Sendo  $R$  uma relação, usando os axiomas da união e da separação, defina

$$\begin{aligned} A &:= \left\{ a \in \bigcup \bigcup R : \exists b (b \in \bigcup \bigcup R \wedge aRb) \right\} \\ B &:= \left\{ b \in \bigcup \bigcup R : \exists a (a \in \bigcup \bigcup R \wedge aRb) \right\} \end{aligned}$$

Seja  $x \in R$ . Então existem  $a$  e  $b$  tais que  $x = (a, b)$ . Se  $\{\{a\}, \{a, b\}\} \in R$ , então  $\{\{a\}, \{a, b\}\} \subseteq \bigcup R$ , donde  $\{a, b\} \in \bigcup R$ , donde  $\{a, b\} \subseteq \bigcup \bigcup R$ , donde

$a, b \in \bigcup \bigcup R$ . Como  $aRb$ , pelas definições de  $A$  e  $B$ , temos  $a \in A$  e  $b \in B$ . Como  $x = (a, b)$  e  $a \in A$  e  $b \in B$ , pelo teorema (3.37) temos  $x \in A \times B$ , donde, por fim, segue que  $R \subseteq A \times B$ .

( $\Leftarrow$ ) Os elementos de  $A \times B$  são pares ordenados; logo, qualquer subconjunto de  $A \times B$  terá pares ordenados como elementos. ■

**Definição 3.41.** Seja  $R$  uma relação.

(a) O domínio de  $R$  é definido como

$$\text{Dom}(R) := \left\{ a \in \bigcup \bigcup R : \exists b((a, b) \in R) \right\}.$$

(b) A imagem de  $R$  é definida como

$$\text{Im}(R) := \left\{ b \in \bigcup \bigcup R : \exists a((a, b) \in R) \right\}.$$

(c) A relação inversa de  $R$  é definida como

$$R^{-1} := \{(b, a) \in \text{Im}(R) \times \text{Dom}(R) : (a, b) \in R\}.$$

(d) A imagem de um conjunto  $X$  por  $R$  é definida como

$$R[X] := \{b \in \bigcup \bigcup R : \exists a(a \in X \wedge (a, b) \in R)\}.$$

(e) A imagem inversa de um conjunto  $Y$  por  $R$  é definida como

$$R^{-1}[Y] := \left\{ a \in \bigcup \bigcup R : \exists b(b \in Y \wedge (a, b) \in R) \right\}$$

Equivalentemente,  $R^{-1}[Y]$  é a imagem de  $Y$  pela relação  $R^{-1}$ .

(f) A restrição de  $R$  a  $X$  é definida como

$$R|_X := \{(a, b) \in R : a \in X\}.$$

(g) A composição de  $R$  e  $S$  é definida como

$$S \circ R := \{(a, c) \in \text{Dom}(R) \times \text{Im}(S) : \exists b(b \in \text{Im}(R) \cap \text{Dom}(S) \wedge (aRb \wedge bSc))\}.$$

**Proposição 3.42.** Sejam  $R$  e  $S$  relações e  $A, B, C$  e  $D$  conjuntos tais que  $R \subseteq A \times B$  e  $S \subseteq C \times D$ .

(a)  $\text{Dom}(R) = \{x \in A : \exists y(y \in B \wedge xRy)\}.$

(b)  $\text{Im}(R) = \{y \in B : \exists x(x \in A \wedge xRy)\}.$

(c)  $S \circ R \subseteq A \times D.$

**Prova.**

(a) Se  $x \in \text{Dom}(R)$ , então existe  $y \in \text{Im}(R)$  tal que  $(x, y) \in R$ . Como  $R \subseteq A \times B$ , temos  $(x, y) \in A \times B$ , donde  $x \in A$  e  $y \in B$ . Assim,  $x \in A$  e existe  $y \in B$  tal que  $xRy$ , o que prova a inclusão  $\subseteq$ . Reciprocamente, se  $x \in A$  e existe  $y \in B$  tal que  $(x, y) \in R$ , então  $x \in \text{Dom}(R)$ , o que prova a inclusão  $\supseteq$ . ■

(b) Se  $y \in \text{Im}(R)$ , então existe  $x \in \text{Dom}(R)$  tal que  $(x, y) \in R$ . Como  $R \subseteq A \times B$ , temos  $(x, y) \in A \times B$ , donde  $x \in A$  e  $y \in B$ . Assim,  $y \in B$  e existe  $x \in A$  tal que  $xRy$ , o que prova a inclusão  $\subseteq$ . Reciprocamente, se  $y \in B$  e existe  $x \in A$  tal que  $(x, y) \in R$ , então  $y \in \text{Im}(R)$ , o que prova a inclusão  $\supseteq$ . ■

(c) Se  $(x, z) \in S \circ R$ , então  $x \in \text{Dom}(R)$  e  $z \in \text{Im}(S)$ . Como  $\text{Dom}(R) \subseteq A$  (primeiro item) e  $\text{Im}(S) \subseteq D$  (segundo item), temos  $x \in A$  e  $z \in D$ , de modo que  $(x, z) \in A \times D$ . Com isso,  $S \circ R \subseteq A \times D$ . ■

**Proposição 3.43.** Sejam  $R, S$  e  $T$  relações. Valem as seguintes afirmações.

- (a) i.  $(R^{-1})^{-1} = R$ .  
ii.  $\text{Dom } R^{-1} = \text{Im}(R)$ .  
iii.  $\text{Im}(R^{-1}) = \text{Dom}(R)$
- (b)  $T \circ (S \circ R) = (T \circ S) \circ R$ .
- (c)  $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ .
- (d) Se  $\text{Im}(R) \subseteq \text{Dom}(S)$ , então  $\text{Dom}(S \circ R) = \text{Dom}(R)$ .
- (e) Se  $\text{Dom}(S) \subseteq \text{Im}(R)$ , então  $\text{Im}(S \circ R) = \text{Im}(S)$ .

**Prova.**

- (a) i. Temos  $(a, b) \in R$  se, e somente se,  $(b, a) \in R^{-1}$ , o que é equivalente a  $(a, b) \in (R^{-1})^{-1}$ . Logo  $R = (R^{-1})^{-1}$ .  
ii.  
iii.
- (b) Se  $(a, d) \in T \circ (S \circ R)$ , então  $a \in \text{Dom}(S \circ R)$ ,  $d \in \text{Im}(T)$  e existe  $c \in \text{Im}(S \circ R) \cap \text{Dom}(T)$  tal que  $(a, c) \in S \circ R$  e  $(c, d) \in T$ . De  $(a, c) \in S \circ R$  segue que  $a \in \text{Dom}(R)$ ,  $c \in \text{Im}(S)$  e existe  $b \in \text{Im}(R) \cap \text{Dom}(S)$  tal que  $(a, b) \in R$  e  $(b, c) \in S$ . Como  $b \in \text{Dom}(S)$ ,  $d \in \text{Im}(T)$  e existe  $c \in \text{Dom}(T) \cap \text{Im}(S)$  tal que  $(b, c) \in S$  e  $(c, d) \in T$ , temos que  $(b, d) \in$

$T \circ S$ . Com isso,  $b \in \text{Dom}(T \circ S)$  e  $d \in \text{Im}(T \circ S)$ . Como  $a \in \text{Dom}(R)$ ,  $d \in \text{Im}(T \circ S)$  e existe  $b \in \text{Dom}(T \circ S) \cap \text{Im}(R)$  tal que  $(a, b) \in R$  e  $(b, d) \in T \circ S$ , temos que  $(a, d) \in (T \circ S) \circ R$ . Com isso,  $T \circ (S \circ R) \subseteq (T \circ S) \circ R$ . A prova de que  $(T \circ S) \circ R \subseteq T \circ (S \circ R)$  é completamente análoga, de modo que  $T \circ (S \circ R) = (T \circ S) \circ R$ . ■

- (c) Se  $(c, a) \in (S \circ R)^{-1}$ , então  $(a, c) \in S \circ R$ ,  $a \in \text{Dom}(R)$ ,  $c \in \text{Im}(S)$  e existe  $b \in \text{Im}(R) \cap \text{Dom}(S)$  tal que  $(a, b) \in R$  e  $(b, c) \in S$  isto é,  $(c, b) \in S^{-1}$ ,  $(b, a) \in R^{-1}$ , com  $c \in \text{Dom}(S^{-1})$ ,  $a \in \text{Im}(R^{-1})$  e  $b \in \text{Im}(S^{-1}) \cap \text{Dom}(R^{-1})$ . Com isso,  $(c, a) \in R^{-1} \circ S^{-1}$ , de modo que  $(S \circ R)^{-1} \subseteq R^{-1} \circ S^{-1}$ . A prova de que  $R^{-1} \circ S^{-1} \subseteq (S \circ R)^{-1}$  é completamente análoga, de modo que  $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ . ■
- (d) Se  $a \in \text{Dom}(R)$ , então existe  $b \in \text{Im}(R)$  tal que  $(a, b) \in R$ . Se  $\text{Im}(R) \subseteq \text{Dom}(S)$ , então  $b \in \text{Dom}(S)$ , de modo que existe  $c \in \text{Im}(S)$  tal que  $(b, c) \in S$ . Assim,  $(a, c) \in S \circ R$ , de modo que  $a \in \text{Dom}(S \circ R)$ . Com isso,  $\text{Dom}(R) \subseteq \text{Dom}(S \circ R)$ . Agora, se  $a \in \text{Dom}(S \circ R)$ , então existe  $c \in \text{Im}(S \circ R)$  tal que  $(a, c) \in S \circ R$ , donde  $a \in \text{Dom}(R)$  e  $\text{Dom}(S \circ R) \subseteq \text{Dom}(R)$ . Com isso,  $\text{Dom}(R) = \text{Dom}(S \circ R)$ . ■
- (e) Se  $c \in \text{Im}(S)$ , então existe  $b \in \text{Dom}(S)$  tal que  $(b, c) \in S$ . Se  $\text{Dom}(S) \subseteq \text{Im}(R)$ , então  $b \in \text{Im}(R)$ , de modo que existe  $a \in \text{Dom}(R)$  tal que  $(a, b) \in R$ . Assim,  $(a, c) \in S \circ R$ , de modo que  $c \in \text{Im}(S \circ R)$ . Com isso,  $\text{Im}(S) \subseteq \text{Im}(S \circ R)$ . Agora, se  $c \in \text{Im}(S \circ R)$ , então existe  $a \in \text{Dom}(S \circ R)$  tal que  $(a, c) \in S \circ R$ , donde  $c \in \text{Im}(S)$  e  $\text{Im}(S \circ R) \subseteq \text{Im}(S)$ . Com isso,  $\text{Im}(S) = \text{Im}(S \circ R)$ . ■

### 3.2.3 Relações de Ordem

**Definição 3.44.** Seja  $R$  uma relação em  $X$ .

- (a) Dizemos que  $R$  é *reflexiva* se

$$\forall x(x \in X \rightarrow (x, x) \in R).$$

- (b) Dizemos que  $R$  é *irreflexiva* se

$$\forall x(x \in X \rightarrow (x, x) \notin R).$$

- (c) Dizemos que  $R$  é *simétrica* se

$$\forall x \forall y(x, y \in X \rightarrow (xRy \rightarrow yRx)).$$

(d) Dizemos que  $R$  é *antissimétrica* se

$$\forall x \forall y (x, y \in X \rightarrow (xRy \wedge yRx \rightarrow x = y)).$$

(e) Dizemos que  $R$  é *transitiva* se

$$\forall x \forall y \forall z (x, y, z \in X \rightarrow (xRy \wedge yRz \rightarrow xRz)).$$

**Definição 3.45** (Ordem parcial).

(a) Uma *relação de ordem parcial* em  $X$  é uma relação  $\leq \subseteq X \times X$  que tem as seguintes propriedades.

- i. Reflexividade:  $\forall x (x \in X \rightarrow x \leq x)$ ;
- ii. Antissimetria:  $\forall x \forall y (x, y \in X \rightarrow (x \leq y \wedge y \leq x \rightarrow x = y))$ ;
- iii. Transitividade:  $\forall x \forall y \forall z (x, y, z \in X \rightarrow (x \leq y \wedge y \leq z \rightarrow x \leq z))$ .

Dizemos que  $X$  é o *domínio* de  $\leq$ .

(b) Um *conjunto parcialmente ordenado* é um par  $(X, \leq)$  onde  $\leq \subseteq X \times X$  é uma relação de ordem parcial.

**Notação 3.46.** Sendo  $\leq$  uma ordem parcial, abreviaremos  $y \leq x$  por  $x \geq y$ ,  $x \leq y$  e  $x \neq y$  por  $x < y$  e  $x < y$  por  $y > x$ . Quando não houver perigo de confusão, podemos escrever somente *ordem* em vez de ordem parcial.

**Exemplo 3.47.** A relação de inclusão  $\subseteq$  é uma relação de ordem parcial (3.4).

**Definição 3.48.** Dois conjuntos parcialmente ordenados  $(X_1, \leq_1)$  e  $(X_2, \leq_2)$  são *ordem-isomorfos* se existe uma bijeção  $f : X_1 \rightarrow X_2$  tal que

$$\forall x \forall y (x, y \in X_1 \rightarrow (x \leq_1 y \leftrightarrow f(x) \leq_2 f(y))).$$

Dizemos que a função  $f$  é um *isomorfismo de ordens parciais*.

**Teorema 3.49.** Se  $(X, \leq)$  é um conjunto ordenado, então existe um conjunto ordenado  $(Y, \preceq)$  ordem-isomorfo a  $(X, \leq)$  tal que

$$\preceq = \{(x, y) \in Y \times Y : x \subseteq y\}.$$

**Prova.** Definindo  $f : X \rightarrow \mathcal{P}(X)$  por  $f(x) := \{y \in X : y \leq x\}$ , temos que  $f$  é bijetiva em relação a  $Y := \text{Im}(f)$ . De fato, se  $f(x) = f(y)$ , então  $x \in f(y)$  e  $y \in f(x)$  já que  $x \in f(x)$  e  $y \in f(y)$ ; daí, pela definição de  $f$ , vem  $x \leq y$  e  $y \leq x$ , de modo que  $x = y$  e  $f$  é injetiva. Provemos então que  $x \leq y$  se, e somente se,  $f(x) \subseteq f(y)$ , para quaisquer  $x, y \in X$ . Se  $z \in f(x)$ , então  $z \leq x$ , e se  $x \leq y$ , então  $z \leq y$ , de modo que  $z \in f(y)$  e  $f(x) \subseteq f(y)$ . Agora, se  $x \in f(x) \subseteq f(y)$ , então  $x \in f(y)$ , donde  $x \leq y$ . Com isso,  $(X, \leq)$  é ordem-isomorfo a  $(Y, \subseteq)$ , como havíamos afirmado. ■

**Definição 3.50.** Sejam  $(X, \leq)$  um conjunto parcialmente ordenado e  $S$  um subconjunto não vazio de  $X$ .

(a) Dizemos que  $M \in X$  é

i. uma *cota superior* de  $S$  se

$$\forall x(x \in S \rightarrow x \leq M).$$

Nesse caso, dizemos que  $S$  é *limitado superiormente* em  $X$ .

ii. o *elemento máximo* de  $S$  se  $M$  é uma cota superior de  $S$  e  $M \in S$ . Isso é denotado por  $\max S := M$ .

iii. o *supremo* de  $S$  se

$$\forall x(x \in S \rightarrow x \leq M) \wedge \forall y(y \in X \wedge \forall x(x \in S \rightarrow x \leq y) \rightarrow M \leq y),$$

isto é, se  $M$  é a menor cota superior de  $S$ . Isso é denotado por  $\sup S := M$ .

(b) Dizemos que  $m \in X$  é

i. uma *cota inferior* de  $S$  se

$$\forall x(x \in S \rightarrow m \leq x).$$

Nesse caso, dizemos que  $S$  é *limitado inferiormente* em  $X$ .

ii. o *elemento mínimo* de  $S$  se  $m$  é uma cota inferior de  $S$  e  $m \in S$ . Isso é denotado por  $\min S := m$ .

iii. o *ínfimo* de  $S$  se

$$\forall x(x \in S \rightarrow m \leq x) \wedge \forall y(y \in X \wedge \forall x(x \in S \rightarrow m \leq y) \rightarrow y \leq m),$$

isto é, se  $m$  é a maior cota inferior de  $S$ . Isso é denotado por  $\inf S := m$ .

**Observação 3.51.** É fácil ver que o máximo de  $S$ , quando existe, é único. De fato, se  $x, y \in S$  são máximos de  $S$ , então  $x \leq y$  e  $y \leq x$ , de modo que  $x = y$ . Essa unicidade também vale para o mínimo, o ínfimo e o supremo de  $S$ , quando existem. Isso justifica o uso do artigo “o” (em o máximo, em vez de *um* máximo, por exemplo) e nos permite denotar esses elementos por  $\max S$ ,  $\min S$ ,  $\inf S$  e  $\sup S$ , respectivamente.

**Definição 3.52.** Seja  $(X, \leq)$  um conjunto parcialmente ordenado.

(a) Dizemos que  $\leq$  é uma relação de ordem *total*<sup>2</sup>, e que o par  $(X, \leq)$  é um *conjunto totalmente ordenado*, se

$$\forall x \forall y(x, y \in X \rightarrow (x \leq y \vee y \leq x)).$$

<sup>2</sup>O termo *ordem linear* também costuma ser usado. Nesse caso, dizemos que o par  $(X, \leq)$  é um *conjunto linearmete ordenado*.

- (b) Dizemos que  $\leq$  é uma *boa ordem* em  $X$ , e que o par  $(X, \leq)$  é um *conjunto bem-ordenado*, se todo subconjunto não vazio de  $X$  possui um elemento mínimo.
- (c) Dizemos que  $\leq$  é um *reticulado* se para quaisquer  $x, y \in X$ , o conjunto  $\{x, y\}$  possui supremo e ínfimo.
- (d) Dizemos que  $\leq$  é uma *árvore* se, para todo  $x \in X$ , o conjunto  $S = \{y \in X : y \leq x\}$  é tal que  $(S, \leq \cap S^2)$  é um conjunto bem-ordenado.

**Proposição 3.53.**

- (a) Toda boa ordem é uma ordem total.
- (b) Toda boa ordem é uma árvore.
- (c) Toda ordem total é um reticulado.

**Prova.** ■

**Proposição 3.54.** Se  $(X, \leq)$  é parcialmente ordenado e  $Y \subseteq X$ , então  $(Y, \leq \cap Y^2)$  é parcialmente ordenado.

**Definição 3.55.** ■

**Definição 3.56.** Sejam  $(X, \leq)$  parcialmente ordenado e  $Y \subseteq X$ .

- (a) Dizemos que  $\leq \cap Y^2$  é uma *subordem* de  $\leq$ .
- (b) Dizemos que  $(Y, \leq \cap Y^2)$  é um *subconjunto parcialmente ordenado* de  $(X, \leq)$ . Isso é denotado por  $(Y, \leq)$ .

**Proposição 3.57.** Sejam  $(X, \leq)$  parcialmente ordenado e  $Y \subseteq X$ .

- (a) Se  $\leq$  é uma ordem total, então  $\leq \cap Y^2$  é uma ordem total.
- (b) Se  $\leq$  é uma boa ordem, então  $\leq \cap Y^2$  é uma boa ordem.
- (c) Se  $\leq$  é uma árvore, então  $\leq \cap Y^2$  é uma árvore.

**Prova.**

- (a)

### 3.2.4 Relações de Equivalência

**Definição 3.58.** (Relações de equivalência)

- (a) Uma *relação de equivalência* em  $X$  é uma relação  $\sim \subseteq X \times X$  que tem as seguintes propriedades.

- i. Reflexividade:  $\forall x(x \in X \rightarrow x \sim x)$ ;
- ii. Simetria:  $\forall x \forall y(x, y \in X \rightarrow (x \sim y \rightarrow y \sim x))$ ;
- iii. Transitividade:  $\forall x \forall y \forall z(x, y, z \in X \rightarrow (x \sim y \wedge y \sim z \rightarrow x \sim z))$ .

(b) A classe de equivalência de  $a \in X$  por  $\sim$  é definida como

$$[a]_{\sim} := \{x \in X : x \sim a\}.$$

(c) O conjunto das classes de equivalência de  $\sim$  é definido como

$$X/\sim := \{Y \in \mathcal{P}(X) : \exists x \forall y(y \in Y \leftrightarrow x \sim y)\} = \{[x]_{\sim} : x \in X\}.$$

**Proposição 3.59.** Seja  $\sim$  uma relação de equivalência num conjunto  $X$ . As seguintes afirmações são equivalentes.

- (a)  $a \sim b$ .
- (b)  $a \in [b]$ .
- (c)  $b \in [a]$ .
- (d)  $[a] = [b]$ .

**Prova.**

- (a)  $\Rightarrow$  (b): Por definição,  $[b] = \{x \in X : x \sim b\}$ , e como  $a \sim b$ , segue  $a \in [b]$ . ■
- (b)  $\Rightarrow$  (c): Se  $a \in [b]$ , então  $a \sim b$ , isto é,  $b \in [a]$ . ■
- (c)  $\Rightarrow$  (d): Se  $b \in [a]$ , então  $b \sim a$ . Se  $x \in [a]$ , então  $x \sim a$ , de modo que  $x \sim b$ , isto é,  $x \in [b]$ . Com isso,  $[a] \subseteq [b]$ . Analogamente temos  $[b] \subseteq [a]$ , de modo que  $[a] = [b]$ . ■
- (d)  $\Rightarrow$  (a): Se  $a \in [a] = [b]$ , então  $a \sim b$ . ■

**Definição 3.60.** Uma *partição* de um conjunto  $X \neq \emptyset$  é um subconjunto  $\mathcal{P} \subseteq \mathcal{P}(X)$  que tem as seguintes propriedades.

- i.  $\emptyset \notin \mathcal{P}$ ;
- ii.  $\bigcup \mathcal{P} = X$ ;
- iii.  $A \cap B = \emptyset$  para quaisquer  $A, B \in \mathcal{P}$  tais que  $A \neq B$ .

**Teorema 3.61.** Se  $\sim$  é uma relação de equivalência num conjunto  $X$ , então  $X/\sim$  é uma partição de  $X$ , isto é, valem as seguintes afirmações.

- (a)  $\emptyset \notin X/\sim$ .
- (b)  $\bigcup X/\sim = X$ .
- (c)  $\forall Y \forall Z((Y, Z \in X/\sim) \rightarrow (Y = Z \vee Y \cap Z = \emptyset))$ .

**Prova.**

- (a) Se  $\emptyset \in X/\sim$ , então existiria  $x \in X$  tal que  $\emptyset = [x]$ , mas  $x \in [x]$ , uma contradição. ■
- (b) Se  $y \in \bigcup X/\sim$ , então existe  $Y \in X/\sim$  tal que  $y \in Y$ . Como  $Y \in X/\sim$ , existe  $x \in X$  tal que  $Y = [x]$ . Como  $[x] \subseteq X$ , vem  $y \in X$ , de modo que  $\bigcup X/\sim \subseteq X$ . Agora, se  $x \in X$ , então  $x \sim x$  e  $x \in [x]$ , e como  $[x] \in X/\sim$ , vem  $x \in \bigcup X/\sim$ , de modo que  $X \subseteq \bigcup X/\sim$ . Logo  $\bigcup X/\sim = X$ . ■
- (c) Se  $Y \cap Z = \emptyset$ , nada há de ser provado. Se  $Y \cap Z \neq \emptyset$ , então existe  $x \in X$  tal que  $x \in Y \cap Z$ . Sendo  $y_0, z_0 \in X$  tais que  $Y = [y_0]$  e  $Z = [z_0]$ , temos  $x \sim y_0$  e  $x \sim z_0$ , de modo que  $[y_0] = [z_0]$ , isto é,  $Y = Z$ . ■

**Teorema 3.62.** Se  $\mathcal{P}$  é uma partição de um conjunto  $X \neq \emptyset$ , então existe uma relação de equivalência  $R$  em  $X$  tal que  $X/R = \mathcal{P}$ .

**Prova.** Pois tome  $R := \{(x, y) \in X \times X : \exists A(A \in \mathcal{P} \wedge x, y \in A)\}$ . ■

### 3.2.5 Funções

**Definição 3.63** (Função).

- (a) Uma relação  $f$  é uma *função* se  $(a, b) \in f$  e  $(a, c) \in f$  implicam  $b = c$ . A *imagem* de  $a \in \text{Dom}(f)$  por  $f$  é denotada por  $f(a)$ .
- (b) Uma *função parcial de  $A$  em  $B$*  é uma função  $f$  tal que  $\text{Dom}(f) \subseteq A$  e  $\text{Im}(f) \subseteq B$ .
- (c) Uma *função total de  $A$  em  $B$*  é uma função  $f$  tal que  $\text{Dom}(f) = A$  e  $\text{Im}(f) \subseteq B$ . Isso é denotado por  $f : A \rightarrow B$ . O conjunto de todas as funções de  $A$  em  $B$  é denotado por  $B^A$ , isto é,

$$B^A := \{f \in \mathcal{P}(A \times B) : \forall a \forall b \forall c ((a, b) \in f \wedge (a, c) \in f \rightarrow b = c) \\ \wedge \forall x(x \in A \rightarrow \exists y((x, y) \in f))\}.$$

**Observação 3.64.** Escrevemos apenas “função de  $A$  em  $B$ ”, omitindo o “total”.

**Definição 3.65.** A *função identidade* de um conjunto  $A$  é a função  $\text{Id}_A : A \rightarrow A$  definida por  $\text{Id}_A(x) = x$  para todo  $x \in A$ .

**Proposição 3.66.** Se  $f : A \rightarrow B$  é uma função, então  $\text{Id}_B \circ f = f$  e  $f \circ \text{Id}_A = f$ .

**Prova.** Teste só para ver se está funcionando. ■

**Proposição 3.67.** Sejam  $f$  e  $g$  funções e  $X$  um conjunto.

- (a)  $f|_X$  é uma função e seu domínio é  $\text{Dom}(f) \cap X$ .
- (b)  $g \circ f$  é uma função.

**Prova.**

- (a) Por definição,  $f|_X = \{(a, b) \in f : a \in X\}$ , isto é,  $f|_X$  é um conjunto de pares ordenados e, portanto, uma relação. Se  $(a, b) \in f|_X$  e  $(a, c) \in f|_X$ , então, pela definição de  $f|_X$ ,  $(a, b) \in f$ ,  $(a, c) \in f$  e  $a \in X$ ; como  $f$  é função,  $b = c$ , de modo que  $f|_X$  é também uma função. Provemos, por fim, que  $\text{Dom}(f|_X) = \text{Dom}(f) \cap X$ . Se  $a \in \text{Dom}(f|_X)$ , então existe  $b \in \text{Im}(f|_X)$  tal que  $(a, b) \in f|_X$ ; pela definição de  $f|_X$ , vem  $(a, b) \in f$  e  $a \in X$ , e de  $(a, b) \in f$  vem  $a \in \text{Dom}(f)$ . Com isso,  $a \in \text{Dom}(f) \cap X$ , de modo que  $\text{Dom}(f|_X) \subseteq \text{Dom}(f) \cap X$ . Por outro lado, se  $a \in \text{Dom}(f) \cap X$ , então de  $a \in \text{Dom}(f)$  segue que existe  $b \in \text{Im}(f)$  tal que  $(a, b) \in f$ , e como  $a \in X$ , vem  $(a, b) \in f|_X$ , de modo que  $\text{Dom}(f) \cap X \subseteq \text{Dom}(f|_X)$ . Logo  $\text{Dom}(f|_X) = \text{Dom}(f) \cap X$ . Em particular, temos  $f|_X = f|_{\text{Dom}(f) \cap X}$ . ■
- (b) Se  $(a, x) \in g \circ f$  e  $(a, y) \in g \circ f$ , então, por definição, existe  $b \in \text{Im}(f) \cap \text{Dom}(g)$  tal que  $(a, b) \in f$  e  $(b, x) \in g$  e existe  $c \in \text{Im}(f) \cap \text{Dom}(g)$  tal que  $(a, c) \in f$  e  $(c, y) \in g$ . Como  $f$  é função, vem  $b = c$ ; daí, vem  $(b, x) \in g$  e  $(b, y) \in g$ , e como  $g$  é função, vem  $x = y$ . ■

### 3.2.6 Bijeções e Funções Inversas

#### Injeções

**Definição 3.68.** Uma função  $f$  é *injetiva* se

$$\forall x \forall y (x, y \in \text{Dom}(f) \rightarrow (x \neq y \rightarrow f(x) \neq f(y))).$$

**Proposição 3.69.** Sejam  $f$  e  $g$  funções.

- (a) Se  $f$  e  $g$  são injetivas, então  $g \circ f$  é injetiva.
- (b) Se  $g \circ f$  é injetiva e  $\text{Im}(f) \subseteq \text{Dom}(g)$ , então  $f$  é injetiva.

**Prova.**

- (a) Sejam  $x, y \in \text{Dom}(g \circ f)$ . Se  $g(f(x)) = g(f(y))$ , então  $f(x) = f(y)$  pela injetividade de  $g$ . Se  $f(x) = f(y)$ , então  $x = y$  pela injetividade de  $f$ . Logo  $g \circ f$  é injetiva. ■
- (b) Sejam  $x, y \in \text{Dom}(f)$  tais que  $f(x) = f(y)$ . Se  $\text{Im}(f) \subseteq \text{Dom}(g)$ , então  $f(x), f(y) \in \text{Dom}(g)$ , e como  $f(x) = f(y)$ , temos  $g(f(x)) = g(f(y))$ . Daí,

como  $\text{Dom}(f) = \text{Dom}(g \circ f)$  (proposição (3.43)) e  $g \circ f$  é injetiva, vem  $x = y$ , de modo que  $f$  é injetiva. ■

**Teorema 3.70.** Seja  $f$  uma função.

- (a) Se a relação  $f^{-1}$  é uma função, então  $f^{-1}$  é injetiva.
- (b) A relação  $f^{-1}$  é uma função se, e somente se,
  - i.  $f$  é injetiva.
  - ii.  $f^{-1} \circ f = \text{Id}_{\text{Dom}(f)}$ .

**Prova.**

- (a) Se  $(y, x) \in f^{-1}$  e  $(z, x) \in f^{-1}$ , então  $(x, y) \in f$  e  $(x, z) \in f$ , e como  $f$  é função vem  $y = z$ , de modo que  $f^{-1}$  é uma função injetiva. ■
- (b) A equivalência mais importante é com  $f$  ser injetiva.
  - i. Se  $f^{-1}$  é uma função, então  $(x, y) \in f^{-1}$  e  $(x, z) \in f^{-1}$  implicam  $y = z$ . Daí, como  $(y, x) \in f$  e  $(z, x) \in f$ , sendo  $y = z$  segue que  $f$  é injetiva. Agora, se  $f$  é injetiva, então  $(y, x) \in f$  e  $(z, x) \in f$  implicam  $y = z$ , e como  $(x, y) \in f^{-1}$  e  $(x, z) \in f^{-1}$ , segue que  $f^{-1}$  é uma função.

Provemos que  $f$  é injetiva se, e somente se,  $f^{-1} \circ f = \text{Id}_{\text{Dom}(f)}$ .

- ii. ( $\Rightarrow$ ) Se  $(x, z) \in f^{-1} \circ f$ , então existe  $y \in \text{Im}(f) \cap \text{Dom}(f^{-1})$  tal que  $(x, y) \in f$  e  $(y, z) \in f^{-1}$ . Com isso,  $(z, y) \in f$ , e como  $f$  é injetiva vem  $z = x$ , de modo que  $(x, x) \in \text{Id}_{\text{Dom}(f)}$ , isto é,  $f^{-1} \circ f \subseteq \text{Id}_{\text{Dom}(f)}$ . Agora, se  $(x, x) \in \text{Id}_{\text{Dom}(f)}$ , então existe  $y \in \text{Im}(f)$  tal que  $(x, y) \in f$ , isto é,  $(y, x) \in f^{-1}$ . Com isso,  $(x, x) \in f^{-1} \circ f$ , de modo que  $\text{Id}_{\text{Dom}(f)} \subseteq f^{-1} \circ f$ . Com isso, vem  $f^{-1} \circ f = \text{Id}_{\text{Dom}(f)}$ . ( $\Leftarrow$ ) Sendo  $(x, y) \in f$  e  $(z, y) \in f$ , temos  $(y, x) \in f^{-1}$ , de modo que  $(z, x) \in f^{-1} \circ f$ , e como  $f^{-1} \circ f = \text{Id}_{\text{Dom}(f)}$ , vem  $x = z$ , o que prova a injetividade de  $f$ .

Com isso, todas as equivalências foram provadas. ■

**Definição 3.71.** Uma função  $f$  é *invertível à esquerda* se existe uma função  $g$  tal que  $g \circ f = \text{Id}_{\text{Dom}(f)}$ . Dizemos que  $g$  é uma *inversa à esquerda* de  $f$ .

**Teorema 3.72.** Uma função  $f$  é invertível à esquerda se, e somente se,  $f$  é injetiva.

**Prova.** Se  $f$  é injetiva, então pelo teorema (3.70)  $f^{-1}$  é uma função e  $f^{-1} \circ f = \text{Id}_{\text{Dom}(f)}$ , de modo que  $f$  é invertível à esquerda. Agora, sendo  $(x, y) \in f$  e  $(z, y) \in f$ , provemos que  $x = z$ . Como  $f$  é invertível à esquerda, existe uma função  $g$  tal que  $g \circ f = \text{Id}_{\text{Dom}(f)}$ . Como  $(x, x) \in g \circ f$ , existe  $w \in \text{Im}(f) \cap \text{Dom}(g)$  tal que  $(x, w) \in f$  e  $(w, x) \in g$ . Como  $f$  é uma função, vem  $w = y$ , de modo que

$(y, x) \in g$ . Analogamente temos  $(y, z) \in g$ , e como  $g$  é uma função vem  $x = z$ , de modo que  $f$  é injetiva. ■

### Sobrejeções

**Definição 3.73.** Uma função  $f : A \rightarrow B$  é *sobrejetiva* se  $\text{Im}(f) = B$ .

**Proposição 3.74.** Uma função  $f : A \rightarrow B$  é sobrejetiva em  $B$  se, e somente se, para todo  $y \in B$  existe  $x \in A$  tal que  $(x, y) \in f$ .

**Prova.** Segue da proposição (3.42). ■

**Lema 3.75.** Sejam  $f : A \rightarrow B$  e  $g : C \rightarrow D$  funções.

- (a)  $\text{Dom}(g \circ f) = \{x \in A : f(x) \in C\}$ .
- (b)  $\text{Dom}(g \circ f) = A$  se, e somente se,  $f(A) \subseteq C$ .

**Prova.**

- (a) Pela proposição (3.42),  $\text{Dom}(g \circ f) = \{x \in A : \exists y(y \in D \wedge (x, y) \in g \circ f)\}$ .
  - i. Se  $x \in \text{Dom}(g \circ f)$ , então existe  $y \in D$  tal que  $(x, y) \in g \circ f$ . Logo existe  $z \in \text{Im}(f) \cap \text{Dom}(g) \subseteq B \cap C$  tal que  $(x, z) \in f$  e  $(z, y) \in g$ , isto é,  $z = f(x)$  e  $y = g(z)$ . Com isso,  $x \in A$  e  $f(x) \in C$ , de modo que  $x \in \{x \in A : f(x) \in C\}$ , isto é,  $\text{Dom}(g \circ f) \subseteq \{x \in A : f(x) \in C\}$ .
  - ii. Se  $x \in \{x \in A : f(x) \in C\}$ , então  $x \in A$  e  $f(x) \in C$ , isto é, existe (um único)  $z \in C$  tal que  $(x, z) \in f$ . Como  $z \in C$ , existe  $y \in \text{Im } g \subseteq D$  tal que  $(z, y) \in g$ . Com isso,  $x \in A$  e existe  $y \in D$  tal que  $(x, y) \in g \circ f$ , de modo que  $x \in \text{Dom}(g \circ f)$ , isto é,  $\{x \in A : f(x) \in C\} \subseteq \text{Dom}(g \circ f)$ .

Logo  $\text{Dom}(g \circ f) = \{x \in A : f(x) \in C\}$ . ■

- (b) A volta ( $\Leftarrow$ ) já foi provada (proposição (3.43)). Agora, se  $y \in f(A)$ , então existe  $x \in A$  tal que  $y = f(x)$ , e como  $A = \text{Dom}(g \circ f)$ , vem  $f(x) \in C$ , isto é,  $y \in C$ . Logo  $f(A) \subseteq C$ . ■

**Proposição 3.76.** Sejam  $f : A \rightarrow B$  e  $g : C \rightarrow D$  funções.

- (a) Se  $f$  e  $g$  são sobrejetivas e  $B = C$ , então  $g \circ f$  é sobrejetiva.
- (b) Se  $g \circ f$  é sobrejetiva e  $f(A) \subseteq C$ , então  $g$  é sobrejetiva.

**Prova.**

- (a) Se  $B = C$ , então  $\text{Dom}(g \circ f) = A$  pelo lema (3.75). Se  $g$  é sobrejetiva, então para todo  $z \in D$  existe  $y \in C = B$  tal que  $(y, z) \in g$ . Se  $f$  é sobrejetiva,

então para esse  $y \in B$  existe  $x \in A$  tal que  $(x, y) \in f$ . Com isso, para todo  $z \in D$  existe  $x \in A$  tal que  $(x, z) \in g \circ f$ , o que prova a sobrejetividade de  $g \circ f$ . ■

- (b) Se  $f(A) \subseteq C$ , então  $\text{Dom}(g \circ f) = A$  pelo lema (3.75). Se  $g \circ f$  é sobrejetiva, então para todo  $z \in D$  existe  $x \in A$  tal que  $(x, z) \in g \circ f$ . Com isso, existe  $y \in f(A) \cap C = C$  tal que  $(x, y) \in f$  e  $(y, z) \in g$ . o que prova a sobrejetividade de  $g$ . ■

**Lema 3.77.** Para qualquer função  $f$ , tem-se  $f \circ f^{-1} = \text{Id}_{\text{Im}(f)}$ .

**Prova.** Provemos que  $f \circ f^{-1} \subseteq \text{Id}_{\text{Im}(f)}$  e  $f \circ f^{-1} \supseteq \text{Id}_{\text{Im}(f)}$ . Se  $(y, z) \in f \circ f^{-1}$ , então existe  $x \in \text{Dom}(f) \cap \text{Im}(f^{-1})$  tal que  $(y, x) \in f^{-1}$  e  $(x, z) \in f$ . Daí,  $(x, y) \in f$ , e como  $f$  é uma função, vem  $y = z$ . Logo  $f \circ f^{-1} \subseteq \text{Id}_{\text{Im}(f)}$ . Por outro lado, se  $(y, y) \in \text{Id}_{\text{Im}(f)}$ , então existe  $x \in \text{Dom}(f)$  tal que  $(x, y) \in f$ . Logo  $(y, x) \in f^{-1}$ , de modo que  $(y, y) \in f \circ f^{-1}$ , isto é,  $f \circ f^{-1} \supseteq \text{Id}_{\text{Im}(f)}$ . Com isso, vem  $f \circ f^{-1} = \text{Id}_{\text{Im}(f)}$ , como queríamos. ■

**Teorema 3.78.** Uma função  $f : A \rightarrow B$  é sobrejetiva se, e somente se,  $f \circ f^{-1} = \text{Id}_B$ .

**Prova.** Se  $f$  é sobrejetiva em  $B$ , então  $\text{Im}(f) = B$ , de modo que  $f \circ f^{-1} = \text{Id}_B$ . Por outro lado, se  $f \circ f^{-1} = \text{Id}_B$ , então  $f$  é sobrejetiva em  $B$  porque, como também  $f \circ f^{-1} = \text{Id}_{\text{Im}(f)}$ , vem  $\text{Im}(f) = B$ . ■

**Definição 3.79.** Uma função  $f : A \rightarrow B$  é *invertível à direita* se existe uma função  $g : B \rightarrow A$  tal que  $f \circ g = \text{Id}_B$ . Dizemos que  $g$  é uma *inversa à direita* de  $f$ .

**Teorema 3.80.** Uma função  $f : A \rightarrow B$  é invertível à direita se, e somente se,  $f$  é sobrejetiva em  $B$ .

**Observação 3.81.** A prova da volta ( $\Leftarrow$ ) deste teorema depende do axioma da escolha. Mais precisamente, de um enunciado equivalente ao axioma da escolha: para toda relação  $R$  existe uma função  $f \subseteq R$  tal que  $\text{Dom}(f) = \text{Dom}(R)$ . Ainda assim, enunciamos este resultado aqui por uma questão de organização didática.

**Prova.** ■

### Bijeções e Funções Inversas

**Definição 3.82.** Uma função  $f : A \rightarrow B$  é *bijetiva em relação a B* se é injetiva e sobrejetiva em  $B$ .

**Proposição 3.83.** Uma função  $f : A \rightarrow B$  é bijetiva em  $B$  se, e somente se, para

todo  $y \in B$  existe um único  $x \in A$  tal que  $(x, y) \in f$ .

**Prova.** Segue imediatamente da definição. ■

**Proposição 3.84.** Se  $f : A \rightarrow B$  e  $g : B \rightarrow C$  são funções bijetivas, então a função  $g \circ f : A \rightarrow C$  é uma função bijetiva.

**Prova.** Segue como corolário imediato das proposições (3.69) e (3.76). ■

**Teorema 3.85.** Seja  $f : A \rightarrow B$  uma função.

- (a) Se a relação  $f^{-1}$  é uma função de  $B$  em  $A$ , então  $f^{-1}$  é bijetiva.
- (b) A relação  $f^{-1}$  é uma função de  $B$  em  $A$  se, e somente se,
  - i.  $f$  é bijetiva em  $B$ .
  - ii.  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ .

**Prova.**

- (a) Como  $f$  é função, para todo  $x \in A$  existe um único  $y \in B$  tal que  $(x, y) \in f$ , isto é,  $(y, x) \in f^{-1}$ . Daí, pela proposição (3.83),  $f^{-1}$  é bijetiva em  $A$ . ■
- (b) A equivalência que mais importa é com  $f$  ser bijetiva em  $B$ .
  - i. Se  $f^{-1} \subseteq B \times A$  é uma função tal que  $\text{Dom}(f^{-1}) = B$ , então para todo  $y \in B$  existe um único  $x \in A$  tal que  $(y, x) \in f^{-1}$ , isto é,  $(x, y) \in f$ . Daí, pela proposição (3.83), temos que  $f$  é bijetiva. Agora, pela mesma proposição, se  $f$  é bijetiva, então para todo  $y \in B$  existe um único  $x \in A$  tal que  $(x, y) \in f$ , isto é,  $(y, x) \in f^{-1}$ . Daí, pela definição de função,  $f^{-1}$  é uma função de  $B$  em  $A$ . ■

Provemos que  $f$  é bijetiva em  $B$  se, e somente se,  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ .

- ii. Se  $f$  é bijetiva em  $B$ , então  $f$  é injetiva e sobrejetiva, de modo que, pelos teoremas (3.70) e (3.78), vem  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ , respectivamente. Agora, se  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ , então pelos mesmos teoremas  $f$  é injetiva e sobrejetiva em  $B$ , isto é,  $f$  é bijetiva em  $B$ . ■

Com isso, todas as equivalências foram provadas. ■

**Definição 3.86.** Uma função  $f : A \rightarrow B$  é *invertível* se existe uma função  $g : B \rightarrow A$  tal que  $g \circ f = \text{Id}_A$  e  $f \circ g = \text{Id}_B$ . Dizemos que  $g$  é a *inversa* de  $f$ .

**Proposição 3.87.** A função inversa de uma função invertível é única.<sup>3</sup>

<sup>3</sup>Note que é esta proposição que nos permite dizer “a função inversa” em vez de “uma função inversa”.

**Prova.** Seja  $f : A \rightarrow B$  uma função invertível. Sejam  $g_1, g_2 : B \rightarrow A$  funções inversas de  $f$ . Provemos que  $g_1 = g_2$ . De fato,

$$g_1 = g_1 \circ \text{Id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \text{Id}_A \circ g_2 = g_2.$$

Logo, a função inversa da função  $f : A \rightarrow B$ , quando existe, é única. ■

**Teorema 3.88.** Seja  $f : A \rightarrow B$  uma função.

- (a)  $f$  é invertível se, e somente se,  $f$  é bijetiva.
- (b) Se  $f$  é invertível, então a função inversa de  $f$  é a relação inversa  $f^{-1}$ .

**Prova.**

- (a) Se  $f$  é invertível, então existe uma função  $g : B \rightarrow A$  tal que  $g \circ f = \text{Id}_A$  e  $f \circ g = \text{Id}_B$ , de modo que  $f$  é invertível à esquerda e à direita, isto é,  $f$  é injetiva (teorema (3.72)) e sobrejetiva em  $B$  (teorema (3.80)), isto é,  $f$  é bijetiva em  $B$ . Por outro lado, se  $f$  é bijetiva em  $B$ , então pelo teorema (3.85) sua relação inversa  $f^{-1} \subseteq B \times A$  é uma função de  $B$  em  $A$  e, mais ainda, satisfaz  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ , de modo que  $f$  é invertível. ■
- (b) Segue imediatamente do primeiro item. ■

**Corolário 3.89.** Uma função é invertível se, e somente se, é invertível à esquerda e à direita.

**Prova.** A ida ( $\Rightarrow$ ) decorre imediatamente das definições. Provemos então a volta ( $\Leftarrow$ ). Se  $f$  é invertível à esquerda e à direita, então pelos teoremas (3.72) e (3.80)  $f$  é bijetiva em  $B$ , de modo que, pelo teorema (3.88),  $f$  é invertível. ■

**Observação 3.90.** Vamos resumir o que está acontecendo. O resultado mais importante é a equivalência entre invertibilidade e bijetividade: por um lado, se  $f : A \rightarrow B$  é bijetiva, então a relação inversa  $f^{-1} \subseteq B \times A$  é uma função de  $B$  em  $A$  tal que  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ , o que prova que  $f$  é invertível. Por outro lado, se  $f$  é invertível, então existe  $f^{-1} : B \rightarrow A$  tal que  $f^{-1} \circ f = \text{Id}_A$  e  $f \circ f^{-1} = \text{Id}_B$ , o que prova que  $f$  é bijetiva.

### 3.3 O Axioma do Infinito e os Números Naturais

**Definição 3.91.** O *sucessor* de um conjunto  $x$  é definido como  $x^+ := x \cup \{x\}$ .

**Proposição 3.92.** Valem as seguintes afirmações sobre o sucessor.

- (a)  $\forall x \forall y ((y \in x^+) \leftrightarrow ((y \in x) \vee (y = x)))$

(b)  $\forall x(x \in x^+)$

(c)  $\forall x(x \subseteq x^+)$

**Prova.**

(a) Pela definição de sucessor,  $x^+ = x \cup \{x\}$ . Pela definição de união,  $y \in x \cup \{x\}$  se, e somente se,  $y \in x$  ou  $y \in \{x\}$ . Como  $y \in \{x\}$  equivale a  $y = x$ , temos que  $y \in x^+$  se, e somente se,  $y \in x$  ou  $y = x$ . ■

(b) Tomando  $y = x$  no item anterior, obtemos  $(x \in x^+) \leftrightarrow ((x \in x) \vee (x = x))$ . Como vale  $x = x$ , vale também a disjunção  $(x \in x) \vee (x = x)$ , de modo que  $x \in x^+$ . ■

(c) Se  $z \in x$ , então  $(z \in x) \vee (z = x)$ , de modo que  $z \in x^+$ . Com isso,  $\forall z(z \in x \rightarrow z \in x^+)$ , isto é,  $x \subseteq x^+$ . ■

**Definição 3.93.** Um conjunto  $x$  é *indutivo* se

$$(\emptyset \in x) \wedge \forall y((y \in x) \rightarrow (y^+ \in x)).$$

Isso é denotado por  $\text{Ind}(x)$ .

**Axioma 3.94** (Infinito). Existe um conjunto indutivo.

$$\boxed{\exists x((\emptyset \in x) \wedge \forall y((y \in x) \rightarrow (y^+ \in x)))}$$

**Teorema 3.95.** Seja  $I$  um conjunto indutivo. Defina

$$\omega(I) := \bigcap \{x \in \mathcal{P}(I) : \text{Ind}(x)\}.$$

(a) Para todo conjunto  $I$ , se  $I$  é indutivo, então  $\omega(I)$  é indutivo.

$$\forall I(\text{Ind}(I) \rightarrow \text{Ind}(\omega(I)))$$

(b) Para quaisquer conjuntos  $I$  e  $J$ , se  $I$  e  $J$  são indutivos, então  $\omega(I) = \omega(J)$ .

$$\forall I \forall J(\text{Ind}(I) \wedge \text{Ind}(J) \rightarrow \omega(I) = \omega(J))$$

**Prova.** Provemos primeiramente que  $\omega(I)$  está bem definido. Pelo axioma das partes, existe o conjunto  $\mathcal{P}(I)$ . Pelo axioma da separação com universo  $\mathcal{P}(I)$  e a fórmula  $(\emptyset \in x) \wedge \forall y((y \in x) \rightarrow (y^+ \in x))$  (que se abrevia por  $\text{Ind}(x)$ ), existe  $z(I) := \{x \in \mathcal{P}(I) : \text{Ind}(x)\}$ . Pelo teorema (3.22), como  $z(I) \neq \emptyset$  já que  $I \in z(I)$ , existe  $\omega(I) := \bigcap z(I)$ .

