Álgebra Linear e Geometria Analítica

Aplicações lineares, matrizes, determinantes, teoria dos autovalores, bem como espaços vetoriais euclidianos e unitários

Lucien Sina

Álgebra Linear e Geometria Analítica

Aplicações lineares, matrizes, determinantes, teoria dos autovalores, bem como espaços vetoriais euclidianos e unitários

Lucien Sina

12.8.2026

Sumário

Prefácio **ix**

1 Conjuntos e aplicações **1**
1.1 Conjuntos 1
1.1.1 Conjuntos numéricos e suas extensões 3
1.1.2 Operações elementares com conjuntos 5
1.2 Aplicações 6
1.2.1 Imagem e imagem inversa 7
1.2.2 Restrição e extensão 8
1.2.3 Propriedades 8
1.2.4 Aplicação inversa 9
1.2.5 Teorema (Injetividade ⇔ sobrejetividade em conjuntos finitos) . 9
1.2.6 Composição 10
1.2.7 Identidade e inversa 12
1.2.8 Outros conceitos 14
1.2.9 Gráficos e relações 16
1.2.10 Relações de equivalência 17
1.2.11 Exercício 18
1.2.12 Classes de equivalência 19
1.3 Exercícios e soluções 20

2 Grupos **25**
2.1 Operação binária / composição 25
2.2 Definição 27
2.3 Convenções 29

2.4 Exemplos de grupos e de estruturas que não são grupos 29
2.5 Exercícios com soluções 30
2.6 Definição alternativa 31
2.7 Subgrupos 34
2.7.1 Exemplos 37
2.7.2 Teorema: classes de congruência módulo m como grupo 40
2.8 Exercícios e soluções 41

3 Anéis **47**
3.1 Definição 47
3.2 Consequências fundamentais 48
3.3 Exemplos 48
3.4 Propriedades 49
3.5 Subanéis e homomorfismos de anéis 50
3.5.1 Exemplos de subanéis 52
3.5.2 Exercícios com soluções 53
3.5.3 Contraexemplos 54

4 Corpos **56**
4.1 Outras regras de cálculo 58
4.2 Exemplos e contraexemplos 59
4.2.1 Dicas breves para provas 61
4.2.2 Respostas às perguntas da prova 61
4.3 Polinômios sobre corpos 63
4.4 Propriedades de $K[x]$ 64
4.5 Divisão em anéis 66
4.6 Existência de raízes 69
4.7 Número de raízes de um polinômio 70
4.8 Polinômios como funções e multiplicidades de raízes 71
4.9 Teorema Fundamental da Álgebra 73
4.10 Raízes de polinômios reais 75
4.11 Teorema de Abel e o resultado de impossibilidade de Abel 77
4.12 Fórmulas de Viète — funções simétricas elementares 79
4.13 Regra de sinais de Descartes 82

5 Espaços vetoriais **86**
5.1 Definição . . . 86
5.2 Subespaços vetoriais . . . 88
5.2.1 Construções e propriedades importantes . . . 89
5.2.2 Exemplos . . . 91
5.2.3 Polinômios de grau limitado . . . 94
5.2.4 Propriedades dos subespaços vetoriais . . . 95
5.3 Interseção e união de subespaços vetoriais . . . 96
5.4 Combinações lineares e subespaço gerado (span) . . . 97
5.5 Independência linear . . . 100
5.5.1 Exemplos de vetores linearmente independentes . . . 102
5.6 Exercícios e soluções . . . 107

6 Base e dimensão **112**
6.1 Definição de uma base . . . 112
6.1.1 Exemplos de bases (e de conjuntos que não são bases) . . . 114
6.1.2 Teorema de extração de uma base . . . 122
6.1.3 Lema da troca . . . 122
6.1.4 O teorema da troca . . . 124
6.1.5 Consequências do teorema da troca . . . 125
6.2 Dimensão . . . 125
6.2.1 Teorema da extensão de uma base . . . 127
6.3 Exemplos de dimensões . . . 127
6.3.1 Exemplos elementares . . . 127
6.3.2 Exemplos de dimensão infinita . . . 128
6.3.3 Exemplos com subespaços e núcleos . . . 129
6.3.4 Exemplo: combinação de geradores redundantes . . . 129
6.4 Exercícios com soluções . . . 130
6.5 Exercícios sobre dimensão . . . 134

7 Aplicações lineares **139**
7.1 Definição . . . 139
7.2 Consequências diretas . . . 141
7.3 Exemplos . . . 143
7.3.1 Multiplicação de matrizes como aplicação linear . . . 144
7.4 Composição e operações pontuais . . . 146

7.5 Outras propriedades . . . 148
7.6 Exercícios com soluções . . . 151
7.7 Núcleo e imagem . . . 154
7.8 Posto e teorema do posto e da nulidade . . . 156
7.9 Teorema da fatoração . . . 157
7.10 Espaços vetoriais quocientes . . . 160
7.10.1 Definição e construção . . . 161
7.10.2 Elementos como classes laterais afins . . . 162
7.10.3 Dimensão (caso de dimensão finita) . . . 162
7.10.4 Universalidade / propriedade de fatoração . . . 162
7.10.5 Primeiro teorema do isomorfismo . . . 163
7.11 Exemplos de espaços vetoriais quocientes . . . 164
7.11.1 Quociente de $\mathbb{R}^2$ pelo eixo x . . . 164
7.11.2 Caso geral em coordenadas . . . 165
7.11.3 Quocientes de polinômios $K[x]/(x^n)$ . . . 165
7.11.4 Exemplo com matrizes: quociente de $M_{n\times n}(K)$ pelo subespaço das matrizes de traço nulo . . . 165
7.11.5 Método geral para a escolha de representantes . . . 166
7.11.6 Breves observações geométricas . . . 166
7.12 Exercícios com soluções . . . 166
7.13 Sistemas de equações lineares . . . 170
7.13.1 Espaços de soluções . . . 173
7.14 Forma escalonada por linhas e representação paramétrica das soluções . 174
7.15 Sistemas fundamentais de soluções . . . 177
7.15.1 Casos especiais . . . 180
7.16 Exercícios com soluções . . . 181
7.17 Aplicações lineares e matrizes . . . 185
7.17.1 Consequências . . . 188
7.17.2 Representação matricial de aplicações lineares . . . 190
7.17.3 Escolha simplificada de bases . . . 193
7.17.4 Exercícios e soluções . . . 195
7.18 Multiplicação de matrizes . . . 198
7.18.1 Composição de aplicações lineares . . . 198
7.18.2 Regras de cálculo para matrizes . . . 203
7.18.3 Posto de um produto de matrizes . . . 206

7.18.4 Invertibilidade 207
7.18.5 Exercícios e soluções 209
7.19 Transformação de coordenadas 213
7.19.1 Coordenadas e sistemas de coordenadas 213
7.19.2 Matriz de mudança de base 215
7.19.3 A matriz de representação 217
7.19.4 Diagramas comutativos 218
7.19.5 Fórmula de transformação 221
7.19.6 Posto das colunas e posto das linhas 223
7.19.7 Equivalência de matrizes 224
7.19.8 Exercícios e soluções 226
7.19.9 Transformações de matrizes 230
7.19.10 Método de eliminação de Gauss 238
7.19.11 Exercícios e soluções 240

8 Determinantes **244**
8.1 Existência e unicidade 252
8.1.1 Permutações e transposições 252
8.1.2 Permutações pares e ímpares 253
8.1.3 A questão do sinal 254
8.1.4 Inversões como recurso de cálculo 254
8.1.5 Dedução da fórmula de Leibniz 256
8.1.6 Unicidade do determinante 257
8.1.7 Existência do determinante 258
8.1.8 Existência e unicidade 258
8.1.9 Propriedade de simetria do determinante 259
8.1.10 Aplicações e aspectos computacionais 259
8.2 Exercícios e soluções 261
8.3 Determinante de um endomorfismo 265

9 Teoria dos autovalores **269**
9.1 O polinômio característico 273
9.2 Diagonalização 277
9.3 Exercícios e soluções 281
9.4 A forma normal de Jordan 291
9.4.1 Exercícios e soluções 295

10 Espaços vetoriais euclidianos e unitários **298**
10.1 O produto interno canônico em $\mathbb{R}^n$ . . . 298
10.1.1 Comprimento e distância em $\mathbb{R}^n$ . . . 299
10.1.2 Propriedades da distância . . . 303
10.1.3 Medida de ângulos . . . 304
10.2 O produto interno em $\mathbb{C}^n$ . . . 306
10.2.1 Números complexos e o produto interno canônico . . . 307
10.2.2 Relação com o produto interno real . . . 311
10.3 Formas bilineares e sesquilineares . . . 313
10.3.1 Formas bilineares . . . 314
10.3.2 Representação matricial de formas bilineares . . . 316
10.3.3 A fórmula de transformação . . . 319
10.3.4 Formas quadráticas . . . 321
10.3.5 Formas sesquilineares e formas hermitianas . . . 322
10.3.6 Definição positiva . . . 326
10.3.7 Normas e métricas . . . 328
10.3.8 Ortogonalidade e ortonormalidade . . . 331
10.3.9 O teorema da ortonormalização . . . 334
10.4 Endomorfismos ortogonais e unitários . . . 337
10.4.1 Definição e primeiros exemplos . . . 337
10.4.2 Matrizes ortogonais e unitárias . . . 341
10.4.3 Espaços-padrão e matrizes . . . 345
10.4.4 Diagonalização unitária . . . 350
10.4.5 A forma normal ortogonal . . . 352
10.5 Endomorfismos autoadjuntos . . . 354
10.5.1 Definição e caracterização matricial . . . 355
10.5.2 O teorema espectral . . . 356
10.5.3 Cálculo de bases ortonormais . . . 359
10.5.4 Uma abordagem real para matrizes simétricas . . . 361
10.6 Transformação dos eixos principais . . . 363
10.6.1 O caso real . . . 363
10.6.2 Lei da inércia de Sylvester . . . 370
10.6.3 O teorema da ortogonalização . . . 372
10.6.4 Cálculo da matriz de transformação . . . 374
10.6.5 O critério de Sylvester . . . 376

