Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação

SMA0341 e SLC0603 - Elementos de Matemática

Notas de Aulas

Ires Dias
Sandra Maria Semensato de Godoy

São Carlos
2012

Sumário

1 Noções de Lógica ***7***

1.1 Proposições e Conectivos Lógicos 7
1.2 Proposições Compostas e Tabelas-verdade 9
1.3 Tautologia e Equivalência Lógica 12
1.4 Teoremas 15
1.5 Definição de $\Longrightarrow$ e $\Longleftrightarrow$ 15
1.6 Quantificadores 18
1.7 Método Dedutivo 21
1.8 Métodos de Demonstração 22
1.9 Exercícios 24

2 Teoria dos Conjuntos ***27***

2.1 Noções Primitivas, Definições e Axiomas 27
2.2 Operações com Conjuntos 34
2.3 O Produto Cartesiano de Dois Conjuntos 40
2.4 Exercícios 42

3 Relações ***45***

3.1 Definições e Exemplos 45
3.2 Relações de Equivalências e Partições 49
3.3 Relações de Ordem 53
3.4 Funções 57
3.5 Exercícios 57

4 Noções de Cardinalidade **63**

4.1 Conjuntos Equipotentes, Enumeráveis e Contáveis 63
4.2 Números Cardinais e a Hipótese do Contínuo 68
4.3 Cardinal de um conjunto - Teorema de Cantor 70
4.4 Aritmética Cardinal 71
4.4.1 Adição de Números Cardinais. 71
4.4.2 Multiplicação de Números Cardinais 72
4.4.3 Potências de Números Cardinais 73
4.5 Exercícios 75

5 Os Números Naturais **79**

5.1 Os Axiomas de Peano 79
5.2 Adição em $\mathbb{N}$ 81
5.3 Multiplicação em $\mathbb{N}$ 83
5.4 Relação de Ordem em $\mathbb{N}$ 85
5.5 Exercícios 89

6 Os Números Inteiros **91**

6.1 A adição em $\mathbb{Z}$ 92
6.2 A multiplicação em $\mathbb{Z}$ 94
6.3 Relação de Ordem em $\mathbb{Z}$ 96
6.4 A Imersão de $\mathbb{N}$ em $\mathbb{Z}$ 97
6.5 Valor Absoluto 98
6.6 Aritmética em $\mathbb{Z}$ 100
6.6.1 Múltiplos e Divisores 100
6.6.2 Algoritmo da divisão ou algoritmo de Euclides 101
6.6.3 Máximo Divisor Comum 102
6.6.4 Mínimo Múltiplo Comum 108
6.7 Números Primos 110
6.8 Congruências e Aplicações 112
6.8.1 Critérios de Divisibilidade 115

6.8.2 A validade de um número de CPF 118
6.8.3 Em que dia da semana você nasceu? 119
6.9 Exercícios 121

7 Números Racionais ***125***

7.1 A adição em $\mathbb{Q}$ 126
7.2 A Multiplicação em $\mathbb{Q}$ 128
7.3 Relação de Ordem em $\mathbb{Q}$ 129
7.4 A imersão de $\mathbb{Z}$ em $\mathbb{Q}$ 131
7.5 Exercícios 132

Referências Bibliográficas ***135***

1
Noções de Lógica

"Lógica é a higiene usada pelos matemáticos para conservar suas idéias saudáveis e fortes". Herman Weyl (1885-1955)

1.1 Proposições e Conectivos Lógicos

O estudo da lógica é o estudo dos princípios e métodos utilizados para distinguir argumentos válidos daqueles que não são válidos.

O principal objetivo desta seção é ajudar o aluno a entender os princípios e métodos usados em cada etapa de uma demonstração. Sem alguns conceitos lógicos básicos, é impossível escrever e/ou entender uma demonstração. Quando demonstramos um teorema, estamos demonstrando a veracidade de certas declarações. Em geral estas declarações são compostas de *proposições, quantificadores, conectivos* e/ou *modificadores*.

O ponto inicial da lógica é o termo "proposição" usado em um *sentido técnico*. Por uma **proposição** entendemos uma sentença declarativa (afirmativa) ou uma afirmação verbal que é verdadeira ou falsa, mas não ambas simultaneamente. A designação *Verdadeira* **(V)** ou *Falsa* **(F)** de uma proposição é dita ser seu **valor verdade** ou seu **valor lógico**.

Exemplo 1.1. As seguintes afirmações são proposições:

(a) $(e^{\pi})^2 = e^{2\pi}$.

(b) 6 é um número primo.

(c) Pedro tem olhos azuis.

(d) O dia 10 de agosto de 1935 foi uma quarta-feira.

(e) O 1000º digito da expansão decimal de $\sqrt{2}$ é 6.

(f) Existe vida inteligente em Marte.

Note que (a) é claramente V; (b) é claramente F; (c) é uma proposição pois é V ou F, mesmo que eu não conheça o Pedro; (d) é V ou F, mesmo que seja difícil saber a resposta; o mesmo vale para (e) e (f).

Exemplo 1.2. As seguintes afirmações **não** são proposições:

(a) $(e^{\pi})^2$ é igual à $e^{2\pi}$?

(b) AH! se eu passar em Elementos!

(c) $x > 3$.

(d) $2 + 3i$ é menor que $5 + 3i$.

(e) $x(x + 4) = x^2 + 4x$.

(f) Esta proposição é falsa.

(g) Hoje é terça-feira.

(h) Está chovendo.

Note que (a) é interrogativa e não declarativa; (b) é exclamativa e não declarativa; (c) é uma sentença aberta, pode ser V ou F dependendo da variável x; (d) não é V ou F, pois não existe ordem em $\mathbb{C}$; (e) não é uma proposição, o que seria proposição é "para todo $x \in \mathbb{R}$, $x(x + 4) = x^2 + 4x$"; (f) é um paradoxo, viola a definição de proposição pois é V e F ao mesmo tempo; (g) é uma sentença aberta que depende da variável "hoje" assim como (h) depende da variável "tempo".

1.2 Proposições Compostas e Tabelas-verdade

As proposições do exemplo 1.1 são todas proposições simples, ou seja, não foram obtidas por combinações ou composições de outras proposições. A combinação ou conecção de duas ou mais proposições simples é uma **proposição composta**. Há várias maneiras de conectar proposições, somente cinco são freqüentemente usadas. São os **conectivos**:

(a) "não", simbolizado por $\sim$, também chamado de modificador.

(b) "e", simbolizado por $\wedge$ (operação de conjunção).

(c) "ou", simbolizado por $\vee$ (operação de disjunção).

(d) "se $\cdots$ então $\cdots$", simbolizado por $\longrightarrow$ (conectivo condicional).

(e) "$\cdots$ se, e somente se $\cdots$", simbolizado por $\longleftrightarrow$ (conectivo bicondicional).

Como em álgebra usamos letras para representar números, em lógica usaremos letras minúsculas para representar proposições.

Definição 1.3. Para proposições p e q, definimos:

(a) A **negação de** p, denotada por $\sim p$, lida "não p", como sendo a proposição com valor verdade diferente do de p.

(b) A **conjunção de** p **e** q, denotada por $p \wedge q$, lida "p e q", como sendo a proposição que é verdadeira somente quando p e q são ambas verdadeiras.

(c) A **disjunção de** p **e** q, denotada por $p \vee q$, lida "p ou q", como sendo a proposição que é falsa somente quando p e q são ambas falsas.

(d) A **condicional de** p **e** q, denotada por $p \longrightarrow q$, lida "se p, então q" ou "p implica q" ou "p condiciona q" ou "p é condição suficiente para q", como sendo a proposição que assume o valor falso somente quando p for verdadeira e q for falsa.

(e) A **bicondicional de** p **e** q, denotada por $p \longleftrightarrow q$, lida "p se, e somente se q" ou "p bicondiciona q" ou "p é condição necessária e suficiente para q", como sendo a proposição que assume o valor verdadeiro somente quando p e q são ambas verdadeiras ou p e q são ambas falsas.

Exemplo 1.4. "Maria tem uma caneta": é uma proposição p. "O sol é uma estrela": é uma proposição q.

Podemos formar as novas proposições:

- Maria tem uma caneta e o sol é uma estrela. $(p \wedge q)$
- Maria tem uma caneta ou o sol é uma estrela. $(p \vee q)$
- Se Maria tem uma caneta, então o sol é uma estrela. $(p \longrightarrow q)$
- Maria tem uma caneta se, e somente se o sol é uma estrela. $(p \longleftrightarrow q)$
- Não é verdade que Maria tem uma caneta. $(\sim p)$
- O sol não é uma estrela. $(\sim q)$

Observação 1.5. As definições são condições necessárias e suficientes e, portanto, são equivalentes a condições que têm o conectivo "se, e somente se" .

Para expressarmos os valores lógicos de uma proposição composta é muito conveniente utilizarmos uma tabela, chamada **tabela-verdade** da proposição, onde cada linha expressa os valores-verdade da composta, obtidos a partir dos valores-verdade das proposições dadas e dos conectivos usados. Vejamos as tabelas-verdade das proposições definidas acima:

p	$\sim p$
V	F
F	V

(a) $\sim p$

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

(b) $p \wedge q$

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

(c) $p \vee q$

p	q	$p \longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

(d) $p \longrightarrow q$

p	q	$p \longleftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

(e) $p \longleftrightarrow q$

Tabela 1.1: Tabelas-verdade da definição 1.3.

A partir destas cinco tabelas-verdade, podemos construir uma tabela-verdade para qualquer proposição composta. Através de exemplos apresentaremos duas maneiras de fazermos isso.

Exemplo 1.6. Construa a tabela-verdade para a proposição $\sim [(\sim p) \wedge (\sim q)]$.

p	q	$\sim p$	$\sim q$	$(\sim p) \wedge (\sim q)$	$\sim [(\sim p) \wedge (\sim q)]$
V	V	F	F	F	V
V	F	F	V	F	V
F	V	V	F	F	V
F	F	V	V	V	F

Tabela 1.2: Construção da tabela-verdade do exemplo 1.6.

Esta tabela representa como chegar na proposição $\sim [(\sim p) \wedge (\sim q)]$ passo a passo. Na realidade a tabela-verdade desta proposição é:

p	q	$\sim [(\sim p) \wedge (\sim q)]$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela 1.3: Tabela-verdade do exemplo 1.6.

Vale observar que:

1. O conectivo $\sim$ abrange somente a primeira expressão que o segue, exceto quando se utiliza parênteses e/ou colchetes

$$\sim p \wedge q \neq \sim (p \wedge q) \qquad\qquad \sim p \wedge q = (\sim p) \wedge q.$$

2. Os conectivos $\longrightarrow$ e $\longleftrightarrow$ abrangem toda a expressão que não contenha o mesmo sinal

$$\sim p \wedge q \longrightarrow p \vee \sim q \quad \text{significa} \quad [(\sim p) \wedge q] \longrightarrow [p \vee (\sim q)].$$

3. O número de linhas de uma tabela-verdade de uma proposição é dado por 2^n, onde n é o número de proposições simples que a compõem.

Exemplo 1.7. Determine se a proposição seguinte é verdadeira:
"Ou $\int_{-\pi}^{\pi} \operatorname{sen} x\,dx \neq 0$ *e* $\frac{d}{dx}(2^x) = x2^{x-1}$ *ou* $\int_{-\pi}^{\pi} \operatorname{sen} x\,dx = 0$ *e* $\ln 6 = (\ln 2)(\ln 3)$*".*

Sejam p a proposição $\int_{-\pi}^{\pi} \operatorname{sen} x\,dx = 0$, q a proposição $\frac{d}{dx}(2^x) = x2^{x-1}$ e $r : \ln 6 = (\ln 2)(\ln 3)$.

Como o conectivo principal é "ou $\cdots$ ou $\cdots$", temos que a proposição dada é $(\sim p \wedge q) \vee (p \wedge r)$. Vamos então construir a tabela-verdade desta proposição. Para tanto, notamos que, neste caso, temos 3 proposições simples p, q e r. Logo, nossa tabela terá $2^3 = 8$ linhas.

p	q	r	$\sim p$	$\sim p \wedge q$	$p \wedge r$	$(\sim p \wedge q) \vee (p \wedge r)$
V	V	V	F	F	V	V
V	V	F	F	F	F	F
V	F	V	F	F	V	V
V	F	F	F	F	F	**F**
F	V	V	V	V	F	V
F	V	F	V	V	F	V
F	F	V	V	F	F	F
F	F	F	V	F	F	F

Tabela 1.4: Tabela-verdade do exemplo 1.7.

Note que p é V pois $\int_{-\pi}^{\pi} \operatorname{sen} x\,dx = 0$, desde que seno é uma função ímpar; q é F pois $\frac{d}{dx}(2^x) = 2^x \ln 2 \neq x2^{x-1}$; r é F pois $\ln 6 = \ln 2 + \ln 3 \neq (\ln 2)(\ln 3)$. Conseqüentemente, p, q e r satisfazem as condições da linha 4 da tabela e, assim, a proposição dada é **Falsa**.

1.3 Tautologia e Equivalência Lógica

Definição 1.8. Uma proposição que é verdadeira em todas as possibilidades lógicas é dita ser uma **tautologia**. Se ela for falsa para todas as possibilidades lógicas, ela é dita ser uma **contradição**.

Note que se p é uma tautologia, então $\sim p$ é uma contradição e vice-versa.

Exemplo 1.9. Para toda proposição p, a proposição $p \vee \sim p$ é uma tautologia e $p \wedge \sim p$ é uma contradição.

De fato, basta observar sua tabela-verdade.

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
V	F	**V**	**F**
F	V	**V**	**F**

Tabela 1.5: Tabela-verdade do exemplo 1.9.

Definição 1.10. Duas proposições são ditas **logicamente equivalentes** se elas tiverem a mesma tabela-verdade, ou seja, se elas têm o mesmo valor verdade para cada uma das possibilidade lógicas.

Exemplo 1.11. As proposições $\sim (p \vee q)$ e $\sim p \wedge \sim q$ são logicamente equivalentes.

De fato, basta verificar na tabela-verdade:

p	q	$p \vee q$	$\sim (p \vee q)$	$\sim p$	$\sim q$	$\sim p \wedge \sim q$
V	V	V	**F**	F	F	**F**
V	F	V	**F**	F	V	**F**
F	V	V	**F**	V	F	**F**
F	F	F	**V**	V	V	**V**

Tabela 1.6: Tabela-verdade do exemplo 1.11.

O que significa a equivalência lógica deste exemplo? Por exemplo, se uma pessoa afirmar que:

$$\lim_{x \to 0} x^2 \neq 0 \qquad \text{e} \qquad \int_0^1 e^x \, dx \neq e$$

e outra pessoa afirmar que:

$$\text{Não é verdade que ou } \lim_{x \to 0} x^2 = 0 \text{ ou } \int_0^1 e^x \, dx = e,$$

temos que as duas pessoas estarão dizendo a mesma coisa, ou seja, ambas estarão certas ou ambas estarão erradas. Neste caso, como $\lim_{x \to 0} x^2 = 0$ e $\int_0^1 e^x \, dx \neq e$, temos que ambas estarão erradas (basta ver a linha 2 da tabela anterior).

Note que se duas proposições p e q são logicamente equivalentes, então $p \longleftrightarrow q$ é uma tautologia e, reciprocamente, se $p \longleftrightarrow q$ for uma tautologia, então p e q serão logicamente equivalentes.

Em Matemática, a principal importância das equivalências lógicas está na idéia que duas proposições logicamente equivalentes podem ser vistas como a "mesma" do ponto de vista lógico. Por exemplo, se duas proposições p e q são logicamente equivalentes e, necessitamos demonstrar p e encontramos uma maneira mais simples ou mais fácil de demonstrarmos q, então podemos demonstrar p provando q.

Exemplo 1.12. A proposição $p \longrightarrow q$ é logicamente equivalente a $\sim q \longrightarrow \sim p$ mas não é logicamente equivalente a $\sim p \longrightarrow \sim q$.

De fato, basta observar a tabela-verdade:

p	q	$p \longrightarrow q$	$\sim p$	$\sim q$	$\sim q \longrightarrow \sim p$	$\sim p \longrightarrow \sim q$
V	V	**V**	F	F	**V**	**V**
V	F	**F**	F	V	**F**	**V**
F	V	**V**	V	F	**V**	**F**
F	F	**V**	V	V	**V**	**V**

Tabela 1.7: Tabela-verdade do exemplo 1.12.

Mais ainda, a proposição $p \longrightarrow q$ é logicamente equivalente a $\sim (p \wedge \sim q)$ que é logicamente equivalente a $\sim p \vee q$, como mostra a tabela abaixo:

p	q	$p \longrightarrow q$	$\sim p$	$\sim q$	$\sim (p \wedge \sim q)$	$\sim p \vee q$
V	V	**V**	F	F	**V**	**V**
V	F	**F**	F	V	**F**	**F**
F	V	**V**	V	F	**V**	**V**
F	F	**V**	V	V	**V**	**V**

Tabela 1.8: Equivalência entre $p \longrightarrow q$, $\sim (p \wedge \sim q)$ e $\sim p \vee q$.

Definição 1.13. Se $p \longrightarrow q$ é uma condicional, então $\sim q \longrightarrow \sim p$ é dita ser a condicional **contra positiva**, $q \longrightarrow p$ é dita ser a condicional **recíproca** e $\sim p \longrightarrow \sim q$ é a

condicional **inversa**.

1.4 Teoremas

Um **teorema** é uma proposição lógica que é uma tautologia. As tautologias de principal interesse em matemática são as que envolvem os conectivos condicional e/ou bicondicional. A demonstração de um teorema nada mais é do que a confecção da tabela-verdade mostrando que a proposição é de fato uma tautologia.

Em matemática usa-se outros termos como **axiomas** e **postulados** que são fatos aceitos sem uma demonstração; **lemas** e/ou **proposições** que são teoremas cujo propósito é utilizá-los na demonstração de outro teorema e **corolários** que são teoremas que seguem imediatamente da demonstração de outro(s) teorema(s).

1.5 Definição de $\Longrightarrow$ e $\Longleftrightarrow$

Sejam p e q proposições. Se $p \longrightarrow q$ é uma tautologia, dizemos que esta proposição condicional é uma **implicação** e que p **implica logicamente** q e escrevemos $p \Longrightarrow q$. Se $p \longleftrightarrow q$ é uma tautologia, dizemos que esta bicondicional é uma **bi-implicação** e denotamos por $p \Longleftrightarrow q$. Lembre-se que $p \longleftrightarrow q$ ser tautologia significa que p e q são logicamente equivalentes e, assim, $p \Longleftrightarrow q$ representa a equivalência entre p e q.

Vamos ao nosso primeiro teorema que apresenta as propriedades básicas de $\Longrightarrow$.

Teorema 1.14. Sejam p, q e r proposições. Então:

1. *Reflexiva* - $p \Longrightarrow p$.
2. *Transitiva* - $(p \longrightarrow q) \wedge (q \longrightarrow r) \Longrightarrow (p \longrightarrow r)$.
3. *Simplificação* - $p \wedge q \Longrightarrow p$.
4. *Adição* - $p \Longrightarrow p \vee q$.
5. *Modus Ponens* - $(p \wedge (p \longrightarrow q)) \Longrightarrow q$.
6. *Modus Tollens* - $(p \longrightarrow q) \wedge \sim q \Longrightarrow \sim p$.
7. *Reduction ad absurdum* - $(\sim p \longrightarrow (q \wedge \sim q)) \Longrightarrow p$.
8. *Simetria* - $(p \longleftrightarrow q) \Longrightarrow (q \longleftrightarrow p)$.

9. *Transitiva* - $(p \longleftrightarrow q) \wedge (q \longleftrightarrow r) \Longrightarrow (p \longleftrightarrow r)$.

10. $(p \longrightarrow r) \Longrightarrow (p \wedge q \longrightarrow r)$.

11. *Disjunção* - $((p \vee q) \wedge \sim p) \Longrightarrow q$.

12. $\sim p \Longrightarrow (p \longrightarrow q)$.

13. $q \Longrightarrow (p \longrightarrow q)$.

14. $(p \longleftrightarrow q) \Longrightarrow (p \longrightarrow q)$.

Prova: Através da tabela-verdade, mostraremos os ítens 3, 6 e 14. Os outros ficam como exercícios. Lembrando que mostrar uma implicação $\Longrightarrow$ é mostrar que a condicional correspondente $\longrightarrow$ é uma tautologia.

3. $p \wedge q \Longrightarrow p$.

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

6. $(p \longrightarrow q) \wedge \sim q \Longrightarrow \sim p$.

p	q	$\sim q$	$p \longrightarrow q$	$(p \longrightarrow q) \wedge \sim q$	$(p \longrightarrow q) \wedge \sim q \longrightarrow \sim p$
V	V	F	V	F	V
V	F	V	F	F	V
F	V	F	V	F	V
F	F	V	V	V	V

14. $(p \longleftrightarrow q) \Longrightarrow (p \longrightarrow q)$.

p	q	$p \longrightarrow q$	$q \longrightarrow p$	$p \longleftrightarrow q$	$(p \longleftrightarrow q) \longrightarrow (p \longrightarrow q)$
V	V	V	V	V	V
V	F	F	V	F	V
F	V	V	F	F	V
F	F	V	V	V	V

■

As correspondentes propriedades de $\Longleftrightarrow$ são apresentadas no próximo teorema.

Teorema 1.15. Sejam p, q e r proposições. Então:

1. *Reflexiva -* $p \Longleftrightarrow p$.
2. *Dupla negação -* $\sim(\sim p)) \Longleftrightarrow p$.
3. *Negação da conjunção - Lei de Morgan -* $\sim(p \wedge q) \Longleftrightarrow (\sim p \vee \sim q)$.
4. *Negação da disjunção - Lei de Morgan -* $\sim(p \vee q) \Longleftrightarrow (\sim p \wedge \sim q)$.
5. *Negação da condicional -* $\sim(p \longrightarrow q) \Longleftrightarrow (p \wedge \sim q)$.
6. *Negação da bicondicional -* $\sim(p \longleftrightarrow q) \Longleftrightarrow (p \wedge \sim q) \vee (\sim p \wedge q)$.
7. *Comutatividade de* $\vee$ - $(p \vee q) \Longleftrightarrow (q \vee p)$.
8. *Comutatividade de* $\wedge$ - $(p \wedge q) \Longleftrightarrow (q \wedge p)$.
9. *Associatividade de* $\vee$ - $(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$.
10. *Associatividade de* $\wedge$ - $(p \wedge q) \wedge r \Longleftrightarrow p \wedge (q \wedge r)$.
11. *Distributividade -* $p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$.
12. *Distributividade -* $p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$.
13. *Bicondicional -* $(p \longleftrightarrow q) \Longleftrightarrow (p \longrightarrow q) \wedge (q \longrightarrow p)$.
14. *Contra positiva -* $(p \longrightarrow q) \Longleftrightarrow (\sim q \longrightarrow \sim p)$.
15. $(p \longrightarrow q) \Longleftrightarrow (\sim p \vee q)$.
16. $(p \longrightarrow (q \vee r)) \Longleftrightarrow (p \wedge \sim q) \longrightarrow r$.
17. $(p \vee q) \longrightarrow r \Longleftrightarrow (p \longrightarrow r) \wedge (q \longrightarrow r)$.
18. $p \longrightarrow q \wedge r \Longleftrightarrow (p \longrightarrow q) \wedge (p \longrightarrow r)$.
19. $(p \wedge q) \longrightarrow r \Longleftrightarrow (p \wedge \sim r) \longrightarrow \sim q$.
20. $(p \wedge q) \longrightarrow r \Longleftrightarrow (p \longrightarrow r) \vee (q \longrightarrow r)$.
21. $(p \wedge q) \longrightarrow r \Longleftrightarrow (p \longrightarrow (q \longrightarrow r))$.

22. $p \longleftrightarrow q \Longleftrightarrow \sim p \longleftrightarrow \sim q$.

23. *Idempotências* - $p \vee p \Longleftrightarrow p$ e $p \wedge p \Longleftrightarrow p$.

24. *Transitividade* - $(p \Longleftrightarrow q$ e $q \Longleftrightarrow r) \Longrightarrow (p \Longleftrightarrow r)$.

Prova: Como exercício, fazer alguns casos. ■

Referentes às tautologias e às contradições temos:

Teorema 1.16. Sejam t uma tautologia, c uma contradição e p uma proposição qualquer. Então:

1. $c \Longrightarrow p$
2. $p \Longrightarrow t$
3. $p \wedge t \Longleftrightarrow p$
4. $p \vee t \Longleftrightarrow t$
5. $p \wedge \sim p \Longleftrightarrow c$
6. $p \wedge c \Longleftrightarrow c$
7. $p \vee c \Longleftrightarrow p$
8. $\sim t \Longleftrightarrow c$
9. $\sim c \Longleftrightarrow t$
10. $p \vee \sim p \Longleftrightarrow t$

Prova: Como exercício, fazer alguns casos. ■

1.6 Quantificadores

Existem sentenças para as quais não há como decidir se assumem valor V ou F. Por exemplo: "$x + y = 5$" e "Ele é jogador de futebol". Estas sentenças são denominadas **sentenças abertas** ou **predicados**. Podemos compor sentenças abertas usando os mesmos conectivos usados nas proposições e formarmos novas sentenças abertas a partir de outras mais simples.

Há duas maneiras formais de transformar uma sentença aberta em uma proposição, utilizando os dois **quantificadores**. Para isso, necessitamos de um "universo" ou "domínio de discussão", isto é, uma coleção de objetos para os quais consideramos propriedades. Por exemplo, na proposição *"Todos os homens são mortais",* o universo é a coleção de todos os homens e tal proposição pode ser escrita como *"Para todo x do universo, x é mortal".*

A frase "Para todo x do universo" é chamada um **quantificador universal** e é simbolizado por "$\forall\ x$". A sentença "x é mortal" diz alguma coisa sobre x, então simbolizamos por $p(x)$. Assim escrevemos "Todos os homens são mortais" como

$$(\forall\ x)(p(x))$$

que pode ser lida como:

- para todo x, $p(x)$;

- para cada x, $p(x)$;

- para qualquer x, $p(x)$.

Vejamos agora a proposição "Alguns os homens são mortais". O universo é o mesmo da proposição anterior. Com este universo em mente, podemos escrever esta proposição como: "Existe no mínimo um homem que é mortal"; "Existe no mínimo um x, tal que x é mortal"; "Existe no mínimo um x, tal que $p(x)$".

A frase "Existe no mínimo um x, tal que" é chamada **quantificador existencial** e denotada por "$\exists\ x$". Usando este símbolo, podemos escrever a proposição "Alguns homens são mortais" como

$$(\exists\ x)(p(x))$$

que pode ser lida como:

- existe x, tal que $p(x)$;

- existe ao menos um x, tal que $p(x)$;

- para algum x, $p(x)$;

- para pelo menos um x, $p(x)$.

Quando existe um único elemento no universo que torna a proposição $(\exists\ x)(p(x))$ verdadeira, denotamos esta proposição por $(\exists!\ x)(p(x))$ e lemos:

- existe um único x, tal que $p(x)$;

- para um único x, $p(x)$.

Note que $(\exists!\ x)(p(x)) \Longrightarrow (\exists\ x)(p(x))$.

O conjunto dos elementos do universo que tornam uma sentença aberta uma proposição verdadeira é denominado **conjunto-verdade**. Por exemplo, para $p(x) : x+1 = 5$, o conjunto universo pode ser $\mathbb{R}$ e o conjunto-verdade é $\{4\}$, enquanto que para a sentença aberta $p(x) : \operatorname{sen}^2 x + \cos^2 x = 1$, temos que o conjunto-verdade é igual ao conjunto universo que é igual a $\mathbb{R}$.

Quando estiver subentendido quem é o conjunto universo, os quantificadores podem ser omitidos, por exemplo, escrevemos "$(x+1)(x-1) = x^2 - 1$" no lugar de escrever "$\forall\ x \in \mathbb{R},\ (x+1)(x-1) = x^2 - 1$". Também é comum escrevermos os quantificadores depois da sentença aberta, por exemplo, escrevemos "$f(x) = 0$, para todo x" no lugar de escrevermos "$(\forall\ x)(f(x) = 0)$".

Observe que claramente temos

$$(\forall\ x)(p(x)) \Longrightarrow (\exists\ x)(p(x)).$$

As negações de proposições com quantificadores são definidas por:

(a) $\sim [(\forall\ x)(p(x))] \Longleftrightarrow (\exists\ x)(\sim p(x))$.

(b) $\sim [(\exists\ x)(p(x))] \Longleftrightarrow (\forall\ x)(\sim p(x))$.

Vamos mostrar (a) em um caso particular. Suponhamos que o conjunto universo de $p(x)$ seja constituído pelos elementos a, b, c. Então a proposição $(\forall\ x)(p(x))$ significa:

$$p(a) \wedge p(b) \wedge p(c) \text{ é verdadeira.}$$

Daí, $\sim [(\forall\ x)(p(x))]$ é o mesmo que $\sim [p(a) \wedge p(b) \wedge p(c)]$ que é equivalente a $\sim p(a) \vee \sim p(b) \vee \sim p(c)$. Mas, se esta última for verdadeira, então um dos casos $\sim p(a), \sim p(b), \sim p(c)$ é verdade, o que é equivalente a $(\exists\ x)(\sim p(x))$. Daí segue que

$$\sim [(\forall\ x)(p(x))] \Longleftrightarrow ((\exists\ x)(\sim p(x))).$$

Exemplo 1.17. A negação de:

$$(\forall\ x)(\operatorname{sen}^2 x + \cos^2 x = 1),$$

significa que

$$(\exists\ x)(\sim (\operatorname{sen}^2 x + \cos^2 x = 1)),$$

ou seja,

$$(\exists\ x)(\operatorname{sen}^2 x + \cos^2 x \neq 1).$$

Os quantificadores nos dão uma idéia do que são os **exemplos** e os **contra-exemplos**. Quando temos uma proposição verdadeira que contém um dos quantificadores, dar um exemplo é escolher uma variável x para o qual ela é verdadeira, ou seja, é escolher um elemento do seu conjunto-verdade. Quando uma proposição que contém um dos quantificadores não é verdadeira, significa que o seu conjunto-verdade é diferente do conjunto universo. Assim, encontrar um contra-exemplo é escolher uma variável x que não esteja no conjunto-verdade.