- (a) Provemos primeiramente que  $\emptyset \in \omega(I)$ . Pelo teorema (3.22),  $\omega(I) := \bigcap z(I)$  é o conjunto que satisfaz

$$\forall x \left( x \in \bigcap z(I) \leftrightarrow \forall y (y \in z(I) \rightarrow x \in y) \right).$$

Com isso,  $\emptyset \in \bigcap z(I) \leftrightarrow \forall y (y \in z(I) \rightarrow \emptyset \in y)$ . Como, por definição,

$$\forall y (y \in z(I) \leftrightarrow y \subseteq I \wedge \text{Ind}(y)),$$

temos  $\emptyset \in \bigcap z(I) \leftrightarrow \forall y (y \subseteq I \wedge \text{Ind}(y) \rightarrow \emptyset \in y)$ , o que sabemos ser verdade: se  $y \subseteq I$  é indutivo, então  $\emptyset \in y$ . Logo,  $\emptyset \in \bigcap z(I) = \omega(I)$ . Agora provemos que  $\forall x ((x \in \omega(I)) \rightarrow (x^+ \in \omega(I)))$ . Isso equivale a

$$\forall x (\forall y (y \in z(I) \rightarrow x \in y) \rightarrow \forall y (y \in z(I) \rightarrow x^+ \in y)),$$

o que equivale a

$$\forall x (\forall y (y \in z(I) \rightarrow (x \in y \rightarrow x^+ \in y))),$$

o que equivale a

$$\forall y (y \subseteq I \wedge \text{Ind}(y) \rightarrow \forall x (x \in y \rightarrow x^+ \in y)),$$

o que sabemos ser verdade: se  $y \subseteq I$  é indutivo, então  $\forall x (x \in y \rightarrow x^+ \in y)$ . Logo,  $\omega(I)$  é indutivo. ■

- (b) Provemos inicialmente que, para quaisquer  $I$  e  $J$  indutivos, tem-se  $\omega(I) \subseteq J$ . O mesmo argumento do item anterior mostra que  $I \cap J$  são indutivos, e como  $I \cap J \subseteq I$ , vem  $I \cap J \in z(I)$ . Com isso, como

$$\forall x \left( x \in \bigcap z(I) \leftrightarrow \forall w (w \in z(I) \rightarrow x \in w) \right),$$

particularmente para  $w = I \cap J$ , se  $x \in \bigcap z(I)$ , então  $x \in I \cap J$ , de modo que  $\bigcap z(I) \subseteq I \cap J \subseteq J$ , isto é,  $\omega(I) \subseteq J$ . Como isso, como  $\omega(I)$  e  $\omega(J)$  são indutivos, temos  $\omega(I) \subseteq \omega(J)$  e  $\omega(J) \subseteq \omega(I)$ , isto é,  $\omega(I) = \omega(J)$ . ■

**Observação 3.96.** O teorema (3.95) nos diz que  $\omega(I)$  é a interseção da família de todos os conjuntos indutivos e que o parâmetro  $I$  pode ser suprimido. A seguinte definição só é possível devido a esse teorema.

**Definição 3.97.** O conjunto dos números naturais é definido como a interseção de todos os conjuntos indutivos. Ele é denotado por  $\omega$ .

**Teorema 3.98 (Indução).** Se  $A \subseteq \omega$  é indutivo, então  $A = \omega$ .

**Prova.** Pelo teorema (3.95), se  $A$  é indutivo, então  $\omega \subseteq A$ . Daí, como  $A \subseteq \omega$ , vem  $A = \omega$ . ■

**Teorema 3.99** (Axiomas de Peano). O conjunto  $\omega$  dos números naturais satisfaz os axiomas de Peano, isto é, valem as seguintes afirmações.

- (a)  $\forall x \forall y (x, y \in \omega \rightarrow (\neg(x = y) \rightarrow \neg(x^+ = y^+)))$ .
- (b)  $\forall x (x \in \omega \rightarrow (\neg(x^+ = \emptyset)))$ .
- (c) Para toda fórmula  $P$ ,

$$P(\emptyset) \wedge \forall x (P(x) \rightarrow P(x^+)) \rightarrow \forall x (x \in \omega \rightarrow P(x)).$$

**Prova.** Ver [5], teorema 3.20, página 89. ■

**Definição 3.100.** Um conjunto  $A$  é *transitivo* se

$$\forall x \forall y (x \in y \wedge y \in A \rightarrow x \in A).$$

**Proposição 3.101.** Um conjunto  $A$  é transitivo se, e somente se,

- i.  $\forall a (a \in A \rightarrow a \subseteq A)$ .
- ii.  $\bigcup A \subseteq A$ .
- iii.  $\bigcup A^+ = A$ .
- iv.  $A \subseteq \mathcal{P}(A)$ .

**Prova.**

- (a) Por um lado ( $\Rightarrow$ ), se  $A$  é transitivo e  $a \in A$ , então para todo  $x \in a$  temos  $x \in A$ , de modo que  $a \subseteq A$ . Se fosse  $a = A$ , teríamos  $a \in a$  ou  $A \in A$ , o que contraria o corolário (3.34). Com isso,  $a \neq A$ , donde  $a \subsetneq A$ . Por outro lado ( $\Leftarrow$ ), se  $a \subsetneq A$  para todo  $a \in A$ , então  $a \subseteq A$ . Logo, se  $x \in y$  e  $y \in A$ , então  $y \subseteq A$ , de modo que  $x \in A$ . ■

**Teorema 3.102.**

- (a) Todo número natural é um conjunto transitivo.
- (b) O conjunto  $\omega$  é transitivo.

**Prova.**

- (a) A prova se dará por indução em  $n$ . O conjunto vazio  $\emptyset$  é trivialmente transitivo (por vacuidade). Agora, supondo que  $n \in \omega$  é transitivo, provemos que  $n^+ \in \omega$  também é transitivo. Se  $x \in n^+$ , então  $x \in n$  ou  $x = n$ .

- Se  $x \in n$ , então, dado  $y \in x$ , como  $n$  é transitivo, vem  $y \in n$ , e como  $n \subsetneq n^+$ , vem  $y \in n^+$ , de modo que  $n^+$  é transitivo.
- Se  $x = n$ , então, dado  $y \in x$ , temos  $y \in n$ , e como  $n \subsetneq n^+$ , vem  $y \in n^+$ , de modo que  $n^+$  é transitivo.

Com isso, todo número natural é transitivo. ■

- (b) Provemos que  $\forall n(n \in \omega \rightarrow n \subsetneq \omega)$  por indução. Trivialmente  $\emptyset \subsetneq \omega$ . Agora, se  $n \in \omega$ , então  $\{n\} \subsetneq \omega$ , e como  $n \subsetneq \omega$  (hipótese de indução), temos  $n \cup \{n\} \subseteq \omega$ , isto é,  $n^+ \subsetneq \omega$ , pois  $n^+ \neq \omega$ . ■

**Lema 3.103.** Para quaisquer  $m, n \in \omega$ , valem as seguintes afirmações.

- (a) Se  $m \in n$ , então  $m^+ \in n$  ou  $m^+ = n$ .  
 (b) Se  $m \in n$ , então  $m \subsetneq n$ .

**Prova.**

- (a) A prova se dará por indução em  $n$ . Se  $m \in \emptyset$ , então a conclusão segue trivialmente por vacuidade. Agora, supondo que  $m \in n$  implica  $m^+ \in n$  ou  $m^+ = n$ , provemos que  $m \in n^+$  implica  $m^+ \in n^+$  ou  $m^+ = n^+$ . Se  $m \in n^+$ , então  $m \in n$  ou  $m = n$ . Se  $m \in n$ , então  $m^+ \in n$  ou  $m^+ = n$  (hipótese de indução). Como  $n \subsetneq n^+$  e  $n \in n^+$ , vem  $m^+ \in n^+$ . Se  $m = n$ , então  $m^+ = n^+$ . ■
- (b) A prova se dará por indução em  $n$ . Se  $m \in \emptyset$ , então a conclusão segue trivialmente por vacuidade. Agora, supondo que  $m \in n$  implica  $m \subsetneq n$ , provemos que  $m \in n^+$  implica  $m \subsetneq n^+$ . Se  $m \in n^+$ , então  $m \in n$  ou  $m = n$ . Se  $m \in n$ , então  $m \subsetneq n$  (hipótese de indução), e como  $n \subsetneq n^+$ , vem  $m \subsetneq n^+$ . Se  $m = n$ , então  $m \subsetneq n^+$  pois  $n \subsetneq n^+$ . ■

**Teorema 3.104.** Para quaisquer  $m, n \in \omega$ , valem as seguintes afirmações.

- (a)  $m \in n$  se, e somente se,  $m^+ \in n^+$ .  
 (b) Ou  $m \in n$ , ou  $n \in m$ , ou  $m = n$ .

**Prova.**

- (a) Por um lado ( $\Rightarrow$ ), se  $m \in n$ , então  $m^+ \in n$  ou  $m^+ = n$ . Como  $n \subsetneq n^+$  e  $n \in n^+$ , em ambos os casos temos  $m^+ \in n^+$ . Por outro lado ( $\Leftarrow$ ), se  $m^+ \in n^+$ , então  $m^+ \in n$  ou  $m^+ = n$ . Se  $m^+ \in n$ , então  $m^+ \subsetneq n$ , e como  $m \in m^+$ , segue que  $m \in n$ . Se  $m^+ = n$ , como  $m \in m^+$ , temos imediatamente  $m \in n$ . ■
- (b) A prova se dará por indução em  $n$ . Se  $n = \emptyset$ , não pode ser  $m \in \emptyset$ . Provemos rapidamente que ou  $\emptyset \in m$  ou  $m = \emptyset$ .

- Se  $m = \emptyset$ , a afirmação é trivialmente verdadeira. Supondo que  $m = \emptyset$  ou  $\emptyset \in m$ , provemos que  $m^+ = \emptyset$  ou  $\emptyset \in m^+$ . Como  $m \in m^+$ , não pode ser  $m^+ = \emptyset$ . Se  $m = \emptyset$ , então  $m^+ = \{\emptyset\}$ , de modo que  $\emptyset \in m^+$ . Se  $\emptyset \in m$ , então  $\emptyset \in m^+$  pois  $m \subseteq m^+$ .

Com isso, o resultado vale para  $n = \emptyset$ . Agora, supondo que o resultado vale para  $n$ , provemos que ele também vale para  $n^+$ . Se  $m \in \omega$ , então, pela hipótese de indução,

- se  $m \in n$ , como  $n \subsetneq n^+$ , temos  $m \in n^+$ ;
- se  $m = n$ , como  $n \in n^+$ , temos  $m \in n^+$ ;
- se  $n \in m$ , então  $n^+ \in m$  ou  $n^+ = m$ .

Com isso, em qualquer caso, pelo menos uma das afirmações  $m \in n^+$ ,  $n^+ \in m$  ou  $m = n^+$  é verdadeira. A exclusividade é garantida pela proposição (3.33) e pelo corolário (3.34). ■

**Corolário 3.105.**

- (a) Para quaisquer  $m, n \in \omega$ , se  $m \subsetneq n$ , então  $m \in n$ .  
 (b)  $\bigcup \omega = \omega$ .

**Prova.**

- (a) Se  $m \subsetneq n$ , então  $m \neq n$ . Pelo teorema (3.104), ou  $m \in n$ , ou  $n \in m$ . Se fosse  $n \in m$ , teríamos  $n \in n$ , uma contradição. Logo, só pode ser  $m \in n$ . ■  
 (b) Se  $x \in \bigcup \omega$ , então existe  $y \in \omega$  tal que  $x \in y$ , e como  $y \subseteq \omega$ , vem  $x \in \omega$ . Com isso,  $\bigcup \omega \subseteq \omega$ . Agora, se  $x \in \omega$ , então existe  $x^+ \in \omega$  tal que  $x \in x^+$ , de modo que  $x \in \bigcup \omega$ . Com isso,  $\bigcup \omega \supseteq \omega$ . Logo,  $\bigcup \omega = \omega$ . ■

**Teorema 3.106.**  $(\omega, \subset)$  é bem ordenado.

**Prova.** Ver [5], teorema 4.26, página 111.

### 3.3.1 O Teorema da Recursão

Para definir funções de domínio  $\omega$  recursivamente, precisamos

1. estabelecer o valor da função em 0;
2. estabelecer uma “regra” para definir o valor da função em  $n^+$  uma vez que se conheça o seu valor em  $n$ .

**Teorema 3.107** (da recursão finita). Sejam  $X$  um conjunto,  $x_0 \in X$  e  $g : X \rightarrow X$ . Existe e é única a função  $f : \omega \rightarrow X$  tal que

- $f(0) = x_0$ ;
- $f(n^+) = g(f(n))$ , para todo  $n \in \omega$ .

**Prova.** A ideia é considerar todas as relações contidas em  $\omega \times X$  que cumprem as condições desejadas e provar que a interseção de todas elas resulta em uma única função de domínio  $\omega$ . Defina

$$\mathcal{C} := \{R \in \mathcal{P}(\omega \times X) : (0, x_0) \in R \wedge \forall n \forall y ((n, y) \in R \rightarrow (n^+, g(y)) \in R)\}.$$

Como  $\omega \times X \in \mathcal{C}$ , temos  $\mathcal{C} \neq \emptyset$ , de modo que, pelo teorema (3.22) podemos tomar  $f := \bigcap \mathcal{C}$ . Temos  $(0, x_0) \in f$  porque  $(0, x_0) \in R$  para toda  $R \in \mathcal{C}$ . Analogamente, se  $(n, y) \in f$ , então  $(n, y) \in R$  para toda  $R \in \mathcal{C}$ , de modo que  $(n^+, g(y)) \in R$  para toda  $R \in \mathcal{C}$ , provando que  $(n^+, g(y)) \in f$  e que  $f \in \mathcal{C}$ .

- $\text{Dom}(f) = \omega$ . Claramente,  $\text{Dom}(f) \subset \omega$ . Como  $(0, x_0) \in f$ , temos  $0 \in \text{Dom}(f)$ . Agora, se  $n \in \text{Dom}(f)$ , então existe  $y \in X$  tal que  $(n, y) \in f$ , já que  $f$  é uma relação. Com isso, vem  $(n^+, g(y)) \in f$ , donde  $n^+ \in \text{Dom}(f)$ . Assim,  $\text{Dom}(f)$  é indutivo, e como  $\text{Dom}(f) \subset \omega$ , temos que  $\text{Dom}(f) = \omega$ .
- $f$  é função. Provaremos que  $(n, y) \in f$  e  $(n, z) \in f$  implicam  $y = z$  por indução em  $n$ .
  - Base de indução. Como  $(0, x_0) \in f$ , provemos que se  $(0, z) \in f$ , então  $z = x_0$ . Equivalentemente, via contrapositiva, podemos provar que se  $z \in X$  é tal que  $z \neq x_0$ , então  $(0, z) \notin f$ . Como  $(0, z) \notin f$  equivale a  $f \setminus \{(0, z)\} \in \mathcal{C}$ , provemos isso para todo  $z \in X$  tal que  $z \neq x_0$ . Sendo  $z \neq x_0$ , o par  $(0, x_0)$  não foi “removido” de  $f$ , de modo que  $(0, x_0) \in f \setminus \{(0, z)\}$ . Agora, se  $(n, y) \in f \setminus \{(0, z)\}$ , então, como  $f \in \mathcal{C}$ , temos que  $(n^+, g(y)) \in f$ . Como, pelo teorema (3.99),  $n^+ \neq 0$  para todo  $n \in \omega$ , temos  $(n^+, g(y)) \in f \setminus \{(0, z)\}$ . Isso prova que  $f \setminus \{(0, z)\}$  é uma relação que satisfaz as condições do teorema e, portanto,  $f \setminus \{(0, z)\} \in \mathcal{C}$ . Com isso, se  $(0, z) \in f$ , então  $z = x_0$ .
  - Passo indutivo. Agora, tomando  $n \in \text{Dom}(f)$ , existe  $y \in X$  tal que  $(n, y) \in f$ , e ainda,  $(n^+, g(y)) \in f$ . Supondo, por hipótese de indução, que  $(n, z) \in f$  implica  $y = z$ , precisamos provar que  $(n^+, z) \in f$  implica  $z = g(y)$ . Provemos, então, via contrapositiva, que se  $z \in X$  é tal que  $z \neq g(y)$ , então  $(n^+, z) \notin f$ . Isso significa provar, assim como fizemos no caso base da indução, que  $f \setminus \{(n^+, z)\} \in \mathcal{C}$ . De fato, como  $n^+ \neq 0$ , temos  $(0, x_0) \in f \setminus \{(n^+, z)\}$  (o par  $(0, x_0)$  não pode ter sido “removido”). Agora, se  $m \in \text{Dom}(f)$ , existe  $t \in X$  tal que  $(m, t) \in f$  e  $(m^+, g(t)) \in f$ . Se for  $m^+ = n^+$ , então  $m = n$  (teorema (3.99)), de modo que, pela hipótese de indução,  $t = y$ , donde  $g(t) = g(y) \neq z$ . Assim,  $f \setminus \{(n^+, z)\}$  satisfaz as condições do teorema e, portanto,  $f \setminus \{(n^+, z)\} \in \mathcal{C}$ . Com isso, se  $(n^+, z) \in f$ , então  $z = g(y)$ .

- iii. Unicidade de  $f$ . Se  $h$  é outra função satisfazendo as condições do teorema, então  $h(0) = x_0 = f(0)$  e, se  $h(n) = f(n)$ , então

$$h(n^+) = g(h(n)) = g(f(n)) = f(n^+).$$

de modo que, por indução,  $h = f$ .

Com isso, vemos que existe uma relação  $f$  que é uma função, tem domínio  $\omega$ , é única e satisfaz as condições do teorema.

**Teorema 3.108** (da recursão com parâmetro). Sejam  $X$  um conjunto,  $x_0 \in X$  e  $g : \omega \times X \rightarrow X$ . Existe e é única a função  $f : \omega \rightarrow X$  tal que

- $f(0) = x_0$ ;
- $f(n^+) = g(n, f(n))$ , para todo  $n \in \omega$ .

**Prova.** Defina  $g' : \omega \times X \rightarrow \omega \times X$  por  $g'(n, y) = (n^+, g(n, y))$ . Pelo teorema da recursão finita (3.107), existe uma única função  $f' : \omega \rightarrow \omega \times X$  tal que  $f'(0) = (0, x_0)$  e  $f'(n^+) = g'(f'(n))$  para todo  $n \in \omega$ .

Afirmamos que a primeira coordenada de  $f'(n)$  é sempre  $n$ , isto é, que  $f'(n) = (n, y_n)$  para todo  $n \in \omega$  e algum  $y_n \in X$ . De fato,  $f'(0) = (0, x_0)$  claramente cumpre a afirmação, e se  $f'(n) = (n, y_n)$  para algum  $y_n \in X$ , então  $f'(n^+) = g'(n, y_n) = (n^+, g(n, y_n))$ , o que prova, via indução, a afirmação. Com isso, podemos definir  $f : \omega \rightarrow X$  de modo que  $f(n) = y_n$ , para todo  $n \in \omega$ .

Provemos que  $f$  satisfaz as condições do teorema. Temos  $f'(0) = (0, x_0)$ , donde  $f(0) = x_0$ . Ainda pela definição de  $f$ , temos  $f'(n) = (n, f(n))$  e  $f'(n^+) = (n^+, f(n^+))$ ; por outro lado,  $f'(n^+) = g'(n, f(n)) = (n^+, g(n, f(n)))$ , de modo que  $f(n^+) = g(n, f(n))$  para todo  $n \in \omega$ .

Por fim, provemos a unicidade de  $f$ . Se  $h : \omega \rightarrow X$  tal que  $h(0) = x_0$  e  $h(n^+) = g(n, h(n))$  para todo  $n \in \omega$ , definindo  $h' : \omega \rightarrow \omega \times X$  por  $h'(n) = (n, h(n))$ , temos que  $h'(0) = (0, x_0)$  e, para todo  $n \in \omega$ ,

$$h(n^+) = (n^+, h(n^+)) = (n^+, g(n, h(n))) = g'(n, h(n)) = g'(h'(n)).$$

Com isso,  $h'$  é uma função que satisfaz as mesmas condições que  $f'$ ; como  $f'$  foi construída pelo teorema da recursão, segue que  $h' = f'$ .

Para a próxima versão do teorema da recursão, denotamos por  $X^{<\omega}$  o conjunto de todas as funções de um certo  $n \in \omega$  em  $X$ .

**Teorema 3.109** (da recursão completa). Sejam  $X$  um conjunto e  $g : X^{<\omega} \rightarrow X$  uma função. Existe e é única a função  $f : \omega \rightarrow X$  tal que  $f(n) = g(f|_n)$  para todo  $n \in \omega$ .

**Prova.** Ver [5], corolário 4.31, página 115. Observe que esse resultado, assim como (3.108), são corolários do teorema (3.107).

### 3.3.2 Aritmética dos Números Naturais

## 3.4 O Axioma da Escolha

**Axioma 3.110** (da Escolha). Para todo conjunto  $x$  de conjuntos não vazios existe uma função  $\varphi : x \rightarrow \bigcup x$  tal que  $\varphi(y) \in y$  para todo  $y \in x$ .

$$\boxed{\forall x \left( \emptyset \notin x \rightarrow \exists \varphi \left( \varphi : x \rightarrow \bigcup x \wedge \forall y (y \in x \rightarrow \varphi(y) \in y) \right) \right)}$$

**Observação 3.111.** Usamos a sigla AC (do inglês *Axiom of Choice*) para nos referirmos ao axioma da escolha. Por seu caráter não construtivo, o axioma da escolha é o axioma mais controverso da matemática, evitado por uns e usado indiscriminadamente por outros. Desastres acontecem com e sem AC: por exemplo, sem AC, muitos resultados matemáticos fundamentais falham, sendo equivalentes em ZF a AC ou a alguma forma fraca de AC.

**Proposição 3.112.** O axioma da escolha é equivalente à seguinte afirmação.

$$\forall x \exists \varphi \left( \varphi : x \setminus \{\emptyset\} \rightarrow \bigcup x \wedge \forall y (y \in x \setminus \{\emptyset\} \rightarrow \varphi(y) \in y) \right).$$

**Prova.** ■

**Definição 3.113.** Uma *sequência* em  $X$  *indexada*  $I$  é uma função  $x : I \rightarrow X$ . Isso é denotado por  $(x_i)_{i \in I}$ .

- (a) Denotamos por  $x_i$  a imagem de  $i \in I$  pela sequência  $x : I \rightarrow X$ , isto é,  $x_i := x(i)$ .
- (b) Denotamos por  $(x_i)_{i \in I}$  a sequência  $x : I \rightarrow X$ .
- (c) Denotamos por  $\{x_i : i \in I\}$  a imagem da sequência  $(x_i)_{i \in I}$ .
- (d) Denotamos por  $\bigcup_{i \in I} x_i$  a união da imagem da sequência  $(x_i)_{i \in I}$ , isto é,  $\bigcup_{i \in I} x_i := \bigcup \{x_i : i \in I\}$ .

**Definição 3.114.** O *produto cartesiano* de uma sequência  $(x_i)_{i \in I}$  é definido como

$$\prod_{i \in I} x_i := \left\{ f \in \left( \bigcup_{i \in I} x_i \right)^I : \forall i (i \in I \rightarrow f(i) \in x_i) \right\},$$

isto é,  $\prod_{i \in I} x_i$  é definido como o conjunto de todas as funções  $f$  de domínio  $I$  tais que  $f(i) \in x_i$  para todo  $i \in I$ .

**Proposição 3.115.** O axioma da escolha é equivalente à seguinte afirmação: se  $(X_i)_{i \in I}$  é uma sequência com  $X_i \neq \emptyset$  para todo  $i \in I$ , então  $\prod_{i \in I} X_i \neq \emptyset$ .

**Prova.** Usemos a notação usual de função escrevendo  $g = (X_i)_{i \in I}$ .

( $\Rightarrow$ ) Como  $g(i) \neq \emptyset$  para todo  $i \in I$ , temos  $\emptyset \notin \text{Im}(g)$ , de modo que, pelo axioma da escolha, existe uma função  $\varphi : \text{Im}(g) \rightarrow \bigcup \text{Im}(g)$  tal que  $\varphi(y) \in y$  para todo  $y \in \text{Im}(g)$ . Tomando  $f := \varphi \circ g : I \rightarrow \bigcup \text{Im} g$ , temos, para todo  $i \in I$ ,

$$f(i) = (\varphi \circ g)(i) = \varphi[g(i)] \in g(i),$$

isto é,  $f(i) \in g(i)$ . Como  $g(i) := X_i$ , vem  $f(i) \in X_i$  para todo  $i \in I$ , de modo que  $f \in \prod_{i \in I} X_i$ , isto é,  $\prod_{i \in I} X_i \neq \emptyset$ .

( $\Leftarrow$ ) Agora, seja  $x \neq \emptyset$  tal que  $\emptyset \notin x$ . Defina  $g = (X_i)_{i \in I}$  assim:  $I = x$  e  $g := \text{Id}_I$ . Como  $X_i = g(i) = \text{Id}_I(i) = i \in I = x$  e  $\emptyset \notin x$ , temos  $X_i \neq \emptyset$  para todo  $i \in I$ , de modo que  $\prod_{i \in I} X_i \neq \emptyset$ . Com isso, existe  $\varphi \in \prod_{i \in I} X_i$  tal que  $\varphi(i) \in X_i$  para todo  $i \in I$ , e como  $X_i = i$  e  $I = x$ , vem  $\varphi(i) \in i$  para todo  $i \in x$ , de modo que  $\varphi : x \rightarrow \bigcup x$  é uma função de escolha em  $x$ . ■

**Definição 3.116.** Sejam  $(X, \leq)$  um conjunto parcialmente ordenado e  $S$  um subconjunto não vazio de  $X$ .

- (a) Dizemos que  $x \in S$  é *maximal* em  $S$  se não existe  $y \in S$  tal que  $x < y$ .
- (b) Dizemos que  $x \in S$  é *minimal* em  $S$  se não existe  $y \in S$  tal que  $y < x$ .
- (c) Dizemos que  $S$  é uma *cadeia* em  $X$  se

$$\forall x \forall y (x, y \in S \rightarrow (x \leq y \vee y \leq x)).$$

**Teorema 3.117** (Lema de Zorn). Seja  $(X, \leq)$  um conjunto parcialmente ordenado. Se toda cadeia em  $X$  é limitada superiormente em  $X$ , então  $X$  possui um elemento maximal.

**Prova.** ■

# **Parte II**

## **Números Reais**

## Capítulo 4

# Números Reais como na Análise

### 4.1 Corpos

**Definição 4.1.** Uma tripla  $(\mathbb{F}, +, \cdot)$  é um *corpo* se no conjunto  $\mathbb{F} \neq \emptyset$  existem duas operações,  $+: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$  e  $\cdot: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$ , para as quais

- A1:  $x + (y + z) = (x + y) + z$  para quaisquer  $x, y, z \in \mathbb{F}$ ;
- A2:  $x + y = y + x$  para quaisquer  $x, y \in \mathbb{F}$ ;
- A3: existe  $0 \in \mathbb{F}$  tal que  $x + 0 = x$  para todo  $x \in \mathbb{F}$ ;
- A4: para cada  $x \in \mathbb{F}$  existe  $y \in \mathbb{F}$  tal que  $x + y = 0$ ;
- M1:  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$  para quaisquer  $x, y, z \in \mathbb{F}$ ;
- M2:  $x \cdot y = y \cdot x$  para quaisquer  $x, y \in \mathbb{F}$ ;
- M3: existe  $1 \in \mathbb{F}_{\neq 0}$  tal que  $x \cdot 1 = x$  para todo  $x \in \mathbb{F}$ ;
- M4: para cada  $x \in \mathbb{F}_{\neq 0}$  existe  $y \in \mathbb{F}$  tal que  $x \cdot y = 1$ ;
- D:  $x \cdot (y + z) = x \cdot y + x \cdot z$  para quaisquer  $x, y, z \in \mathbb{F}$ .

Para simplificar a notação, e quando não houver perigo de confusão, vamos nos referir ao corpo  $(\mathbb{F}, +, \cdot)$  simplesmente como o conjunto  $\mathbb{F}$ .

**Observação 4.2.** As operações  $+$  e  $\cdot$  são chamadas, respectivamente, de *adição* e *multiplicação*. As propriedades descritas em A1 e M1 são chamadas de *associatividade*; em A2 e M2, de *comutatividade*; em A3 e M3, de existência de *elementos neutros*; em A4, de existência de um *oposto aditivo*; em M4, de existência de um *inverso multiplicativo*; e em D, de *distributividade*.

**Proposição 4.3.** Seja  $(\mathbb{F}, +, \cdot)$  um corpo. Valem as seguintes afirmações.

**(a)** (Unicidade)

- i. O elemento neutro 0 de  $+$  é único.
- ii. O elemento neutro 1 de  $\cdot$  é único.
- iii. O inverso multiplicativo de cada elemento de  $\mathbb{F}_{\neq 0}$  é único.

**(b)** (Leis do corte) Para quaisquer  $x, y, z \in \mathbb{F}$ , temos

- i.  $x + z = y + z \Rightarrow x = y$ ;
- ii.  $x \cdot z = y \cdot z$  e  $z \in \mathbb{F}_{\neq 0} \Rightarrow x = y$ .

**(c)** (Integridade) Para quaisquer  $x, y \in \mathbb{F}$ , temos

- i.  $x \cdot 0 = 0$ ;
- ii.  $x \cdot y = 0 \Rightarrow x = 0$  ou  $y = 0$ ;

**(d)** (Regras dos sinais) Para quaisquer  $x, y \in \mathbb{F}$ , temos

- i.  $(-1) \cdot x = -x$ ;
- ii.  $-(-x) = x$ ;
- iii.  $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ ;
- iv.  $(-x) \cdot (-y) = x \cdot y$ .

**(e)** Para quaisquer  $x, y \in \mathbb{F}$ , temos

$$x^2 = y^2 \Leftrightarrow x = y \text{ ou } x = -y.$$

**Prova.** ■

**Definição 4.4.** Um corpo  $(\mathbb{F}, +, \cdot)$  é *ordenado* se existe uma relação  $\leq \subseteq \mathbb{F} \times \mathbb{F}$  tal que  $(\mathbb{F}, \leq)$  é um conjunto totalmente ordenado e

- i. para quaisquer  $x, y, z \in \mathbb{F}$ , se  $x \leq y$ , então  $x + z \leq y + z$ ;
- ii. para quaisquer  $x, y, z \in \mathbb{F}$ , se  $x \leq y$  e  $0 \leq z$ , então  $x \cdot z \leq y \cdot z$ .

Isso é denotado por  $(\mathbb{F}, +, \cdot, \leq)$ .

**Proposição 4.5.** Seja  $(\mathbb{F}, +, \cdot, \leq)$  um corpo ordenado.

**(a)** A relação  $< \subseteq \mathbb{F} \times \mathbb{F}$  definida como

$$< := \{(x, y) \in \mathbb{F} \times \mathbb{F} : x \leq y \wedge x \neq y\}$$

é de ordem estrita total.

**(b)** Existe um subconjunto  $\mathbb{F}_{>0} \subseteq \mathbb{F}$  tal que

- i. se  $x, y \in \mathbb{F}_{>0}$ , então  $x + y \in \mathbb{F}_{>0}$  e  $x \cdot y \in \mathbb{F}_{>0}$ ;
- ii. se  $x \in \mathbb{F}$ , então ou  $x = 0$ , ou  $x \in \mathbb{F}_{>0}$ , ou  $-x \in \mathbb{F}_{>0}$ , exclusivamente.

**Prova.**

(a)

(b) Como a notação “ $\mathbb{F}_{>0}$ ” sugere, basta tomar  $\mathbb{F}_{>0} := \{x \in \mathbb{F} : x > 0\}$ , onde  $y > x$  significa  $x < y$ .

**Observação 4.6.** Sendo  $\mathbb{F}$  um corpo ordenado, escrevemos  $x < y$  quando  $y > x$  e  $x \leq y$  quando  $y \geq x$ .

**Proposição 4.7.** Propriedades cringe de ordem

**Definição 4.8.** Seja  $\mathbb{F}$  um corpo ordenado. A função  $|\cdot| : \mathbb{F} \rightarrow \mathbb{F}_{\geq 0}$  definida por

$$|x| := \begin{cases} x & \text{se } x \in \mathbb{F}_{\geq 0} \\ -x & \text{se } x \in \mathbb{F}_{<0} \end{cases}$$

é chamada de *função modular*. O *módulo*, ou o *valor absoluto*, de  $x \in \mathbb{F}$ , é a imagem de  $x$  pela função modular, isto é,  $|x| \in \mathbb{F}_{\geq 0}$ .

**Proposição 4.9.** Seja  $\mathbb{F}$  um corpo ordenado. Valem as seguintes afirmações.

- (a)  $x \leq |x|$  para todo  $x \in \mathbb{F}$ ;
- (b)  $|x \cdot y| = |x| \cdot |y|$  para quaisquer  $x, y \in \mathbb{F}$ ;
- (c)  $|x + y| \leq |x| + |y|$  para quaisquer  $x, y \in \mathbb{F}$ ;
- (d)  $|x| - |y| \leq ||x| - |y|| \leq |x - y|$  para quaisquer  $x, y \in \mathbb{F}$ ;
- (e)  $|x - z| \leq |x - y| + |y - z|$ ;
- (f)  $|x| \leq \epsilon \Leftrightarrow -\epsilon \leq x \leq \epsilon$  para quaisquer  $x \in \mathbb{F}$  e  $\epsilon \in \mathbb{F}_{>0}$ .

**Prova.** Ver [15], teorema 4.5, página 14. ■

## 4.2 Números Naturais

Em toda esta seção,  $(\mathbb{F}, +, \cdot, \leq)$  é um corpo ordenado qualquer.

**Definição 4.10.** Um subconjunto  $I \subseteq \mathbb{F}$  é *indutivo* se  $1 \in I$  e  $n \in I \Rightarrow n + 1 \in I$ . Isso é denotado por  $\text{Ind } I$ .

**Exemplo 4.11.**  $\mathbb{F}$  é um conjunto indutivo. Com isso, o conjunto de todos os subconjuntos indutivos de  $\mathbb{F}$  é não vazio, isto é,  $\{I \in \mathcal{P}(\mathbb{F}) : \text{Ind}(I)\} \neq \emptyset$ . Em particular, isso nos permite considerar  $\bigcap \{I \in \mathcal{P}(\mathbb{F}) : \text{Ind}(I)\}$ .

**Proposição 4.12.** Se  $\mathcal{A}$  é uma coleção não vazia de subconjuntos indutivos de  $\mathbb{F}$ , isto é, se

$$\mathcal{A} \in \mathcal{P}(\{I \in \mathcal{P}(\mathbb{F}) : \text{Ind}(I)\})_{\neq \emptyset},$$

então  $\bigcap \mathcal{A}$  é um conjunto indutivo.

**Prova.** Como  $1 \in A$  para todo  $A \in \mathcal{A}$ , temos  $1 \in \bigcap \mathcal{A}$ . Agora, se  $n \in \bigcap \mathcal{A}$ , então  $n \in A$  para todo  $A \in \mathcal{A}$ ; como cada  $A \in \mathcal{A}$  é indutivo, temos  $n + 1 \in A$ , donde  $n + 1 \in \bigcap \mathcal{A}$ . ■

**Definição 4.13.** O conjunto dos números naturais é definido como o menor subconjunto indutivo de  $\mathbb{F}$ :

$$\mathbb{N}_{\mathbb{F}} := \bigcap \{I \in \mathcal{P}(\mathbb{F}) : \text{Ind}(I)\}.$$

**Observação 4.14.** Explicação

**Teorema 4.15** (Indução).

- (a) Se um subconjunto  $A \subseteq \mathbb{N}$  é indutivo, então  $A = \mathbb{N}$ .
- (b) Seja  $s(n)$  uma proposição bem definida para cada  $n \in \mathbb{N}$ . Se  $s(1)$  é verdadeira e se  $s(n + 1)$  é verdadeira sempre que  $s(n)$  é verdadeira, então  $s(n)$  é verdadeira para todo  $n \in \mathbb{N}$ .

**Prova.**

- (a) Se  $A$  é um conjunto indutivo, então, pela definição de  $\mathbb{N}$ , temos  $\mathbb{N} \subseteq A$ . Daí, se  $A \subseteq \mathbb{N}$ , então  $A = \mathbb{N}$ . ■
- (b) Definindo  $A := \{n \in \mathbb{N} : s(n)\}$ , temos  $A \subseteq \mathbb{N}$ . Além disso,  $1 \in A$  e  $n + 1 \in A$  sempre que  $n \in A$ , de modo que  $A$  é indutivo. Com isso,  $\mathbb{N} \subseteq A$ , de modo que  $A = \mathbb{N}$ , isto é, vale  $s(n)$  para todo  $n \in \mathbb{N}$ . ■

**Proposição 4.16.**

- (a) Para quaisquer  $m, n \in \mathbb{N}$  tem-se  $m + n \in \mathbb{N}$ .
- (b) Para quaisquer  $m, n \in \mathbb{N}$  tem-se  $m \cdot n \in \mathbb{N}$ .
- (c) Para qualquer  $n \in \mathbb{N}$ , tem-se  $n \geq 1$ . Isso significa, em particular, que  $\mathbb{N}$  é limitado inferiormente.

**Prova.**

- (a) Fixe  $m \in \mathbb{N}$  e defina  $A := \{n \in \mathbb{N} : m + n \in \mathbb{N}\}$ . Temos  $1 \in A$  pois se  $m \in \mathbb{N}$  então  $m + 1 \in \mathbb{N}$  já que  $\mathbb{N}$  é indutivo. Agora, se  $n \in A$ , então  $m + n \in \mathbb{N}$ , e como  $\mathbb{N}$  é indutivo vem  $(m + n) + 1 \in \mathbb{N}$ , isto é,  $m + (n + 1) \in \mathbb{N}$ , de modo que  $n + 1 \in A$ . Com isso,  $A$  é indutivo, isto é,  $\mathbb{N} \subseteq A$ . Como  $A \subseteq \mathbb{N}$

pela definição de  $A$ , segue que  $A = \mathbb{N}$ . Como  $m$  foi fixado arbitrariamente, segue que  $m + n \in \mathbb{N}$  para quaisquer  $m, n \in \mathbb{N}$ . ■

- (b) Fixe  $m \in \mathbb{N}$  e defina  $A := \{n \in \mathbb{N} : m \cdot n \in \mathbb{N}\}$ . Temos  $1 \in A$  pois  $m \cdot 1 = m \in \mathbb{N}$ . Agora, se  $n \in A$ , então  $m \cdot n \in \mathbb{N}$ , e pelo item anterior  $m \cdot n + m \in \mathbb{N}$ , isto é,  $m \cdot (n + 1) \in \mathbb{N}$ , de modo que  $n + 1 \in A$ . Com isso,  $A$  é indutivo, isto é,  $\mathbb{N} \subseteq A$ . Como  $A \subseteq \mathbb{N}$  pela definição de  $A$ , segue que  $A = \mathbb{N}$ . Como  $m$  foi fixado arbitrariamente, segue que  $m \cdot n \in \mathbb{N}$  para quaisquer  $m, n \in \mathbb{N}$ . ■
- (c) Definindo  $A := \{n \in \mathbb{N} : n \geq 1\}$ , temos  $A \subseteq \mathbb{N}$ . Claramente  $1 \in A$  pois  $1 \geq 1$ . Agora, se  $n \in A$ , então  $1 > 0 \Rightarrow n + 1 > n \geq 1 \Rightarrow n + 1 \geq 1$ , de modo que  $n + 1 \in A$ . Com isso  $\mathbb{N} \subseteq A$ , donde  $A = \mathbb{N}$ . ■

**Lema 4.17.**

- (a) Para qualquer  $n \in \mathbb{N}$ , se  $n \neq 1$ , então  $n - 1 \in \mathbb{N}$ .
- (b) Para quaisquer  $m, n \in \mathbb{N}$ , se  $n < m$ , então  $m - n \in \mathbb{N}$ .
- (c) Para qualquer  $n \in \mathbb{N}$  não existe  $m \in \mathbb{N}$  tal que  $n < m < n + 1$ .

**Prova.**

- (a) Suponha que existe  $p \in \mathbb{N}$  com  $p \neq 1$  tal que  $p - 1 \notin \mathbb{N}$ , e seja  $A = \mathbb{N} \setminus \{p\}$ . Como  $1 \in \mathbb{N}$  e  $p \neq 1$ , temos  $1 \in A$ . Agora, se  $n \in A$ , então  $n \neq p$ , e também  $n + 1 \neq p$  (se fosse  $n + 1 = p$ , então  $p - 1 = n \in \mathbb{N}$ , mas supomos  $p - 1 \notin \mathbb{N}$ ), de modo que  $A$  é indutivo. Assim,  $\mathbb{N} \setminus \{p\} = \mathbb{N}$ , uma clara contradição, de modo que não existe tal  $p$ . ■
- (b) Definindo  $A := \{n \in \mathbb{N} : \forall m(m \in \mathbb{N} \wedge n < m \Rightarrow m - n \in \mathbb{N})\}$ , temos  $A \subseteq \mathbb{N}$ . Para todo  $m \in \mathbb{N}$  com  $m > 1$ , temos  $m \neq 1$ , de modo que  $m - 1 \in \mathbb{N}$  pelo item anterior. Com isso,  $1 \in A$ . Agora, se  $n \in A$ , então para todo  $m \in \mathbb{N}$  com  $m > n$  tem-se  $m - n \in \mathbb{N}$ , e precisamos provar que  $n + 1 \in A$ , isto é, que para todo  $m \in \mathbb{N}$  com  $m > n + 1$  tem-se  $m - (n + 1) \in \mathbb{N}$ . Se  $m > n + 1$ , então  $m > n + 1 > n$ , de modo que, pela hipótese de indução, temos  $m - n \in \mathbb{N}$ . Agora, como  $m > n + 1$ , temos  $m - n \neq 1$ , e como  $m - n \in \mathbb{N}$ , pelo item anterior temos  $(m - n) - 1 \in \mathbb{N}$ , isto é,  $m - (n + 1) \in \mathbb{N}$ , de modo que  $n + 1 \in A$ . Com isso,  $A$  é indutivo, isto é,  $\mathbb{N} \subseteq A$ , de modo que  $A = \mathbb{N}$ . ■
- (c) Sendo  $n \in \mathbb{N}$ , suponha que existe  $m \in \mathbb{N}$  tal que  $n < m < n + 1$ . Daí,  $m - n < 1$  e, pelo item anterior,  $m - n \in \mathbb{N}$ , absurdo! Logo, tal  $m$  não pode existir. ■

**Teorema 4.18** (Princípio da Boa Ordenação). Todo subconjunto não vazio de números naturais possui um elemento mínimo. Isto é, se  $A \in \mathcal{P}(\mathbb{N})_{\neq \emptyset}$ , então

existe  $a \in A$  tal que  $a \leq x$  para todo  $x \in A$ .

**Prova.** Suponha por contradição que existe um subconjunto  $A \in \mathcal{P}(\mathbb{N})_{\neq \emptyset}$  que não tem um elemento mínimo. Definindo  $[n] := \{x \in \mathbb{N} : x \leq n\}$  e  $X := \{n \in \mathbb{N} : [n] \cap A = \emptyset\}$ , temos  $1 \in X$  (de fato, se  $1 \notin X$ , então  $[1] \cap A \neq \emptyset$ , de modo que  $1 \in A$  seria o elemento mínimo de  $A$ , absurdo!). Agora, se  $n \in X$ , então  $[n] \cap A = \emptyset$ ; daí, se fosse  $n+1 \in A$ , este seria o elemento mínimo de  $A$ , absurdo! Logo, só pode ser  $n+1 \in X$ , de modo que  $X$  é indutivo e  $\mathbb{N} \subseteq X$ . Como  $X \subseteq \mathbb{N}$  por definição, temos que  $X = \mathbb{N}$ , donde  $A = \emptyset$ , uma contradição. ■

**Prova.** Suponha por contradição que existe um subconjunto  $A \in \mathcal{P}(\mathbb{N})_{\neq \emptyset}$  que não tem um elemento mínimo. Definindo

$$X := \{n \in \mathbb{N} : \forall r (r \in \mathbb{N} \wedge 1 \leq r \leq n \Rightarrow r \in \mathbb{N} \setminus A)\},$$

temos  $1 \in X$ . De fato, se fosse  $1 \notin X$ , então existiria  $r \in \mathbb{N}$  tal que  $1 \leq r \leq 1$  e  $r \notin \mathbb{N} \setminus A$ , isto é, teríamos  $1 \in A$ , de modo que  $A$  teria um elemento mínimo, uma contradição. Agora, provemos que se  $n \in X$  então  $n+1 \in X$ . Se fosse  $n+1 \notin X$ , então teríamos  $n+1 \in A$ , e como  $A$  não tem um elemento mínimo existiria  $p \in A$  tal que  $p < n+1$ . Como  $p \in \mathbb{N}$ , pelo lema (4.17) teríamos  $1 \leq p \leq n$  (não poderia ser  $n < p < n+1$  justamente pelo lema), mas como  $n \in X$  teríamos  $p \in \mathbb{N} \setminus A$ , uma contradição pois  $p \in A$ . Com isso,  $n+1 \in X$  e  $X$  é indutivo, de modo que,  $X = \mathbb{N}$ . Logo, para todo  $n \in \mathbb{N}$  temos  $n \in \mathbb{N} \setminus A$ , isto é,  $A = \emptyset$ , de modo que não existe um subconjunto não vazio de  $\mathbb{N}$  que não tenha um elemento mínimo. ■

**Prova.** Defina  $X := \{n \in \mathbb{N} : [n] \subseteq \mathbb{N} \setminus A\}$ . Se  $1 \in A$ , então  $1 = \min A$ . Se  $1 \notin A$ , então  $[1] = \{1\} \subset \mathbb{N} \setminus A$ , de modo que  $1 \in X$ . Agora, como  $A \neq \emptyset$ , temos que  $X \neq \mathbb{N}$ . Se  $1 \in X$  e  $X \neq \mathbb{N}$ , então existe  $n_0 \in X$  tal que  $n_0 + 1 \notin X$  (se um tal  $n_0$  não existisse,  $X$  seria indutivo e teríamos  $X = \mathbb{N}$ ), isto é,  $[n_0] \cap A = \emptyset$  e  $[n_0 + 1] \cap A \neq \emptyset$ . Com isso, temos  $n_0 + 1 \in A$ , sendo este o elemento mínimo de  $A$  (pois, pelo lema (4.17), não existe um natural entre  $n_0$  e  $n_0 + 1$ ). ■

**Corolário 4.19.** Todo subconjunto não vazio de números naturais limitado superiormente possui um elemento máximo. Isto é, se  $A \in \mathcal{P}(\mathbb{N})_{\neq \emptyset}$  é limitado superiormente, então existe  $a \in A$  tal que  $x \leq a$  para todo  $x \in A$ .

**Prova.**

**Teorema 4.20** (Indução forte). Se  $A \subseteq \mathbb{N}$  é tal que  $n \in A$  sempre que  $m \in A$  para todo  $m < n$ , então  $A = \mathbb{N}$ .

**Prova.** Provemos que  $X := \mathbb{N} - A$  é vazio. De fato, se  $X \neq \emptyset$ , então pela Boa Ordenação existiria  $p \in X$  mínimo; daí, todo  $m < p$  seria  $m \in A$ , de modo que, pela definição de  $A$ ,  $p \in A$ , absurdo! Logo,  $X = \emptyset$ . ■

**Definição 4.21.** Um corpo ordenado  $\mathbb{F}$  é *arquimediano* se para quaisquer  $a \in \mathbb{F}_{>0}$  e  $b \in \mathbb{F}$  existe  $n \in \mathbb{N}_{\mathbb{F}}$  tal que  $n \cdot a > b$ .

**Teorema 4.22.**  $\mathbb{N}_{\mathbb{F}}$  é ilimitado superiormente em  $\mathbb{F}$  se, e somente se,

- i.  $\mathbb{F}$  é arquimediano;
- ii. para todo  $\epsilon \in \mathbb{F}_{>0}$  existe  $n \in \mathbb{N}$  tal que  $0 < \frac{1}{n} < \epsilon$ .

**Prova.** Ver [19], teorema 3 do capítulo 3. ■

### 4.2.1 A Unicidade dos Números Naturais

**Teorema 4.23** (da Recursão). Sejam  $(\mathbb{F}, +_{\mathbb{F}}, \cdot_{\mathbb{F}}, \leq_{\mathbb{F}})$  um corpo ordenado,  $X$  um conjunto,  $a \in X$  e  $f : X \rightarrow X$  uma função. Existe e é única a função  $\varphi : \mathbb{N}_{\mathbb{F}} \rightarrow X$  tal que

- $\varphi(1_{\mathbb{F}}) = a$ ;
- $\varphi(n +_{\mathbb{F}} 1_{\mathbb{F}}) = f(\varphi(n))$ , para todo  $n \in \mathbb{N}_{\mathbb{F}}$ .

**Prova.** Para simplificar a notação vamos omitir o índice  $\mathbb{F}$ . Sendo  $\mathcal{C}$  o conjunto de todas as relações de  $\mathbb{N}$  em  $X$  que tem as propriedades desejadas, deve existir um único elemento de  $\mathcal{C}$  que seja uma função de domínio  $\mathbb{N}$ . Formalmente,

$$\mathcal{C} := \{R \in \mathcal{P}(\mathbb{N} \times X) : (1, a) \in R \wedge \forall n \forall x ((n, x) \in R \Rightarrow (n+1, f(x)) \in R)\}.$$

Como  $\mathbb{N} \times X \in \mathcal{C}$ , temos  $\mathcal{C} \neq \emptyset$ , logo existe  $\varphi := \bigcap \mathcal{C} \in \mathcal{C}$ . Afirmamos que  $\varphi$  é esse único elemento procurado. Provemos então que  $\varphi$  é uma função de domínio  $\mathbb{N}$ . Para tanto,  $\varphi$  deve ter as seguintes propriedades:

- A relação  $\varphi$  tem domínio  $\mathbb{N}$ :  $\forall n (n \in \mathbb{N} \Rightarrow \exists x (x \in X \wedge (n, x) \in \varphi))$ .
- A relação  $\varphi$  é funcional:  $\forall n \forall x \forall y ((n, x) \in \varphi \wedge (n, y) \in \varphi \Rightarrow x = y)$ .

Sendo  $S := \{n \in \mathbb{N} : \exists x ((n, x) \in \varphi \wedge \forall y ((n, y) \in \varphi \Rightarrow y = x))\}$ , se  $S = \mathbb{N}$ , então  $\varphi$  terá essas propriedades. Como  $S \subseteq \mathbb{N}$ , basta provar que  $\mathbb{N} \subseteq S$ , e para isso basta provar que  $S$  é um conjunto indutivo.