10.6.6 Retrospectiva 379
10.7 Exercícios e soluções 380
10.7.1 O produto interno canônico em $\mathbb{R}^n$ 380
10.7.2 O produto interno canônico em $\mathbb{C}^n$ 380
10.7.3 Formas bilineares e sesquilineares 381
10.7.4 Endomorfismos ortogonais e unitários 382
10.7.5 Endomorfismos autoadjuntos 383
10.7.6 Transformação para os eixos principais 384

11 Considerações finais **386**
11.1 Retrospectiva 386
11.2 Perspectivas 387
11.3 Recomendações de leitura 387

12 Aviso legal **392**

Prefácio

A Álgebra Linear constitui um dos fundamentos centrais da matemática moderna e, ao mesmo tempo, uma ferramenta indispensável nas ciências naturais e nas engenharias. Seus conceitos e métodos manifestam-se, sob formas sempre renovadas, em numerosas áreas, desde a resolução de sistemas de equações lineares e o estudo de problemas geométricos até estruturas profundas da álgebra abstrata e da análise. Este livro tem por objetivo apresentar a Álgebra Linear e a Geometria Analítica de maneira tão clara, estruturada e abrangente quanto possível. Para isso, adota-se deliberadamente uma abordagem que não se limita à exposição dos resultados clássicos, mas desenvolve passo a passo as estruturas que lhes servem de fundamento. Partindo de conceitos elementares, como conjuntos e aplicações, introduzem-se gradualmente as principais estruturas algébricas: grupos, anéis e corpos. Sobre essa base, os espaços vetoriais surgem como o ambiente natural da álgebra linear. Dedica-se especial atenção ao desenvolvimento sistemático da teoria das aplicações lineares e das matrizes. Conceitos como base, dimensão, núcleo e imagem não são tratados isoladamente, mas apresentados em um contexto estrutural unificado. A partir daí, desenvolve-se a teoria dos autovalores, que permite compreender em profundidade a estrutura interna das aplicações lineares. Outro componente central é o estudo dos espaços vetoriais euclidianos e unitários. Nesse contexto, os aspectos geométricos ganham destaque: produtos internos, ortogonalidade, normas e bases ortonormais estabelecem uma ligação entre conceitos algébricos e a intuição geométrica. Resultados como o teorema espectral exemplificam a estreita relação entre álgebra e geometria. O livro foi concebido tanto como material de apoio para uma disciplina quanto para o estudo autônomo. Numerosos exemplos, exercícios e soluções-modelo visam aprofundar a compreensão e incentivar o uso ativo dos conceitos abordados. Um dos principais propósitos desta obra é não apenas transmitir técnicas de cálculo, mas também promover a compreensão das estruturas subjacentes. Assim, a Álgebra Linear não é apresentada como uma coleção de métodos isolados, mas como um

sistema matemático coeso que estabelece conexões entre diversas áreas da matemática.

Capítulo 1

Conjuntos e aplicações

Conjuntos e aplicações constituem a base da álgebra linear e da maior parte da matemática.

1.1 Conjuntos

Um *conjunto* é uma coleção de objetos bem distintos, denominados seus *elementos*. A seguir, apresentamos alguns conceitos e notações usuais que serão empregados regularmente ao longo do texto.

Conjuntos finitos: Um conjunto finito pode ser representado pela enumeração completa de seus elementos. Escreve-se, por exemplo, $M := \{x_1, x_2, \ldots, x_n\}$. O símbolo $:=$ significa "é definido como". Os símbolos x_i são denominados *elementos* de M; escreve-se $x_i \in M$ para $1 \leq i \leq n$. A ordem da enumeração é irrelevante, e repetições não são contabilizadas: a representação $\{a, b, a\}$ designa o mesmo conjunto que $\{a, b\}$. Se os elementos enumerados forem dois a dois distintos, isto é, se $x_i \neq x_j$ para todos $i \neq j$, então n será exatamente o número de elementos de M. O número de elementos, ou a cardinalidade, de um conjunto finito M é denotado por $|M|$.

Conjunto vazio: O conjunto vazio não contém elemento algum e é denotado por $\varnothing$ (ou $\{\}$).

Subconjuntos: Um conjunto M' é denominado subconjunto de M, e escreve-se $M' \subseteq M$, se, e somente se, $\forall x \ (x \in M' \Rightarrow x \in M)$. Se $M' \subseteq M$ e $M' \neq M$, escreve-se $M' \subsetneq M$, e M' é denominado *subconjunto próprio* de M. Dois conjuntos são iguais se,

e somente se, cada um deles for subconjunto do outro:

$$M = N \quad \Longleftrightarrow \quad M \subseteq N \ \text{ e } \ N \subseteq M.$$

Notação de conjuntos por compreensão: Frequentemente, define-se um conjunto por meio de uma propriedade: $\{\, x \in X \mid P(x) \,\}$ lê-se "o conjunto de todos os x pertencentes a X para os quais a propriedade $P(x)$ è satisfeita". Por exemplo: $\{n \in \mathbb{Z} \mid n \text{ é par}\}$.

Conjuntos infinitos e os números naturais: O exemplo mais conhecido de um conjunto infinito simples è o conjunto dos números naturais. Adotaremos aqui a convenção $\mathbb{N} := \{0, 1, 2, 3, \dots\}$. A estrutura de $\mathbb{N}$ pode ser descrita axiomaticamente pelos *axiomas de Peano* (em uma de suas formulações usuais):

1. $0 \in \mathbb{N}$.
2. Existe uma aplicação $S : \mathbb{N} \to \mathbb{N}$, denominada *aplicação sucessor*, que associa a cada n o seu sucessor $S(n)$.
3. 0 não è sucessor de nenhum número natural: $\forall n \in \mathbb{N} : \ S(n) \neq 0$.
4. A aplicação sucessor è injetiva: $\forall m, n \in \mathbb{N} : \ S(m) = S(n) \Rightarrow m = n$.
5. (Axioma da indução) Se $K \subseteq \mathbb{N}$, $0 \in K$ e $\forall n \in K : \ S(n) \in K$, então $K = \mathbb{N}$.

Os axiomas de Peano estabelecem a estrutura fundamental dos números naturais: existe um menor elemento, 0; cada elemento possui um sucessor univocamente determinado; e o princípio da indução permite demonstrar propriedades para todos os números naturais. (Alguns autores adotam a convenção de iniciar os números naturais em 1, em vez de 0; isso altera algumas formulações, mas não a teoria fundamental.)

Observação 1. *Os conceitos e as notações aqui utilizados — representação de conjuntos por chaves, $\in$, $\subseteq$, $|M|$, $\varnothing$ e a notação de conjuntos por compreensão — são empregados constantemente na àlgebra linear; a familiaridade com essas notações facilitará consideravelmente o estudo dos tópicos subsequentes.*

1.1.1 Conjuntos numéricos e suas extensões

Partindo dos números naturais, podem-se obter, por meio de extensões sistemáticas, outros conjuntos numéricos importantes para a análise e para a álgebra linear.

Números inteiros: O conjunto dos números inteiros é definido por $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$. Intuitivamente, obtém-se $\mathbb{Z}$ a partir de $\mathbb{N}$ introduzindo, para cada n positivo, um elemento negativo $-n$. Formalmente, pode-se interpretar $\mathbb{Z}$ como o conjunto das classes de equivalência de pares de números naturais (a, b), em que (a, b) representa a diferença $a - b$.

Números racionais: Os números racionais são as "frações" de números inteiros: $\mathbb{Q} := \{\, p/q \mid p, q \in \mathbb{Z},\ q \neq 0 \,\}$. Também neste caso há uma construção formal por meio de classes de equivalência de pares (p, q), com a relação de equivalência $(p, q) \sim (p', q')$ se, e somente se, $pq' = p'q$. O conjunto $\mathbb{Q}$ é um corpo (isto é, nele são válidas as regras usuais de cálculo para $+, \cdot$, exceto a divisão por 0) e é denso em $\mathbb{R}$: entre quaisquer dois números reais distintos existe sempre um número racional.

Números reais: Os números reais $\mathbb{R}$ contêm $\mathbb{Q}$ e constituem o ambiente adequado para o estudo de limites, continuidade e análise clássica. Existem várias construções equivalentes de $\mathbb{R}$; duas das mais usuais são:

- *cortes de Dedekind*: um número real é interpretado por meio de um corte, isto é, uma partição dos números racionais em dois conjuntos não vazios A, B, tais que $a < b$ para todos $a \in A$ e $b \in B$;
- *completamento por sequências de Cauchy*: consideram-se sequências de Cauchy de números racionais e formam-se classes de equivalência, identificando-se duas sequências quando a diferença entre elas converge para zero.

De maneira intuitiva, os números reais podem ser representados por expansões decimais (por exemplo, 3,14159… para π); nem todas essas expansões são finitas ou periódicas. Os números cujas expansões decimais não são finitas nem periódicas são denominados *irracionais* (por exemplo, $\sqrt{2}$ e π). Uma propriedade fundamental de $\mathbb{R}$ é a *completude*: todo subconjunto não vazio de $\mathbb{R}$ que seja limitado superiormente possui um supremo, isto é, uma menor cota superior.