1.7 Método Dedutivo

Vimos que demonstrar teoremas significa verificar que a proposição dada é uma tautologia e, fizemos isso, construindo tabelas-verdade. Veremos agora outra maneira de verificar a validade de proposições. Este procedimento é chamado de **método dedutivo** e consiste na utilização de definições, de outros resultados pré-estabelecidos e das propriedades transitivas de $\Longrightarrow$ e $\Longleftrightarrow$. Vejamos como utilizá-lo em exemplos.

Exemplo 1.18. Usando o método dedutivo mostrar a validade de

$$(p \longrightarrow q) \Longleftrightarrow (\sim q \longrightarrow \sim p).$$

Como

$$\begin{array}{rcll} (p \longrightarrow q) & \Longleftrightarrow & \sim p \vee q & \text{Teorema 1.15 (15)} \\ \sim p \vee q & \Longleftrightarrow & q \vee \sim p & \text{Teorema 1.15 (7)} \\ q \vee \sim p & \Longleftrightarrow & \sim (\sim q) \vee \sim p & \text{Teorema 1.15 (2)} \\ \sim (\sim q) \vee \sim p & \Longleftrightarrow & \sim q \longrightarrow \sim p & \text{Teorema 1.15 (15)} \end{array}$$

usando a transitividade de $\Longleftrightarrow$, obtemos a equivalência desejada.

Exemplo 1.19. Usando o método dedutivo, mostre a validade de

$$(p \longrightarrow r) \vee (q \longrightarrow s) \Longleftrightarrow (p \wedge q) \longrightarrow (r \vee s).$$

Como

$$\begin{array}{rcll} (p \longrightarrow r) \vee (q \longrightarrow s) & \Longleftrightarrow & (\sim p \vee r) \vee (\sim q \vee s) & \text{Teorema 1.15 (15)} \\ & \Longleftrightarrow & (\sim p \vee \sim q) \vee (r \vee s) & \text{Teorema 1.15 (7,9)} \\ & \Longleftrightarrow & \sim (p \wedge q) \vee (r \vee s) & \text{Teorema 1.15 (3)} \\ & \Longleftrightarrow & (p \wedge q) \longrightarrow (r \vee s) & \text{Teorema 1.15 (15)} \end{array}$$

usando a transitividade de $\Longleftrightarrow$, obtemos a equivalência.

Exemplo 1.20. Considere as seguintes afirmações:

H_1 : Tempo é dinheiro.

H_2 : Vagabundo tem muito tempo.

T : Vagabundo tem muito dinheiro.

A proposição $(H_1 \wedge H_2 \Longrightarrow T)$ é um teorema?

Se considerarmos p : "Ter tempo", q : "Ter dinheiro" e r : "Ser vagabundo", teremos que $H_1 : p \longrightarrow q$, $H_2 : r \longrightarrow p$ e $T : r \longrightarrow q$. Assim, podemos escrever a proposição $H_1 \wedge H_2 \Longrightarrow T$ como $(p \longrightarrow q) \wedge (r \longrightarrow p) \Longrightarrow (r \longrightarrow q)$ que é verdadeira, mostrando que a proposição dada é um teorema.

Exemplo 1.21. Considere agora as seguintes afirmações:

H_1 : Penso, logo existo.

H_2 : Pedras não pensam.

T : Pedras não existem.

A proposição $(H_1 \wedge H_2 \Longrightarrow T)$ é um teorema?

Se considerarmos p : "Pensar" e q : "Existir", teremos que $H_1 : p \longrightarrow q$, $H_2 :\sim p$ e $T :\sim q$. Assim, podemos escrever a proposição $H_1 \wedge H_2 \Longrightarrow T$ como $((p \longrightarrow q) \wedge \sim p) \Longrightarrow \sim q$ que não é verdadeira, pois $((p \longrightarrow q) \wedge \sim p) \longrightarrow \sim q$ não é uma tautologia, mostrando que a proposição dada não é um teorema.

1.8 Métodos de Demonstração

Veremos três maneiras ou métodos de demonstrar um teorema da forma $p \Longrightarrow q$.

(1) Prova ou demonstração direta: Consiste na utilização do método dedutivo, assumindo que p é verdadeira e, utilizando equivalências lógicas e fatos pré estabelecidos, deduzir que q é verdadeira.

Por exemplo, mostre que:

"Se x é um número inteiro par, então x^2 é um inteiro par".

Note que esta é uma implicação do tipo $p \Longrightarrow q$, onde p é a proposição "x é um número inteiro par" e q é a proposição "x^2 é um número inteiro par".

Assumindo p verdadeira, temos que x é um número inteiro par $\Longrightarrow$ x é divisível por 2, por definição $\Longleftrightarrow$ x é múltiplo de 2 $\Longleftrightarrow$ existe $n \in \mathbb{Z}$, tal que $x = 2n \Longrightarrow$ $x^2 = (2n)^2 = 4n^2 = 2(2n^2) = 2m$, para algum $m \in \mathbb{Z} \Longrightarrow$ x^2 é um número inteiro par $= q$.

(2) Demonstração por contraposição: Consiste na utilização da equivalência lógica $p \longrightarrow q \Longleftrightarrow \sim q \longrightarrow \sim p$, ou seja, para mostrarmos o teorema $p \Longrightarrow q$, mostramos, utilizando o método da demonstração direta que $\sim q \Longrightarrow \sim p$.

Por exemplo, mostre que:

"Se x é um número inteiro tal que x^2 é ímpar, então x é um inteiro ímpar".

Esta é uma implicação do tipo $p \Longrightarrow q$, onde p é a proposição "x^2 é um número inteiro ímpar" e q é a proposição "x é um número inteiro ímpar".

Note que não é possível utilizar o método da demonstração direta neste caso, pois de x^2 é um número inteiro ímpar, temos que existe $n \in \mathbb{Z}$ tal que $x^2 = 2n + 1$ e, não conseguimos chegar que existe um $m \in \mathbb{Z}$ tal que $x = 2m + 1$.

Utilizando a equivalência lógica citada acima, vamos mostrar que $\sim q \Longrightarrow \sim p$.

Agora, $\sim q : x$ não é ímpar $\Longrightarrow x$ é par $\Longrightarrow x^2$ é par, pelo exemplo anterior $\Longrightarrow \sim p$. Consequentemente, $p \Longrightarrow q$.

(3) Demonstração por contradição (Reduction ad absurdum): Consiste na utilização da equivalência lógica $p \longrightarrow q \Longleftrightarrow (p \wedge \sim q) \longrightarrow \sim p$, ou seja, para mostrarmos o teorema $p \Longrightarrow q$, mostramos, que $(p \wedge \sim q) \Longrightarrow \sim p$, o que nos leva a um absurdo, pois, como p é sempre verdadeira e concluímos que $\sim p$ é também verdadeira, teremos que $p \wedge \sim p$ é verdadeira, o que é uma contradição.

Por exemplo, mostre que:

"Se x é um número inteiro tal que x^2 é par, então x é um inteiro par".

Aqui, p é a proposição "x^2 é um número inteiro par" e q é a proposição "x é um número inteiro par". Note que, novamente, não dá para demonstrar direto que $p \Longrightarrow q$. Assuma então que $(p \wedge \sim q)$ seja verdadeira, isto é, que x^2 é par e x é ímpar $\Longrightarrow$ $x = 2n + 1$, para algum $n \in \mathbb{Z} \Longrightarrow x^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1 =$

$2m+1$, para algum $m \in \mathbb{Z} \Longrightarrow x^2$ é ímpar $\Longrightarrow \sim p$, o que é uma contradição. Logo, a proposição "x é par" não pode ser falsa, o que mostra que $p \Longrightarrow q$.

1.9 Exercícios

1. Considere as proposições p : "Fred tem cabelos vermelhos", q : "Fred tem nariz grande" e r : "Fred gosta de comer figos". Passe para a linguagem simbólica as seguintes proposições:

   (a) Fred não gosta de comer figos.

   (b) Fred tem cabelos vermelhos ou gosta de comer figos.

   (c) Fred tem cabelos vermelhos e não tem nariz grande.

   (d) Fred gosta de comer figos e, tem cabelos vermelhos ou tem nariz grande.

   (e) Fred gosta de comer figos e tem cabelos vermelhos, ou tem nariz grande.

   (f) Não é o caso de Fred ter nariz grande ou cabelos vermelhos.

   (g) Fred tem nariz grande e cabelos vermelhos, ou ele tem nariz grande e gosta de comer figos.

2. Sejam p : "A casa é azul", q : "A casa tem 30 anos" e r : "A casa é feia". Passe para a linguagem simbólica as seguintes sentenças:

   (a) Se a casa tem 30 anos, então ela é feia.

   (b) Se a casa é azul, então ela é feia ou tem 30 anos.

   (c) Se a casa é azul então ela é feia, ou tem 30 anos.

   (d) A casa não é feia se e somente se ela tem 30 anos.

   (e) A casa tem 30 anos se ela é azul, e ela não é feia se ela tem 30 anos.

   (f) Para que a casa seja feia é necessário e suficiente que ela seja feia e tenha 30 anos.

3. Supondo que p seja uma sentença verdadeira, que q seja falsa, que r seja falsa e que s seja verdadeira, decidir quais das sentenças abaixo são verdadeiras e quais são falsas.

(a) $p \vee r$.

(b) $(r \wedge s) \vee q$.

(c) $\sim (p \wedge q)$.

(d) $\sim s \vee \sim r$.

(e) $(s \wedge p) \vee (q \wedge r)$.

(f) $r \vee (s \vee (p \wedge q))$.

4. Suponha que p seja uma sentença falsa, que q seja verdadeira, que r seja falsa e que s seja verdadeira. Quais das seguintes sentenças são verdadeiras e quais são falsas?

(a) $r \rightarrow q$.

(b) $p \longleftrightarrow r$.

(c) $(q \longleftrightarrow s) \wedge p$.

(d) $s \rightarrow (p \rightarrow \sim s)$.

(e) $[(q \rightarrow s) \longleftrightarrow s] \wedge \sim p$.

(f) $(s \rightarrow p) \longleftrightarrow \sim (r \vee q)$.

5. Construir a tabela-verdade de cada uma das proposições abaixo:

(a) $p \wedge \sim q$.

(b) $(r \vee s) \wedge \sim r$.

(c) $p \vee (\sim q \vee r)$.

(d) $(p \vee q) \wedge (p \vee s)$.

(e) $(p \wedge r) \vee \sim (q \wedge s)$.

(f) $(p \wedge q \wedge r) \vee (\sim p \wedge q \wedge \sim r) \vee (\sim p \wedge \sim q \wedge \sim r)$.

(g) $(p \rightarrow q) \rightarrow [p \vee (q \wedge r) \rightarrow p \wedge (p \vee r)]$.

(h) $\sim p \wedge q$.

(i) $\sim (p \rightarrow \sim q)$.

(j) $(p \wedge q) \rightarrow (p \vee q)$.

(k) $\sim (p \wedge q) \vee \sim (p \longleftrightarrow q)$.

(l) $(p \rightarrow q) \vee \sim (p \longleftrightarrow \sim q)$.

(m) $(p \rightarrow (\sim q \vee r)) \wedge \sim (q \vee (p \longleftrightarrow \sim r))$.

6. Quais das proposições acima são equivalentes? Quais são tautologias? Quais são contradições? Justifique suas respostas.

7. Verificar que as seguintes proposições são equivalentes:

(a) $\sim (p \wedge q)$ e $\sim p \vee \sim q$.

(b) $\sim (p \vee q)$ e $\sim p \wedge \sim q$.

(c) $\sim (p \rightarrow q)$ e $p \wedge \sim q$.

(d) $\sim (p \longleftrightarrow q)$ e $(p \longleftrightarrow \sim q)$.

8. Quantificar as sentenças abertas a fim de obter proposições verdadeiras:

(a) $x^2 + y^2 + z^2 = (x + y + z)^2 - 2xz - 2xy - 2yz$.

(b) $x + y = 8$.

(c) $\sec^2 x = 1 + \tan^2 x$.

(d) $\operatorname{sen} x = 2$.

9. Dar a negação das proposições abaixo:

(a) $(\forall\, x)(p(x) \vee q(x) \rightarrow s(x))$.

(b) $(\forall\, x)p(x) \rightarrow s(x)$.

(c) $(\exists\, x)(p(x) \wedge q(x))$.

(d) $(\exists\, x)p(x) \longleftrightarrow q(x)$.

(e) $(\exists\, x)(\forall\, y)p(x, y)$.

(f) $(\forall\, x)(\exists\, y)(p(x) \vee q(y))$.

(g) $(\exists\, x)(\exists\, y)(p(x) \wedge \sim q(y))$.

(h) $(\forall\, x)(\forall\, y)p(x, y)$.

2
Teoria dos Conjuntos

2.1 Noções Primitivas, Definições e Axiomas

A maioria das noções em Matemática são definidas utilizando outras noções que já foram estabelecidas. Assim, para definirmos uma noção, precisamos de outra pré-estabelecida, para esta outra, precisamos de mais outra, etc... Aí surge a pergunta natural: E a primeira de todas as noções, como é estabelecida?

É natural que esta primeira noção não possa ser definida usando-se outra pré-estabelecida, de onde concluímos que não podemos definir tudo. Somos obrigados, ao iniciar o estudo de um certo conteúdo matemático, adotar, sem definir, as primeiras noções, que são chamadas **noções primitivas**.

Isto foi o que Euclides (330 a.C. a 270 a.C.) fez com a Geometria quando escreveu "Os Elementos", onde alguns axiomas foram admitidos e tudo o mais foi deduzido a partir deles.

Na teoria dos conjuntos adotamos duas noções primitivas, a saber, a de **conjunto** e a de **pertinência**, denotada por $\in$.

A segunda noção estabelece uma relação entre conjuntos da seguinte forma: se x e A são conjuntos, a expressão $x \in A$ pode ser lida como "x pertence a A" ou "x está em A". Com esta noção podemos definir a noção de **elemento**, da seguinte forma:

Definição 2.1. Seja x um conjunto. Se existe um conjunto A tal que $x \in A$, então x é dito ser **elemento**, ou seja, dizemos que x **é um elemento de** A, ou ainda que x **pertence**

a A.

Quando um conjunto x não for um elemento do conjunto A, escrevemos $x \notin A$, e lemos "x **não pertence** a A", ou ainda "x não está em A", que é a negação de $x \in A$.

Parece estranho escolhermos conjunto e pertinência como elementos primitivos ao invés de conjunto e elemento, mas é mais fácil definir elemento usando a noção de pertinência do que definir a noção de pertinência usando a noção de elemento.

Estabeleceremos como convenção o uso de letras maiúsculas para denotar conjuntos e letras minúsculas para denotar elementos.

A seguir definimos a noção de igualdade de conjuntos.

Definição 2.2. Sejam A e B conjuntos. Dizemos que o conjunto A é **igual** ao conjunto B, e denotamos por $A = B$, se todo elemento de A é um elemento de B e vice-versa. Simbolicamente escrevemos

$$A = B \Longleftrightarrow (\forall\, x)[(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)].$$

Note que, com esta definição, dois conjuntos são iguais se, e somente se eles têm os mesmos elementos.

A nosso intuição nos diz que quando um elemento x está em um conjunto A e x é igual a outro elemento y, então é natural esperar que y também seja elemento de A; isso é garantido pelo primeiro axioma da teoria dos conjuntos.

Axioma da Extensão: *Se $x = y$ e $x \in A$, então $y \in A$.*

A seguir definimos a noção de **inclusão** de conjuntos.

Definição 2.3. Sejam A e B conjuntos. Dizemos que A **está contido** em B, (ou B **contém** A) e denotamos por $A \subseteq B$(ou $B \supseteq A$), se todo elemento de A for um elemento de B. Neste caso, dizemos também que A é um **subconjunto** de B. Simbolicamente escrevemos

$$A \subseteq B \Longleftrightarrow (\forall\, x)(x \in A \longrightarrow x \in B).$$

Se $A \subseteq B$ e A é diferente de B, dizemos que A é um **subconjunto próprio** de B e denotamos por $A \subsetneq B$ ou $A \subset B$.

Estas noções, definições e axioma, nos permitem demonstrar o seguinte resultado:

Proposição 2.4. Sejam A, B e C conjuntos. Então as seguintes propriedades são válidas:

(a) *Reflexiva:* $A = A$.

(b) *Simétrica:* $A = B \Longrightarrow B = A$.

(c) *Transitiva:* $(A = B) \wedge (B = C) \Longrightarrow A = C$.

(d) *Reflexiva:* $A \subseteq A$.

(e) *Anti-simétrica:* $(A \subseteq B) \wedge (B \subseteq A) \Longleftrightarrow A = B$.

(f) *Transitiva:* $(A \subseteq B) \wedge (B \subseteq C) \Longrightarrow A \subseteq C$.

Prova: Vamos mostrar alguns ítens; as demonstrações dos restantes ficam como exercício.

(a) A proposição $x \in A \longleftrightarrow x \in A$ é uma tautologia, logo, da Definição 2.2, temos $A = A$.

(b) Da Definição 2.2 temos que

$$A = B \Longleftrightarrow (\forall\, x)[(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)].$$

Agora, pela comutatividade do conectivo $\wedge$ e novamente pela Definição 2.2, concluímos que $B = A$.

(e) Da Definição 2.3, temos que $A \subseteq B \wedge B \subseteq A$ é equivalente a proposição

$$(\forall\, x)[(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)],$$

que por sua vez, é equivalente a $A = B$ pela Definição 2.2. ■

Uma maneira de representar um conjunto é exibir seus elementos entre chaves e separados por vírgulas, mas podemos também caracterizar um conjunto através de uma propriedade que o defina. Isso deve ser feito axiomaticamente, tomando certos cuidados para evitar contradições. Vejamos o axioma que nos permite construir conjuntos a partir de propriedades.

Axioma da especificação: *Sejam A um conjunto e $p(x)$ uma proposição em x que deve ser expressa totalmente em função dos símbolos $\wedge$, $\vee$, $\sim$, $\longrightarrow$, $\in$, $\exists$, $\forall$, $[\,]$ e variáveis $x, y, z, \ldots, A, B, C, \ldots$. Então existe um conjunto que consiste de todos os elementos x de A que tornam $p(x)$ verdadeira. Simbolicamente, escrevemos*

$$\{x \in A;\ p(x) \text{ é verdadeira}\}.$$

Observação 2.5. A restrição de $p(x)$ utilizar somente símbolos lógicos e variáveis faz sentido para evitar paradoxos do tipo semântico. Um exemplo disso é o seguinte paradoxo, que numa versão simplificada, diz:

Paradoxo de Richard: Todo número inteiro pode ser descrito em palavras utilizando um certo número de letras. Por exemplo, o número 36 pode ser descrito como "trinta e seis" ou "quatro vezes nove". A primeira descrição utiliza 11 letras e a segunda 15 letras. Vamos dividir o conjunto dos números inteiros positivos em dois grupos, o primeiro contendo todos os números inteiros positivos que podem ser escritos com no máximo 100 letras e o segundo inclui todos os números inteiros positivos que necessitam de pelo menos 101 letras para descrevê-los. Há um número finito de números no primeiro grupo, pois existem no máximo 24^{100} expressões com no máximo 100 letras. Existe então um menor inteiro positivo no segundo grupo. Este menor inteiro pode ser descrito pela frase "o menor inteiro que não é descrito com menos de 100 letras", o que o descreve com menos de 100 letras. Então este número pertence ao primeiro grupo, o que é uma contradição.

Note que este conjunto não pode ser construído pelo axioma da especificação, pois a propriedade do axioma está restrita a operadores lógicos e alguns símbolos. Por isso estamos livres desta contradição.

Observação 2.6. Outra aplicação mais interessante deste axioma é que ele garante que não existe um conjunto que contenha todos os conjuntos.

De fato, supondo que exista o conjunto cujos elementos sejam todos os conjuntos, seja U tal conjunto. Assim, usando o axioma da especificação, podemos formar o conjunto $B = \{x \in U;\ x \notin x\}$. A questão agora é: será que $B \in U$?

Se sim, temos duas possibilidades, $B \in B$ ou $B \notin B$.

Se $B \in B$, pela especificação de B, temos que $B \notin B$ e, se $B \notin B$, então $B \in B$, o que é uma contradição. Assim, chegamos à conclusão que $B \notin U$, ou seja, não existe um conjunto universo. O argumento que levou a essa conclusão chama-se o **paradoxo de Russel**, cuja versão popular é: Numa certa cidade existe um barbeiro que só faz a barba nos homens que não barbeiam a si próprios. Quem faz a barba do barbeiro?

Com o auxílio do axioma da especificação, podemos construir vários conjuntos importantes.

Definição 2.7. O **conjunto vazio**, denotado por $\emptyset$, é o conjunto que não possui elemento algum.

A existência deste conjunto é garantida pelo axioma da especificação, pois dado qualquer conjunto A, temos que $\emptyset = \{x \in A;\ x \neq x\}$.

Definição 2.8. Sejam A e B dois conjuntos. A **união de A e B**, denotada por $A \cup B$, é o conjunto formado pelos elementos x tais que x está em pelo menos um dos dois conjuntos A ou B. Simbolicamente,

$$A \cup B = \{x; x \in A \vee x \in B\}.$$

A **intersecção de A e B**, denotada por $A \cap B$, é o conjunto formado pelos elementos x tais que x está em ambos os conjuntos A e B. Simbolicamente,

$$A \cap B = \{x; x \in A \wedge x \in B\}.$$

Dessa definição, temos as seguintes equivalências lógicas:

$$x \in A \cup B \iff (x \in A \vee x \in B)$$

e

$$x \in A \cap B \iff (x \in A \wedge x \in B).$$

Note que a existência dos conjuntos $A \cup B$ e $A \cap B$ é garantida pelo axioma da especificação.

Com relação à união e à intersecção de conjuntos temos as seguintes propriedades:

Teorema 2.9. Sejam A e B conjuntos. Então:

(a) $A \subseteq A \cup B$ e $B \subseteq A \cup B$.

(b) $A \cap B \subseteq A$ e $A \cap B \subseteq B$.

(c) $A \subseteq B \iff A \cup B = B$ e $A \subseteq B \iff A \cap B = A$.

(d) $A \cup (B \cap A) = A$ e $A \cap (B \cup A) = A$.

Prova: Para os ítens (a) e (b), mostraremos uma das inclusões, as outras são demonstradas de forma análoga e ficam como exercício.

Vamos mostrar que $A \subseteq A \cup B$, o que é equivalente, por definição, a mostrar que $x \in A \Longrightarrow x \in A \cup B$, o que é equivalente a mostrar que $x \in A \longrightarrow x \in A \vee x \in B$ é uma tautologia , o que é verdade, pois é uma implicação do tipo $p \longrightarrow p \vee q$.

No ítem (c), também provaremos somente uma das equivalências, ficando a outra como exercício.

Vamos mostrar que $A \subseteq B \iff A \cup B = B$. Como $(p \iff q) \iff (p \Longrightarrow q) \wedge (q \Longrightarrow p)$, vamos mostrar as implicações $\Longrightarrow$ e $\Longleftarrow$ separadamente.

($\Longrightarrow$) Queremos mostrar que se $A \subseteq B$, então $A \cup B = B$. Note que pela igualdade de conjuntos, temos que mostrar que $A \cup B \subseteq B$ e $B \subseteq A \cup B$. A segunda inclusão segue de (a). Para a primeira, seja $x \in A \cup B$, então, $x \in A \vee x \in B$. Se $x \in A$, como por hipótese, $A \subseteq B$, temos que $x \in B$. Assim, $x \in B$, em ambos os casos, como queríamos.

($\Longleftarrow$) Se $A \cup B = B$, então, como $A \subseteq A \cup B = B$, temos claramente que $A \subseteq B$.

A demonstração do ítem (d) fica como exercício. ■

Dizemos que dois conjuntos A e B são **disjuntos** se eles não possuem elementos em comum, ou seja, se $A \cap B = \emptyset$.

Teorema 2.10. Sejam X, A e B conjuntos. Então temos:

(a) $\emptyset \subseteq A$, $A \cup \emptyset = A$ e $A \cap \emptyset = \emptyset$.

(b) $X \subseteq A \cap B \iff (X \subseteq A) \wedge (X \subseteq B)$.

(c) $(X \subseteq A) \vee (X \subseteq B) \Longrightarrow X \subseteq A \cup B$ e não vale a volta desta implicação.

Prova: Vamos mostrar a primeira inclusão do ítem (a), ou seja que $\emptyset \subseteq A$. Por definição, temos que mostrar que $x \in \emptyset \Longrightarrow x \in A$.

Como a proposição $p : x \in \emptyset$ é sempre falsa, então $p \longrightarrow q$ é verdadeira para qualquer proposição q, o que mostra a inclusão. Outra maneira de mostrar este fato é usando-se a contra-positiva, isto é, supondo que $x \notin A$, então certamente temos que $x \notin \emptyset$, pois o conjunto vazio não contém elementos, assim, $x \notin A \Longrightarrow x \notin \emptyset$.

Mostremos agora a equivalência $X \subseteq A \cap B \Longleftrightarrow (X \subseteq A) \wedge (X \subseteq B)$, deixando o restante como exercício.

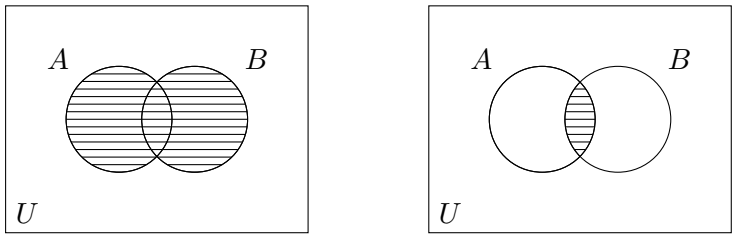
($\Longrightarrow$) Nesta implicação, a hipótese é $X \subseteq A \cap B$ e a tese é $(X \subseteq A) \wedge (X \subseteq B)$. Seja $x \in X$; como por hipótese $X \subseteq A \cap B$, temos que $x \in A \cap B$ e, pela definição de intersecção, temos que $x \in A \wedge x \in B$. Portanto $(X \subseteq A) \wedge (X \subseteq B)$.

($\Longleftarrow$) Nesta implicação, a hipótese é $(X \subseteq A) \wedge (X \subseteq B)$ e a tese é $X \subseteq A \cap B$. Seja $x \in X$; por hipótese $x \in A \wedge x \in B$ e, pela definição de intersecção, temos que $x \in A \cap B$. Portanto $X \subseteq A \cap B$. ■

Diagramas de Venn e de Linha

Uma maneira simples de ilustrar as relações entre conjuntos é por meio de diagramas. Existem dois tipos mais utilizados, que são os **diagramas de Venn** e os **diagramas de linha**.

No diagrama de Venn os conjuntos são representados por regiões limitadas do plano e suas relações são representadas pelas posições dessas regiões. Nas figuras abaixo, representamos algumas relações entre os conjuntos A e B.



(a) $A \cup B$ (b) $A \cap B$

Figura 2.1: União e intersecção de conjuntos.

No diagrama de linha, não representamos os conjuntos mas sim a relação de inclusão entre eles. Um conjunto que contém o outro conjunto estará num nível vertical acima ligado ao primeiro por um segmento de reta. Caso os conjuntos não possuam a relação de inclusão, eles não são unidos pelo segmento de reta. Neste caso, eles são colocados

horizontalmente, em posições diferentes. Na figura abaixo vemos um exemplo de um diagrama de linha.

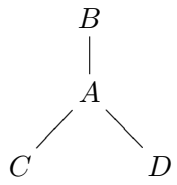


Figura 2.2: Diagrama de Linha.

2.2 Operações com Conjuntos

Em Aritmética podemos adicionar, multiplicar ou subtrair dois números. Nos conjuntos, as operações união, intersecção e diferença (como definida abaixo), se comportam de maneira semelhante às operações aritméticas.

Definição 2.11. Sejam A e B dois conjuntos. A **diferença** entre A e B, denotado por $A \setminus B$ ou $A - B$, é o conjunto formado pelos elementos que estão em A e não estão em B. Simbolicamente, escrevemos

$$A \setminus B = \{x;\, x \in A \wedge x \notin B\}.$$

Se $A \subseteq B$, o conjunto $B - A$ é dito também ser o **complementar** de A em B e denotado por A^c_B. Se A está contido em um conjunto universo U, o complementar de A em U é denotado simplesmente por $A^c = \{x; x \notin A\}$.

Com estas noções temos os seguintes diagramas de Venn:

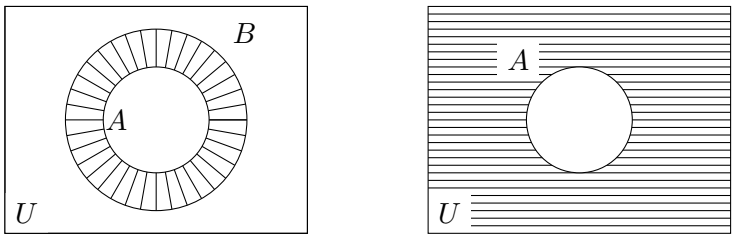
Com respeito a estas operações entre conjuntos, temos as seguintes propriedades:

Teorema 2.12. Sejam A, B e C conjuntos. Então:

(a) *Associativa* - $A \cup (B \cup C) = (A \cup B) \cup C$,
$A \cap (B \cap C) = (A \cap B) \cap C$.