- i. Como  $(1, a) \in \varphi$ , provemos a unicidade de  $a$  como imagem de 1 por  $\varphi$ . Se existisse  $b \in X$  tal que  $(1, b) \in \varphi$  e  $b \neq a$ , então  $(1, a) \in \varphi \setminus \{(1, b)\}$ , e se  $(n, x) \in \varphi \setminus \{(1, b)\}$ , então  $(n, x) \in \varphi$ , de modo que  $(n+1, f(x)) \in \varphi$ ; como  $n+1 \neq 1$ , teríamos  $(n+1, f(x)) \in \varphi \setminus \{(1, b)\}$ , de modo que  $\varphi \setminus \{(1, b)\} \in \mathcal{C}$ , uma contradição. Com isso,  $1 \in S$ .
- ii. Se  $n \in S$ , então existe um único  $x \in X$  tal que  $(n, x) \in \varphi$ . Com isso, vem  $(n+1, f(x)) \in \varphi$ ; provemos então a unicidade de  $f(x)$  como imagem de

$n + 1$  por  $\varphi$ . Suponha que exista  $b \in X$  tal que  $(n + 1, b) \in \varphi$  e  $b \neq f(x)$ . Temos  $(1, a) \in \varphi \setminus \{(n + 1, b)\}$  pois  $n + 1 \neq 1$ . Se  $(m, y) \in \varphi \setminus \{(n + 1, b)\}$ , então  $(m, y) \in \varphi$  e  $(m + 1, f(y)) \in \varphi$ . Se  $m = n$ , então  $y = x$ ,  $m + 1 = n + 1$  e  $f(y) = f(x) \neq b$ , de modo que  $(m + 1, f(x)) \in \varphi \setminus \{(n + 1, b)\}$ . Se  $m \neq n$ , então  $m + 1 \neq n + 1$ , de modo que  $(m + 1, f(x)) \in \varphi \setminus \{(n + 1, b)\}$ . Com isso, vem  $\varphi \setminus \{(n + 1, b)\} \in \mathcal{C}$ , uma contradição. Logo, se  $n \in S$ , então  $n + 1 \in S$ , de modo que  $S = \mathbb{N}$ .

Com isso, fica provada a existência de uma função  $\varphi : \mathbb{N} \rightarrow X$  com as propriedades desejadas. Provemos, por fim, sua unicidade. Sendo  $\psi : \mathbb{N} \rightarrow X$  uma função com essas mesmas propriedades e definindo  $T := \{n \in \mathbb{N} : \psi(n) = \varphi(n)\}$ , claramente  $1 \in T$ , e se  $n \in T$ , então  $\psi(n) = \varphi(n)$ , de modo que  $\psi(n + 1) = f(\psi(n)) = f(\varphi(n)) = \varphi(n + 1)$ , isto é,  $n + 1 \in T$ . Com isso, vem  $T = \mathbb{N}$ , o que prova a unicidade de  $\varphi$ . ■

**Teorema 4.24.** Sejam  $(\mathbb{F}_1, +_1, \cdot_1, \leq_1)$  e  $(\mathbb{F}_2, +_2, \cdot_2, \leq_2)$  corpos ordenados. Existe uma única bijeção  $\varphi : \mathbb{N}_{\mathbb{F}_1} \rightarrow \mathbb{N}_{\mathbb{F}_2}$  tal que, para quaisquer  $m, n \in \mathbb{N}_{\mathbb{F}_1}$ , valem as seguintes propriedades.

- i.  $\varphi(m +_1 n) = \varphi(m) +_2 \varphi(n)$ .
- ii.  $\varphi(m \cdot_1 n) = \varphi(m) \cdot_2 \varphi(n)$ .
- iii.  $m \leq_1 n \Leftrightarrow \varphi(m) \leq_2 \varphi(n)$ .

**Prova.** Tomando  $X = \mathbb{N}_{\mathbb{F}_2}$ ,  $a = 1_{\mathbb{F}_2}$  e  $f : \mathbb{N}_{\mathbb{F}_2} \rightarrow \mathbb{N}_{\mathbb{F}_2}$  dada por  $f(n) = n +_2 1_{\mathbb{F}_2}$  no teorema da recursão (4.23), existe uma única função  $\varphi : \mathbb{N}_{\mathbb{F}_1} \rightarrow \mathbb{N}_{\mathbb{F}_2}$  tal que  $\varphi(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_2}$  e  $\varphi(n +_1 1_{\mathbb{F}_1}) = f[\varphi(n)] = \varphi(n) +_2 1_{\mathbb{F}_2}$ . Provemos a bijetividade de  $\varphi$  construindo explicitamente sua função inversa. Tomando  $X = \mathbb{N}_{\mathbb{F}_1}$ ,  $a = 1_{\mathbb{F}_1}$  e  $g : \mathbb{N}_{\mathbb{F}_1} \rightarrow \mathbb{N}_{\mathbb{F}_1}$  dada por  $g(n) = n +_1 1_{\mathbb{F}_1}$  no teorema da recursão (4.23), existe uma única função  $\psi : \mathbb{N}_{\mathbb{F}_2} \rightarrow \mathbb{N}_{\mathbb{F}_1}$  tal que  $\psi(1_{\mathbb{F}_2}) = 1_{\mathbb{F}_1}$  e  $\psi(n +_2 1_{\mathbb{F}_2}) = g[\psi(n)] = \psi(n) +_1 1_{\mathbb{F}_1}$ . Vamos provar que  $\psi \circ \varphi = \text{Id}_{\mathbb{F}_1}$  e  $\varphi \circ \psi = \text{Id}_{\mathbb{F}_2}$ . Sendo  $F := \psi \circ \varphi : \mathbb{N}_{\mathbb{F}_1} \rightarrow \mathbb{N}_{\mathbb{F}_1}$ , temos

$$F(1_{\mathbb{F}_1}) = \psi[\varphi(1_{\mathbb{F}_1})] = \psi(1_{\mathbb{F}_2}) = 1_{\mathbb{F}_1},$$

e ainda,

$$F(n +_1 1_{\mathbb{F}_1}) = \psi[\varphi(n +_1 1_{\mathbb{F}_1})] = \psi[\varphi(n) +_2 1_{\mathbb{F}_2}] = F(n) +_1 1_{\mathbb{F}_1}.$$

Agora, como  $\text{Id}_{\mathbb{N}_{\mathbb{F}_1}}(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_1}$  e  $\text{Id}_{\mathbb{N}_{\mathbb{F}_1}}(n +_1 1_{\mathbb{F}_1}) = \text{Id}_{\mathbb{N}_{\mathbb{F}_1}}(n) +_1 1_{\mathbb{F}_1}$ , e como só existe uma função com essas propriedades, vem  $F = \text{Id}_{\mathbb{N}_{\mathbb{F}_1}}$ . A prova de que  $\varphi \circ \psi = \text{Id}_{\mathbb{N}_{\mathbb{F}_2}}$  é completamente análoga, de modo que  $\psi$  é a função inversa de  $\varphi$  e, portanto,  $\varphi$  é bijetiva.

- i. Fixe  $m \in \mathbb{N}_{\mathbb{F}_1}$  e defina  $A := \{n \in \mathbb{N}_{\mathbb{F}_1} : \varphi(m +_1 n) = \varphi(m) +_2 \varphi(n)\}$ . Como  $\varphi(m +_1 1_{\mathbb{F}_1}) = \varphi(m) +_2 1_{\mathbb{F}_2}$ , temos  $1_{\mathbb{F}_1} \in A$  pois  $\varphi$  foi obtida pelo teorema da recursão. Agora, se  $n \in A$ , então  $\varphi(m +_1 n) = \varphi(m) +_2 \varphi(n)$  e

$$\begin{aligned} \varphi[m +_1 (n +_1 1_{\mathbb{F}_1})] &= \varphi[(m +_1 n) +_1 1_{\mathbb{F}_1}] \\ &= \varphi[(m +_1 n)] +_2 1_{\mathbb{F}_2} \\ &= [\varphi(m) +_2 \varphi(n)] +_2 1_{\mathbb{F}_2} \\ &= \varphi(m) +_2 [\varphi(n) +_2 1_{\mathbb{F}_2}] \\ &= \varphi(m) +_2 \varphi(n +_1 1_{\mathbb{F}_1}), \end{aligned}$$

de modo que  $n +_1 1_{\mathbb{F}_1} \in A$ , isto é,  $A$  é indutivo. Logo  $A = \mathbb{N}$ .

- ii. Fixe  $m \in \mathbb{N}_{\mathbb{F}_1}$  e defina  $A := \{n \in \mathbb{N}_{\mathbb{F}_1} : \varphi(m \cdot_1 n) = \varphi(m) \cdot_2 \varphi(n)\}$ . Como

$$\varphi(m \cdot_1 1_{\mathbb{F}_1}) = \varphi(m) = \varphi(m) \cdot_2 1_{\mathbb{F}_2} = \varphi(m) \cdot_2 \varphi(1_{\mathbb{F}_1}),$$

temos  $1_{\mathbb{F}_1} \in A$ . Agora, se  $n \in A$ , então  $\varphi(m \cdot_1 n) = \varphi(m) \cdot_2 \varphi(n)$  e

$$\begin{aligned} \varphi[m \cdot_1 (n +_1 1_{\mathbb{F}_1})] &= \varphi(m \cdot_1 n +_1 m \cdot_1 1_{\mathbb{F}_1}) \\ &= \varphi(m \cdot_1 n) +_2 \varphi(m) \\ &= \varphi(m) \cdot_2 \varphi(n) +_2 \varphi(m) \\ &= \varphi(m) \cdot_2 (\varphi(n) +_2 1_{\mathbb{F}_2}) \\ &= \varphi(m) \cdot_2 [\varphi(n +_1 1_{\mathbb{F}_1})], \end{aligned}$$

de modo que  $n +_1 1_{\mathbb{F}_1} \in A$ , isto é,  $A$  é indutivo. Logo  $A = \mathbb{N}$ .

- iii. Se  $m = n$ , então  $\varphi(m) = \varphi(n)$ , e se  $\varphi(m) = \varphi(n)$ , então  $m = n$  pela injetividade de  $\varphi$ . Com isso, basta provarmos  $m <_1 n \Leftrightarrow \varphi(m) <_2 \varphi(n)$ . Se  $m <_1 n$ , então pelo lema (4.17) existe  $k \in \mathbb{N}_{\mathbb{F}_1}$  tal que  $n = m +_1 k$ . Com isso,  $\varphi(n) = \varphi(m) +_2 \varphi(k)$ , e se fosse  $\varphi(m) \geq_2 \varphi(n)$ , teríamos  $\varphi(k) \leq_2 0_{\mathbb{F}_2}$ , um absurdo. Agora, se  $\varphi(m) <_2 \varphi(n)$ , então  $m \neq n$  pela injetividade de  $\varphi$ , e se fosse  $m >_1 n$  existiria  $k \in \mathbb{N}_{\mathbb{F}_1}$  tal que  $m = n +_1 k$ , de modo que  $\varphi(n +_1 k) <_2 \varphi(n)$ , uma contradição.

Com isso, vemos que a função  $\varphi : \mathbb{N}_{\mathbb{F}_1} \rightarrow \mathbb{N}_{\mathbb{F}_2}$ , obtida pelo teorema da recursão, é bijetiva, preserva a adição, a multiplicação e a ordem, como queríamos. ■

## 4.2.2 Definições recursivas

O objetivo desta subseção é usar o teorema da recursão (4.23) para fazermos definições recursivas.

### 4.3 Conjuntos Finitos

Seguimos [19] e [18] de perto.

**Definição 4.25.** Um conjunto  $X \neq \emptyset$  é *finito* se existem um natural  $n \in \mathbb{N}$  e uma bijeção  $f : [n] \rightarrow X$ . Isso é denotado por  $|X| = n$ . O natural  $n$  é o *número de elementos* de  $X$ , enquanto  $f$  é uma *contagem dos elementos* de  $X$ . Em particular, o conjunto vazio  $\emptyset$  é finito e tem 0 elementos.

**Teorema 4.26.**

- (a) Para todo  $n \in \mathbb{N}$ , não existe uma bijeção  $f : A \subsetneq [n] \rightarrow [n]$ .
- (b) Para todo  $n \in \mathbb{N}$ , se existe uma bijeção  $f : [n] \rightarrow A \subseteq [n]$ , então  $A = [n]$ .

**Prova.**

- (a) Começamos com um lema: se existe uma bijeção  $f : X \rightarrow Y$ , então, dados  $a \in X$  e  $b \in Y$ , existe também uma bijeção  $g : X \rightarrow Y$  tal que  $g(a) = b$ . De fato, como  $f$  é sobrejetora, então existe  $a' \in X$  tal que  $f(a') = b$ ; sendo  $b' = f(a)$ , definamos  $g : X \rightarrow Y$  pondo  $g(a) = b$ ,  $g(a') = b'$  e  $g(x) = f(x)$  para todo  $x \neq a, a'$  em  $X$ . É fácil ver que  $g$  é uma bijeção. Agora, seja  $n_0$  o menor natural para o qual existe uma bijeção  $f : A \subsetneq [n_0] \rightarrow [n_0]$ . Se  $n_0 \in A$ , então, pelo lema, existe uma bijeção  $g : A \subsetneq [n_0] \rightarrow [n_0]$  com  $g(n_0) = n_0$ ; daí, a restrição  $\tilde{g} : A \setminus \{n_0\} \subsetneq [n_0 - 1] \rightarrow [n_0 - 1]$  é uma bijeção, o que contraria a minimalidade de  $n_0$ . Por outro lado, se  $n_0 \notin A$ , então  $A \subsetneq [n_0 - 1]$ ; tomando  $a \in A$  com  $f(a) = n_0$ , a restrição  $\tilde{f} : A \setminus \{a\} \subsetneq A \subseteq [n_0 - 1] \rightarrow [n_0 - 1]$  é uma bijeção, o que, novamente, contraria a minimalidade de  $n_0$ . ■
- (b) Basta ver que esse enunciado é a contrapositiva do item anterior. No entanto, ainda assim, daremos uma outra prova, que se dará por indução em  $n$ . Evidentemente, o resultado vale para  $n = 1$ . Agora, supondo que o resultado vale para  $n \in \mathbb{N}$ , tomando uma bijeção  $f : [n+1] \rightarrow A \subseteq [n+1]$  provaremos que  $A = [n+1]$ . Sendo  $a := f(n+1)$ , a restrição  $\tilde{f} : [n] \rightarrow A \setminus \{a\}$  é uma bijeção.

- Se for  $A \setminus \{a\} \subseteq [n]$ , então, pela hipótese de indução,  $A \setminus \{a\} = [n]$ , donde  $a = n+1$  e  $A = [n+1]$ .
- Se for  $A \setminus \{a\} \not\subseteq [n]$ , então  $n+1 \in A \setminus \{a\}$  e existe  $p \in [n]$  tal que  $f(p) = n+1$ . Agora, definindo a bijeção  $g : [n+1] \rightarrow A \subseteq [n+1]$  por

$$g(x) = \begin{cases} f(x), & \text{se } x \neq p \text{ e } x \neq n+1 \\ a, & \text{se } x = p \\ n+1, & \text{se } x = n+1 \end{cases},$$

a restrição  $\tilde{g} : [n] \rightarrow A \setminus \{n+1\}$  é uma bijeção; daí, como  $A \setminus \{n+1\} \subseteq [n]$ , pela hipótese de indução  $A \setminus \{n+1\} = [n]$ , donde  $A = [n+1]$ .

Com isso, temos  $A = [n+1]$  em ambos os casos, como queríamos provar. ■

**Corolário 4.27.**

- (a) O número de elementos de um conjunto finito está bem definido. Isto é, se  $f : [m] \rightarrow X$  e  $g : [n] \rightarrow X$  são bijeções, então  $m = n$ .
- (b) (Princípio bijetivo) Sejam  $A, B \neq \emptyset$  conjuntos finitos. Temos  $|A| = |B|$  se, e somente se, existe uma bijeção  $f : A \rightarrow B$ .

**Prova.**

- (a) Se fosse  $m < n$ , teríamos  $[m] \subsetneq [n]$ , donde existiria uma bijeção  $g^{-1} \circ f : [m] \rightarrow [n]$ , o que contraria o teorema (4.26). Analogamente, se fosse  $n < m$ , teríamos  $[n] \subsetneq [m]$ , donde existiria uma bijeção  $f^{-1} \circ g : [n] \rightarrow [m]$ , o que novamente contraria o teorema (4.26)! Logo, só pode ser  $m = n$ .

Uma outra prova é o que segue. Se  $h = g^{-1} \circ f : [m] \rightarrow [n]$  é uma bijeção, então  $m = n$ . De fato, se  $m \leq n$ , então  $[m] \subseteq [n]$ , e como  $h^{-1} : [n] \rightarrow [m] \subseteq [n]$ , pelo teorema (4.26) só pode ser  $[m] = [n]$ , donde  $m = n$ . ■

- (b) Como  $A, B \neq \emptyset$  são finitos, existem  $n, m \in \mathbb{N}$  e bijeções  $g : [n] \rightarrow A$  e  $h : [m] \rightarrow B$ .

( $\Rightarrow$ ) Sendo  $|B| = n$ , existe uma bijeção  $\varphi : [n] \rightarrow B$ , donde  $g^{-1} \circ \varphi : A \rightarrow B$  é uma bijeção.

( $\Leftarrow$ ) Existindo uma bijeção  $f : A \rightarrow B$ , temos que  $g^{-1} \circ f^{-1} \circ h : [m] \rightarrow [n]$  é também uma bijeção, donde  $m = n$ , isto é,  $|A| = |B|$ . ■

### 4.3.1 Resultadinhos

**Proposição 4.28.** Seja  $X$  um conjunto finito.

- (a) Para todo subconjunto próprio  $Y \subsetneq X$  não existe uma bijeção  $f : X \rightarrow Y$ .
- (b) Todo subconjunto  $Y \subseteq X$  também é finito. Se  $Y \subsetneq X$ , então  $|Y| < |X|$ , sendo  $|Y| = |X|$  somente quando  $Y = X$ .

**Prova.**

- (a) Suponha que existe uma tal bijeção. Se  $X$  é finito, então existe uma bijeção  $h : [n] \rightarrow X$  para algum  $n \in \mathbb{N}$ . Definindo  $A := h^{-1}(Y)$ , temos  $A \subsetneq [n]$  e, além disso, a restrição de  $h$  a  $A$  é uma bijeção  $h_A : A \rightarrow Y$ . Com isso, a

composta  $h^{-1} \circ f^{-1} \circ h_A : A \rightarrow [n]$  é uma bijeção de  $A \subsetneq [n]$  em  $[n]$ , o que contraria o teorema (4.26)! Logo, não pode existir uma bijeção  $f : X \rightarrow Y$  onde  $X$  é finito e  $Y \subsetneq X$ . ■

Observe que esse item é uma mera reformulação do teorema (4.26).

(b) Ver [19], página 31, teorema 4. Ver [18], página 5, teorema 2.

**Corolário 4.29.**

- (a) Se  $X$  é um conjunto finito, então uma função  $f : X \rightarrow X$  será injetora se, e somente se, for sobrejetora.
- (b) Seja  $f : X \rightarrow Y$  uma função injetora. Se  $Y$  é finito, então  $X$  é finito e  $|X| \leq |Y|$ .
- (c) Seja  $f : X \rightarrow Y$  uma função sobrejetora. Se  $X$  é finito, então  $Y$  é finito e  $|Y| \leq |X|$ .

**Prova.**

- (a) Ver [18], página 4, corolário 2.
- (b) Ver [18], página 5, corolário 1. Ver [19], página 31, corolário 1.
- (c) Ver [18], página 5, corolário 1. Ver [19], página 31, corolário 2.

**Definição 4.30.**

- (a) Um conjunto  $X \subseteq \mathbb{N}$  é *limitado* se existe  $n \in \mathbb{N}$  tal que  $x \leq n$  para todo  $x \in X$ .
- (b) (Maior elemento)

**Teorema 4.31.** Dado  $\emptyset \neq X \subseteq \mathbb{N}$ , as seguintes afirmações são equivalentes.

1.  $X$  é finito;
2.  $X$  é limitado;
3.  $X$  possui um maior elemento.

**Prova.** Ver [19], página 32, teorema 5. Para finito sse limitado, ver [18], página 5, corolário 2.

## 4.4 Conjuntos Infinitos

**Definição 4.32.**

- (a) Um conjunto  $X$  é *infinito* quando ele não é finito, isto é, quando  $X \neq \emptyset$  e quando não existe uma bijeção  $f : [n] \rightarrow X$  para todo  $n \in \mathbb{N}$ .
- (b) Um subconjunto  $X \subseteq \mathbb{N}$  é *ilimitado* se ele não é limitado, isto é, se para todo  $n \in \mathbb{N}$  existe  $p \in X$  tal que  $p > n$ .

**Corolário 4.33.**  $\mathbb{N}$  é infinito.

**Proposição 4.34.** Segue como contrapositiva do teorema (4.31): um conjunto  $\emptyset \neq X \subseteq \mathbb{N}$  é infinito se, e somente se, não é limitado. Como  $\mathbb{N}$  não é limitado, ele é infinito.

**Teorema 4.35.** Se  $X$  é um conjunto infinito, então existe uma função  $f : \mathbb{N} \rightarrow X$  injetora.

**Prova.**

**Corolário 4.36.** Um conjunto  $X$  é infinito se, e somente se, existe uma bijeção  $f : X \rightarrow Y \subsetneq X$ .

**Prova.**

**Corolário 4.37.**

- (a) Seja  $f : X \rightarrow Y$  uma função injetora. Se  $X$  é infinito, então  $Y$  é infinito.
- (b) Seja  $f : X \rightarrow Y$  uma função sobrejetora. Se  $Y$  é infinito, então  $X$  é infinito.

**Prova.** Basta ver que essas afirmações são equivalentes às afirmações do resultado (4.29) por contrapositiva.

**Proposição 4.38.** Se  $X$  é um conjunto finito e  $Y$  é um conjunto infinito, então existem funções  $f : X \rightarrow Y$  injetora e  $g : Y \rightarrow X$  sobrejetora.

**Prova.**

## 4.5 Conjuntos Enumeráveis e Não-Enumeráveis

**Definição 4.39.** Um conjunto  $X$  é *enumerável* se é finito ou se existe uma bijeção  $f : \mathbb{N} \rightarrow X$ . A função  $f$  é uma *enumeração* de  $X$ .

**Teorema 4.40.** Todo subconjunto de  $\mathbb{N}$  é enumerável.

**Prova.** Seja  $X \subseteq \mathbb{N}$ . Se  $X$  é finito, nada há de ser provado.

**Corolário 4.41.** (a) Seja  $f : X \rightarrow Y$  uma função injetora. Se  $Y$  é enumerável, então  $X$  é enumerável.

(b) Seja  $f : X \rightarrow Y$  uma função sobrejetora. Se  $X$  é enumerável, então  $Y$  é enumerável.

**Prova.**

**Corolário 4.42. (a)** O produto cartesiano de um número finito de conjuntos enumeráveis é enumerável.

(b) A união de uma família enumerável de conjuntos enumeráveis é enumerável.

## 4.6 Números Inteiros

**Definição 4.43.** O conjunto dos números inteiros é definido como

$$\mathbb{Z}_{\mathbb{F}} := \mathbb{N}_{\mathbb{F}} \cup \{0\} \cup -\mathbb{N}_{\mathbb{F}}.$$

**Proposição 4.44.**

- (a) Para quaisquer  $m, n \in \mathbb{Z}$  tem-se  $m + n \in \mathbb{Z}$ .
- (b) Para quaisquer  $m, n \in \mathbb{Z}$  tem-se  $m - n \in \mathbb{Z}$  e  $n - m \in \mathbb{Z}$ .
- (c) Para quaisquer  $m, n \in \mathbb{Z}$  tem-se  $m \cdot n \in \mathbb{Z}$ .

**Prova.**

**Proposição 4.45.** Para todo  $x \in \mathbb{F}$  existe um único  $n \in \mathbb{Z}$  tal que  $n \leq x < n + 1$ .

### 4.6.1 Teoria Elementar dos Números

## 4.7 Números Racionais

(Racionais) Sendo  $y, w \neq 0$ , temos que  $x \cdot w = y \cdot z \Leftrightarrow x \cdot y^{-1} = z \cdot w^{-1}$ .

**Definição 4.46.** O conjunto dos números racionais é definido como

$$\mathbb{Q}_{\mathbb{F}} := \{x \in \mathbb{F} : \exists a \exists b (a \in \mathbb{Z}_{\mathbb{F}} \wedge b \in \mathbb{Z}_{\mathbb{F}} \wedge b \neq 0 \wedge x = a \cdot b^{-1})\}.$$

**Proposição 4.47.** Para quaisquer  $p, q \in \mathbb{Q}$ , temos  $p + q \in \mathbb{Q}$  e  $p \cdot q \in \mathbb{Q}$ .

**Prova.**

**Definição 4.48.** Dado  $x \in \mathbb{R}$ , definimos, para cada  $n \in \mathbb{N}$ ,  $x^1 := x$  e  $x^{n+1} := x^n \cdot x$ , e sendo  $x \neq 0$ , definimos, para cada  $n \in \mathbb{N}_0$ ,  $x^0 := 1$  e  $x^{-n} := \frac{1}{x^n}$ .

**Teorema 4.49. (a)** Seja  $n \in \mathbb{N}$ . Para todo  $a \in \mathbb{R}_{\geq 0}$  existe um único  $b \in \mathbb{R}_{\geq 0}$  tal que  $b^n = a$ . Notação:  $b := \sqrt[n]{a}$

**(b)** Seja  $n \in \mathbb{N}$  ímpar. Para todo  $a \in \mathbb{R}$  existe  $b \in \mathbb{R}$  tal que  $b^n = a$ . Notação:  $b := \sqrt[n]{a}$ .

**Prova.**

**Definição 4.50. (a)** Seja  $n \in \mathbb{N}$ . Dado  $x \in \mathbb{R}_{\geq 0}$ , definimos  $x^{\frac{1}{n}} := \sqrt[n]{x}$ . Se  $n$  for ímpar, dado  $x \in \mathbb{R}$ , definimos  $x^{\frac{1}{n}} := \sqrt[n]{x}$ .

**(b)** Seja  $n \in \mathbb{N}$ . Dado  $x \in \mathbb{R}$ , definimos  $x^{-\frac{1}{n}} := \frac{1}{x^{\frac{1}{n}}}$ , desde que  $x^{\frac{1}{n}} \neq 0$  esteja definido.

**(c)** Seja  $r := \frac{p}{q} \in \mathbb{Q}$ , com  $p \in \mathbb{Z}$  e  $q \in \mathbb{Z}_{\neq 0}$ . Dado  $x \in \mathbb{R}$ , definimos  $x^r := \left(x^{\frac{1}{q}}\right)^p$ , desde que  $x^{\frac{1}{q}}$  esteja definido.

**Teorema 4.51. (a)** Se  $a, b \in \mathbb{R}$  cumprem  $a < b$ , então existe  $r \in \mathbb{Q}$  tal que  $a < r < b$ .

**(b)** Se  $a, b \in \mathbb{R}$  cumprem  $a < b$ , então existe  $s \in \mathbb{R} \setminus \mathbb{Q}$  tal que  $a < s < b$ .

**Prova.**

## 4.8 Números Reais

**Definição 4.52.** Sejam  $(\mathbb{F}, +, \cdot, \leq)$  um corpo ordenado e  $S \in \mathcal{P}(\mathbb{F})_{\neq \emptyset}$ .

**(a)** Dizemos que  $S$  é

- i. *limitado superiormente* se existe  $M \in \mathbb{F}$  tal que  $x \leq M$  para todo  $x \in S$ . Nesse caso, dizemos que  $M$  é uma *cota superior* de  $S$ .
- ii. *limitado inferiormente* se existe  $m \in \mathbb{F}$  tal que  $m \leq x$  para todo  $x \in S$ . Nesse caso, dizemos que  $m$  é uma *cota inferior* de  $S$ .
- iii. *limitado* se  $S$  é limitado superiormente e inferiormente.

**(b)** Dizemos que  $\alpha \in \mathbb{F}$  é o

- i. *supremo* de  $S$  se  $\alpha$  é uma cota superior de  $S$  e  $\alpha \leq x$  para toda cota superior  $x \in \mathbb{F}$  de  $S$ . Denotamos  $\alpha$  por  $\sup S$ .
- ii. *ínfimo* de  $S$  se  $\alpha$  é uma cota inferior de  $S$  e  $x \leq \alpha$  para toda cota inferior  $x \in \mathbb{F}$  de  $S$ . Denotamos  $\alpha$  por  $\inf S$ .

**Proposição 4.53.** Sejam  $(\mathbb{F}, +, \cdot, \leq)$  um corpo ordenado e  $S \in \mathcal{P}(\mathbb{F})_{\neq \emptyset}$ .

- (a) O supremo de  $S$ , quando existe, é único.
- (b) O ínfimo de  $S$ , quando existe, é único.

**Prova.**

- (a) Sejam  $\alpha$  e  $\beta$  supremos de  $S$ . Como  $\alpha$  é a menor das cotas superiores de  $S$  e  $\beta$  é uma cota superior de  $S$ , temos  $\alpha \leq \beta$ . Como  $\beta$  é a menor das cotas superiores de  $S$  e  $\alpha$  é uma cota superior de  $S$ , temos  $\beta \leq \alpha$ . Logo  $\alpha = \beta$ . ■
- (b) Segue analogamente. ■

**Teorema 4.54.** Sejam  $(\mathbb{F}, +, \cdot, \leq)$  um corpo ordenado e  $S \in \mathcal{P}(\mathbb{F})_{\neq \emptyset}$ .

- (a) Suponha que existe  $\sup S$ .
  - i. Se  $\beta \in \mathbb{F}$  e  $\beta < \sup S$ , então existe  $x \in S$  tal que  $x > \beta$ .
  - ii. Para todo  $\epsilon \in \mathbb{F}_{>0}$  existe  $x \in S$  tal que  $\sup S - \epsilon < x$ .
- (b) Suponha que existe  $\inf S$ .
  - i. Se  $\beta \in \mathbb{F}$  e  $\inf S < \beta$ , então existe  $x \in S$  tal que  $x < \beta$ .
  - ii. Para todo  $\epsilon \in \mathbb{F}_{>0}$  existe  $x \in S$  tal que  $x < \inf S + \epsilon$ .

**Prova.**

- (a) Segue facilmente por contradição.
  - i. Do contrário, seria  $x \leq \beta < \sup S$  para todo  $x \in S$ , de modo que  $\beta$  seria uma cota superior de  $S$  menor que  $\sup S$ , um absurdo. ■
  - ii. Do contrário, existiria  $\epsilon \in \mathbb{F}_{>0}$  tal que  $x \leq \sup S - \epsilon < \sup S$  para todo  $x \in S$ , de modo que  $\sup S - \epsilon$  seria uma cota superior de  $S$  menor que  $\sup S$ , um absurdo. ■
- (b) Segue analogamente. ■

**Definição 4.55.** Um corpo ordenado  $\mathbb{F}$  é *completo* se todo subconjunto não vazio de  $\mathbb{F}$  limitado superiormente possui supremo em  $\mathbb{F}$ .

**Corolário 4.56.** Um corpo ordenado  $\mathbb{F}$  é *completo* se, e somente se, todo subconjunto não vazio de  $\mathbb{F}$  limitado inferiormente possui ínfimo em  $\mathbb{F}$ .

**Prova.** Ver [23], teorema 1-10, página 32. Ver [22], corolário 1.12, página 13. ■

**Proposição 4.57.** Todo corpo ordenado completo é arquimediano.

**Prova.** Provemos que em todo corpo ordenado completo  $\mathbb{F}$  o conjunto  $\mathbb{N}_{\mathbb{F}}$  é ilimitado superiormente. Daí, pelo teorema (4.22), seguirá que  $\mathbb{F}$  é arquimediano.

Suponha, por absurdo, que  $\mathbb{N}_{\mathbb{F}}$  seja limitado superiormente. Como  $\mathbb{N}_{\mathbb{F}} \in \mathcal{P}(\mathbb{F})_{\neq \emptyset}$ ,

existe  $a := \sup \mathbb{N}_{\mathbb{F}}$ . Por (4.54), para  $\epsilon = 1$  existe  $n \in \mathbb{N}_{\mathbb{F}}$  tal que  $a - 1 < n$ , isto é,  $a < n + 1$ , e como  $n + 1 \in \mathbb{N}_{\mathbb{F}}$ , temos uma contradição. ■

**Teorema 4.58.** Existe um corpo ordenado completo.

**Observação 4.59.** Veremos mais a frente que, a menos de isomorfismos, existe um único corpo ordenado completo. Ele é denotado por  $\mathbb{R}$  e seus elementos são chamados de *números reais*.

## Propriedades do Supremo e do Ínfimo

**Prova.**

## Capítulo 5

# Números Reais como na Álgebra

**Definição 5.1** (Grupo).

- (a) Um par  $(G, *)$  é um *grupo* se no conjunto  $G \neq \emptyset$  existe uma operação  $* : G \times G \rightarrow G$  para a qual
- G1:  $x * (y * z) = (x * y) * z$  para quaisquer  $x, y, z \in G$ ;
  - G3: existe  $e \in G$  tal que  $x * e = x = e * x$  para todo  $x \in G$ ;
  - G4: para cada  $x \in G$  existe  $y \in G$  tal que  $x * y = e = y * x$ .
- (b) Um grupo  $(G, *)$  é *comutativo*, ou *abeliano*, se
- G2:  $x * y = y * x$  para quaisquer  $x, y \in G$ ,

**Observação 5.2.** As propriedades descritas em G1–G4 se chamam, respectivamente, *associatividade*, *comutatividade*, existência de um *elemento neutro* e *invertibilidade* (ou existência de *inversos operativos*).

**Proposição 5.3.** Seja  $(G, *)$  um grupo.

- (a) O elemento neutro de  $*$  é único.
- (b) O inverso de cada elemento de  $G$  é único.

**Prova.**

- (a) Se  $e' \in G$  é um elemento neutro de  $*$ , então

$$e = e * e' = e' * e = e',$$

como havíamos afirmado. ■

- (b) Segue analogamente. ■

## Anéis

**Definição 5.4.** Uma tripla  $(A, +, \cdot)$  é um *anel* se no conjunto  $A \neq \emptyset$  existem duas operações,  $+: A \times A \rightarrow A$  e  $\cdot: A \times A \rightarrow A$ , para as quais

- A1:  $a + (b + c) = (a + b) + c$  para quaisquer  $a, b, c \in A$ ;
- A2:  $a + b = b + a$  para quaisquer  $a, b \in A$ ;
- A3: existe  $0 \in A$  tal que  $a + 0 = a$  para todo  $a \in A$ ;
- A4: para cada  $a \in A$  existe  $b \in A$  tal que  $a + b = 0$ ;
- M1:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  para quaisquer  $a, b, c \in A$ ;
- AM:  $a \cdot (b + c) = a \cdot b + a \cdot c$  e  $(a + b) \cdot c = a \cdot c + b \cdot c$  para quaisquer  $a, b, c \in A$ .

**Proposição 5.5.** Seja  $(A, +, \cdot)$  um anel.

- (a) O elemento neutro 0 de  $+$  é único.
- (b) (Lei do corte) Para quaisquer  $a, b, c \in A$ , vale
- i.  $a + c = b + c \Rightarrow a = b$ ;
  - ii.  $a + b = a \Rightarrow b = 0$ .
- (c)  $a \cdot 0 = 0$  para todo  $a \in A$ .

**Prova.**

- (a) Se  $0' \in A$  é um elemento neutro de  $+$ , então

$$0' = 0' + 0 = 0 + 0' = 0,$$

conforme afirmado. ■

(b)

- (c) Observando que  $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ , somando  $-(a \cdot 0)$  aos dois lados de  $a \cdot 0 = a \cdot 0 + a \cdot 0$ , segue que  $0 \cdot a = 0$ . ■

**Definição 5.6.** Um anel  $(A, +, \cdot)$  é um *anel comutativo* se

- M2:  $a \cdot b = b \cdot a$  para quaisquer  $a, b \in A$ .

**Definição 5.7.** Um anel  $(A, +, \cdot)$  é um *anel com unidade* se

- M3: existe  $1 \in A_{\neq 0}$  tal que  $a \cdot 1 = 1 \cdot a = a$  para todo  $a \in A$ .

**Proposição 5.8.** Seja  $(A, +, \cdot)$  um anel com unidade.

- (a) O elemento neutro 1 de  $\cdot$  é único.

(b) (Regras dos sinais) Para quaisquer  $a, b \in A$ , vale

- i.  $(-1) \cdot a = -a$ ;
- ii.  $-(-a) = a$ ;
- iii.  $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ ;
- iv.  $(-a) \cdot (-b) = a \cdot b$ .

**Prova.** ■

**Definição 5.9.** Um anel comutativo com unidade  $(A, +, \cdot)$  é um *domínio de integridade* se

- M4:  $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$  para quaisquer  $a, b \in A$ .

**Proposição 5.10.** Seja  $(A, +, \cdot)$  um domínio de integridade.

(a) (Leis do corte) Para quaisquer  $a, b, c \in A$ , com  $c \neq 0$ ,

- i.  $a \cdot c = b \cdot c \Rightarrow a = b$ ;
- ii.  $a \cdot b = a \Rightarrow a = 0 \vee b = 1$ ;
- iii.  $a^2 = \begin{cases} 0 \Leftrightarrow a = 0 \\ 1 \Leftrightarrow a = 1 \text{ ou } a = -1 \\ a \Leftrightarrow a = 0 \text{ ou } a = 1 \end{cases}$ .

**Prova.**

**Definição 5.11.** Um anel comutativo com unidade  $(A, +, \cdot)$  é um *corpo* se

- M5: para cada  $a \in A_{\neq 0}$  existe  $b \in A$  tal que  $a \cdot b = 1$ .

**Proposição 5.12.** Todo corpo é um domínio de integridade.

**Prova.** ■

**Observação 5.13.** Para simplificar a linguagem, um anel comutativo com unidade será chamado simplesmente de anel.

**Definição 5.14.** Um anel  $(A, +, \cdot)$  é um *anel ordenado* se existe uma relação de ordem total  $\leq \subseteq A \times A$  tal que

- OA:  $a \leq b \Rightarrow a + c \leq b + c$  para quaisquer  $a, b, c \in A$ ;
- OM:  $a \leq b \Rightarrow a \cdot c \leq b \cdot c$  para quaisquer  $a, b, c \in A$  com  $0 \leq c$ .

**Proposição 5.15.** Se  $(A, +, \cdot, \leq)$  é um anel ordenado e  $a, b, c, d \in A$ , então

(a)  $a \geq 0 \Rightarrow -a \leq 0$  e  $a \leq 0 \Rightarrow -a \geq 0$ ;

(b)  $a + c \leq b + c \Rightarrow a \leq b$ ;

$$(c) a \leq b, c \leq d \Rightarrow a + c \leq b + d;$$

$$(d) a \leq b, c \leq 0 \Rightarrow a \cdot c \geq b \cdot c;$$

$$(e) a \geq 0, b \leq 0 \Rightarrow a \cdot b \leq 0 \text{ e } a \leq 0, b \leq 0 \Rightarrow a \cdot b \geq 0;$$

$$(f) a^2 \geq 0, 1 > 0 \text{ e } -1 < 0.$$

**Prova.**

**Definição 5.16.** Seja  $(A, +, \cdot, \leq)$  um anel ordenado. O *valor absoluto* de  $a \in A$  é definido como

$$|a| := \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}.$$

**Proposição 5.17.** Seja  $(A, +, \cdot, \leq)$  um anel ordenado. Para quaisquer  $a, b \in A$ , vale

$$(a) |a \cdot b| = |a| \cdot |b|.$$

$$(b) -|a| \leq a \leq |a|.$$

$$(c) |a| \leq b \Leftrightarrow -b \leq a \leq b.$$

$$(d) ||a| - |b|| \leq |a \pm b| \leq |a| + |b|.$$

**Prova.** ■

**Definição 5.18.** Seja  $(A, +, \cdot, \leq)$  um anel ordenado.

(a) Um subconjunto  $X \subseteq A$  é

- i. *limitado inferiormente* se existe  $a \in A$  tal que  $a \leq x$  para todo  $x \in X$ ;
- ii. *limitado superiormente* se existe  $a \in A$  tal que  $a \geq x$  para todo  $x \in X$ .

(b) Um subconjunto  $X \subseteq A$  tem um

- i. *menor elemento* se existe  $a \in X$  tal que  $a \leq x$  para todo  $x \in X$ ;
- ii. *maior elemento* se existe  $a \in X$  tal que  $a \geq x$  para todo  $x \in X$ .

**Proposição 5.19.** Seja  $(A, +, \cdot, \leq)$  um domínio ordenado. Todo subconjunto não vazio de  $A$ , limitado inferiormente, possui um menor elemento se, e somente se, todo subconjunto não vazio de  $A$ , limitado superiormente, possui um maior elemento.

**Prova.** ■

**Definição 5.20.** Um domínio ordenado  $(A, +, \cdot, \leq)$  é um *domínio bem ordenado* se

- PBO: todo subconjunto não vazio de  $A$ , limitado inferiormente, possui um menor elemento.

**Teorema 5.21.** Existe um único domínio bem ordenado.

**Teorema 5.22.** Seja  $(A, +, \cdot, \leq)$  um domínio bem ordenado.

(a) Para quaisquer  $a, b \in A$ , vale

- i.  $a > 0 \Rightarrow a \geq 1$ ;
- ii.  $a > b \Rightarrow a \geq b + 1$ ;
- iii.  $b \neq 0 \Rightarrow |a \cdot b| \geq |a|$ .

(b) Para quaisquer  $a, b \in A$ , com  $b \neq 0$ , existe  $n \in A$  tal que  $n \cdot b \geq a$ .

**Prova.** ■

## 5.1 Homomorfismos

**Definição 5.23.**

- (a) Um *homomorfismo de anéis*  $(A, +, \cdot)$  e  $(B, +, \cdot)$  é uma função  $f : A \rightarrow B$  tal que  $f(a + b) = f(a) + f(b)$  e  $f(a \cdot b) = f(a) \cdot f(b)$  para quaisquer  $a, b \in A$ .
- (b) Um *homomorfismo de anéis com unidade*  $(A, +, \cdot)$  e  $(B, +, \cdot)$  é um homomorfismo  $f : A \rightarrow B$  tal que  $f(1_A) = 1_B$ .
- (c) Um *homomorfismo de anéis ordenados*  $(A, +, \cdot, \leq)$  e  $(B, +, \cdot, \leq)$  é um homomorfismo  $f : A \rightarrow B$  tal que  $a \leq b \Rightarrow f(a) \leq f(b)$  para quaisquer  $a, b \in A$ .

Isso é denotado por  $A \cong B$ .

**Parte III**

**Análise Real I**

# Capítulo 6

## Sequências

**Definição 6.1.** Uma *sequência numérica* é qualquer função  $x : \mathbb{N} \rightarrow \mathbb{R}$ , que associa a cada número natural  $n$  um número real  $x_n := x(n)$  (isto é,  $n \mapsto x_n$ ), que será chamado de  $n$ -ésimo termo da sequência. Escreveremos  $(x_1, x_2, \dots, x_n, \dots)$ ,  $(x_n)_{n \in \mathbb{N}}$  ou  $(x_n)$  para indicar a sequência  $x : \mathbb{N} \rightarrow \mathbb{R}$  cujo  $n$ -ésimo termo é  $x_n \in \mathbb{R}$ .

**Definição 6.2.** Uma sequência  $(x_n)$  é

- i. *crescente* se  $n > m \Rightarrow x_n \geq x_m$ ;
- ii. *decrescente* se  $n > m \Rightarrow x_n \leq x_m$ ;
- iii. *estritamente crescente* se  $n > m \Rightarrow x_n > x_m$ ;
- iv. *estritamente decrescente* se  $n > m \Rightarrow x_n < x_m$ ;
- v. *monótona* se cumprir exatamente uma das condições acima.

**Definição 6.3.** Uma sequência  $(x_n)$  é

- i. *limitada superiormente* se existe  $M \in \mathbb{R}$  tal que  $x_n \leq M$  para todo  $n \in \mathbb{N}$ ;
- ii. *limitada inferiormente* se existe  $m \in \mathbb{R}$  tal que  $m \leq x_n$  para todo  $n \in \mathbb{N}$ ;
- iii. *limitada* se é limitada superiormente e limitada inferiormente.
- iv. *ilimitada* se não é limitada.

**Proposição 6.4.** Uma sequência  $(x_n)$  é limitada se, e somente se, existe  $L \in \mathbb{R}_{>0}$  tal que  $|x_n| \leq L$  para todo  $n \in \mathbb{N}$ .

**Prova.** Absolutamente trivial. ■

**Exemplo 6.5.** A sequência  $(x_n)$  é limitada se, e somente se, a sequência  $\{|x_n|\}$  é limitada.

**Prova.** Elão, início da seção 4.1.

**Definição 6.6.**

- (a) Uma sequência  $(x_n)$  é *convergente* e *converge* para  $a \in \mathbb{R}$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $n_0 \in \mathbb{N}$  tal que  $n > n_0 \Rightarrow |x_n - a| < \epsilon$ . Isso é denotado por

$$\lim_{n \rightarrow +\infty} x_n = a.$$

- (b) Uma sequência  $(x_n)$  é *divergente* se não for convergente.

**Observação 6.7.** As notações “ $\lim_{n \in \mathbb{N}} x_n = a$ ”, “ $\lim x_n = a$ ”, “ $x_n \rightarrow a$  quando  $n \rightarrow +\infty$ ” e “ $x_n \rightarrow a$ ” também são frequentemente usadas para indicar que  $\lim_{n \rightarrow +\infty} x_n = a$ .

**Proposição 6.8** (Unicidade). Uma sequência convergente converge para um único limite.

**Prova.** Provemos que se a sequência  $(x_n)$  converge para  $a \in \mathbb{R}$  e para  $b \in \mathbb{R}$ , então  $a = b$ .

**Proposição 6.9.** Toda sequência convergente é limitada.

**Prova.**

**Teorema 6.10** (Convergência monótona).

- (a) Toda sequência crescente e limitada superiormente é convergente.  
 (b) Toda sequência decrescente e limitada inferiormente é convergente.  
 (c) Toda sequência monótona e limitada é convergente.

**Prova. (a)** Seja  $(x_n)_{n \in \mathbb{N}}$  uma sequência crescente e limitada superiormente. Como o conjunto  $X := \{x_n \mid n \in \mathbb{N}\}$  é, por hipótese, não vazio e limitado superiormente, pela propriedade do supremo existe  $\sup X$ . Como, para todo  $\epsilon \in \mathbb{R}_{>0}$ ,  $\sup X - \epsilon$  não é uma cota superior de  $X$ , existe  $n_0 \in \mathbb{N}$  tal que  $\sup X - \epsilon < x_{n_0} \leq \sup X$ . Como  $(x_n)_{n \in \mathbb{N}}$  é crescente, para todo  $n \in \mathbb{N}$ , se  $n > n_0$ , então  $\sup X - \epsilon < x_{n_0} \leq x_n \leq \sup X < \sup X + \epsilon$ . Temos então que  $x_n \rightarrow \sup X$ , isto é,  $(x_n)_{n \in \mathbb{N}}$  converge para  $\sup X$ . ■

**(b)** Segue analogamente: sendo  $(x_n)_{n \in \mathbb{N}}$  uma sequência decrescente e limitada inferiormente, basta provar que  $x_n \rightarrow \inf \{x_n : n \in \mathbb{N}\}$ .

**Definição 6.11.** Uma *subsequência* de uma sequência  $x : \mathbb{N} \rightarrow \mathbb{R}$  dada por  $n \mapsto x_n$  é qualquer composição  $x \circ n : \mathbb{N} \rightarrow \mathbb{R}$ , onde  $n : \mathbb{N} \rightarrow \mathbb{N}$  dada por  $k \mapsto n_k$  é

uma sequência estritamente crescente de números naturais. A subsequência de  $(x_n)_{n \in \mathbb{N}}$  definida por  $(n_k)_{k \in \mathbb{N}}$  será denotada por  $(x_{n_k})_{k \in \mathbb{N}}$ .

**Proposição 6.12.** Se uma sequência  $(x_n)_{n \in \mathbb{N}}$  converge para  $a \in \mathbb{R}$ , então toda subsequência  $(x_{n_k})_{k \in \mathbb{N}}$  converge para  $a$ .

**Prova.**

**Teorema 6.13.** (Bolzano-Weierstrass) Toda sequência limitada possui uma subsequência convergente.

**Prova.** Pelo teorema (6.10), basta mostrar que toda sequência possui uma subsequência monótona. Seja  $(x_n)_{n \in \mathbb{N}}$  uma sequência limitada. Um índice  $k \in \mathbb{N}$  é dito *básico* quando  $x_p \geq x_k$  para todo  $p > k$ , isto é,  $x_k$  é menor ou igual aos termos que o sucedem.

- Se existem infinitos índices básicos  $n_1 < n_2 < n_3 < \dots$ , então  $x_{n_1} \leq x_{n_2} \leq x_{n_3} \leq \dots$ , de modo que a subsequência  $(x_{n_k})_{k \in \mathbb{N}}$  é crescente; como ela é limitada, pelo teorema (6.10), ela é convergente.
- Por outro lado, se o número de índices básicos é finito, seja  $n_1 \in \mathbb{N}$  maior que todos eles (se o número de índices básicos for 0, qualquer  $n_1$  funciona). Como  $n_1$  não é um índice básico, existe um índice  $n_2 \in \mathbb{N}_{>n_1}$  tal que  $x_{n_2} < x_{n_1}$ . Como  $n_2$  não é um índice básico, existe um índice  $n_3 \in \mathbb{N}_{>n_2}$  tal que  $x_{n_3} < x_{n_2}$ . Prosseguindo deste modo, obtemos uma subsequência  $(x_{n_k})_{k \in \mathbb{N}}$  estritamente decrescente; como ela é limitada, pelo teorema (6.10), ela é convergente.