Números complexos: Os números complexos são definidos por $\mathbb{C} := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{R},\ \mathrm{i}^2 = -1\}$. Também se pode interpretar $\mathbb{C}$ como o conjunto dos pares (a, b), munido de operações adequadas de adição e multiplicação. O conjunto $\mathbb{C}$ é um corpo, mas não

um corpo ordenado, pois não existe uma ordem total compatível com suas operações de adição e multiplicação. Um resultado fundamental, aqui apresentado sem demonstração, é o Teorema Fundamental da Álgebra: todo polinômio não constante com coeficientes complexos possui pelo menos uma raiz em $\mathbb{C}$. Portanto, $\mathbb{C}$ é algebricamente fechado.

Cadeia de inclusões: Esses conjuntos numéricos estão relacionados pela seguinte cadeia natural de inclusões:

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

Cada uma dessas inclusões é própria (por exemplo, $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ e $\mathrm{i} \in \mathbb{C} \setminus \mathbb{R}$).

Propriedades algébricas e de ordem:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são fechados em relação às operações $+$ e $\cdot$; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos.
- $\mathbb{Q}$ é denso em $\mathbb{R}$: entre quaisquer dois números reais distintos existe um número racional.
- $\mathbb{R}$ é, a menos de isomorfismo, o único corpo ordenado completo; essa completude explica por que muitas afirmações da análise (por exemplo, as relativas à existência de limites) são válidas em $\mathbb{R}$, mas não necessariamente em $\mathbb{Q}$.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ são conjuntos infinitos enumeráveis, enquanto $\mathbb{R}$ e $\mathbb{C}$ têm cardinalidade não enumerável.

Observação 2. *Em uma primeira leitura, é útil compreender claramente a motivação de cada extensão:*

- $\mathbb{Z}$ *surge para que a subtração possa ser sempre efetuada;*
- $\mathbb{Q}$ *surge para permitir a divisão, exceto por* 0*;*
- $\mathbb{R}$ *surge para completar o sistema numérico em relação a limites (por exemplo, limites de sequências);*
- $\mathbb{C}$ *surge para assegurar a fatoração completa de polinômios em fatores lineares e completar algebricamente a estrutura.*

Exemplos simples (por exemplo, $2-5$ *requer* $\mathbb{Z}$*, a equação* $2x = 1$ *requer* $\mathbb{Q}$*, e a sequência* $1; 1{,}4; 1{,}41; 1{,}414; \ldots$ *conduz a* $\sqrt{2} \in \mathbb{R}$*) tornam essas extensões mais concretas para os estudantes.*

1.1.2 Operações elementares com conjuntos

A partir de um conjunto dado M, podem-se formar numerosos subconjuntos selecionando-se os elementos de acordo com determinadas propriedades. O *conjunto das partes* $\mathcal{P}(M)$ designa o conjunto de todos os subconjuntos de M.

Subconjunto definido por uma propriedade (notação por compreensão): Se M for um conjunto e $E(x)$ uma propriedade de x, define-se $M' := \{\, x \in M \mid E(x) \,\}$, lido como "o conjunto de todos os x pertencentes a M para os quais $E(x)$ é satisfeita". Exemplo: $\{n \in \mathbb{N} \mid n \text{ é primo}\}$.

União e interseção (formas finitas e indexadas): Sejam $M_1, \ldots, M_n$ conjuntos. Definem-se a união e a interseção por

$$M_1 \cup \cdots \cup M_n := \{x \mid \exists i \in \{1, \ldots, n\} : \ x \in M_i\},$$

$$M_1 \cap \cdots \cap M_n := \{x \mid \forall i \in \{1, \ldots, n\} : \ x \in M_i\}.$$

Para famílias de conjuntos $(X_i)_{i \in I}$, indexadas por um conjunto de índices I, utilizam-se as notações usuais de união e interseção indexadas:

$$\bigcup_{i \in I} X_i := \{x \mid \exists i \in I : \ x \in X_i\},$$
$$\bigcap_{i \in I} X_i := \{x \mid \forall i \in I : \ x \in X_i\}.$$

Exemplo com intervalos: Considere $I = \mathbb{N}$, segundo a convenção aqui adotada $\mathbb{N} = \{0, 1, 2, \ldots\}$, e $X_i := [-i, i] \subset \mathbb{R}$. Então, $\bigcup_{i \in \mathbb{N}} [-i, i] = \mathbb{R}$, pois, para todo número real x, existe um i tal que $|x| \leq i$. Por outro lado,

$$\bigcap_{i \in \mathbb{N}} [-i, i] = [-0, 0] = \{0\},$$

pois $X_0 = [0, 0] = \{0\}$ já está incluído na interseção. (Se, alternativamente, fosse adotada a convenção de que $\mathbb{N}$ começa em 1, isto é, $I = \{1, 2, \ldots\}$, ter-se-ia $\bigcap_{i \geq 1} [-i, i] = [-1, 1]$.)

Diferença e complemento: Se $X' \subseteq X$, então

$$X \setminus X' := \{\, x \in X \mid x \notin X' \,\}$$

é denominada a *diferença* entre X e X'. O *complemento* de um conjunto A é sempre definido em relação a um conjunto universo U; nesse caso, escreve-se

$$A^{\complement} := U \setminus A = \{\, x \in U \mid x \notin A \,\}.$$

Outras operações úteis: A *diferença simétrica* entre A e B é definida por

$$A \triangle B := (A \setminus B) \cup (B \setminus A),$$

isto é, consiste exatamente nos elementos que pertencem a apenas um dos dois conjuntos, mas não a ambos.

Leis fundamentais das operações com conjuntos: Para os conjuntos A, B, C, valem as seguintes leis elementares, úteis em manipulações algébricas e demonstrações:

- *Comutatividade:* $A \cup B = B \cup A, \quad A \cap B = B \cap A.$
- *Associatividade:* $(A \cup B) \cup C = A \cup (B \cup C)$, e, analogamente, para $\cap$.
- *Idempotência:* $A \cup A = A, \quad A \cap A = A.$
- *Distributividade:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- *Leis de De Morgan (também para famílias indexadas):*

$$\Big(\bigcup_{i \in I} X_i\Big)^{\complement} = \bigcap_{i \in I} X_i^{\complement}, \qquad \Big(\bigcap_{i \in I} X_i\Big)^{\complement} = \bigcup_{i \in I} X_i^{\complement}.$$

- *Leis da diferença:* $A \setminus B = A \cap B^{\complement}$. Além disso, $(A \setminus B) \cup (B \setminus A) = A \triangle B$.

1.2 Aplicações

Para descrever relações entre conjuntos, utilizam-se *aplicações.*

Definição 3. *Sejam X e Y conjuntos. Uma* aplicação *(ou* função*) de X em Y é uma regra f que associa a cada $x \in X$ um único elemento $f(x) \in Y$. Escrevemos $f : X \to Y, \qquad x \mapsto f(x)$. Aqui, $\to$ relaciona os conjuntos (domínio e contradomínio), enquanto $\mapsto$ descreve a associação do elemento x a $f(x)$.*

Definição 4. *Duas aplicações $f, g : X \to Y$ são ditas iguais, e escreve-se $f = g$, se, e somente se, $\forall x \in X : \ f(x) = g(x)$. O conjunto de todas as aplicações de X em Y é denotado por* $\mathrm{Abb}(X, Y)$ *(também se escreve* $\mathrm{Fun}(X, Y)$*).*

1.2.1 Imagem e imagem inversa

Por meio de aplicações, podem-se associar entre si não apenas elementos individuais, mas também subconjuntos de conjuntos.

Definição 5 (Imagem)**.** *Sejam $f : X \to Y$ uma aplicação e $M \subseteq X$ um subconjunto. A* imagem *de M por f é $f(M) := \{\, y \in Y \mid \exists x \in M : \; y = f(x) \,\}$. Em particular, $f(\{x\}) = \{f(x)\}$ para $x \in X$, e $f(X) \subseteq Y$ também é denominado* conjunto imagem *ou simplesmente* imagem *de f.*

Definição 6 (Imagem inversa)**.** *Sejam $f : X \to Y$ uma aplicação e $N \subseteq Y$. A* imagem inversa *de N por f é $f^{-1}(N) := \{\, x \in X \mid f(x) \in N \,\} \subseteq X$. Para um único elemento $y \in Y$, escreve-se, de forma abreviada, $f^{-1}(\{y\})$ ou $f^{-1}(y)$ para designar o conjunto de todos os elementos $x \in X$ tais que $f(x) = y$.*

Importante: Neste contexto, f^{-1} é uma aplicação entre conjuntos de partes (uma operação $\mathcal{P}(Y) \to \mathcal{P}(X)$), e não necessariamente uma aplicação no sentido de $Y \to X$. A imagem inversa de um conjunto unitário pode conter vários elementos ou ser vazia.

Exemplos:

- A aplicação identidade $\mathrm{id}_X : X \to X$, definida por $\mathrm{id}_X(x) = x$, satisfaz, para todo subconjunto $M \subseteq X$, $\mathrm{id}_X(M) = M$ e $\mathrm{id}_X^{-1}(M) = M$.

- A aplicação constante $c : X \to Y$, definida por $c(x) = y_0$ para todo $x \in X$, tem imagem $\{y_0\}$; a imagem inversa de $\{y\}$, para $y \neq y_0$, é vazia, enquanto $c^{-1}(\{y_0\}) = X$.