(b) *Comutativa* - $A \cup B = B \cup A$ e $A \cap B = B \cap A$.

(c) *Distributiva* - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.



(a) $B - A$ (b) A^c

Figura 2.3: Diferença entre Conjuntos e Complementar.

(d) *Idempotência* - $A \cup A = A$ e $A \cap A = A$.

(e) $A - B \subseteq A$ e $(A - B) \cap B = \emptyset$.

(f) $A - B = \emptyset \iff A \subseteq B$ e $A - (A - B) = B \iff B \subseteq A$.

Se A e B são subconjuntos de um mesmo conjunto universo U, então:

(g) *Leis de Morgan* - $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$.

(h) $(A^c)^c = A$ e $A \cap A^c = \emptyset$.

(i) $A \subseteq B$ se, e somente se, $B^c \subseteq A^c$.

Prova: Mostraremos uma das igualdades do ítem (a) e uma das leis de Morgan do ítem (g) deixando a demonstrações do restante do teorema como exercício.

A igualdade $A \cup (B \cup C) = (A \cup B) \cup C$ segue das seguintes equivalências:

$$\begin{array}{lll}
x \in A \cup (B \cup C) & \iff & x \in A \vee x \in (B \cup C) \qquad \text{Definição de } \cup \\
& \iff & x \in A \vee (x \in B \vee x \in C) \qquad \text{Definição de } \cup \\
& \iff & (x \in A \vee x \in B) \vee x \in C \qquad \text{Distributividade de } \vee \\
& \iff & x \in (A \cup B) \vee x \in C \qquad \text{Definição de } \cup \\
& \iff & x \in (A \cup B) \cup C \qquad \text{Definição de } \cup.
\end{array}$$

A igualdade $(A \cup B)^c = A^c \cap B^c$, segue de maneira análoga a negação da disjunção 1.15 (4). ■

Axioma da potência: *Para cada conjunto, existe uma coleção de conjuntos que contém entre seus elementos todos os subconjuntos do conjunto dado.*

Definição 2.13. Seja A um conjunto. O **conjunto potência** de A ou **conjunto das partes** de A, denotado por $\wp(A)$, é o conjunto cujos elementos são os subconjuntos de A. Simbolicamente, temos $\wp(A) = \{B;\ B \subseteq A\}$.

Exemplo 2.14. Para $A = \{a, b, c\}$, temos

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

Proposição 2.15. Sejam A e B conjuntos. Então:

(a) $\wp(A \cap B) = \wp(A) \cap \wp(B)$.

(b) $\wp(A \cup B) \supseteq \wp(A) \cup \wp(B)$.

Prova: Temos as seguintes equivalências:

$$\begin{aligned}
X \in \wp(A \cap B) &\iff X \subseteq A \cap B, && \text{Definição 2.13}\\
&\iff X \subseteq A \wedge X \subseteq B, && \text{Teorema 2.10}\\
&\iff X \in \wp(A) \wedge X \in \wp(B), && \text{Definição 2.13}\\
&\iff X \in \wp(A) \cap \wp(B), && \text{Definição de } \cap
\end{aligned}$$

o que demonstra o ítem (a).

A demonstração do ítem (b) fica como exercício. ■

Observação 2.16. Note que a inclusão $\wp(A \cup B) \subseteq \wp(A) \cup \wp(B)$ não é verdadeira. De fato, para $A = \{1\}$ e $B = \{2\}$, temos $\wp(A \cup B) = \wp(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ e $\wp(A) \cup \wp(B) = \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}$.

Para definirmos a união e a intersecção de um número finito de conjuntos, podemos usar o axioma da especificação. Para uma coleção qualquer de conjuntos, já não é possível utilizar esse axioma para construir um conjunto união e um conjunto intersecção. Para tanto, necessitamos do seguinte axioma:

Axioma da união: *Para toda coleção de conjuntos existe um conjunto que contém todos os elementos que pertencem a algum conjunto da coleção dada.*

Em outras palavras, este axioma garante que, para toda coleção de conjuntos $\mathcal{C}$, existe um conjunto U tal que, se $x \in A$ para algum A em $\mathcal{C}$, então $x \in U$. Assim podemos definir:

Definição 2.17. Seja $\mathcal{C}$ uma coleção de conjuntos. A **união dos conjuntos em** $\mathcal{C}$ ou a **união dos elementos de** $\mathcal{C}$, denotada por $\bigcup_{A\in\mathcal{C}} A$ ou $\bigcup\mathcal{C}$, consiste de todos os elementos que pertencem a pelo menos um conjunto da coleção. Em símbolos,

$$\bigcup_{A\in\mathcal{C}} A = \{x \in A;\ A \in \mathcal{C}\}.$$

Note que, nesta definição utilizamos o axioma da união e o axioma da especificação para garantir a existência de $\bigcup_{A\in\mathcal{C}} A$. A unicidade é garantida pelo axioma da extensão.

Podemos também escrever

$$\bigcup_{A\in\mathcal{C}} A = \{x; \exists\ A \in \mathcal{C} \text{ tal que } x \in A\}.$$

Para a intersecção de conjuntos de uma coleção temos:

Definição 2.18. Seja $\mathcal{C}$ uma coleção de conjuntos. A **intersecção dos conjuntos em** $\mathcal{C}$ ou a **intersecção dos elementos de** $\mathcal{C}$, denotada por $\bigcap_{A\in\mathcal{C}} A$ ou $\bigcap\mathcal{C}$, consiste de todos os elementos que pertencem a todos os conjuntos da coleção. Em símbolos

$$\bigcap_{A\in\,\mathcal{C}} A = \{x;\ x \in A \text{ para todo } A \in\ \mathcal{C}\}.$$

Também podemos escrever

$$\bigcap\mathcal{C} = \{x; (A \in\ \mathcal{C} \longrightarrow x \in A)\}.$$

Vejamos a noção de família ou coleção indexada de conjuntos.

Definição 2.19. Seja Γ um conjunto. Assuma que para cada elemento $\gamma \in \Gamma$ está associado um conjunto A_γ. A coleção de tais conjuntos A_γ é dita ser uma **família indexada de conjuntos**, indexada pelo conjunto Γ e denotada por $\{A_\gamma;\ \gamma \in \Gamma\}$ ou $(A_\gamma)_{\gamma\in\Gamma}$.

Observação 2.20. Se $\mathcal{C} = \{A_\gamma;\ \gamma \in \Gamma\}$, escrevemos

$$\bigcup\mathcal{C} = \bigcup_{\gamma\in\Gamma} A_\gamma = \{x;\ x \in A_\gamma \text{ para algum } \ \gamma \in \Gamma\}$$

e

$$\bigcap\mathcal{C} = \bigcap_{\gamma\in\Gamma} A_\gamma = \{x;\ x \in A_\gamma \text{ para todo } \gamma \in \Gamma\}.$$

Note que dada qualquer coleção de conjuntos, sempre é possível encontrar um conjunto de índices Γ e tornar esta coleção uma família indexada de conjuntos, indexada por Γ.

Mais ainda, se o conjunto de índices é finito, $\Gamma = \{1, 2, 3, \ldots, n\}$, escrevemos

$$\bigcup_{\gamma\in\Gamma} A_\gamma = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

e

$$\bigcap_{\gamma\in\Gamma} A_\gamma = \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n.$$

Se $\Gamma = \mathbb{N}$, escrevemos $\bigcup_{\gamma\in\Gamma} A_\gamma = \bigcup_{i=1}^{\infty} A_i$ e $\bigcap_{\gamma\in\Gamma} A_\gamma = \bigcap_{i=1}^{\infty} A_i$.

Exemplo 2.21. Seja $A_i = \{i\}$, $i \in \mathbb{N}-\{0\}$. Temos que $A = (A_i)_{i\in\mathbb{N}} = \{\{1\}, \{2\}, \{3\}, \ldots\}$ é uma família de conjuntos unitários.

Exemplo 2.22. Seja $A_i \cap \mathbb{N}$, with $A_i = [i, \infty)$, $i \in \mathbb{N} - \{0\}$.

Assim, $A = (A_i)_{i\in\mathbb{N}} = \{\{1, 2, 3, \ldots\}, \{2, 3, 4, \ldots\}, \{3, 4, 5, \ldots\}, \ldots\}$. Observe que para $i < j$, temos que $A_j \subsetneq A_i$. Neste caso, dizemos que A é uma família decrescente de conjuntos.

Exemplo 2.23. Para cada $i \in \mathbb{N} - \{0\}$, seja $A_i = \{i, i+1, \ldots, 2i-1\}$. Encontre $\bigcup_{i=1}^{n} A_i$.

Note que, cada inteiro entre 1 e $2n-1$ pertence a algum A_i da família e nenhum outro inteiro pertence a estes A_i. Logo $\bigcup_{i=1}^{n} A_i = \{1, 2, 3, \ldots, 2n-1\}$.

Teorema 2.24. Seja $\{A_\gamma;\ \gamma \in \Gamma\}$ uma família vazia de subconjuntos de um conjunto U, ou seja, $\Gamma = \emptyset$. Então

(a) $\bigcup_{\gamma\in\Gamma} A_\gamma = \emptyset$.

(b) $\bigcap_{\gamma\in\Gamma} A_\gamma = U$.

Prova: (a) Note que mostrar que $\bigcup_{\gamma\in\emptyset} A_\gamma = \emptyset$ é equivalente a mostrar que para todo

$x \in U$, temos $x \notin \bigcup_{\gamma \in \emptyset} A_\gamma$. Para $x \in U$, temos que

$$\begin{aligned}
x \notin \bigcup_{\gamma \in \emptyset} A_\gamma &\iff \sim \left(x \in \bigcup_{\gamma \in \emptyset} A_\gamma \right), && \text{por notação} \\
&\iff \sim (x \in A_\gamma, \text{ para algum } \gamma \in \emptyset), && \text{pela definição de } \cup \\
&\iff (x \notin A_\gamma, \text{ para todo } \gamma \in \emptyset), && \text{pela negação} \\
&\iff (\gamma \in \emptyset \longrightarrow x \notin A_\gamma)
\end{aligned}$$

e esta última proposição é verdade para todo $x \in U$, pois $\gamma \in \emptyset$ é uma contradição. Isso completa a demonstração da parte (a).

(b) Temos que mostrar que para todo $x \in U$, temos $x \in \bigcap_{\gamma \in \emptyset} A_\gamma$. Observe que por definição $x \in \bigcap_{\gamma \in \emptyset} A_\gamma \iff (x \in A_\gamma, \ \forall \gamma \in \emptyset)$ que é equivalente à proposição $(\gamma \in \emptyset \longrightarrow x \in A_\gamma)$, que, como visto na demonstração do ítem (a), é verdadeira para todo $x \in U$. ■

Os próximos dois teoremas generalizam, para uma família qualquer, resultados mostrados.

Teorema 2.25 (Leis de Morgan Generalizadas)**.** Seja $\{A_\gamma; \ \gamma \in \Gamma\}$ uma família arbitrária de subconjuntos de um conjunto U. Então

(a) $\left(\bigcup_{\gamma\in\Gamma} A_\gamma\right)^c = \bigcap_{\gamma\in\Gamma} A_\gamma^c$.

(b) $\left(\bigcap_{\gamma\in\Gamma} A_\gamma\right)^c = \bigcup_{\gamma\in\Gamma} A_\gamma^c$.

Prova: (a) Para todo $x \in U$, temos

$$\begin{aligned}
x \in \left(\bigcup_{\gamma\in\Gamma} A_\gamma\right)^c &\iff \sim \left(x \in \bigcup_{\gamma\in\Gamma} A_\gamma\right), && \text{definição de complementar} \\
&\iff \sim (\exists\, \gamma \in \Gamma)(x \in A_\gamma), && \text{definição de união} \\
&\iff (\forall\, \gamma \in \Gamma)(x \notin A_\gamma), && \text{negação} \\
&\iff (\forall\, \gamma \in \Gamma)(x \in A_\gamma^c), && \text{definição de complementar} \\
&\iff x \in \bigcap A_\gamma^c. && \text{definição de } \cap
\end{aligned}$$

Assim, por definição de igualdade de conjuntos temos a igualdade do ítem (a). A demonstração da igualdade do ítem (b) fica como exercício. ■

Teorema 2.26 (Leis Distributivas Generalizadas)**.** Sejam A um conjunto e $\mathcal{C} = \{B_\gamma;\ \gamma \in \Gamma\}$ uma família de conjuntos. Então

(a) $A \cap \left(\bigcup_{\gamma\in\Gamma} B_\gamma\right) = \bigcup_{\gamma\in\Gamma}(A \cap B_\gamma)$.

(b) $A \cup \left(\bigcap_{\gamma\in\Gamma} B_\gamma\right) = \bigcap_{\gamma\in\Gamma}(A \cup B_\gamma)$.

Prova: Vamos provar a igualdade do ítem (a), a outra fica como exercício. Um elemento x está no conjunto $A\cap\left(\bigcup_{\gamma\in\Gamma} B_\gamma\right)$ se, e somente se $x \in A$ e $x \in \bigcup_{\gamma\in\Gamma} B_\gamma$, pela definição de $\cap$. Agora, da definição de união de uma família qualquer de conjuntos, temos que esta proposição é equivalente a $x \in A$ e $x \in B_\gamma$, para algum $\gamma \in \Gamma$, que pode ser expressa como $x \in A\cap B_\gamma$, para algum $\gamma \in \Gamma$, a qual, por definição de $\cup$ é precisamente $x \in \bigcup_{\gamma\in\Gamma}(A \cap B_\gamma)$, o que mostra (a) pela definição de igualdade de conjunto. ■

2.3 O Produto Cartesiano de Dois Conjuntos

Sejam A e B dois conjuntos arbitrários. Para $a \in A$ e $b \in B$, utilizando o axioma da especificação, podemos construir o conjunto

$$\{a, b\} = \{x;\ x = a \text{ ou } x = b\}.$$

Note que, como conjuntos $\{a, b\} = \{b, a\}$.

Agora, queremos definir a noção de **par ordenado**, ou seja, um conjunto com dois elementos dados, onde possamos dizer qual é o primeiro e qual é o segundo elemento. Para tanto, precisamos da certeza que este par é também um elemento. Isso é garantido pelo seguinte axioma.

Axioma do par: *Para dois conjuntos quaisquer existe um conjunto ao qual ambos pertencem.*

Este axioma garante a existência do conjunto definido a seguir:

Definição 2.27. O **par ordenado** de a e b, denotado por (a, b), com primeira coordenada a e segunda coordenada b é o conjunto

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

Dados dois conjuntos A e B, o **produto cartesiano** de A e B, denotado por $A \times B$, é o conjunto

$$A \times B = \{x;\ x = (a, b) \text{ para algum } a \in A \text{ e algum } b \in B\}.$$

Note que em geral $(a, b) \neq (b, a)$ e $A \times B \neq B \times A$.

Vejamos como esta nova operação entre conjuntos se comporta com relação às outras definidas anteriormente.

Teorema 2.28. Sejam A, B e C conjuntos quaisquer. Então temos:

(a) $A \times \emptyset = \emptyset \times A = \emptyset$.

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(c) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(d) $A \times (B - C) = (A \times B) - (A \times C)$.

Prova: (a) Pela definição de produto cartesiano, temos

$$A \times \emptyset = \{(a, b);\ a \in A \text{ e } b \in \emptyset\}.$$

Como não existe $b \in \emptyset$, temos que não existe par ordenado cuja segunda coordenada seja b, assim $A \times \emptyset = \emptyset$. A outra igualdade é análoga.

(b) Aqui, podemos assumir que os 3 conjuntos são diferentes do vazio, pois, caso contrário, a demonstração segue facilmente do ítem (a). Para $a \in A$ e $x \in (B \cap C)$, temos

$$\begin{array}{lll}
 & (a, x) \in A \times (B \cap C) & \\
\iff & (a \in A) \wedge (x \in B \cap C), & \text{def. de prod. cartesiano} \\
\iff & (a \in A) \wedge (x \in B \wedge x \in C), & \text{def. de } \cap \\
\iff & (a \in A) \wedge (x \in B) \wedge (x \in C), & \text{associatividade do } \wedge \\
\iff & (a \in A) \wedge (x \in B) \wedge (a \in A) \wedge (x \in C), & \text{canc. e comut. do } \wedge \\
\iff & [(a \in A) \wedge (x \in B)] \wedge [(a \in A) \wedge (x \in C)], & \text{associatividade do } \wedge \\
\iff & [(a, x) \in A \times B] \wedge [(a, x) \in A \times C], & \text{def. de prod. cartesiano} \\
\iff & (a, x) \in (A \times B) \cap (A \times C), & \text{def. de } \cap
\end{array}$$

o que mostra a igualdade do ítem (b).

As demonstrações de (c) e (d) ficam como exercício. ■

2.4 Exercícios

1. Determine se as afirmações abaixo são verdadeiras ou falsas, justificando.

   (a) $3 = \{3\}$.

   (b) $5 \in \{\{5\}\}$.

   (c) $4 \in \{\{4\}, 4\}$.

   (d) $\emptyset \in \{3\}$.

   (e) $\{2, 8\} \subseteq \{2, 8, 9\}$.

   (f) $\{3, 4\} \subseteq \{\{3, 4\}, \{5, 6\}\}$.

   (g) $(\forall\, A)(\forall\, B)(\forall\, C)(A \cap B \cap C = A \cap B \cap (C \cup B))$.

   (h) $(\forall\, A)(\forall\, B)(\forall\, C)((A \cup B) - C = A \cup (B - C))$.

   (i) $(\forall\, A)(\forall\, B)(\forall\, C)(A \cup B = A \cup C \Longrightarrow B = C)$.

   (j) $(\{\emptyset\} \subseteq \wp(A)), (\forall A)$.

   (k) $(\{\emptyset\} \in \wp(A)), (\forall A)$.

   (l) $\wp(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

2. Mostre que se A é um conjunto finito com n elementos, então $\wp(A)$ é finito e tem 2^n elementos. Mostre também que A é infinito se, e somente se $\wp(A)$ é infinito.

3. Sejam A e B conjuntos. Determine se cada uma das afirmações abaixo são verdadeiras. Se sim, mostre, caso contrário, dê um contra exemplo.

   (a) $x \in A$ e $A \in B \Longrightarrow x \in B$.

   (b) $x \in A$ e $A \subseteq B \Longrightarrow x \in B$.

   (c) $x \in A$ e $A \not\subseteq B \Longrightarrow x \notin B$.

   (d) $A \subseteq B$ e $x \notin B \Longrightarrow x \notin A$.

   (e) $A \subseteq B \Longleftrightarrow \wp(A) \subseteq \wp(B)$.

4. Para A, B e C conjuntos dados, mostre que:

   (a) $C - (A \cup B) = (C - A) \cap (C - B)$.

   (b) $C - (A \cap B) = (C - A) \cup (C - B)$.

   (c) $A = B \Longleftrightarrow \wp(A) = \wp(B)$.

(d) $A \times (B - C) = (A \times B) - (A \times C)$.

(e) Se $B \subseteq A$, então $A \times A - B \times B = [(A - B) \times A] \cup [A \times (A - B)]$.

(f) $A \cap B = A \iff A \cup B = B$.

(g) Se $A \subseteq C$ e $B \subseteq C$, então $A \subseteq B \iff (C - B) \subseteq (C - A)$.

(h) $\bigcap_{X \in \wp(A)} X = \emptyset$ e $\bigcup_{X \in \wp(A)} X = A$.

5. Sejam A, B e C conjuntos. Para cada uma das afirmações abaixo, mostre ou dê um contra-exemplo:

(a) $(A - B) \cup C = (A \cup B \cup C) - (A \cap B)$.

(b) $(A \cup C) - B = (A - B) \cup (C - B)$.

(c) $(A \cup B) - (A \cap B \cap C) = [A - (B \cap C)] \cup [B - ((A \cap C))]$.

(d) $\wp(A \cup B) = \wp(A) \cup \wp(B)$.

(e) $\wp(A \cap B) = \wp(A) \cap \wp(B)$.

(f) $A \subseteq C$ e $B \subseteq C \Longrightarrow (A \cup B) \subseteq C$.

(g) $A \subseteq B$ e $A \subseteq C \Longrightarrow A \subseteq B \cap C$.

6. Para conjuntos A e B, definimos a **diferença simétrica** de A e B, e denotamos por $A \triangle B$, como sendo o conjunto $A \triangle B = (A \cup B) - (A \cap B)$. Mostre que:

(a) $A \triangle B = (A - B) \cup (B - A)$.

(b) *Comutativa* - $A \triangle B = B \triangle A$.

(c) *Associativa* - $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

(d) *Elemento Neutro* - Existe um conjunto Φ tal que, para todo conjunto A tem-se que $A \triangle \Phi = A$.

(e) *Elemento Inverso* - Para cada conjunto A, existe um conjunto B tal que $A \triangle B = \Phi$.

(f) Mostre que $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$, para quaisquer conjuntos A, B e C.

7. Sejam A, B e E conjuntos tais que $E \neq \emptyset$. Mostre que se $A \times E = B \times E$, então $A = B$.

8. Sejam A e B conjuntos tais que $A \nsubseteq B$. Suponha que E seja um conjunto tal que $A \times E = B \times E$. Mostre que $E = \emptyset$.

9. Em cada um dos casos abaixo, considere a família infinita de conjuntos $\{B_i;\ i \in \mathbb{N} - \{0\}\}$ e determine $\bigcup_{i=1}^{+\infty} B_i$ e $\bigcap_{i=1}^{+\infty} B_i$.

   (a) $B_i = \{0, 1, 2, 3, \ldots, 2i\}$.

   (b) $B_i = \{i - 1, i, i + 1\}$.

   (c) $B_i = \left[\frac{3}{i}, \frac{5i+2}{i}\right] \bigcup \{10 + i\}$.

   (d) $B_i = \left[-1, 3 + \frac{1}{i}\right] \bigcup \left[5, \frac{5i+1}{i}\right]$.

10. Sejam I e J conjuntos tais que $J \subseteq I$ e $(A_i)_{i \in I}$ uma família indexada de conjuntos. Mostre que:

    (a) $\bigcup_{j \in J} A_j \subseteq \bigcup_{i \in I} A_i$. (b) $\bigcap_{i \in I} A_i \subseteq \bigcap_{j \in J} A_j$.

11. Determine:

    (a) $\bigcup_{n=1}^{+\infty} [-1 + 1/n, 1 - 1/n]$.

    (b) $\bigcap_{n=1}^{+\infty} (-1 - 1/n, 1 + 1/n)$.

    (c) $\bigcap_{n=1}^{+\infty} (-1/n, 1/n)$.

12. Sejam A um conjunto e $\mathcal{C} = \{B_\gamma;\ \gamma \in \Gamma\}$ uma família de conjuntos. Mostre que:

    (a) $A \cap \left(\bigcup_{\gamma \in \Gamma} B_\gamma\right) = \bigcup_{\gamma \in \Gamma} (A \cap B_\gamma)$.

    (b) $A \cup \left(\bigcap_{\gamma \in \Gamma} B_\gamma\right) = \bigcap_{\gamma \in \Gamma} (A \cup B_\gamma)$.

3
Relações

3.1 Definições e Exemplos

Utilizando pares ordenados, podemos estabelecer a teoria matemática das relações através da linguagem de conjuntos.

Começamos considerando o conjunto $A \times B$, onde A é o conjunto das mulheres e B é o conjunto dos homens. Quando falamos "Maria é esposa de João" estamos dizendo que Maria está relacionada com João pela relação "ser esposa de", ou seja, o par ordenado (a, b), onde $a =$ Maria e $b =$ João, pertencem à relação. Note que o par (b, a) não pertence à relação, pois João não é esposa de Maria. Se a relação fosse "ser casado com", então ambos os pares estariam na relação. Formalmente temos:

Definição 3.1. Uma **relação entre dois conjuntos** A e B, denotada por $\mathcal{R}(A, B)$, ou simplesmente por $\mathcal{R}$, é um subconjunto de $A \times B$.

Se um par $(a, b) \in \mathcal{R}$, dizemos que a **está relacionado com** b**, pela relação** $\mathcal{R}$ e escrevemos $a\mathcal{R}b$.

Se $A = B$, então $\mathcal{R}(A, A)$ é dita ser uma **relação sobre um conjunto** A ou uma **relação em** A.

Se $\mathcal{R}(A, B)$ é uma relação em $A \times B$, dizemos que $\mathcal{R}^{-1} = \{(b, a) \in B \times A : a\mathcal{R}b\}$ é a **relação inversa** de $\mathcal{R}$.

Como conjuntos, há duas maneiras de representar uma relação, uma é listando os seus elementos e a outra é definindo uma regra, na qual escolhemos os pares ordenados

que satisfazem esta regra.

Exemplo 3.2. Exemplos de relações:

(1) Sejam $A = \{1, 2, 3\}$ e $B = \{a, b, c, d\}$. Definimos, a seguir 3 relações:
$\mathcal{R}_1 = \{(1, a), (1, b), (3, c)\}$
$\mathcal{R}_2 = \{(2, a), (2, b), (1, a), (1, b), (3, a), (3, b)\}$
$\mathcal{R}_3 = \emptyset$.

(2) Seja $A = \{a, b, c\}$. Definimos, sobre A as relações:
$\mathcal{R}_1 = \{(a, a), (b, b), (c, c)\}$
$\mathcal{R}_2 = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b), (c, c)\}$
$\mathcal{R}_3 = A \times A$.

(3) Seja $A = \mathbb{Z}$. Definimos, sobre A as relações:
$\mathcal{R}_1 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ a < b\}$
$\mathcal{R}_2 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ a \mid b\}$.

(4) Seja $A = \mathbb{Z}$. Para as relações definidas no exemplo anterior, temos:
$\mathcal{R}_1^{-1} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ a > b\}$
$\mathcal{R}_2^{-1} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ b \mid a\}$.

Podemos visualizar algumas propriedades de uma relação através de sua representação gráfica. Para vermos isso, necessitamos definir algumas noções.

Definição 3.3. Seja $\mathcal{R}$ uma relação em $A \times B$. O **domínio** de $\mathcal{R}$, denotado por $\mathrm{Dom}(\mathcal{R})$, é o subconjunto de A dado por

$$\mathrm{Dom}(\mathcal{R}) = \{a \in A; a\mathcal{R}b \text{ para algum } b \in B\}.$$

A **imagem** de $\mathcal{R}$, denotado por $\mathrm{Im}(\mathcal{R})$, é o subconjunto de B dado por

$$\mathrm{Im}(\mathcal{R}) = \{b \in B; a\mathcal{R}b \text{ para algum } a \in A\}.$$

Podemos colocar os pares ordenados da relação $\mathcal{R}$ num diagrama coordenado de $A \times B$ e o conjuntos destes pontos é dito ser o **gráfico ou diagrama cartesiano** de $\mathcal{R}$

Outro tipo de representação geométrica de uma relação, muito usado quando o conjunto A é finito, é o **diagrama de setas**, onde representamos os elementos de A

por pontos e a relação $\mathcal{R}$ por setas ligando estes pontos, ou seja, se $(a, b) \in \mathcal{R}$, então desenhamos uma seta com início no ponto a e término no ponto b. Por exemplo, se $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b), (c, c)\}$, então o diagrama de setas de $\mathcal{R}$ é

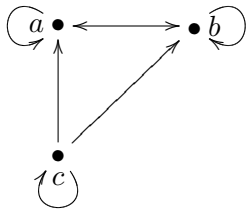


Figura 3.1: Diagrama de setas da relação $\mathcal{R}$ acima.

Daremos a seguir as propriedades mais importantes que uma relação $\mathcal{R}$ sobre um conjunto A poderá satisfazer.

Definição 3.4. Seja $\mathcal{R}$ uma relação sobre um conjunto A. Então dizemos que:

- $\mathcal{R}$ é **reflexiva** se a condição $(\forall\, x \in A)(x\mathcal{R}x)$ for verdadeira, ou seja, se para todo $x \in A,\ (x, x) \in \mathcal{R}$.
- $\mathcal{R}$ é **simétrica** se a condição $(\forall\, x,\, y \in A)(x\mathcal{R}y \longrightarrow y\mathcal{R}x)$ for verdadeira, ou seja, se para todo $x,\, y \in A$, se $(x, y) \in \mathcal{R}$, então $(y, x) \in \mathcal{R}$.
- $\mathcal{R}$ é **transitiva** se a condição $(\forall\, x,\, y,\, z \in A)(x\mathcal{R}y \wedge y\mathcal{R}z \longrightarrow x\mathcal{R}z)$ for verdadeira, ou seja, se para todo $x,\, y,\, z \in A$, se $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$, então $(x, z) \in \mathcal{R}$.
- $\mathcal{R}$ é **anti-simétrica** se a condição $(\forall\, x,\, y \in A)(x\mathcal{R}y \wedge y\mathcal{R}x \longrightarrow x = y)$ for verdadeira, ou seja, se para todo $x,\, y \in A$, se $(x, y) \in \mathcal{R}$ e $(y, x) \in \mathcal{R}$, então $x = y$.

Exemplo 3.5. Exemplos de relações satisfazendo tais propriedades:

(1) Seja A um conjunto qualquer. A relação $\Delta = \{(x, x);\, x \in A\}$ é uma relação sobre A que é reflexiva, simétrica, anti-simétrica e transitiva. Esta é chamada a relação identidade ou a diagonal.

(2) Seja A um conjunto qualquer. A relação $A \times A$ é uma relação sobre A que é reflexiva, simétrica e transitiva. Não é anti-simétrica.