Com isso, vemos que toda sequência possui uma subsequência monótona, e como a sequência original é limitada, a subsequência monótona também é (proposição (6.12)), sendo, portanto, convergente.

# Capítulo 7

## Limites e Continuidade

### 7.1 Topologia da Reta

**Definição 7.1.** Uma *vizinhança* de um ponto  $a \in \mathbb{R}$  com raio  $r \in \mathbb{R}_{>0}$  é definida como

$$V_r(a) := \{x \in \mathbb{R} : |x - a| < r\}.$$

**Corolário 7.2.** Para quaisquer  $a \in \mathbb{R}$  e  $r \in \mathbb{R}_{>0}$ , temos  $V_r(a) = (a - r, a + r)$ .

**Definição 7.3.** Um *ponto de acumulação* de um subconjunto  $A \subseteq \mathbb{R}$  é um ponto  $a \in \mathbb{R}$  tal que

$$V_\delta(a) \cap A_{\neq a} \neq \emptyset$$

para todo  $\delta \in \mathbb{R}_{>0}$ . O conjunto de todos os pontos de acumulação de  $A$  é denotado por  $A'$ .

**Proposição 7.4.** Seja  $A \subseteq \mathbb{R}$ .

- (a)  $a \in A'$  se, e somente se, para todo  $\delta \in \mathbb{R}_{>0}$  existe  $x \in A$  tal que  $0 < |x - a| < \delta$ .
- (b)  $a \in A'$  se, e somente se,  $0 \in B'$ , onde  $B := \{h \in \mathbb{R}_{\neq 0} : a + h \in A\}$ .

**Prova.**

(a)  $(\Rightarrow)$  blabla.

$(\Leftarrow)$  blabla. ■

- (b)  $(\Rightarrow)$  Para que 0 seja um ponto de acumulação de  $B$ , para todo  $\delta \in \mathbb{R}_{>0}$  deve existir  $h \in B$  tal que  $0 < |h - 0| < \delta$ . Bem, como  $a$  é um ponto de acumulação de  $A$ , para todo  $\delta \in \mathbb{R}_{>0}$  existe  $x \in A$  tal que  $0 < |x - a| < \delta$ .

Pois tomando  $h := x - a$ , temos que  $x = a + h$ , e como  $x \in A$ , temos  $a + h \in A$ , de modo que  $h \in B$ . Daí, segue a conclusão.

( $\Leftarrow$ ) Para que  $a$  seja um ponto de acumulação de  $A$ , para todo  $\delta \in \mathbb{R}_{>0}$  deve existir  $x \in A$  tal que  $0 < |x - a| < \delta$ . Bem, como  $0$  é ponto de acumulação de  $B$ , para todo  $\delta \in \mathbb{R}_{>0}$  existe  $h \in B$  tal que  $0 < |h| < \delta$ . Pois tome  $x := a + h$ : como  $h \in B$ , temos que  $a + h \in A$ , de modo que  $x \in A$ . Daí, segue a conclusão. ■

### Definição 7.5.

- (a) Diremos que  $a \in \mathbb{R}$  é um *ponto de acumulação à direita* de  $A \subseteq \mathbb{R}$  se  $(a, a + \delta) \cap A \neq \emptyset$  para todo  $\delta \in \mathbb{R}_{>0}$ .
- (b) Diremos que  $a \in \mathbb{R}$  é um *ponto de acumulação à esquerda* de  $A \subseteq \mathbb{R}$  se  $(a - \delta, a) \cap A \neq \emptyset$  para todo  $\delta \in \mathbb{R}_{>0}$ .

## 7.2 Limites

**Definição 7.6** (Limite). Uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  tem *limite*  $L \in \mathbb{R}$  quando  $x$  *tende a*  $a \in A'$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon$$

para todo  $x \in A$ . Isso é denotado por

$$\lim_{x \rightarrow a} f(x) = L.$$

**Proposição 7.7** (Unicidade).

**Prova.** ■

**Definição 7.8** (Limites laterais).

- (a) Diremos que uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  tem *limite lateral à direita*  $L \in \mathbb{R}$  quando  $x$  *tende ao ponto de acumulação à direita*  $a \in \mathbb{R}$  de  $A$ , indicando isso por

$$\lim_{x \rightarrow a^+} f(x) = L,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$a < x < a + \delta \Rightarrow |f(x) - L| < \epsilon$$

para todo  $x \in A$ .

- (b) Diremos que uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  tem *limite lateral à esquerda*  $L \in \mathbb{R}$  quando  $x$  *tende* ao ponto de acumulação à esquerda  $a \in \mathbb{R}$  de  $A$ , indicando isso por

$$\lim_{x \rightarrow a^-} f(x) = L,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$a - \delta < x < a \Rightarrow |f(x) - L| < \epsilon$$

para todo  $x \in A$ .

**Proposição 7.9** (Unicidade).

**Prova.** ■

**Teorema 7.10** (Bilateral  $\Leftrightarrow$  Laterais).

**Prova.** ■

**Definição 7.11.** (Limites no infinito)

- (a) Diremos que uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$ , onde  $A$  é ilimitado superiormente, tem limite  $L \in \mathbb{R}$  quando  $x$  *crece indefinidamente*, ou *tende ao infinito positivo*, indicando isso por

$$\lim_{x \rightarrow +\infty} f(x) = L,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon) \in \mathbb{R}_{>0}$  tal que

$$x > \delta \Rightarrow |f(x) - L| < \epsilon$$

para todo  $x \in A$ .

- (b) Diremos que uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$ , onde  $A$  é ilimitado inferiormente, tem limite  $L \in \mathbb{R}$  quando  $x$  *decresce indefinidamente*, ou *tende ao infinito negativo*, indicando isso por

$$\lim_{x \rightarrow -\infty} f(x) = L,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon) \in \mathbb{R}_{>0}$  tal que

$$x < -\delta \Rightarrow |f(x) - L| < \epsilon$$

para todo  $x \in A$ .

**Teorema 7.12. (a)** (Unicidade do Limite) Seja  $f$  uma função. O limite de  $f$  quando  $x \rightarrow p, p^\pm, \pm\infty$ , quando existe, é único, isto é, se  $\lim f(x) = L_1$  e  $\lim f(x) = L_2$ , então  $L_1 = L_2$ .

**(b)** (Bilateral  $\Leftrightarrow$  Laterais) Sejam  $f$  uma função e  $p$  um número real. Se existem números reais  $a$  e  $b$ , com  $a < p < b$ , tais que  $]a, p[$ ,  $]p, b[ \subset D_f$ , então

$$\lim_{x \rightarrow p} f(x) = L \in \mathbb{R} \Leftrightarrow \lim_{x \rightarrow p^+} f(x) = L = \lim_{x \rightarrow p^-} f(x).$$

**(c)** (Cálculo de Limites) Sejam  $f$  e  $g$  funções para as quais existe  $r > 0$  tal que  $f(x) = g(x)$  sempre que  $0 < |x - p| < r$  (caso  $x \rightarrow p$ ), ou  $p < x < p + r$  (caso  $x \rightarrow p^+$ ), ou  $p - r < x < p$  (caso  $x \rightarrow p^-$ ), ou  $x > r$  (caso  $x \rightarrow +\infty$ ), ou  $x < -r$  (caso  $x \rightarrow -\infty$ ). Nestas condições, se  $\lim f(x) = L \in \mathbb{R}$ , então  $\lim g(x) = L$ .

**(d)** (do *Confronto*) Sejam  $f$ ,  $g$  e  $h$  funções para as quais existe  $r > 0$  tal que  $f(x) \leq g(x) \leq h(x)$  sempre que  $0 < |x - p| < r$  (caso  $x \rightarrow p$ ), ou  $p < x < p + r$  (caso  $x \rightarrow p^+$ ), ou  $p - r < x < p$  (caso  $x \rightarrow p^-$ ), ou  $x > r$  (caso  $x \rightarrow +\infty$ ), ou  $x < -r$  (caso  $x \rightarrow -\infty$ ). Nestas condições, se  $\lim f(x) = \lim h(x) = L \in \mathbb{R}$ , então  $\lim g(x) = L$ .

**(e)** (Limites Básicos) Dados  $a, p \in \mathbb{R}$ , temos que

$$\lim_{x \rightarrow p} a = \lim_{x \rightarrow \pm\infty} a = a; \quad \lim_{x \rightarrow p} x = p; \quad \lim_{x \rightarrow \pm\infty} \frac{1}{x} = 0.$$

**Prova.** **(a)** Consideremos o caso em que  $x \rightarrow p$ . Como  $\lim_{x \rightarrow p} f(x) = L_1$  e  $\lim_{x \rightarrow p} f(x) = L_2$ , temos por definição que para todo  $\epsilon > 0$  existem  $\delta_1, \delta_2 > 0$  para os quais

$$\begin{aligned} 0 < |x - p| < \delta_1 &\Rightarrow |f(x) - L_1| < \frac{\epsilon}{2}; \\ 0 < |x - p| < \delta_2 &\Rightarrow |f(x) - L_2| < \frac{\epsilon}{2}. \end{aligned}$$

Tomando  $\delta := \min\{\delta_1, \delta_2\}$ , temos que para todo  $\epsilon > 0$  existe  $\delta > 0$  tal que

$$0 < |x - p| < \delta \Rightarrow |f(x) - L_1| + |f(x) - L_2| < \epsilon.$$

Com isso, temos que, para todo  $\epsilon > 0$ ,

$$\begin{aligned} |L_1 - L_2| &= |L_1 - f(x) + f(x) - L_2| \\ &\leq |L_1 - f(x)| + |f(x) - L_2| \\ &= |f(x) - L_1| + |f(x) - L_2| \\ &< \epsilon, \end{aligned}$$

donde  $L_1 = L_2$ . ■

**(b)**

(c)

(d) Consideremos o caso em que  $x \rightarrow p$ . Como, por hipótese,  $\lim_{x \rightarrow p} f(x) = L = \lim_{x \rightarrow p} h(x)$ , temos

$$\forall \epsilon > 0, \exists \delta_1 > 0 : 0 < |x - p| < \delta_1 \Rightarrow L - \epsilon < f(x) < L + \epsilon;$$

$$\forall \epsilon > 0, \exists \delta_2 > 0 : 0 < |x - p| < \delta_2 \Rightarrow L - \epsilon < h(x) < L + \epsilon.$$

Pois tome  $\delta = \min \{\delta_1, \delta_2, r\}$ ; daí, vem

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow L - \epsilon < f(x) \leq g(x) \leq h(x) < L + \epsilon,$$

e então

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow L - \epsilon < g(x) < L + \epsilon,$$

donde  $\lim_{x \rightarrow p} g(x) = L$ .

**Teorema 7.13.** (Propriedades Operatórias) Se  $f_1, f_2, \dots, f_n$  são funções tais que  $\lim f_1(x) = L_1, \lim f_2(x) = L_2, \dots, \lim f_n(x) = L_n$ , em que  $x \rightarrow p, p^\pm, \pm\infty$ , então:

(a) O limite da soma é igual à soma dos limites:

$$\lim \left[ \sum_{i=1}^n f_i(x) \right] = \sum_{i=1}^n [\lim f_i(x)] = \sum_{i=1}^n L_i = L_1 + L_2 + \dots + L_n.$$

(b) O limite do produto é igual ao produto dos limites:

$$\lim \left[ \prod_{i=1}^n f_i(x) \right] = \prod_{i=1}^n [\lim f_i(x)] = \prod_{i=1}^n L_i = L_1 \cdot L_2 \cdot \dots \cdot L_n.$$

(c) O limite do quociente é igual ao quociente dos limites, desde que o denominador seja diferente de 0:

$$\lim \frac{f_1(x)}{f_2(x)} = \frac{\lim f_1(x)}{\lim f_2(x)} = \frac{L_1}{L_2}. \quad (L_2 \neq 0)$$

**Prova.**

**Teorema 7.14.** (Composição de Limites) Sejam  $f$  e  $g$  funções tais que  $Im_f \subset D_g$  e  $\lim f(x) := a$ , com  $x \rightarrow p, \pm\infty$ .

(a) Se  $\lim_{u \rightarrow a} g(u) = g(a)$ , então

$$\lim g[f(x)] = \lim_{u \rightarrow a} g(u),$$

sendo  $u := f(x)$ .

(b) Se  $\lim_{u \rightarrow a} g(u) := L$  e  $a \notin D_g$ , então

$$\lim g[f(x)] = \lim_{u \rightarrow a} g(u),$$

sendo  $u := f(x)$ .

**Prova.**

**Observação 7.15.** Para o item (a) do teorema acima, como, por hipótese,  $\lim_{u \rightarrow a} g(u) = g(a)$ , podemos expressar o teorema como  $\lim g[f(x)] = g[\lim f(x)]$ .

**Corolário 7.16. (a)** (Conservação do sinal) Se  $\lim_{x \rightarrow p} f(x) := L \neq 0$ , então existe  $\delta > 0$  tal que, para todo  $x \in D_f$ , temos  $0 < |x - p| < \delta \Rightarrow f(x) \neq 0$ .

(b) Temos

$$\begin{aligned} \lim_{x \rightarrow p} f(x) = L &\Leftrightarrow \lim_{h \rightarrow 0} f(p + h) = L \\ &\Leftrightarrow \lim_{x \rightarrow p} [f(x) - L] = 0 \\ &\Leftrightarrow \lim_{x \rightarrow p} |f(x) - L| = 0. \end{aligned}$$

**Prova. (a)** Basta tomar  $\epsilon = L$ . ■

(b)

## 7.3 Continuidade

**Definição 7.17** (Continuidade). Seja  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função.

(a)  $f$  é *contínua* em  $a \in A$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$\forall x (x \in A \cap V_\delta(a) \Rightarrow f(x) \in V_\epsilon(f(a))),$$

ou ainda, equivalentemente,

$$\forall x (x \in A \wedge |x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon).$$

- (b)  $f$  é *contínua* em  $X \subseteq A$  se  $f$  é contínua em todos os pontos de  $X$ , isto é, se para cada  $a \in X$  e todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon$$

para todo  $x \in A$ .

- (c)  $f$  é *uniformemente contínua* em  $A$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon) \in \mathbb{R}_{>0}$  tal que

$$|x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$$

para quaisquer  $x, y \in A$ .

**Teorema 7.18.** Uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  é contínua em  $a \in A \cap A'$  se, e somente se,  $\lim_{x \rightarrow a} f(x) = f(a)$ .

**Prova.**

**Teorema 7.19.** Se  $f$  e  $g$  são funções contínuas em  $p$ , então as funções  $f + g$  e  $f \cdot g$  são contínuas em  $p$ ; e se  $g(p) \neq 0$ , então a função  $\frac{f}{g}$  é contínua em  $p$ .

**Prova.** Segue como corolário do Teorema (7.13).

**Proposição 7.20. (a)** Seja  $a \in \mathbb{R}$ . A função constante  $f(x) := a$  é contínua.

(b) A função identidade  $f(x) := x$  é contínua.

(c) Toda função polinomial é contínua. E ainda, toda função racional é contínua.

**Prova.**

**Teorema 7.21.** Sejam  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : B \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções tais que  $f(A) \subseteq B$ . Se  $f$  é contínua em  $a \in A$  e se  $g$  é contínua em  $f(a) \in B$ , então a função composta  $g \circ f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}$  é contínua em  $a$ .

**Teorema 7.22.** Sejam  $f$  e  $g$  funções tais que  $Im_f \subset D_g$ . Se  $f$  é contínua em  $p$  e  $g$  é contínua em  $f(p)$ , então a função composta  $(g \circ f)(x) = g[f(x)]$  é contínua em  $p$ .

**Prova.** Pois tome:  $\lim_{x \rightarrow p} g[f(x)] = g \left[ \lim_{x \rightarrow p} f(x) \right] = g[f(p)]$ .

**Teorema 7.23. (Intervalos)** Sejam  $f$  uma função e  $p \in D_f$  um número real.

(a) Se para todo  $\epsilon > 0$  existir um intervalo aberto  $]a, b[$ , com  $p \in ]a, b[$ , tal que  $\forall x \in D_f : x \in ]a, b[ \Rightarrow |f(x) - f(p)| < \epsilon$ , então  $f$  é contínua em  $p$ .

(b) Seja  $r > 0$ . Se para todo  $0 < \epsilon < r$  existir um intervalo aberto  $I$  (como no

item anterior, com  $p \in I$  tal que  $\forall x \in D_f : x \in I \Rightarrow |f(x) - f(p)| < \epsilon$ , então  $f$  é contínua em  $p$ .

**Prova. (a)** Segue imediatamente do seguinte fato: para todo intervalo  $]a, b[$ , existe  $\delta > 0$  tal que  $]p - \delta, p + \delta[ \subset ]a, b[$ . Com efeito, basta tomar  $\delta = \min\{b - p, p - a\}$ . Com isso, escolhendo esse  $\delta$ , temos que

$$x \in ]p - \delta, p + \delta[ \Rightarrow x \in ]a, b[.$$

Como, por hipótese,  $x \in ]a, b[ \Rightarrow |f(x) - f(p)| < \epsilon$ , temos então que

$$x \in ]p - \delta, p + \delta[ \Rightarrow |f(x) - f(p)| < \epsilon.$$

Como  $x \in ]p - \delta, p + \delta[ \Leftrightarrow |x - p| < \delta$ , vemos que para todo  $\epsilon > 0$  existe um  $\delta > 0$  tal que  $|x - p| < \delta \Rightarrow |f(x) - f(p)| < \epsilon$ , isto é,  $f$  é contínua em  $p$ . ■

**(b)** Pelo item anterior, se  $\epsilon < r$ , então nada há de ser provado. Temos que provar o resultado para todos os  $\epsilon$ 's, isto é, falta provar o caso  $\epsilon \geq r$ .

Pois tome  $\epsilon_1 < r$ . Para esse  $\epsilon_1$ , existe (por hipótese) um intervalo aberto  $I$  tal que  $x \in I \Rightarrow |f(x) - f(p)| < \epsilon_1$ . Como  $\epsilon_1 < \epsilon$ , também vale

$$x \in I \Rightarrow |f(x) - f(p)| < \epsilon,$$

o que completa a prova.

**Proposição 7.24** (Conservação do sinal). Seja  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função contínua em  $a \in A$ .

**(a)** Se  $f(a) > 0$ , então existe  $\delta \in \mathbb{R}_{>0}$  tal que  $f(x) > 0$  para todo  $x \in V_\delta(a) \cap A$ .

**(b)** Se  $f(a) < 0$ , então existe  $\delta \in \mathbb{R}_{>0}$  tal que  $f(x) < 0$  para todo  $x \in V_\delta(a) \cap A$ .

**Prova.**

**(a)** Para  $\epsilon = f(a)$  na definição de continuidade, existe  $\delta \in \mathbb{R}_{>0}$  tal que

$$\forall x(x \in V_\delta(a) \cap A \Rightarrow |f(x) - f(a)| < f(a)).$$

Observando que

$$|f(x) - f(a)| < f(a) \Leftrightarrow 0 = f(a) - f(a) < f(x) < 2f(a),$$

a conclusão segue. ■

**(b)** Tomando  $\epsilon = -f(a)$ , segue analogamente. ■

## 7.4 Limites Infinitos

**Definição 7.25.** (Limites infinitos quando  $x \rightarrow \pm\infty$ ) Seja  $f$  uma função.

(a) Suponha que existe um número real  $a$  tal que  $]a, +\infty[ \subset D_f$ .

- i. Diremos que  $f$  *cresce indefinidamente*, ou *tende ao infinito positivo*, quando  $x$  tende ao infinito positivo, indicando  $\lim_{x \rightarrow +\infty} f(x) = +\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $\delta > a$ , tal que  $x > \delta \Rightarrow f(x) > \epsilon$ .
- ii. Diremos que  $f$  *decresce indefinidamente*, ou *tende ao infinito negativo*, quando  $x$  tende ao infinito positivo, indicando  $\lim_{x \rightarrow +\infty} f(x) = -\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $\delta > a$ , tal que  $x > \delta \Rightarrow f(x) < -\epsilon$ .

(b) Suponha que existe um número real  $a$  tal que  $] -\infty, a[ \subset D_f$ .

- i. Diremos que  $f$  *tende ao infinito positivo*, quando  $x$  tende ao infinito negativo, indicando  $\lim_{x \rightarrow -\infty} f(x) = +\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $-\delta < a$ , tal que  $x < -\delta \Rightarrow f(x) > \epsilon$ .
- ii. Diremos que  $f$  *tende ao infinito negativo*, quando  $x$  tende ao infinito negativo, indicando  $\lim_{x \rightarrow -\infty} f(x) = -\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $-\delta < a$ , tal que  $x < -\delta \Rightarrow f(x) < -\epsilon$ .

**Definição 7.26.** (Limites infinitos quando  $x \rightarrow p^\pm$ ) Seja  $f$  uma função e  $p$  um número real.

(a) Suponha que existe um número real  $b$  tal que  $]p, b[ \subset D_f$ .

- i. Diremos que  $f$  *tende ao infinito positivo*, quando  $x$  tende a  $p$ , pela direita, indicando  $\lim_{x \rightarrow p^+} f(x) = +\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $p + \delta < b$ , tal que  $p < x < p + \delta \Rightarrow f(x) > \epsilon$ .
- ii. Diremos que  $f$  *tende ao infinito negativo*, quando  $x$  tende a  $p$ , pela direita, indicando  $\lim_{x \rightarrow p^+} f(x) = -\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $p + \delta < b$ , tal que  $p < x < p + \delta \Rightarrow f(x) < -\epsilon$ .

(b) Suponha que existe um número real  $a$  tal que  $]a, p[ \subset D_f$ .

- i. Diremos que  $f$  *tende ao infinito positivo*, quando  $x$  tende a  $p$ , pela esquerda, indicando  $\lim_{x \rightarrow p^-} f(x) = +\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $a < p - \delta$ , tal que  $p - \delta < x < p \Rightarrow f(x) > \epsilon$ .

- ii. Diremos que  $f$  tende ao infinito negativo, quando  $x$  tende a  $p$ , pela esquerda, indicando  $\lim_{x \rightarrow p^-} f(x) = -\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $a < p - \delta$ , tal que  $p - \delta < x < p \Rightarrow f(x) < -\epsilon$ .

**Definição 7.27.** (Limites infinitos quando  $x \rightarrow p$ ) Seja  $f$  uma função e  $p$  um número real. Suponha que existem números reais  $a$  e  $b$ , com  $a < p < b$ , tais que  $]a, p[ , ]p, b[ \subset D_f$ .

- i. Diremos que  $f$  tende ao infinito positivo, quando  $x$  tende a  $p$ , indicando  $\lim_{x \rightarrow p} f(x) = +\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $a < p - \delta$  e  $p + \delta < b$ , tal que  $0 < |x - p| < \delta \Rightarrow f(x) > \epsilon$ .
- ii. Diremos que  $f$  tende ao infinito negativo, quando  $x$  tende a  $p$ , indicando  $\lim_{x \rightarrow p} f(x) = -\infty$ , se para todo  $\epsilon > 0$  existir  $\delta > 0$ , com  $a < p - \delta$  e  $p + \delta < b$ , tal que  $0 < |x - p| < \delta \Rightarrow f(x) < -\epsilon$ .

**Teorema 7.28.** Seja  $f$  uma função e  $p$  um número real. Se existem números reais  $a$  e  $b$ , com  $a < p < b$ , tais que  $]a, p[ , ]p, b[ \subset D_f$ , então

$$\lim_{x \rightarrow p} f(x) = \pm\infty \Leftrightarrow \lim_{x \rightarrow p^+} f(x) = \pm\infty = \lim_{x \rightarrow p^-} f(x).$$

**Prova.**

**Teorema 7.29.** Os resultados a seguir valem para  $x \rightarrow p$ ,  $x \rightarrow p^\pm$  e  $x \rightarrow \pm\infty$ .

- (a) Se  $\lim f(x) = \lim g(x) = \pm\infty$ , então  $\lim[f(x) + g(x)] = \pm\infty$  e  $\lim[f(x)g(x)] = +\infty$ .
- (b) Se  $\lim f(x) = -\infty$  e  $\lim g(x) = +\infty$ , então  $\lim[f(x)g(x)] = -\infty$ .
- (c) Seja  $\lim f(x) = L$ . Se  $\lim g(x) = \pm\infty$ , então  $\lim[f(x) + g(x)] = \pm\infty$ .
- (d) Seja  $\lim f(x) = L > 0$ . Se  $\lim g(x) = \pm\infty$ , então  $\lim[f(x)g(x)] = \pm\infty$ .
- (e) Seja  $\lim f(x) = L < 0$ . Se  $\lim g(x) = \pm\infty$ , então  $\lim[f(x)g(x)] = \mp\infty$ .

**Prova.**

**Proposição 7.30.** (a) Seja  $\lim f(x) = 0$ , com  $x \rightarrow p^\pm$ . Se existe  $r > 0$  tal que  $f(x) > 0$  sempre que  $p < x < p + r$ , se  $x \rightarrow p^+$ , ou  $p - r < x < p$ , se  $x \rightarrow p^-$ , então  $\lim \frac{1}{f(x)} = +\infty$ .

(b) Sejam  $\lim f(x) = L \neq 0$  e  $\lim g(x) = 0$ , com  $x \rightarrow p^\pm$ . Se existe  $r > 0$  tal que  $f(x) > 0$  sempre que  $p < x < p + r$ , se  $x \rightarrow p^+$ , ou  $p - r < x < p$ , se  $x \rightarrow p^-$ ,

então ou  $\lim \frac{f(x)}{g(x)} = +\infty$ , ou  $\lim \frac{f(x)}{g(x)} = -\infty$ , ou  $\lim \frac{f(x)}{g(x)}$  não existe.

**Prova.**

## 7.5 Limites e Sequências

**Definição 7.31. (c)** Diremos que  $(x_n)_{n \in \mathbb{N}}$

1. *diverge* para  $+\infty$ , indicando

$$\lim_{n \rightarrow +\infty} x_n = +\infty,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $n_0 \in \mathbb{N}$  tal que  $n > n_0 \Rightarrow x_n > \epsilon$ .

2. *diverge* para  $-\infty$ , indicando

$$\lim_{n \rightarrow +\infty} x_n = -\infty,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $n_0 \in \mathbb{N}$  tal que  $n > n_0 \Rightarrow x_n < -\epsilon$ .

**Observação 7.32. (a)** Note que as definições acima são análogas àquelas que demos aos limites no infinito de funções. Assim, os resultados sobre os limites da forma  $\lim_{x \rightarrow +\infty} f(x)$  também são válidos para os limites da forma  $\lim_{x \rightarrow +\infty} x_n$ .

**(b)** A notação “ $x_n \rightarrow a$  quando  $n \rightarrow +\infty$ ” também é frequentemente usada para indicar  $\lim_{n \rightarrow +\infty} x_n = a$ . Quando não houver confusão, podemos escrever simplesmente  $x_n \rightarrow a$ . Analogamente, também podemos escrever  $x_n \rightarrow \pm\infty$  quando  $n \rightarrow \infty$  ou, simplesmente,  $x_n \rightarrow \pm\infty$ .

**Teorema 7.33. (Convergência Monótona)**

**(a)** Toda sequência crescente e limitada superiormente é convergente.

**(b)** Toda sequência decrescente e limitada inferiormente é convergente.

**Prova. (a)** Seja  $(x_n)_{n \in \mathbb{N}}$  uma sequência crescente e limitada superiormente. Como o conjunto  $X := \{x_n \mid n \in \mathbb{N}\}$  é, por hipótese, não vazio e limitado superiormente, pela propriedade do supremo existe  $\sup X$ . Como, para todo  $\epsilon \in \mathbb{R}_{>0}$ ,  $\sup X - \epsilon$  não é uma cota superior de  $X$ , existe  $n_0 \in \mathbb{N}$  tal que  $\sup X - \epsilon < x_{n_0} \leq \sup X$ . Como  $(x_n)_{n \in \mathbb{N}}$  é crescente, para todo  $n \in \mathbb{N}$ , se  $n > n_0$ , então  $\sup X - \epsilon < x_{n_0} \leq x_n \leq \sup X < \sup X + \epsilon$ . Temos então que  $x_n \rightarrow \sup X$ , isto é,  $(x_n)_{n \in \mathbb{N}}$  converge para  $\sup X$ . ■

(b) Segue analogamente: sendo  $(x_n)_{n \in \mathbb{N}}$  uma sequência decrescente e limitada inferiormente, basta provar que  $x_n \rightarrow \inf \{x_n : n \in \mathbb{N}\}$ .

**Teorema 7.34.** (Bolzano-Weierstrass) Toda sequência limitada possui uma subsequência convergente.

**Prova.** Pelo teorema (7.33), basta mostrar que toda sequência possui uma subsequência monótona. Seja  $(x_n)_{n \in \mathbb{N}}$  uma sequência limitada. Um índice  $k \in \mathbb{N}$  é dito *básico* quando  $x_p \geq x_k$  para todo  $p > k$ , isto é,  $x_k$  é menor ou igual aos termos que o sucedem.

- Se existem infinitos índices básicos  $n_1 < n_2 < n_3 < \dots$ , então  $x_{n_1} \leq x_{n_2} \leq x_{n_3} \leq \dots$ , de modo que a subsequência  $(x_{n_i})_{i \in \mathbb{N}}$  é crescente; como ela é limitada, pelo teorema (7.33), ela é convergente.
- Por outro lado, se o número de índices básicos é finito, seja  $n_1 \in \mathbb{N}$  maior que todos eles (se o número de índices básicos for 0, qualquer  $n_1$  funciona). Como  $n_1$  não é um índice básico, existe um índice  $n_2 \in \mathbb{N}_{>n_1}$  tal que  $x_{n_2} < x_{n_1}$ . Como  $n_2$  não é um índice básico, existe um índice  $n_3 \in \mathbb{N}_{>n_2}$  tal que  $x_{n_3} < x_{n_2}$ . Prosseguindo deste modo, obtemos uma subsequência  $(x_{n_i})_{i \in \mathbb{N}}$  estritamente decrescente; como ela é limitada, pelo teorema (7.33), ela é convergente.

Com isso, toda sequência possui uma subsequência monótona, e como a sequência original é limitada, a subsequência monótona também é, sendo, portanto, convergente.

**Teorema 7.35.** Seja  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função e  $a \in A$ . As seguintes afirmações são equivalentes:

- $f$  é contínua em  $a$ ;
- toda sequência  $(x_n)_{n \in \mathbb{N}}$ , com  $x_n \in A$  para todo  $n \in \mathbb{N}$ , satisfaz

$$x_n \rightarrow a \Rightarrow f(x_n) \rightarrow f(a).$$

**Prova.**

**Teorema 7.36.** Toda função  $f : [a, b] \rightarrow \mathbb{R}$  contínua em  $[a, b]$  é uniformemente contínua em  $[a, b]$ .

**Prova.** Suponha que exista uma função  $f$  contínua em  $[a, b]$  que não seja uniformemente contínua em  $[a, b]$ . Negando a definição de continuidade uniforme (7.17), isso significa que existe  $\epsilon_0 \in \mathbb{R}_{>0}$  tal que, para todo  $\delta \in \mathbb{R}_{>0}$ , existem  $x, y \in [a, b]$  tais que  $|x - y| < \delta$  e  $|f(x) - f(y)| \geq \epsilon_0$ . Em particular, escolhendo  $\delta_n = \frac{1}{n}$  para cada  $n \in \mathbb{N}$ , existem  $x_n, y_n \in [a, b]$  tais que  $|x_n - y_n| < \frac{1}{n}$  e

$|f(x_n) - f(y_n)| \geq \epsilon_0$ ; definimos, assim, duas sequências  $(x_n)_{n \in \mathbb{N}}$  e  $(y_n)_{n \in \mathbb{N}}$ . Como  $x_n \in [a, b]$  para todo  $n \in \mathbb{N}$ , a sequência  $(x_n)_{n \in \mathbb{N}}$  é limitada, de modo que, pelo teorema de Bolzano-Weierstrass (7.34), existe uma subsequência  $(x_{n_k})_{k \in \mathbb{N}}$  que converge para algum  $L \in [a, b]$ , isto é,  $x_{n_k} \rightarrow L$ . Considerando a subsequência correspondente  $(y_{n_k})_{k \in \mathbb{N}}$ , temos, para todo  $k \in \mathbb{N}$ ,

$$|x_{n_k} - y_{n_k}| < \frac{1}{n_k}.$$

Como  $n_k \rightarrow +\infty$  (pois  $(n_k)_{k \in \mathbb{N}}$  é uma sequência de índices), temos que  $\frac{1}{n_k} \rightarrow 0$ , de modo que

$$\lim_{k \rightarrow +\infty} |x_{n_k} - y_{n_k}| = 0.$$

Com isso, sendo  $x_{n_k} \rightarrow L$ , só pode ser  $y_{n_k} \rightarrow L$ . Como  $f$  é contínua em  $L \in [a, b]$ , pelo teorema (7.35) temos que

$$\lim_{k \rightarrow +\infty} f(x_{n_k}) = f(L) \quad \text{e} \quad \lim_{k \rightarrow +\infty} f(y_{n_k}) = f(L),$$

de modo que  $\lim_{k \rightarrow +\infty} |f(x_{n_k}) - f(y_{n_k})| = 0$ , o que contraria a hipótese de ser  $|f(x_{n_k}) - f(y_{n_k})| \geq \epsilon_0 > 0$  para todo  $k \in \mathbb{N}$ . Assim, uma tal função  $f$  não pode existir.

**Teorema 7.37.** Se  $(a_n)_{n \geq 0}$  e  $(b_n)_{n \geq 0}$  são sequências tais que  $\lim_{n \rightarrow +\infty} (b_n - a_n) = 0$  e, para todo  $n \in \mathbb{N}$ ,  $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ , então existe um único  $\alpha \in \mathbb{R}$  tal que, para todo  $n \in \mathbb{N}$ ,  $a_n \leq \alpha \leq b_n$ .

**Prova.** (Existência) A segunda condição nos diz que  $(a_n)_{n \geq 0}$  é crescente (pois  $a_n \leq a_{n+1}$ ) e limitada superiormente (pois todo  $b_n$  é uma cota superior dessa sequência). Analogamente,  $(b_n)_{n \geq 0}$  é decrescente e limitada inferiormente. Assim, pelo Teorema (7.33), existem  $\alpha := \lim_{n \rightarrow +\infty} a_n$  e  $\beta := \lim_{n \rightarrow +\infty} b_n$ , e então  $0 = \lim_{n \rightarrow +\infty} (b_n - a_n) = \alpha - \beta$ , donde  $\alpha = \beta$ . Ainda pelo Teorema (7.33),  $\alpha = \sup\{a_n \mid n \in \mathbb{N}\}$ , e então, para todo  $n \in \mathbb{N}$ ,  $a_n \leq \alpha$ . Analogamente,  $\alpha = \beta = \inf\{b_n \mid n \in \mathbb{N}\}$ , e então, para todo  $n \in \mathbb{N}$ , temos que  $\alpha \leq b_n$ . Logo, existe um  $\alpha \in \mathbb{R}$  tal que, para todo  $n \in \mathbb{N}$ ,  $a_n \leq \alpha \leq b_n$ .

(Unicidade) Suponha que existe  $\alpha_1 \in \mathbb{R}$  para o qual também vale  $a_n \leq \alpha_1 \leq b_n$ . Daí,  $0 \leq \alpha_1 - a_n \leq b_n - a_n$ ; observando que  $\lim_{n \rightarrow +\infty} 0 = 0$  e  $\lim_{n \rightarrow +\infty} (b_n - a_n) = 0$ , temos, pelo Teorema do Confronto, que  $0 = \lim_{n \rightarrow +\infty} (\alpha_1 - a_n) = \alpha_1 - \alpha$ , isto é,  $\alpha_1 = \alpha$ . Logo, é único o  $\alpha \in \mathbb{R}$  tal que, para todo  $n \in \mathbb{N}$ ,  $a_n \leq \alpha \leq b_n$ .

**Corolário 7.38.** (Intervalos Encaixantes) Se  $([a_n, b_n])_{n \geq 0}$  for uma sequência de intervalos fechados em que, para todo  $n \in \mathbb{N}$ ,  $[a_n, b_n] \supset [a_{n+1}, b_{n+1}]$ , e  $\lim_{n \rightarrow +\infty} (b_n - a_n) = 0$ , então o conjunto  $\bigcap_{n=0}^{\infty} [a_n, b_n]$  é unitário.

**Prova.** Este enunciado é equivalente ao enunciado do Teorema (7.37).

**Corolário 7.39.** Se  $([a_n, b_n])_{n \geq 0}$  for uma sequência de intervalos encaixantes, com  $a_n, b_n \geq 0$ , então  $([a_n^m, b_n^m])_{n \geq 0}$ , com  $m \geq 2$  natural, também será uma sequência de intervalos encaixantes.

**Prova.** Basta ver que, para todo  $n \in \mathbb{N}$ ,

$$\begin{aligned} [a_n, b_n] \supset [a_{n+1}, b_{n+1}] &\Leftrightarrow a_n \leq a_{n+1} \leq b_{n+1} \leq b_n \\ &\Leftrightarrow a_n^m \leq a_{n+1}^m \leq b_{n+1}^m \leq b_n^m \\ &\Leftrightarrow [a_n^m, b_n^m] \supset [a_{n+1}^m, b_{n+1}^m], \end{aligned}$$

e ainda,

$$\begin{aligned} \lim_{n \rightarrow +\infty} (b_n^m - a_n^m) &= \left( \lim_{n \rightarrow +\infty} b_n \right)^m - \left( \lim_{n \rightarrow +\infty} a_n \right)^m \\ &= \left( \lim_{n \rightarrow +\infty} a_n \right)^m - \left( \lim_{n \rightarrow +\infty} a_n \right)^m = 0. \end{aligned}$$

Logo,  $([a_n^m, b_n^m])_{n \geq 0}$  é de intervalos encaixantes.

Ademais, se  $\alpha$  é o real que satisfaz, para todo  $k \in \mathbb{N}$ ,  $a_k \leq \alpha \leq b_k$ , então  $\alpha^m$  é o real que satisfaz, para todo  $k \in \mathbb{N}$ ,  $a_k^m \leq \alpha^m \leq b_k^m$ .<sup>1</sup>

## 7.6 Teoremas do Valor Intermediário e de Weierstrass

**Teorema 7.40 (Bolzano).** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função contínua em  $[a, b]$ . Se  $f(a) \cdot f(b) < 0$ , então existe  $c \in (a, b)$  tal que  $f(c) = 0$ .

**Prova.** Suponha, sem perda de generalidade, que  $f(a) < 0$  e  $f(b) > 0$ . Pois tome

$$S := \{x \in [a, b] : f(x) \leq 0\}.$$

Temos  $S \neq \emptyset$  pois  $a \in S$  já que  $f(a) < 0$ .  $S$  é limitado pois  $S \subseteq [a, b]$ . Assim, existe  $p := \sup S$ . Provemos que  $f(p) = 0$ . De fato, pela tricotomia de  $<$  em  $\mathbb{R}$ , ou  $f(p) > 0$ , ou  $f(p) < 0$ , ou  $f(p) = 0$ .

- Se fosse  $f(p) > 0$ , pela conservação do sinal existiria  $\delta \in \mathbb{R}_{>0}$  tal que  $f(x) > 0$  para todo  $x \in (p - \delta, p + \delta) \cap [a, b]$ . Com isso, se  $x \in S$ , então  $x \leq p - \delta$ , de modo que  $p - \delta$  é uma cota superior de  $S$ , uma contradição pois  $p - \delta < p = \sup S$ .

<sup>1</sup>Prove! O argumento é semelhante ao argumento da unicidade no Teorema (7.37).

- Se fosse  $f(p) < 0$ , pela conservação do sinal existiria  $\delta \in \mathbb{R}_{>0}$  tal que  $f(x) < 0$  para todo  $x \in (p - \delta, p + \delta) \cap [a, b]$ . Em particular, se  $x \in (p, p + \delta) \cap [a, b]$ , então  $f(x) > 0$  e  $x \in S$ , uma contradição pois  $x > p = \sup S$ .

Logo, só pode ser  $f(p) = 0$ . Além disso, como  $p \in [a, b]$  e  $f(a) < 0$  e  $f(b) > 0$ , temos que  $p \in (a, b)$ . ■

**Prova.** Suponha, sem perda de generalidade, que  $f(a) < 0$  e  $f(b) > 0$ . Construa-mos uma sequência de intervalos  $([a_n, b_n])_{n \geq 0}$  recursivamente do seguinte modo:  $a_0 := a, b_0 := b$  e

$$\begin{cases} a_{n+1} := \frac{a_n + b_n}{2} \text{ e } b_{n+1} := b_n, & \text{se } f\left(\frac{a_n + b_n}{2}\right) < 0 \\ a_{n+1} := a_n \text{ e } b_{n+1} := \frac{a_n + b_n}{2}, & \text{se } f\left(\frac{a_n + b_n}{2}\right) \geq 0. \end{cases}$$

É fácil ver que, para todo  $n \in \mathbb{N}$ , temos  $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$  e  $\lim_{n \rightarrow +\infty} (b_n - a_n) = 0$ . Com isso,  $([a_n, b_n])_{n \geq 0}$  é uma sequência de intervalos encaixantes, de modo que existe um único  $c \in [a, b]$  tal que, para todo  $n \in \mathbb{N}$ ,  $a_n \leq c \leq b_n$ . Em particular, temos que  $f(a_n) < 0 \leq f(b_n)$  para todo  $n \in \mathbb{N}$ .

Pela continuidade de  $f$ ,  $\lim_{n \rightarrow +\infty} f(a_n) = f(c)$  e  $\lim_{n \rightarrow +\infty} f(b_n) = f(c)$ , e como  $f(a_n) < 0 \leq f(b_n)$  para todo  $n \in \mathbb{N}$ , temos, pelo Teorema do Confronto, que  $f(c) = 0$ .

**Teorema 7.41** (Valor Intermediário). Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função contínua em  $[a, b]$ .

- Se  $f(a) \leq f(b)$ , então para todo  $\gamma \in [f(a), f(b)]$  existe  $c \in [a, b]$  tal que  $f(c) = \gamma$ .
- Se  $f(b) \leq f(a)$ , então para todo  $\gamma \in [f(b), f(a)]$  existe  $c \in [a, b]$  tal que  $f(c) = \gamma$ .
- Para todo  $\gamma \in [\min\{f(a), f(b)\}, \max\{f(a), f(b)\}]$  existe  $c \in [a, b]$  tal que  $f(c) = \gamma$ .

**Prova.** Pois tome  $g(x) := f(x) - \alpha$ , com  $x \in [a, b]$ . Como  $f$  é contínua em  $[a, b]$ ,  $g$  também o é. Em particular,  $g(a) = f(a) - \alpha < 0$  e  $g(b) = f(b) - \alpha > 0$ , de modo que, pelo Teorema do Anulamento, existe  $c \in [a, b]$  tal que  $g(c) = 0$ , isto é,  $f(c) = \alpha$ .

**Teorema 7.42.** (Limitação) Se uma função  $f : [a, b] \rightarrow \mathbb{R}$  é contínua em  $[a, b]$ , então  $f$  é limitada em  $[a, b]$ .

**Prova.** Suponhamos, por absurdo, que  $f$  não seja limitada em  $[a, b]$ . Colocando

$a_0 := a$  e  $b_0 := b$ , existe  $x_0 \in [a_0, b_0]$  tal que  $|f(x_0)| > 0$ . Suponha, indutivamente, que  $[a_n, b_n] \subset [a_0, b_0]$  esteja bem definido, sendo  $f$  não limitada em  $[a_n, b_n]$ . Em particular, existe  $x_n \in [a_n, b_n]$  tal que  $|f(x_n)| > n$ . Agora, defina  $a_{n+1} := a_n$  e  $b_{n+1} := \frac{a_n + b_n}{2}$ , se  $f$  não for limitada em  $\left[a_n, \frac{a_n + b_n}{2}\right]$ , ou  $a_{n+1} := \frac{a_n + b_n}{2}$  e  $b_{n+1} := b_n$  se  $f$  não for limitada em  $\left[\frac{a_n + b_n}{2}, b_n\right]$ . No intervalo em que  $f$  não for limitada, existirá  $x_{n+1}$  nesse intervalo tal que  $|f(x_{n+1})| > n + 1$ .

Assim, fica construída uma sequência  $([a_n, b_n])_{n \geq 0}$  de intervalos encaixantes tal que, para todo  $n \in \mathbb{N}$ , existe  $x_n \in [a_n, b_n]$  com  $|f(x_n)| > n$ . Em particular, isso significa que  $\lim_{n \rightarrow +\infty} |f(x_n)| = +\infty$ . Agora, sendo  $c$  o único real tal que  $a_n \leq c \leq b_n$  para todo  $n \in \mathbb{N}$ , pelo Teorema do Confronto temos que  $x_n \rightarrow c$ , e sendo  $f$  contínua em  $c$ , temos que  $\lim_{n \rightarrow +\infty} |f(x_n)| = |f(c)|$ , absurdo! Logo,  $f$  não ser limitada em  $[a, b]$  nos leva a uma contradição, de modo que  $f$  é, então, limitada em  $[a, b]$ .

**Teorema 7.43** (Valor Extremo, ou Weierstrass). Se uma função  $f : [a, b] \rightarrow \mathbb{R}$  é contínua em  $[a, b]$ , então existem  $x_1, x_2 \in [a, b]$  tais que  $f(x_1) \leq f(x) \leq f(x_2)$  para todo  $x \in [a, b]$ .

**Prova.** Pelo teorema da limitação (7.42),  $f$  é limitada em  $[a, b]$ , de modo que o conjunto  $A := \{f(x) : x \in [a, b]\}$  admite  $M := \sup A$  e  $m := \inf A$ . Isto significa que  $m \leq f(x) \leq M$  para todo  $x \in [a, b]$ . Afirmamos que existe  $x_2 \in [a, b]$  para o qual  $M = f(x_2)$ . De fato, se um tal  $x_2$  não existisse, seria  $f(x) < M$  para todo  $x \in [a, b]$ , de modo que a função  $g(x) := \frac{1}{M - f(x)}$ , com  $x \in [a, b]$ , seria contínua, mas não limitada, em  $[a, b]$ , o que é uma contradição (se  $g$  fosse limitada, então existiria  $\gamma > 0$  tal que  $0 < \frac{1}{M - f(x)} < \gamma$ , donde  $f(x) < M - \frac{1}{\gamma}$ , de modo que  $M$  não seria supremo de  $A$ ). Assim, não pode ser  $f(x) < M$ , e como  $f(x) \leq M$ , existirá  $x_2 \in [a, b]$  para o qual  $f(x_2) = M$ . Analogamente, prova-se que existe  $x_1 \in [a, b]$  para o qual  $f(x_1) = m$ .

## 7.7 Algumas Funções Transcendentais

### 7.7.1 Trigonometria, parte I

**Teorema 7.44.** Existe um único par de funções,  $s, c : \mathbb{R} \rightarrow \mathbb{R}$ , para as quais

- $s(0) = 0$  e  $c(0) = 1$ ;
- $\forall x \forall y : s(x - y) = s(x)c(y) - s(y)c(x)$  e  $c(x - y) = c(x)c(y) + s(x)s(y)$ ;
- $\exists r > 0 : 0 < x < r \Rightarrow 0 < s(x) < x < \frac{s(x)}{c(x)}$ .

A função  $s$  é chamada de *seno* e será indicada por  $\sin x$ , enquanto  $c$  é chamada de *co seno* e será indicada por  $\cos x$ .

**Prova.**

**Proposição 7.45. (a)** (Identidade Fundamental) Temos  $\sin^2 x + \cos^2 x = 1$  para todo  $x \in \mathbb{R}$ .

**(b)**  $\sin$  é uma função ímpar, isto é,  $\sin -x = -\sin x$  para todo  $x \in \mathbb{R}$ , enquanto  $\cos$  é uma função par, isto é,  $\cos -x = \cos x$  para todo  $x \in \mathbb{R}$ .

**(c)** Temos, para todos  $x, y \in \mathbb{R}$ ,

$$\sin(x + y) = \sin x \cos y + \sin y \cos x$$

$$\cos(x + y) = \cos x \cos y - \sin x \sin y$$

**(d)** Temos  $\sin 2x = 2 \sin x \cos x$  e  $\cos 2x = \cos^2 x - \sin^2 x$  para todo  $x \in \mathbb{R}$ .

**(e)** Temos  $\sin^2 x = \frac{1}{2} - \frac{1}{2} \cos 2x$  e  $\cos^2 x = \frac{1}{2} + \frac{1}{2} \cos 2x$  para todo  $x \in \mathbb{R}$ .

**Prova.**

**Teorema 7.46.** As funções  $\sin$  e  $\cos$  são contínuas em  $\mathbb{R}$ .

**Prova.** Pelo terceiro item no resultado (7.44), existe  $r > 0$  tal que  $|x| < r \Rightarrow |\sin x| \leq |x|$ . Usaremos isso para provar que  $|x - p| < 2r \Rightarrow |\sin x - \sin p| \leq |x - p|$ . Pois tome:

$$\begin{aligned} |\sin x - \sin p| &= \left| 2 \sin \left( \frac{x - p}{2} \right) \cos \left( \frac{x + p}{2} \right) \right| \\ &= 2 \left| \sin \left( \frac{x - p}{2} \right) \right| \left| \cos \left( \frac{x + p}{2} \right) \right|; \end{aligned}$$

como  $\left| \cos \left( \frac{x + p}{2} \right) \right| \leq 1$ , temos que

$$|\sin x - \sin p| \leq 2 \left| \sin \left( \frac{x - p}{2} \right) \right|,$$

e então, pelo fato mencionado acima, vem

$$|x - p| < 2r \Rightarrow \left| \sin \left( \frac{x - p}{2} \right) \right| \leq \left| \frac{x - p}{2} \right|,$$

donde  $|x - p| < 2r \Rightarrow |\sin x - \sin p| \leq |x - p|$ . De maneira completamente análoga, prova-se que  $|x - p| < 2r \Rightarrow |\cos x - \cos p| \leq |x - p|$ .