- Exemplo de inclusão estrita envolvendo interseção e imagem: sejam $X = \{1, 2\}$, $Y = \{a\}$ e $f(1) = f(2) = a$. Tomando $M_1 = \{1\}$ e $M_2 = \{2\}$, tem-se $f(M_1) \cap f(M_2) = \{a\}$, mas $f(M_1 \cap M_2) = f(\varnothing) = \varnothing$. Portanto, em geral, vale apenas

  $$f(M_1 \cap M_2) \subseteq f(M_1) \cap f(M_2),$$

  e a inclusão pode ser estrita.

Regras de cálculo importantes: Para uma aplicação $f : X \to Y$, uma família $(M_i)_{i \in I}$ de subconjuntos de X e uma família $(N_j)_{j \in J}$ de subconjuntos de Y, valem as seguintes relações:

$$f\left(\bigcup_{i\in I} M_i\right) = \bigcup_{i\in I} f(M_i),$$
$$f\left(\bigcap_{i\in I} M_i\right) \subseteq \bigcap_{i\in I} f(M_i),$$
$$f^{-1}\left(\bigcup_{j\in J} N_j\right) = \bigcup_{j\in J} f^{-1}(N_j),$$
$$f^{-1}\left(\bigcap_{j\in J} N_j\right) = \bigcap_{j\in J} f^{-1}(N_j),$$
$$f^{-1}(Y \setminus N) = X \setminus f^{-1}(N),$$
$$f(\varnothing) = \varnothing.$$

A primeira igualdade mostra que a imagem de uma união é a união das imagens; para interseções, em geral, vale apenas a inclusão indicada por $\subseteq$ (há igualdade, por exemplo, quando f é injetiva). As imagens inversas, por sua vez, comutam tanto com uniões quanto com interseções e, portanto, apresentam um comportamento particularmente adequado em relação às operações entre conjuntos: a imagem inversa de uma união é a união das imagens inversas, e a imagem inversa de uma interseção é a interseção das imagens inversas. Em contrapartida, para imagens diretas de interseções, em geral, vale apenas uma inclusão.

1.2.2 Restrição e extensão

Definição 7 (Restrição)**.** *Sejam $f : X \to Y$ uma aplicação e $M \subseteq X$. A* restrição *de f a M é a aplicação $f|_M : M \to Y$, $\quad x \mapsto f(x)$.*

Observação sobre a ampliação do contradomínio: Se $Y \subseteq Y'$ e $f : X \to Y$, então f também pode ser considerada uma aplicação $f : X \to Y'$, com os mesmos valores e um contradomínio maior. Nesse caso, fala-se em uma ampliação do contradomínio.

1.2.3 Propriedades

Definição 8. *Uma aplicação $f\colon X \to Y$ denomina-se*

- injetiva *(ou* um a um*) se*

$$\forall x, x' \in X: \quad f(x) = f(x') \implies x = x'.$$

- sobrejetiva *se*

$$f(X) = Y \quad \iff \quad \forall y \in Y \ \exists x \in X: \ y = f(x).$$

- bijetiva *se for simultaneamente injetiva e sobrejetiva.*

1.2.4 Aplicação inversa

Se $f\colon X \to Y$ é bijetiva, então, para cada $y \in Y$, existe um único $x \in X$ tal que $f(x) = y$. Nesse caso, define-se a *aplicação inversa* $f^{-1}\colon Y \to X, \qquad y \mapsto f^{-1}(y)$, de modo que $f^{-1}(f(x)) = x$ para todo $x \in X$ e $f(f^{-1}(y)) = y$ para todo $y \in Y$.

Importante: Não se devem confundir os dois significados de f^{-1}:

- Para uma aplicação arbitrária f e um subconjunto $N \subseteq Y$, a expressão $f^{-1}(N)$ denota a *pré-imagem* de N, isto é,

$$f^{-1}(N) = \{x \in X \mid f(x) \in N\} \subseteq X.$$

  Trata-se de uma operação $\mathcal{P}(Y) \to \mathcal{P}(X)$.

- Se f é bijetiva, f^{-1} denota também a *aplicação inversa* $Y \to X$. Nesse caso, a pré-imagem de um conjunto unitário é o conjunto unitário que contém o elemento correspondente pela aplicação inversa: $f^{-1}(\{y\}) = \{\, f^{-1}(y) \,\} \qquad (y \in Y)$.

1.2.5 Teorema (Injetividade ⇔ sobrejetividade em conjuntos finitos)

Teorema 9. *Seja X um conjunto finito e seja $f\colon X \to X$ uma aplicação. Então, as seguintes afirmações são equivalentes:*

1. *f é injetiva.*
2. *f é sobrejetiva.*
3. *f é bijetiva.*

Demonstração. Se $X = \varnothing$, as três afirmações são imediatamente verdadeiras. Suponhamos, portanto, que $X = \{x_1, \ldots, x_n\}$, em que os elementos x_i são dois a dois distintos e $n \geq 1$.

(**1**) $\Rightarrow$ (**2**): Suponhamos que f seja injetiva. Então, as imagens $f(x_1), \ldots, f(x_n)$ são duas a duas distintas; logo, o conjunto $f(X) = \{f(x_1), \ldots, f(x_n)\}$ possui exatamente n elementos. Como $f(X) \subseteq X$ e X também possui n elementos, segue que $f(X) = X$. Portanto, f é sobrejetiva.

(**2**) $\Rightarrow$ (**1**): Suponhamos que f seja sobrejetiva, isto é, $f(X) = X$. Se f não fosse injetiva, existiriam $x_i \neq x_j$ tais que $f(x_i) = f(x_j)$. Nesse caso, a imagem teria no máximo $n-1$ elementos, ou seja, $|f(X)| \leq n-1$, o que contradiz a hipótese $f(X) = X$, pois $|X| = n$. Consequentemente, f é injetiva.

A equivalência com (3) é agora imediata, pois uma aplicação é bijetiva precisamente quando é simultaneamente injetiva e sobrejetiva. Portanto, (1), (2) e (3) são equivalentes. □

Observação 10. *Para conjuntos infinitos, a afirmação não é válida em geral: em* $\mathbb{N}$*, existem aplicações injetivas que não são sobrejetivas, como* $n \mapsto n+1$*, e aplicações sobrejetivas que não são injetivas, como* $n \mapsto \lfloor n/2 \rfloor$*. A finitude é, portanto, a hipótese decisiva deste teorema. Em resumo:* para aplicações de um conjunto finito em si mesmo, injetividade e sobrejetividade são equivalentes.

1.2.6 Composição

Definição 11. *Sejam* X, Y, Z *conjuntos e sejam* $f\colon X \to Y$ *e* $g\colon Y \to Z$ *aplicações. A* composição *de* f *e* g *é a aplicação*

$$g \circ f\colon X \longrightarrow Z, \qquad (g \circ f)(x) := g(f(x)).$$

Lê-se $g \circ f$ *como "*g *composta com* f*" (primeiro aplica-se* f *e, em seguida,* g*). Em notação diagramática:*

$$X \xrightarrow{f} Y \xrightarrow{g} Z \qquad \textit{ou, equivalentemente,} \qquad Z \xleftarrow{g} Y \xleftarrow{f} X.$$

Teorema 12 (Associatividade da composição)**.** *Para aplicações* $f\colon X \to Y$*,* $g\colon Y \to Z$ *e* $h\colon Z \to W$*, vale*

$$(h \circ g) \circ f \;=\; h \circ (g \circ f).$$

Demonstração. Seja $x \in X$. Então,

$$\begin{aligned}((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= (h \circ (g \circ f))(x).\end{aligned}$$

Como os dois membros são iguais para todo $x \in X$, as aplicações são iguais. □

Teorema 13 (Não comutatividade em geral)**.** *A composição de aplicações, em geral,* não *é comutativa, isto é, em geral, tem-se* $g \circ f \neq f \circ g$.

Exemplo. Considere $X = Y = Z = \mathbb{R}$ e as aplicações

$$f(x) = x + 1, \qquad g(x) = 2x \quad (x \in \mathbb{R}).$$

Então, para todo $x \in \mathbb{R}$, tem-se:

$$(g \circ f)(x) = g(f(x)) = g(x + 1) = 2(x + 1) = 2x + 2,$$

enquanto

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1.$$

Como $2x + 2 \neq 2x + 1$ (por exemplo, para $x = 0$), as aplicações $g \circ f$ e $f \circ g$ são distintas, o que demonstra a afirmação. □

Observação:

- Convém lembrar: $\circ$ é uma operação *associativa*, mas não *comutativa*. Por isso, a notação $h \circ g \circ f$, sem parênteses, é inequívoca.
- A ordem de execução é importante: $g \circ f$ significa aplicar primeiro f e, em seguida, g. Pratique essa ordem com exemplos simples de cálculo até que ela se torne intuitiva.
- Mais adiante, aprofundaremos a relação entre composição, aplicações identidade e aplicações inversas.