(3) Para $A = \{a, b, c\}$, temos: $\mathcal{R}_1 = \{(a, a), (b, b), (c, c), (a, b)\}$ é uma relação reflexiva, anti-simétrica e transitiva. Não é simétrica. $\mathcal{R}_2 = \{(a, a), (b, b), (a, b), (b, a)\}$ é

uma relação simétrica e transitiva. Não é reflexiva e nem anti-simétrica. $\mathcal{R}_3 = \{(a,a),(b,b),(a,b),(b,a),(b,c)\}$ é uma relação que não é simétrica, nem transitiva, nem reflexiva e nem anti-simétrica.

(4) Para $A = \mathbb{N}$, temos: $\mathcal{R} = \{(x,y) \in \mathbb{N} \times \mathbb{N}; x \text{ é um divisor de } y\}$ é uma relação reflexiva, anti-simétrica e transitiva. Não é simétrica.

(5) Para $A = \mathbb{Z}$, temos: $\mathcal{R} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}; x - y \text{ é múltiplo de } 3\}$ é uma relação reflexiva, simétrica e transitiva. Não é anti-simétrica.

(6) Seja A uma família de conjuntos. Para X, $Y \in A$, a relação "X está contido em Y" é uma relação reflexiva, anti-simétrica e transitiva. Não é simétrica.

(7) Seja A o conjunto das proposições. Para p, $q \in A$, a relação "se p então q" é uma relação reflexiva e transitiva. Não é simétrica e nem anti-simétrica.

Observação 3.6. Se A é um conjunto finito, com "poucos" elementos, podemos visualizar se a relação satisfaz uma ou mais das propriedades definida acima, através do diagrama de flechas, da seguinte maneira:

(1) Reflexiva - Em cada ponto do diagrama deve ter um laço.

Figura 3.2: Exemplo e Contra-exemplo.

(2) Simétrica - Toda flecha deve ter duas "pontas".

Figura 3.3: Exemplo e Contra-exemplo.

(3) Anti-simétrica - Não há flechas de duas pontas.

Figura 3.4: Exemplo e Contra-exemplo.

(4) Transitiva - Para todo par de flechas consecutivas existe uma flecha com origem na origem da primeira e extremidade na extremidade da segunda.

Figura 3.5: Exemplo e Contra-exemplo.

3.2 Relações de Equivalências e Partições

Um tipo de relação muito importante na matemática moderna, que aparece em todas as áreas de estudo são as relações de equivalência.

Definição 3.7. Uma relação $\mathcal{R}$ sobre um conjunto A é dita ser uma **relação de equivalência sobre** A se $\mathcal{R}$ for reflexiva, simétrica e transitiva.

Exemplo 3.8. A relação diagonal definida no exemplo 3.5(1) é uma relação de equivalência sobre A. Esta é a "menor" relação de equivalência sobre A e a relação definida no exemplo 3.5(2) é a "maior" relação de equivalência sobre A. Também como visto acima, a relação $\mathcal{R}$ definida no exemplo 3.5(5) é uma relação de equivalência sobre o conjunto dos números inteiros.

Definição 3.9. Seja $\mathcal{R}$ uma relação de equivalência sobre um conjunto não vazio A. Para cada $a \in A$, o subconjunto de A definido por $\overline{a} = \{x \in A;\ x\mathcal{R}a\}$ é dito ser a **classe**

de equivalência determinada pelo elemento a **módulo** $\mathcal{R}$. Observe que o conjunto $\overline{a}$ é um subconjunto de A consistindo de todos os elementos de A aos quais a está relacionado.

O conjunto das classes de equivalência módulo $\mathcal{R}$ será indicado por $A/\mathcal{R}$ e chamado de **conjunto quociente de** A **por** $\mathcal{R}$.

Note que se $\mathcal{R}$ é uma relação de equivalência sobre um conjunto não vazio A, então para todo $a \in A$, temos $a \in \overline{a}$, ou seja, cada classe de equivalência é um subconjunto não vazio de A.

Exemplo 3.10. Considere a relação de equivalência $\mathcal{R}$ definidas no exemplo 3.5(5), ou seja, $A = \mathbb{Z}$ e $\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; x - y \text{ é múltiplo de } 3\}$.

Para $0 \in \mathbb{Z}$, temos

$$\begin{aligned} \overline{0} &= \{x \in \mathbb{Z};\ x \text{ é múltiplo de } 3\} \\ &= \{x \in \mathbb{Z};\ x = 3k, \text{ para algum } k \in \mathbb{Z}\} \\ &= 3\mathbb{Z}. \end{aligned}$$

Para $1 \in \mathbb{Z}$, temos

$$\begin{aligned} \overline{1} &= \{x \in \mathbb{Z};\ x - 1 \text{ é múltiplo de } 3\} \\ &= \{x \in \mathbb{Z};\ x = 3k + 1, \text{ para algum } k \in \mathbb{Z}\} \\ &= 3\mathbb{Z} + 1. \end{aligned}$$

Para $2 \in \mathbb{Z}$, temos

$$\begin{aligned} \overline{2} &= \{x \in \mathbb{Z};\ x - 2 \text{ é múltiplo de } 3\} \\ &= \{x \in \mathbb{Z};\ x = 3k + 2, \text{ para algum } k \in \mathbb{Z}\} \\ &= 3\mathbb{Z} + 2. \end{aligned}$$

Para $3 \in \mathbb{Z}$, temos

$$\begin{aligned} \overline{3} &= \{x \in \mathbb{Z};\ x - 3 \text{ é múltiplo de } 3\} \\ &= \{x \in \mathbb{Z};\ x = 3k + 3 = 3(k + 1), \text{ para algum } k \in \mathbb{Z}\} \\ &= 3\mathbb{Z} \\ &= \overline{0}. \end{aligned}$$

Veremos no próximo teorema que de fato $\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1}, \overline{2}\}$.

Exemplo 3.11. Considere a relação de equivalência

$$\mathcal{R} = \{(1,1),(2,2),(3,3),(4,4),(5,5),(2,5),(5,2),(3,5),(5,3),(2,3),(3,2)\}$$

(mostre este fato).

Vamos calcular $A/\mathcal{R}$:

$$\overline{1} = \{1\};\ \overline{2} = \{2,3,5\};\ \overline{3} = \{2,3,5\};\ \overline{4} = \{4\};\ \overline{5} = \{2,3,5\}.$$

Portanto, $A/\mathcal{R} = \{\{1\},\{4\},\{2,3,5\}\}$.

Com relação às classes de equivalência temos:

Teorema 3.12. Sejam $\mathcal{R}$ uma relação de equivalência sobre um conjunto não vazio A e a, $b \in A$. As seguintes proposições são equivalentes:

$$(a)\quad a\mathcal{R}b \qquad (b)\quad a \in \overline{b} \qquad (c)\quad b \in \overline{a} \qquad (d)\quad \overline{a} = \overline{b}.$$

Prova: (a) $\Longleftrightarrow$ (b): Decorre imediatamente da definição de classe de equivalência.
(b) $\Longrightarrow$ (c): $a \in \overline{b} \Longrightarrow a\mathcal{R}b$, pela definição de classe,
$\Longrightarrow b\mathcal{R}a$, pois $\mathcal{R}$ é simétrica,
$\Longrightarrow b \in \overline{a}$, pela definição de classe.
(c) $\Longrightarrow$ (d): Note que $\overline{a}$ e $\overline{b}$ são dois conjuntos, assim, mostrar que $\overline{a} = \overline{b}$ é equivalente a mostrar que $\overline{a} \subseteq \overline{b}$ e $\overline{b} \subseteq \overline{a}$. Mostremos que $\overline{a} \subseteq \overline{b}$; a outra inclusão é análoga. Para $x \in \overline{a}$, temos que $x\mathcal{R}a$ e, como por hipótese, $b \in \overline{a}$, temos também que $b\mathcal{R}a$. Como $\mathcal{R}$ é simétrica, obtemos $x\mathcal{R}a$ e $a\mathcal{R}b$, o que implica pela transitividade de $\mathcal{R}$ que $x\mathcal{R}b$, ou seja, $x \in \overline{b}$.
(d) $\Longrightarrow$ (a): Seja $x \in \overline{a} = \overline{b}$. Então, pela definição de classe, temos que $x\mathcal{R}a$ e $x\mathcal{R}b$. Agora, da propriedade simétrica e transitiva de $\mathcal{R}$, obtemos $a\mathcal{R}b$. ■

Mostremos agora a afirmação feita no final do exemplo anterior, ou seja, para $A = \mathbb{Z}$ e $\mathcal{R} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}; x - y \text{ é múltiplo de } 3\}$, temos $\mathbb{Z}/\mathcal{R} = \{\overline{0},\overline{1},\overline{2}\}$.

É obvio que $\mathbb{Z}/\mathcal{R} \supseteq \{\overline{0},\overline{1},\overline{2}\}$. Agora, se $\overline{a} \in \mathbb{Z}/\mathcal{R}$, então dividindo a por 3, obtemos que $a = 3q + r$, com $r = 0, 1$ ou 2. Neste caso, temos claramente que $r \in \overline{a}$ e, pelo teorema anterior, temos $\overline{a} = \overline{r}$, ou seja $\mathbb{Z}/\mathcal{R} \subseteq \{\overline{0},\overline{1},\overline{2}\}$.

Relações de equivalências estão diretamente relacionadas com a noção de partição de um conjunto.

Definição 3.13. Seja A um conjunto não vazio. Dizemos que uma família $\mathcal{F}$ de subconjuntos não vazios de A é uma **partição** de A se as seguintes afirmações são verdadeiras:

(a) dois elementos quaisquer de $\mathcal{F}$ ou são iguais ou são disjuntos;

(b) a união dos elementos de $\mathcal{F}$ é igual a A.

Exemplo 3.14. Exemplos de partições:

(1) A família $\mathcal{F} = \{\{1\}, \{2\}, \{3, 4\}\}$ é uma partição do conjunto $A = \{1, 2, 3, 4\}$.

(2) Seja $A = \mathbb{Z}$. A família $\mathcal{F} = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\}$ é uma partição de A.

(3) A família $\mathcal{F} = \{(-\infty, -1), [-1, 1], (1, +\infty)\}$ é uma partição de $\mathbb{R}$.

O próximo teorema nos mostra como uma relação de equivalência determina uma partição de um conjunto.

Teorema 3.15. Se $\mathcal{R}$ é uma relação de equivalência sobre um conjunto não vazio A, então $A/\mathcal{R}$ é uma partição de A.

Prova: Pela definição de partição, temos que mostrar que cada elemento de $A/\mathcal{R}$ é não vazio e que valem as propriedades (a) e (b) da definição 3.13.

Para cada $\overline{a} \in A/\mathcal{R}$, como $\mathcal{R}$ é reflexiva, temos que $a \in \overline{a}$, o que mostra que $\overline{a} \neq \emptyset$.

Mostremos agora que vale a propriedade (a), ou seja, para cada $\overline{a}$ e $\overline{b}$ em $A/\mathcal{R}$, temos $\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$.

Suponhamos que $\overline{a} \cap \overline{b} \neq \emptyset$ e seja $x \in \overline{a} \cap \overline{b}$. Então $x \in \overline{a}$ e $x \in \overline{b}$. Da definição de classes de equivalência, temos que $x\mathcal{R}a$ e $x\mathcal{R}b$. Agora, do fato de $\mathcal{R}$ ser simétrica e transitiva, obtemos que $a\mathcal{R}b$. Das equivalências do teorema anterior temos $\overline{a} = \overline{b}$, o que mostra (a).

Para mostrar que vale a propriedade (b), temos que mostrar que $\bigcup_{a \in A} \overline{a} = A$, ou seja que $\bigcup_{a \in A} \overline{a} \subseteq A$ e $\bigcup_{a \in A} \overline{a} \supseteq A$.

A inclusão $\bigcup_{a \in A} \overline{a} \subseteq A$ é imediata, pois $\overline{a} \subseteq A$ para cada $a \in A$.

Agora, seja $x \in A$. Como $x\mathcal{R}x$, temos que $x \in \overline{x}$, o que implica que $x \in \bigcup_{a \in A} \overline{a}$. Portanto $\bigcup_{a \in A} \overline{a} \supseteq A$. ■

Agora, vejamos que toda partição de um conjunto é do tipo descrita no teorema anterior.

Teorema 3.16. Seja A um conjunto não vazio. Se $\mathcal{F}$ é uma partição de A, então existe uma relação de equivalência $\mathcal{R}$ sobre A tal que $A/\mathcal{R} = \mathcal{F}$.

Prova: Para todo $a, b \in A$, definimos $\mathcal{R}$ por:

$$a\mathcal{R}b \iff \text{existe } X \in \mathcal{F} \text{ tal que } a, b \in X.$$

Mostremos que $\mathcal{R}$ é uma relação de equivalência.

(i) Para cada $a \in A$, desde que $\bigcup \mathcal{F} = A$, existe um $X \in \mathcal{F}$ tal que $a \in X$. Assim, $a\mathcal{R}a$, ou seja, $\mathcal{R}$ é reflexiva.

(ii) Para a, $b \in A$, se $a\mathcal{R}b$, então pela definição de $\mathcal{R}$, existe um elemento $X \in \mathcal{F}$, tal que a, $b \in X$, o que claramente implica que $b\mathcal{R}a$. Logo, $\mathcal{R}$ é simétrica.

(iii) Se a, b, $c \in A$ são tais que $a\mathcal{R}b$ e $b\mathcal{R}c$, então existem X, $Y \in \mathcal{F}$ tais que a, $b \in X$ e b, $c \in Y$. Assim, $b \in X \cap Y$, ou seja, $X \cap Y \neq \emptyset$. Como $\mathcal{F}$ é uma partição, temos que $X = Y$ e então a, $c \in X = Y$, o que mostra que $a\mathcal{R}c$. Logo $\mathcal{R}$ é transitiva.

Mostremos agora que $A/\mathcal{R} = \mathcal{F}$. Dado $a \in A$, temos que existe um único $X \in \mathcal{F}$, tal que $a \in X$, onde a unicidade segue da propriedade (a) da definição de $\mathcal{F}$. Da definição de $\mathcal{R}$ é claro que $\overline{a} = X$, o que implica que $A/\mathcal{R} \subseteq \mathcal{F}$.

Por outro lado, para cada $X \in \mathcal{F}$, desde que $X \neq \emptyset$, temos que existe $a \in X$. Claramente $X = \overline{a}$, o que mostra que $A/\mathcal{R} \supseteq \mathcal{F}$. ■

Exemplo 3.17. Dada a partição $\mathcal{F} = \{\{a, b\}, \{c\}, \{d, e, f\}\}$ do conjunto $A = \{a, b, c, d, e, f\}$, temos a relação de equivalência associada

$$\mathcal{R} = \{(a,a), (a,b), (b,a), (b,b), (c,c), (d,d), (d,e), (d,f), \\ (e,d), (f,d), (e,e), (e,f), (f,e), (f,f)\}.$$

3.3 Relações de Ordem

Definição 3.18. Uma relação $\mathcal{R}$ sobre um conjunto não vazio A é dita ser uma **relação de ordem** sobre A se $\mathcal{R}$ é reflexiva, anti-simétrica e transitiva.

Se existe uma relação de ordem sobre o conjunto A, dizemos que A é um conjunto **parcialmente ordenado** ou, simplesmente **ordenado**.

Dada uma relação de ordem sobre um conjunto A, dizemos que os elementos a, $b \in A$ são **comparáveis** mediante $\mathcal{R}$ se $a\mathcal{R}b$ ou $b\mathcal{R}a$.

Se quaisquer dois elementos de A são comparáveis mediante $\mathcal{R}$, então dizemos que $\mathcal{R}$ é uma **ordem total** sobre A e, neste caso, dizemos que A é um conjunto **totalmente ordenado**.

Em uma relação de ordem, se $a\mathcal{R}b$, também usaremos a notação $a \prec b$ que lemos "a precede b na relação $\mathcal{R}$".

Exemplo 3.19. Exemplos de relações de ordem:

(1) A relação $\mathcal{R} = \{(a,a),(b,b),(c,c),(a,b),(a,c),(b,c)\}$ é uma relação de ordem total sobre $A = \{a,b,c\}$. Faça o diagrama de setas desta relação e observe que não há dois pontos que não estejam ligados por uma flecha. Isso deve ocorrer sempre que a ordem for total.

(2) A relação $\mathcal{R}$ definida sobre $\mathbb{R}$ por

$$x\mathcal{R}y \iff x \leq y$$

é uma ordem total sobre $\mathbb{R}$ chamada a ordem usual.

(3) A relação $\mathcal{R}$ definida sobre $\mathbb{N}$ por

$$x\mathcal{R}y \iff x \text{ divide } y$$

é uma relação de ordem sobre $\mathbb{N}$, que não é total.

(4) A relação de inclusão sobre uma família de subconjuntos de um dado conjunto é uma relação de ordem, que em geral não é total.

Definição 3.20. Sejam A um conjunto ordenado pela relação de ordem $\prec$ e $S \subseteq A$, um subconjunto não vazio. Dizemos que:

(a) Um elemento $L \in A$ é um **limite superior** de S se a seguinte proposição for verdadeira

$$(\forall\, x)(x \in S \longrightarrow x \prec L),$$

isto é, quando qualquer elemento de S precede L.

(b) Um elemento $l \in A$ é um **limite inferior** de S se a seguinte proposição for verdadeira

$$(\forall\, x)(x \in S \longrightarrow l \prec x),$$

isto é, quando l precede qualquer elemento de S.

(c) Um elemento $M \in S$ é um **máximo** de S se a seguinte proposição for verdadeira

$$(\forall\, x)(x \in S \longrightarrow x \prec M),$$

isto é, quando M é um limite superior de S e $M \in S$.

(d) Um elemento $m \in S$ é um **mínimo** de S se a seguinte proposição for verdadeira

$$(\forall\, x)(x \in S \longrightarrow m \prec x),$$

isto é, quando m é um limite inferior de S e $m \in S$.

(e) O **supremo** de S é o mínimo, caso exista, do conjunto dos limites superiores de S.

(f) O **ínfimo** de S é o máximo, caso exista, do conjunto dos limites inferiores de S.

Exemplo 3.21. Para $A = \mathbb{R}$ e $S = (0, 1]$, com a ordem usual, temos:

1. O conjunto dos limites superiores de S é $[1, +\infty)$.
2. O conjunto dos limites inferiores de S é $(-\infty, 0]$.
3. O máximo de S é 1.
4. S não tem mínimo.
5. O supremo de S é 1.
6. O ínfimo de S é 0.

Exemplo 3.22. Para $A = \{1, 2, 3, 4, 6, 9, 12, 18, 24, 36\}$, $S = \{2, 4, 6\}$ e a relação de ordem sendo a divisibilidade, temos:

1. O conjunto dos limites superiores de S é $\{12, 24, 36\}$.
2. O conjunto dos limites inferiores de S é $\{1, 2\}$.

3. S não tem máximo.

4. O mínimo de S é 2.

5. O supremo de S é 12.

6. O ínfimo de S é 2.

Observação 3.23. Frequentemente, representamos uma relação de ordem sobre um conjunto finito, com "poucos" elementos, através de um diagrama simplificado, onde omitimos as propriedades reflexiva e transitiva, para não sobrecarregar o diagrama de flechas e, se $a \prec b$, indicamos b numa posição relativamente acima de a. Tal diagrama é dito ser o **Diagrama de Hasse** da relação de ordem $\prec$. Por exemplo, o diagrama de Hasse da relação de ordem do exemplo 3.22 é

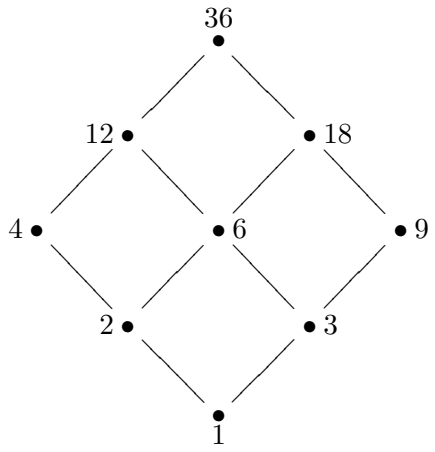


Figura 3.6: Diagrama de Hasse do Exemplo 3.22

Teorema 3.24. Seja S um subconjunto de um conjunto parcialmente ordenado A. Se existe um máximo (resp. mínimo) de S, então ele é único.

Prova: Vamos fazer a demonstração para a unicidade do máximo, o caso de mínimo é análogo.

Suponhamos que M_1 e M_2 são máximos de S. Temos então:

- M_1 é máximo e $M_2 \in S$, o que implica que $M_2 \prec M_1$.

- M_2 é máximo e $M_1 \in S$, o que implica que $M_1 \prec M_2$.

Como $\prec$ é anti-simétrica, temos que $M_1 = M_2$. ■

3.4 Funções

Aqui somente apresentaremos a definição de função usando a noção de relação. As propriedades e as noções de injetividade, sobrejetividade, bijetividade, função composta e função inversa serão assumidas conhecidas para o desenvolvimento dos próximos capítulos.

Normalmente, o que vemos como definição de função é:

> *Função é uma regra de correspondência que associa a cada elemento x de um certo conjunto (chamado de domínio da função) um único elemento y em um outro conjunto (chamado de contra-domínio da função).*

A definição formal de função usando conjuntos e a noção de relação é:

Definição 3.25. Sejam A e B conjuntos. Uma **função** de A em B é uma relação f de A em B satisfazendo as seguintes propriedades:

(a) $\text{Dom}(f) = A$.

(b) Se $x \in A$ e $y, z \in B$ são tais que $x\ f\ y$ e $x\ f\ z$, então $y = z$.

Escreveremos $f : A \to B$, para denotar que f é uma função de A em B.

3.5 Exercícios

1. Determine quais das propriedades: reflexiva, simétrica, transitiva, anti-simétrica são satisfeitas por cada uma das seguintes relações sobre o conjunto $\mathbb{R}$ dos números reais:

   (a) $\mathcal{R} = \{(x, y);\ y = 1/x\}$.
   (b) $\mathcal{R} = \{(x, y);\ \ |x - y| \leq 1\}$.
   (c) $\mathcal{R} = \{(x, y);\ y^2 = x^2\}$.
   (d) $\mathcal{R} = \{(x, y);\ \ x \neq y\}$.
   (e) $\mathcal{R} = \{(x, y);\ xy \geq 0\}$.

2. Dê um exemplo de uma relação $\mathcal{R}$ sobre um conjunto A que seja simétrica e transitiva e não seja reflexiva.

3. Dê dois exemplos, um listando os pares ordenados e o outro descrevendo-os através de uma regra, de relações que tenham as propriedades reflexiva e simétrica e não tenham a transitiva.

4. Sejam $\mathcal{R}$ uma relação sobre A e Δ a relação identidade sobre um conjunto não vazio A, isto é, $\Delta = \{(x, x);\ x \in A\}$. Mostre que:

   (a) $\mathcal{R}$ é reflexiva se, e somente se, $\Delta \subseteq \mathcal{R}$.

   (b) Se $\mathcal{R}$ tiver ambas as propriedades simétrica e anti-simétrica, então $\mathcal{R} \subseteq \Delta$.

   (c) $\mathcal{R}$ é simétrica se, e somente se, $\mathcal{R} = \mathcal{R}^{-1}$.

   (d) Se $\mathcal{R} \neq \emptyset$ é anti-simétrica, então $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq \Delta$.

5. Sejam A um conjunto e $\mathcal{R}$ e $\mathcal{R}'$ relações sobre A. Diga se cada uma das seguintes proposições é verdadeira ou falsa, justificando sua resposta:

   (a) Se $\mathcal{R}$ é simétrica, então $\mathcal{R}^{-1}$ é simétrica.

   (b) Se $\mathcal{R}$ é anti-simétrica, então $\mathcal{R}^{-1}$ é anti-simétrica.

   (c) Se $\mathcal{R}$ é transitiva, então $\mathcal{R}^{-1}$ é transitiva.

   (d) Se $\mathcal{R}$ é reflexiva, então $\mathcal{R} \cap \mathcal{R}^{-1} \neq \emptyset$.

   (e) Se $\mathcal{R}$ é simétrica, então $\mathcal{R} \cap \mathcal{R}^{-1} \neq \emptyset$.

   (f) Se $\mathcal{R}$ e $\mathcal{R}'$ são simétricas, então $\mathcal{R} \cup \mathcal{R}'$ é simétrica.

   (g) Se $\mathcal{R}$ e $\mathcal{R}'$ são simétricas, então $\mathcal{R} \cap \mathcal{R}'$ é simétrica.

   (h) Se $\mathcal{R}$ e $\mathcal{R}'$ são transitivas, então $\mathcal{R} \cup \mathcal{R}'$ é transitiva.

   (i) Se $\mathcal{R}$ e $\mathcal{R}'$ são transitivas, então $\mathcal{R} \cap \mathcal{R}'$ é transitiva.

   (j) Se $\mathcal{R}$ e $\mathcal{R}'$ são anti-simétricas, então $\mathcal{R} \cup \mathcal{R}'$ é anti-simétrica.

   (k) Se $\mathcal{R}$ e $\mathcal{R}'$ são anti-simétricas, então $\mathcal{R} \cap \mathcal{R}'$ é anti-simétrica.

   (l) Se $\mathcal{R}$ e $\mathcal{R}'$ são reflexivas, então $\mathcal{R} \cup \mathcal{R}'$ é reflexiva.

   (m) Se $\mathcal{R}$ e $\mathcal{R}'$ são reflexivas, então $\mathcal{R} \cap \mathcal{R}'$ é reflexiva.

6. Existe algum conjunto A tal que toda relação sobre A seja:

   (a) Reflexiva?

   (b) Simétrica?

   (c) Transitiva?

   (d) Anti-simétrica?

Existe mais de um conjunto?

7. Quais das relações dadas no primeiro exercício são de equivalência? Justifique.

8. (a) Verifique que a relação

$$\mathcal{R} = \{(1,1),(2,2),(3,3),(4,4),(5,5),\\ (2,5),(5,2),(3,5),(5,3),(2,30,(3,2)\}$$

é uma relação de equivalência em $A = \{1,2,3,4,5\}$.

(b) Determine $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ e $\bar{5}$.

(c) Determine $A/\mathcal{R}$.

9. Seja $\sim$ a relação sobre $\mathbb{R}$ definida por $x \sim y$ se, e somente se, $x - y \in \mathbb{Z}$, para todo $x, y \in \mathbb{R}$. Mostre que $\sim$ é uma relação de equivalência sobre $\mathbb{R}$.

10. Defina a relação $\mathcal{R}$ sobre $\mathbb{R}$ por $x\mathcal{R}y$ se, e somente se $\cos(x) = \cos(y)$ e $\text{sen}(x) = \text{sen}(y)$, para todo x, $y \in \mathbb{R}$.

(a) Mostre que $\mathcal{R}$ é uma relação de equivalência.

(b) Se $a \in \mathbb{R}$, determine $\bar{a}$.

11. Seja $\mathbb{R}^3 = \{x = (x_1, x_2, x_3);\ x_i \in \mathbb{R},\ i = 1,\ 2,\ 3\}$. Defina em $A = \mathbb{R}^3 - \{(0,0,0)\}$ a seguinte relação:

$$x \sim y \text{ se existe } \alpha \in \mathbb{R} \text{ tal que } x = \alpha y, \text{ para todo } x,\ y \in A.$$

(a) Mostre que $\sim$ é uma relação de equivalência.

(b) Descreva geometricamente $\bar{x}$, para algum $x \in A$.

12. Seja f uma função real com domínio real. Defina a relação $\mathcal{R}_f$ pela regra

$$x\mathcal{R}_f y \iff f(x) = f(y).$$

Mostre que $\mathcal{R}_f$ é uma relação de equivalência.

13. Em $A = \mathbb{N} \times \mathbb{N}$, defina a seguinte relação:

$$(a,b) \sim (c,d) \Longleftrightarrow a + d = b + c, \text{ para todo } a,\ b,\ c,\ d \in \mathbb{N}.$$

(a) Mostre que $\sim$ é uma relação de equivalência.

(b) Encontre as seguintes classe de equivalências $\overline{(1,0)}$, $\overline{(0,1)}$, $\overline{(1,1)}$ e $\overline{(0,0)}$.

14. Defina em $\mathbb{Z} \times \mathbb{N}$ a seguinte relação:

$$(a,b) \sim (c,d) \Longleftrightarrow ad = bc, \text{ para todo } a,\, c \in \mathbb{Z} \text{ e } b,\, d \in \mathbb{N}.$$

(a) Mostre que $\sim$ é uma relação de equivalência em $\mathbb{Z} \times \mathbb{N}$.

(b) Pense um pouco sobre o conjunto $\mathbb{Z} \times \mathbb{N}/\sim$. Compare-o com $\mathbb{Q}$, o conjunto dos números racionais.

15. Seja $\mathcal{R}$ a relação dos números naturais $\mathbb{N}$ definida por "m é um múltiplo de n". Mostre que esta é uma relação de ordem em $\mathbb{N}$. Esta é uma relação de ordem total em $\mathbb{N}$?

16. Considere o conjunto $S = \{2,\, 4,\, 8, \ldots, 2^n, \ldots\}$ e considere a relação $\mathcal{R}$ definida no exercício anterior. Mostre que S é um subconjunto de $\mathbb{N}$ totalmente ordenado.

17. Seja $S = \{2,\, 3,\, 4, 5, \ldots\}$ ordenado por "m divide n".

(a) Encontre todos os elementos maximais

(b) Encontre todos os elementos minimais.

18. Mostre que se a e b são elementos minimais num conjunto A totalmente ordenado. Então $a = b$.

19. Considere a relação de divisibilidade sobre o conjunto $\mathbb{Z}$ dos números inteiros:

$$\mathcal{R}:\ a/b \quad \text{se, e somente se } \exists\, c \in \mathbb{Z} \text{ tal que } b = ac.$$

$\mathcal{R}$ é uma relação de ordem sobre $\mathbb{Z}$?