Com isso,  $|x - p| < 2r \Rightarrow 0 \leq |\sin x - \sin p| \leq |x - p|$ , e como  $\lim_{x \rightarrow p} |x - p| = 0$ , pelo Teorema do Confronto vem  $\lim_{x \rightarrow p} |\sin x - \sin p| = 0$ , donde  $\lim_{x \rightarrow p} \sin x = \sin p$ . De modo completamente análogo, prova-se que  $\lim_{x \rightarrow p} \cos x = \cos p$ . Logo,  $\sin$  e  $\cos$  são contínuas em todo  $p \in \mathbb{R}$ .

**Teorema 7.47.** Temos  $\lim_{x \rightarrow 0} \frac{\sin x}{x} = 1$  e  $\lim_{x \rightarrow 0} \frac{1 - \cos x}{x} = 0$ .

**Prova.**

## 7.7.2 Exponencial e Logaritmo

### Expoentes Racionais

O intuito aqui é definir  $a^x$  quando  $x \in \mathbb{Q}$ . A referência é [10].

**Teorema 7.48.**

- (a) Para quaisquer  $a \in \mathbb{R}_{>0}$  e  $n \in \mathbb{N}_{\geq 2}$  existe um único  $x \in \mathbb{R}_{>0}$  tal que  $x^n = a$ .
- (b) Para quaisquer  $a \in \mathbb{R}$  e  $n \in \mathbb{N}$  ímpar existe um único  $x \in \mathbb{R}$  tal que  $x^n = a$ .

**Prova.** (a) Iremos construir duas seqüências,  $(a_k)_{k \geq 0}$  e  $(b_k)_{k \geq 0}$ , no sentido dos Teoremas (7.37) e (7.38).

Seja  $A_0$  o maior natural tal que  $A_0^n \leq a < (A_0 + 1)^n$ . Em particular, isso nos diz que, se o real  $x > 0$  existe, então ele satisfaz  $A_0 \leq x < A_0 + 1$ . Agora, para cada  $k \geq 1$ , seja  $A_k$  um elemento do conjunto  $\{0, 1, \dots, 9\}$  (isto é,  $A_k$  é um *dígito*, ou *algarismo*), e defina  $(a_k)_{k \geq 0}$  e  $(b_k)_{k \geq 0}$  por

$$a_k := \max \left\{ \sum_{i=0}^k \frac{A_i}{10^i} \mid \left( \sum_{i=0}^k \frac{A_i}{10^i} \right)^n \leq a \right\}, \forall k \geq 0$$

$$b_k := \begin{cases} A_0 + 1, & \text{se } k = 0 \\ a_{k-1} + \frac{A_k + 1}{10^k}, & \text{se } k \geq 1 \end{cases}$$

É imediato que, para todo  $k \in \mathbb{N}$ ,  $a_k^n \leq a < b_k^n$ . Em particular, isso nos diz que, se o real  $x > 0$  existe, então ele satisfaz  $a_k \leq x < b_k$ . Provemos agora que  $a_k \leq a_{k+1} \leq b_{k+1} \leq b_k$ :

i.  $a_k \leq a_{k+1}$ : para ver isso, basta ver que

$$a_{k+1} = \sum_{i=0}^{k+1} \frac{A_i}{10^i} = \sum_{i=0}^k \frac{A_i}{10^i} + \frac{A_{k+1}}{10^{k+1}} = a_k + \frac{A_{k+1}}{10^{k+1}}.$$

Daí,  $a_{k+1} - a_k = \frac{A_{k+1}}{10^{k+1}} \geq 0 \Rightarrow a_k \leq a_{k+1}$ .

ii.  $a_{k+1} \leq b_{k+1}$ : releia uma das afirmações ditas acima.

iii.  $b_k \leq b_{k+1}$ : basta ver que

$$\begin{aligned} b_k - b_{k+1} &= \left( a_{k-1} + \frac{A_k + 1}{10^k} \right) - \left( a_k + \frac{A_{k+1} + 1}{10^{k+1}} \right) \\ &= \left( a_{k-1} + \frac{A_k + 1}{10^k} \right) - \left( a_{k-1} + \frac{A_k}{10^k} + \frac{A_{k+1} + 1}{10^{k+1}} \right) \\ &= \frac{A_k + 1}{10^k} - \frac{A_k}{10^k} - \frac{A_{k+1} + 1}{10^{k+1}} \\ &= \frac{1}{10^k} - \frac{A_{k+1} + 1}{10^{k+1}} = \frac{9 - A_{k+1}}{10^{k+1}}. \end{aligned}$$

Como  $A_{k+1} \in \{1, 2, \dots, 9\}$ , temos que  $\frac{9 - A_{k+1}}{10^{k+1}} \geq 0$ , donde  $b_{k+1} \leq b_k$ .

Por fim, provemos que  $\lim_{k \rightarrow +\infty} (b_k - a_k) = 0$ . De fato, veja que

$$\begin{aligned} b_k - a_k &= a_{k-1} + \frac{A_k + 1}{10^k} - \sum_{i=0}^k \frac{A_i}{10^i} \\ &= \sum_{i=0}^{k-1} \frac{A_i}{10^i} + \frac{A_k}{10^k} + \frac{1}{10^k} - \sum_{i=0}^k \frac{A_i}{10^i} \\ &= \sum_{i=0}^k \frac{A_i}{10^i} + \frac{1}{10^k} - \sum_{i=0}^k \frac{A_i}{10^i} = \frac{1}{10^k}, \end{aligned}$$

e então  $\lim_{k \rightarrow +\infty} (b_k - a_k) = \lim_{k \rightarrow +\infty} \frac{1}{10^k} = 0$ .

Com isso, a sequência  $([a_k, b_k])_{k \geq 0}$  é de intervalos encaixantes, e então existe um único  $x \in \mathbb{R}$  tal que, para todo  $k \in \mathbb{N}$ ,  $a_k \leq x \leq b_k$ . Pelo resultado (7.39), a sequência  $([a_k^n, b_k^n])_{k \geq 0}$  também é de intervalos encaixantes; temos então que, para todo  $k \in \mathbb{N}$ ,  $a_k^n \leq x^n \leq b_k^n$ . No entanto, vimos isso também vale para o real  $a > 0$ : para todo  $k \in \mathbb{N}$ ,  $a_k^n \leq a \leq b_k^n$ . Daí,  $x^n = a$ .

(b) Se  $a > 0$ , então, pelo item (a), existe  $x > 0$  tal que  $x^n = a$ . Por outro lado, se  $a < 0$ , então  $-a > 0$ , e pelo item (a) existe  $x > 0$  tal que  $x^n = -a$ ; daí,  $(-x)^n = a$ .

**Definição 7.49.** Seja  $n \geq 1$  um natural.

(a) Para cada real  $a$ , o único real  $x$  tal que  $x^n = a$  será chamado de *raíz  $n$ -ésima* de  $a$  e será denotado por  $\sqrt[n]{a}$ . Assim, temos que  $(\sqrt[n]{a})^n = a$ .

(b) Como para todo  $x \in \mathbb{R}_+$  existe um único  $\sqrt[n]{x} \in \mathbb{R}_+$ , a relação  $\{(x, y) \in \mathbb{R}_+ \times \mathbb{R}_+ : y = \sqrt[n]{x}\}$  é uma função, que será chamada de *função raiz*.

**Corolário 7.50.** Se  $a, b > 0$  são reais,  $m, n \geq 1$  são naturais e  $p$  é um inteiro, então

$$(a) \sqrt[n]{a^p} = \sqrt[nm]{a^{pm}};$$

$$(b) \sqrt[n]{\sqrt[m]{a}} = \sqrt[nm]{a};$$

$$(c) \sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab};$$

$$(d) a < b \Leftrightarrow \sqrt[n]{a} < \sqrt[n]{b}.$$

**Prova.**

**Proposição 7.51.** A função  $f(x) := \sqrt[n]{x}$  é contínua em todo seu domínio.

**Prova.**

**Definição 7.52.** (Expoente Racional) Seja  $a > 0$  um real. Para cada racional  $r$  (isto é,  $r := m/n$ , com  $m \in \mathbb{Z}$  e  $n \in \mathbb{N} \setminus \{0\}$ ), definimos  $a^r = a^{\frac{m}{n}} := \sqrt[n]{a^m}$ .<sup>2</sup>

**Proposição 7.53.** Para quaisquer  $a, b > 0$  reais e  $r, s$  racionais, temos que

$$(a) a^r \cdot a^s = a^{r+s};$$

$$(b) (a^r)^s = a^{rs};$$

$$(c) (ab)^r = a^r b^r;$$

$$(d) \frac{a^r}{a^s} = a^{r-s};$$

$$(e) \left(\frac{a}{b}\right)^r = \frac{a^r}{b^r};$$

$$(f) \text{ Se } 1 < a \text{ e } r < s, \text{ então } a^r < a^s;$$

---

<sup>2</sup>Como  $\sqrt[n]{a^p} = \sqrt[nm]{a^{pm}}$ , a definição acima não depende da escolha da fração  $m/n$ . Em particular,  $f: \mathbb{Q} \rightarrow \mathbb{R}_+^*$  tal que  $f(r) = a^r$  fica bem definida como função.

(g) Se  $0 < a < 1$  e  $r < s$ , então  $a^s < a^r$ .

**Prova.**

### Expoentes Reais

O intuito aqui é definir  $a^x$  quando  $x \in \mathbb{R}$ .

**Teorema 7.54. (a)** Se  $f : \mathbb{R} \rightarrow \mathbb{R}$  é contínua em  $\mathbb{R}$  e  $f(x) = 0$  para todo  $x \in \mathbb{Q}$ , então  $f(x) = 0$  para todo  $x \in \mathbb{R}$ .

(b) Se  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  são contínuas em  $\mathbb{R}$  e  $f(x) = g(x)$  para todo  $x \in \mathbb{Q}$ , então  $f(x) = g(x)$  para todo  $x \in \mathbb{R}$ .<sup>3</sup>

(c) Se  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  são contínuas em  $\mathbb{R}$  e existe  $0 < a \neq 1$  tal que  $f(x) = a^x$  e  $g(x) = a^x$  para todo  $x \in \mathbb{Q}$ , então  $f(x) = g(x)$  para todo  $x \in \mathbb{R}$ .<sup>4</sup>

**Prova. (a)** Segue como corolário da conservação do sinal (7.24). ■

(b) Basta aplicar o resultado do item (a) na função  $h(x) := f(x) - g(x)$ . ■

(c) Segue como corolário do item (b) acima.

**Teorema 7.55. (a)** Se  $a > 1$  é um real, então para todo  $\epsilon > 0$  existe um natural  $n$  tal que  $a^{\frac{1}{n}} - 1 < \epsilon$ .

(b) Se  $a > 1$  e  $x$  são reais, então para todo  $\epsilon > 0$  existem racionais  $r$  e  $s$  tais que  $r < x < s$  e  $a^s - a^r < \epsilon$ .

(c) Se  $a > 1$  é um real, então para todo  $x$  real existe um único real  $\gamma$  tal que  $a^r < \gamma < a^s$  para todos os racionais  $r$  e  $s$  com  $r < x < s$ .

(d) Se  $0 < a \neq 1$  é um real, então existe uma única função definida e contínua em  $\mathbb{R}$  tal que  $f(r) = a^r$  para todo  $x \in \mathbb{Q}$ .

**Prova. (a)** Sabemos que  $(1 + \epsilon)^n \geq 1 + n\epsilon$  para todo natural  $n \geq 1$ . Pois tome  $n$  tal que  $1 + n\epsilon > a$  (basta que  $n > \frac{a-1}{\epsilon}$ ); daí,  $(1 + \epsilon)^n > a$ , donde  $a^{\frac{1}{n}} - 1 < \epsilon$ . ■

(b) Para racionais  $t > x$  temos  $a^r < a^t$  para todo racional  $r < x$ . Pelo item anterior, existe um natural  $n$  para o qual  $a^{\frac{1}{n}} - 1 < \epsilon \cdot a^{-t}$ , donde  $a^t(a^{\frac{1}{n}} - 1) < \epsilon$ . Tomando racionais  $r$  e  $s$ , com  $r < x < s$ , para os quais  $s - r < 1/n$ , temos  $a^s - a^r = a^r(a^{s-r} - 1) < a^t(a^{\frac{1}{n}} - 1) < \epsilon$ . ■

<sup>3</sup>Isto nos diz que se duas funções contínuas em  $\mathbb{R}$  coincidem em  $\mathbb{Q}$ , então elas são iguais.

<sup>4</sup>Isto significa que poderá existir no máximo uma função definida e contínua em  $\mathbb{R}$  que coincide com  $a^x$  para todo  $x \in \mathbb{Q}$ .

(c) O conjunto  $A := \{a^r : r \in \mathbb{Q} \wedge r < x\}$  é não vazio e limitado superiormente (por todo  $a^s$ , com  $s > x$ ). Assim, existe  $\gamma := \sup A$ . Claramente,  $a^r \leq \gamma \leq a^s$ , mas, mais geralmente,  $a^r < \gamma < a^s$  (prove!). Provemos, agora, a unicidade de  $\gamma$ . Se  $\gamma'$  for tal que  $a^r < \gamma' < a^s$  para quaisquer racionais  $r$  e  $s$ , com  $r < x < s$ , então  $|\gamma - \gamma'| < a^s - a^r$ . Pelo item anterior, para todo  $\epsilon > 0$  existem  $r_0$  e  $s_0$ , com  $r_0 < x < s_0$ , para os quais  $a^{s_0} - a^{r_0} < \epsilon$ ; logo, temos  $|\gamma - \gamma'| < \epsilon$  para todo  $\epsilon > 0$ , donde  $\gamma = \gamma'$ . ■

(d) Pelo item anterior, para quaisquer  $a > 1$  e  $x$  reais existe um único  $\gamma$ ; assim, basta tomar  $f(x) := \gamma$ . Antes de provar a continuidade de  $f$ , provemos que  $f$  é estritamente crescente. De fato, tomando reais  $x_1 < x_2$  temos que  $a^{r_1} < f(x_1) < a^{s_1}$  e  $a^{r_2} < f(x_2) < a^{s_2}$  para todos os racionais  $r_1, r_2, s_1$  e  $s_2$  tais que  $r_1 < x_1 < s_1$  e  $r_2 < x_2 < s_2$ . Como existe  $s$  racional tal que  $x_1 < s < x_2$ , temos  $f(x_1) < a^s < f(x_2)$ , donde  $f$  é estritamente crescente.

Agora, sendo  $p \in \mathbb{R}$ , pelo item (b) deste teorema, para todo  $\epsilon > 0$  existem racionais  $r$  e  $s$ , com  $r < x < s$ , para os quais  $a^s - a^r < \epsilon$ . Em particular, para todo  $x \in ]r, s[$ , temos  $a^r < f(x) < a^s$ , e como também  $a^r < f(p) < a^s$ , temos  $|f(x) - f(p)| < a^s - a^r < \epsilon$ . Assim, pelo Teorema (7.23),  $f$  é contínua em  $p$ . Como  $p$  foi tomado de modo arbitrário, segue que  $f$  é contínua em  $\mathbb{R}$ .

Por outro lado, se  $0 < a < 1$ , então  $f(x) := \left(\frac{1}{a}\right)^{-x}$  está bem definida em  $\mathbb{R}$ , é contínua em  $\mathbb{R}$  e coincide com  $a^r$  nos racionais.

**Definição 7.56.** Seja  $0 < a \neq 1$  um real. Para todo  $x \in \mathbb{R}$ , definimos  $a^x := f(x)$ , em que  $f$  é a função a que se refere o item (d) do Teorema (7.55).

**Proposição 7.57.** Para quaisquer  $0 < a, b \neq 1$  reais e  $x, y$  reais, temos que

(a)  $a^x \cdot a^y = a^{x+y}$ ;

(b)  $(a^x)^y = a^{xy}$ ;

(c)  $(ab)^x = a^x b^x$ ;

(d)  $\frac{a^x}{a^y} = a^{x-y}$ ;

(e)  $\left(\frac{a}{b}\right)^x = \frac{a^x}{b^x}$ ;

(f) Se  $1 < a$  e  $x < y$ , então  $a^x < a^y$ ;

(g) Se  $0 < a < 1$  e  $x < y$ , então  $a^y < a^x$ .

**Prova.**

**Logaritmos**

**Teorema 7.58.** Para quaisquer reais  $0 < a \neq 1$  e  $b > 0$ , existe um único real  $\gamma := \log_a b$  tal que  $a^\gamma = a^{\log_a b} = b$ . Em particular,  $f : \mathbb{R}_+ \rightarrow \mathbb{R}$  tal que  $f(x) := \log_a x$  fica bem definida.

**Prova.**

**Teorema 7.59.** Para quaisquer  $0 < a, b \neq 1$  e  $x, y > 0$ , temos que

$$\log_a xy = \log_a x + \log_a y$$

$$\log_a x^y = y \log_a x$$

$$\log_a \frac{x}{y} = \log_a x - \log_a y$$

$$\log_a x = \frac{\log_b x}{\log_b a}$$

E ainda, se  $a > 1$  e  $x < y$ , então  $\log_a x < \log_a y$  (isto é, se  $a > 1$  então  $f(x) := \log_a x$  é crescente), e se  $0 < a < 1$  e  $x < y$ , então  $\log_a y < \log_a x$  (isto é, se  $0 < a < 1$ , então  $f(x) := \log_a x$  é decrescente).

**Prova.**

**Teorema 7.60.** Se  $a > 1$ , então  $\lim_{x \rightarrow +\infty} \log_a x = \infty$  e  $\lim_{x \rightarrow 0^+} \log_a x = -\infty$ ; se  $0 < a < 1$ , então  $\lim_{x \rightarrow +\infty} \log_a x = -\infty$  e  $\lim_{x \rightarrow 0^+} \log_a x = +\infty$ .

**Prova.**

**Teorema 7.61.** A função logarítmica  $f(x) := \log_a x$  é contínua em todo seu domínio.

**Prova.**

# Capítulo 8

## Derivadas

### 8.1 Definições e Resultados Iniciais

**Definição 8.1.** Uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  é *derivável* em  $a \in A \cap A'$ , se existe o limite

$$f'(a) := \lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a}.$$

Noutros termos,  $f$  é derivável em  $a$  se existe o limite  $\lim_{x \rightarrow a} \frac{\Delta f}{\Delta x}(a)$ , onde  $\frac{\Delta f}{\Delta x}(a) : A \setminus \{a\} \rightarrow \mathbb{R}$  é a *função quociente de diferenças*, definida por

$$\frac{\Delta f}{\Delta x}(a) := \frac{f(x) - f(a)}{x - a}.$$

Sendo  $f$  derivável em  $a$ , o limite  $f'(a)$  é a *derivada* de  $f$  em  $a$ .

**Observação 8.2.** O objetivo das proposições seguintes é estabelecer precisamente a equivalência

$$\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} = L \Leftrightarrow \lim_{h \rightarrow 0} \frac{f(a + h) - f(a)}{h} = L,$$

por vezes assumida sem mais explicações.

**Proposição 8.3.** Sejam  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $a \in A'$ . Tem-se  $\lim_{x \rightarrow a} f(x) = L$  para algum  $L \in \mathbb{R}$  se, e somente se,  $\lim_{h \rightarrow 0} g(h) = L$ , onde  $g : \{h \in \mathbb{R}_{\neq 0} : a + h \in A\} \rightarrow \mathbb{R}$  é definida por  $g(h) := f(a + h)$ .

**Prova.** A proposição (???) estabelece que  $a \in A' \Leftrightarrow 0 \in \{h \in \mathbb{R}_{\neq 0} : a + h \in A\}'$ .

Daí,  $\lim_{x \rightarrow a} f(x) = L$  se, e somente se, para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que  $0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon$  para todo  $x \in A$ . Tomando  $h := x - a$ , temos  $x = a + h \in A$ , de modo que  $h \in B$ . Assim, para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que  $0 < |h| < \delta \Rightarrow |f(a + h) - L| < \epsilon$  para todo  $h \in B$ , de modo que  $\lim_{h \rightarrow 0} g(h) = L$ .

**Corolário 8.4.** Uma função  $f : A \subseteq \mathbb{R} \rightarrow \mathbb{R}$  é derivável em  $a \in A \cap A'$ , com derivada  $L \in \mathbb{R}$ , se, e somente se,  $\lim_{h \rightarrow 0} g(h) = L$ , onde  $g : \{h \in \mathbb{R}_{\neq 0} : a + h \in A \setminus \{a\}\} \rightarrow \mathbb{R}$  é definida por  $g(h) := \frac{\Delta f}{\Delta x}(a + h)$ .

**Prova.** Por definição,  $f$  ser derivável em  $a$  com derivada  $L$  significa que  $\lim_{x \rightarrow a} g(x) = L$ . Definindo  $\varphi : \{h \in \mathbb{R}_{\neq 0} : a + h \in A \setminus \{a\}\} \rightarrow \mathbb{R}$  por

$$\varphi(h) = g(a + h) = \frac{f(a + h) - f(a)}{(a + h) - a} = \frac{f(a + h) - f(a)}{h},$$

pela proposição (8.3) temos  $\lim_{x \rightarrow a} g(x) = L \Leftrightarrow \lim_{h \rightarrow 0} \varphi(h) = L$ , como havíamos afirmado.

**Definição 8.5.** Seja  $f$  uma função e  $A \subseteq D_f$  o conjunto dos  $x \in D_f$  para os quais existe  $f'(x)$ . A função  $f' : A \rightarrow \mathbb{R}$  dada por  $x \rightarrow f'(x)$  denomina-se *função derivada* ou, simplesmente, *derivada* de  $f$ . Diremos, ainda, que  $f'$  é a *derivada de 1ª ordem* de  $f$ , que também pode ser denotada por  $f^{(1)}$ . Por fim, definimos, indutivamente,  $f^{(n+1)} := [f^{(n)}]'$ .

**Definição 8.6.** Seja  $f$  uma função, sendo  $y := f(x)$ . O símbolo  $\frac{dy}{dx}$ , que se lê “derivada de  $y$  em relação a  $x$ ”, denota a derivada de  $f$  em  $x$ , isto é,  $\frac{dy}{dx} := f'(x)$ . Já  $\frac{d^n y}{dx^n}$  denota a  $n$ -ésima derivada de  $f$  em  $x$ :  $\frac{d^n y}{dx^n} := f^{(n)}(x)$ . E ainda,  $\frac{df}{dx}$  denota a função derivada de  $y = f(x)$ :  $\frac{df}{dx} := f'$ . Naturalmente, então,  $\frac{df}{dx}(x) := f'(x)$ .

A derivada de  $y = f(x)$  no ponto  $p$  é denotada por  $\left. \frac{dy}{dx} \right|_{x=p}$ .

**Teorema 8.7.** Se  $f$  for derivável em  $p$ , então  $f$  será contínua em  $p$ .

**Prova.**

**Teorema 8.8.** Se  $f$  e  $g$  são funções deriváveis em  $p$ , então

(a) a função  $f + g$  é derivável em  $p$  e

$$(f + g)'(p) = f'(p) + g'(p);$$

(b) a função  $f \cdot g$  é derivável em  $p$  e

$$(f \cdot g)'(p) = f'(p) \cdot g(p) + g'(p) \cdot f(p);$$

(c) a função  $\frac{f}{g}$  é derivável em  $p$ , desde que  $g(p) \neq 0$ , sendo

$$\left(\frac{f}{g}\right)'(p) = \frac{f'(p) \cdot g(p) - g'(p) \cdot f(p)}{[g(p)]^2}.$$

**Prova.**

**Corolário 8.9.** derivada de n funções, derivada de kf.

**Lema 8.10.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável em  $p \in D_f$ . Definindo  $\rho : D_f \setminus \{p\} \rightarrow \mathbb{R}$  de modo que

$$f(x) = f(p) + f'(p)(x - p) + \rho(x)(x - p),$$

temos que  $\lim_{x \rightarrow p} \rho(x) = 0$ .

**Prova.**

**Teorema 8.11.** (Regra da Cadeia) Se  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  são funções deriváveis, com  $Im_g \subseteq D_f$ , então a função composta  $h : D_g \rightarrow \mathbb{R}$  dada por  $h(x) = f(g(x))$  é derivável e

$$h'(x) = f'(g(x)) \cdot g'(x).$$

Sendo  $y = f(u)$  e  $u = g(x)$ , a regra da cadeia nos diz que

$$\frac{dy}{dx} = \frac{dy}{du} \cdot \frac{du}{dx},$$

em que  $\frac{dy}{du}$  deve ser calculada em  $u = g(x)$ .

**Prova.**

**Teorema 8.12.** (Derivada de Função Inversa) Seja  $f$  uma função inversível e  $g$  a função inversa de  $f$ . Se  $f$  for derivável em  $q = g(p)$ , com  $f'(q) \neq 0$ , e se  $g$  for contínua em  $p$ , então  $g$  será derivável em  $p$  e

$$g'(p) = \frac{1}{f'(g(p))}.$$

**Prova.**

## 8.2 Teoremas de Rolle, do Valor Médio e de Cauchy

**Definição 8.13.** Sejam  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função e  $p \in D_f$  um ponto no domínio de  $f$ .

(a) Diremos que  $f(p)$  é o *valor máximo global* de  $f$ , ou que  $p$  é um *ponto de máximo global* de  $f$ , se  $f(x) \leq f(p)$  para todo  $x \in D_f$ . Diremos que  $f(p)$  é o *valor mínimo global* de  $f$ , ou que  $p$  é um *ponto de mínimo global* de  $f$ , se  $f(x) \geq f(p)$  para todo  $x \in D_f$ .

(b) Suponha ainda que  $p \in A \subseteq D_f$ . Diremos que  $f(p)$  é o *valor máximo* de  $f$  em  $A$ , ou que  $p$  é um *ponto de máximo* de  $f$  em  $A$ , se  $f(x) \leq f(p)$  para todo  $x \in A$ . Diremos que  $f(p)$  é o *valor mínimo* de  $f$  em  $A$ , ou que  $p$  é um *ponto de mínimo* de  $f$  em  $A$ , se  $f(x) \geq f(p)$  para todo  $x \in A$ .

(c) Diremos que  $f(p)$  é o *valor máximo local* de  $f$ , ou que  $p$  é um *ponto de máximo local* de  $f$ , se existir  $r > 0$  tal que  $f(x) \leq f(p)$  para todo  $x \in ]p - r, p + r[ \cap D_f$ . Diremos que  $f(p)$  é o *valor mínimo local* de  $f$ , ou que  $p$  é um *ponto de mínimo local* de  $f$ , se existir  $r > 0$  tal que  $f(x) \geq f(p)$  para todo  $x \in ]p - r, p + r[ \cap D_f$ .

**Definição 8.14.** Dada uma função  $f$ , diremos que o ponto  $p$  é *interior* a  $D_f$  se existir um intervalo aberto  $I \subset D_f$  tal que  $p \in I$ .

**Teorema 8.15.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável no ponto interior  $p \in D_f$ . Se  $p$  é ponto de máximo (mínimo) local de  $f$ , então  $f'(p) = 0$ .

**Prova.** Como  $p$  é ponto de máximo local de  $f$ , existe  $r_1 > 0$  tal que  $f(x) \leq f(p)$  para todo  $x \in ]p - r_1, p + r_1[ \cap D_f$ . Como  $p$  é um interior a  $D_f$ , existe  $r_2 > 0$  tal que  $]p - r_2, p + r_2[ \subseteq D_f$ . Sendo  $r := \min\{r_1, r_2\}$ , temos  $f(x) \leq f(p)$  para todo  $x \in ]p - r, p + r[$ . Como  $f$  é derivável em  $p$ , temos que  $f'(p) = \lim_{x \rightarrow p^+} \frac{f(x) - f(p)}{x - p} = \lim_{x \rightarrow p^-} \frac{f(x) - f(p)}{x - p}$ . Sendo  $p < x < p + r$ , temos  $\frac{f(x) - f(p)}{x - p} \leq 0$ ; daí, pela conservação do sinal,  $\lim_{x \rightarrow p^+} \frac{f(x) - f(p)}{x - p} \leq 0$ . Analogamente, sendo  $p - r < x < p$ , temos  $\frac{f(x) - f(p)}{x - p} \geq 0$ ; daí, pela conservação do sinal,  $\lim_{x \rightarrow p^-} \frac{f(x) - f(p)}{x - p} \geq 0$ . Com isso, temos  $f'(p) \leq 0$  e  $f'(p) \geq 0$ , donde,  $f'(p) = 0$ . O caso em que  $p$  é ponto de mínimo local de  $f$  segue de forma completamente análoga.

$\subseteq D_f$  e derivável em  $]a, b[$ .

**Teorema 8.16.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  contínua em  $[a, b]$  e derivável em  $]a, b[$ .

(a) (Rolle) Se  $f(a) = f(b)$ , então existe  $c \in ]a, b[$  tal que  $f'(c) = 0$ .

(b) (Valor Médio) Existe  $c \in ]a, b[$  tal que

$$f(b) - f(a) = f'(c) \cdot (b - a).$$

**Prova.** (a) Se  $f$  for constante em  $[a, b]$ , então  $f'(x) = 0$  para todo  $x \in ]a, b[$ . Suponha, então, que  $f$  não seja constante em  $[a, b]$ . Sendo  $f$  contínua em  $[a, b]$ , pelo Teorema de Weierstrass (7.43), existem  $x_1, x_2 \in [a, b]$  tais que  $f(x_1) \leq f(x) \leq f(x_2)$  para todo  $x \in [a, b]$ . Se fosse  $f(x_1) = f(x_2)$ , então  $f$  seria constante; logo,  $f(x_1) \neq f(x_2)$ . E como, por hipótese,  $f(a) = f(b)$ , temos que  $x_1$  ou  $x_2$  estão em  $]a, b[$ . O  $x_i \in ]a, b[$  é um ponto de máximo local de  $f$ ; daí, pelo Teorema (8.15),  $f'(x_i) = 0$ . ■

(b) Defina  $S : [a, b] \rightarrow \mathbb{R}$  por

$$S(x) := f(a) + \frac{f(b) - f(a)}{b - a}(x - a).$$

Observe que o gráfico de  $S$  é a reta que passa pelos pontos  $(a, f(a))$  e  $(b, f(b))$ . Agora, defina  $g : [a, b] \rightarrow \mathbb{R}$  por  $g(x) := f(x) - S(x)$ . Note que  $g$  é contínua em  $[a, b]$  e derivável em  $]a, b[$ ; daí, pelo Teorema de Rolle, existe  $c \in ]a, b[$  tal que  $g'(c) = 0$ . Como

$$g'(x) = f'(x) - \frac{f(b) - f(a)}{b - a},$$

temos que

$$g'(c) = f'(c) - \frac{f(b) - f(a)}{b - a} = 0,$$

donde  $f(b) - f(a) = f'(c)(b - a)$ .

**Teorema 8.17. (Cauchy)** Se  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  são funções contínuas em  $[a, b] \subseteq D_f \cap D_g$  e deriváveis em  $]a, b[$ , então existe pelo menos um ponto  $c \in ]a, b[$  tal que

$$[f(b) - f(a)]g'(c) = [g(b) - g(a)]f'(c).$$

Em particular, se  $g'(x) \neq 0$  para todo  $x \in ]a, b[$ , então

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(c)}{g'(c)}.$$

**Prova.** Defina  $h : [a, b] \rightarrow \mathbb{R}$  por

$$h(x) := [f(b) - f(a)]g(x) - [g(b) - g(a)]f(x).$$

É fácil ver que  $h$  é contínua em  $[a, b]$ , derivável em  $]a, b[$  e  $h(a) = h(b)$ . Daí, pelo Teorema de Rolle (8.16), existe  $c \in ]a, b[$  tal que

$$[f(b) - f(a)]g(c) - [g(b) - g(a)]f(c) = 0,$$

donde

$$[f(b) - f(a)]g'(c) = [g(b) - g(a)]f'(c).$$

Em particular, se  $g'(x) \neq 0$  para todo  $x \in ]a, b[$ , então

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(c)}{g'(c)},$$

pois o Teorema do Valor Médio (8.16) aplicado à função  $g$  nos diz que existe  $\tilde{c} \in ]a, b[$  tal que  $g(b) - g(a) = g'(\tilde{c})(b - a)$ ; como  $g'(\tilde{c}) \neq 0$  e  $b \neq a$ , temos  $g(b) - g(a) \neq 0$ .

### 8.3 Gráficos de Funções

**Teorema 8.18.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável no intervalo aberto  $I \subset D_f$ .

(a) Se  $f'(x) > 0$  para todo  $x \in I$  interior, então  $f$  será estritamente crescente em  $I$ .

(b) Se  $f'(x) < 0$  para todo  $x \in I$  interior, então  $f$  será estritamente decrescente em  $I$ .

**Prova.** (a) Provemos que para quaisquer  $a, b \in I$  temos  $a < b \Rightarrow f(a) < f(b)$ . Sejam, então,  $a, b \in I$  com  $a < b$ . Evidentemente, temos que  $f$  é contínua em  $[a, b]$  e derivável em  $]a, b[$ ; daí, pelo Teorema do Valor Médio (8.16), existe  $c \in ]a, b[$  tal que  $f(b) - f(a) = f'(c)(b - a)$ . Como  $f'(c) > 0$  e  $b > a$ , temos que  $f(b) - f(a) > 0$ , donde  $f(a) < f(b)$ . ■

(b) Segue analogamente.

**Corolário 8.19.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável até a 2ª ordem em  $]a, b[ \subseteq D_f$ . Se  $f''(x) > 0$  para todo  $x \in ]a, b[$  e se existe  $c \in ]a, b[$  tal que  $f'(c) = 0$ , então  $f$  é estritamente decrescente em  $]a, c[$  e estritamente crescente em  $]c, b[$ .

**Prova.** Se  $f''(x) > 0$  para todo  $x \in ]a, b[$ , então  $f'$  é estritamente crescente em  $]a, b[$ . Com isso,  $f'(x) < f'(c) = 0$  para todo  $x \in ]a, c[$  e  $f'(x) > f'(c) = 0$  para todo  $x \in ]c, b[$ . Com isso,  $f$  é estritamente decrescente em  $]a, c[$  e estritamente crescente em  $]c, b[$ .

**Definição 8.20.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável no intervalo aberto  $I \subseteq D_f$ .

(a) Se  $f(x) > f(p) + f'(p)(x - p)$  para todos  $x, p \in I$ , com  $x \neq p$ , diremos que  $f$  tem a *concavidade para cima* em  $I$ , ou que  $f$  é *convexa* em  $I$ .

(b) Se  $f(x) < f(p) + f'(p)(x - p)$  para todos  $x, p \in I$ , com  $x \neq p$ , diremos que  $f$  tem a *concavidade para baixo* em  $I$ , ou que  $f$  é *côncava* em  $I$ .

**Teorema 8.21.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável até a 2ª ordem no intervalo aberto  $I \subseteq D_f$ .

(a) Se  $f''(x) > 0$  em  $I$ , então  $f$  terá a concavidade para cima em  $I$ .

(b) Se  $f''(x) < 0$  em  $I$ , então  $f$  terá a concavidade para baixo em  $I$ .

**Prova.** (a) Sendo  $p \in I$ , provemos que para todo  $x \in I$ , com  $x \neq p$ , temos  $f(x) > f(p) + f'(p)(x - p)$ . Definindo  $g : I \rightarrow \mathbb{R}$  por  $g(x) := f(x) - f(p) - f'(p)(x - p)$ , basta provar que  $g(x) > 0$  para todo  $x \in I$ , com  $x \neq p$ . É fácil ver que  $g'(x) = f'(x) - f'(p)$ . Como  $f''(x) > 0$  em  $I$ , temos que  $f'$  é estritamente crescente em  $I$ . Com isso,  $g'(x) > 0$  para  $x > p$  e  $g'(x) < 0$  para  $x < p$ . Com isso,  $g$  é estritamente decrescente em  $\{x \in I : x < p\}$  e estritamente crescente em  $\{x \in I : x > p\}$ . Com isso, sendo  $g(p) = 0$ , temos  $g(x) > 0$  para todo  $x \in I$ , com  $x \neq p$ . ■

(b) Segue analogamente.

**Definição 8.22.** Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função contínua em  $p \in D_f$ . Diremos que  $p$  é um *ponto de inflexão* de  $f$  se existirem  $a, b \in \mathbb{R}$ , com  $p \in ]a, b[ \subseteq D_f$ , para os quais a concavidade de  $f$  em  $]a, p[$  é diferente da concavidade de  $f$  em  $]p, b[$ .

**Proposição 8.23.** (a) Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável até a 3ª ordem no intervalo aberto  $]a, b[ \subseteq D_f$ . Se  $f'''$  é contínua em  $p \in ]a, b[$ ,  $f'''(p) \neq 0$  e  $f'''(p) = 0$ , então  $p$  é um ponto de inflexão de  $f$ .

(b) Seja  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  uma função derivável até a 2ª ordem no intervalo aberto  $I \subseteq D_f$ . Se  $f''$  é contínua em  $p \in I$  e  $p$  é um ponto de inflexão de  $f$ , então  $f''(p) = 0$ .

**Prova.** (a) Suponha, sem perda de generalidade, que  $f'''(p) > 0$ . Como  $f'''$  é contínua em  $p$ , pela conservação do sinal (7.24) existe  $r_1 > 0$  tal que  $f'''(x) > 0$  para

todo  $x \in ]p - r_1, p + r_1[$ . Por outro lado, existe  $r_2 > 0$  tal que  $]p - r_2, p + r_2[ \subseteq ]a, b[$  (de fato, basta tomar  $r_2 = \min \{b - p, p - a\}$ ). Sendo, então,  $r := \min \{r_1, r_2\}$ , temos que  $f'''(x) > 0$  para todo  $x \in ]p - r, p + r[ \subseteq ]a, b[$ . Com isso,  $f''$  é estritamente crescente em  $]p - r, p + r[$ , e como  $f''(p) = 0$ , só pode ser  $f''(x) < 0$  para todo  $x \in ]p - r, p + r[$  e  $f''(x) > 0$  para todo  $x \in ]p, p + r[$ . Logo,  $p$  é um ponto de inflexão de  $f$ .

**(b)** Se fosse  $f''(p) \neq 0$ , como  $f''$  é contínua em  $p$ , pela conservação do sinal existiria  $r > 0$  tal que  $f''(p)$  e  $f''(x)$  teriam o mesmo sinal em  $]p - r, p + r[$ , donde  $p$  não seria ponto de inflexão de  $f$ , absurdo. Logo,  $f''(p) = 0$ .

## 8.4 Regras de L'Hospital

**Teorema 8.24.** (Regra de L'Hospital para indeterminações do tipo 0/0)

**(a)** Sejam  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções para as quais existe  $r \in \mathbb{R}_{>0}$  tal que  $f$  e  $g$  são deriváveis e  $g'(x) \neq 0$  em

- $I := ]p, p + r[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow p^+$ ); ou
- $I := ]p - r, p[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow p^-$ ); ou
- $I := ]p - r, p + r[ \setminus \{p\} \subseteq D_f \cap D_g$  (caso  $x \rightarrow p$ ).

Se  $\lim_{x \rightarrow p} f(x) = \lim_{x \rightarrow p} g(x) = 0$  e  $\lim_{x \rightarrow p} \frac{f'(x)}{g'(x)} \in \mathbb{R} \cup \{\pm\infty\}$ , então

$$\lim_{x \rightarrow p} \frac{f(x)}{g(x)} = \lim_{x \rightarrow p} \frac{f'(x)}{g'(x)}.$$

**(b)** Sejam  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções para as quais existe  $r \in \mathbb{R}$  tal que  $f$  e  $g$  são deriváveis e  $g'(x) \neq 0$  em

- $I := ]r, +\infty[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow +\infty$ ); ou
- $I := ]-\infty, r[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow -\infty$ ).

Se  $\lim_{x \rightarrow \pm\infty} f(x) = \lim_{x \rightarrow \pm\infty} g(x) = 0$  e  $\lim_{x \rightarrow \pm\infty} \frac{f'(x)}{g'(x)} \in \mathbb{R} \cup \{\pm\infty\}$ , então

$$\lim_{x \rightarrow \pm\infty} \frac{f(x)}{g(x)} = \lim_{x \rightarrow \pm\infty} \frac{f'(x)}{g'(x)}.$$

**Prova. (a)** Suponha  $\lim_{x \rightarrow p^+} \frac{f'(x)}{g'(x)} = L \in \mathbb{R}$ . Façamos o caso  $x \rightarrow p^+$ , isto é,

$$\lim_{x \rightarrow p^+} f(x) = \lim_{x \rightarrow p^+} g(x) = 0 \quad \text{e} \quad \lim_{x \rightarrow p^+} \frac{f'(x)}{g'(x)} = L.$$

Defina  $F, G : I \rightarrow \mathbb{R}$  por

$$F(x) := \begin{cases} f(x) & x \in I \\ 0 & x = p \end{cases} \quad \text{e} \quad G(x) := \begin{cases} g(x) & x \in I \\ 0 & x = p \end{cases}$$

Afirmamos que  $G'(x) \neq 0$  para todo  $x \in I$  e  $G(p) = 0$  resultam em  $G(x) \neq 0$  para todo  $x \in I$ . De fato, se não fosse  $G(x) \neq 0$  para todo  $x \in I$ , então existiria  $a \in I$  com  $G(a) = 0$ ; pelo Teorema do Valor Médio, existiria  $b \in ]p, a[$  tal que

$$\underbrace{G(a) - G(p)}_{=0} = G'(b) \underbrace{(a - p)}_{\neq 0},$$

donde  $G'(b) = 0$ , contrariando a hipótese de ser  $G'(x) \neq 0$  para todo  $x \in I$ .

Agora, sendo  $\lim_{x \rightarrow p^+} \frac{f'(x)}{g'(x)} = L$ , para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$ , com  $\delta < r$ , tal que

$$p < x < p + \delta \Rightarrow \left| \frac{f'(x)}{g'(x)} - L \right| < \epsilon,$$

isto é,  $\left| \frac{F'(x)}{G'(x)} - L \right| < \epsilon$ . Por outro lado, o Teorema de Cauchy aplicado às funções  $F$  e  $G$  no intervalo  $[p, x]$  nos diz que existe  $q \in ]p, x[$  tal que

$$\frac{F(x) - F(p)}{G(x) - G(p)} = \frac{F'(q)}{G'(q)},$$

daí,

$$\left| \frac{F(x)}{G(x)} - L \right| = \left| \frac{F(x) - F(p)}{G(x) - G(p)} - L \right| = \left| \frac{F'(q)}{G'(q)} - L \right| < \epsilon,$$

pois  $p < q < x < p + \delta$ . Com isso,  $\lim_{x \rightarrow p^+} \frac{f(x)}{g(x)} = L$ , como queríamos provar.

**(b)**

**Teorema 8.25.** (Regra de L'Hospital para indeterminações do tipo  $\infty/\infty$ )

**(a)** Sejam  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções para as quais existe  $r \in \mathbb{R}_{>0}$  tal que  $f$  e  $g$  são deriváveis e  $g'(x) \neq 0$  em

- $I := ]p, p + r[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow p^+$ ); ou
- $I := ]p - r, p[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow p^-$ ); ou
- $I := ]p - r, p + r[ \setminus \{p\} \subseteq D_f \cap D_g$  (caso  $x \rightarrow p$ ).

Se  $\lim f(x) = \lim g(x) = \pm\infty$  e  $\lim \frac{f'(x)}{g'(x)} \in \mathbb{R} \cup \{\pm\infty\}$ , então

$$\lim \frac{f(x)}{g(x)} = \lim \frac{f'(x)}{g'(x)}.$$

**(b)** Sejam  $f : D_f \subseteq \mathbb{R} \rightarrow \mathbb{R}$  e  $g : D_g \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções para as quais existe  $r \in \mathbb{R}$  tal que  $f$  e  $g$  são deriváveis e  $g'(x) \neq 0$  em

- $I := ]r, +\infty[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow +\infty$ ); ou
- $I := ]-\infty, r[ \subseteq D_f \cap D_g$  (caso  $x \rightarrow -\infty$ ).

Se  $\lim f(x) = \lim g(x) = \pm\infty$  e  $\lim \frac{f'(x)}{g'(x)} \in \mathbb{R} \cup \{\pm\infty\}$ , então

$$\lim \frac{f(x)}{g(x)} = \lim \frac{f'(x)}{g'(x)}.$$

**Prova.**

## 8.5 Trigonometria, parte II

**Teorema 8.26.** Existe um menor real  $a > 0$  tal que  $\cos a = 0$  e  $\sin a = 1$ .

**Prova.**

**Definição 8.27.** Definimos  $\pi := 2a$ , em que  $a$  é o menor real a que se refere o Teorema (8.26). Assim,  $\cos \frac{\pi}{2} = 0$  e  $\sin \frac{\pi}{2} = 1$ .

**Teorema 8.28.** As funções  $\sin$  e  $\cos$  são periódicas com período  $2\pi$ , isto é,  $\sin(x + 2\pi) = \sin x$  e  $\cos(x + 2\pi) = \cos x$  para todo  $x \in \mathbb{R}$ .

## 8.6 Polinômio de Taylor

**Definição 8.29.** Seja  $I \subset \mathbb{R}$  um intervalo aberto,  $f : I \rightarrow \mathbb{R}$  uma função  $n$  vezes diferenciável e  $x_0 \in I$  um ponto de  $I$ . O polinômio

$$P_n(x) := \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k$$

chama-se *polinômio de Taylor de ordem  $n$  de  $f$  centrado, ou em volta, de  $x_0$* .

**Proposição 8.30.** Nas condições da definição (8.29),  $P_n^{(k)}(x_0) = f^{(k)}(x_0)$  para todo  $k \leq n$ .

**Prova.**

# Capítulo 9

## Integrais

### 9.1 A integral de Darboux

#### Definição 9.1.

- (a) Uma *partição* de um intervalo  $[a, b]$  é um conjunto finito  $P := \{x_0, \dots, x_n\}$  tal que  $a = x_0 < x_1 < \dots < x_n = b$ . Isso é denotado por

$$P : a = x_0 < \dots < x_n = b.$$

O conjunto de todas as partições de  $[a, b]$  é denotado por  $\mathcal{P}[a, b]$ .

- (b) A *amplitude* do  $i$ -ésimo intervalo  $[x_{i-1}, x_i]$ , para cada  $i \in [n]$ , é definida como  $\Delta x_i := x_i - x_{i-1}$ .
- (c) Um *refinamento* de uma partição  $P \in \mathcal{P}[a, b]$  é uma partição  $Q \in \mathcal{P}[a, b]$  tal que  $P \subseteq Q$ .

**Definição 9.2.** Sejam  $f : [a, b] \rightarrow \mathbb{R}$  uma função limitada e  $P : a = x_0 < \dots < x_n = b$  uma partição de  $[a, b]$ .

- (a) A *soma superior* de  $f$  com relação à  $P$  é definida como

$$U(f, P) := \sum_{i=1}^n M_i \Delta x_i,$$

onde  $M_i := \sup_{[x_{i-1}, x_i]} f$  para cada  $i \in [n]$ .

- (b) A *soma inferior* de  $f$  com relação à  $P$  é definida como

$$L(f, P) := \sum_{i=1}^n m_i \Delta x_i,$$

onde  $m_i := \inf_{[x_{i-1}, x_i]} f$  para cada  $i \in [n]$ .

**Proposição 9.3.** Sejam  $f : [a, b] \rightarrow \mathbb{R}$  uma função limitada e  $P : a = x_0 < \dots < x_n = b$  uma partição de  $[a, b]$ .

- (a) Tem-se  $L(f, P) \leq U(f, P)$ .
- (b) Se  $Q$  é um refinamento de  $P$ , então  $U(f, Q) \leq U(f, P)$  e  $L(f, Q) \geq L(f, P)$ .
- (c) Se  $Q$  é uma qualquer outra partição de  $[a, b]$ , então  $L(f, P) \leq U(f, Q)$ .

**Prova.**

- (a) Para todo  $i \in [n]$  temos  $m_i \leq M_i$  e  $\Delta x_i > 0$ . Logo  $m_i \Delta x_i \leq M_i \Delta x_i$  para todo  $i \in [n]$ . Tomando a soma, temos que

$$\sum_{i=1}^n m_i \Delta x_i \leq \sum_{i=1}^n M_i \Delta x_i,$$

de modo que  $L(f, P) \leq U(f, P)$ , como havíamos afirmado. ■

- (b) Façamos indução em  $|Q \setminus P|$ . Se  $|Q \setminus P| = 1$ , então  $Q$  só tem um ponto a mais que  $P$ , isto é, existe  $\bar{x} \in Q$  tal que  $\bar{x} \notin P$ . Em particular, existe um único índice  $j \in [n]$  tal que  $x_{j-1} < \bar{x} < x_j$ . Com isso, tomando

$$M'_j := \sup_{[x_{j-1}, \bar{x}]} f \quad \text{e} \quad M''_j := \sup_{[\bar{x}, x_j]} f,$$

temos  $M'_j, M''_j \leq M_j$ , donde

$$\begin{aligned} U(f, Q) &= \sum_{\substack{i=1 \\ i \neq j}}^n M_i \Delta x_i + M'_j (\bar{x} - x_{j-1}) + M''_j (x_j - \bar{x}) \\ &\leq \sum_{\substack{i=1 \\ i \neq j}}^n M_i \Delta x_i + M_j (\bar{x} - x_{j-1}) + M_j (x_j - \bar{x}) \\ &= \sum_{\substack{i=1 \\ i \neq j}}^n M_i \Delta x_i + M_j (x_j - x_{j-1}) \\ &= \sum_{i=1}^n M_i \Delta x_i = U(f, P). \end{aligned}$$

Isso completa a base da indução. Agora, suponha que se  $|Q \setminus P| = k > 1$ , então  $U(f, Q) \leq U(f, P)$ . Tomando  $Q'$  com só um ponto a mais que  $Q$ ,

temos que  $U(f, Q') \leq U(f, Q)$ , de modo que se  $|Q' \setminus P| = k + 1$  então  $U(f, Q') \leq U(f, P)$ . Isso completa o passo indutivo e, portanto, completa a prova. A prova de que  $L(f, P') \geq L(f, P)$  segue de modo completamente análogo. ■

- (c) Para quaisquer partições  $P$  e  $Q$  de  $[a, b]$ , sempre existe um refinamento comum a ambas. De fato, basta tomar a união  $P \cup Q$  e reindexar os índices conforme a definição. Assim, pelos itens anteriores,

$$L(f, P) \leq L(f, P \cup Q) \leq U(f, P \cup Q) \leq U(f, Q),$$

como havíamos afirmado. ■

**Definição 9.4.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função limitada.

- (a) A *integral inferior* de  $f$  é definida como

$$\int_a^b f(x) dx := \sup_{P \in \mathcal{P}[a, b]} L(f, P).$$

- (b) A *integral superior* de  $f$  é definida como

$$\int_a^{\bar{b}} f(x) dx := \inf_{P \in \mathcal{P}[a, b]} U(f, P).$$

**Observação 9.5.** A proposição (9.3) garante que  $\{L(f, P) \in \mathbb{R} : P \in \mathcal{P}[a, b]\}$  é limitado superiormente; logo, pela propriedade do supremo, existe  $\sup_{P \in \mathcal{P}[a, b]} L(f, P)$ .