1.2.7 Identidade e inversa

Definição 14. *Para todo conjunto X, denomina-se* aplicação identidade *a aplicação*

$$\mathrm{id}_X \colon X \longrightarrow X, \qquad \mathrm{id}_X(x) := x \quad (x \in X).$$

Teorema 15. *Seja $f \colon X \to Y$ uma aplicação, com $X, Y \neq \varnothing$. Então valem as seguintes afirmações:*

1. *f é injetiva $\iff$ existe $g \colon Y \to X$ tal que $g \circ f = \mathrm{id}_X$.*
2. *f é sobrejetiva $\iff$ existe $g \colon Y \to X$ tal que $f \circ g = \mathrm{id}_Y$.*
3. *f é bijetiva $\iff$ existe $g \colon Y \to X$ tal que*

$$g \circ f = \mathrm{id}_X \quad e \quad f \circ g = \mathrm{id}_Y.$$

Nesse caso, g é única e denomina-se aplicação inversa*, ou simplesmente* inversa*, de f; escreve-se $g = f^{-1}$.*

Demonstração. **(1)** "⇒": Seja f injetiva. Fixe um elemento $x_0 \in X$ (o que é possível, pois $X \neq \varnothing$). Defina $g \colon Y \to X$ por

$$g(y) := \begin{cases} \text{o único } x \in X \text{ tal que } f(x) = y, & y \in f(X), \\ x_0, & y \notin f(X). \end{cases}$$

Essa definição é bem definida, pois, para $y \in f(X)$, a injetividade garante a existência de exatamente um x tal que $f(x) = y$. Para todo $x \in X$, tem-se então

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

portanto, $g \circ f = \mathrm{id}_X$.

"⇐": Seja $g \colon Y \to X$ tal que $g \circ f = \mathrm{id}_X$. Se $f(x) = f(x')$, então

$$x = \mathrm{id}_X(x) = g(f(x)) = g(f(x')) = \mathrm{id}_X(x') = x',$$

logo, $x = x'$. Portanto, f é injetiva.

(2) "⇒": Seja f sobrejetiva. Para cada $y \in Y$, escolha e fixe um elemento $x_y \in X$ tal que $f(x_y) = y$, e defina $g(y) := x_y$. Então $f(g(y)) = y$ para todo $y \in Y$, de modo que $f \circ g = \mathrm{id}_Y$.

"$\Leftarrow$": Seja $g\colon Y \to X$ tal que $f \circ g = \mathrm{id}_Y$. Para todo $y \in Y$, tem-se $y = f(g(y))$, logo $y \in f(X)$. Portanto, $f(X) = Y$ e f é sobrejetiva.

Observação sobre (2): A construção de uma aplicação g desse tipo a partir de uma aplicação sobrejetiva f consiste em escolher, para cada $y \in Y$, uma preimagem $x_y \in f^{-1}(\{y\})$. Em situações finitas ou construtivas, isso não apresenta dificuldades; para conjuntos arbitrários, a afirmação geral de que "toda sobrejeção possui uma inversa à direita" requer uma função de escolha e, portanto, está relacionada ao *axioma da escolha*.

(3) Se f é bijetiva, então existe a aplicação inversa f^{-1}, e valem imediatamente as identidades

$$f^{-1} \circ f = \mathrm{id}_X, \qquad f \circ f^{-1} = \mathrm{id}_Y.$$

Reciprocamente, das duas identidades e dos itens (1) e (2), conclui-se que f é injetiva e sobrejetiva e, portanto, bijetiva.

Unicidade da inversa: Se $g, h\colon Y \to X$ satisfazem ambas as identidades, então

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h,$$

isto é, $g = h$. Logo, a inversa é única. □

Observações:

- Os conceitos de "inversa à esquerda" (para g tal que $g \circ f = \mathrm{id}_X$) e de "inversa à direita" (para g tal que $f \circ g = \mathrm{id}_Y$) são úteis: injetividade $\iff$ existência de uma inversa à esquerda; sobrejetividade $\iff$ existência de uma inversa à direita.

- A existência de uma inversa à direita de uma sobrejeção exige que se escolha, para cada y, uma preimagem; no caso de conjuntos infinitos, esse é um ponto em que se pode abordar o axioma da escolha.

- Deve-se ter cuidado com a notação: em geral, f^{-1} denota a imagem inversa de subconjuntos. No caso de bijeções, f^{-1} também é empregada para denotar a aplicação inversa $Y \to X$.

1.2.8 Outros conceitos

Definição 16 (Tuplas ordenadas / funções de escolha)**.** *Sejam $X_1, \ldots, X_n$ conjuntos. Uma n-*tupla ordenada *é uma expressão $x = (x_1, \ldots, x_n)$ com $x_i \in X_i$ para $i = 1, \ldots, n$. Pode-se interpretar x como a função*

$$x : \{1, \ldots, n\} \longrightarrow X_1 \cup \cdots \cup X_n, \qquad i \mapsto x(i) = x_i,$$

e, nesse sentido, x também é por vezes denominada função de escolha*, pois, para cada índice i, escolhe-se um elemento x_i de X_i. Frequentemente, escreve-se também, de forma abreviada, $x_i := x(i)$ ou $x = \{x_1, \ldots, x_n\}$ (esta última notação apenas informalmente).*

Observação 17. *Duas tuplas são iguais se, e somente se, todas as suas componentes forem iguais:*

$$(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) \quad \Longleftrightarrow \quad x_1 = x'_1, \ \ldots, \ x_n = x'_n.$$

Portanto, a ordem das componentes é relevante (ao contrário do que ocorre com conjuntos).

Definição 18 (Produto cartesiano / produto direto)**.** *O* produto cartesiano*, ou* produto direto*, dos conjuntos $X_1, \ldots, X_n$ é*

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) \mid x_i \in X_i \ \text{ para } i = 1, \ldots, n\}.$$

No caso particular em que $X_1 = \cdots = X_n = X$, escreve-se $X^n := X \times \cdots \times X$.

Proposição 19. *Se n é finito, então*

$$X_1 \times \cdots \times X_n \neq \varnothing \quad \Longleftrightarrow \quad X_i \neq \varnothing \ \text{ para todo } i.$$

Observação 20. *Para famílias infinitas $(X_i)_{i \in I}$, a implicação $\left(\prod_{i \in I} X_i \neq \varnothing \Rightarrow X_i \neq \varnothing \ \forall i\right)$ é sempre válida. A implicação recíproca $\left(X_i \neq \varnothing \ \forall i \Rightarrow \prod_{i \in I} X_i \neq \varnothing\right)$, contudo, em geral só é válida mediante o uso do* axioma da escolha*. Trata-se de uma distinção importante, embora frequentemente técnica: para produtos finitos, o axioma da escolha não é necessário; para uma quantidade arbitrária de fatores, em geral, ele é necessário.*

Definição 21 (Projeções)**.** *Para cada $i \in \{1, \ldots, n\}$, define-se a i-ésima* projeção *por*

$$\pi_i : X_1 \times \cdots \times X_n \longrightarrow X_i, \qquad \pi_i(x_1, \ldots, x_n) := x_i.$$

Observação 22. *Se $X_1 \times \cdots \times X_n \neq \varnothing$, então π_i é sobrejetiva em X_i: para cada $y \in X_i$, existe uma tupla em $X_1 \times \cdots \times X_n$ cuja i-ésima componente é y (em produtos finitos, podem-se escolher arbitrariamente as demais componentes; em produtos infinitos, a construção de tais tuplas pode exigir o axioma da escolha).*

Definição 23 (Famílias e sequências)**.** *Seja I um conjunto arbitrário (conjunto de índices). Uma aplicação*

$$\varphi : I \longrightarrow X, \qquad i \mapsto x_i = \varphi(i),$$

é denominada uma família indexada *de elementos de X. Essa família é denotada abreviadamente por $(x_i)_{i\in I}$. Se $I = \mathbb{N}$, então $(x_i)_{i\in\mathbb{N}}$ é denominada uma* sequência*.*

Observação 24. *Ao contrário de um subconjunto $X' \subseteq X$, uma família $(x_i)_{i\in I}$ contém também a informação relativa à correspondência entre os índices i e os elementos x_i:*

- *É permitida a ocorrência repetida de um mesmo elemento (por exemplo, $x_i = x_j$ para $i \neq j$).*
- *A ordem ou, mais geralmente, os rótulos i são relevantes.*
- *A imagem $\varphi(I) = \{x_i \mid i \in I\}$ é um subconjunto de X, mas, em geral, ao se passar para esse simples subconjunto, perde-se a informação sobre a correspondência entre índices e elementos.*

Definição 25 (Função de escolha)**.** *Seja $\mathcal{C}$ um conjunto de conjuntos não vazios (por exemplo, $\mathcal{C} = \{X_i\}_{i\in I}$). Uma* função de escolha *é uma aplicação*

$$c : \mathcal{C} \longrightarrow \bigcup \mathcal{C}, \qquad C \mapsto c(C) \in C,$$

que associa a cada conjunto $C \in \mathcal{C}$ um elemento $c(C) \in C$.

Observação 26. *A questão de saber se existe uma função de escolha para toda família de conjuntos não vazios é precisamente o* axioma da escolha*. Esse axioma já foi mencionado na discussão sobre aplicações inversas e produtos e desempenha um papel fundamental em muitas áreas da matemática; contudo, para muitos fins práticos (em particular, em construções finitas), ele não é necessário.*

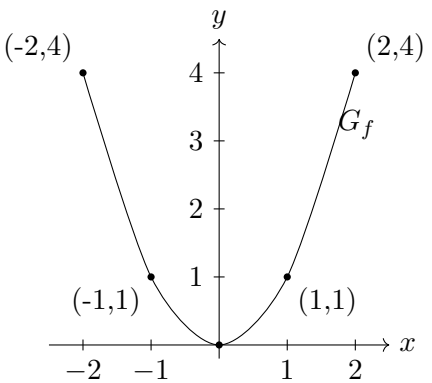
1.2.9 Gráficos e relações

Definição 27 (Gráfico de uma aplicação)**.** *Seja $f\colon X \to Y$ uma aplicação. O* gráfico *de f é o conjunto*

$$G_f := \{\, (x, f(x)) \in X \times Y \mid x \in X \,\} \subseteq X \times Y.$$

O gráfico G_f é, portanto, precisamente o conjunto de todos os pares ordenados que indicam qual elemento $y \in Y$ está associado a cada elemento $x \in X$. A aplicação f pode ser completamente descrita por seu gráfico, e, reciprocamente, o gráfico determina f.