20. Consideremos o conjunto dos números naturais que são divisores próprios de 36, isto é, $E = \{2,\, 3,\, 4,\, 6,\, 9,\, 12,\, 18\}$ e ordenemos E pela relação de divisibilidade

$$\mathcal{R} : a \leq b \quad \text{se, e somente se } a/b,$$

isto é, $\exists\ c \in \mathbb{N}$ tal que $b = ac$. $\mathcal{R}$ é uma relação de ordem sobre E? $\mathcal{R}$ é uma relação de ordem total sobre E?

21. Consideremos a ordem habitual $\leq$ sobre o conjunto $\mathbb{N}$ dos números naturais e seja $E = \mathbb{N} \times \mathbb{N}$, o produto cartesiano de $\mathbb{N}$ por si mesmo.

    (a) Se (a, b) e (c, d) são dois elementos quaisquer de E então, por definição

    $$(a, b)\mathcal{R}(c, d) \quad \text{se, e somente se } a \leq c \text{ e } b \leq d.$$

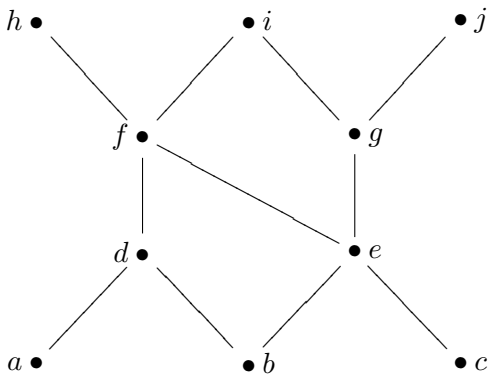
    Mostre que $\mathcal{R}$ uma relação de ordem sobre E que não é total.

    (b) Se (a, b) e (c, d) são dois elementos quaisquer de E colocaremos, por definição,

    $$(a, b)\mathcal{R}'(c, d) \quad \text{se, e somente se } a < c \text{ ou } a = c \text{ e } b \leq d.$$

    Mostre que $\mathcal{R}'$ é uma ordem total sobre E.

22. Seja $\mathcal{R}$ a relação de ordem sobre $E = \{a, b, c, d, e, f, g, h, i, j\}$ com o seguinte diagrama de Hasse:



Determinar, caso existam, os limites superiores, os limites inferiores, o ínfimo, o supremo, o máximo e o mínimo de $A = \{d, e\}$ e de $B = \{b, d, f\}$..

4 Noções de Cardinalidade

4.1 Conjuntos Equipotentes, Enumeráveis e Contáveis

Como podemos determinar quando dois conjuntos têm o mesmo tamanho?

Se tais conjuntos forem finitos podemos fazer isso contando os seus elementos. Mas esta técnica não funciona para conjuntos infinitos.

Iremos determinar quando dois conjuntos têm o mesmo tamanho, ou o mesmo número de elementos, não contando quantos elementos cada um deles tem, mas sim, fazendo uma correspondência entre cada elemento de um conjunto com um único elemento do outro e vice-versa. Mais especificamente, temos:

Definição 4.1. Sejam A e B conjuntos. Dizemos que A e B têm a **mesma cardinalidade**, ou que eles são **equipotentes**, e escrevemos $A \sim B$, se existir uma função bijetora $f : A \to B$.

Vale observar que com esta definição, estamos dizendo quando dois conjuntos têm o mesmo número de elementos sem necessariamente dizer qual é esse número.

Uma importante propriedade da noção de conjuntos equipotentes, é que podemos separar os conjuntos em classes de conjuntos que têm a mesma cardinalidade, ou seja, a relação $\sim$ é de fato uma relação de equivalência.

Teorema 4.2. Para um conjunto universo U, a relação de equipotência é uma relação de equivalência em $\wp(U)$.

Prova: Temos que mostrar que $\sim$ é reflexiva, simétrica e transitiva.

(i) Para todo $A \in \wp(U)$, temos que $I : A \to A$, dada por $I(a) = a$, para todo $a \in A$, isto é, a função identidade, é uma bijeção. Logo $A \sim A$.

(ii) Se A, $B \in \wp(U)$ são tais que $A \sim B$, então existe $f : A \to B$ bijetora. Logo $f^{-1} : B \to A$ também é bijetora, o que mostra que $B \sim A$.

(iii) Se A, B, $C \in \wp(U)$ são tais que $A \sim B$ e $B \sim C$, então existem $f : A \to B$ e $g : B \to C$ bijetoras. Logo $g \circ f : A \to C$ também é bijetora, o que mostra que $A \sim C$.

Ou seja, $\sim$ é uma relação de equivalência, como queríamos demonstrar. ■

Exemplo 4.3. Exemplos de cardinalidades de conjuntos:

(1) Sejam $\mathbb{N}$ o conjunto dos números naturais. Então $\mathbb{N}$ e $2\mathbb{N}$ têm a mesma cardinalidade, ou seja, o conjunto dos naturais e o conjunto dos naturais pares têm a mesma cardinalidade.

De fato, basta observar que $f : \mathbb{N} \to 2\mathbb{N}$, definida por $f(n) = 2n$, para todo $n \in \mathbb{N}$, é uma função bijetora.

De maneira análoga mostra-se que $\mathbb{N}$ e o conjunto dos naturais ímpares $2\mathbb{N} + 1$ são equipotentes.

(2) O conjunto dos números inteiros $\mathbb{Z}$ tem a mesma cardinalidade que $\mathbb{N}$.

De fato, basta observar que $f : \mathbb{Z} \to \mathbb{N}$, definida por

$$f(n) = \begin{cases} 2n & \text{se } n \geq 0 \\ -(2n+1) & \text{se } n < 0 \end{cases}$$

para todo $n \in \mathbb{Z}$, é uma bijeção.

(3) Sejam $[a, b]$ e $[c, d]$ intervalos fechados de $\mathbb{R}$, onde $a < b$ e $c < d$. Então $[a, b] \sim [c, d]$.

De fato, a função $g : [a, b] \to [c, d]$, definida por $g(x) = \dfrac{d-c}{b-a}(x - a) + c$, para todo $x \in [a, b]$ é uma bijeção.

Usando restrições da função g definida acima, pode-se mostrar que se $a < b$ e $c < d$ são números reais, então $(a, b] \sim (c, d]$, $(a, b) \sim (c, d)$ e $[a, b) \sim [c, d)$.

(4) O intervalo $(-1, 1)$ tem a mesma cardinalidade que $\mathbb{R}$.

Basta ver que a função $h : (-1, 1) \to \mathbb{R}$, definida por $h(x) = \dfrac{x}{1 - |\, x \,|}$, para todo $x \in (-1, 1)$ é uma bijeção.

Para uma melhor análise da cardinalidade de conjuntos, necessitamos definir conjunto finito, infinito, enumerável, não enumerável, contável, etc... É obvio que um conjunto infinito é um conjunto que não é finito e vice-versa. Assim, precisamos definir uma destas noções e teremos a outra. Escolhemos definir conjunto infinito.

Definição 4.4. Seja A um conjunto. Dizemos que:

(a) A é um **conjunto infinito** se A é equipotente a um subconjunto próprio de A.

(b) A é um **conjunto finito** se A não for infinito.

(c) A é um **conjunto enumerável** se $A \sim \mathbb{N}$.

(d) A é um **conjunto contável** se A é finito ou enumerável.

(e) A é um **conjunto não enumerável** se A não é contável.

Exemplo 4.5. Exemplos de conjuntos envolvendo as noções acima:

(1) Do exemplo anterior, temos que $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ e qualquer intervalo aberto, fechado ou semi-aberto de $\mathbb{R}$ são exemplos de conjuntos infinitos.

(2) O conjunto vazio é finito, pois não contém subconjunto próprio.

(3) Para cada $n \in \mathbb{N},\ n \geq 1$, o conjunto $\mathbb{N}_n = \{1, 2, \ldots, n\}$ é finito.

Veremos por indução sobre n. Para $n = 1$, o resultado é imediato, desde que o único subconjunto próprio de $\mathbb{N}_n$ é o vazio e não existe uma bijeção $f : \emptyset \to \mathbb{N}_1$. Se $n > 1$, suponhamos que o resultado vale para n e provaremos que ele vale para $n + 1$. Mais adiante provaremos que isso implica que o resultado vale para todo $n \in \mathbb{N}$.

Se $\mathbb{N}_{n+1}$ não for finito, então existe um subconjunto próprio A de $\mathbb{N}_{n+1}$ tal que $A \sim \mathbb{N}_{n+1}$. Seja $f : \mathbb{N}_{n+1} \to A$ uma bijeção. Então a restrição $f : \mathbb{N}_n \to A - \{f(n+1)\}$ é claramente uma bijeção, o que contradiz o fato de $\mathbb{N}_n$ ser finito.

(4) Segue diretamente do teorema 4.2 que $\mathbb{N}$ é um conjunto enumerável. Do exemplo 4.3(2), temos que $\mathbb{Z}$ também é um conjunto enumerável.

Vejamos alguns resultados sobre conjuntos enumeráveis.

Teorema 4.6. Todo subconjunto infinito de um conjunto enumerável é enumerável. Todo subconjunto de um conjunto contável é contável.

Prova: Vamos demonstrar a primeira afirmação. A demonstração da segunda afirmação fica como exercício.

Sejam A um conjunto enumerável e B um subconjunto infinito de A. Desde que $A \sim \mathbb{N}$, podemos escrever $A = \{a_1, a_2, \ldots\}$, onde $a_i = f(i-1)$ para alguma bijeção $f : \mathbb{N} \to A$.

Seja n_1 o menor índice para o qual $a_{n_1} \in B$. Desde que B é infinito, temos que $B - \{a_{n_1}\}$ é também infinito (mostre esta afirmação). Assim, seja n_2 o menor índice para o qual $a_{n_2} \in B - \{a_{n_1}\}$. Tendo definido $a_{n_{k-1}} \in B$, seja n_k o menor índice para o qual $a_{n_k} \in B - \{a_{n_1}, a_{n_2}, \ldots, a_{n_{k-1}}\}$. Usando que B é infinito, temos que $B - \{a_{n_1}, a_{n_2}, \ldots, a_{n_{k-1}}\} \neq \emptyset$, para cada $k \in \mathbb{N}$ é infinito. Assim, temos uma função bijetora $g : \mathbb{N} \to B$, dada por $g(k) = a_{n_k}$, para cada $k \in \mathbb{N}$, o que mostra que B é enumerável. ■

Teorema 4.7. O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.

Prova: Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definida por $f(n, m) = 2^n 3^m$. Usando o Teorema Fundamental da Aritmética temos que f é injetora. Assim, $\mathbb{N} \times \mathbb{N} \sim f(\mathbb{N} \times \mathbb{N}) \subseteq \mathbb{N}$. Como $\mathbb{N} \times \mathbb{N}$ é um conjunto infinito (mostre isso), temos que $f(\mathbb{N} \times \mathbb{N})$ é infinito e, pelo teorema anterior, obtemos que $\mathbb{N} \times \mathbb{N}$ é enumerável. ■

Teorema 4.8. A união de dois conjuntos enumeráveis é enumerável.

Prova: Sejam A e B conjuntos enumeráveis. Vamos mostrar que $A \cup B$ é enumerável. Consideremos dois casos:

1. $A \cap B = \emptyset$. Como $A \sim \mathbb{N}$ e $\mathbb{N} \sim 2\mathbb{N}$, pela transitividade de $\sim$, temos que $A \sim 2\mathbb{N}$. De maneira análoga, temos $B \sim 2\mathbb{N} + 1$. Sejam $f : A \to 2\mathbb{N}$ e $g : B \to 2\mathbb{N} + 1$ as correspondentes bijeções. A função $h : A \cup B \to (2\mathbb{N}) \cup (2\mathbb{N} + 1)$, onde $h = f \cup g$ é uma bijeção, pois $A \cap B = \emptyset$, o que implica que $A \cup B \sim (2\mathbb{N}) \cup (2\mathbb{N} + 1) \sim \mathbb{N}$.

2. $A \cap B \neq \emptyset$. Neste caso, para $C = B - A$, temos $A \cup B = A \cup C$ e $A \cap C = \emptyset$. Como $C \subseteq B$, temos que C é enumerável ou finito. Se C for enumerável, recaímos no caso anterior. Se C for finito, é fácil ver que $A \cup C$ é enumerável. ■

Corolário 4.9. Sejam $A_1, A_2, \ldots, A_k$ conjuntos enumeráveis. Então $\bigcup_{k=1}^{n} A_k$ é enumerável.

Teorema 4.10. O conjunto dos números racionais é enumerável.

Prova: Vamos usar que cada número racional pode ser representado de maneira única como $\frac{p}{q}$, onde $p \in \mathbb{Z}$, $q \in \mathbb{N} - \{0\}$ com $\text{mdc}\,(p, q) = 1$. Sejam $\mathbb{Q}_+ = \{\frac{p}{q};\ \frac{p}{q} > 0\}$ e $\mathbb{Q}_- = \{\frac{p}{q};\ \frac{p}{q} < 0\}$. Temos então $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_- \cup \{0\}$ e, evidentemente $\mathbb{Q}_+ \sim \mathbb{Q}_-$. Do teorema anterior temos que, para mostrar que $\mathbb{Q}$ é enumerável, é suficiente mostrar que $\mathbb{Q}_+$ é enumerável.

Para isso, considere a função $f : \mathbb{Q}_+ \to \mathbb{N} \times \mathbb{N}$, definida por $f(\frac{p}{q}) = (p, q)$. É fácil ver que f é injetora. Logo, $\mathbb{Q}_+ \sim f(\mathbb{Q}_+) \subseteq \mathbb{N} \times \mathbb{N}$. Como claramente $\mathbb{N} \subseteq \mathbb{Q}_+$ e $\mathbb{N} \times \mathbb{N}$ é enumerável, temos que $f(\mathbb{Q}_+)$ é um subconjunto infinito de um conjunto enumerável. Do teorema 4.6 temos que $f(\mathbb{Q}_+)$ é enumerável. Portanto $\mathbb{Q}_+ \sim f(\mathbb{Q}_+) \sim \mathbb{N}$, ou seja, $\mathbb{Q}_+$ é enumerável, como queríamos. ■

Teorema 4.11. Todo conjunto infinito contém um conjunto enumerável.

Prova: Seja X um conjunto infinito. Então $X \neq \emptyset$ e, portanto, existe $x_1 \in X$. Considere o conjunto $X - \{x_1\}$. Como X é infinito, existe $x_2 \in X - \{x_1\}$. Considere o conjunto $X - \{x_1, x_2\}$. Tendo escolhido $x_k \in X - \{x_1, x_2, \ldots, x_{k-1}\}$ e observando que x_k sempre existe, para cada $k \in \mathbb{N}$, pois X é infinito, temos que o conjunto $\{x_1, x_2, \ldots, x_k, \ldots\} = \{x_k;\ k \in \mathbb{N}\}$ é um subconjunto enumerável de X. ■

Vejamos agora alguns conjuntos não enumeráveis.

Teorema 4.12. O intervalo aberto $(0, 1) \subseteq \mathbb{R}$ é um conjunto não enumerável.

Prova: Dado qualquer número real $x \in (0, 1)$, podemos expressá-lo na forma decimal

$$x = 0, x_1 x_2 x_3 \ldots,$$

onde cada $x_i \in \{0, 1, \ldots, 9\}$. Para obtermos a unicidade nesta representação, os decimais finitos terão seu último dígito decrescido de uma unidade e adicionado 9's infini-

tamente. Assim, dois números no intervalo $(0,1)$ serão iguais se, e somente se os dígitos correspondentes em sua representação decimal são iguais.

Agora, suponhamos por absurdo que $(0,1)$ é um conjunto enumerável. Então existe uma função bijetora $f : \mathbb{N} \to (0,1)$ e, conseqüentemente, podemos listar os elementos de $(0,1)$ como segue:

$$\begin{aligned} f(0) &= 0, a_{01}a_{02}a_{03}\ldots \\ f(1) &= 0, a_{11}a_{12}a_{13}\ldots \\ f(2) &= 0, a_{21}a_{22}a_{23}\ldots \\ &\vdots \\ f(k) &= 0, a_{k1}a_{k2}a_{k3}\ldots \end{aligned}$$

onde cada $a_{kj} \in \{0, 1, \ldots, 9\}$.

Vamos construir um elemento de $(0,1)$ que não está na listagem acima, ou seja, vamos contradizer o fato de f ser sobrejetora.

Seja $y = 0, y_1y_2y_3\ldots$, onde $y_k = 3$ se $a_{kk} \neq 3$ e $y_k = 1$ se $a_{kk} = 3$, para todo $k \in \mathbb{N}$. Claramente $y \in (0,1)$, mas $y \neq f(k)$, para todo $k \in \mathbb{N}$, pois $y_k \neq a_{kk}$. Portanto, $(0,1)$ é não enumerável. ■

Corolário 4.13. O conjunto dos números reais $\mathbb{R}$ é não enumerável.

Prova: Imediata, pois $\mathbb{R} \sim (0,1)$. ■

Corolário 4.14. O conjunto dos números irracionais $\mathbb{I}$ é não enumerável.

Prova: De fato, se $\mathbb{I}$ for enumerável, como $\mathbb{Q}$ é enumerável e $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, teríamos que $\mathbb{R}$ seria enumerável. ■

4.2 Números Cardinais e a Hipótese do Contínuo

Aqui não iremos definir o que é um **número cardinal**, somente vamos introduzi-los como uma noção primitiva relacionada com o tamanho de conjuntos. Assumiremos que esta nova noção será regida pelas seguintes leis:

C-1. A cada conjunto A é associado um número cardinal, denotado por $\text{card}(A)$, e a cada número cardinal a existe um conjunto A com $\text{card}(A) = a$.

C-2. $\text{card}(A) = 0$ se, e somente se $A = \emptyset$.

C-3. Se $A \neq \emptyset$ e A é finito, isto é, $A \sim \{1, 2, \ldots, k\}$ para algum $k \in \mathbb{N}$, então $\text{card}(A) = k$.

C-4. Para quaisquer dois conjuntos A e B, temos $\text{card}(A) = \text{card}(B)$ se, e somente se $A \sim B$.

As leis C-2 e C-3 definem os números cardinais de conjuntos finitos, ou seja, **o número cardinal de um conjunto finito é o número de elementos deste conjunto.** Em termos de teoria dos conjuntos, C-1 e C-4 formam um axioma, o *axioma da cardinalidade*. Note que C-2 e C-3 são mais fáceis de serem aceitos, enquanto que C-1 e C-4 são mais difíceis pois estas leis não expressam nada concretamente sobre $\text{card}(A)$ quando A é um conjunto infinito.

Dizemos que o número cardinal de um conjunto finito é um **número cardinal finito** e o de um conjunto infinito é um **número cardinal transfinito**.

Das propriedades C-2 e C-3, temos que os números cardinais finitos são precisamente os números naturais. Assim, temos uma relação de ordem natural: $0 < 1 < 2 < \cdots < k < k+1 < \cdots$. Já para dois números cardinais transfinitos, a propriedade C-4 nos diz quando eles são iguais ou não. O problema, agora, é saber decidir quando um é **menor** que o outro.

Definição 4.15. Sejam A e B conjuntos. Dizemos que $A \preceq B$, ou que $\text{card}(A) \leq \text{card}(B)$ se existir uma função injetora $f : A \to B$. Dizemos que $A \prec B$, ou que $\text{card}(A) < \text{card}(B)$ se existir uma função injetora $f : A \to B$ e $A \nsim B$.

Exemplo 4.16. $\text{card}(\mathbb{N}) < \text{card}(\mathbb{R})$.

De fato, existe $f : \mathbb{N} \hookrightarrow \mathbb{R}$ a inclusão, que é injetora e $\mathbb{N} \nsim \mathbb{R}$ pois $\mathbb{R}$ não é enumerável.

Vejamos se $\leq$ define uma relação de ordem no conjunto dos números cardinais.

(i) $\text{card}(A) \leq \text{card}(A)$, pois a identidade $I_A : A \to A$ é injetora.

(ii) Se $\text{card}(A) \leq \text{card}(B)$ e $\text{card}(B) \leq \text{card}(C)$, então $\text{card}(A) \leq \text{card}(C)$, pois a composta de funções injetoras é injetora.

(iii) Se $\text{card}(A) \leq \text{card}(B)$ e $\text{card}(B) \leq \text{card}(A)$, então $\text{card}(A) = \text{card}(B)$. A demonstração que esta propriedade é verdadeira é mais complicada e foge do

objetivo deste curso. Ela segue do seguinte resultado, que enunciaremos sem demonstrar.

Teorema 4.17 (Schröder-Bernstein)**.** Se A e B são conjuntos tais que A é equipotente a um subconjunto de B e B é equipotente a um subconjunto de A, então $A \sim B$.

Corolário 4.18. Se A e B são conjuntos tais que $\text{card}(A) \leq \text{card}(B)$ e $\text{card}(B) \leq \text{card}(A)$, então $\text{card}(A) = \text{card}(B)$.

Com isso temos que o conjunto dos números cardinais é um conjunto ordenado pela ordem $\leq$.

Do exemplo 4.16 temos dois números cardinais transfinitos distintos, $\text{card}(\mathbb{N})$ e $\text{card}(\mathbb{R})$, com $\text{card}(\mathbb{N}) < \text{card}(\mathbb{R})$.

Sejam $\aleph_0 = \text{card}(\mathbb{N})$ e $\aleph_1 = \text{card}(\mathbb{R})$. Note que $\aleph_0$ e $\aleph_1$ não são números reais. A pergunta que surge é: *Existe algum conjunto cuja cardinalidade está entre* $\aleph_0$ *e* $\aleph_1$*?* A conjectura de que a resposta a esta pergunta é negativa é conhecida como a Hipótese do Contínuo.

Hipótese do Continuo: Não existe conjunto algum A com a propriedade

$$\aleph_0 < \text{card}(A) < \aleph_1.$$

4.3 O Número Cardinal de um Conjunto Potência - o Teorema de Cantor

Seja X um conjunto. Já sabemos que se X é finito com n elementos, então $\wp(X)$ também é finito e tem 2^n elementos. Cantor provou que $\text{card}(X) < \text{card}(\wp(X))$, para qualquer conjunto X, o que nos permite construir uma infinidade de números cardinais transfinitos, por exemplo

$$\aleph_0 = \text{card}(\mathbb{N}) < \text{card}(\wp(\mathbb{N})) < \text{card}(\wp(\wp(\mathbb{N}))) < \cdots$$

Teorema 4.19 (Cantor)**.** Se X é um conjunto, então $\text{card}(X) < \text{card}(\wp(X))$.

Prova: Se $X = \emptyset$, então $\text{card}(X) = 0$ e $\wp(X) = \{\emptyset\}$. Portanto, $\text{card}(\wp(X)) = 1 > 0$.

Se $X \neq \emptyset$, seja $g : X \to \wp(X)$ a função definida por $g(x) = \{x\}$, para todo $x \in X$. É claro que g é injetora, o que mostra que $\text{card}(X) \leq \text{card}(\wp(X))$.

Para mostrarmos que $\text{card}(X) < \text{card}(\wp(X))$, temos que mostrar que $X \nsim \wp(X)$. Suponhamos, por absurdo, que $X \sim \wp(X)$. Seja $f : X \to \wp(X)$ uma bijeção. Considere $S = \{x \in X;\ x \notin f(x)\} \subseteq X$. Desde que f é sobrejetora e $S \in \wp(X)$, temos que existe $a \in X$ tal que $S = f(a)$. Se $a \in S$, então pela definição de S, temos que $a \notin f(a) = S$, o que é uma contradição. Se $a \notin S$, então novamente pela definição de S, temos que $a \in f(a) = S$, o que leva a uma contradição. Portanto $X \nsim \wp(X)$, como queríamos. ■

Para alguns autores, a hipótese do contínuo é que não existe um número cardinal x tal que $\aleph_0 < x < \text{card}(\wp(\mathbb{N}))$.

4.4 Aritmética Cardinal

4.4.1 Adição de Números Cardinais.

Queremos uma definição de adição de números cardinais que generalize a noção de adição de números naturais, ou seja, dos números cardinais finitos.

Definição 4.20. Sejam a e b números cardinais. A **soma cardinal** de a e b, denotada por $a + b$, é o números cardinal $\text{card}(A \cup B)$, onde A e B são conjuntos tais que $\text{card}(A) = a$, $\text{card}(B) = b$ e $A \cap B = \emptyset$.

Para mostrar que esta operação está bem definida, devemos mostrar que sempre existem tais conjuntos A e B e que a definição não depende da escolha de tais conjuntos.

Dados a e b cardinais, da propriedade C-1, existem conjuntos X e Y tais que $a = \text{card}(X)$ e $b = \text{card}(Y)$. Se $X \cap Y \neq \emptyset$, temos que $A = X \times \{0\}$ e $B = Y \times \{1\}$ são conjuntos tais que $\text{card}(A) = a$, $\text{card}(B) = b$ e $A \cap B = \emptyset$, o que mostra que existem conjuntos A e B como descritos na definição.

Se A' e B' são conjuntos com $A \sim A'$, $B \sim B'$ e $A' \cap B' = \emptyset$, então existem $f : A \to A'$ e $g : B \to B'$ bijetoras e, podemos ver facilmente que $f \cup g : A \cup B \to A' \cup B'$ é também bijetora, o que mostra que $A \cup B \sim A' \cup B'$, ou seja $\text{card}(A \cup B) = \text{card}(A' \cup B')$.

Desde que a união de conjuntos é comutativa e associativa, obtemos as propriedades correspondentes para soma cardinal.

Teorema 4.21. Sejam a, b e c números cardinais. Então:

1. $a + b = b + a$.

2. $a + (b + c) = (a + b) + c$.

Exemplo 4.22. Encontre as seguintes somas cardinais:

(1) $4 + 3$.
Desde que $4 = \text{card}(\{1, 2, 3, 4\} = \mathbb{N}_4)$, $\mathbb{N}_7 = \mathbb{N}_4 \cup \{5, 6, 7\}$, $\text{card}\{5, 6, 7\} = 3$ e $\mathbb{N}_4 \cap \{5, 6, 7\} = \emptyset$, temos que $4 + 3 = \text{card}(\mathbb{N}_7) = 7$, o que coincide com a soma dos números naturais.

(2) $\aleph_0 + \aleph_0$.
Desde que $\mathbb{N} = (2\mathbb{N}) \cup (2\mathbb{N} + 1)$, esta união é disjunta, $\text{card}(2\mathbb{N}) = \text{card}(\mathbb{N}) = \aleph_0$ e $\text{card}(2\mathbb{N} + 1) = \text{card}(\mathbb{N}) = \aleph_0$, temos $\aleph_0 + \aleph_0 = \aleph_0$.

(3) $\aleph_1 + \aleph_0$.
Desde que $(0, 1) \sim \mathbb{R}$, temos que $\aleph_1 = \text{card}((0, 1))$. Seja $S = (0, 1) \cup \mathbb{N}$. Como $(0, 1) \cap \mathbb{N} = \emptyset$, temos que $\text{card}(S) = \aleph_1 + \aleph_0$. Agora, $\mathbb{R} \sim (0, 1) \subseteq S$ e $S \subseteq \mathbb{R}$, então pelo teorema de Schröder-Bernstein, temos $\text{card}(\mathbb{R}) = \text{card}(S)$, ou seja, $\aleph_1 + \aleph_0 = \aleph_1$.

4.4.2 Multiplicação de Números Cardinais

Analogamente, queremos uma definição de multiplicação de cardinais que generalize a multiplicação dos naturais.

Definição 4.23. Sejam a e b cardinais. O **produto cardinal** ab é definido como sendo o número cardinal do produto cartesiano $A \times B$, onde A e B são conjuntos com $\text{card}(A) = a$ e $\text{card}(B) = b$.

Exercício 4.24. Mostre que se A, B, A' e B' são conjuntos com $A \sim A'$ e $B \sim B'$, então $A \times B \sim A' \times B'$, ou seja, que o produto cardinal está bem definido.

Como no caso da adição, usando-se propriedades do produto cartesiano de conjuntos, mostra-se as seguintes propriedades do produto de cardinais.

Teorema 4.25. Se a, b e c são cardinais, então:

1. $ab = ba$.
2. $a(bc) = (ab)c$.
3. $a(b + c) = ab + ac$.

Prova: Exercício. ■

Exemplo 4.26. Calcule os seguintes produtos cardinais:

(1) $1 \cdot a$, onde a é um número cardinal arbitrário. Seja A um conjunto com $\text{card}(A) = a$. Como $\{1\} \times A \sim A$, temos que $1 \cdot a = a$.

(2) $0 \cdot a$, onde a é um número cardinal arbitrário. Seja A um conjunto com $\text{card}(A) = a$. Como $\emptyset \times A = \emptyset$, temos que $0 \cdot a = 0$.

(3) $\aleph_0 \cdot \aleph_0$. Desde que $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, temos que $\aleph_0 \cdot \aleph_0 = \aleph_0$.

(4) $\aleph_1 \cdot \aleph_1$. Vamos mostrar que $\aleph_1 \cdot \aleph_1 = \aleph_1$.

Note que $\aleph_1 = \text{card}((0,1))$. Considere $f : (0,1) \times (0,1) \to (0,1)$, definida por $f(0, x_1x_2x_3 \ldots, 0, y_1y_2y_3 \ldots) = 0, x_1y_1x_2y_2 \ldots$. É fácil ver que f é injetora e, conseqüentemente $\aleph_1 \cdot \aleph_1 \leq \aleph_1$. Por outro lado, a aplicação

$$g : (0,1) \to (0,1) \times (0,1),$$

definida por $g(x) = (x, x)$, para todo $x \in (0,1)$, é claramente injetora, o que mostra que $\aleph_1 \cdot \aleph_1 \geq \aleph_1$. Agora, o resultado segue do teorema 4.17.