Analogamente, existe  $\inf_{P \in \mathcal{P}[a, b]} U(f, P)$ . Isso garante que as definições de integral superior e inferior são consistentes (estão bem definidas).

**Proposição 9.6.** Se uma função  $f : [a, b] \rightarrow \mathbb{R}$  é limitada, então

$$\int_a^b f(x) dx \leq \int_a^{\bar{b}} f(x) dx.$$

**Prova.** Vimos que  $L(f, P) \leq U(f, Q)$  para quaisquer partições  $P, Q \in \mathcal{P}[a, b]$ . Fixando  $Q$ , temos que  $U(f, Q)$  é uma cota superior de  $L(f, P)$ , para qualquer  $P \in \mathcal{P}[a, b]$ , de modo que

$$\int_a^b f(x) dx \leq U(f, Q).$$

Com isso,  $\int_a^b f(x) dx$  é uma cota inferior de  $U(f, Q)$ , para qualquer  $Q \in \mathcal{P}[a, b]$ , de modo que

$$\int_a^b f(x) dx \leq \int_a^{\bar{b}} f(x) dx,$$

como havíamos afirmado. ■

**Definição 9.7.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função limitada.

(a)  $f$  é integrável em  $[a, b]$  segundo Darboux se

$$\int_a^b f(x) dx = \int_a^{\bar{b}} f(x) dx.$$

(b) Seja  $f$  Darboux-integrável em  $[a, b]$ . A integral de Darboux de  $f$  em  $[a, b]$  é definida como

$$\int_a^b f(x) dx := \int_a^b f(x) dx = \int_a^{\bar{b}} f(x) dx.$$

(c) Se  $f$  está definida em  $c \in \mathbb{R}$ , estendemos a definição dizendo que  $f$  é integrável em  $c$  colocando

$$\int_c^c f(x) dx = 0.$$

(d) Se  $f$  é integrável, estendemos a definição colocando

$$\int_b^a f(x) dx := - \int_a^b f(x) dx.$$

**Observação 9.8.** Decorre das definições que, sendo  $f : [a, b] \rightarrow \mathbb{R}$  integrável, vale

$$L(f, P) \leq \int_a^b f(x) dx = \int_a^b f(x) dx = \int_a^{\bar{b}} f(x) dx \leq U(f, P),$$

para qualquer  $P \in \mathcal{P}[a, b]$ .

**Teorema 9.9** (Critério de integrabilidade). Uma função limitada  $f : [a, b] \rightarrow \mathbb{R}$  é integrável em  $[a, b]$  se, e somente se, para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $P \in \mathcal{P}[a, b]$  tal que  $U(f, P) - L(f, P) < \epsilon$ .

**Prova. (a)** ( $\Rightarrow$ )<sup>1</sup> Sendo  $f$  integrável, para todo  $\epsilon \in \mathbb{R}_{>0}$  existem partições  $P_1, P_2 \in \mathcal{P}$  tais que

$$S(P_2, f) - \int_a^b f(x) dx < \frac{\epsilon}{2} \quad \text{e} \quad \int_a^b f(x) dx - s(P_1, f) < \frac{\epsilon}{2}.$$

Com isso, sendo  $P$  uma partição comum à  $P_1$  e  $P_2$ , temos que

$$S^+(f, P) \leq S(P_2, f) < \int_a^b f(x) dx + \frac{\epsilon}{2} < s(P_1, f) + \epsilon \leq S_-(f, P) + \epsilon,$$

de modo que  $S^+(f, P) - S_-(f, P) < \epsilon$ .

( $\Leftarrow$ ) Agora, suponha que para todo  $\epsilon \in \mathbb{R}_{>0}$  existe uma partição  $P$  de  $[a, b]$  tal que  $S^+(f, P) - S_-(f, P) < \epsilon$ . Como

$$S_-(f, P) \leq \int_a^b f(x) dx \leq \int_a^b f(x) dx \leq S^+(f, P),$$

temos que  $0 \leq \int_a^b f(x) dx - \int_a^b f(x) dx \leq S^+(f, P) - S_-(f, P) < \epsilon$ , de modo que  $\int_a^b f(x) dx - \int_a^b f(x) dx < \epsilon$  para todo  $\epsilon \in \mathbb{R}_{>0}$ , donde  $\int_a^b f(x) dx = \int_a^b f(x) dx$ . Assim,  $f$  é integrável.

### 9.1.1 Estendendo a definição

**Proposição 9.10. (a)** Se  $f : [a, b] \rightarrow \mathbb{R}$  é uma função tal que  $f(x) = 0$  para todo  $x \in [a, b] \setminus \{c\}$ , onde  $c \in [a, b]$  e  $f(c) \neq 0$ , então  $f$  é integrável em  $[a, b]$  e

$$\int_a^b f(x) dx = 0.$$

**(b)** Se  $f : [a, b] \rightarrow \mathbb{R}$  é uma função tal que  $f(x) = 0$  para todo  $x \in [a, b] \setminus \{c_1, c_2, \dots, c_n\}$ , onde  $c_i \in [a, b]$  e  $f(c_i) \neq 0$  para todo  $i \in [n]$ , então  $f$  é integrável em  $[a, b]$  e

$$\int_a^b f(x) dx = 0.$$

<sup>1</sup>Esta prova depende de um resultado sobre supremos e ínfimos.

(c) Sejam  $f, g : [a, b] \rightarrow \mathbb{R}$  funções tais que  $f(x) = g(x)$  para todo  $x \in [a, b] \setminus \{c_1, c_2, \dots, c_n\}$ , onde  $c_i \in [a, b]$  e  $f(c_i) \neq g(c_i)$  para todo  $i \in [n]$ . Se  $f$  é integrável, então  $g$  é integrável e

$$\int_a^b g(x) dx = \int_a^b f(x) dx.$$

**Prova.** Táboas, observação 4.1.16, página 171.

**Definição 9.11.** Seja  $f : [a, b] \setminus \{c_1, c_2, \dots, c_n\} \rightarrow \mathbb{R}$  uma função,  $c_i \in [a, b]$  para todo  $i \in [n]$ . Diremos que  $f$  é integrável em  $[a, b]$  se qualquer extensão  $g$  de  $f$  a  $[a, b]$  o for, pondo

$$\int_a^b f(x) dx := \int_a^b g(x) dx.$$

## 9.2 Resultados

**Teorema 9.12. (a)** Toda função  $f : [a, b] \rightarrow \mathbb{R}$  contínua é integrável.

(b) Se a função  $f : [a, b] \rightarrow \mathbb{R}$  é limitada e tem apenas um número finito de pontos de descontinuidade, então  $f$  é integrável.

**Prova. (a)** Pelo teorema da limitação (7.42),  $f$  é limitada. Pelo teorema (7.36),  $f$  é uniformemente contínua, de modo que para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que

$$|x - y| < \delta \Rightarrow |f(x) - f(y)| < \frac{\epsilon}{b - a}.$$

Escolha uma partição  $P : a = x_0 < \dots < x_n = b$  tal que  $\Delta x_i < \delta$  para todo  $i \in [n]$ . Uma tal partição existe: tomando  $n \in \mathbb{N}$  tal que  $n > \frac{b - a}{\delta}$ , é fácil ver que

definindo  $x_i = a + i \cdot \frac{b - a}{n}$  para cada  $i \in [n]_0$  temos  $\Delta x_i < \delta$  para cada  $i \in [n]$ .

Agora,  $f$  é contínua em cada intervalo  $[x_{i-1}, x_i]$ , de modo que, pelo teorema de Weierstrass (7.43), existem  $a_i, b_i \in [x_{i-1}, x_i]$  tais que  $f(a_i) = m_i$  e  $f(b_i) = M_i$ , onde

$$M_i := \sup_{x \in [x_{i-1}, x_i]} f(x);$$

$$m_i := \inf_{x \in [x_{i-1}, x_i]} f(x).$$

Como  $|b_i - a_i| \leq \Delta x_i < \delta$  para todo  $i \in [n]$ , pela continuidade uniforme de  $f$

temos  $M_i - m_i = |f(b_i) - f(a_i)| < \frac{\epsilon}{b-a}$  para todo  $i \in [n]$ , de modo que

$$S^+(f, P) - S_-(f, P) = \sum_{i=1}^n (M_i - m_i) \Delta x_i < \frac{\epsilon}{b-a} \sum_{i=1}^n \Delta x_i = \epsilon.$$

Assim, pelo critério de integrabilidade,  $f$  é integrável. ■

**(b)** Como  $f$  é limitada, existe  $M \in \mathbb{R}_{>0}$  tal que  $|f(x)| \leq M$  para todo  $x \in [a, b]$ . Se  $f$  tem, digamos  $p \in \mathbb{N}$  pontos de descontinuidade, sejam eles  $x_j \in [a, b]$ , para cada  $j \in [p]$ . Agora, seja  $\epsilon \in \mathbb{R}_{>0}$  arbitrário. Para cada  $j \in [p]$ , tome  $[c_j, d_j]$  centrado em  $x_j$  tal que  $[c_i, d_i] \cap [c_j, d_j] = \emptyset$  se  $i \neq j$  e  $\sum_{j=1}^p (d_j - c_j) < \epsilon$ . Tomando  $[a_j, b_j] = [c_j, d_j] \cap [a, b]$  para cada  $j \in [p]$ , sendo  $A := [a, b] \setminus \bigcup_{j=1}^p ]a_j, b_j[$  temos que  $f$  é uniformemente contínua em  $A$ .

**Teorema 9.13. (a)** Toda função  $f : [a, b] \rightarrow \mathbb{R}$  monótona é integrável.

**(b)** Se a função  $f : [a, b] \rightarrow [m, M]$  é integrável e a função  $g : [m, M] \rightarrow \mathbb{R}$  é contínua, então a função  $g \circ f : [a, b] \rightarrow \mathbb{R}$  é integrável.

**Prova. (a)** Suponha, num primeiro caso, que  $f$  seja crescente. Com isso,  $f(a) \leq f(x) \leq f(b)$  para todo  $x \in [a, b]$  e  $f$  é limitada em  $[a, b]$ . Para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $n = n(\epsilon) \in \mathbb{N}$  suficientemente grande de modo que

$$n > \frac{(b-a)[f(b) - f(a)]}{\epsilon}.$$

Agora, a partição  $P : a = x_0 < \dots < x_n = b$  definida por  $x_i = a + i \cdot \frac{b-a}{n}$  para todo  $i \in [n] \cup \{0\}$  é tal que  $\Delta x_i = \frac{b-a}{n}$ ,  $M_i = f(x_i)$  e  $m_i = f(x_{i-1})$  (pois  $f$  é crescente), donde

$$\begin{aligned} S^+(f, P) - S_-(f, P) &= \sum_{i=1}^n \left[ M_i \frac{b-a}{n} \right] - \sum_{i=1}^n \left[ m_i \frac{b-a}{n} \right] \\ &= \frac{b-a}{n} \cdot \sum_{i=1}^n [f(x_i) - f(x_{i-1})] \\ &= \frac{b-a}{n} [f(b) - f(a)] \\ &< \epsilon. \end{aligned}$$

Assim, pelo critério de integrabilidade,  $f$  é integrável. No caso em que  $f$  é decrescente, a demonstração é análoga. ■

**(b)**

**Teorema 9.14.** Se  $f, g : [a, b] \rightarrow \mathbb{R}$  são funções integráveis em  $[a, b]$ , então

(a)  $f + g : [a, b] \rightarrow \mathbb{R}$  é integrável em  $[a, b]$  e

$$\int_a^b [f(x) + g(x)] dx = \int_a^b f(x) dx + \int_a^b g(x) dx.$$

(b)  $c \cdot f : [a, b] \rightarrow \mathbb{R}$  (onde  $c \in \mathbb{R}$  é uma constante) é integrável em  $[a, b]$  e

$$\int_a^b [c \cdot f(x)] dx = c \cdot \int_a^b f(x) dx.$$

(c)  $\int_a^b f(x) dx \leq \int_a^b g(x) dx$  sempre que  $f(x) \leq g(x)$  para todo  $x \in [a, b]$ .

(d)  $f \cdot g : [a, b] \rightarrow \mathbb{R}$  é integrável em  $[a, b]$ .

(e)  $|f| : [a, b] \rightarrow \mathbb{R}$  é integrável em  $[a, b]$  e

$$\left| \int_a^b f(x) dx \right| \leq \int_a^b |f(x)| dx.$$

**Prova.** Táboas, página 173.

**Proposição 9.15.** Se  $I \subseteq \mathbb{R}$  é um intervalo fechado e  $f : I \rightarrow \mathbb{R}$  é uma função integrável em  $I$ , então

$$\int_a^b f(x) dx = \int_a^c f(x) dx + \int_c^b f(x) dx$$

para quaisquer  $a, b, c \in I$ .

**Prova.**

### 9.3 O Teorema Fundamental do Cálculo

**Teorema 9.16.** Sejam  $I \subseteq \mathbb{R}$  um intervalo e  $f, g : I \rightarrow \mathbb{R}$  funções contínuas.

(a) Se  $f'(x) = 0$  para todo  $x \in I$  interior, então existe uma constante  $C \in \mathbb{R}$  tal que  $f(x) = C$  para todo  $x \in I$ .

(b) Se  $f'(x) = g'(x)$  para todo  $x \in I$  interior, então existe uma constante  $C \in \mathbb{R}$  tal que  $f(x) = g(x) + C$  para todo  $x \in I$ .

**Prova.**

**Definição 9.17.** Seja  $I \subseteq \mathbb{R}$  um intervalo. Diremos que a função  $F : I \rightarrow \mathbb{R}$  é uma *primitiva* da função  $f : I \rightarrow \mathbb{R}$  se  $F'(x) = f(x)$  para todo  $x \in I$ .

**Teorema 9.18.** (Fundamental do Cálculo, parte I) Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função integrável.

(a) A função  $F : [a, b] \rightarrow \mathbb{R}$  definida por

$$F(x) := \int_a^x f(t) dt$$

é uniformemente contínua em  $[a, b]$ .

(b) Se  $f$  é contínua em  $x_0 \in [a, b]$ , então  $F$  é derivável em  $x_0$  e  $F'(x_0) = f(x_0)$ .

**Prova.**

(a) Precisamos provar que para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que

$$|x - y| < \delta \Rightarrow |F(x) - F(y)| < \epsilon$$

para quaisquer  $x, y \in [a, b]$ . Como  $f$  é integrável,  $f$  é limitada, de modo que existe  $M \in \mathbb{R}_{>0}$  tal que  $|f(x)| \leq M$  para todo  $x \in [a, b]$ . Como, para quaisquer  $x, y \in [a, b]$ , temos

$$|F(x) - F(y)| = \left| \int_x^y f(t) dt \right| \leq |M(y - x)| = M|x - y|,$$

basta tomar  $\delta \leq \frac{\epsilon}{M}$ . De fato, se  $\delta = \frac{\epsilon}{M}$  e  $x, y \in [a, b]$  são tais que  $|x - y| < \frac{\epsilon}{M}$ , então  $|F(x) - F(y)| \leq M|x - y| < M \cdot \frac{\epsilon}{M} = \epsilon$ , como queríamos.

(b) Para provar que  $F$  é derivável em  $x_0$  e  $F'(x_0) = f(x_0)$ , basta provar que

$$\lim_{h \rightarrow 0} \left[ \frac{F(x_0 + h) - F(x_0)}{h} - f(x_0) \right] = 0.$$

Mais precisamente, basta provar que para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que

$$0 < |h| < \delta \Rightarrow \left| \frac{F(x_0 + h) - F(x_0)}{h} - f(x_0) \right| < \epsilon$$

para todo  $h \in \mathbb{R}_{\neq 0}$  tal que  $x_0 + h \in [a, b]$ . Da continuidade de  $f$  em  $x_0$ , para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta \in \mathbb{R}_{>0}$  tal que

$$|t - x_0| < \delta \Rightarrow |f(t) - f(x_0)| < \epsilon$$

para todo  $t \in [a, b]$ . Veja que todo  $h \in \mathbb{R}_{\neq 0}$  com  $0 < |h| < \delta$  e  $x_0 + h \in [a, b]$  é tal que  $|t - x_0| \leq |h| < \delta$  para todo  $t$  no intervalo definido por  $x_0$  e  $x_0 + h$  (especificamente,  $t \in [x_0, x_0 + h]$  se  $h > 0$  ou  $t \in [x_0 + h, x_0]$  se  $h < 0$ ), de modo que  $|f(t) - f(x_0)| < \epsilon$  para todo  $t$  no intervalo definido por  $x_0$  e  $x_0 + h$ . Com isso,

$$\begin{aligned} \left| \frac{F(x_0 + h) - F(x_0)}{h} - f(x_0) \right| &= \left| \frac{1}{h} \int_{x_0}^{x_0+h} [f(t) - f(x_0)] dt \right| \\ &\leq \frac{1}{|h|} \left| \int_{x_0}^{x_0+h} |f(t) - f(x_0)| dt \right| \\ &< \frac{1}{|h|} \left| \int_{x_0}^{x_0+h} \epsilon dt \right| = \frac{1}{|h|} \epsilon |h| = \epsilon, \end{aligned}$$

o que prova que

$$\lim_{h \rightarrow 0} \left[ \frac{F(x_0 + h) - F(x_0)}{h} - f(x_0) \right] = 0,$$

como havíamos afirmado. ■

(a)

(b)

**Corolário 9.19.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função contínua em  $[a, b]$ .

(a) A função  $F : [a, b] \rightarrow \mathbb{R}$  definida por

$$F(x) := \int_a^x f(t) dt$$

é uma primitiva de  $f$  em  $[a, b]$ .

(b) Se  $G : [a, b] \rightarrow \mathbb{R}$  é qualquer outra primitiva de  $f$ , então

$$G(x) = G(a) + \int_a^x f(t) dt$$

para todo  $x \in [a, b]$ . Particularmente para  $x = b$ , temos

$$\int_a^b f(t) dt = G(b) - G(a).$$

**Prova.**

**Teorema 9.20** (Fundamental do Cálculo, parte II). Se  $f : [a, b] \rightarrow \mathbb{R}$  é uma função integrável e  $F : [a, b] \rightarrow \mathbb{R}$  é uma primitiva qualquer de  $f$ , então

$$F(x) = F(a) + \int_a^x f(t) dt$$

para todo  $x \in [a, b]$ . Particularmente para  $x = b$ , temos

$$\int_a^b f(t) dt = F(b) - F(a).$$

**Prova.**

## 9.4 A Integral de Riemann

**Definição 9.21.** Seja  $P : a < x_0 \cdots < x_n = b$  uma partição do intervalo  $[a, b]$ .

- (a) Definimos  $\max \Delta x_i$  como a *norma* de  $P$ , a qual denotaremos por  $\|P\|$ , isto é,  $\|P\| := \max \Delta x_i$ .
- (b) (Partição marcada)
- (c) (Soma de Riemann)

**Definição 9.22.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função. Diremos que a soma de Riemann  $S(f, P, \xi)$  tem limite  $L \in \mathbb{R}$  quando  $\|P\|$  tende a 0, denotando isso por

$$\lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L,$$

se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon) \in \mathbb{R}_{>0}$  tal que

$$|S(f, P, \xi) - L| < \epsilon$$

para toda partição marcada  $(P, \xi)$  de  $[a, b]$  com  $\|P\| < \delta$ .

**Proposição 9.23.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função. O limite das somas de Riemann, quando existe, é único, isto é, se

$$\lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L_1 \quad \text{e} \quad \lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L_2,$$

então  $L_1 = L_2$ .

**Prova.**

**Definição 9.24.** Diremos que uma função  $f : [a, b] \rightarrow \mathbb{R}$  é *integrável em  $[a, b]$  segundo Riemann* se  $\lim_{\|P\| \rightarrow 0} S(f, P, \xi)$  existir. Nesse caso, esse número real será chamado de *integral de  $f$  em  $[a, b]$  segundo Riemann*, o qual será denotado por

$$\int_a^b f(x) dx,$$

isto é,

$$\int_a^b f(x) dx := \lim_{\|P\| \rightarrow 0} S(f, P, \xi).$$

**Proposição 9.25.** Se  $f : [a, b] \rightarrow \mathbb{R}$  é uma função integrável segundo Riemann, então  $f$  é limitada em  $[a, b]$ .

**Prova.**

**Teorema 9.26.** Seja  $f : [a, b] \rightarrow \mathbb{R}$  uma função.

- (a)  $f$  é integrável segundo Riemann se, e somente se, é integrável segundo Darboux.
- (b) Sendo  $f$  integrável, as integrais de Riemann e Darboux coincidem.

**Prova.**

## 9.5 Integrais Impróprias

**Definição 9.27.** Seja

# Capítulo 10

## Demonstrações

**Prova.** (a) Consideremos o caso em que  $x \rightarrow p$ . Como  $\lim_{x \rightarrow p} f(x) = L_1$  e  $\lim_{x \rightarrow p} f(x) = L_2$ , temos por definição que para todo  $\epsilon > 0$  existem  $\delta_1, \delta_2 > 0$  para os quais

$$\begin{aligned} 0 < |x - p| < \delta_1 &\Rightarrow |f(x) - L_1| < \frac{\epsilon}{2}; \\ 0 < |x - p| < \delta_2 &\Rightarrow |f(x) - L_2| < \frac{\epsilon}{2}. \end{aligned}$$

Tomando  $\delta := \min\{\delta_1, \delta_2\}$ , temos que para todo  $\epsilon > 0$  existe  $\delta > 0$  tal que

$$0 < |x - p| < \delta \Rightarrow |f(x) - L_1| + |f(x) - L_2| < \epsilon.$$

Com isso, temos que, para todo  $\epsilon > 0$ ,

$$\begin{aligned} |L_1 - L_2| &= |L_1 - f(x) + f(x) - L_2| \\ &\leq |L_1 - f(x)| + |f(x) - L_2| \\ &= |f(x) - L_1| + |f(x) - L_2| \\ &< \epsilon. \end{aligned}$$

Daí,  $L_1 = L_2$ . ■

(b) ■

(c) ■

(d) (Verificar) Como, por hipótese,  $\lim_{x \rightarrow p} f(x) = L = \lim_{x \rightarrow p} h(x)$ , temos

$$\forall \epsilon > 0, \exists \delta_1 > 0 : 0 < |x - p| < \delta_1 \Rightarrow L - \epsilon < f(x) < L + \epsilon;$$

$$\forall \epsilon > 0, \exists \delta_2 > 0 : 0 < |x - p| < \delta_1 \Rightarrow L - \epsilon < h(x) < L + \epsilon.$$

Pois tome  $\delta = \min \{\delta_1, \delta_2, r\}$ ; daí, vem

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow L - \epsilon < f(x) \leq g(x) \leq h(x) < L + \epsilon,$$

e então

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow L - \epsilon < g(x) < L + \epsilon,$$

isto é,  $\lim_{x \rightarrow p} g(x) = L$ .

**Prova. (a)** (Verificar) Consideremos o caso em que  $x \rightarrow p$ . Precisamos provar que

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow \lim_{u \rightarrow a} g(u) - \epsilon < g[f(x)] < \lim_{u \rightarrow a} g(u) + \epsilon.$$

Como  $\lim_{u \rightarrow a} g(u) = g(a)$ , temos que provar que

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow g(a) - \epsilon < g[f(x)] < g(a) + \epsilon. \quad (1)$$

Por definição,

$$\begin{aligned} \lim_{u \rightarrow a} g(u) = g(a) &\Leftrightarrow \forall \epsilon > 0, \exists \delta_1 > 0 : \\ &a - \delta_1 < u < a + \delta_1 \Rightarrow g(a) - \epsilon < g(u) < g(a) + \epsilon, \end{aligned}$$

sendo esta última parte equivalente a

$$a - \delta_1 < f(x) < a + \delta_1 \Rightarrow g(a) - \epsilon < g[f(x)] < g(a) + \epsilon. \quad (2)$$

Como, por hipótese,  $\lim_{x \rightarrow p} f(x) = a$ , temos que

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow a - \epsilon < f(x) < a + \epsilon. \quad (3)$$

Para  $\epsilon = \delta_1$  em (3), existe um  $\delta > 0$  tal que

$$0 < |x - p| < \delta \Rightarrow a - \delta_1 < f(x) < a + \delta_1. \quad (4)$$

Daí, (4), com (2), resulta que

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow g(a) - \epsilon < g[f(x)] < g(a) + \epsilon,$$

como queríamos provar. ■

**(b) (Verificar)** Precisamos provar que

$$\forall \epsilon > 0, \exists \delta > 0 : 0 < |x - p| < \delta \Rightarrow \left| g[f(x)] - \lim_{u \rightarrow a} g(u) \right| < \epsilon,$$

isto é,

$$0 < |x - p| < \delta \Rightarrow |g[f(x)] - L| < \epsilon.$$

Bem, por definição,

$$\lim_{u \rightarrow a} g(u) = g(a) \Leftrightarrow \forall \epsilon > 0, \exists \delta_1 > 0 : 0 < |u - a| < \delta_1 \Rightarrow |g(u) - L| < \epsilon.$$

Lembrando que  $u := f(x)$ , temos então

$$0 < |f(x) - a| < \delta_1 \Rightarrow |g[f(x)] - L| < \epsilon.$$

Por outro lado,

$$\lim_{x \rightarrow p} f(x) = a \Leftrightarrow \forall \epsilon > 0, \exists \delta_2 > 0 : 0 < |x - p| < \delta_2 \Rightarrow |f(x) - a| < \epsilon,$$

e então, tomando  $\epsilon = \delta_1$ ,  $0 < |x - p| < \delta_2 \Rightarrow |f(x) - a| < \delta_1$ .

Pois tome  $\delta = \{\delta_2, r\}$ ; teremos  $0 < |x - p| < \delta \Rightarrow 0 < |f(x) - a| < \delta_1$ .

**Prova.**

Um *designador* é uma expressão que é um termo ou uma fórmula. Como se vê na definição de termo e fórmula, todo designador tem a forma  $uv_1 \dots v_n$ , onde  $u$  é um símbolo,  $v_1, \dots, v_n$  são designadores, e  $n$  é um número natural determinado por  $u$ . Por exemplo, se  $u$  é uma variável, então  $n = 0$ ; se  $u$  é um símbolo funcional  $k$ -ário, então  $n = k$ ; se  $u$  é  $\exists$ , então  $n = 2$ . Chamamos  $n$  de *índice* de  $u$ .

Dizemos que duas expressões são *compatíveis* se uma delas pode ser obtida adicionando alguma expressão (possivelmente a expressão vazia) ao final da outra.

- Se  $uv$  e  $u'v'$  são compatíveis, então  $u$  e  $u'$  são compatíveis;
- se  $uv$  e  $uv'$  são compatíveis, então  $v$  e  $v'$  são compatíveis.

**Lema.** Seja  $n$  um natural fixo. Se  $u_1, \dots, u_n$  e  $u'_1, \dots, u'_n$  são designadores, e  $u_1 \dots u_n$  e  $u'_1 \dots u'_n$  são compatíveis, então  $u'_i$  é  $u_i$ , para  $i = 1, \dots, n$ .

**Prova.** Fazemos indução no comprimento de  $u_1 \dots u_n$ , isto é, no número de símbolos totais dessa expressão. Sendo  $|u_1 \dots u_n| = L$ , provemos que se o resultado vale para toda sequência de designadores de comprimento menor que  $L$ , então vale para as sequências de designadores de comprimento  $L$ . Escrevendo  $u_1$  como  $vv_1 \dots v_k$ , onde  $v$  é um símbolo e  $v_1, \dots, v_k$  são designadores, vemos que  $u'_1$  é da forma  $vv'_1 \dots v'_k$ , onde  $v'_1, \dots, v'_k$  são designadores. Agora, como  $u_1$  é compatível com  $u'_1$  (isso segue do primeiro bullet point, fazendo  $u$  ser  $u_1$ ,  $v$  ser  $u_2 \dots u_n$ ,  $u'$  ser  $u'_1$  e  $v'$  ser  $u'_2 \dots u'_n$ ), temos que  $vv_1 \dots v_k$  é compatível com  $vv'_1 \dots v'_k$ , de modo que  $v_1 \dots v_k$  é compatível com  $v'_1 \dots v'_k$  (isso segue do segundo bullet point). Como, evidentemente,  $|v_1 \dots v_k| < L$ , pela hipótese de indução concluímos que  $v_i$  é  $v'_i$  para cada  $i = 1, \dots, k$ . Com isso, temos que  $u_1$  é  $u'_1$ , de modo que  $u_2 \dots u_n$  é compatível com  $u'_2 \dots u'_n$  (pela segunda observação), e como  $|u_2 \dots u_n| < L$ , pela hipótese de indução concluímos que  $u_i$  é  $u'_i$  para  $i = 2, \dots, n$ . Isso nos dá a tese de indução, já que já sabemos que  $u_1$  é  $u'_1$ .

**Prova.** Fazemos indução forte no comprimento de  $u_1 \dots u_n$ , isto é, no número de símbolos totais dessa expressão. Sendo  $|u_1 \dots u_n| = L$ , provemos que se o resultado vale para toda sequência de designadores de comprimento menor que  $L$ , então vale para as sequências de designadores de comprimento  $L$ . Escrevendo  $u_1$  como  $vv_1 \dots v_k$ , onde  $v$  é um símbolo e  $v_1, \dots, v_k$  são designadores, vemos que  $u'_1$  é da forma  $vv'_1 \dots v'_k$ , onde  $v'_1, \dots, v'_k$  são designadores. Agora, como  $u_1$  é compatível com  $u'_1$  (isso segue da primeira observação “se  $uv$  e  $u'v'$  são compatíveis, então  $u$  e  $u'$  são compatíveis”, fazendo  $u$  ser  $u_1$ ,  $v$  ser  $u_2 \dots u_n$ ,  $u'$  ser  $u'_1$  e  $v'$  ser  $u'_2 \dots u'_n$ ), temos que  $vv_1 \dots v_k$  é compatível com  $vv'_1 \dots v'_k$ , de modo que  $v_1 \dots v_k$  é compatível com  $v'_1 \dots v'_k$  (isso segue da segunda observação “se  $uv$  e  $uv'$  são compatíveis, então  $v$  e  $v'$  são compatíveis”). Como, evidentemente,  $|v_1 \dots v_k| < L$ , pela hipótese de indução concluímos que  $v_i$  é  $v'_i$  para cada

$i = 1, \dots, k$ . Com isso, temos que  $\mathbf{u}_1$  é  $\mathbf{u}'_1$ , de modo que  $\mathbf{u}_2 \dots \mathbf{u}_n$  é compatível com  $\mathbf{u}'_2 \dots \mathbf{u}'_n$  (pela segunda observação), e como  $|\mathbf{u}_2 \dots \mathbf{u}_n| < L$ , pela hipótese de indução concluímos que  $\mathbf{u}_i$  é  $\mathbf{u}'_i$  para  $i = 2, \dots, n$ . Isso nos dá a tese de indução, já que já sabemos que  $\mathbf{u}_1$  é  $\mathbf{u}'_1$ .

Consideremos um conjunto enumerável correspondente aos símbolos do alfabeto e  $X$  o conjunto de todas as sequências finitas de símbolos. Seja  $Z$  o conjunto de todos os subconjuntos  $Y$  de  $X$  tais que

- as variáveis proposicionais pertencem a  $Y$ ;
- se  $A$  pertence a  $Y$ , então  $(\neg A)$  pertence a  $Y$ ;
- se  $A$  e  $B$  pertencem a  $Y$ , então  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$  e  $(A \leftrightarrow B)$  pertencem a  $Y$ .

**Teorema 10.1.** Suponha que uma propriedade vale para toda fórmula atômica e que, se vale para as fórmulas  $A$  e  $B$ , também vale para  $(\neg A)$ ,  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$  e  $(A \leftrightarrow B)$ . Então essa propriedade vale para todas as fórmulas da lógica proposicional.

**Prova.** Tomando  $F$  a interseção de  $Z$ , temos que  $F$  satisfaz as condições acima (isto é, pertence à família  $Z$ ) e é o menor conjunto (na ordem da inclusão) que pertence a  $Z$ . Isto é, se  $Y \in Z$ , então  $F \subset Y$ . Segue facilmente, daí, o teorema. Deixamos os detalhes ao leitor.

**Parte IV**

**Álgebra Linear**

# Capítulo 11

## Matrizes e Sistemas Lineares

### 11.1 Definições Iniciais e Operações Matriciais

**Definição 11.1. (a)** Sejam  $m, n \in \mathbb{N}$ . Uma *matriz*  $A = (a_{ij})_{m \times n}$  é uma função  $A : \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \rightarrow \mathbb{R}$  que associa a cada par  $(i, j)$ , com  $i \in [m]$  e  $j \in [n]$ , um elemento  $a_{ij} \in \mathbb{R}$ . A representação canônica de uma matriz é uma tabela com  $m$  linhas e  $n$  colunas

$$A := \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Dizemos que a matriz  $A$  definida acima tem *tamanho*, ou *tipo*,  $m \times n$  (lê-se  $m$  por  $n$ ). Dizemos que  $a_{ij}$ , ou  $[A]_{ij}$ , é o *elemento*, ou a *entrada*, de posição  $i, j$ . O conjunto de todas as matrizes de tamanho  $m \times n$  com entradas reais será denotado por  $\mathcal{M}_{m \times n}(\mathbb{R})$ .

**(b)** Duas matrizes são ditas *iguais* se elas são do mesmo tipo e se os elementos correspondentes forem iguais. Mais especificamente, as matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{p \times q}$  são iguais se  $m = p$ ,  $n = q$  e  $a_{ij} = b_{ij}$  para todos  $i \in [m]$  e  $j \in [n]$ .

**Definição 11.2.** Dada uma matriz  $A := (a_{ij})_{m \times n}$ , definimos

$$L_i(A) := [a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}]$$

como a  $i$ -ésima linha da matriz  $A$ , com  $i \in [m]$ . Definimos, ainda,

$$C_j(A) := \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

como a  $j$ -ésima coluna da matriz  $A$ , com  $j \in [n]$ .

## Operações Matriciais

**Definição 11.3.** A soma, ou *adição*, de duas matrizes do mesmo tipo  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$  é definida como a matriz  $C = (c_{ij})_{m \times n}$  em que  $c_{ij} = a_{ij} + b_{ij}$  para todos  $i \in [m]$  e  $j \in [n]$ . Denotamos isso com  $C = A + B$ .

**Proposição 11.4.** Para quaisquer matrizes  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$  e  $C = (c_{ij})_{m \times n}$ , valem

- (a) a associatividade da adição, isto é,  $A + (B + C) = (A + B) + C$ ;
- (b) a comutatividade da adição, isto é,  $A + B = B + A$ ;
- (c) a existência de um elemento neutro, isto é,  $A + 0 = A$ ;
- (d) a existência de um oposto aditivo, isto é,  $A + (-A) = 0$ .

**Prova.**

**Definição 11.5.** A multiplicação de uma matriz  $A = (a_{ij})_{m \times n}$  por um *escalar*  $\alpha$  é definida como a matriz  $B = (b_{ij})_{m \times n}$  em que  $b_{ij} = \alpha \cdot a_{ij}$  para todos  $i \in [m]$  e  $j \in [n]$ . Denotamos isso com  $B = \alpha \cdot A = \alpha A$ .

**Proposição 11.6.** Para quaisquer matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$  e escalares  $\alpha, \beta \in \mathbb{R}$ , temos que

- (a)  $\alpha \cdot (\beta \cdot A) = (\alpha \cdot \beta) \cdot A$ ;
- (b)  $\alpha \cdot (A + B) = \alpha \cdot A + \alpha \cdot B$ ;
- (c)  $(\alpha + \beta) \cdot A = \alpha \cdot A + \beta \cdot A$ ;
- (d)  $1 \cdot A = A$ .

**Prova.**

**Definição 11.7. (a)** O *produto*, ou *multiplicação*, de duas matrizes, em que o número de colunas da primeira matriz é igual ao número de linhas da segunda,

$A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{n \times p}$ , é definido como a matriz  $C = (c_{ij})_{m \times p}$  em que

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj},$$

para todos  $i \in [m]$  e  $j \in [p]$ . Denotamos isso por  $C = A \cdot B = AB$ .

**(b)** O produto de duas matrizes, em que o número de colunas da primeira matriz é igual ao número de linhas da segunda,  $A = (a_{ij})_{m \times n}$  e  $B = (b_{jk})_{n \times p}$  também pode ser definido como a matriz  $C = (c_{ik})_{m \times p}$  em que

$$c_{ik} = \sum_{j=1}^n a_{ij} b_{jk},$$

para todos  $i \in [m]$ ,  $k \in [p]$  e  $j \in [n]$ . Essa definição pode ser útil para evitar confusões com os índices.

**Proposição 11.8.** Para quaisquer matrizes  $A$ ,  $B$  e  $C$ , de tamanhos compatíveis, e escalares  $\alpha, \beta \in \mathbb{R}$ , valem

- (a)** a associatividade do produto, isto é,  $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ ;
- (b)** a existência de um elemento neutro, isto é  $A \cdot I = I \cdot A = A$ ;
- (c)** a distributividade da multiplicação com relação à adição, isto é,  $A \cdot (B + C) = A \cdot B + A \cdot C$  e  $(A + B) \cdot C = A \cdot C + B \cdot C$ ;
- (d)** a associatividade do produto de matrizes com relação ao produto por escalar, isto é,  $(\alpha \cdot A) \cdot B = \alpha \cdot (A \cdot B) = A \cdot (\alpha \cdot B)$ ;

**Prova.**

## Matrizes Especiais

**Definição 11.9.** Uma matriz  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$  é dita

1. *invertível à esquerda* se existir uma matriz  $B \in \mathcal{M}_{n \times m}(\mathbb{R})$  tal que  $BA = I_n$ ;
2. *invertível à direita* se existir uma matriz  $C \in \mathcal{M}_{n \times m}(\mathbb{R})$  tal que  $AC = I_m$ ;
3. *invertível*, ou ainda, *não singular*, se for invertível à esquerda e à direita;
4. *singular* se não for invertível.

**Proposição 11.10.** Se uma matriz possui uma matriz inversa, então ela é única.

**Prova.** Se  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$  é invertível, então, por definição, existem  $B \in \mathcal{M}_{n \times m}(\mathbb{R})$  e  $C \in \mathcal{M}_{n \times m}(\mathbb{R})$  tais que  $BA = I_n$  e  $AC = I_m$ . Com isso, basta ver que

$$B = BI_m = B(AC) = (BA)C = I_n C = C,$$

isto é,  $B = C$ .

## 11.2 Operações e Matrizes Elementares

Dada uma matriz, podemos

- trocar a posição de duas de suas linhas;
- multiplicar uma de suas linhas por um escalar;<sup>1</sup>
- e somar a uma de suas linhas uma outra linha que foi multiplicada por um escalar.

Estas são as chamadas *operações elementares*. Elas estão formalizadas na próxima definição e serão úteis no nosso estudo dos sistemas de equações lineares.

**Definição 11.11.** Sejam  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$  e  $p, q \in [m]$ , com  $p < q$ .

(a) Definimos  $A_{L_p \leftrightarrow L_q}$  como a matriz, também  $m \times n$ , tal que

$$L_i(A_{L_p \leftrightarrow L_q}) := \begin{cases} L_q(A) & \text{se } i = p \\ L_p(A) & \text{se } i = q \\ L_i(A) & \text{se } i \neq p, q \end{cases}.$$

(b) Seja  $\lambda \in \mathbb{R}^*$  um escalar. Definimos  $A_{L_p \leftarrow \lambda L_p}$  como a matriz, também  $m \times n$ , tal que

$$L_i(A_{L_p \leftarrow \lambda L_p}) := \begin{cases} \lambda L_p(A), & \text{se } i = p \\ L_i(A), & \text{se } i \neq p \end{cases}.$$

(c) Seja  $\lambda \in \mathbb{R}^*$  um escalar. Definimos  $A_{L_p \leftarrow L_p + \lambda L_q}$  como a matriz, também  $m \times n$ , tal que

$$L_i(A_{L_p \leftarrow L_p + \lambda L_q}) := \begin{cases} L_p(A) + \lambda L_q(A), & \text{se } i = p \\ L_i(A), & \text{se } i \neq p \end{cases},$$

---

<sup>1</sup>Esperamos ser evidente que nos referimos a uma multiplicação que ocorre em *cada entrada* da referida linha.

e definimos  $A_{L_q \leftarrow L_q + \lambda L_p}$  como a matriz, também  $m \times n$ , tal que

$$L_i(A_{L_q \leftarrow L_q + \lambda L_p}) := \begin{cases} L_q(A) + \lambda L_p(A), & \text{se } i = q \\ L_i(A), & \text{se } i \neq q \end{cases}.$$

Na proposição a seguir, mostramos que cada operação elementar equivale à multiplicar a matriz  $A$  por uma matriz dita *elementar*, obtida pela aplicação de operações elementares na matriz identidade  $I_m$ .

**Proposição 11.12.** Sejam  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$  e  $p, q \in [m]$ , com  $p < q$ .

(a) Temos  $I_{L_p \leftrightarrow L_q} \cdot A = A_{L_p \leftrightarrow L_q}$ .

(b) Temos  $I_{L_p \leftarrow \lambda L_p} \cdot A = A_{L_p \leftarrow \lambda L_p}$ .

(c) Temos  $I_{L_p \leftarrow L_p + \lambda L_q} \cdot A = A_{L_p \leftarrow L_p + \lambda L_q}$  e  $I_{L_q \leftarrow L_q + \lambda L_p} \cdot A = A_{L_q \leftarrow L_q + \lambda L_p}$ .

**Prova.**

**Proposição 11.13.** As operações (matrizes) elementares são invertíveis.

**Prova.** A demonstração é feita exibindo-se, explicitamente, as inversas.

- A inversa de  $I_{L_p \leftrightarrow L_q}$  é ela mesma, isto é,  $I_{L_p \leftrightarrow L_q} \cdot I_{L_p \leftrightarrow L_q} = I$ .
- A inversa de  $I_{L_p \leftarrow \lambda L_p}$  é  $I_{L_p \leftarrow \frac{1}{\lambda} L_p}$ , isto é,

$$I_{L_p \leftarrow \lambda L_p} \cdot I_{L_p \leftarrow \frac{1}{\lambda} L_p} = I_{L_p \leftarrow \frac{1}{\lambda} L_p} \cdot I_{L_p \leftarrow \lambda L_p} = I.$$

- A inversa de  $I_{L_q \leftarrow L_q + \lambda L_p}$  é  $I_{L_q \leftarrow L_q - \lambda L_p}$ , isto é,

$$I_{L_q \leftarrow L_q + \lambda L_p} \cdot I_{L_q \leftarrow L_q - \lambda L_p} = I_{L_q \leftarrow L_q - \lambda L_p} \cdot I_{L_q \leftarrow L_q + \lambda L_p} = I.$$

**Definição 11.14. (a)** (Informal) Uma matriz  $A$  é dita *equivalente por linhas* a uma matriz  $B$ , de mesmo tamanho, se existir uma sequência finita de operações elementares que, quando aplicadas em  $A$ , tem  $B$  como resultado. Denotamos isso por

$$E \cdot A = B, \text{ em que } E = E_k \cdot E_{k-1} \cdot \dots \cdot E_2 \cdot E_1,$$

em que  $E_i$  é uma matriz elementar para cada  $i \in [k]$ .

(b) Diremos que uma matriz  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$  é dita *equivalente por linhas* a uma matriz  $B \in \mathcal{M}_{m \times n}(\mathbb{R})$ , denotando isso por  $A \sim B$ , se existir uma sequência finita de matrizes elementares  $E_1, \dots, E_k \in \mathcal{M}_{m \times m}(\mathbb{R})$  tais que

$$E_k \cdot E_{k-1} \cdot \dots \cdot E_2 \cdot E_1 \cdot A = B.$$

**Proposição 11.15.** A equivalência por linhas definida em (11.14) é uma relação de equivalência.

### 11.3 Eliminação Gaussiana e Decomposição LU

**Definição 11.16. (a)** (Intuitiva) Uma matriz será dita *escalonada* se (i) o primeiro elemento não nulo de cada linha está à esquerda do primeiro elemento não nulo de cada uma das linhas seguintes e (ii) as linhas nulas (se houver) estão abaixo das demais.

**(b)** Uma matriz  $A = (a_{ij})_{m \times n}$  será dita *escalonada* se existir uma sequência de índices  $1 \leq b_1 < b_2 < \dots < b_r \leq n$  tal que  $a_{ib_i} \neq 0$  para todo  $i = 1, 2, \dots, r$  e  $a_{ij} = 0$  para todo  $1 \leq j < b_i$ . Os termos  $a_{ib_i}$  são chamados de *pivôs*, enquanto o número de pivôs,  $r$ , é chamado de *posto*.

**Proposição 11.17.** Toda matriz é equivalente por linhas a uma matriz escalonada.

**Prova.** Hefez, 32 e 44.

**Definição 11.18. (a)** (Intuitiva) Uma matriz escalonada será dita *reduzida* se todo pivô for unitário e se todos os outros elementos da coluna de um pivô forem iguais a 0.

**(b)** Uma matriz  $A = (a_{ij})_{m \times n}$  será dita *escalonada reduzida* se existir uma sequência de índices  $1 \leq b_1 < b_2 < \dots < b_r \leq n$  tal que  $a_{ib_i} = 1$  para todo  $1 \leq i \leq r$ ,  $a_{kb_i} = 0$  para todo  $k \neq i$  e  $a_{ij} = 0$  para todo  $1 \leq j < b_i$ .

**Teorema 11.19.** Toda matriz é equivalente por linhas a uma única matriz escalonada reduzida.

**Prova.** Hefez, 32 e 44. Reginaldo, 68.

**Proposição 11.20.** Se  $A \in \mathcal{M}_{n \times n}(\mathbb{R})$  é uma matriz escalonada reduzida e  $A \neq I_n$ , então  $A$  possui pelo menos uma linha nula.

**Prova.** Reginaldo, 47.

### 11.4 Sistemas Lineares

**Definição 11.21. (a)** Uma *equação linear* nas incógnitas  $x_1, x_2, \dots, x_n$  é qualquer equação do tipo

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b,$$

onde  $a_1, a_2, \dots, a_n, b \in \mathbb{R}$ . Cada  $a_i$  é chamado de *coeficiente*, enquanto  $b$  é chamado de *termo independente*.

(b) O conjunto das soluções de uma equação linear é

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n : a_1x_1 + \dots + a_nx_n = b\}.$$

**Definição 11.22. (a)** Definimos *sistema de equações lineares* como todo conjunto finito de equações lineares nas incógnitas  $x_1, x_2, \dots, x_n$ . Com  $m$  equações, a representação canônica é

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}.$$

Por simplicidade, diremos apenas *sistema linear*, ou ainda, apenas *sistema*, em vez de sistema de equações lineares.

(b) O conjunto das soluções de um sistema linear é

$$\bigcap_{i=1}^m \{(x_1, \dots, x_n) \in \mathbb{R}^n : a_{i1}x_1 + \dots + a_{in}x_n = b_i\}.$$

**Fato 11.23.** Todo sistema linear

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}.$$

pode ser representado matricialmente como  $Ax = b$ , onde

$$A := \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}_{m \times n} \quad x := \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n \times 1} \quad b := \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}_{m \times 1}.$$

Observe que  $A \in \mathcal{M}_{m \times n}(\mathbb{R})$ ,  $x \in \mathcal{M}_{n \times 1}(\mathbb{R})$  e  $b \in \mathcal{M}_{m \times 1}(\mathbb{R})$ . Trabalharemos, preferencialmente, com a forma matricial dos sistemas lineares, tendo em mente que as abordagens são equivalentes.

**Definição 11.24.** Seja  $Ax = b$  um sistema linear como acima.

(a) Denominamos a matriz  $A$  como a *matriz incompleta*, ou ainda, a *matriz*, desse sistema. Ela também é chamada de *matriz de coeficientes*.

(b) Denominamos a matriz

$$[A|b] := \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{bmatrix}_{m \times (n+1)}$$

como a *matriz completa*, ou a *matriz aumentada*, desse sistema.

**Definição 11.25.** Um sistema linear é dito *possível* se ele tiver pelo menos uma solução. Se houver mais de uma solução, ele será dito *possível e indeterminado*, no sentido do resultado a seguir; se a solução for única, então ele será dito *possível e determinado*. Por fim, se não houver solução alguma, ele será dito *impossível*.

**Teorema 11.26.** Se um sistema linear  $Ax = b$  tem (pelo menos) duas soluções distintas, então, na verdade, ele tem infinitas soluções distintas.

**Prova.** Se  $x_1 \neq x_2$  são soluções, então  $x_3 := \lambda x_1 + (1 - \lambda)x_2$ , para qualquer  $\lambda \in \mathbb{R}$ , também é uma solução. De fato, basta observar que  $Ax_3 = A[\lambda x_1 + (1 - \lambda)x_2] = b$ .

**Definição 11.27.** Diremos que dois sistemas de equações lineares são equivalentes se eles têm o mesmo conjunto solução.

**Proposição 11.28.** Os sistemas lineares  $Ax = b$  e  $Cx = d$  são equivalentes se, e somente se, as matrizes  $[A|b]$  e  $[C|d]$  são equivalentes por linhas.