Representação gráfica: Em geral, representa-se o gráfico G_f em um sistema de coordenadas, no qual cada par $(x, f(x))$ é marcado como um ponto no plano (x, y). Um exemplo simples e ilustrativo é dado por $f(x) = x^2$, considerando-se alguns valores de x. A figura a seguir apresenta uma representação esquemática desse tipo:



Projeção sobre a primeira componente: Considere a projeção

$$\pi_X\colon X \times Y \longrightarrow X, \qquad \pi_X(x, y) := x.$$

A restrição $\pi_X|_{G_f}\colon G_f \to X$ é bijetiva:

- *Sobrejetiva:* Para todo $x \in X$, tem-se $(x, f(x)) \in G_f$; logo, $\pi_X|_{G_f}$ assume todo valor $x \in X$.

- *Injetiva:* Se $\pi_X(x, f(x)) = \pi_X(x', f(x'))$, então $x = x'$. Como os pares pertencentes ao gráfico são univocamente determinados pela primeira componente, segue que $(x, f(x)) = (x', f(x'))$.

Intuitivamente, a projeção sobre X "ignora" a segunda componente; entretanto, quando restrita ao gráfico, ela estabelece uma correspondência biunívoca entre os pontos do gráfico e os elementos de X.

Unicidade da imagem / Teste da reta vertical: O gráfico G_f de uma aplicação nunca associa a um mesmo valor de x dois ou mais valores distintos de y. Formalmente, para cada $x \in X$, existe um único $y \in Y$ tal que $(x, y) \in G_f$. Geometricamente, isso significa que nenhuma reta vertical $x = \text{const}$ intersecta o gráfico em mais de um ponto (esse é o conhecido *teste da reta vertical*).

Definição 28 (Relação)**.** *Uma* relação *em um conjunto X é um subconjunto $R \subseteq X \times X$. Para $(x, y) \in R$, escreve-se frequentemente $x \sim_R y$, ou simplesmente $x \sim y$, e diz-se que "x está relacionado com y".*

Exemplos de relações: (Em cada caso, escolha adequadamente o conjunto X.)

1. A relação de ordem $\leq$ em $\mathbb{R}$: $(x, y) \in R$ se, e somente se, $x \leq y$.
2. A relação de divisibilidade $\mid$ em $\mathbb{N}$: $(a, b) \in R$ se, e somente se, $a \mid b$.
3. A relação "ter o mesmo comprimento" no conjunto de todas as palavras sobre um alfabeto: $(u, v) \in R$ se, e somente se, $|u| = |v|$.

1.2.10 Relações de equivalência

Definição 29 (Relação de equivalência)**.** *Uma relação $\sim$ sobre X é denominada* relação de equivalência *se, para todos $x, y, z \in X$, forem satisfeitas as seguintes propriedades:*

1. *(Reflexividade) $x \sim x$.*
2. *(Simetria) $x \sim y \Rightarrow y \sim x$.*
3. *(Transitividade) $x \sim y$ e $y \sim z \Rightarrow x \sim z$.*

Exemplos de relações de equivalência:

1. A igualdade $=$ em qualquer conjunto X.

2. A congruência módulo n em $\mathbb{Z}$: $a \equiv b \pmod{n}$ se, e somente se, $n \mid (a - b)$.

3. "Pertencer ao mesmo bloco de uma partição": se X estiver particionado em blocos (subconjuntos) dois a dois disjuntos, então dois elementos serão equivalentes quando pertencerem ao mesmo bloco.

1.2.11 Exercício

Seja $X = \{1, 2, 3, 4\}$. Para cada uma das relações a seguir sobre X, verifique se ela é uma relação de equivalência. Justifique sua resposta.

1. $R_1 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$.

2. $R_2 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,3)\}$.

3. $R_3 = \{(a,b) \in X \times X \mid a \equiv b \pmod{2}\}$ ("mesma paridade").

Solução-modelo:

1. *Verificação da reflexividade, da simetria e da transitividade:* Reflexividade: Todos os pares (x, x), com $x \in X$, pertencem a R_1. Logo, R_1 é reflexiva. Simetria: $(1, 2)$ pertence a R_1 e $(2, 1)$ também pertence a R_1; para os demais pares não diagonais, não há outra condição a verificar, pois existe apenas o par $1 \leftrightarrow 2$. Portanto, R_1 é simétrica. Transitividade: Consideremos as cadeias relevantes: de $1 \sim 2$ e $2 \sim 1$ segue $1 \sim 1$, que pertence à relação. Não há uma cadeia da forma $1 \sim 2$ e $2 \sim 3$, portanto não surge nenhuma condição adicional não satisfeita. Assim, R_1 é transitiva. $\Rightarrow$ R_1 é uma relação de equivalência; suas classes de equivalência são $\{1, 2\}$, $\{3\}$ e $\{4\}$.

2. Reflexividade: Sim, todos os pares (x, x) pertencem a R_2. Simetria: $(1, 2) \in R_2$, mas $(2, 1) \notin R_2$. Portanto, R_2 não é simétrica e, consequentemente, não é uma relação de equivalência. (Desse modo, não é necessário concluir a verificação das demais propriedades.)

3. *Mesma paridade (par ou ímpar):* Reflexividade: $a \equiv a \pmod 2$ para todo $a \in X$. Simetria: Se $a \equiv b \pmod 2$, então $b \equiv a \pmod 2$. Transitividade: Se $a \equiv b \pmod 2$ e $b \equiv c \pmod 2$, então $a \equiv c \pmod 2$. $\Rightarrow R_3$ é uma relação de equivalência. Suas duas classes de equivalência são $\{1, 3\}$ (números ímpares) e $\{2, 4\}$ (números pares).

1.2.12 Classes de equivalência

Uma vez definida uma relação de equivalência $\sim$ em um conjunto X, é possível agrupar elementos "equivalentes" e representá-los por um único objeto novo. Desse modo, abstraem-se diferenças irrelevantes.

Definição 30 (Classe de equivalência)**.** *Seja $\sim$ uma relação de equivalência em X. Para $a \in X$, define-se a* classe de equivalência *de a por $[a] := \{\, x \in X \mid x \sim a \,\}$. Um subconjunto $A \subseteq X$ é denominado* classe de equivalência *com respeito a $\sim$ se satisfaz as seguintes condições:*

1. *$A \neq \varnothing$,*

2. *para todos $x, y \in A$, vale $x \sim y$,*

3. *se $x \in A$ e $y \in X$ satisfazem $y \sim x$, então $y \in A$.*

Teorema 31. *As classes de equivalência formam uma partição de X: cada $a \in X$ pertence a exatamente uma classe de equivalência. Em particular, dadas duas classes de equivalência A, A', tem-se $A = A'$ ou $A \cap A' = \varnothing$.*

Demonstração. Fixado $a \in X$, seja $A := [a] = \{x \in X \mid x \sim a\}$. Como $\sim$ é reflexiva, $a \in A$, de modo que $A \neq \varnothing$. Se $x, y \in A$, então $x \sim a$ e $y \sim a$; pela simetria e pela transitividade, segue que $x \sim y$. Além disso, se $x \in A$ e $y \in X$ satisfazem $y \sim x$, então $x \sim a$ e, pela transitividade, $y \sim a$, isto é, $y \in A$. Portanto, A satisfaz as condições (2) e (3) da definição. Sejam agora A e A' duas classes de equivalência tais que $A \cap A' \neq \varnothing$. Escolha $z \in A \cap A'$. Para todo $x \in A$, vale $x \sim z$, pois $z \in A$; como $z \in A'$, a condição (3) implica $x \in A'$. Logo, $A \subseteq A'$. Trocando-se os papéis de A e A', obtém-se $A' \subseteq A$, e, portanto, $A = A'$. Assim, duas classes de equivalência distintas são disjuntas. Como cada $a \in X$ pertence à classe $[a]$, conclui-se que pertence a exatamente uma classe de equivalência. □

Definição 32 (Conjunto quociente e projeção canônica)**.** *O conjunto das classes de equivalência é denominado* conjunto quociente *e denotado por* $X/\sim$ *ou* X/R. *A aplicação* $\pi\colon X \longrightarrow X/\sim, \qquad \pi(a) := [a]$ *é denominada* projeção canônica *(ou aplicação quociente). Ela é sobrejetiva, e as pré-imagens de seus valores são precisamente as classes de equivalência:* $\pi^{-1}([a]) = [a]$. *Cada elemento* $a \in [a]$ *é denominado* representante *da classe* $[a]$.

Exemplo 33 (Congruência módulo n)**.** *Em* $\mathbb{Z}$, *para um* $n \in \mathbb{N}_{\geq 1}$ *fixo, define-se a relação*

$$a \equiv b \pmod{n} \quad :\Longleftrightarrow \quad n \mid (a-b).$$

Essa é uma relação de equivalência. O conjunto quociente $\mathbb{Z}/n\mathbb{Z}$ *é constituído pelas* n *classes*

$$[0], [1], \ldots, [n-1],$$

sendo, por exemplo, $[1] = \{\ldots, -2, 1, 4, 7, \ldots\}$ *quando* $n = 3$. *Essas classes constituem exemplos típicos de classes de equivalência; cada elemento de uma classe é um de seus representantes.*

1.3 Exercícios e soluções

Os exercícios a seguir abrangem os conceitos introduzidos até aqui: conjuntos e operações entre conjuntos, aplicações (injetividade, sobrejetividade e bijetividade), composição, gráficos, relações, relações de equivalência, classes de equivalência e conjuntos quocientes. As soluções propostas são apresentadas de forma concisa; como exercício, recomenda-se que os estudantes desenvolvam integralmente as demonstrações.