4.4.3 Potências de Números Cardinais

Sejam A e B conjuntos. Denotaremos por B^A o conjunto de todas as funções de A em B, ou seja $B^A = \{f : A \to B; f \text{ é função}\}$.

Definição 4.27. Sejam a e b números cardinais com $a \neq 0$. Definimos a **potência cardinal** b^a como sendo o cardinal do conjunto B^A, onde A e B são conjuntos com $\text{card}(A) = a$ e $\text{card}(B) = b$.

O próximo teorema nos garante que esta operação está bem definida.

Teorema 4.28. Sejam A, B, X e Y conjuntos tais que $A \sim X$ e $B \sim Y$. Então $B^A \sim Y^X$.

Prova: Desde que $A \sim X$ e $B \sim Y$, temos que existem funções bijetoras $g : A \to X$ e $h : B \to Y$. Queremos definir uma bijeção entre B^A e Y^X.

Para cada $f \in B^A$, temos

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ X & \xrightarrow{\psi(f)} & Y \end{array}$$

onde definimos $\psi(f) \in Y^X$ por $\psi(f) = h \circ f \circ g^{-1}$. Agora é fácil mostrar que $\psi : B^A \to Y^X$ é uma bijeção. ■

Como propriedades da potenciação de cardinais temos:

Teorema 4.29. Sejam a, b, x e y números cardinais. Então:

1. $a^x \cdot a^y = a^{x+y}$.
2. $(a^x)^y = a^{xy}$.
3. $(ab)^x = a^x \cdot b^x$.

Prova: Exercício. ■

Com a noção de potenciação, podemos calcular a cardinalidade do conjunto das partes de um conjunto A, que generaliza o resultado que diz que se A tem n elementos, então $\wp(A)$ tem 2^n elementos.

Teorema 4.30. Seja A um conjunto. Então $\text{card}(\wp(A)) = 2^{\text{card}(A)}$.

Prova: Seja $B = \{0, 1\}$. Agora, é suficiente mostrarmos que $\wp(A) \sim B^A$. Assim, queremos encontrar uma função bijetora $\psi : \wp(A) \to B^A$.

Para cada $X \in \wp(A)$, considere $f_X \in B^A$ definida por

$$f_X(a) = \begin{cases} 0 & \text{se} \quad a \notin X \\ 1 & \text{se} \quad a \in X \end{cases}$$

que é a função característica de X.

Assim, definimos $\psi(X) = f_X$, para cada $X \in \wp(A)$. É fácil ver que para X, $Y \in \wp(A)$, temos $X = Y$ se, e somente se $f_X = f_Y$, ou seja, ψ é injetora. Agora, para cada $f \in B^A$, seja $X = \{a \in A;\ f(a) = 1\}$. Claramente temos $f = f_X$, ou seja, ψ é sobrejetora. Portanto $\text{card}(\wp(A)) = \text{card}(B^A) = 2^{\text{card}(A)}$. ■

Como conseqüência deste teorema temos que $\text{card}(\wp(\mathbb{N})) = 2^{\aleph_0}$.

Vamos finalizar o estudo sobre cardinalidades mostrando que $2^{\aleph_0} = \aleph_1$, ou seja, que $\mathbb{R}$ e $\wp(\mathbb{N})$ têm a mesma cardinalidade.

Teorema 4.31. $2^{\aleph_0} = \aleph_1$.

Prova: Usando o teorema de S-B (teorema 4.17), é suficiente mostrarmos que $2^{\aleph_0} \leq \aleph_1$ e $2^{\aleph_0} \geq \aleph_1$.

Note que $\aleph_0 = \text{card}(\mathbb{Q})$, o que implica que $2^{\aleph_0} = \text{card}(\wp(\mathbb{Q}))$.

Considere $f : \mathbb{R} \to \wp(\mathbb{Q})$, definida por $f(a) = \{x \in \mathbb{Q};\ x < a\} \in \wp(\mathbb{Q})$, para cada $a \in \mathbb{R}$. Se a e b são números reais distintos, então, sem perda de generalidade, podemos supor que $a < b$. Logo, existe $r \in \mathbb{Q}$ tal que $a < r < b$, o que implica que $r \in f(b)$ e $r \notin f(a)$, o que mostra que $f(a) \neq f(b)$. Conseqüentemente, f é uma função injetora. Portanto $\aleph_1 = \text{card}(\mathbb{R}) \leq \text{card}(\wp(\mathbb{Q})) = 2^{\aleph_0}$.

Por outro lado, é fácil ver que a função $\psi : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$, definida por $\psi(g) = 0, g(0)g(1)g(2)\ldots \in \mathbb{R}$, para cada $g : \mathbb{N} \to \{0,1\}$, é injetora, o que mostra que $2^{\aleph_0} \leq \aleph_1$, como queríamos. ■

Corolário 4.32. $\aleph_0 < \aleph_1$.

Prova: Segue do teorema acima e do teorema de Cantor. ■

4.5 Exercícios

1. Seja A um subconjunto infinito de $\mathbb{N}$. Mostre que $\text{card}(\mathbb{N}) = \text{card}(A)$.

2. Sejam A e B conjuntos tais que $A \sim \mathbb{N}$ e $B \sim \mathbb{N}$. Mostre que:

   (a) $A \cup B \sim \mathbb{N}$.

   (b) $A \times B \sim \mathbb{N}$.

3. Sejam $A_1, \ldots, A_n$ conjuntos tais que $A_i \sim \mathbb{N}$, para todo $i \in \{1, \ldots, n\}$. Mostre que $\bigcup_{i=1}^{n} A_i \sim \mathbb{N}$, ou seja, a união finita de conjuntos enumeráveis é enumerável.

4. Seja $\{A_n\}_{n\in\mathbb{N}}$ uma família de conjuntos com $A_i \sim \mathbb{N}$, para cada $i \in \mathbb{N}$. Mostre que $\bigcup_{i=1}^{\infty} A_i \sim \mathbb{N}$, ou seja, a união enumerável de conjuntos enumeráveis é enumerável.

5. Mostre que $f : \mathbb{N} \to \mathbb{Z}$, definida por:

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{se } n \text{ é par} \\ -\dfrac{n-1}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

é bijetora. Conclua que $\mathbb{N} \sim \mathbb{Z}$.

6. Seja X um conjunto infinito, $x_0 \in X$ e $Y \subseteq X$ finito. Mostre que:

   (a) $X - \{x_0\}$ é infinito.
   (b) $X - Y$ é infinito.
   (c) $\text{card}(X) = \text{card}(X - \{x_0\})$.
   (d) $\text{card}(X) = \text{card}(X - Y)$.

7. Para todo $a,\ b \in \mathbb{R}$, com $a < b$, mostre que os intervalos seguintes são equivalentes a $\mathbb{R}$ e, conseqüentemente, todos são não enumeráveis:

$$(a, b), \quad (a, b], \quad [a, b), \quad (-\infty, b], \quad [a, +\infty), \quad (-\infty, b) \quad \text{e} \quad (a, +\infty).$$

8. Seja X um conjunto com $\text{card}(X) > \aleph_0$. Se $A \subseteq X$ é tal que $\text{card}(A) = \aleph_0$, mostre que $\text{card}(X - A) = \text{card}(X)$.

9. Sejam $A,\ B,\ A'$ e B' conjuntos tais que $\text{card}(A) = \text{card}(A')$ e $\text{card}(B) = \text{card}(B')$, $A \cap B = \emptyset$ e $A' \cap B' = \emptyset$. Mostre que $\text{card}(A' \cup B') = \text{card}(A \cup B)$.

10. Sejam $X,\ Y,\ Z$ e W conjuntos tais que $X \sim Y$ e $Z \sim W$. Mostre que $X \times Z \sim Y \times W$.

11. Seja n um número cardinal finito. Mostre que $n < \aleph_0$.

12. Seja a o cardinal de um conjunto infinito. Mostre que $\aleph_0 \leq a$. Conclua que $\aleph_0 = \text{card}(\mathbb{N})$ é o menor cardinal transfinito.

13. Mostre que se $A,\ B$ e C são conjuntos tais que $A \subseteq B \subseteq C$ e $A \sim C$ então $A \sim B$. (*Sug.: Use o Teorema de Schröder-Berstein*)

14. Sejam A e B conjuntos. Mostre que se $A \sim B$ então $\wp(A) \sim \wp(B)$

15. Sejam $A,\ B$ e C conjuntos. Mostre que:

   (a) Se $\text{card}(A) \leq \text{card}(B)$ e $\text{card}(B) \leq \text{card}(C)$, então $\text{card}(A) \leq \text{card}(C)$.

(b) Se $\text{card}(A) < \text{card}(B)$ e $\text{card}(B) < \text{card}(C)$, então $\text{card}(A) < \text{card}(C)$.

16. Determine as seguintes operações cardinais, onde $n = \text{card}(\{1, 2, \cdots, n\})$.

(a) $n + \aleph_0$ (b) $n + \aleph_1$ (c) $\aleph_0 + \aleph_1$ (d) $n \cdot \aleph_0$
(e) $n \cdot \aleph_1$ (f) $\aleph_0 \cdot \aleph_1$ (g) $\aleph_1 \cdot \aleph_1$.

17. Mostre que $\aleph_0^{\aleph_0} = \aleph_1$.

5
Os Números Naturais

5.1 Os Axiomas de Peano

Para a construção lógica formal dos números naturais, Peano escolheu três conceitos primitivos: *o zero, o número natural* e a relação *é sucessor de*. Assumindo estes conceitos primitivos, ele deu a caracterização dos números naturais através de cinco axiomas, chamados **axiomas de Peano**, que são:

1. Zero é um número natural.
2. Se a é um número natural, então a tem um único sucessor que também é um número natural.
3. Zero não é sucessor de nenhum número natural.
4. Dois números naturais que têm sucessores iguais são iguais.
5. Se um conjunto S de números naturais contém o zero e, também, o sucessor de cada um de seus elementos, então S é o conjunto de todos os números naturais.

Usaremos as notações 0 para indicar o zero, a^+ para indicar o sucessor de um número natural a e $\mathbb{N}$ para indicar o conjunto de todos os números naturais. Com estas notações, podemos reescrever os axiomas de Peano como:

1. $0 \in \mathbb{N}$.
2. $(\forall\, a)(a \in \mathbb{N} \Longrightarrow a^+ \in \mathbb{N})$.

3. $(\forall\, a)(a \in \mathbb{N} \Longrightarrow a^+ \neq 0)$.

4. $(\forall\, a)(\forall\, b)(a^+ = b^+ \Longrightarrow a = b)$.

5. Se $S \subseteq \mathbb{N}$ e valem as propriedades

   (i) $0 \in S$; (ii) $(\forall\, a)(a \in S \Longrightarrow a^+ \in S)$,

   então $S = \mathbb{N}$.

O axioma (1) garante que $\mathbb{N} \neq \emptyset$. Em (2) subentende-se a unicidade do sucessor. O axioma (5) chama-se **axioma da indução completa**.

Vejamos agora, algumas propriedades dos números naturais que decorrem destes axiomas.

Proposição 5.1. Se $a \in \mathbb{N}$, então $a^+ \neq a$.

Prova: Seja $S = \{a \in \mathbb{N};\ a^+ \neq a\}$. Queremos mostrar que $S = \mathbb{N}$. Pelo axioma (5), temos que basta mostrar que S satisfaz as hipóteses (i) e (ii) de tal axioma.

De (3) temos que $0 \in S$, o que mostra que S satisfaz o item (i) de (5). Mais ainda, para todo $a \in \mathbb{N}$, se $a \in S$, então pela definição de S, temos que $a^+ \neq a$. Do axioma (4), segue que $(a^+)^+ \neq a^+$, o que implica que $a^+ \in S$, o que mostra que S satisfaz o item (ii) de (5). Portanto, $S = \mathbb{N}$. ■

Proposição 5.2. Todo número natural diferente de zero é sucessor de algum número natural.

Prova: Seja $S = \{0\} \cup \{y \in N;\ y \neq 0 \text{ e } y = x^+, \text{ para algum } x \in \mathbb{N}\}$. Por definição $0 \in S$, o que mostra que S satisfaz (i) de (5). Seja $a \in S$. Se $a = 0$, então $0 \neq a^+ = 0^+$, ou seja, $0^+ \in S$. Se $a \neq 0$, então $a = b^+$, para algum $b \in \mathbb{N}$, o que implica que $a^+ = (b^+)^+$, ou seja $a^+ \in S$. Assim, S satisfaz (ii) de (5). Portanto, o axioma (5) garante que $S = \mathbb{N}$, o que mostra a proposição. ■

O próximo resultado é muito importante para quando queremos mostrar que algum resultado vale para todos os números naturais.

Proposição 5.3 (Primeiro Princípio de Indução Completa)**.** Suponhamos que a todo número natural n esteja associada uma afirmação $P(n)$ tal que:

(i) $P(0)$ é verdadeira.

(ii) Para todo $r \in \mathbb{N}$, se $P(r)$ é verdadeira, então $P(r^+)$ é verdadeira.

Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Prova: Segue imediatamente do fato que $S = \{n \in \mathbb{N};\ P(n) \text{ é verdadeira}\}$ satisfaz as hipóteses do axioma (5). ■

Uma boa visualização deste princípio é o chamado efeito dominó.

5.2 Adição em $\mathbb{N}$

A operação de **adição** em $\mathbb{N}$ é definida, por recorrência, da seguinte forma

- $a + 0 = a$, para todo $a \in \mathbb{N}$;
- $a + b^+ = (a + b)^+$, para todo a e $b \in \mathbb{N}$.

Para os números naturais a, b e c, na expressão $a + b = c$, a e b são ditos serem as **parcelas** e c a **soma**.

Como esperado, da forma mais natural possível, adotaremos as seguintes notações $0^+ = 1$, $1^+ = 2$, $2^+ = 3, \ldots$. Com estas notações, temos por exemplo que

$$\begin{aligned}
&1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2\\
&1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3\\
&2 + 1 = 2 + 0^+ = (2 + 0)^+ = 2^+ = 3\\
&a + 1 = a + 0^+ = (a + 0)^+ = a^+, \text{ para todo } a \in \mathbb{N}.
\end{aligned}$$

Antes de apresentarmos as propriedades da operação de adição, vamos mostrar alguns fatos básicos:

Proposição 5.4. Para todo $a \in \mathbb{N}$, temos $0 + a = a$ e $1 + a = a^+$.

Prova: Considerando $P(a) : 0 + a = a$, para $a \in \mathbb{N}$, temos

(i) $P(0)$ é verdadeira, pois $0 + 0 = 0$.

(ii) Para todo $r \in \mathbb{N}$, se $P(r)$ é verdadeira, então $0 + r = r$. Da definição da adição e deste fato, temos $0 + r^+ = (0 + r)^+ = (r)^+$, ou seja, $P(r^+)$ é também verdadeira.

Assim, pelo primeiro princípio de indução, temos que $P(a)$ é verdadeira para todo $a \in \mathbb{N}$, o que mostra que $0 + a = a$, para todo $a \in \mathbb{N}$.

Agora, para $a \in \mathbb{N}$, se $P(a) : 1 + a = a^+$, então temos

(i) $P(0)$ é verdadeira, pois $1 + 0 = 1 = 0^+$.

(ii) Para todo $r \in \mathbb{N}$, se $P(r)$ é verdadeira, então $1 + r = r^+$. Então $1 + r^+ = (1 + r)^+ = [(r)^+]^+$, ou seja, $P(r^+)$ é também verdadeira.

Assim, de 5.3, temos que $P(a)$ é verdadeira para todo $a \in \mathbb{N}$, o que completa a demonstração da proposição. ■

Usando a definição da adição de números naturais e a proposição acima, mostraremos as principais propriedades da operação de adição.

Teorema 5.5. Para todo a, b e $c \in \mathbb{N}$, temos:

(a) *Associativa* - $a + (b + c) = (a + b) + c$.

(b) *Comutativa* - $a + b = b + a$.

(c) *Elemento neutro* - O zero é o elemento neutro da adição.

(d) *Lei do Cancelamento* - Se $a + b = a + c$, então $b = c$.

(e) Se $a + b = 0$, então $a = b = 0$.

Prova: (a) Faremos por indução sobre c, ou seja, a afirmação $P(c)$ é $(\forall\, a, b \in \mathbb{N})(a + (b + c) = (a + b) + c)$.

(i) $P(0)$ é verdadeira, pois $a + (b + 0) = a + b = (a + b) + 0$.

(ii) Para todo $r \in \mathbb{N}$, se $P(r)$ é verdadeira, então $a + (b + r) = (a + b) + r$. Então $a + (b + r^+) = a + (b + r)^+ = [a + (b + r)]^+ = [(a + b) + r]^+ = (a + b) + r^+$, ou seja, $P(r^+)$ é também verdadeira.

Portanto, pelo primeiro princípio de indução, temos que $P(c)$ é verdadeira para todo $c \in \mathbb{N}$, como queríamos.

(b) Mostraremos usando indução sobre b e 5.4.

(i) Se $b = 0$, então $a + 0 = a = 0 + a$, por 5.4.

(ii) Se $r \in \mathbb{N}$ é tal que $a+r = r+a$, então $a+r^+ = (a+r)^+ = (r+a)^+ = r+a^+$. De 5.4 e do item (a), obtemos $r + a^+ = r + (1 + a) = (r + 1) + a = r^+ + a$, ou seja, o resultado vale para r^+.

Assim, de 5.3, o resultado vale para todo $b \in \mathbb{N}$, como queríamos.

(c) Decorre do item (b) e do mostrado acima que $0+a = a = a+0$, para todo $a \in \mathbb{N}$. Resta mostrar que o zero é o único elemento de $\mathbb{N}$ satisfazendo este fato, ou seja que o elemento neutro é único, mostre este fato como exercício.

(d) Por indução sobre a.

(i) Se $a = 0$, então $0 + b = 0 + c$, o que implica que $b = c$.

(ii) Se o resultado vale para $r \in \mathbb{N}$ e $r^+ + b = r^+ + c$, usando o item (b) obtemos que $r^+ + b = (r + b)^+$, e então $(r + b)^+ = (r + c)^+$ e, do axioma (4) temos $r + b = r + c$. Por hipótese de indução, temos que $b = c$. Assim, o resultado vale para r^+.

Agora, o resultado segue de 5.3.

(e) Sejam a e $b \in \mathbb{N}$ tais que $a + b = 0$ e suponhamos que $b \neq 0$. Então, pela proposição 5.2, temos que $b = r^+$, para algum $r \in \mathbb{N}$. Assim, $0 = a + b = a + r^+ = (a + r)^+$, o que contradiz o axioma (3). Conseqüentemente, $b = 0$ e $a = a + 0 = a + b = 0$. ■

Observação 5.6. Observe que, de 5.4 e 5.5 (b), segue que $a + b^+ = a^+ + b$, para todo a e $b \in \mathbb{N}$.

5.3 Multiplicação em $\mathbb{N}$

A operação de **multiplicação** em $\mathbb{N}$ é definida, também por recorrência, por:

- $a \cdot 0 = 0$, para todo $a \in \mathbb{N}$;
- $a \cdot b^+ = a \cdot b + a$, para todo a e $b \in \mathbb{N}$.

Na multiplicação $a \cdot b = c$, a e b são os **fatores** e c é o **produto**. Vejamos alguns exemplos:

$$1 \cdot 1 = 1 \cdot 0^+ = 1 \cdot 0 + 1 = 0 + 1 = 1$$
$$1 \cdot 2 = 1 \cdot 1^+ = 1 \cdot 1 + 1 = 1 + 1 = 2$$
$$2 \cdot 1 = 2 \cdot 0^+ = 2 \cdot 0 + 2 = 0 + 2 = 2$$
$$a \cdot 1 = a \cdot 0^+ = a \cdot 0 + a = 0 + a = a, \text{ para todo } a \in \mathbb{N}.$$

Decorre da definição e de 5.3, os seguintes fatos básicos:

Proposição 5.7. Para todo $a \in \mathbb{N}$, temos $0 \cdot a = 0$ e $1 \cdot a = a$.

Prova: Para mostrar que $0 \cdot a = a$, para todo $a \in \mathbb{N}$, faremos por indução sobre a. Se $a = 0$, o resultado segue da definição. Se $0 \cdot r = 0$, então $0 \cdot r^+ = 0 \cdot r + 0 = 0 + 0 = 0$. E, o resultado segue de 5.3.

Novamente, por indução sobre a, mostraremos que $1 \cdot a = a$, para todo $a \in \mathbb{N}$. Se $a = 0$, então $1 \cdot 0 = 0$, por definição. Se $1 \cdot r = r$, então $1 \cdot r^+ = 1 \cdot r + 1 = r + 1 = r^+$ e, o resultado segue pelo primeiro princípio de indução. ■

Usando a definição da multiplicação de números naturais e a proposição acima, mostraremos as principais propriedades da operação de multiplicação.

Teorema 5.8. Para todo a, b e $c \in \mathbb{N}$, temos:

(a) *Associativa* - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(b) *Comutativa* - $a \cdot b = b \cdot a$.

(c) *Elemento neutro* - O 1 é o elemento neutro da multiplicação.

(d) *Distributivas* - $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

(e) *Lei do anulamento do produto* - Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Prova: Para demonstrarmos a associatividade e a comutatividade, necessitamos da distributividade. Assim, mostraremos primeiro o item (d).

(d) Por indução sobre c. Se $c = 0$, temos $a \cdot (b + 0) = a \cdot b = a \cdot b + a \cdot 0$.

Se $a \cdot (b + r) = a \cdot b + a \cdot r$, então $a \cdot (b + r^+) = a \cdot (b + r)^+ = a \cdot (b + r) + a = (a \cdot b + a \cdot r) + a = a \cdot b + (a \cdot r + a) = a \cdot b + a \cdot r^+$. Logo, pelo primeiro princípio de indução, temos que $a \cdot (b + c) = a \cdot b + a \cdot c$, para todo a, b e $c \in \mathbb{N}$.

Para demonstrarmos a outra propriedade distributiva, novamente usaremos indução sobre c. Se $c = 0$, então $(a + b) \cdot 0 = 0 = a \cdot 0 + b \cdot 0$.

Se $(a+b)\cdot r = a\cdot r+b\cdot r$, então $(a+b)\cdot r^+ = (a+b)\cdot r+(a+b) = (a\cdot r+b\cdot r)+(a+b)$. Usando a associatividade e a comutatividade da adição, obtemos $(a + b) \cdot r^+ = (a \cdot r + a) + (b \cdot r + b) = a \cdot r^+ + b \cdot r^+$ e, o resultado segue pelo primeiro princípio de indução.

(a) Por indução sobre c. Se $c = 0$, da definição, temos $a \cdot (b \cdot 0) = a \cdot 0 = 0 = (a \cdot b) \cdot 0$.

Se $a \cdot (b \cdot r) = (a \cdot b) \cdot r$, então $a \cdot (b \cdot r^+) = a \cdot (b \cdot r + b)$, e do item (d), obtemos $a \cdot (b \cdot r^+) = a \cdot (b \cdot r) + a \cdot b = (a \cdot b) \cdot r + (a \cdot b) = (a \cdot b) \cdot r^+$. Logo, pelo primeiro princípio de indução, temos que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo a, b e $c \in \mathbb{N}$.

(b) Por indução sobre b. Se $b = 0$, então da definição e de 5.7, temos $a \cdot 0 = 0 = 0 \cdot a$.

Se $a \cdot r = r \cdot a$, então $a \cdot r^+ = a \cdot r + a = r \cdot a + a$. Usando a associatividade e o fato que $1 \cdot a = a$ de 5.7, obtemos $r \cdot a + a = (r + 1) \cdot a = r^+ \cdot a$ e, pelo primeiro princípio de indução, obtemos a comutatividade do produto de números naturais.

(c) Da definição e de 5.7, temos que $a \cdot 1 = a = 1 \cdot a$, para todo $a \in \mathbb{N}$. Resta mostrar a unicidade do elemento neutro, que fica como exercício.

(e) Se $a \cdot b = 0$ e $b \neq 0$, então de 5.2 temos que $b = r^+$, para algum $r \in \mathbb{N}$. Logo $0 = a \cdot b = a \cdot r^+ = a \cdot r + a$, o que implica, do teorema 5.5 (e), que $a = a \cdot r = 0$. ■

5.4 Relação de Ordem em $\mathbb{N}$

Para a e b em $\mathbb{N}$ considere a seguinte relação

$$a \leq b \iff b = a + u, \text{ para algum } u \in \mathbb{N}.$$

Se $b = a + u$, para algum $u \in \mathbb{N}$ com $u \neq 0$, escrevemos $a < b$.
O próximo teorema nos mostra que $\leq$ é uma relação de ordem total sobre $\mathbb{N}$.

Teorema 5.9. A relação $\leq$ é uma relação de ordem total sobre $\mathbb{N}$.

Prova: De fato, valem as seguintes propriedades:

(i) $\leq$ é reflexiva, ou seja, para todo $a \in \mathbb{N}$, temos $a \leq a$, pois $a = a + 0$.

(ii) $\leq$ é anti-simétrica, pois para todo a e $b \in \mathbb{N}$, se $a \leq b$ e $b \leq a$, então existem u e $v \in \mathbb{N}$ tais que $b = a + u$ e $a = b + v$. Logo $b = (b + v) + u$. De onde obtemos $v + u = 0$, o que implica de 5.5 (e) que $u = v = 0$, ou seja, $a = b$.

(iii) $\leq$ é transitiva, pois para todo a, b e $c \in \mathbb{N}$, se $a \leq b$ e $b \leq c$, então existem u e $v \in \mathbb{N}$ tais que $b = a + u$ e $c = b + v$. Assim, $c = (a + u) + v = a + (u + v)$, o que mostra que $a \leq c$.

(iv) Quaisquer dois elementos de $\mathbb{N}$ são comparáveis com respeito a relação $\leq$. De fato, para cada $b \in \mathbb{N}$, considere o conjunto

$$S_b = \{n \in \mathbb{N};\ (n = b + v \text{ para algum } v \in \mathbb{N}) \vee (b = n + u \text{ para algum } u \in \mathbb{N})\}.$$

(i) $0 \in S_b$, pois $b = 0 + b$, o que mostra que $n = 0$ satisfaz a segunda condição para pertencer a S_b.

(ii) Se $r \in S_b$, então ($r = b + v$ para algum $v \in \mathbb{N}$) ou ($b = r + u$ para algum $u \in \mathbb{N}$).

Se $r = b + v$ para algum $v \in \mathbb{N}$, então $r^+ = (b + v)^+ = b + v^+$, para algum $v^+ \in \mathbb{N}$, ou seja, $r^+ \in S_b$.

Se $b = r + u$ para algum $u \in \mathbb{N}$, com $u \neq 0$, então $u = d^+$, para algum $d \in \mathbb{N}$ e, neste caso, $b = r + d^+ = r^+ + d$, o que mostra que $r^+ \in S_b$. Se $b = r$, então $r^+ = b^+ = b + 1$, o que mostra que $r^+ \in S_b$.

De (i) e (ii), pelo primeiro princípio de indução, temos que $S_b = \mathbb{N}$. Conseqüentemente, para todo $b \in \mathbb{N}$, qualquer que seja $a \in \mathbb{N}$, temos que $a \in S_b$, ou seja, $a = b + v$ ou $b = a + u$, com u e $v \in \mathbb{N}$, o que mostra que $b \leq a$ ou $a \leq b$, concluindo a demonstração do teorema. ■

O próximo resultado mostra que esta relação de ordem é compatível com as operações de adição e multiplicação em $\mathbb{N}$. No que segue, usaremos a notação ab para denotar $a \cdot b$, com a e $b \in \mathbb{N}$.

Teorema 5.10. Para todo a, b e $c \in \mathbb{N}$, temos:

(a) *Compatibilidade com a adição* - Se $a \leq b$, então $a + c \leq b + c$.

(b) *Compatibilidade com a multiplicação* - Se $a \leq b$, então $ac \leq bc$.

Prova: (a) Se $a \leq b$, então existe $u \in \mathbb{N}$ tal que $b = a + u$. Logo, da comutatividade e associatividade da adição, temos $b + c = (a + u) + c = (a + c) + u$, o que mostra que $a + c \leq b + c$.

(b) Se $a \leq b$, então existe $u \in \mathbb{N}$ tal que $b = a + u$. Logo, da distributividade, temos $bc = (a + u)c = ac + uc$, com $uc \in \mathbb{N}$, ou seja, $ac \leq bc$. ■

Com respeito a sucessores, temos:

Proposição 5.11. Se a e $b \in \mathbb{N}$ são tais que $a < b$, então $a^+ \leq b$.

Prova: Exercício. ■

Um importante resultado, que está relacionado com o axioma (5) da construção dos naturais, é o princípio do menor elemento.

Teorema 5.12 (Princípio do menor número natural)**.** Todo subconjunto não vazio de $\mathbb{N}$ tem mínimo.

Prova: Seja $S \subseteq \mathbb{N}$, com $S \neq \emptyset$. Queremos mostrar que existe $\min(S)$. Para tanto, considere $H = \{n \in \mathbb{N};\ n \leq x,\ \text{para todo } x \in S\}$.

Como $S \subseteq \mathbb{N}$, temos que $0 \leq a$, para todo $a \in S$, ou seja, $0 \in H$.

Desde que $S \neq \emptyset$, temos que existe $a \in S$. Para tal elemento, $a + 1 \notin H$, pois $a < a + 1 = a^+$. Assim, temos que $H \neq \mathbb{N}$ e, pelo axioma (5), segue que existe $b \in \mathbb{N}$, tal que $b \in H$ e $b^+ \notin H$. Mostremos que $b = \min(S)$.