**Prova.** Reginaldo, 32.

**Definição 11.29.** Um sistema de equações lineares em que todos os termos independentes são nulos, isto é,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases},$$

ou ainda, em notação matricial,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

é dito *homogêneo*.

**Proposição 11.30.** Todo sistema homogêneo é possível.

**Prova.** Basta ver que  $x = 0_{n \times 1}$  é uma solução, dita *trivial*.

**Teorema 11.31.** Todo sistema linear homogêneo em que o número de incógnitas é maior que o número de equações possui uma solução não trivial (e, portanto, possui infinitas soluções).

**Prova.** Elon, 27

# Capítulo 12

## Espaços Vetoriais

### 12.1 Espaços e Subespaços Vetoriais

**Definição 12.1.** Uma tripla  $(V, +, \cdot)$  é um *espaço vetorial real* se no conjunto  $V \neq \emptyset$  existem duas operações,  $+: V \times V \rightarrow V$  e  $\cdot: \mathbb{R} \times V \rightarrow V$ , para as quais

- A1:  $u + (v + w) = (u + v) + w$  para quaisquer  $u, v, w \in V$ ;
- A2:  $u + v = v + u$  para quaisquer  $u, v \in V$ ;
- A3: existe  $0_V \in V$  tal que  $u + 0_V = u$  para todo  $u \in V$ ;
- A4: para cada  $u \in V$  existe  $v \in V$  tal que  $u + v = 0_V$ ;
- M1:  $\lambda_1 \cdot (\lambda_2 \cdot u) = (\lambda_1 \cdot \lambda_2) \cdot u$  para quaisquer  $u \in V$  e  $\lambda_1, \lambda_2 \in \mathbb{R}$ ;
- M2:  $(\lambda_1 + \lambda_2) \cdot u = \lambda_1 \cdot u + \lambda_2 \cdot u$  para quaisquer  $u \in V$  e  $\lambda_1, \lambda_2 \in \mathbb{R}$ ;
- M3:  $\lambda_1 \cdot (u + v) = \lambda_1 \cdot u + \lambda_1 \cdot v$  para quaisquer  $u, v \in V$  e  $\lambda_1 \in \mathbb{R}$ ;
- M4:  $1 \cdot u = u$  para todo  $u \in V$ .

Os elementos de  $V$  são chamados de *vetores*. Para simplificar a notação, e quando não houver perigo de confusão, pomos  $0 := 0_V$ ,  $\lambda v := \lambda \cdot v = \mathbf{e} - v := w$  se  $v + w = 0$ . Vamos nos referir ao espaço vetorial  $(V, +, \cdot)$  simplesmente como o conjunto  $V$ .

**Exemplo 12.2.**

- (a) O espaço  $\mathbb{R}^n$ , com soma e produto por escalar usuais, é um espaço vetorial.
- (b) O conjunto  $\mathbb{R}^X$  de todas as funções reais  $f: X \subseteq \mathbb{R} \rightarrow \mathbb{R}$ , com soma e produto por escalar usuais, é um espaço vetorial.

- (c) O conjunto  $\mathcal{P}(\mathbb{R})$  de todos os polinômios em  $x$ , com soma e multiplicação por escalar usuais, é um espaço vetorial.
- (d) O conjunto  $\mathbb{R}_{>0}$  dos números reais positivos, com as operações  $x \oplus y := x \cdot y$  e  $\alpha \odot x := x^\alpha$ , é um espaço vetorial.

**Prova.**

**Proposição 12.3.** Seja  $(V, +, \cdot)$  um espaço vetorial. Valem as seguintes afirmações.

- (a) (Unicidade)
- (b) (Integridade) Para quaisquer  $u \in V$  e  $\lambda \in \mathbb{R}$ , temos
- i.  $\lambda \cdot 0_V = 0_V$ ;
  - ii.  $0 \cdot u = 0_V$ ;
  - iii. se  $\lambda \cdot u = 0_V$ , então  $\lambda = 0$  ou  $u = 0_V$ .
- (c) (Sinais) Para quaisquer  $u \in V$  e  $\lambda \in \mathbb{R}$ , temos
- i.  $(-1) \cdot u = -u$ ;
  - ii.  $-(-u) = u$ ;
  - iii.  $(-\lambda) \cdot u = \lambda(-u) = -(\lambda \cdot u)$ .
- (d) (Lei do Corte) Para quaisquer  $u, v, w \in V$  e  $\lambda, \lambda_1, \lambda_2 \in \mathbb{R}$ , vale
- i.  $u + w = v + w \Rightarrow u = v$ ;
  - ii.  $\lambda \neq 0 \wedge \lambda \cdot u = \lambda \cdot v \Rightarrow u = v$ ;
  - iii.  $v \neq 0_V \wedge \lambda_1 u = \lambda_2 u \Rightarrow \lambda_1 = \lambda_2$ .
- (e) Se  $V \neq \{0\}$ , então  $V$  é infinito.

**Prova.**

**Definição 12.4.** Um espaço vetorial  $(W, +, \cdot)$  é um *subespaço vetorial* de um espaço vetorial  $(V, +, \cdot)$  se  $W \subseteq V$ .

**Teorema 12.5.** Uma tripla  $(W, +, \cdot)$  é um subespaço vetorial de  $(V, +, \cdot)$  se  $W \subseteq V$  e  $u + v, \lambda \cdot v \in W$  para quaisquer  $u, v \in W$  e  $\lambda \in \mathbb{R}$ .

**Definição 12.6.** Seja  $V$  um espaço vetorial. Um subconjunto  $W \subseteq V$  é um *subespaço vetorial* de  $V$  se  $u + v \in W$  e  $\lambda u \in W$  para quaisquer  $u, v \in W$  e  $\lambda \in \mathbb{R}$ .

**Corolário 12.7.** Sejam  $V$  um espaço vetorial. Se  $u + \lambda \cdot v \in W$  para quaisquer  $u, v \in W \subseteq V$  e  $\lambda \in \mathbb{R}$ , então  $W$  é um subespaço vetorial de  $V$ .

**Prova.** Particularmente para  $\lambda = 1$ , temos  $u + v \in W$ . Particularmente para  $v = 0_V$ , temos  $\lambda u \in W$ . ■

**Proposição 12.8.** Se  $V$  é um espaço vetorial e  $W \subseteq V$  é um subespaço, então  $W$  é um espaço vetorial.

**Prova.** Para provar que  $W$  é um espaço vetorial, precisamos verificar que (i) existem operações  $+$  e  $\cdot$  bem definidas em  $W$  e que (ii) essas operações satisfazem as propriedades A1–A4 e M1–M4 de um espaço vetorial.

- i. Como esperado, as operações  $+$  e  $\cdot$  de  $W$  serão as mesmas de  $V$ : como  $V$  é um espaço vetorial, as operações  $+$  e  $\cdot$ , bem definidas em  $V$ , também estão bem definidas em qualquer subconjunto não vazio de  $V$ ; em particular, também em  $W$ . Por exemplo, podemos tomar  $w_1, w_2 \in W$  e considerar sua soma,  $w_1 + w_2$ , porque  $W \subset V \Rightarrow w_1, w_2 \in V$  e, em  $V$ , a operação  $+$  está bem definida.
- ii. O fechamento das operações  $+$  e  $\cdot$  em  $W$  garantem, de cara, A1–A2 e M1–M4. Falta, então, provar A3 e A4. Dado  $w \in W$ , temos que  $0_V = 0 \cdot w \in W$ ; com isso, tomando  $0_W := 0_V$ , teremos um elemento neutro de  $+$  em  $W$  porque  $w + 0_W = w + 0_V = w$ . Por fim, dado  $w \in W$ ,  $-w = (-1) \cdot w \in W$ , e então o oposto aditivo de  $w \in W$  está em  $W$ .

Logo,  $W$  é um espaço vetorial, como queríamos.

**Exemplo 12.9.**

- (a) Todo espaço vetorial  $V$  tem pelo menos dois subespaços vetoriais, dito *triviais*:  $\{0_V\}$  e o próprio  $V$ .
- (b) O conjunto  $\mathcal{P}_n(\mathbb{R})$  dos polinômios de grau menor ou igual a  $n$ , juntamente com o polinômio nulo, é um subespaço de  $\mathcal{P}(\mathbb{R})$ .

**Prova.** (a) Elon, 10. Reginaldo, 26.

**Proposição 12.10** (Interseção de subespaços). Se  $W_1$  e  $W_2$  são dois subespaços vetoriais de um espaço vetorial  $V$ , então

- (a)  $W_1 \cap W_2$  é um subespaço vetorial;
- (b)  $W_1 \cup W_2$  é um subespaço vetorial se, e somente se,  $W_1 \subset W_2$  ou  $W_2 \subset W_1$ .

**Prova.**

- (a) Para quaisquer  $u, v \in W_1 \cap W_2$ , temos, em particular,  $u, v \in W_1$  e  $u, v \in W_2$ . Como  $W_1$  e  $W_2$  são espaços vetoriais, temos que  $u + \lambda v \in W_1$  e  $u + \lambda v \in W_2$  para todo  $\lambda \in \mathbb{R}$ , donde  $u + \lambda v \in W_1 \cap W_2$ . Logo  $W_1 \cap W_2$  é um subespaço vetorial de  $V$ . ■
- (b) Por contradição, suponha que existam  $w_1 \in W_1$  e  $w_2 \in W_2$  tais que  $w_1 \notin W_2$  e  $w_2 \notin W_1$ . Como, por hipótese,  $W_1 \cup W_2$  é um subespaço vetorial,

$w := w_1 + w_2 \in W_1 \cup W_2$ , isto é,  $w \in W_1$  ou  $w \in W_2$ .

- Se  $w \in W_1$ , então  $w + (-w_1) = w_2 \in W_1$ , absurdo!
- Se  $w \in W_2$ , então  $w + (-w_2) = w_1 \in W_2$ , absurdo!

Logo, a prova da ida está completa. A volta é evidente. Logo, a prova está completa.

**Corolário 12.11.** Seja  $V$  um espaço vetorial e  $I$  um conjunto de índices. Se para cada  $\lambda \in I$  o conjunto  $W_\lambda \subseteq V$  for um subespaço vetorial de  $V$ , então  $\bigcap_{\lambda \in I} W_\lambda$  é ainda um subespaço vetorial de  $V$ .

**Prova.** Elon, 10.

**Definição 12.12.** Sejam  $W_1$  e  $W_2$  subespaços vetoriais de um espaço vetorial  $V$ .

- (a) (Soma de subespaços) Definimos  $W_1 + W_2$  como sendo o conjunto de todos os vetores de  $V$  que são soma de um elemento de  $W_1$  com um elemento de  $W_2$ , isto é,

$$W_1 + W_2 := \{v \in V : \exists w_1 \exists w_2 (w_1 \in W_1 \wedge w_2 \in W_2 \wedge v = w_1 + w_2)\}.$$

- (b) (Soma direta) Diremos que  $W_1 \oplus W_2 := W_1 + W_2$  é a *soma direta* de  $W_1$  e  $W_2$  se  $W_1 \cap W_2 = \{0_V\}$ .

**Proposição 12.13.** Nos termos da definição acima,  $W_1 + W_2$  é um subespaço vetorial de  $V$ .

**Prova.** Veja inicialmente que  $W_1, W_2 \subset W_1 + W_2$ .

- i. Se  $u, v \in W_1 + W_2$ , então existem  $u_1, v_1 \in W_1$  e  $u_2, v_2 \in W_2$  tais que  $u = u_1 + u_2$  e  $v = v_1 + v_2$ . Com isso,

$$u + v = (u_1 + u_2) + (v_1 + v_2) = \underbrace{(u_1 + v_1)}_{\in W_1} + \underbrace{(u_2 + v_2)}_{\in W_2},$$

de modo que  $u + v$  é a soma de um vetor de  $W_1$  com um vetor de  $W_2$ , isto é,  $u + v \in W_1 + W_2$ .

- ii. Se  $u \in W_1 + W_2$ , então existem  $u_1 \in W_1$  e  $u_2 \in W_2$  tais que  $u = u_1 + u_2$ . Com isso, para qualquer  $\lambda \in \mathbb{R}$ ,

$$\lambda u = \lambda(u_1 + u_2) = \underbrace{\lambda u_1}_{\in W_1} + \underbrace{\lambda u_2}_{\in W_2},$$

de modo que  $\lambda u$  é a soma de um vetor de  $W_1$  com um vetor de  $W_2$ , isto é,  $\lambda u \in W_1 + W_2$ .

Assim,  $W_1 + W_2$  é um subespaço vetorial de  $V$ .

**Teorema 12.14.** Sejam  $W_1$  e  $W_2$  dois subespaços vetoriais de um espaço vetorial  $V$ . Teremos  $V = W_1 \oplus W_2$  se, e somente se, para cada  $v \in V$  existirem únicos  $w_1 \in W_1$  e  $w_2 \in W_2$  tais que  $v = w_1 + w_2$ .

**Prova.** ( $\Rightarrow$ ) Se  $V = W_1 \oplus W_2$ , então temos a existência da decomposição. Provemos, então, sua unicidade. Dado  $v \in V$ , sejam  $v_1, w_1 \in W_1$  e  $v_2, w_2 \in W_2$  tais que  $v = v_1 + v_2 = w_1 + w_2$ . Somando  $[(-w_1) + (-v_2)]$ , vem

$$\begin{aligned} v &= v_1 + v_2 = w_1 + w_2 \\ v_1 + v_2 + [(-w_1) + (-v_2)] &= w_1 + w_2 + [(-w_1) + (-v_2)] \\ \underbrace{v_1 + (-w_1)}_{\in W_1} &= \underbrace{w_2 + (-v_2)}_{\in W_2}. \end{aligned}$$

Como  $W_1 \cap W_2 = \{0\}$ , temos então que  $v_1 = w_1$  e  $v_2 = w_2$ , como queríamos.

( $\Leftarrow$ ) Segue da hipótese que  $V = W_1 + W_2$ ; provemos, então, que  $W_1 \cap W_2 = \{0\}$ . Como  $W_1 \cap W_2 \neq \emptyset$  (pelo menos  $0 \in W_1 \cap W_2$ ), tome  $v \in W_1 \cap W_2$ , para o qual, por hipótese, existem únicos  $w_1 \in W_1$  e  $w_2 \in W_2$ . Com isso, temos

$$v = \underbrace{w_1}_{\in W_1} + \underbrace{w_2}_{\in W_2} = \underbrace{(w_1 + v)}_{\in W_1} + \underbrace{(w_2 + (-v))}_{\in W_2},$$

e como a decomposição é única, temos  $w_1 = w_1 + v$  e  $w_2 = w_2 - v$ , donde  $v = 0$ . Logo,  $W_1 \cap W_2 = \{0\}$ , como queríamos.

**Exemplo 12.15.** O conjunto das funções reais pares,

$$W_1 = \{f \in \mathbb{R}^{\mathcal{X}} : \forall x (x \in \mathcal{X} \subseteq \mathbb{R} \rightarrow f(-x) = f(x))\},$$

bem como o conjunto das funções reais ímpares,

$$W_2 = \{f \in \mathbb{R}^{\mathcal{X}} : \forall x (x \in \mathcal{X} \subseteq \mathbb{R} \rightarrow f(-x) = -f(x))\}$$

são subespaços de  $\mathbb{R}^{\mathcal{X}}$ . E ainda, temos que  $\mathbb{R}^{\mathcal{X}} = W_1 \oplus W_2$ .

**Prova.** Reginaldo, 35.

## 12.2 Combinações Lineares e Geradores

**Definição 12.16.** Seja  $(V, +, \cdot)$  um espaço vetorial. Um vetor  $u \in V$  é uma *combinação linear* dos vetores  $u_1, u_2, \dots, u_n \in V$  se existem escalares  $\lambda_1, \lambda_2, \dots, \lambda_n \in$

$\mathbb{R}$  para os quais

$$u = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n = \sum_{i=1}^n \lambda_i u_i.$$

**Teorema 12.17.** Seja  $V$  um espaço vetorial e  $\emptyset \neq S \subseteq V$  um subconjunto de vetores de  $V$ . O conjunto de todas as combinações lineares dos vetores de  $S$ , que denotaremos por  $[S]$ , é um subespaço vetorial de  $V$ .

**Prova.** Se  $u, v \in [S]$ , então, por definição, existem vetores e escalares

$$\begin{aligned} u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_m &\in S \\ \lambda_1, \lambda_2, \dots, \lambda_n, \alpha_1, \alpha_2, \dots, \alpha_m &\in \mathbb{R} \end{aligned}$$

para os quais  $u = \sum_{i=1}^n \lambda_i u_i$  e  $v = \sum_{i=1}^m \alpha_i v_i$ . Com isso, para qualquer  $\lambda \in \mathbb{R}$ ,

$$u + \lambda v = \sum_{i=1}^n \lambda_i u_i + \sum_{i=1}^m (\lambda \alpha_i) v_i,$$

de modo que  $u + \lambda v$  é uma combinação linear de vetores de  $S$ , isto é,  $u + \lambda v \in [S]$ . Logo, pelo resultado (12.7),  $[S]$  é um subespaço vetorial de  $V$ .

**Definição 12.18.** Sejam  $V$  um espaço vetorial e  $\emptyset \neq S \subseteq V$  um subconjunto de vetores de  $V$ .

- (a) Diremos que  $[S]$  é o *subespaço gerado* por  $S$ , ou que  $S$  *gera*  $[S]$ . Diremos, ainda, que os elementos de  $S$  são *geradores* de  $[S]$ .
- (b) Se  $S$  é finito e  $[S] = V$ , diremos que  $V$  é *finitamente gerado* e que  $S$  é um *conjunto de geradores* para (ou de)  $V$ .
- (c) Convenciona-se pôr  $[\emptyset] = \{0\}$ .

**Proposição 12.19.** Sejam  $V$  um espaço vetorial e  $\emptyset \neq S, T \subseteq V$  subconjuntos de vetores de  $V$ . Valem as seguintes afirmações.

- (a)  $S \subseteq [S]$ .
- (b)  $[[S]] = [S]$ .
- (c) Se  $S$  é um subespaço vetorial, então  $[S] = S$ .
- (d)  $S \subset T \Rightarrow [S] \subset [T]$ .
- (e)  $[S \cup T] = [S] + [T]$ .

**Prova.**

- (a) Se  $u \in S$ , então  $u = 1u \in [S]$ . ■
- (b) Pelo item anterior,  $[S] \subseteq [[S]]$ . Agora, se  $u \in [[S]]$ , então  $u$  é uma combinação linear de vetores de  $[S]$ , que por sua vez são combinações lineares de vetores de  $[S]$ , de modo que  $u \in [S]$ . Assim,  $[[S]] \subseteq [S]$ , de modo que  $[[S]] = [S]$ . ■
- (c) Se  $u \in [S]$ , então  $u$  é uma combinação linear de elementos de  $S$ ; como  $S$  é um subespaço vetorial, temos então  $u \in S$ , de modo que  $[S] \subseteq S$ . Como  $S \subseteq [S]$ , temos então  $[S] = S$ . ■
- (d) Se  $u \in S$ , então existem vetores  $u_1, \dots, u_n \in S$  e escalares  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$  tais que  $u = \lambda_1 u_1 + \dots + \lambda_n u_n$ . Como  $u_1, \dots, u_n \in S$ , por ser  $S \subseteq T$  vem  $u_1, \dots, u_n \in T$ , de modo que  $\lambda_1 u_1 + \dots + \lambda_n u_n \in T$ . ■
- (e)

## 12.3 Dependência e Independência Linear

**Definição 12.20.** Seja  $(V, +, \cdot)$  um espaço vetorial.

- (a) Os vetores  $u_1, u_2, \dots, u_n \in V$  são *linearmente independentes* (L.I.) se a equação

$$\lambda_1 u_1 + \lambda_2 u_2 + \dots + \lambda_n u_n = 0$$

possuir somente a solução trivial  $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ . Caso contrário, ou seja, se existir pelo menos uma solução com pelo menos um  $\lambda_i \neq 0$ , diremos que os vetores  $u_1, u_2, \dots, u_n \in V$  são *linearmente dependentes* (L.D.).

- (b) Um subconjunto finito  $S \subseteq V^1$  é L.D. (L.I.) se os vetores de  $S$  são L.D. (L.I.).
  - i. Um subconjunto infinito  $S \subseteq V$  é L.D. se pelo menos um subconjunto finito de  $S$  é L.D..
  - ii. Um subconjunto infinito  $S \subseteq V$  é L.I. se todo subconjunto finito de  $S$  é L.I..

**Proposição 12.21.** Sejam  $(V, +, \cdot)$  um espaço vetorial e  $S \subseteq V$  não vazio. Valem as seguintes afirmações.

- (a) Se  $|S| = 1$  e  $0_V \notin S$ , então  $S$  é L.I..
- (b)  $S$  é L.D. se, e somente se, pelo menos um vetor de  $S$  é combinação linear de outros vetores de  $S$ .

<sup>1</sup>Sendo  $S$  finito, só pode ser  $S = V$  se for  $V = \{0\}$ .

Equivalentemente, pela contrapositiva,  $S$  é L.I. se, e somente se, nenhum vetor de  $S$  é combinação linear de outros vetores de  $S$ .

(c) Se  $0_V \in S$ , então  $S$  é L.D..

Equivalentemente, pela contrapositiva, se  $S$  é L.I., então  $0_V \notin S$ .

(d) Suponha  $S$  L.I. e seja  $u \in V$ . Se  $S \cup \{u\}$  é L.D., então  $u \in [S]$ .

Equivalentemente, pela contrapositiva, se  $u \notin [S]$ , então  $S \cup \{u\}$  é L.I..

(e) Sejam  $S_1, S_2 \neq \emptyset$  subconjuntos de  $V$  tais que  $S_1 \subseteq S_2$ . Temos que

i. se  $S_1$  é L.D., então  $S_2$  também é L.D..

ii. se  $S_2$  é L.I., então  $S_1$  também é L.I..

(f) Se  $S$  é finito e L.I., então cada vetor  $u \in [S]$  se escreve de maneira única como combinação linear de vetores de  $S$ .

(g) Se  $u \in S$  é tal que  $u \in [S \setminus \{u\}]$ , então  $[S] = [S \setminus \{u\}]$ .

**Prova.**

(a) Sendo  $S = \{u\}$ , se  $\lambda \cdot u = 0_V$  então  $\lambda \neq 0$  já que  $u \neq 0_V$ . Logo  $S$  é L.I. ■

(b) ( $\Rightarrow$ ) Se  $S$  é L.D., então existem  $v_1, v_2, \dots, v_n \in S$  para os quais vale

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0$$

com  $\lambda_i \neq 0$  para pelo menos um  $i \in [n]$ . Suponha, sem perda de generalidade, que  $i = 1$ , isto é, que  $\lambda_1 \neq 0$ ; com isso,

$$v_1 = \left( \frac{-\lambda_2}{\lambda_1} \right) v_2 + \left( \frac{-\lambda_3}{\lambda_1} \right) v_3 + \dots + \left( \frac{-\lambda_n}{\lambda_1} \right) v_n,$$

de modo que  $v_1 \in S$  é combinação linear de  $v_2, v_3, \dots, v_n \in S$ .

( $\Leftarrow$ ) Se  $v = \lambda_1 v_1 + \dots + \lambda_n v_n$ , com  $v_1, \dots, v_n \in V$  e  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ , então

$$\lambda_1 v_1 + \dots + \lambda_n v_n + (-1)v = 0;$$

como  $-1 \neq 0$ , temos, por definição, que  $S$  é L.D. ■

(c) Basta ver que  $0_V$  é combinação linear de quaisquer  $v_1, v_2, \dots, v_n \in V$ : temos  $0_V = 0v_1 + 0v_2 + \dots + 0v_n$ . Assim, pelo item anterior,  $S$  é L.D. ■

(d)

(e)

(f)

(g) Esta afirmação nos diz que se um vetor de  $S$  é combinação linear de outros vetores de  $S$ , então ele pode ser removido do subespaço gerado por  $S$  sem alterá-lo.

## 12.4 Base e Dimensão

**Lema 12.22.** Seja  $(V, +, \cdot)$  um espaço vetorial. Se um subconjunto finito  $S \subseteq V$  é L.I., então todo subconjunto  $T \subseteq [S]$  tal que  $|T| = |S| + 1$  é L.D..

**Prova.** Fazemos indução em  $|S|$ . Se  $|S| = 1$ , então  $S = \{u_1\}$ , com  $u_1 \neq 0_V$  já que  $S$  é L.I.. Tomando  $v_1, v_2 \in [S]$  distintos, existem escalares  $\lambda_1, \lambda_2 \in \mathbb{R}$  tais que  $v_1 = \lambda_1 u_1$  e  $v_2 = \lambda_2 u_1$ . Multiplicando  $v_1$  por  $\lambda_2$  e  $v_2$  por  $\lambda_1$ , obtemos

$$\lambda_2 v_1 - \lambda_1 v_2 = 0_V,$$

isto é, uma combinação linear não trivial dos vetores de  $T = \{v_1, v_2\}$ , de modo que eles são L.D.. Isso completa a base de indução. Suponha então, por hipótese de indução, que o resultado vale para subconjuntos de  $V$  de  $n - 1$  vetores. Agora, sejam  $S = \{u_1, \dots, u_n\} \subsetneq V$  e  $T = \{v_1, \dots, v_n, v_{n+1}\} \subseteq [S]$ . Provemos que  $T$  é L.D.. Como  $v_i \in [S]$  para todo  $i \in [n + 1]$ , existem escalares  $a_{ij} \in \mathbb{R}$ , com  $i \in [n + 1]$  e  $j \in [n]$ , tais que

$$v_i = a_{i1}u_1 + \dots + a_{in}u_n$$

para todo  $i \in [n + 1]$ .

- $a_{i1} = 0$  para todo  $i \in [n + 1]$ . Nesse caso, temos

$$v_i = a_{i2}u_2 + \dots + a_{in}u_n$$

para todo  $i \in [n + 1]$ , donde  $T \subsetneq [S \setminus \{u_1\}]$ , e como  $|S \setminus \{u_1\}| = n - 1$ , segue da hipótese de indução que todo subconjunto de  $T$  com  $n$  vetores é L.D., de modo que  $T$  é L.D..

- $a_{i1} \neq 0$  para algum  $i \in [n + 1]$ . Nesse caso, suponha, sem perda de generalidade, que  $a_{11} \neq 0$ . Definindo

$$w_i := \frac{a_{i1}}{a_{11}} \cdot v_1 - v_i$$

para cada  $i \in [n + 1] \setminus \{1\}$ , fazendo as contas obtemos

$$w_i = \sum_{j=2}^n \left[ \left( \frac{a_{i1}}{a_{11}} a_{1j} - a_{ij} \right) u_j \right].$$

Com isso, vemos que cada  $w_i$  é uma combinação linear dos vetores  $u_2, \dots, u_n$ , de modo que  $T' := \{w_2, \dots, w_n, w_{n+1}\} \subsetneq [S \setminus \{u_1\}]$ . Como  $|S \setminus \{u_1\}| =$

$n - 1$  e  $|T'| = n$ , pela hipótese de indução temos que  $T'$  é L.D., de modo que existem  $n$  escalares,  $\lambda_2, \dots, \lambda_{n+1} \in \mathbb{R}$ , com algum  $\lambda_i \neq 0$ , tais que

$$\sum_{i=2}^{n+1} \lambda_i w_i = 0_V.$$

Daí, obtemos

$$\sum_{i=2}^{n+1} \left( \lambda_i \frac{a_{i1}}{a_{11}} \right) v_1 - \sum_{i=2}^{n+1} \lambda_i v_i = 0_V,$$

uma combinação linear não trivial de  $T$ , de modo que  $T$  é L.D..

Com isso, vemos que se o resultado vale para subconjuntos de  $V$  com  $n - 1$  vetores, então ele também vale para subconjuntos de  $V$  com  $n$  vetores. Isso completa o passo indutivo e, portanto, completa a prova. ■

**Corolário 12.23.** Seja  $(V, +, \cdot)$  um espaço vetorial. Se um subconjunto finito  $S \subseteq V$  é L.I., então todo subconjunto  $T \subseteq [S]$  tal que  $|T| \geq |S| + 1$  é L.D..

**Definição 12.24.** Seja  $(V, +, \cdot)$  um espaço vetorial. Um subconjunto  $\mathcal{B} \subsetneq V$  é uma *base* de  $V$  se  $\mathcal{B}$  é L.I. e  $[\mathcal{B}] = V$ .

**Teorema 12.25 (Completamento).** Todo espaço vetorial finitamente gerado possui uma base.

**Prova.** Seja  $(V, +, \cdot)$  um espaço vetorial finitamente gerado. Se  $V = \{0\}$ , então  $\emptyset$  é uma base de  $V$ , já que os vetores de  $\emptyset$  são L.I. por vacuidade e convencionamos pôr  $[\emptyset] = \{0\}$ . Suponha, então,  $V \neq \{0\}$ . Como  $V$  é finitamente gerado, existe um subconjunto finito  $S := \{v_1, v_2, \dots, v_n\} \subsetneq V$  que gera  $V$ . Se  $S$  for L.I., então  $S$  será uma base de  $V$ . Se  $S$  for L.D., então vale

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0,$$

sendo  $\lambda_i \neq 0$  para pelo menos um  $i \in [n]$ . Suponha, sem perda de generalidade, que  $i = n$ , isto é, que  $\lambda_n \neq 0$ ; com isso,

$$v_n = \left( \frac{-\lambda_1}{\lambda_n} \right) v_1 + \left( \frac{-\lambda_2}{\lambda_n} \right) v_2 + \dots + \left( \frac{-\lambda_{n-1}}{\lambda_n} \right) v_{n-1},$$

de modo que  $v_n$  é uma combinação linear de  $v_1, v_2, \dots, v_{n-1} \in S$ . Pelo item (g) de (12.21), removemos  $v_n$  e obtemos  $[S \setminus \{v_n\}] = [S] = V$ . Repetindo esse processo (em um número finito de vezes, digamos,  $m$ , já que  $V$  é finitamente gerado) eventualmente obteremos um subconjunto L.I. de  $S$  com  $n - m$  vetores que continua gerando  $V$ ; esse subconjunto vem a ser, então, a base de  $V$ . ■

**Prova.** Alternativamente, suponha que  $S$  é L.D.. Como  $V \neq \{0\}$ , existe  $i \in [n]$  tal que  $v_i \neq 0$ . Suponha, sem perda de generalidade, que  $i = 1$ , isto é, que  $v_1 \neq 0$ ; se todo  $v_i$ , com  $i \in [n] \setminus \{1\}$ , puder ser escrito como combinação linear de  $v_1$ , então  $V = [v_1]$  e  $\{v_1\}$  é uma base de  $V$ . Se isso não ocorre, então existe algum  $v_i$ , com  $i \in [n] \setminus \{1\}$ , que não pode ser escrito como combinação linear de  $v_1$ . Suponha, sem perda de generalidade, que  $i = 2$ ; se todo  $v_i$ , com  $i \in [n] \setminus \{1, 2\}$ , puder ser escrito como combinação linear de  $v_1$  e  $v_2$ , então  $V = [v_1, v_2]$  e  $\{v_1, v_2\}$  é uma base de  $V$ . Repetindo esse processo (em um número finito de vezes, já que  $V$  é finitamente gerado) eventualmente obteremos um subconjunto L.I. de  $S$  que gera  $V$ ; esse subconjunto vem a ser, então, a base de  $V$ . ■

**Teorema 12.26** (Invariância). Seja  $V$  um espaço vetorial finitamente gerado. Se  $\mathcal{B}_1$  e  $\mathcal{B}_2$  são bases de  $V$ , então  $|\mathcal{B}_1| = |\mathcal{B}_2|$ .

**Prova.** Como  $\mathcal{B}_1$  é L.I. e  $[\mathcal{B}_1] = V$ , pelo lema (12.22) temos que  $|\mathcal{B}_2| \leq |\mathcal{B}_1|$  já que  $\mathcal{B}_2 \subsetneq V = [\mathcal{B}_1]$ . De fato, se fosse  $|\mathcal{B}_2| > |\mathcal{B}_1|$ , pelo lema (12.22)  $\mathcal{B}_2$  seria L.D., o que contradiz a hipótese. Analogamente, como  $\mathcal{B}_2$  é L.I. e  $[\mathcal{B}_2] = V$ , temos que  $|\mathcal{B}_1| \leq |\mathcal{B}_2|$ . Sendo  $|\mathcal{B}_2| \leq |\mathcal{B}_1|$  e  $|\mathcal{B}_1| \leq |\mathcal{B}_2|$ , temos que  $|\mathcal{B}_1| = |\mathcal{B}_2|$ , conforme afirmado. ■

**Definição 12.27.** A *dimensão* de um espaço vetorial finitamente gerado  $(V, +, \cdot)$  é o número de vetores de qualquer uma de suas bases. Mais especificamente, se  $\mathcal{B}$  é uma base de  $V$ , a dimensão de  $V$  é definida como  $\dim V := |\mathcal{B}|$ .

**Teorema 12.28.** Seja  $(V, +, \cdot)$  um espaço vetorial de dimensão finita  $n > 0$ .

- (a) Todo subconjunto de  $V$  com  $n$  vetores L.I. é uma base de  $V$ .
- (b) Todo subconjunto de  $V$  com  $n$  vetores que gera  $V$  é uma base de  $V$ .
- (c) Todo subconjunto de  $V$  que gera  $V$  tem pelo menos  $n$  elementos.
- (d) Todo subconjunto de  $V$  com  $m < n$  vetores não é uma base de  $V$ .
- (e) Todo subconjunto de  $V$  com  $m < n$  vetores L.I. pode ser completado para formar uma base de  $V$ .
- (f) Se  $W$  é um subespaço vetorial de  $V$ , então  $W$  tem dimensão finita e  $\dim W \leq \dim V$ . Em particular, se  $\dim W = \dim V$ , então  $W = V$ .
- (g) Se  $W_1$  e  $W_2$  são subespaços vetoriais de  $V$ , então

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

**Prova.** (a) Reginaldo, 88.

(b) Reginaldo, 88.

(c) Reginaldo, 88.

(d) Zani, 44.

(e) Reginaldo, 88. Zani, 48.

(f) Reginaldo, 87.

(g) Reginaldo, 93. Zani, 49.

**Definição 12.29.** Seja  $V$  um espaço vetorial de dimensão finita  $n > 0$  e  $\mathcal{B} := \{v_1, v_2, \dots, v_n\}$  uma base ordenada (indexada) de  $V$ . Para cada  $v \in V$ , diremos que os únicos  $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{R}$  tais que  $v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n$  são as *coordenadas* de  $v$  com relação à base  $\mathcal{B}$  e denotamos isso por

$$v := \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix}_{\mathcal{B}} := \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix}_{v_1, v_2, \dots, v_n}.$$

**Teorema 12.30.** (Mudança de Base) Seja  $(V, +, \cdot)$  um espaço vetorial de dimensão finita  $n > 0$  e  $v \in V$ . Sejam  $\mathcal{B}$  e  $\mathcal{C}$  duas bases de um espaço vetorial de dimensão finita  $(V, +, \cdot)$  e  $v \in V$ .

# Capítulo 13

## Transformações Lineares

**Definição 13.1.** Sejam  $(V, +, \cdot)$  e  $(W, +, \cdot)$  espaços vetoriais.

- (a) Uma *transformação linear* de  $(V, +, \cdot)$  em  $(W, +, \cdot)$  é uma função  $T : V \rightarrow W$  tal que  $T(u+v) = T(u)+T(v)$  e  $T(\lambda \cdot u) = \lambda \cdot T(u)$  para quaisquer  $u, v \in V$  e  $\lambda \in \mathbb{R}$ .
- (b) Um *operador linear* é uma transformação linear  $T : V \rightarrow V$ .

**Exemplo 13.2.** Sejam  $(V, +, \cdot)$  e  $(W, +, \cdot)$  espaços vetoriais.

- (a) A função  $0 : V \rightarrow W$  definida por  $0(v) = 0_W$  para todo  $v \in V$  é uma transformação linear, chamada de *transformação nula*.
- (b) A função  $I_V : V \rightarrow V$  definida por  $I_V(v) = v$  para todo  $v \in V$  é um operador linear, chamada de *transformação identidade*.

**Proposição 13.3.** Uma função  $T : V \rightarrow W$  é uma transformação linear se, e somente se,

$$T\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i T(v_i)$$

para quaisquer  $n \in \mathbb{N}$ ,  $v_1, \dots, v_n \in V$  e  $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ .

**Prova.**

**Proposição 13.4.** Seja  $T : V \rightarrow W$  uma transformação linear. Valem as seguintes afirmações.

- (a)  $T(0_V) = 0_W$ .

**Definição 13.5.** Sejam  $V$  e  $W$  espaços vetoriais. O conjunto de todas as transformações lineares de  $V$  em  $W$  é denotado por  $\mathcal{L}(V, W)$

**Definição 13.6.** Seja  $T : V \rightarrow W$  uma transformação linear.

(a) O *núcleo* de  $T$  é definido como

$$\ker T := \{v \in V : T(v) = 0_W\}.$$

(b) A *imagem* de  $T$  é definida como

$$\operatorname{Im} T := \{w \in W : \exists v(v \in V \wedge T(v) = w)\}.$$

**Teorema 13.7.** Seja  $T : V \rightarrow W$  uma transformação linear.

(a)  $\ker T$  é um subespaço vetorial de  $V$ .

(b)  $\operatorname{Im} T$  é um subespaço vetorial de  $W$ .

## 13.1 Matrizes

O conjunto  $\mathcal{M}_{m \times n}(\mathbb{R})$  de todas as matrizes  $m \times n$  com entradas reais, com soma e produto por escalar usuais (vistas no capítulo 1), é um espaço vetorial.

**Exemplo 13.8. (a)** Dado  $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ , temos que

$$W := \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n : a_1x_1 + a_2x_2 + \dots + a_nx_n = 0\}$$

é um subespaço de  $\mathbb{R}^n$ . No caso desinteressante em que  $a_i = 0$  para todo  $i \in [n]$ , o subespaço  $W$  é todo o  $\mathbb{R}^n$ . Se, por outro lado, existe pelo menos um  $i \in [n]$  tal que  $a_i \neq 0$ , diremos que  $W$  é um *hiperplano* que passa pela origem.

(b) Seja  $m \in \mathbb{N}$ . Para cada  $i \in [m]$ , sendo  $(a_{i1}, a_{i2}, \dots, a_{in}) \in \mathbb{R}^n$ , pelo item anterior temos que cada

$$W_i := \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n : a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n = 0\}$$

é um subespaço vetorial de  $V$ . Pela proposição (12.11), temos que  $W := W_1 \cap W_2 \cap \dots \cap W_m$  é ainda um subespaço vetorial de  $V$ , que é exatamente o conjunto das soluções do sistema linear homogêneo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases}.$$

Outra maneira de verificar que o conjunto das soluções de um sistema linear homogêneo é um espaço vetorial é a seguinte.

O conjunto das matrizes simétricas,

$$W_1 = \{A \in \mathcal{M}_{n \times n} : A^T = A\},$$

bem como o conjunto das matrizes antissimétricas,

$$W_2 = \{A \in \mathcal{M}_{n \times n} : A^T = -A\},$$

são subespaços de  $\mathcal{M}_{n \times n}$ . E ainda, temos que  $\mathcal{M}_{n \times n} = W_1 \oplus W_2$ .

# Capítulo 14

## Geometria Analítica

Seguimos os capítulos 12 e 13 de [1].

**Definição 14.1.**

- (a) Dois vetores  $A, B \in \mathbb{R}^n$  são *paralelos* se existe  $c \in \mathbb{R}_{\neq 0}$  tal que  $B = cA$ .
- (b) Dois vetores  $A, B \in \mathbb{R}^n$  têm a mesma *direção* se existe  $c \in \mathbb{R}_{>0}$  tal que  $B = cA$ .
- (c) Dois vetores  $A, B \in \mathbb{R}^n$  têm *direções opostas* se existe  $c \in \mathbb{R}_{<0}$  tal que  $B = cA$ .

**Definição 14.2.** O *produto escalar* de dois vetores  $A = (a_1, \dots, a_n)$  e  $B = (b_1, \dots, b_n)$  é definido como

$$A \cdot B := \sum_{i=1}^n a_i b_i.$$

**Proposição 14.3.**

**Prova.** ■

**Teorema 14.4** (Cauchy-Schwarz). Para quaisquer  $A, B \in \mathbb{R}^n$ , tem-se

$$(A \cdot B)^2 \leq (A \cdot A)(B \cdot B).$$

**Prova.** Se  $A = 0$  ou  $B = 0$ , o resultado segue trivialmente. Suponha, então, que  $A, B \in \mathbb{R}_{\neq 0}^n$ . ■

**Definição 14.5.** A *norma* de um vetor  $A \in \mathbb{R}^n$  é definida como

$$\|A\| := \sqrt{A \cdot A}.$$

**Definição 14.6.** A *projeção* de  $A \in \mathbb{R}^n$  em  $B \in \mathbb{R}_{\neq 0}^n$  é definida como

$$\text{proj}_B A := \left( \frac{A \cdot B}{\|B\|^2} \right) B.$$

**Definição 14.7.** Uma *reta* no  $\mathbb{R}^n$  que passa pelo ponto  $P \in \mathbb{R}^n$  e é paralela ao vetor  $A \in \mathbb{R}_{\neq 0}^n$  é a imagem da função  $L : \mathbb{R} \rightarrow \mathbb{R}^n$  definida por  $L(t) = P + tA$ . Denota-se  $L(P, A) := \text{Im } L$ , isto é,

$$L(P, A) := \{X \in \mathbb{R}^n : \exists t(t \in \mathbb{R} \wedge X = P + tA)\}.$$

**Proposição 14.8.** Sejam  $P, Q, A, B \in \mathbb{R}^n$ .

- (a)  $L(P, A) = L(P, B) \Leftrightarrow A \parallel B$ .
- (b)  $L(P, A) = L(Q, B) \Leftrightarrow Q \in L(P, A) \vee P \in L(Q, B)$ .
- (c) Se  $P \neq Q$ , então existe uma única reta  $L \subsetneq \mathbb{R}^n$  tal que  $P, Q \in L$ .

**Prova.**

- (a)
- (b)
- (c) Pois tome  $L = L(P, Q - P)$ . Temos  $P \in L$  pois  $P = P + 0 \cdot (Q - P)$  e temos  $Q \in L$  pois  $Q = P + 1 \cdot (Q - P)$ . Agora, seja  $L'$  uma reta tal que  $P, Q \in L'$ . Como  $P \in L'$ , temos por definição  $L' = L(P, A)$  para algum vetor  $A \in \mathbb{R}_{\neq 0}^n$ . Como  $Q \in L' = L(P, A)$ , existe  $t \in \mathbb{R}$  tal que  $Q = P + tA$ . Daí,  $Q - P = tA$ , e como  $Q - P \neq 0$ , temos  $t \neq 0$  e  $Q - P \parallel A$ , donde  $L' = L$  pelo primeiro item. ■

**Definição 14.9.** Duas retas  $L(P, A)$  e  $L(Q, B)$  são *paralelas* se  $A \parallel B$ . Isso é denotado por  $L(P, A) \parallel L(Q, B)$ .

**Teorema 14.10** (Paralelas). Seja  $L \subsetneq \mathbb{R}^n$  uma reta. Para todo ponto  $Q \notin L$  existe uma única reta  $L' \subsetneq \mathbb{R}^n$  tal que  $Q \in L'$  e  $L' \parallel L$ .

**Prova.** Seja  $L = L(P, A)$  e tome  $L' = L(Q, A)$ . De cara,  $Q \in L'$  e  $L' \parallel L$ . A unicidade segue imediatamente da proposição (14.8). ■

**Teorema 14.11.** Sejam  $P, A \in \mathbb{R}^2$ . Se  $N \in \mathbb{R}^2$  é tal que  $N \cdot A = 0$ , então

- i.  $\{X \in \mathbb{R}^2 : (X - P) \cdot N = 0\} = L(P, A)$ ;

ii. vale

$$\|X\| \geq \frac{|P \cdot N|}{\|N\|}$$

para todo  $X \in L(P, A)$ , com igualdade somente se  $X = \text{proj}_N P$ ;

iii. Se  $Q \notin L(P, A)$ , então

$$\|X - Q\| \geq \frac{|(P - Q) \cdot N|}{\|N\|}$$

para todo  $X \in L(P, A)$ , com igualdade somente se  $Q = \text{proj}_N (P - Q)$ ;

**Prova.** Começemos com um lema: se  $(a, b), (c, d) \in \mathbb{R}^2$  são tais que  $(a, b) \cdot (c, d) = 0$ , então  $(c, d) = t \cdot (b, -a)$  para algum  $t \in \mathbb{R}$ .

**Definição 14.12.** Seja  $n \in \mathbb{N}_{\geq 2}$ . Um *plano* no  $\mathbb{R}^n$  que passa por um ponto  $P \in \mathbb{R}^n$  e é gerado por vetores  $u, v \in \mathbb{R}^n$ , linearmente independentes, é a imagem da função  $\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^n$  definida por  $\alpha(s, t) = P + su + tv$ . Denota-se  $\{P + su + tv\} := \text{Im } \alpha$ , isto é,

$$\{P + su + tv\} = \{X \in \mathbb{R}^n : \exists s \exists t (s, t \in \mathbb{R} \wedge X = P + su + tv)\}.$$

**Teorema 14.13.**

- (a) Se  $M = \{P + sA + tB\}$  e  $M' = \{P + sC + tD\}$  são planos, então  $M = M'$  se, e somente se,  $[A, B] = [C, D]$ .
- (b) Se  $\alpha = \{P + su + tv\}$  e  $\beta = \{Q + su + tv\}$  são planos, então  $\alpha = \beta$  se, e somente se,  $Q \in \alpha$  ou  $P \in \beta$ .
- (c) Se  $P, Q, R \in \mathbb{R}^n$  não são colineares, então existe um único plano  $\alpha \subsetneq \mathbb{R}^n$  tal que  $P, Q, R \in \alpha$ .

**Prova.**

(a)  $(\Rightarrow)$  bla bla

$(\Leftarrow)$

(b)  $(\Rightarrow)$  bla bla

$(\Leftarrow)$

(c)

**Definição 14.14.** Sejam  $\alpha = \{P + sA + tB\}$  e  $\beta = \{Q + sC + tD\}$  planos no  $\mathbb{R}^n$ .

- (a) Um vetor  $v \in \mathbb{R}^n$  é *paralelo ao plano*  $\alpha$  se  $v \in [A, B]$ .

(b) Os planos  $\alpha$  e  $\beta$  são *paralelos* se  $[A, B] = [C, D]$ .

**Teorema 14.15** (Paralelas). Seja  $\alpha \subsetneq \mathbb{R}^n$  um plano. Para todo ponto  $Q \notin \alpha$  existe um único plano  $\beta \subsetneq \mathbb{R}^n$  tal que  $Q \in \beta$  e  $\beta \parallel \alpha$ .

**Prova.** ■

**Teorema 14.16.**

- (a) Dois vetores  $u, v \in \mathbb{R}^n$  são L.I. se, e somente se, existe uma reta  $r \subsetneq \mathbb{R}^n$  tal que  $u, v, 0 \in r$ .
- (b) Três vetores  $u, v, w \in \mathbb{R}^n$  são L.I. se, e somente se, existe um plano  $\alpha \subsetneq \mathbb{R}^n$  tal que  $u, v, w, 0 \in \alpha$ .

**Prova.**

(a)

(b)

**Parte V**

**Cálculo II**

# Capítulo 15

## Topologia do Espaço Euclidiano

**Definição 15.1.** Uma *bola aberta* de raio  $r \in \mathbb{R}_{>0}$  e centro  $a \in \mathbb{R}^n$  é definida como

$$B_r(a) := \{x \in \mathbb{R}^n : \|x - a\| < r\}.$$

**Definição 15.2.**

- (a) Um ponto  $a \in \mathbb{R}^n$  é um *ponto interior* de  $A \subseteq \mathbb{R}^n$  se existe  $r \in \mathbb{R}_{>0}$  tal que  $B_r(a) \subseteq A$ .
- (b) O *interior* de  $A \subseteq \mathbb{R}^n$ , denotado por  $\text{int } A$ , é definido como o conjunto de todos os pontos interiores de  $A$ , isto é,

$$\text{int } A = \{x \in A : \exists r(r \in \mathbb{R}_{>0} \wedge B_r(x) \subseteq A)\}.$$

- (c) Um subconjunto  $A \subseteq \mathbb{R}^n$  é *aberto* se  $\text{int } A = A$ .

**Corolário 15.3.** Toda bola aberta é um conjunto aberto.

**Prova.** Ver [11], página 113. ■

**Definição 15.4.** Um ponto  $a \in \mathbb{R}^n$  é um *ponto de acumulação* de  $A \subseteq \mathbb{R}^n$  se  $B_r(a) \cap A_{\neq a} \neq \emptyset$  para todo  $r \in \mathbb{R}_{>0}$ .

**Definição 15.5.**

- (a) Um ponto  $a \in \mathbb{R}^n$  é um *ponto exterior* de  $A \subseteq \mathbb{R}^n$  se existe  $r \in \mathbb{R}_{>0}$  tal que  $B_r(a) \cap A = \emptyset$ .
- (b) O *exterior* de  $A \subseteq \mathbb{R}^n$ , denotado por  $\text{ext } A$ , é definido como o conjunto de todos os pontos exteriores de  $A$ , isto é,

$$\text{ext } A = \{x \in \mathbb{R}^n : \exists r(r \in \mathbb{R}_{>0} \wedge B_r(x) \cap A = \emptyset)\}.$$

**Definição 15.6.** Um ponto  $a \in \mathbb{R}^n$  é um *ponto da fronteira* de  $A \subseteq \mathbb{R}^n$  se  $a \notin \text{int } A$  e  $a \notin \text{ext } A$ . O conjunto de todos os pontos da fronteira de  $A$  é denotado por  $\partial A$ .

# Capítulo 16

## Caminhos

**Definição 16.1.** Uma *função vetorial de variável real* é uma função  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$ .

As funções vetoriais de variável real que nos interessam, nesse momento, são aquelas cujo domínio é um intervalo ou uma união de intervalos.