Exercício 1 (Operações fundamentais): Sejam

$$A = \{1, 2, 3\}, \qquad B = \{2, 3, 4\}, \qquad C = \{3, 4, 5\}.$$

Determine:

$$A \cup B, \quad A \cap B, \quad (A \cup B) \cap C, \quad A \setminus C.$$

Solução proposta 1: $A \cup B = \{1, 2, 3, 4\}$. $A \cap B = \{2, 3\}$. $(A \cup B) \cap C = \{1, 2, 3, 4\} \cap \{3, 4, 5\} = \{3, 4\}$. $A \setminus C = \{1, 2, 3\} \setminus \{3, 4, 5\} = \{1, 2\}$.

Exercício 2 (Famílias indexadas de conjuntos): Para $I = \mathbb{N} = \{0, 1, 2, \dots\}$ e $X_i = [-i, i] \subset \mathbb{R}$, com $i \in I$, calcule

$$\bigcup_{i \in I} X_i, \qquad \bigcap_{i \in I} X_i.$$

Solução proposta 2: Para todo $x \in \mathbb{R}$, existe $i \in I$ tal que $|x| \leq i$; portanto, $\bigcup_{i \in I} X_i = \mathbb{R}$. Como $X_0 = [0, 0] = \{0\}$ e $X_0 \subseteq X_i$ para todo $i \in I$, segue que $\bigcap_{i \in I} X_i = \{0\}$.

Exercício 3 (Propriedades de uma aplicação): Considere $f\colon \{1, 2, 3\} \to \{a, b\}$, definida por $f(1) = a,\ f(2) = a,\ f(3) = b$. A aplicação f é injetiva? Sobrejetiva? Bijetiva?

Solução proposta 3: A aplicação f *não* é injetiva, pois $f(1) = f(2) = a$, embora $1 \neq 2$. A aplicação f é *sobrejetiva*, pois $f(\{1, 2, 3\}) = \{a, b\}$, que coincide com o contradomínio. Como não é injetiva, f também não é bijetiva.

Exercício 4 (Composição e aplicação identidade): Dê um exemplo concreto de conjuntos X, Y e de aplicações $f\colon X \to Y,\ g\colon Y \to X$ tais que $g \circ f = \mathrm{id}_X$, mas $f \circ g \neq \mathrm{id}_Y$. O que a igualdade $g \circ f = \mathrm{id}_X$ permite concluir sobre f (injetividade/sobrejetividade)?

Solução proposta 4: Considere $X = \{1, 2\}$ e $Y = \{a, b, c\}$. Defina $f(1) = a,\ f(2) = b$ e escolha $g(a) = 1,\ g(b) = 2,\ g(c) = 1$. Então, $g \circ f = \mathrm{id}_X$, pois $g(f(1)) = g(a) = 1$, e analogamente para o outro elemento de X. Entretanto, $f \circ g$ envia c em $f(1) = a$; portanto, $f \circ g \neq \mathrm{id}_Y$. Da igualdade $g \circ f = \mathrm{id}_X$, segue que f é injetiva (pois possui uma inversa à esquerda) e que g é sobrejetiva (pois possui uma inversa à direita).

Exercício 5 (Imagens, interseções e uniões): Demonstre que:

$$f\left(\bigcup_{i \in I} M_i\right) = \bigcup_{i \in I} f(M_i), \qquad f\left(\bigcap_{i \in I} M_i\right) \subseteq \bigcap_{i \in I} f(M_i).$$

Solução proposta 5: Primeira igualdade: seja $y \in f(\bigcup_i M_i)$. Então, existe $x \in \bigcup_i M_i$ tal que $y = f(x)$. Logo, existe algum i para o qual $x \in M_i$; assim, $y \in f(M_i) \subseteq \bigcup_i f(M_i)$. Reciprocamente, se $y \in \bigcup_i f(M_i)$, então existem i e $x \in M_i$ tais que $y = f(x)$. Portanto, $x \in \bigcup_i M_i$ e $y \in f(\bigcup_i M_i)$. Segunda inclusão: seja

$y \in f(\bigcap_i M_i)$. Então, existe $x \in \bigcap_i M_i$ tal que $y = f(x)$. Como $x \in M_i$ para todo i, tem-se $y \in f(M_i)$ para todo i; logo, $y \in \bigcap_i f(M_i)$. (A inclusão inversa pode ser falsa em geral, por exemplo, quando f não é injetiva.)

Exercício 6 (Preimagens e operações com conjuntos): Mostre que:

$$f^{-1}\left(\bigcup_{j\in J} N_j\right) = \bigcup_{j\in J} f^{-1}(N_j),$$
$$f^{-1}\left(\bigcap_{j\in J} N_j\right) = \bigcap_{j\in J} f^{-1}(N_j).$$

Solução proposta 6: As duas inclusões que compõem cada igualdade decorrem diretamente da definição $f^{-1}(N) = \{x \mid f(x) \in N\}$ e das relações lógicas entre os quantificadores $\exists$, $\forall$ e os conectivos $\vee$, $\wedge$. (Formalmente, $f(x) \in \bigcup_j N_j \Leftrightarrow \exists j : f(x) \in N_j \Leftrightarrow \exists j : x \in f^{-1}(N_j)$. Para a interseção, procede-se de modo análogo, utilizando $\forall$.)

Exercício 7 (Gráfico de uma aplicação): Seja $f\colon X \to Y$ uma aplicação. Mostre que, para cada $x \in X$, existe exatamente um par $(x, y) \in G_f$. A partir desse fato, explique o teste da reta vertical.

Solução proposta 7. Por definição, $G_f = \{(x, f(x)) \mid x \in X\}$. Para cada x fixado, existe o par $(x, f(x))$ e, pela unicidade de $f(x)$, não pode haver no gráfico outro par (x, y') com $y' \neq f(x)$. Geometricamente, isso significa que a cada x corresponde no máximo um y (e, pela definição de aplicação, exatamente um); portanto, nenhuma reta vertical intersecta o gráfico em mais de um ponto.

Exercício 8 (Relações e relações de equivalência): Para $X = \{1, 2, 3, 4\}$, verifique se as relações a seguir são relações de equivalência:

1. $R_1 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$.
2. $R_2 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,3)\}$.

Solução proposta 8: R_1: a reflexividade é satisfeita. Quanto à simetria, tanto $(1,2)$ quanto $(2,1)$ pertencem à relação; logo, ela é simétrica. A transitividade é verificada mediante a análise dos casos não triviais (por exemplo, de $1 \sim 2$ e $2 \sim 1$ resulta $1 \sim 1$, que pertence à relação). Portanto, R_1 é uma relação de equivalência,

cujas classes são $\{1,2\}$, $\{3\}$ e $\{4\}$. R_2: a reflexividade é satisfeita, mas a simetria não, pois $(1,2) \in R_2$, enquanto $(2,1) \notin R_2$. Portanto, R_2 não é uma relação de equivalência.

Exercício 9 (Classes de equivalência e conjunto quociente): Em $\mathbb{Z}$, defina $a \sim b$ se, e somente se, $a \equiv b \pmod 4$. Determine as classes de equivalência e o conjunto quociente $\mathbb{Z}/4\mathbb{Z}$. Indique três sistemas distintos de representantes.

Solução proposta 9. As classes de equivalência são $[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$, $[1]$, $[2]$ e $[3]$. Portanto, $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$. Três possíveis sistemas de representantes são $\{0,1,2,3\}$, $\{4,5,6,7\}$ e $\{0,-3,-2,-1\}$.

Exercício 10 (Conjuntos finitos e princípio da casa dos pombos): Seja X um conjunto finito com $|X| = n$, e seja $f\colon X \to X$. Mostre que f injetiva $\implies$ f sobrejetiva. (Sugestão: princípio da casa dos pombos, também conhecido como princípio das gavetas ou princípio de Dirichlet.)

Solução proposta 10. Se f é injetiva, então as n imagens $f(x)$, com $x \in X$, são duas a duas distintas; logo, $f(X)$ possui n elementos. Como $f(X) \subseteq X$ e X possui apenas n elementos, segue que $f(X) = X$. Portanto, f é sobrejetiva. Em termos do princípio da casa dos pombos: se n objetos são distribuídos em n compartimentos sem que dois objetos ocupem o mesmo compartimento, então todos os compartimentos estão ocupados.

Exercício 11 (Axioma da escolha): Seja $(X_i)_{i \in I}$ uma família de conjuntos não vazios. Formule, em palavras, a questão respondida pelo axioma da escolha e indique se esse problema ocorre quando I é finito.

Solução proposta 11. A questão é: *existe sempre uma aplicação* $c\colon I \to \bigcup_{i \in I} X_i$ *tal que* $c(i) \in X_i$ *para todo* $i \in I$*?* Isso equivale precisamente à existência de uma função de escolha. Quando o conjunto de índices I é finito, sempre se pode construir tal função, escolhendo-se um elemento de cada X_i. A questão surge para famílias infinitas e, em sua forma geral, é resolvida pelo axioma da escolha; em modelos da teoria dos conjuntos nos quais esse axioma não é assumido, tal função nem sempre precisa existir.