De fato, como $b \in H$, temos que $b \leq x$, para todo $x \in S$. Resta portanto mostrarmos que $b \in S$. Suponhamos, por absurdo, que $b \notin S$. Então $b < x$, para todo $x \in S$ e, pela proposição 5.11, $b^+ \leq x$, para todo $x \in S$, o que implica que $b^+ \in H$, o que é uma contradição. Portanto $b \in S$ e $b = \min(S)$, como queríamos. ■

Depois da construção axiomática dos números naturais, uma pergunta que surge naturalmente é: *Será que o conjunto formado por zero e seus sucessores esgota realmente o conjunto dos números naturais?* Ou seja, será que não haveria mais números naturais entre um natural e seu sucessor? Mostraremos que não.

Proposição 5.13. Para cada $a \in \mathbb{N}$, não existe $x \in \mathbb{N}$ tal que $a < x < a^+$.

Prova: Suponhamos, por absurdo, que existam a e $x \in \mathbb{N}$ tais que $a < x < a^+$. Como $a < x$, temos que existe $u \in \mathbb{N}$, com $u \neq 0$, tal que $x = a + u$. Mais ainda, como $x < a^+ = a + 1$, temos que existe $v \in \mathbb{N}$, com $v \neq 0$, tal que $a + 1 = x + v$. Logo, $a + 1 = (a + u) + v = a + (u + v)$, o que implica pelo lei do cancelamento da adição, que $u + v = 1$. Mas $v \neq 0$, ou seja, $v = c^+$, para algum $c \in \mathbb{N}$. Assim, $1 = u + v = u + c^+ = u + (c + 1) = (u + c) + 1$ e, novamente, pela lei do cancelamento da adição, obtemos $u + c = 0$. Então de 5.5 (e), $u = c = 0$, o que é uma contradição, pois $u \neq 0$. Portanto não existe $x \in \mathbb{N}$, tal que $a < x < a^+$. ■

Um resultado útil na demonstração de outros é a *lei da tricotomia* em $\mathbb{N}$.

Proposição 5.14 (Lei da Tricotomia)**.** Para todos a e b em $\mathbb{N}$, vale uma e somente uma das relações $a = b$ ou $a < b$ ou $b < a$.

Prova: Para números naturais a e b, desde que $\leq$ é uma ordem total em $\mathbb{N}$, temos que $a \leq b$ ou $b \leq a$. Então $b = a + u$, com $u \in \mathbb{N}$, ou $a = b + v$, com $v \in \mathbb{N}$. Se $a \neq b$, então temos que $u \neq 0$ e $v \neq 0$, ou seja, se $a \neq b$, então $a < b$ ou $b < a$. Resta mostrar que estas duas afirmações não podem ocorrer simultaneamente. De fato, se $a < b$ e $b < a$, então $b = a + u$ com $u \neq 0$ e $a = b + v$ com $v \neq 0$. Assim, $a = (a + u) + v = a + (u + v)$, o que implica, do cancelamento da adição, que $u + v = 0$, com $u \neq 0$ e $v \neq 0$, o que contradiz 5.5 (e). Portanto o resultado segue. ■

Usando a lei da tricotomia, podemos mostrar que vale a lei do cancelamento para o produto.

Proposição 5.15 (Lei do Cancelamento)**.** Se a, b e $c \in \mathbb{N}$ são tais que $c \neq 0$ e $ac = bc$, então $a = b$.

Prova: Se $a < b$, então existe $u \in \mathbb{N}$, com $u \neq 0$, tal que $b = a + u$. Multiplicando por c ambos os lados, obtemos $bc = (a + u)c = ac + uc$. Mas, por hipótese, $ac = bc$, então $uc = 0$, o que contradiz a Lei do Anulamento, pois $u \neq 0$ e $c \neq 0$. De maneira análoga mostra-se que não pode ocorrer $b < a$. Consequentemente, pela lei da tricotomia, temos $a = b$, como queríamos. ■

Finalizamos este capítulo com o seguinte resultado.

Proposição 5.16. Se a e $b \in \mathbb{N}$ são tais que $ab = 1$, então $a = 1$ e $b = 1$.

Prova: Se $ab = 1$, como $1 \neq 0$, temos pela Lei do Anulamento que $a \neq 0$ e $b \neq 0$. Logo, $a \geq 1$ e $b \geq 1$. Suponhamos que $a > 1$. Então existe $u \in \mathbb{N}$, com $u \neq 0$, tal que $a = 1 + u$. Como $b = 1 + v$, para algum $v \in \mathbb{N}$, temos

$$1 = ab = (1 + u)(1 + v) = 1 + u + (v + uv).$$

Usando o cancelamento para a adição e 5.5 (e), obtemos $u = (v + uv) = 0$, o que é uma contradição. Logo $a = 1$ e, consequentemente $b = 1b = ab = 1$, como queríamos. ■

5.5 Exercícios

1. Usando a lei da tricotomia, mostre que para a, b e $c \in \mathbb{N}$, se $ab = ac$ com $a \neq 0$, então $b = c$.

2. Mostre as propriedades abaixo relativas aos números naturais usando o princípio de indução:

   (a) $1.2 + 2.3 + ... + n \cdot (n + 1) = \dfrac{n(n + 1)(n + 2)}{3}$, para todo número natural $n \geq 1$.

   (b) Se $a \geq 2$, então $1 + a + ... + a^n < a^{n+1}$, para todo número natural $n \geq 1$.

   (c) Se $a \geq 2$, então $2a^n \leq a^{n+1}$, para todo número natural $n \geq 1$.

   (d) $1 + 3 + ... + (2n - 1) = n^2$, para todo número natural $n \geq 1$.

   (e) Se $n \geq 3$, então $2n^3 \geq 3n^2 + 3n + 1$.

   (f) $1^2 + 2^2 + 3^2 + ...n^2 = \dfrac{n\,(2n + 1)(n + 1)}{6}$, para todo número natural $n \geq 1$.

3. Mostre, usando indução, que o número de subconjuntos de um conjunto finito com n elementos é 2^n.

4. Mostre que o produto de quatro números naturais consecutivos, acrescidos de 1, é um quadrado perfeito.

5. Seja $x \in \mathbb{N}$. Mostre que $(1 + x)^n > 1 + nx$, para todo $n \geq 2$.

6. Sejam a e b números naturais tais que $a + b = 1$. Mostre que $a = 1$ ou $b = 1$.

7. Sejam a e b números naturais não nulos. Mostre que $a \leq ab$ e $b \leq ab$.

8. Sejam a e b números naturais não nulos tais que $a+b = 2$. Mostre que $a = b = 1$.

9. Sejam a e b números naturais tais que $a \cdot b = 3$. Mostre que $a = 1$ ou $b = 1$.

10. Sejam a e b números naturais não nulos tais que $a + b = 3$. Mostre que $a = 1$ ou $b = 1$.

11. Mostre que dados a e b números naturais, existe um número natural n tal que $na > b$. (Propriedade **Arquimediana** em $\mathbb{N}$)

6
Os Números Inteiros

No conjunto dos números naturais, temos que a equação $a+X=b$, com a e $b \in \mathbb{N}$, tem solução se, e somente se $a \leq b$. Mais ainda, usando que vale o cancelamento para a adição, temos que quando esta equação tem solução, ela é única. Queremos ampliar o conjunto dos naturais, construindo um conjunto onde esta equação sempre tenha solução única, mesmo quando não temos $a \leq b$. Note que a solução será $b-a$, com a e $b \in \mathbb{N}$. Assim, queremos construir um conjunto, "contendo" $\mathbb{N}$, onde faça sentido esta "diferença" e que contenha todas as diferenças deste tipo.

Seguindo essa idéia intuitiva, a construção formal dos números inteiros surgiu da necessidade de se ampliar o conjunto dos naturais para definir a diferença entre dois números naturais a e b, mesmo para $b > a$.

Observe, por exemplo, que expressões do tipo $8-3$, $10-5$, $5-0$, $11-6$, representam, todas, o número 5. Mas, seria muito bom se tivéssemos uma certa unicidade de representação. Note que a igualdade $8-3=10-5$ em $\mathbb{N}$ é equivalente a $8+5=10+3$. Isso nos ajuda a entender a construção que faremos a seguir.

Considere em $\mathbb{N} \times \mathbb{N}$ a relação definida por

$$(a,b) \sim (c,d) \Longleftrightarrow a+d=b+c,$$

para todo (a,b) e $(c,d) \in \mathbb{N} \times \mathbb{N}$.

A relação $\sim$ é uma relação de equivalência sobre $\mathbb{N} \times \mathbb{N}$. De fato,

(i) $\sim$ é reflexiva, pois para cada $(a,b) \in \mathbb{N} \times \mathbb{N}$, temos $a+b=b+a$, ou seja $(a,b) \sim (a,b)$.

(ii) $\sim$ é simétrica, pois para (a,b) e $(c,d) \in \mathbb{N}\times\mathbb{N}$, com $(a,b)\sim(c,d)$, temos $a+d=b+c$, o que implica que $c+b=d+a$, ou seja $(c,d)\sim(a,b)$.

(iii) $\sim$ é transitiva, pois para (a,b), (c,d) e $(e,f) \in \mathbb{N}\times\mathbb{N}$, com $(a,b)\sim(c,d)$ e $(c,d)\sim(e,f)$, temos $a+d=b+c$ e $c+f=d+e$. Somando f em ambos os lados da primeira igualdade e b da segunda, por transitividade obtemos $a+d+f=e+d+b$ e, portanto $a+f=b+e$, ou seja, $(a,b)\sim(e,f)$.

Esta relação de equivalência determina uma partição de $\mathbb{N}\times\mathbb{N}$, em classes de equivalência. Para cada $(a,b)\in\mathbb{N}\times\mathbb{N}$, seja $\overline{(a,b)}$ a classe de equivalência determinada por $(a,b)\in\mathbb{N}\times\mathbb{N}$, isto é,

$$\overline{(a,b)} = \{(x,y)\in\mathbb{N}\times\mathbb{N};\ (x,y)\sim(a,b)\} = \{(x,y)\in\mathbb{N}\times\mathbb{N};\ x+b=y+a\}.$$

O conjunto quociente de $\mathbb{N}\times\mathbb{N}$ pela relação $\sim$, ou seja, o conjunto de todas as classes de equivalência $\overline{(a,b)}$, com $(a,b)\in\mathbb{N}\times\mathbb{N}$, será indicado por $\mathbb{Z}$. Assim

$$\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim = \{\overline{(a,b)};\ (a,b)\in\mathbb{N}\times\mathbb{N}\}.$$

Por exemplo:

$$\overline{(5,1)} = \{(5,1),(4,0),(6,2),\ldots\},$$
$$\overline{(3,2)} = \{(3,2),(4,3),(5,4)...\},$$
$$\overline{(2,5)} = \{(2,5),(0,3),(3,6)...\}.$$

6.1 A adição em $\mathbb{Z}$

Para os números naturais $4=5-1$ e $2=3-1$, temos que $4+2=(5-1)+(3-1)=(5+3)-(1+1)$. Isso nos leva a entender o porque da seguinte definição:

Definição 6.1. Sejam $x=\overline{(a,b)}$ e $y=\overline{(c,d)}$ elementos quaisquer de $\mathbb{Z}$. Definimos a **adição** de x com y, e indicamos por $x+y$, como sendo o elemento de $\mathbb{Z}$

$$x+y = \overline{(a+c,b+d)}.$$

Como estamos definindo a adição de classes de equivalência, necessitamos mostrar que esta definição não depende da escolha dos representantes de cada classe de equivalência.

Exercício 6.2. Mostre que a operação de adição está bem definida, isto é, se $\overline{(a,b)} = \overline{(a_1,b_1)}$ e $\overline{(c,d)} = \overline{(c_1,d_1)}$, mostre que $\overline{(a+c,b+d)} = \overline{(a_1+c_1,b_1+d_1)}$.

Para a adição em $\mathbb{Z}$ temos as principais propriedades:

Teorema 6.3. Para todo x, y e $z \in \mathbb{Z}$, temos:

(a) *Associativa* - $(x+y)+z = x+(y+z)$.

(b) *Comutativa* - $x+y = y+x$.

(c) *Elemento neutro* - Existe $0 = \overline{(0,0)} = \{(x,x) \in \mathbb{N}\times\mathbb{N}\}$, tal que $x+0 = x$, para todo $x \in \mathbb{Z}$.

(d) *Elemento oposto* - Para cada $x \in \mathbb{Z}$, existe $x' \in \mathbb{Z}$ tal que $x+x' = 0$.

(e) *Lei do cancelamento* - Se $x+z = y+z$, então $x = y$.

Prova: (a) Sejam $x = \overline{(a,b)}$, $y = \overline{(c,d)}$ e $z = \overline{(e,f)}$ elementos de $\mathbb{Z}$. Então, usando a associatividade da adição de números naturais, obtemos

$$\begin{aligned}(x+y)+z &= (\overline{(a,b)}+\overline{(c,d)})+\overline{(e,f)} = \overline{(a+c,b+d)}+\overline{(e,f)} = \\ &= \overline{((a+c)+e,(b+d)+f)} = \overline{(a+(c+e),b+(d+f))} = \\ &= \overline{(a,b)}+\overline{(c+e,d+f)} = \overline{(a,b)}+(\overline{(c,d)}+\overline{(e,f)}) = \\ &= x+(y+z),\end{aligned}$$

o que mostra o ítem (a).

(b) Exercício.

(c) Para todo $x = \overline{(a,b)} \in \mathbb{Z}$, queremos mostrar que existe $0 \in \mathbb{Z}$ tal que $x+0 = x$. Seja $0 = \overline{(a',b')} \in \mathbb{Z}$ satisfazendo esta igualdade. Então $x+0 = \overline{(a,b)}+\overline{(a',b')} = \overline{(a+a',b+b')} = \overline{(a,b)} = x$ se, e somente se $(a+a',b+b') \sim (a,b)$, ou seja, $(a+a')+b = (b+b')+a$ em $\mathbb{N}$. Usando as propriedades da adição de números naturais obtemos $a' = b'$. Assim, existe $0 = \overline{(a',a')} = \overline{(0,0)} \in \mathbb{Z}$ satisfazendo o requerido.

(d) Dado $x = \overline{(a,b)} \in \mathbb{Z}$, seja $x' = \overline{(a',b')} \in \mathbb{Z}$ tal que $x+x' = 0$. Então $\overline{(a+a',b+b')} = \overline{(0,0)}$, o que implica que $a+a' = b+b'$ em $\mathbb{N}$. Mas esta igualdade é equivalente a $x' = \overline{(b,a)}$, o que mostra a afirmação do item (d).

(e) Se $x+z=y+z$ então, de (d) temos que existe $z' \in \mathbb{Z}$ tal que $z+z'=0$. Assim, usando as propriedades mostradas acima, obtemos
$x = x+0 = x+(z+z') = (x+z)+z' = (y+z)+z' = y+(z+z') = y+0 = y$,
como queríamos mostrar. ■

Vale observar que da maneira como foi mostrado os ítens (c) e (d), temos que o elemento $0 = \overline{(0,0)}$ é o único elemento de $\mathbb{Z}$ satisfazendo a igualdade do item (c) e, também o elemento $x' = \overline{(b,a)}$ é o único elemento de $\mathbb{Z}$ satisfazendo $x+x'=0$, para $x = \overline{(a,b)} \in \mathbb{Z}$. Assim, dizemos que 0 é o **elemento neutro** da adição e que x' é o **oposto** de x que denotaremos por $-x$. Com esta notação, escrevemos $x-y$ para denotar o elemento $x+(-y)$ em $\mathbb{Z}$ e com isso temos a operação de subtração em $\mathbb{Z}$, dada por

$$\begin{array}{rcl} \mathbb{Z}\times\mathbb{Z} & \to & \mathbb{Z} \\ (x,y) & \mapsto & x-y \end{array}$$

que não é associativa, nem comutativa e não admite elemento neutro. (Verifique!)

Observação 6.4. Para cada $x \in \mathbb{Z}$, temos que $x = \overline{(u,0)}$ ou $x = \overline{(0,u)}$, com $u \in \mathbb{N}$.

De fato, se $x = \overline{(a,b)}$, com $a \geq b$, então existe $u \in \mathbb{N}$ tal que $a = b+u$. Assim, $x = \overline{(b+u,b)} = \overline{(b,b)} + \overline{(u,0)} = \overline{(u,0)}$. Se $x = \overline{(a,b)}$, com $a \leq b$, de maneira análoga mostra-se que $x = \overline{(0,u)}$, com $u \in \mathbb{N}$.

6.2 A multiplicação em $\mathbb{Z}$

Uma maneira nada elegante de multiplicarmos os números naturais $3 = 4-1$ e $2 = 5-3$ é

$$3 \cdot 2 = (4-1)\cdot(5-3) = (4\cdot 5 + 1\cdot 3) - (4\cdot 3 + 1\cdot 5) = 23 - 17 = 6$$

mas, isso nos ajuda a entender a seguinte definição:

Definição 6.5. Para $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$ em $\mathbb{Z}$, definimos a **multiplicação** de x por y e indicamos por $x \cdot y$, ou simplesmente xy, o elemento de $\mathbb{Z}$ dado por

$$xy = \overline{(ac+bd, ad+bc)}.$$

Exercício 6.6. Mostre que a operação de multiplicação está bem definida, isto é, que não depende da escolha dos representantes das classes de equivalência.

As principais propriedades da operação de multiplicação sobre $\mathbb{Z}$ são:

Teorema 6.7. Para todos x, y e $z \in \mathbb{Z}$, temos:

(a) *Associativa* - $x(yz) = (xy)z$;

(b) *Comutativa* - $xy = yx$;

(c) *Elemento Neutro* - Existe $1 = \overline{(1,0)} \in \mathbb{Z}$, tal que $1 \cdot x = x$, para todo $x \in \mathbb{Z}$;

(d) *Distributiva* - $x(y+z) = xy + xz$;

(e) *Lei do Anulamento* - Se x e $y \in \mathbb{Z}$ são tais que $xy = 0$, então $x = 0$ ou $y = 0$.

Prova: A demonstração dos resultados dos ítens (a), (b) e (d) ficam como exercício.

(c) Para todo $x = \overline{(a,b)} \in \mathbb{Z}$, queremos encontrar $x' = \overline{(a',b')} \in \mathbb{Z}$ tal que $xx' = x$.

Se existe tal elemento x', então

$$x = \overline{(a,b)} = xx' = \overline{(a,b)} \cdot \overline{(a',b')} = \overline{(aa'+bb', ab'+ba')},$$

ou seja, $(a,b) \sim (aa'+bb', ab'+ba')$, o que é equivalente a $a + (ab'+ba') = b + (aa'+bb')$ em $\mathbb{N}$, para todo a e $b \in \mathbb{N}$. Em particular, tomando $a = 0$ temos $ba' = b(1+b')$ em $\mathbb{N}$, para todo $b \in \mathbb{N}$. Para $b \neq 0$, temos $a' = 1 + b'$ e, mais ainda, substituindo $a' = 1 + b'$ na equação $xx' = x$, obtemos $a + ab' + b(1+b') = b + a(1+b') + bb'$ em $\mathbb{N}$. Assim, $x' = \overline{(a',b')} = \overline{(1+b',b')} = \overline{(1,0)} + \overline{(b',b')} = \overline{(1,0)}$.

Da maneira como foi encontrado, x' é o único elemento de $\mathbb{Z}$ satisfazendo esta igualdade, o qual denotaremos por $1 = \overline{(1,0)}$.

(d) Da observação 6.4, temos que cada $x \in \mathbb{Z}$ é da forma $x = \overline{(a,0)}$ ou $x = \overline{(0,a)}$, com $a \in \mathbb{N}$. Então, para mostrarmos a Lei do Anulamento em $\mathbb{Z}$, consideremos x e $y \in \mathbb{Z}$ tais que $xy = 0$ e, separemos em quatro casos:

(i) $x = \overline{(a,0)}$ e $y = \overline{(b,0)}$, com a e $b \in \mathbb{N}$.

(ii) $x = \overline{(a,0)}$ e $y = \overline{(0,b)}$, com a e $b \in \mathbb{N}$.

(iii) $x = \overline{(0,a)}$ e $y = \overline{(b,0)}$, com a e $b \in \mathbb{N}$.

(iv) $x = \overline{(0,a)}$ e $y = \overline{(0,b)}$, com a e $b \in \mathbb{N}$.

É fácil ver que em todos os casos, recaímos na igualdade $ab = 0$ em $\mathbb{N}$ e, pela lei do anulamento em $\mathbb{N}$, obtemos $a = 0$ ou $b = 0$, o que implica que $x = 0$ ou $y = 0$ em $\mathbb{Z}$. ■

O conjunto $\mathbb{Z}$, com as operações de adição e multiplicação introduzidas acima, é dito ser o **conjunto dos números inteiros** e, seus elementos são chamados **números inteiros**. Mais, ainda, usando a observação 6.4, podemos separar este conjunto em dois subconjuntos

$$\mathbb{Z}_+ = \{\overline{(a,0)} \in \mathbb{Z};\ a \in \mathbb{N}\}, \qquad \text{e} \qquad \mathbb{Z}_- = \{\overline{(0,a)} \in \mathbb{Z};\ a \in \mathbb{N}\}.$$

Os elementos de $\mathbb{Z}_+$ são ditos serem **inteiros positivos** e os de $\mathbb{Z}_-$ **inteiros negativos**. Note que para $x \in \mathbb{Z}$, temos $x \in \mathbb{Z}_+$ se, e somente se $-x \in \mathbb{Z}_-$. Esta nomenclatura ficará clara na próxima seção.

6.3 Relação de Ordem em $\mathbb{Z}$

A relação de ordem em $\mathbb{Z}$ é definida de maneira análoga a dos números naturais.

Definição 6.8. Sejam x e $y \in \mathbb{Z}$. Dizemos que x é **menor ou igual** a y, e escrevemos $x \leq y$, se $x = y + z$ para algum $z \in \mathbb{Z}_+$. Também podemos escrever $y \geq x$, e dizer y é **maior ou igual** a x. Se $z \in \mathbb{Z}_+$, com $z \neq 0$, escrevemos $x < y$, e dizemos x é **menor** do que y. Equivalentemente $y > x$.

Observe que para todo $x \in \mathbb{Z}_+$, temos que $0 \leq x$, pois $x = 0 + x$ e, para $y \in \mathbb{Z}_-$, temos que $y \leq 0$, pois $-y \in \mathbb{Z}_+$ e $0 = y + (-y)$. Isso justifica a nomenclatura usada no final da seção anterior.

Proposição 6.9. A relação $\leq$ é uma relação de ordem total sobre $\mathbb{Z}$.

Prova: Demonstrar que é uma relação de ordem sobre $\mathbb{Z}$, fica como exercício. Mostraremos somente que é total, ou seja, que quaisquer dois elementos de $\mathbb{Z}$ são comparáveis com respeito a esta relação.

Sejam x e $y \in \mathbb{Z}$. Temos novamente quatro casos a considerar:

(i) $x = \overline{(a,0)}$ e $y = \overline{(b,0)}$, com a e $b \in \mathbb{N}$.

Neste caso, como $a \leq b$ ou $b \leq a$ em $\mathbb{N}$, temos que existe $u \in \mathbb{N}$ tal que $b = a + u$ ou $a = b + u$. Assim, $y = \overline{(b,0)} = \overline{(a+u,0)} = x + \overline{(u,0)}$, ou

$x = \overline{(a,0)} = \overline{(b+u,0)} = y + \overline{(u,0)}$, com $\overline{(u,0)} \in \mathbb{Z}_+$, o que mostra que $x \leq y$ ou $y \leq x$.

(ii) $x = \overline{(a,0)}$ e $y = \overline{(0,b)}$, com a e $b \in \mathbb{N}$.

Neste caso, $x = \overline{(a,0)} = \overline{(a+b,b)} = \overline{(a+b,0)} + y$, com $\overline{(a+b,0)} \in \mathbb{Z}_+$, ou seja $y \leq x$.

(iii) $x = \overline{(0,a)}$ e $y = \overline{(b,0)}$, com a e $b \in \mathbb{N}$.

Análogo ao caso anterior, obtemos neste caso que $x \leq y$.

(iv) $x = \overline{(0,a)}$ e $y = \overline{(0,b)}$, a e $b \in \mathbb{N}$.

De maneira análoga ao caso (i), obtemos $x \leq y$ ou $y \leq x$. ■

Note que, como conseqüência da proposição anterior, temos que se $x \in \mathbb{Z}_-$ e $y \in \mathbb{Z}_+$, então $x \leq y$.

O próximo resultado mostra que esta relação de ordem é compatível com as operações de adição e multiplicação em $\mathbb{Z}$.

Proposição 6.10. Sejam x, y e $z \in \mathbb{Z}$.

(a) *Compatibilidade com a adição* - Se $x \leq y$, então $x + z \leq y + z$.

(b) *Compatibilidade com a multiplicação* - Se $x \leq y$ e $0 \leq z$, então $xz \leq yz$.

Prova: (a) Se $x \leq y$, então existe $w \in \mathbb{Z}_+$ tal que $y = x + w$. Logo, de 6.7 segue que $y + z = (x + w) + z = (x + z) + w$, com $w \in \mathbb{Z}_+$, ou seja $x + z \leq y + z$.

(b) Se $x \leq y$, então existe $w = \overline{(a,0)} \in \mathbb{Z}_+$ tal que $y = x + w$. Se $z = \overline{(b,0)}$, novamente de 6.7 obtemos $yz = (x + w)z = xz + wz$, com $wz = \overline{(ab,0)} \in \mathbb{Z}_+$. Portanto, $xz \leq yz$. ■

6.4 A Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Nesta seção estamos interessados em identificar $\mathbb{N}$ com um subconjunto de $\mathbb{Z}$. Isto será feito através de uma imersão, ou seja, uma função injetora $f : \mathbb{N} \to \mathbb{Z}$, que preserva as operações de adição e multiplicação e as relações de ordem.

Definimos $f : \mathbb{N} \to \mathbb{Z}$, por $f(a) = \overline{(a,0)}$, para todo $a \in \mathbb{N}$. Temos então:

- $\text{Im}(f) = \{f(a);\ a \in \mathbb{N}\} = \mathbb{Z}_+$.

- f é injetora, ou seja, se $f(a) = f(b)$, então $\overline{(a,0)} = \overline{(b,0)}$ em $\mathbb{Z}$, o que implica que $a = b$ em $\mathbb{N}$, para todo a e $b \in \mathbb{N}$.

- f preserva as operações de adição, ou seja, $f(a+b) = \overline{(a+b,0)} = \overline{(a,0)} + \overline{(b,0)} = f(a) + f(b)$, para todo a e $b \in \mathbb{N}$.

- f preserva as operações de multiplicação, ou seja, $f(ab) = \overline{(ab,0)} = \overline{(a,0)} \cdot \overline{(b,0)} = f(a)f(b)$, para todo a e $b \in \mathbb{N}$.

- f preserva as relações de ordem, ou seja, se $a \leq b$ em $\mathbb{N}$, então existe $u \in \mathbb{N}$ tal que $b = a + u$. Logo, $f(b) = \overline{(b,0)} = \overline{(a+u,0)} = \overline{(a,0)} + \overline{(u,0)} = f(a) + \overline{(u,0)}$, com $\overline{(u,0)} \in \mathbb{Z}_+$, o que implica que $f(a) \leq f(b)$ em $\mathbb{Z}$.

Assim, no que se refere aos aspectos algébricos e quanto a ordenação, $\mathbb{Z}_+$ é uma cópia de $\mathbb{N}$ dentro de $\mathbb{Z}$. É coerente portanto, identificarmos N com $\mathbb{Z}_+$ através de f e considerarmos que $\mathbb{N} \subseteq \mathbb{Z}$. Mais especificamente, identificaremos o número natural 0 com o número inteiro $\overline{(0,0)}$, o número natural 1 com o número inteiro $\overline{(1,0)}$ e, mas geralmente, o número natural a com o número inteiro $\overline{(a,0)}$. Isso feito, temos que $\mathbb{N} = \mathbb{Z}_+$ e, para cada elemento $\overline{(0,b)} \in \mathbb{Z}_-$, temos $\overline{(0,b)} = -\overline{(b,0)}$ que será identificado com $-b$, ou seja $\mathbb{Z}_- = \{-b;\ b \in \mathbb{N}\}$, como era de se esperar.

Assumindo estas identificações, temos

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

e cada número inteiro x pode ser visto como uma diferença de dois números naturais, isto é, $x = \overline{(a,b)} = \overline{(a,0)} + \overline{(0,b)} = a - b$, com a e $b \in \mathbb{N}$, mesmo quando $a \leq b$, que era o que tínhamos em vista com a construção do conjunto dos números inteiros.

6.5 Valor Absoluto

Como em $\mathbb{Z}$ temos a noção de inteiros negativos, podemos definir o valor absoluto de um número inteiro.

Definição 6.11. Seja $a \in \mathbb{Z}$. O **valor absoluto** ou **módulo** de a é o número inteiro $|a|$, definido por:

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

Temos as seguintes propriedades básicas:

Proposição 6.12. Sejam a e $b \in \mathbb{Z}$. Então:

(a) $|a| = |-a|$.

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

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

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

Prova: Se $a = 0$ ou $b = 0$, as afirmações são imediatas. Então assumiremos que $a \neq 0$ e $b \neq 0$. Note que $a > 0$ se, e somente se $-a < 0$, para todo $a \in \mathbb{Z}$, com $a \neq 0$.

(a) Se $a > 0$, então $|a| = a = -(-a) = |-a|$.

Se $a < 0$, então $|a| = -a = |-a|$.

(b) Se $a > 0$, então $|a| = a$ e $-|a| = -a < a = |a|$, ou seja, $-|a| \leq a \leq |a|$.

Se $a < 0$, então $|a| = -a$ e $-|a| = a < |a|$, ou seja, $-|a| \leq a \leq |a|$.