**Proposição 16.2.** Seja  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  uma função. Existem e são únicas as funções  $f_i : X \rightarrow \mathbb{R}$ , com  $i \in [n]$ , tais que

$$f(t) = (f_1(t), f_2(t), \dots, f_n(t))$$

para todo  $t \in X$ . Isso é denotado por  $f = (f_1, f_2, \dots, f_n)$ .

**Prova.** Trivial. ■

**Definição 16.3.** Uma função  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  tem limite  $L \in \mathbb{R}^n$  quando  $t$  tende ao ponto  $t_0 \in X'$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, t_0) \in \mathbb{R}_{>0}$  tal que

$$0 < |t - t_0| < \delta \rightarrow \|f(t) - L\| < \epsilon$$

para todo  $t \in X$ . Isso é denotado por

$$\lim_{t \rightarrow t_0} f(t) = L.$$

**Proposição 16.4** (Unicidade do limite). Se uma função  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  tem limites  $L_1, L_2 \in \mathbb{R}^n$ , então  $L_1 = L_2$ .

**Prova.**

**Proposição 16.5.** Sejam  $F : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$ ,  $t_0 \in X'$  e  $L \in \mathbb{R}^n$ . Vale

$$\lim_{t \rightarrow t_0} F(t) = L \Leftrightarrow \lim_{t \rightarrow t_0} \|F(t) - L\| = 0.$$

**Prova.** Ver [11], p. 124. ■

**Teorema 16.6.** Sejam  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$ ,  $t_0 \in X'$  e  $L \in \mathbb{R}^n$ , com  $f = (f_1, f_2, \dots, f_n)$  e  $L = (L_1, L_2, \dots, L_n)$ . Para todo  $i \in [n]$ , vale

$$\lim_{t \rightarrow t_0} f(t) = L \Leftrightarrow \lim_{t \rightarrow t_0} f_i(t) = L_i.$$

**Prova.** Ver [11], p. 124. ■

**Proposição 16.7** (Propriedades operatórias). Oi

**Prova.**

**Definição 16.8** (Continuidade). Sejam  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  e  $t_0 \in X \cap X'$ .

(a)  $f$  é contínua em  $t_0$  se

$$\lim_{t \rightarrow t_0} f(t) = f(t_0).$$

(b)  $f$  é contínua em  $Y \subseteq X$  se  $f$  for contínua em todo  $t_0 \in Y$ .

(c)  $f$  é contínua se  $f$  for contínua em  $X$ .

**Corolário 16.9.** Sejam  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  uma função, com  $f = (f_1, f_2, \dots, f_n)$ , e  $t_0 \in X \cap X'$ .  $f$  é contínua em  $t_0$  se, e somente se,  $f_i$  é contínua em  $t_0$ , para todo  $i \in [n]$ .

**Definição 16.10.** Sejam  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  e  $t_0 \in X \cap X'$ .

(a)  $f$  é derivável, ou diferenciável, em  $t_0$ , se existir o limite

$$f'(t_0) := \lim_{t \rightarrow t_0} \frac{f(t) - f(t_0)}{t - t_0}.$$

Mais precisamente,  $f$  é derivável em  $t_0$  se existir o limite  $\lim_{t \rightarrow t_0} g(t)$ , onde  $g : X \setminus \{t_0\} \rightarrow \mathbb{R}^n$  é a função definida por

$$g(t) := \frac{f(t) - f(t_0)}{t - t_0}.$$

Sendo  $F$  derivável em  $t_0$ , ou ainda, diferenciável em  $t_0$ , dizemos que o limite  $F'(t_0)$  é a derivada de  $F$  em  $t_0$ .

(b) Diremos que  $F$  é derivável em  $Y \subseteq X$  se  $F$  for derivável em todo  $t \in Y$ ; se for  $Y = X$ , diremos que  $F$  é derivável.

**Proposição 16.11.** Sejam  $F : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  e  $t_0 \in X$ . Sendo  $F = (f_1, f_2, \dots, f_n)$ , temos que  $F$  é derivável em  $t_0$  se, e somente se,  $f_i$  é derivável em  $t_0$  para todo  $i \in [n]$ . Sendo  $F$  derivável em  $t_0$ , temos que

$$F'(t) = (f'_1(t), f'_2(t), \dots, f'_n(t)).$$

**Prova.**

**Definição 16.12.** Seja  $F : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  derivável em  $t_0 \in X$ , com  $F'(t_0) \neq 0$ .

(a)

**Proposição 16.13** (Propriedades operatórias).

**Prova.**

**Proposição 16.14** (Regra da cadeia).

**Proposição 16.15.** Se  $F : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  uma função vetorial derivável em  $X$  tal que  $\|F(t)\| = k \in \mathbb{R}$  para todo  $t \in X$ , então  $F(t) \cdot F'(t) = 0$  para todo  $t \in X$ .

**Prova.**

**Definição 16.16.** Seja  $f : [a, b] \rightarrow \mathbb{R}^n$  uma função. A soma de Riemann  $S(f, P, \xi)$  tem limite  $L \in \mathbb{R}^n$  quando  $\|P\|$  tende a 0 se para todo  $\epsilon \in \mathbb{R}_{>0}$  existir  $\delta = \delta(\epsilon) \in \mathbb{R}_{>0}$  tal que

$$\|S(f, P, \xi) - L\| < \epsilon$$

para toda partição marcada  $(P, \xi)$  de  $[a, b]$  com  $\|P\| < \delta$ . Isso é denotado por

$$\lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L.$$

**Proposição 16.17.** Seja  $f : [a, b] \rightarrow \mathbb{R}^n$  uma função. O limite das somas de Riemann, quando existe, é único, isto é, se

$$\lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L_1 \quad \text{e} \quad \lim_{\|P\| \rightarrow 0} S(f, P, \xi) = L_2,$$

então  $L_1 = L_2$ .

**Prova.**

**Definição 16.18.** Uma função  $f : [a, b] \rightarrow \mathbb{R}^n$  é *integrável em  $[a, b]$  segundo Riemann* se  $\lim_{\|P\| \rightarrow 0} S(f, P, \xi)$  existe. Nesse caso, esse número real é chamado de *integral de  $f$  em  $[a, b]$  segundo Riemann* e é denotado por

$$\int_a^b F(x) dx,$$

isto é,

$$\int_a^b f(x) dx := \lim_{\|P\| \rightarrow 0} S(f, P, \xi).$$

**Proposição 16.19.** Seja  $f : X \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  uma função com  $F = (f_1, f_2, \dots, f_n)$ .  $f$  é integrável em  $[a, b]$  se, e somente se,  $f_i$  é integrável em  $[a, b]$  para todo  $i \in [n]$ , sendo nesse caso

$$\int_a^b F(t) dt = \left( \int_a^b f_1(t) dt, \int_a^b f_2(t) dt, \dots, \int_a^b f_n(t) dt \right).$$

**Prova.**

**Proposição 16.20** (Propriedades operatórias).

**Teorema 16.21.** (Fundamental do Cálculo, parte I) Seja  $f : [a, b] \rightarrow \mathbb{R}^n$  uma função integrável.

(a) A função  $F : [a, b] \rightarrow \mathbb{R}^n$  definida por

$$F(x) := \int_a^x f(t) dt$$

é uniformemente contínua em  $[a, b]$ .

(b) Se  $f$  é contínua em  $x_0 \in [a, b]$ , então  $F$  é derivável em  $x_0$  e  $F'(x_0) = f(x_0)$ .

**Prova.**

**Corolário 16.22.** Seja  $f : [a, b] \rightarrow \mathbb{R}^n$  uma função contínua em  $[a, b]$ .

(a) A função  $F : [a, b] \rightarrow \mathbb{R}^n$  definida por

$$F(x) := \int_a^x f(t) dt$$

é uma primitiva de  $f$  em  $[a, b]$ .

(b) Se  $G : [a, b] \rightarrow \mathbb{R}^n$  é qualquer outra primitiva de  $f$ , então

$$G(x) = G(a) + \int_a^x f(t) dt$$

para todo  $x \in [a, b]$ . Particularmente para  $x = b$ , temos

$$\int_a^b f(t) dt = G(b) - G(a).$$

**Prova.**

**Teorema 16.23** (Fundamental do Cálculo, parte II). Se  $f : [a, b] \rightarrow \mathbb{R}^n$  é uma função integrável e  $F : [a, b] \rightarrow \mathbb{R}^n$  é uma primitiva qualquer de  $f$ , então

$$F(x) = F(a) + \int_a^x f(t) dt$$

para todo  $x \in [a, b]$ . Particularmente para  $x = b$ , temos

$$\int_a^b f(t) dt = F(b) - F(a).$$

**Prova.**

**Proposição 16.24.** Seja  $C \in \mathbb{R}^n$ . Se  $f : [a, b] \rightarrow \mathbb{R}^n$  é uma função integrável, então a função  $C \cdot f : [a, b] \rightarrow \mathbb{R}$  é integrável e

$$C \cdot \left[ \int_a^b f(t) dt \right] = \int_a^b [C \cdot f(t)] dt.$$

**Prova.**

**Proposição 16.25.** Se  $f : [a, b] \rightarrow \mathbb{R}^n$  e  $\|f\| : [a, b] \rightarrow \mathbb{R}$  são funções integráveis em  $[a, b]$ , então

$$\left\| \int_a^b f(t) dt \right\| \leq \int_a^b \|f(t)\| dt.$$

## 16.1 Curvas

No que segue,  $I, J \subseteq \mathbb{R}$  são intervalos.

**Definição 16.26.**

- (a) Uma *curva* no  $\mathbb{R}^n$  é uma função vetorial de variável real  $\alpha : I \rightarrow \mathbb{R}^n$ .
- (b) Uma *curva paramétrica* é uma curva  $\alpha : I \rightarrow \mathbb{R}^n$  contínua. O *traço* da curva é a imagem de  $I$  por  $\alpha$ , isto é, o conjunto  $\alpha(I)$ .
- (c) Uma curva paramétrica  $\alpha : I \rightarrow \mathbb{R}^n$  é *regular* se  $\alpha$  é derivável em  $I$  com  $\alpha'(t) \neq 0$  para todo  $t \in I$ .

**Definição 16.27.** Seja  $\alpha : I \rightarrow \mathbb{R}^n$  uma curva paramétrica regular. Uma curva paramétrica  $\beta : J \rightarrow \mathbb{R}^n$  é uma *reparametrização* de  $\alpha$  se  $\beta(J) = \alpha(I)$  e se existe uma *função de reparametrização*  $\varphi : J \rightarrow I$  bijetora, derivável em  $J$ , com  $\varphi'(t) \neq 0$ , tal que  $\beta(t) = \alpha(\varphi(t))$ .

**Proposição 16.28** (Reparametrização conserva regularidade). Se uma curva paramétrica  $\beta : J \rightarrow \mathbb{R}^n$  é uma reparametrização de uma curva paramétrica regular  $\alpha : I \rightarrow \mathbb{R}^n$ , então  $\beta$  é regular.

**Prova.** ■

**Definição 16.29.** Sejam  $\alpha : I \rightarrow \mathbb{R}^n$  uma curva paramétrica regular e  $\beta : J \rightarrow \mathbb{R}^n$  uma reparametrização de  $\alpha$  por meio de uma função de reparametrização  $\varphi : J \rightarrow I$ .

- (a)  $\beta$  é uma reparametrização *positiva* se  $\varphi'(t) > 0$  para todo  $t \in J$ .
- (b)  $\beta$  é uma reparametrização *negativa* se  $\varphi'(t) < 0$  para todo  $t \in J$ .

**Definição 16.30.** Seja  $\alpha : I \rightarrow \mathbb{R}^n$  uma curva paramétrica derivável e com derivada integrável.

- (a) O *comprimento do arco* de  $a \in I$  até  $b \in I$  é definido como

$$L_a^b(\alpha) := \int_a^b \|\alpha'(t)\| dt.$$

- (b) Seja  $t_0 \in I$ . A *função comprimento de arco* de  $\alpha$  é definida como

$$L(t) := \int_{t_0}^t \|\alpha'(u)\| du.$$

**Proposição 16.31.** Se  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  é uma curva paramétrica regular e  $\beta : [c, d] \rightarrow \mathbb{R}^n$  é uma reparametrização de  $\alpha$ , então  $L_c^d(\beta) = L_a^b(\alpha)$ .

**Proposição 16.32.** A função comprimento de arco de uma curva paramétrica  $\alpha : I \rightarrow \mathbb{R}^n$  é uma função de reparametrização.

**Definição 16.33.** Uma curva paramétrica  $\alpha : I \rightarrow \mathbb{R}^n$  é *reparametrizada por comprimento de arco* se  $\|\alpha'(t)\| = 1$  para todo  $t \in I$ .

**Definição 16.34.**

- (a) Um caminho  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  é *retificável* se existe  $M \in \mathbb{R}$  tal que

$$L_a^b(\alpha, P) \leq M$$

para toda partição  $P : a = t_0 < \dots < t_k = b$  de  $[a, b]$ , onde

$$L_a^b(\alpha, P) := \sum_{i=1}^k \|\alpha(t_i) - \alpha(t_{i-1})\|.$$

(b) Seja  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  um caminho retificável. O *comprimento da curva* descrita por  $\alpha$  é definido como

$$L_a^b(\alpha) := \sup \{L_a^b(\alpha, P) : P \in \mathcal{P}[a, b]\}.$$

**Teorema 16.35.** Se um caminho  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  é de classe  $C^1$  em  $[a, b]$ , então

$$L_a^b(\alpha) = \int_a^b \|\alpha'(t)\| dt.$$

**Prova.**



# Capítulo 17

## Campos Escalares e Vetoriais

**Definição 17.1.** Sejam  $m, n \in \mathbb{N}$ .

- (a) Um *campo* é uma função  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$ .
- (b) Um campo  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  é um *campo escalar* se  $m = 1$ . Ou seja, um *campo escalar* é uma função  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$ .
- (c) Um campo  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  é um *campo vetorial* se  $m \geq 2$ .

**Teorema 17.2.** Se  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  é um campo, então existem e são únicas as funções  $f_i : X \rightarrow \mathbb{R}$ , com  $i \in [m]$ , tais que

$$f(x) = (f_1(x), f_2(x), \dots, f_m(x))$$

para todo  $x \in X$ . Isso é denotado por  $f = (f_1, f_2, \dots, f_m)$ .

**Prova.** ■

**Definição 17.3.** Uma função  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  tem limite  $L \in \mathbb{R}^m$  quando  $x$  tende a  $a \in X'$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$0 < \|x - a\| < \delta \Rightarrow \|f(x) - L\| < \epsilon$$

para todo  $x \in X$ . Isso é denotado por

$$\lim_{x \rightarrow a} f(x) = L.$$

**Proposição 17.4.** Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$ ,  $L \in \mathbb{R}^m$  e  $a \in X'$ . Vale

$$\lim_{x \rightarrow a} f(x) = L \Leftrightarrow \lim_{\|x-a\| \rightarrow 0} \|f(x) - L\| = 0.$$

**Prova.** ■

**Proposição 17.5** (Propriedades operatórias).

**Definição 17.6** (Continuidade). Seja  $f : A \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  um campo.

- (a) Dizemos que  $f$  é *contínua em*  $a \in A$  se para todo  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$\|x - a\| < \delta \Rightarrow \|f(x) - f(a)\| < \epsilon$$

para todo  $x \in A$ .

- (b) Dizemos que  $f$  é *contínua em*  $X \subseteq A$  se  $f$  é contínua em todo ponto  $a \in X$ . Mais especificamente,  $f$  é contínua em  $X$  se para cada  $a \in X$  e cada  $\epsilon \in \mathbb{R}_{>0}$  existe  $\delta = \delta(\epsilon, a) \in \mathbb{R}_{>0}$  tal que

$$\|x - a\| < \delta \Rightarrow \|f(x) - f(a)\| < \epsilon$$

para todo  $x \in A$ .

**Teorema 17.7.** Uma função  $f : A \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  é contínua em  $a \in A \cap A'$  se, e somente se,  $\lim_{x \rightarrow a} f(x) = f(a)$ .

**Prova.** ■

**Teorema 17.8.** Sejam  $f : A \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^m$  e  $g : B \subseteq \mathbb{R}^m \rightarrow \mathbb{R}^k$  funções tais que  $f(A) \subseteq B$ . Se  $f$  é contínua em  $a \in A$  e se  $g$  é contínua em  $f(a) \in B$ , então a função composta  $g \circ f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^k$  é contínua em  $a$ .

**Prova.**

**Proposição 17.9.** Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  e  $a \in X \cap X'$  tais que  $\lim_{x \rightarrow a} f(x)$  existe. Se  $\alpha : I \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  é contínua em  $t_0 \in I$ , com  $\alpha(t_0) = a$ , e  $\alpha(t) \in X$  para todo  $t \in I$ , com  $t \neq t_0 \Rightarrow \alpha(t) \neq \alpha(t_0)$ , então

$$\lim_{t \rightarrow t_0} f(\alpha(t)) = \lim_{x \rightarrow a} f(x).$$

**Prova.** Ver [11], p. 165, exemplo 4. ■

**Teorema 17.10** (Compostas).

- (a) Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  e  $g : Y \subseteq \mathbb{R} \rightarrow \mathbb{R}$  funções tais que  $f(X) \subseteq Y$ . Se  $f$  é contínua em  $a \in X$  e  $g$  é contínua em  $f(a) \in Y$ , então a função composta  $g \circ f : \mathbb{R}^n \rightarrow \mathbb{R}$  é contínua em  $a$ .
- (b) Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  uma função e  $\alpha : I \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  uma curva tais que  $\alpha(t) \in X$  para todo  $t \in I$ . Se  $\alpha$  é contínua em  $a \in I$  e  $f$  é contínua em  $\alpha(a) \in X$ , então a função composta  $f \circ \alpha : \mathbb{R} \rightarrow \mathbb{R}$  é contínua em  $a$ .

- (c) Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  e  $f_1, \dots, f_n : Y \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  funções tais que  $(f_1(x), \dots, f_n(x)) \in X$  para todo  $x \in Y$ . Se  $f_1, \dots, f_n$  são contínuas em  $a \in Y$ , e se  $f$  é contínua em  $(f_1(a), \dots, f_n(a))$ , então a função composta  $f((f_1(x), \dots, f_n(x)))$  é contínua em  $a$ .

**Prova.** Ver [11], pg. 170, Teorema 1. ■

**Teorema 17.11.** Sejam  $f : X \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  e  $\alpha : I \subseteq \mathbb{R} \rightarrow \mathbb{R}^n$  tais que  $\alpha(t) \in X$  para todo  $t \in I$ . Se  $\alpha$  é contínua em  $a \in I$  e  $f$  é contínua em  $\alpha(a) \in X$ , então a função composta  $f \circ \alpha : \mathbb{R} \rightarrow \mathbb{R}$  é contínua em  $a$ .

**Prova.**

**Definição 17.12.** Sejam  $A \subseteq \mathbb{R}^n$  aberto,  $a \in A$  e  $y \in \mathbb{R}^n$ .

- (a) Um campo escalar  $f : A \rightarrow \mathbb{R}$  é *derivável* em  $a$  com respeito a  $y$  se existe o limite

$$f'_y(a) := \lim_{h \rightarrow 0} g(h),$$

onde  $g : \{h \in \mathbb{R}_{\neq 0} : a + hy \in A\} \rightarrow \mathbb{R}$  é definida por

$$g(h) := \frac{f(a + hy) - f(a)}{h}.$$

- (b) Seja  $f : A \rightarrow \mathbb{R}$  derivável em  $a$  com respeito a  $y$ .

- i. Se  $\|y\| = 1$ , então dizemos que  $f'_y(a)$  é a *derivada direcional* de  $f$  na direção de  $y$ .
- ii. Se  $y = e_k$  para algum  $k \in [n]$ , então dizemos que  $f'_{e_k}(a)$  é a *derivada parcial* de  $f$  com respeito a  $e_k$ . Outras notações para  $f'_{e_k}(a)$  são

$$\frac{\partial f}{\partial x_k}(a), \quad D_k f(a) \quad \text{e} \quad f'_{x_k}(a).$$

**Definição 17.13.** Sejam  $A \subseteq \mathbb{R}^n$  aberto e  $f : A \rightarrow \mathbb{R}$  derivável em  $a \in A$  com respeito a  $e_k$  para todo  $k \in [n]$ . O *gradiente* de  $f$  em  $a$  é definido como

$$\nabla f(a) := \left( \frac{\partial f}{\partial x_1}(a), \frac{\partial f}{\partial x_2}(a), \dots, \frac{\partial f}{\partial x_n}(a) \right).$$

**Definição 17.14.** Seja  $A \subseteq \mathbb{R}^n$  aberto. Um campo escalar  $f : A \rightarrow \mathbb{R}$  é *diferenciável* em  $a \in A$  se existe uma transformação linear  $T_a : \mathbb{R}^n \rightarrow \mathbb{R}$  para a qual a função  $r_a : \{h \in \mathbb{R}^n : a + h \in A\} \rightarrow \mathbb{R}$  definida por

$$r_a(h) := f(a + h) - f(a) - T_a(h)$$

satisfaz  $\lim_{h \rightarrow 0} \frac{|r_a(h)|}{\|h\|} = 0$ . A transformação linear  $T_a$  é a *derivada total* de  $f$  em  $a$ .

# Capítulo 18

## Integrais de Linha

### Definição 18.1.

- (a) Um *caminho* é uma função contínua  $\gamma : [a, b] \rightarrow \mathbb{R}^n$ .
- (b) Um caminho  $\gamma : [a, b] \rightarrow \mathbb{R}^n$  é *suave* se  $\gamma$  é de classe  $C^1$  em  $]a, b[$ .
- (c) Um caminho  $\gamma : [a, b] \rightarrow \mathbb{R}^n$  é *suave por partes* se existe uma partição

$$P : a = x_0 < x_1 < \cdots < x_k = b$$

tal que  $\gamma_i := \gamma|_{[x_{i-1}, x_i]}$  é suave para todo  $i \in [k]$ .

**Definição 18.2.** Sejam  $\gamma : [a, b] \rightarrow \mathbb{R}^n$  um caminho suave por partes e  $f : \gamma([a, b]) \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^n$  um campo vetorial limitado. A *integral de linha* de  $f$  com respeito a  $\gamma$  em  $C := \gamma([a, b])$  é definida como

$$\int_C f \cdot d\gamma := \int_a^b f[\gamma(t)] \cdot \gamma'(t) dt.$$

**Definição 18.3.** Seja  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  um caminho. Um caminho  $\beta : [c, d] \rightarrow \mathbb{R}^n$  é uma *reparametrização* de  $\alpha$  se existe uma bijeção  $\varphi : [c, d] \rightarrow [a, b]$ , derivável em  $[c, d]$ , com  $\varphi'(t) \neq 0$  para todo  $t \in [c, d]$ , tal que  $\beta(t) = \alpha(\varphi(t))$  para todo  $t \in [c, d]$ . Os caminhos  $\alpha$  e  $\beta$  são *equivalentes*, enquanto a bijeção  $\varphi$  é uma *mudança de parâmetro*.

**Proposição 18.4.** Dois caminhos equivalentes descrevem a mesma curva.

**Definição 18.5.** Sejam  $\alpha : [a, b] \rightarrow \mathbb{R}^n$  um caminho e  $\beta : [c, d] \rightarrow \mathbb{R}^n$  uma reparametrização de  $\alpha$  por meio de uma mudança de parâmetro  $\varphi : [c, d] \rightarrow [a, b]$ .

- (a)  $\beta$  é uma reparametrização *positiva* se  $\varphi'(t) > 0$  para todo  $t \in [c, d]$ . Dizemos que os caminhos  $\alpha$  e  $\beta$  têm o *mesmo sentido* e que a mudança de parâmetro *conserva a orientação* do traço.
- (b)  $\beta$  é uma reparametrização *negativa* se  $\varphi'(t) < 0$  para todo  $t \in [c, d]$ . Dizemos que os caminhos  $\alpha$  e  $\beta$  têm *sentidos opostos* e que a mudança de parâmetro *inverte a orientação* do traço.

**Teorema 18.6.** Sejam  $\gamma_1 : [a, b] \rightarrow \mathbb{R}^n$  e  $\gamma_2 : [c, d] \rightarrow \mathbb{R}^n$  caminhos suaves por partes equivalentes. Seja  $f : C \subseteq \mathbb{R}^n \rightarrow \mathbb{R}^n$  um campo vetorial limitado, onde  $C$  é o traço dos caminhos  $\gamma_1$  e  $\gamma_2$ .

- (a) Se  $\gamma_1$  e  $\gamma_2$  têm o mesmo sentido, então

$$\int_C f \cdot d\gamma_1 = \int_C f \cdot d\gamma_2.$$

- (b) Se  $\gamma_1$  e  $\gamma_2$  têm sentidos opostos, então

$$\int_C f \cdot d\gamma_1 = - \int_C f \cdot d\gamma_2.$$

**Prova.** ■

**Definição 18.7.** Sejam  $\gamma : [a, b] \rightarrow \mathbb{R}^n$  um caminho de classe  $C^1$  em  $[a, b]$  e  $f : \gamma([a, b]) \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$  um campo escalar limitado. A *integral de linha* de  $f$  com respeito a  $\gamma$  em  $C := \gamma([a, b])$  é definida como

$$\int_C f \cdot ds := \int_a^b f[\gamma(t)] \cdot \|\gamma'(t)\| dt.$$

# **Parte VI**

## **Probabilidade**

# Capítulo 19

## Combinatória Finita

### Proposição 19.1.

- (a) (Regra da soma) Se  $X_1, X_2, \dots, X_n$  são conjuntos finitos dois a dois disjuntos, então o conjunto  $\bigcup_{i=1}^n X_i$  é finito e

$$\left| \bigcup_{i=1}^n X_i \right| = \sum_{i=1}^n |X_i|.$$

- (b) (Regra do produto) Se  $X_1, X_2, \dots, X_n$  são conjuntos finitos, então o conjunto  $X_1 \times X_2 \times \dots \times X_n$  é finito e

$$|X_1 \times X_2 \times \dots \times X_n| = \prod_{i=1}^n |X_i|.$$

### Prova.

- (a) Façamos indução em  $n \geq 2$ .

Para  $n = 2$ , ver [19], p. 32, teorema 6, [9], p. 14, [4], p. 2.

Para completar a indução, ver [19], p. 33, corolário 1, [9], p. 15, [4], p. 2.

- (b) Ver [19], p. 33, corolário 3.

### Proposição 19.2.

- (a) Se  $X$  é um conjunto finito, então  $\mathcal{P}(X)$  é finito e  $|\mathcal{P}(X)| = 2^{|X|}$ .
- (b) Se  $X$  e  $Y$  são conjuntos finitos, então o conjunto  $X^Y$  (de todas as funções  $f : X \rightarrow Y$ ) é finito  $|X^Y| = |Y|^{|X|}$ .

**Prova.**

(a)

(b) Ver [19], p. 33, corolário 3.

# Capítulo 20

## Espaços de Probabilidade

**Definição 20.1.** Seja  $\Omega$  um conjunto.

(a) Uma  $\sigma$ -álgebra é um subconjunto  $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ , tal que

- i.  $\Omega \in \mathcal{F}$ ;
- ii. se  $A \in \mathcal{F}$ , então  $A^C \in \mathcal{F}$ ;
- iii. se  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$ , então  $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{F}$ .

(b) Um *espaço mensurável* é um par  $(\Omega, \mathcal{F})$ , onde  $\mathcal{F}$  é uma  $\sigma$ -álgebra em  $\Omega$ .

**Exemplo 20.2.** Seja  $\Omega$  um conjunto.

(a)  $(\Omega, \mathcal{P}(\Omega))$  é um espaço mensurável.

(b)  $(\Omega, \{\emptyset, \Omega\})$  é um espaço mensurável, dito *trivial*, pois  $\{\emptyset, \Omega\}$  é uma  $\sigma$ -álgebra em  $\Omega$ .

**Corolário 20.3.** Seja  $(\Omega, \mathcal{F})$  um espaço mensurável. Valem as seguintes afirmações.

(a)  $\emptyset \in \mathcal{F}$ .

(b) Se  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$ , então  $\bigcap_{n \in \mathbb{N}} A_n \in \mathcal{F}$ .

(c) Se  $A, B \in \mathcal{F}$ , então  $A \setminus B \in \mathcal{F}$  e  $B \setminus A \in \mathcal{F}$ .

**Prova.**

(a) Temos  $\Omega \in \mathcal{F}$ , de modo que  $\Omega^C \in \mathcal{F}$ , isto é,  $\emptyset \in \mathcal{F}$ . ■

(b) ■

**Definição 20.4.** Seja  $(\Omega, \mathcal{F})$  um espaço mensurável com  $\Omega \neq \emptyset$ .

(a) Uma *medida de probabilidade* em  $(\Omega, \mathcal{F})$  é uma função  $\mathbb{P} : \mathcal{F} \rightarrow \mathbb{R}$  tal que

- i.  $\mathbb{P}(\Omega) = 1$ ;
- ii.  $\mathbb{P}(A) \geq 0$  para todo  $A \in \mathcal{F}$ ;
- iii. se  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  e  $A_i \cap A_j = \emptyset$  para  $i \neq j$ , então

$$\mathbb{P}\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sum_{n \in \mathbb{N}} \mathbb{P}(A_n).$$

(b) Um *espaço de probabilidade* é uma terna  $(\Omega, \mathcal{F}, \mathbb{P})$ , onde  $\mathbb{P} : \mathcal{F} \rightarrow \mathbb{R}$  é uma medida de probabilidade definida em  $(\Omega, \mathcal{F})$ . Neste contexto, dizemos que  $\Omega$  é um *espaço amostral* e que os elementos de  $\mathcal{F}$  (subconjuntos de  $\Omega$ ) são *eventos aleatórios*, ou simplesmente *eventos*.

**Proposição 20.5.** Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade,  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  e  $A, B \in \mathcal{F}$ . Valem as seguintes afirmações.

- (a)  $\mathbb{P}(\emptyset) = 0$ ;
- (b)  $\mathbb{P}(A^C) = 1 - \mathbb{P}(A)$ ;
- (c) se  $A \subseteq B$ , então  $\mathbb{P}(B \setminus A) = \mathbb{P}(B) - \mathbb{P}(A) \geq 0$ ;
- (d)  $0 \leq \mathbb{P}(A) \leq 1$ ;
- (e)  $\mathbb{P}\left(\bigcup_{i \in \mathbb{N}} A_i\right) \leq \sum_{i \in \mathbb{N}} \mathbb{P}(A_i)$ ;
- (f)  $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ .

**Prova.**

(a) Temos  $\mathbb{P}(\emptyset) \geq 0$ . Notando que  $\mathbb{P}(\emptyset) = \mathbb{P}\left(\bigcup_{n \in \mathbb{N}} \emptyset\right) = \sum_{n \in \mathbb{N}} \mathbb{P}(\emptyset)$ , só pode ser  $\mathbb{P}(\emptyset) = 0$ . ■

**Teorema 20.6.** Seja  $\Omega$  um conjunto enumerável. Se  $p : \Omega \rightarrow \mathbb{R}$  é uma função tal que  $p(\omega) \geq 0$  para todo  $\omega \in \Omega$  e

$$\sum_{\omega \in \Omega} p(\omega) = 1,$$

então a tripla  $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ , onde  $\mathbb{P} : \mathcal{P}(\Omega) \rightarrow \mathbb{R}$  é a função definida por

$$\mathbb{P}(A) := \sum_{\omega \in A} p(\omega)$$

para todo  $A \in \mathcal{P}(\Omega)$ , é um espaço de probabilidade.

**Prova.** ■

**Definição 20.7.** Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade,  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  e  $A \in \mathcal{F}$ .

(a) Denota-se

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \quad \text{e} \quad \bigcup_{n \in \mathbb{N}} A_n = A$$

por  $A_n \uparrow A$ .

(b) Denota-se

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \quad \text{e} \quad \bigcap_{n \in \mathbb{N}} A_n = A$$

por  $A_n \downarrow A$ .

**Proposição 20.8.** Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade,  $\{A_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  e  $A \in \mathcal{F}$ .

(a) Se  $A_n \uparrow A$ , então  $\lim_{n \rightarrow +\infty} \mathbb{P}(A_n) = \mathbb{P}(A)$ .

(b) Se  $A_n \downarrow A$ , então  $\lim_{n \rightarrow +\infty} \mathbb{P}(A_n) = \mathbb{P}(A)$ .

**Prova.**

(a) Pois tome  $A_0 := \emptyset$  e defina  $\{B_n\}_{n \in \mathbb{N}}$  por  $B_n := A_n \setminus A_{n-1}$  para todo  $n \in \mathbb{N}$ . É fácil provar que  $\{B_n\}_{n \in \mathbb{N}}$  é disjunto e que  $\bigcup_{n \in \mathbb{N}} B_n = \bigcup_{n \in \mathbb{N}} A_n$ . Com isso,

$$\begin{aligned} \mathbb{P}(A) &= \mathbb{P}\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \mathbb{P}\left(\bigcup_{n \in \mathbb{N}} B_n\right) = \sum_{k=1}^{\infty} \mathbb{P}(B_k) \\ &= \sum_{k=1}^{\infty} \mathbb{P}(A_k \setminus A_{k-1}) = \lim_{n \rightarrow +\infty} \sum_{k=1}^n \mathbb{P}(A_k \setminus A_{k-1}) \\ &= \lim_{n \rightarrow +\infty} \sum_{k=1}^n [\mathbb{P}(A_k) - \mathbb{P}(A_{k-1})] = \lim_{n \rightarrow +\infty} \mathbb{P}(A_n), \end{aligned}$$

como queríamos. ■

(b) Se  $A_n \downarrow A$ , então  $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$  e  $\bigcap_{n \in \mathbb{N}} A_n = A$ . Observando que

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \Leftrightarrow A_1^C \subseteq A_2^C \subseteq A_3^C \subseteq \cdots,$$

trivialmente temos  $A_n^C \uparrow \bigcup_{n \in \mathbb{N}} A_n^C = A^C$ , donde  $\lim_{n \rightarrow +\infty} \mathbb{P}(A_n^C) = \mathbb{P}(A^C)$  pelo item anterior. Com isso,

$$\lim_{n \rightarrow +\infty} \mathbb{P}(A_n) = \lim_{n \rightarrow +\infty} [1 - \mathbb{P}(A_n^C)] = 1 - \mathbb{P}(A^C) = \mathbb{P}(A),$$

como queríamos. ■

**Definição 20.9.** Seja  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade. A *probabilidade condicional de  $A \in \mathcal{F}$  dado  $B \in \mathcal{F}$*  é definida como

$$\mathbb{P}(A|B) := \begin{cases} \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} & \text{se } \mathbb{P}(B) > 0; \\ \mathbb{P}(A) & \text{se } \mathbb{P}(B) = 0. \end{cases}$$

**Proposição 20.10.** Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade e  $B \in \mathcal{F}$ . A terna  $(\Omega, \mathcal{F}, \bar{\mathbb{P}})$ , onde  $\bar{\mathbb{P}} : \mathcal{F} \rightarrow \mathbb{R}$  é definida por  $\bar{\mathbb{P}}(A) := \mathbb{P}(A|B)$  para todo  $A \in \mathcal{F}$ , é um espaço de probabilidade.

**Prova.** Ver [20], proposição 2.2. ■

**Teorema 20.11** (Regra do produto). Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade e  $A_1, A_2, \dots, A_n \in \mathcal{F}$ . Tem-se

$$\mathbb{P}\left(\bigcap_{i=1}^n A_i\right) = \mathbb{P}(A_1) \cdot \prod_{i=2}^n \mathbb{P}\left(A_i \mid \bigcap_{j=1}^{i-1} A_j\right).$$

**Prova.** Basta fazer indução em  $n$ . Ver [20], teorema 2.5. ■

**Teorema 20.12** (Probabilidade total). Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade e  $A \in \mathcal{F}$ . Se  $\{B_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  é uma partição de  $\Omega$ , então

$$\mathbb{P}(A) = \sum_{n \in \mathbb{N}} \mathbb{P}(B_n) \mathbb{P}(A|B_n).$$

**Prova.** ■

**Corolário 20.13** (fórmula de Bayes). Sejam

(a) Oi

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A|B)}{\mathbb{P}(A)} \cdot \mathbb{P}(B).$$

(b) Se  $\{B_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}$  é uma partição de  $\Omega$ , então

$$\mathbb{P}(B_j|A) = \frac{\mathbb{P}(B_j)\mathbb{P}(B_j|A)}{\sum_{n \in \mathbb{N}} \mathbb{P}(B_n)\mathbb{P}(A|B_n)}$$

para todo  $j \in \mathbb{N}$ .

**Prova.** ■

**Definição 20.14.** Dois eventos  $A, B \in \mathcal{F}$  são *independentes* se  $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$ .

**Proposição 20.15.** Dois eventos  $A, B \in \mathcal{F}$  são independentes se, e somente se,  $\mathbb{P}(A|B) = \mathbb{P}(A)$ .

**Prova.** ■

**Definição 20.16.** Seja  $J$  um conjunto de índices.

- (a) Eventos independentes dois a dois.
- (b) Eventos independentes

## 20.1 Variáveis Aleatórias

Seja  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade.

**Definição 20.17.** Uma *variável aleatória* é uma função  $X : \Omega \rightarrow \mathbb{R}$  tal que  $X^{-1}(I) \in \mathcal{F}$  para todo intervalo  $I \subseteq \mathbb{R}$ .

**Definição 20.18.** Seja  $X : \Omega \rightarrow \mathbb{R}$  uma variável aleatória. A *função de distribuição acumulada* de  $X$  é a função  $F_X : \mathbb{R} \rightarrow \mathbb{R}$  definida por  $F_X(x) = \mathbb{P}(X \in ]-\infty, x])$  para todo  $x \in \mathbb{R}$ .

**Proposição 20.19.** Sejam  $(\Omega, \mathcal{F}, \mathbb{P})$  um espaço de probabilidade,  $X : \Omega \rightarrow \mathbb{R}$  uma variável aleatória e  $F_X : \mathbb{R} \rightarrow [0, 1]$  a FDA de  $X$ . Valem as seguintes afirmações.

- (a)  $F_X$  é crescente.
- (b)  $F_X$  é contínua à direita.
- (c)  $\lim_{x \rightarrow -\infty} F_X(x) = 0$  e  $\lim_{x \rightarrow +\infty} F_X(x) = 1$ .

**Definição 20.20.** Uma função  $F : \mathbb{R} \rightarrow \mathbb{R}$  é uma *função de distribuição* se é crescente, contínua à direita e  $\lim_{x \rightarrow -\infty} F(x) = 0$  e  $\lim_{x \rightarrow +\infty} F(x) = 1$ .

**Definição 20.21.** Uma função  $f : \mathbb{R} \rightarrow \mathbb{R}$  é uma *função de densidade* se  $f \geq 0$  e

$$\int_{-\infty}^{+\infty} f(x) dx = 1.$$

**Proposição 20.22.** Se  $f : \mathbb{R} \rightarrow \mathbb{R}$  é uma função de densidade, então a função  $F : \mathbb{R} \rightarrow \mathbb{R}$  definida por

$$F(x) = \int_{-\infty}^x f(t) dt$$

para todo  $x \in \mathbb{R}$  é uma função de distribuição.

**Prova.** ■

**Definição 20.23.** Duas variáveis aleatórias  $X, Y : \Omega \rightarrow \mathbb{R}$  são *independentes* se os eventos  $[X \in I_1], [Y \in I_2] \in \mathcal{F}$  são independentes para quaisquer intervalos  $I_1, I_2 \subseteq \mathbb{R}$ .

### 20.1.1 Distribuições Discretas

**Definição 20.24.** Uma variável aleatória  $X : \Omega \rightarrow \mathbb{R}$  é *discreta* se existe  $A \subsetneq \mathbb{R}$  enumerável tal que  $\mathbb{P}(X \in A) = 1$ .

**Definição 20.25.** Seja  $X : \Omega \rightarrow \mathbb{R}$  uma variável aleatória.

- (a) Dizemos que  $X$  tem distribuição *Bernoulli* de parâmetro  $p \in ]0, 1[$  se  $\mathbb{P}(X = 1) = p$  e  $\mathbb{P}(X = 0) = 1 - p$ . Isso é denotado por  $X \sim \text{Bernoulli}(p)$ .
- (b) Dizemos que  $X$  tem distribuição *geométrica* de parâmetro  $p \in ]0, 1[$  se  $\mathbb{P}(X = k) = p(1 - p)^{k-1}$  para todo  $k \in \mathbb{N}$ . Isso é denotado por  $X \sim \text{Geom}(p)$ .
- (c) Dizemos que  $X$  tem distribuição *binomial* de parâmetros  $n \in \mathbb{N}$  e  $p \in ]0, 1[$  se

$$\mathbb{P}(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$$

para todo  $k \in \mathbb{N}$ . Isso é denotado por  $X \sim \text{Binom}(n, p)$ .

- (d) Dizemos que  $X$  tem distribuição *Poisson* de parâmetro  $\lambda \in \mathbb{R}_{>0}$  se

$$\mathbb{P}(X = k) = e^{-\lambda} \frac{\lambda^k}{k!}$$

para todo  $k \in \mathbb{N}$ . Isso é denotado por  $X \sim \text{Poisson}(\lambda)$ .

**Proposição 20.26.** As distribuições da definição (20.25) são discretas.

**Prova.**

(a)

### 20.1.2 Distribuições Absolutamente Contínuas

**Definição 20.27.** Uma variável aleatória  $X : \Omega \rightarrow \mathbb{R}$  é *absolutamente contínua* se existe uma função contínua por partes  $f : \mathbb{R} \rightarrow \mathbb{R}$  tal que  $f(x) \geq 0$  para todo  $x \in \mathbb{R}$  e

$$\mathbb{P}(X \in I) = \int_I f$$

para todo intervalo  $I \subseteq \mathbb{R}$ .

## **Parte VII**

### **Outros**

# Capítulo 21

## Shoenfield

**Definição 21.1** (Linguagens de Primeira Ordem).

- (a) Um *alfabeto* é uma coleção infinita de símbolos distintos, nenhum deles propriamente contido em outro, separados nas seguintes categorias:
- i. Conectivos:  $\vee, \neg$ .
  - ii. Quantificador existencial:  $\exists$ .
  - iii. Variáveis, uma para cada inteiro positivo  $n$ :  $u_1, u_2, \dots, u_n, \dots$ .
  - iv. Símbolos de função: para cada natural  $n$ , uma coleção de símbolos de função  $n$ -ários. Os símbolos de função 0-ários são chamados de *constantes*.
  - v. Símbolos de predicado: para cada natural  $n$ , uma coleção de símbolos de predicado  $n$ -ários.
  - vi. Símbolo de predicado binário de igualdade  $=$ .

Símbolos de função e de predicado distintos de  $=$  são chamados de símbolos *não lógicos*. Os demais são chamados de símbolos lógicos. Usamos  $x, y, z$  e  $w$  para denotar variáveis sintáticas que variam entre variáveis,  $f$  e  $g$  para denotar variáveis sintáticas que variam entre símbolos de funções,  $p$  e  $q$  para denotar variáveis sintáticas que variam entre símbolos de predicado e  $e$  para denotar uma variável sintática que varia entre constantes.

- (b) Os *termos* de um alfabeto são definidos do seguinte modo:

- i. toda variável é um termo;
- ii. se  $u_1, \dots, u_n$  são termos e  $f$  é  $n$ -ário, então  $fu_1 \dots u_n$  é um termo.

Termos são apenas expressões que denotam indivíduos. Note que constantes também são termos. Usamos  $a, b, c$  e  $d$  para denotar variáveis sintáticas que variam entre termos.

(c) As fórmulas de um alfabeto são definidas do seguinte modo:

- i. se  $u_1, \dots, u_n$  são termos e  $p$  é  $n$ -ário, então  $pu_1 \dots u_n$  é uma fórmula;
- ii. se  $u$  é uma fórmula, então  $\neg u$  é uma fórmula;
- iii. se  $u$  e  $v$  são fórmulas, então  $\vee uv$  é uma fórmula;
- iv. se  $u$  é uma fórmula, então  $\exists xu$  é uma fórmula.

As fórmulas do tipo i. são chamadas de *atômicas*.

(d) Uma *linguagem de primeira ordem*  $\mathcal{L}$  consiste num alfabeto como descrito no item (a) e termos ( $\mathcal{L}$ -termos) e fórmulas ( $\mathcal{L}$ -fórmulas) como descritos nos itens (b) e (c). Uma linguagem de primeira ordem fica então completamente determinada pelos seus símbolos não lógicos.

**Definição 21.2.** Um *designador* é uma expressão que é um termo ou uma fórmula.

**Proposição 21.3.** Todo designador tem a forma  $uv_1 \dots v_n$ , onde  $u$  é um símbolo do alfabeto,  $v_1, \dots, v_n$  são designadores e  $n$  é um natural determinado por  $u$ .

**Prova.** Se  $d$  é um designador, então  $d$

**Definição 21.4.** Duas expressões são *compatíveis* se uma delas puder ser obtida adicionando alguma expressão (possivelmente a expressão vazia) ao final da outra.

**Proposição 21.5.** Sejam  $u, u', v$  e  $v'$  expressões.

- (a) Se  $uv$  e  $u'v'$  são compatíveis, então  $u$  e  $u'$  são compatíveis;
- (b) se  $uv$  e  $uv'$  são compatíveis, então  $v$  e  $v'$  são compatíveis.

**Prova.**

**Lema 21.6.** Seja  $n$  um natural. Se  $u_1, \dots, u_n$  e  $u'_1, \dots, u'_n$  são designadores, e  $u_1 \dots u_n$  e  $u'_1 \dots u'_n$  são compatíveis, então  $u'_i$  é  $u_i$ , para  $i = 1, \dots, n$ .

**Prova.** Faremos indução no comprimento de  $u_1 \dots u_n$ . Escreva  $u_1$  como  $vv_1 \dots v_k$ , onde  $v$  é um símbolo de índice  $k$  e  $v_1, \dots, v_k$  são designadores. Como  $u'_1$  começa com  $v$ , ele tem a forma  $vv'_1 \dots v'_k$ , onde  $v'_1, \dots, v'_k$  são designadores. Com isso, temos que  $u_1$  é compatível com  $u'_1$ , donde  $v_1 \dots v_k$  é compatível com  $v'_1 \dots v'_k$ . Daí, pela hipótese de indução,  $v_i$  é  $v'_i$  para  $i = 1, \dots, k$ , donde  $u_1$  é  $u'_1$ . Com isso, temos que  $u_2 \dots u_n$  é compatível com  $u'_2 \dots u'_n$ ; assim, pela hipótese de indução,  $u_i$  é  $u'_i$  para  $i = 2, \dots, n$ .

**Teorema 21.7** (Formação).

**Lema 21.8.**

**Teorema 21.9** (Ocorrência).

# Bibliografia

- [1] APOSTOL, Tom Mike. *Calculus Volume I*. 2ª ed. John Wiley e Sons, Inc., 1969.
- [2] APOSTOL, Tom Mike. *Calculus Volume II*. 2ª ed. John Wiley e Sons, Inc., 1969.
- [3] AURICHI, Leandro F. *Cálculo não renal*. Notas de Aula, 2025.
- [4] CAMINHA, Antonio. *Tópicos de Matemática Elementar - volume 4: Combinatória*. 3ª ed. Editora da SBM, 2024.
- [5] FAJARDO, Rogério A. S. *A Teoria dos Conjuntos e os Fundamentos da Matemática*. 1ª ed. Edusp, 2024.
- [6] FAJARDO, Rogério A. S. *Lógica Matemática*. 1ª ed. Edusp, 2017.
- [7] FEITOSA, Hércules de Araújo; ALFONSO, Alexys Bruno; NASCIMENTO, Maria Cunha. *Teoria dos Conjuntos*. 1ª ed. Editora Ciência Moderna, 2010.
- [8] FEITOSA, Hércules de Araújo; PAULOVICH, Leonardo. *Um Prelúdio à Lógica*. 1ª ed. Editora UNESP, 2005.
- [9] FRANCO, Tertuliano. *Princípios de Combinatória e Probabilidade*. 1ª ed. Editora do IMPA, 2020.
- [10] GUIDORIZZI, Hamilton Luiz. *Um Curso de Cálculo Volume 1*. 5ª ed. LTC, 2001.
- [11] GUIDORIZZI, Hamilton Luiz. *Um Curso de Cálculo Volume 2*. 5ª ed. LTC, 2001.
- [12] GUIDORIZZI, Hamilton Luiz. *Um Curso de Cálculo Volume 3*. 5ª ed. LTC, 2001.
- [13] GUIDORIZZI, Hamilton Luiz. *Um Curso de Cálculo Volume 4*. 5ª ed. LTC, 2001.
- [14] JECH, Thomas; HRBACEK, Karel. *Introduction to Set Theory*. 3ª ed. CRC Press, 1999.

- [15] JOHNSONBAUGH, Richard; PFAFFENBERGER, W. E. *Foundations of Mathematical Analysis*. 1ª ed. MARCEL DEKKER, INC., 1981.
- [16] LEARY, Christopher; KRISTIANSEN, Lars. *A Friendly Introduction to Mathematical Logic*. 2ª ed. Milne Library Publishing, 2015.
- [17] LIMA, Elon Lages. *Álgebra Linear*. 10ª ed. Editora do IMPA, 2020.
- [18] LIMA, Elon Lages. *Análise Real vol. 1*. 13ª ed. Editora do IMPA, 2024.
- [19] LIMA, Elon Lages. *Curso de Análise vol. 1*. 15ª ed. Editora do IMPA, 2022.
- [20] ROLLA, Leonardo T.; LIMA, Bernardo N. B. de. *Probabilidade*. 1ª ed. Editora do IMPA, 2026.
- [21] SHOENFIELD, Joseph R. *Mathematical Logic*. 1ª ed. Addison-Wesley Publishing Company, 1967.
- [22] STROMBERG, Karl R. *An Introduction to Classical Real Analysis*. 1ª ed. Wadsworth, Inc., 1981.
- [23] WHITE, A. J. *Real Analysis: an introduction*. 1ª ed. Addison-Wesley Publishing Company, 1968.