Observação 34. *Esta coletânea pode ser utilizada como lista de exercícios em uma disciplina ou em aulas de tutoria. Os exercícios 1–4 têm caráter mais diretamente computacional ou conceitual; os exercícios 5–7 concentram-se em técnicas de demonstração; e os exercícios 8–11 combinam a compreensão conceitual com observações mais aprofundadas sobre quocientes e o axioma da escolha. Para trabalhos extraclasse,*

recomenda-se uma combinação de problemas simples e de dificuldade intermediária; em avaliações, podem ser utilizadas, por exemplo, variantes dos exercícios 3, 4, 5 e 10.

Capítulo 2

Grupos

2.1 Operação binária / composição

Definição 35. *Uma* operação *(ou* composição*,* operação binária*) sobre um conjunto G é uma aplicação*

$$* : G \times G \longrightarrow G, \qquad (a, b) \mapsto a * b,$$

que associa a cada par ordenado $(a, b) \in G \times G$ um elemento bem determinado $a * b \in G$.

Observações importantes:

- A condição $* : G \times G \to G$ é denominada *fechamento*: o resultado da operação entre dois elementos de G deve pertencer novamente a G.

- Para representar operações, utilizam-se frequentemente notações infixas concisas, como $a * b$, ab, ou símbolos usuais, como $a + b$ e $a \cdot b$. Dependendo do contexto, também se escrevem $a \circ b$ ou $a \circledast b$.

- Algumas propriedades das operações que serão importantes posteriormente na teoria dos grupos são, por exemplo, a *associatividade*, $(a * b) * c = a * (b * c)$, a existência de um *elemento neutro* e a existência de *elementos inversos*. Essas propriedades conduzem à definição de grupo, apresentada na próxima seção.

Exemplos de operações binárias:

1. *Adição* no conjunto dos números inteiros:

$$+ \ : \ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad (a, b) \mapsto a + b.$$

Essa operação é fechada, associativa e comutativa.

2. *Multiplicação* no conjunto dos números reais:

$$\cdot \ : \ \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad (a, b) \mapsto a \cdot b.$$

Também nesse caso, a operação é fechada e associativa; além disso, a multiplicação de números reais é comutativa.

3. *Multiplicação de matrizes* em $M_n(\mathbb{R})$ (o conjunto de todas as matrizes $n \times n$ com entradas reais):

$$* \ : \ M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R}), \qquad (A, B) \mapsto A \cdot B.$$

A operação é fechada e associativa, mas, em geral, *não é* comutativa. Esse é um exemplo importante de estrutura não comutativa.

4. *Composição de aplicações* de um conjunto X em si mesmo:

$$\begin{aligned} \circ \ : \ \mathrm{Abb}(X, X) \times \mathrm{Abb}(X, X) &\longrightarrow \mathrm{Abb}(X, X), \\ (f, g) &\longmapsto f \circ g. \end{aligned}$$

Essa operação é fechada e associativa, mas, em geral, não é comutativa.

5. *Concatenação de palavras* sobre um alfabeto A: em A^* (o conjunto de todas as palavras finitas), define-se

$$\cdot \ : \ A^* \times A^* \to A^*, \qquad (u, v) \mapsto uv$$

pela justaposição das palavras. Essa operação é fechada e associativa.

6. *Ou exclusivo* em $\{0, 1\}$:

$$\oplus \ : \ \{0,1\} \times \{0,1\} \to \{0,1\}, \qquad (a, b) \mapsto a \oplus b$$

com $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$. Essa operação é fechada, associativa e comutativa.

7. *Subtração* no conjunto dos números inteiros:

$$- \ : \ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad (a, b) \mapsto a - b.$$

Essa operação é fechada em $\mathbb{Z}$, mas *não é* associativa; portanto, não constitui um exemplo adequado para muitas estruturas algébricas que exigem associatividade. (Em $\mathbb{N}$, além disso, a subtração não é fechada.)

Observações:

- Ao estudar uma nova operação, deve-se verificar sistematicamente: *(i)* A operação é fechada? *(ii)* É associativa? *(iii)* Existe um elemento neutro? *(iv)* Os elementos possuem inversos? *(v)* A operação é comutativa? Essas verificações preparam para a definição formal de grupo.
- Apresentamos tanto exemplos simples e comutativos quanto exemplos não comutativos; estes últimos ajudam a evitar intuições equivocadas.
- Convém empregar uma notação consistente: na teoria dos grupos, frequentemente se adota uma única forma de escrita (por exemplo, ab em vez de $a * b$), a fim de tornar as fórmulas mais claras.

2.2 Definição

Grupos são conjuntos munidos de uma operação que satisfaz determinadas propriedades fundamentais. Apresentamos inicialmente uma definição precisa.

Definição 36 (Grupo)**.** *Sejam G um conjunto e $*\colon G \times G \to G$ uma operação. O par $(G, *)$ é denominado* grupo *se os seguintes axiomas forem satisfeitos:*

1. ***Fechamento:*** *Para todos $a, b \in G$, tem-se $a * b \in G$.*
2. ***Associatividade:*** *Para todos $a, b, c \in G$, tem-se*

$$(a * b) * c \ = \ a * (b * c).$$

3. ***Existência de um elemento neutro:*** *Existe um elemento $e \in G$, denominado* elemento neutro*, tal que, para todo $a \in G$, $e * a = a = a * e$.*

4. ***Existência de inversos:*** *Para cada $a \in G$, existe um elemento $a^{-1} \in G$, denominado* inverso *de a, tal que $a * a^{-1} = e = a^{-1} * a$.*

Se, adicionalmente, $a * b = b * a$ para todos $a, b \in G$, o grupo é denominado abeliano *(ou* comutativo*).*

Explicações e observações:

- Às vezes, o símbolo da operação é omitido e escreve-se ab em vez de $a * b$; nesse caso, utiliza-se a notação multiplicativa. Na notação *aditiva*, escreve-se $a + b$, o elemento neutro é denotado por 0 e o inverso de a é chamado de oposto de a e denotado por $-a$. Para grupos cuja operação é naturalmente comutativa, como $(\mathbb{Z}, +)$, é usual empregar a notação aditiva.
- O fechamento foi exigido explicitamente, pois a operação deve produzir um resultado que pertença ao próprio conjunto.
- Diversas consequências importantes podem ser deduzidas diretamente dos axiomas, como a unicidade do elemento neutro e dos inversos, as leis de cancelamento e a regra do inverso $(ab)^{-1} = b^{-1}a^{-1}$. É fundamental exercitar a demonstração desses resultados.

Demonstrações breves de consequências fundamentais:

Proposição 37 (Unicidade do elemento neutro e do elemento inverso)**.** *Em um grupo $(G, *)$, o elemento neutro é único e, para cada $a \in G$, o elemento inverso a^{-1} também é único.*

Demonstração. Sejam e, e' dois elementos neutros. Então, $e = e * e' = e'$. Logo, $e = e'$. Sejam b, b' dois elementos inversos de a. Então, $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$. Logo, $b = b'$. □

Proposição 38 (Regra do inverso e leis de cancelamento)**.** *Em um grupo, para quaisquer $a, b \in G$, vale $(ab)^{-1} = b^{-1}a^{-1}$. Além disso, valem as leis de cancelamento: de $ax = ay$ segue $x = y$, e de $xa = ya$ segue $x = y$.*

Demonstração. Multiplicando ab por $b^{-1}a^{-1}$, obtemos $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. De modo análogo, demonstra-se que $(b^{-1}a^{-1})(ab) = e$. Portanto, $b^{-1}a^{-1}$ é o inverso de ab. Quanto ao cancelamento, de $ax = ay$, multiplicando ambos os membros à esquerda por a^{-1}, segue que $x = y$. A lei de cancelamento à direita é demonstrada de maneira análoga. □

2.3 Convenções

- *Escolha da notação:* Na prática, emprega-se, conforme o contexto:
  - Notação multiplicativa: produto ab, elemento neutro e e inverso a^{-1}.
  - Notação aditiva: soma $a + b$, elemento neutro 0 e inverso aditivo $-a$.

  Uma vez fixada uma convenção, deve-se mantê-la de forma consistente ao longo de cada seção.

- *Omissão de parênteses:* Em virtude da associatividade, podem-se omitir os parênteses em produtos com vários fatores, como $a * b * c * d$, pois seu significado é inequívoco.

- *Intuição multiplicativa e aditiva:* Muitas demonstrações podem ser formuladas em ambas as notações; deve-se escolher aquela mais adequada à aplicação considerada (por exemplo, a notação aditiva para espaços vetoriais).

2.4 Exemplos de grupos e de estruturas que não são grupos

Exemplos de grupos

1. $(\mathbb{Z}, +)$: o conjunto dos números inteiros com a adição (grupo abeliano).

2. $(\mathbb{Q}^\times, \cdot)$: o conjunto dos números racionais não nulos com a multiplicação (grupo abeliano).

3. $(\mathbb{R}^\times, \cdot)$ e $(\mathbb{C}^\times, \cdot)$: os conjuntos dos números reais e complexos não nulos, respectivamente, com a multiplicação (grupos abelianos).

4. O grupo linear geral $GL(n, \mathbb{R})$: o conjunto das matrizes invertíveis de ordem n com a multiplicação de matrizes (em geral, não abeliano).

5. O grupo simétrico S_n: o conjunto das permutações de um conjunto com n elementos, munido da composição (não abeliano para $n \geq 3$).

6. O grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, formado pelas classes de congruência módulo n, com a adição módulo n (grupo abeliano finito).