(c) Se $a > 0$ e $b > 0$, então $ab > 0$ e, portanto, $|ab| = ab = |a||b|$.

Se $a > 0$ e $b < 0$, temos que $|a| = a$, $|b| = -b$, $|ab| = -(ab)$. Daí, $|a||b| = a(-b) = -ab$ e, portanto, $|ab| = |a||b|$. O caso em que $a < 0$ e $b > 0$, é análogo.

Se $a < 0$ e $b < 0$, então $|a| = -a$, $|b| = -b$ e, como $ab > 0$, segue que $|ab| = ab$. Daí, $|a||b| = (-a)(-b) = ab$, e então $|ab| = |a||b|$.

(d) Temos do item (b) que $-|a| \leq a \leq |a|$ e $-|b| \leq b \leq |b|$. Somando membro a membro, obtemos $-(|a| + |b|) \leq a + b \leq |a| + |b|$.

Se $|a+b| = a + b$, como $a + b \leq |a| + |b|$, segue que $|a+b| \leq |a| + |b|$.

Se $|a+b| = -(a+b)$, então $-|a+b| = a + b$ e, como $-(|a| + |b|) \leq a + b$, temos $-(|a| + |b|) \leq -|a+b|$. Portanto $|a+b| \leq |a| + |b|$. ■

Exercício 6.13. Mostre que $|a| - |b| \leq |a - b| \leq |a| + |b|$, para todo a e $b \in \mathbb{Z}$.

6.6 Aritmética em $\mathbb{Z}$

6.6.1 Múltiplos e Divisores

Nesta seção apresentaremos as noções de múltiplos e divisores e suas principais propriedades.

Definição 6.14. Sejam a e $b \in \mathbb{Z}$. Dizemos que a **divide** b se existir $c \in \mathbb{Z}$ tal que $b = ac$. Também denotamos tal número inteiro c por $\frac{b}{a}$. Neste caso também dizemos que a **é divisor de** b ou que b **é múltiplo de** a e, denotamos este fato por $a \mid b$. Caso contrário, dizemos que a **não divide** b e escrevemos $a \nmid b$.

Exemplo 6.15. Por exemplo, $1 \mid a$, para todo $a \in \mathbb{Z}$, pois $a = 1 \cdot a$. Mas, $a \mid 1$ se, e somente se $a = \pm 1$, pois $1 = ab$ em $\mathbb{Z}$ se, e somente se $a = b = \pm 1$.

Para o inteiro zero temos, $a \mid 0$, para todo $a \in \mathbb{Z}$, pois $0 = a \cdot 0$. Mas, $0 \mid a$, se e somente se $a = 0$, pois $0 \cdot b = 0$, para todo $b \in \mathbb{Z}$.

As principais propriedades da relação de divisibilidade em $\mathbb{Z}$, são:

Proposição 6.16. Sejam a, b, c e $d \in \mathbb{Z}$.

(a) *Reflexiva* - $a \mid a$, para todo $a \in \mathbb{Z}$.

(b) Se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$.

(c) Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

(d) *Transitiva* - Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(e) Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, para todo x e $y \in \mathbb{Z}$.

(f) $a \mid b$ se, e somente se $|a| \mid |b|$.

(g) Se $a = b + c$ e $d \mid c$, então $d \mid a$ se, e somente se $d \mid b$.

Prova: Mostraremos as afirmações dos ítens (c) e (e), ficando as outras como exercício.

Se $a \mid b$ e $b \mid a$, então existem a' e $b' \in \mathbb{Z}$ tais que $b = aa'$ e $a = bb'$. Logo, $b = (bb')a'$, o que implica que $a'b' = 1$ em $\mathbb{Z}$, de onde segue que $a' = b' = \pm 1$, ou seja $a = \pm b$, mostrando assim a afirmação do ítem (c).

Para o ítem (e), se $a \mid b$ e $a \mid c$, então existem a' e $b' \in \mathbb{Z}$ tais que $b = aa'$ e $c = ab'$. Então $bx + cy = aa'x + ab'y = a(a'x + b'y)$, com $a'x + b'y \in \mathbb{Z}$, ou seja, $a \mid (bx + cy)$. ■

6.6.2 Algoritmo da divisão ou algoritmo de Euclides

Dados dois números inteiros a e b, sabemos que se $b \mid a$, então existe um número inteiro c tal que $a = bc$. Quando $b \nmid a$, será que podemos pensar em algo parecido? Nesta direção temos o algoritmo da divisão, ou algoritmo de Euclides que diz que para cada par de números inteiros a e b, existem únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$. Note que este algoritmo não tem sentido se $b = 0$, pois $a = qb + r$, daria $a = r$ o que contradiz $0 \leq r < 0$.

Mostraremos primeiramente a existência dos inteiros q e r no caso em que $a \geq 0$ e $b > 0$.

Lema 6.17. Sejam a e $b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem números inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$.

Prova: Consideremos o conjunto $S = \{a - bx;\ x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$.

Se $x = 0$, temos que $a - bx = a \geq 0$ é um elemento de S, ou seja, $S \neq \emptyset$. Pelo princípio do menor número natural, temos que existe $r = \min(S)$. Como $r \in S$, podemos escrever r na forma $r = a - bq \geq 0$, para algum $q \in \mathbb{Z}$. Resta agora mostrar que $r < b$.

Suponhamos que $r \geq b$. Então temos que $a - b(q + 1) = a - bq - b = r - b \geq 0$ e, portanto, $a - b(q + 1) \in S$. Mas isto é uma contradição, pois $a - b(q + 1) = r - b < r = \min(S)$. Logo $r < b$, como queríamos. ■

Mostremos agora o caso geral.

Teorema 6.18 (Algoritmo da Divisão)**.** Sejam a e $b \in \mathbb{Z}$ com $b \neq 0$. Então existem únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.

Prova: Mostremos primeiramente a existência dos números inteiros q e r. Começamos considerando $b > 0$ e $a \in \mathbb{Z}$.

O caso $a \geq 0$ segue do lema anterior. Consideremos então $a < 0$. Do lema anterior, temos que existem q' e $r' \in \mathbb{Z}$, tais que $|a| = bq' + r'$, com $0 \leq r' < b$. Como $|a| = -a$,

temos que $a = b(-q') - r'$. Se $r' = 0$, basta tomar $q = q'$ e $r = 0$. Se $r' > 0$ temos que $a = b(-q') - r' = b(-q') - b + (b - r') = b(-q' - 1) + (b - r')$ e, neste caso, basta tomar $q = -q' - 1$ e $r = b - r'$.

Seja agora $b < 0$. Para todo $a \in \mathbb{Z}$, do feito acima, existem q' e $r' \in \mathbb{Z}$, tais que $a = |b|q' + r'$, com $0 \leq r' < |b|$. Ou seja, $a = (-b)q' + r' = b(-q') + r'$. E, agora, basta tomar $q = -q'$ e $r = r'$.

Mostremos agora a unicidade dos números inteiros q e r. Suponhamos que existem inteiros q, r, q' e r' satisfazendo as condições do teorema. Então $a = bq + r = bq' + r'$. Isto implica que $b(q - q') = r' - r$. Assim $|b(q - q')| = |r' - r|$ e, como $|b| > r'$ e $|b| > r$, temos que $|r' - r| < |b|$ e, consequentemente, $|b||(q - q')| < |b|$. Mas $|b| > 0$, logo segue que $0 \leq |q - q'| < 1$, ou seja, $|q - q'| = 0$, o que implica que $q = q'$. Substituindo na igualdade $a = bq + r = bq' + r'$ segue que $r = r'$, o que finaliza a demonstração do teorema. ■

Na expressão $a = bq + r$, com $0 \leq r < |b|$, o número inteiro a é chamado de **dividendo**, b de **divisor**, q de **quociente** e r de **resto**.

Exemplo 6.19. Para $a = -79$ e $b = 11$, encontre números inteiros q e r tais que $-79 = 11\,q + r$, com $0 \leq r < 11$.

Fazendo a divisão de 79 por 11 encontramos $79 = 11 \cdot 7 + 2$ e, multiplicando ambos os membros por -1 obtemos $-79 = 11\,(-7) + (-2)$. Claramente, o resto -2 não satisfaz a exigência $0 \leq r < 11$ mas, adicionando e subtraindo 11, obtemos

$$-79 = [11\,(-7) - 11] + [-2 + 11] = 11\,(-8) + 9.$$

Como $0 \leq 9 < 11$, temos que $q = -8$ e $r = 9$ satisfazem o requerido.

6.6.3 Máximo Divisor Comum

Nesta seção apresentamos a definição de máximo divisor comum de dois números inteiros. Mostramos que sempre existe o máximo divisor comum de quaisquer dois inteiros dados e, mais ainda, que ele é único.

Definição 6.20. Sejam a e $b \in \mathbb{Z}$. Dizemos que o número inteiro d é um **máximo divisor comum** de a e b se:

(i) $d \geq 0$.

(ii) $d \mid a$ e $d \mid b$;

(iii) Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

Começamos mostrando a unicidade.

Proposição 6.21. Para números inteiros a e b, se existir um máximo divisor comum de a e b, então ele é único.

Prova: Sejam d e d' em $\mathbb{Z}$ dois máximos divisores comum de a e b. Então d e d' satisfazem as condições (i), (ii) e (iii) da definição 6.20. Usando que (ii) vale para d e que (iii) vale para d', obtemos que $d \mid d'$. Analogamente, usando que (ii) vale para d' e que (iii) vale para d, obtemos que $d' \mid d$. Assim, $d \mid d'$ e $d' \mid d$. De 6.16 (c), temos que $d = \pm d'$ e, usando (i), obtemos $d = d'$. ■

Desde que temos a unicidade, quando existir o máximo divisor comum d de a e b, escreveremos $d = \text{mdc}(a, b)$, ou seja, no que segue, sempre que escrevermos $d = \text{mdc}(a, b)$ estará subentendido que existe o máximo divisor comum de a e b e que ele é igual a d.

Para mostrarmos a existência iniciaremos com alguns resultados auxiliares.

Proposição 6.22. Sejam a e $b \in \mathbb{Z}$. Então $\text{mdc}(a, b) = \text{mdc}(|a|, b) = \text{mdc}(a, |b|) = \text{mdc}(|a|, |b|)$.

Prova: Segue diretamente da definição e de 6.16 (d). ■

Usando 6.22 é suficiente mostrarmos a existência do máximo divisor comum de dois inteiros positivos. Mais ainda, da próxima proposição, podemos assumir que os dois números inteiros são não nulos.

Proposição 6.23. Se $a = 0$, então $\text{mdc}(a, b) = |b|$, para todo $b \in \mathbb{Z}$.

Prova: Segue diretamente da definição e do fato que $b \mid 0$, para todo $b \in \mathbb{Z}$. ■

Proposição 6.24. Se $a \mid b$, então $\text{mdc}(a, b) = |a|$.

Prova: De fato, $|a|$ satisfaz:

(i) $|a| \geq 0$.

(ii) $|a| \mid a$ e $|a| \mid b$;

(iii) Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $c \mid |a|$;

ou seja, $|a| = \text{mdc}(a, b)$. ■

Proposição 6.25. Se $a = bq + r$ em $\mathbb{Z}$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Prova: Por 6.22, podemos assumir que $a \geq 0$ e $b \geq 0$. Se $d = \text{mdc}(a, b)$, então $d \mid a$ e $d \mid b$. De 6.16 (e), temos que $d \mid a - bq = r$. Portanto $d \mid b$ e $d \mid r$.

Por outro lado, se $c \mid b$ e $c \mid r$, então novamente por 6.16 (e), obtemos $c \mid bq + r = a$. Portanto $c \mid a$ e $c \mid b$, o que implica que $c \mid d = \text{mdc}(a, b)$. Logo, $d = \text{mdc}(b, r)$, como queríamos demonstrar. ■

Usando os resultados acima, mostraremos agora que existe o máximo divisor comum de quaisquer dois inteiros.

Teorema 6.26. Dados a e b em $\mathbb{Z}$, temos que existe $d \in \mathbb{Z}$ satisfazendo a definição 6.20.

Prova: Usando que $\text{mdc}(a, b) = \text{mdc}(b, a)$ e os resultados acima, podemos assumir que $a \geq b > 0$. Assim, aplicando o algoritmo da divisão repetidas vezes obtemos:

$$\begin{aligned} a &= b\,q + r_1, \quad \text{com} \quad 0 \leq r_1 < b, \\ b &= r_1\,q_2 + r_2, \quad \text{com} \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2\,q_3 + r_3, \quad \text{com} \quad 0 \leq r_3 < r_2, \\ &\vdots \end{aligned}$$

Observe que, o fato de $b > r_1 > r_2 > r_3 > \cdots \geq 0$, implica que existe um menor índice n tal que $r_{n+1} = 0$. Assim, para algum n, temos:

$$\begin{aligned} r_{n-2} &= r_{n-1}\,q_n + r_n, \quad \text{com} \quad 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n\,q_{n+1}. \end{aligned}$$

Da proposição 6.25 temos que

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n-1}, r_n).$$

Como $r_n \mid r_{n-1}$, segue de 6.24 que $\text{mdc}(r_{n-1}, r_n) = r_n$, e portanto, $\text{mdc}(a, b)$ existe e é igual a r_n, que é o último resto diferente de zero. ■

Exemplo 6.27. Encontre $\text{mdc}(3248, 226)$.

Aplicando o algoritmo da divisão até chegarmos em um resto igual a zero, temos:

$$\begin{aligned} 3248 &= 14 \cdot 226 + 84 \\ 226 &= 2 \cdot 84 + 58 \\ 84 &= 1 \cdot 58 + 26 \\ 58 &= 2 \cdot 26 + 6 \\ 26 &= 4 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Logo, $\text{mdc}(3248, 226) = 2$.

Podemos representar estas divisões repetidas através de uma tabela da seguinte forma:

	14	2	1	2	4	3
3248	226	84	58	26	6	2
84	58	26	6	2	0	

Definição 6.28. Dizemos que dois números inteiros a e b são **primos entre si** ou que a é **primo** com b se $\text{mdc}(a, b) = 1$.

O próximo resultado mostra que o máximo divisor comum de dois números inteiros é uma combinação inteira destes números.

Proposição 6.29. Sejam a e $b \in \mathbb{Z}$. Se $d = \text{mdc}(a, b)$, então existem x_0 e $y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$.

Prova: Se $a = b = 0$, então $d = 0$ e quaisquer x_0, $y_0 \in \mathbb{Z}$ satisfazem o requerido.

Se $a \neq 0$ ou $b \neq 0$, considere $S = \{ax + by;\ x, y \in \mathbb{Z}\}$.

Como $a \cdot a + b \cdot b = a^2 + b^2 > 0$ e $a^2 + b^2 \in S$, temos que em S existem elementos estritamente positivos. Logo, pelo princípio do menor número natural, existe o menor deles. Seja d este mínimo. Agora é suficiente mostrar que $d = \text{mdc}(a, b)$. De fato:

(i) $d \geq 0$ pela maneira como foi escolhido.

(ii) Como $d \in S$, temos que existem x_0 e $y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Do algoritmo da divisão temos que $a = dq + r$, com $0 \leq r < d$. Substituindo d nesta igualdade obtemos

$$a = (ax_0 + by_0)q + r,$$

de onde segue que

$$r = a(1 - qx_0) + b[q(-y_0)].$$

Assim, $r \in S$ e, como $r \geq 0$, pela minimalidade de d, temos que $r = 0$. Portanto $a = dq$, o que mostra que $d \mid a$.

De maneira análoga mostra-se que $d \mid b$.

(iii) Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então de 6.16 (e) temos que $c \mid d = ax_0 + by_0$. ■

Em geral, não vale a volta de 6.29, somente quando $d = 1$, ou seja, quando os inteiros a e b são primos entre si.

Corolário 6.30. Dois números inteiros a e b são primos entre si se, e somente se existem x_0 e $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$.

Prova: ($\Longrightarrow$) Segue de 6.29 para $d = 1$.

($\Longleftarrow$) É imediato que $1 \geq 0$, $1 \mid a$ e $1 \mid b$. Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então de 6.16 (e) temos que $c \mid ax_0 + by_0 = 1$, o que mostra que $1 = \text{mdc}(a, b)$. ■

Observação 6.31. Uma maneira de encontrar os inteiros x_0 e y_0 satisfazendo a igualdade de 6.29 é usando as divisões sucessivas da demonstração da proposição 6.26. Vejamos como fazer utilizando o exemplo 6.27.

Vimos em 6.27 que $2 = \text{mdc}(3248, 226)$, obtido através das divisões sucessivas:

$$\begin{aligned}
3248 &= 14 \cdot 226 + 84 \\
226 &= 2 \cdot 84 + 58 \\
84 &= 1 \cdot 58 + 26 \\
58 &= 2 \cdot 26 + 6 \\
26 &= 4 \cdot 6 + 2 \\
6 &= 3 \cdot 2 + 0
\end{aligned}$$

Isolando os restos em cada uma das igualdades acima e, começando na penúltima igualdade e substituindo os respectivos restos em cada uma delas, em ordem inversa, obtemos:

$$\begin{aligned}
2 &= 26 - 4 \cdot 6 \\
&= 26 - 4 \cdot (58 - 2 \cdot 26) = -4 \cdot 58 + 9 \cdot 26 \\
&= -4 \cdot 58 + 9 \cdot (84 - 1 \cdot 58) = 9 \cdot 84 - 13 \cdot 58 \\
&= 9 \cdot 84 - 13 \cdot (226 - 2 \cdot 84) = -13 \cdot 226 + 35 \cdot 84 \\
&= -13 \cdot 226 + 35 \cdot (3248 - 14 \cdot 226) = 35 \cdot 3248 - 503 \cdot 226.
\end{aligned}$$

Assim, $x_0 = 35$ e $y_0 = -503$ satisfaz

$$2 = \text{mdc}(3248, 226) = 3248 \cdot x_0 + 226 \cdot y_0.$$

Observe também que esta não é a única solução, somando e subtraindo números inteiros convenientes, obtemos outras soluções.

Corolário 6.32. Se a e b são números inteiros com $a \neq 0$ ou $b \neq 0$ e $d = \text{mdc}(a, b)$, então

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

Prova: Como $a \neq 0$ ou $b \neq 0$, temos que $d = \text{mdc}(a, b) > 0$. De 6.29 temos que existem x_0 e $y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Então,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1,$$

e o resultado segue do corolário 6.30. ■

Também como conseqüência da proposição 6.29, temos os seguintes resultados sobre divisibilidade de números inteiros:

Corolário 6.33. Se a, b e c são números inteiros com $a \mid bc$ e $\text{mdc}(a, b) = 1$, então $a \mid c$.

Prova: De 6.29 temos que existem x_0 e $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Então, $(ac)x_0 + (bc)y_0 = c$ e, como $a \mid ac$ e $a \mid bc$, de 6.16 (e), temos que $a \mid c$. ■

Corolário 6.34. Se a e b são números inteiros divisores do inteiro $c \neq 0$ e $\text{mdc}(a, b) = 1$, então $ab \mid c$.

Prova: De 6.29 temos que existem x_0 e $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Então, $(ac)x_0 + (bc)y_0 = c$. Como $a \mid c$ e $b \mid c$, temos que $ab \mid bc$ e $ab \mid ac$. Novamente de 6.16 (e), obtemos que $ab \mid c$. ■

Observação 6.35. A noção de máximo divisor comum pode ser estendida, por recorrência, para mais de dois números inteiros, ou seja, para $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, temos

$$\text{mdc}(a_1, a_2, \ldots, a_n) = \text{mdc}(\text{mdc}(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Nestas condições temos que $d \in \mathbb{Z}$ é o máximo divisor comum dos números inteiros $a_1, a_2, \ldots, a_n$ se, e somente se

(i) $d \geq 0$.

(ii) $d \mid a_i$, para todo $i = 1, \ldots, n$.

(iii) Se $c \in \mathbb{Z}$ é tal que $c \mid a_i$, para todo $i = 1, \ldots, n$, então $c \mid d$.

6.6.4 Mínimo Múltiplo Comum

Agora, apresentamos a definição de mínimo múltiplo comum de dois números inteiros.

Definição 6.36. Sejam a e $b \in \mathbb{Z}$. Dizemos que o número inteiro m é um **mínimo múltiplo comum** de a e b se:

(i) $m \geq 0$;

(ii) m é múltiplo de a e de b, isto é, $a \mid m$ e $b \mid m$;

(iii) Se $m' \in \mathbb{Z}$ for múltiplo de a e de b, então m' será múltiplo de m, isto é, $m \mid m'$.

A existência e a unicidade do mínimo múltiplo comum de dois inteiros, segue diretamente da proposição abaixo, pois o máximo divisor comum de dois números inteiros existe e é único, assim como o valor absoluto de um número inteiro.

Proposição 6.37. Sejam a e $b \in \mathbb{Z}$. Então existe um número inteiro m tal que

$$\text{mdc}(a,b) \cdot m = |ab| = |a|\,|b|,$$

e, tal inteiro é um mínimo múltiplo comum da a e b.

Prova: Note que se $a = 0$ ou $b = 0$, então $m = 0$ satisfaz a igualdade acima e também a definição 6.36. Podemos então supor que a e b são não nulos e, neste caso, $d = \text{mdc}(a,b) \neq 0$.

Vamos então mostrar que $m = \dfrac{|ab|}{d}$ satisfaz a definição 6.36.

(i) É óbvio que $m \geq 0$.

(ii) Escrevendo $m = |a| \cdot \dfrac{|b|}{d}$, como $d \mid b$, temos que $\dfrac{|b|}{d} \in \mathbb{Z}$ e, consequentemente, $a \mid |a| \mid m$. Analogamente, mostra-se que $b \mid m$, ou seja m é múltiplo de a e de b.

(iii) Seja $m' \in \mathbb{Z}$ múltiplo de a e de b.

Então existem r e $s \in \mathbb{Z}$ tais que $m' = ar$ e $m' = bs$. Mais ainda, como $d \mid a$ e $d \mid b$, temos que existem a' e $b' \in \mathbb{Z}$ tais que $a = a'd$ e $b = b'd$ e, do corolário 6.32, temos que $\text{mdc}(a', b') = 1$.

Substituindo a e b na igualdade $m' = ar = bs$ e usando que $d \neq 0$, obtemos $a'r = b's$. Logo $a' \in \mathbb{Z}$ é tal que $a' \mid b's$ com $\text{mdc}(a', b') = 1$, o que implica do corolário 6.33 que $a' \mid s$, ou seja $s = a's'$, para algum $s' ain\mathbb{Z}$. Assim, $m' = bs = b(a's') = (a'b)s' = \dfrac{ab}{d}s'$, para algum $s' \in \mathbb{Z}$, de onde segue que $m \mid m'$.

Assim, $m = \dfrac{|ab|}{d}$ satisfaz a definição 6.36, como queríamos mostrar. ■

Provado a existência e a unicidade do mínimo múltiplo comum de dois números inteiros a e b, o denotaremos por $\text{mmc}(a,b)$.

Observe que, como no caso do $\text{mdc}(a,b)$, usando 6.37, podemos calcular o $\text{mmc}(a,b)$ sem necessariamente fatorar os números inteiros a e b.

De maneira análoga ao feito para o máximo divisor comum, podemos definir, usando recorrência, o mínimo múltiplo comum de mais de dois números inteiros.

6.7 Números Primos

O objetivo desta seção é demonstrar o Teorema Fundamental da Aritmética para números inteiros. Iniciamos com a noção de números primos.

Definição 6.38. Dizemos que um número inteiro p, com $p \neq 0$ e $p \neq \pm 1$ é **primo** se os únicos divisores de p são ± 1 e $\pm p$. Se $a \in \mathbb{Z}$, com $a \neq 0$ e $a \neq \pm 1$ não é primo, então dizemos que a é **composto**.

Observação 6.39. Note que um número inteiro composto a pode sempre ser fatorado num produto $a = bc$, onde $b \neq \pm 1$ e $c \neq \pm 1$. Mais ainda, devido as propriedades de divisibilidade, temos que um número inteiro negativo p é primo se, e somente se $|p|$ é primo.

O primeiro resultado sobre números primos relaciona estes com divisibilidade e, de fato fornece uma definição equivalente de número inteiro primo.

Proposição 6.40. Sejam a, b, e $p \in \mathbb{Z}$. Se p é primo e $p \mid a\,b$, então $p \mid a$ ou $p \mid b$. Reciprocamente, se $p \in \mathbb{Z}$ é tal que $p \neq 0$ e $p \neq \pm 1$ e $p \mid a\,b$, implica que $p \mid a$ ou $p \mid b$, então p é um número primo.

Prova: O caso $a = 0$ ou $b = 0$ é imediato, pois $p \mid 0$.

Suponhamos então que $a \neq 0$, $b \neq 0$ e que $p \nmid a$. Neste caso, como os únicos divisores positivos que p são 1 e $|p|$, e $|p| \nmid a$, temos que $\text{mdc}(a, p) = 1$. Agora segue de 6.33 que $p \mid b$.

Para a recíproca, suponhamos que p seja um inteiro composto. Então existem a e $b \in \mathbb{Z}$, ambos diferentes de ± 1, tais que $p = ab$. Assim, $|p| = |a|\,|b|$, com $1 < |a|$, $|b| < |p|$, o que implica que $|p| \nmid |a|$ e $|p| \nmid |b|$. Consequentemente, $p \nmid a$, $p \nmid b$ e $p \mid ab = p$, o que contradiz a hipótese. ■

O próximo resultado mostra que o menor divisor positivo, diferente de 1, de um número inteiro dado, é um número primo.

Proposição 6.41. Seja $a \in \mathbb{Z}$, com $a \neq 0$ e $a \neq 1$. Então o mínimo do conjunto $S = \{x \in \mathbb{Z};\ x > 1 \text{ e } x \mid a\}$ é um número primo.

Prova: Observe que $S \neq \emptyset$, pois $|a| \in S$. Então pelo princípio do menor número

natural, temos que existe $p = \min(S)$. Se p é composto, como $p > 0$, temos que existem b e $c \in \mathbb{Z}$, positivos, com $b \neq 1$, $c \neq 1$, tais que $p = bc$. Assim, $0 < b < p$ é um inteiro tal que $b \mid p$, e como $p \mid a$, então $b \mid a$, o que implica que $b \in S$, o que contradiz a minimalidade de p. Logo $p = \min(S)$ é primo. ■

Para a demonstração do Teorema Fundamental da Aritmética, usaremos o Segundo Princípio de Indução que apresentaremos sem demonstração.

Proposição 6.42 (Segundo Princípio de Indução)**.** Sejam $a \in \mathbb{Z}$ e $P(n)$ uma afirmação associada a todo número inteiro $n \geq a$. Se:

(i) $P(a)$ é verdadeira.

(ii) Para todo inteiro $r > a$, se $P(k)$ é verdadeira para todo $k \in \mathbb{Z}$, com $a \leq k < r$, então $P(r)$ também é verdadeira.

Então $P(n)$ é verdadeira para todo $n \in \mathbb{Z}$, com $n \geq a$.

Teorema 6.43 (Teorema Fundamental da Aritmética)**.** Seja $a \in \mathbb{Z}$ com $a \neq 0$ e $a \neq \pm 1$. Então existem números primos positivos $p_1, p_2, \ldots, p_r \in \mathbb{Z}$, com $r \geq 1$, tais que

$$a = p_1 \cdot p_2 \cdots p_r, \qquad \text{ou} \qquad a = -p_1 \cdot p_2 \cdots p_r,$$

se $a > 0$ ou $a < 0$ respectivamente. Mais ainda, essa decomposição é única, a menos das ordens dos fatores.

Prova: Trocando a por $|a|$ se necessário, basta mostrarmos o resultado para $a \in \mathbb{Z}$, com $a > 1$.

Mostraremos a existência da decomposição usando o Segundo Princípio de Indução.

Se $a = 2$, o resultado segue trivialmente pois 2 é primo. Seja $a > 2$ e suponhamos que exista a decomposição para todo número inteiro b, tal que $2 \leq b < a$. Mostremos que o resultado vale para a. Da proposição 6.41, temos que existe um número primo positivo p_1 tal que $a = p_1 \cdot a_1$, para algum $a_1 \in \mathbb{Z}$. Se $a_1 = 1$ ou a_1 é primo, temos que o resultado segue. Caso contrário, como $2 \leq a_1 < a$, por hipótese de indução temos que existem números primos positivos $p_2, p_3, \ldots, p_r$ tais que $a_1 = p_2 \cdot p_3 \cdots p_r$, e, consequentemente $a = p_1 \cdot p_2 \cdots p_r$. Assim, de 6.42, temos a existência da decomposição, para todo número inteiro $a > 1$.

Para mostrarmos a unicidade da decomposição, suponhamos que existam números naturais $1 \leq r \leq s$ e números primos positivos $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots, q_s$ tais que

$$a = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

Então $p_1 \mid q_1 \cdot q_2 \cdots q_s$ e, da proposição 6.40, temos que $p_1 \mid q_j$, para algum $j = 1, \ldots, s$. Do fato que p_1 e q_j são números primos positivos, obtemos que $p_1 = q_j$. Como queremos demonstrar a unicidade a menos da ordem dos fatores, sem perda de generalidade, podemos assumir que $j = 1$, ou seja, que $q_j = q_1$. Cancelando p_1 em ambas as fatorações de a, obtemos

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Repetindo este procedimento r vezes obtemos $1 = q_{r+1} \cdots q_s$, e, como cada q_j é um número primo, isso só é possível se $r = s$, o que demonstra a unicidade. ■

Observação 6.44. Na decomposição $a = \pm p_1 \cdot p_2 \cdots p_r$, os números primos envolvidos não são necessariamente distintos. Usando somente números primos distintos podemos escrever

$$a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

para algum $1 \leq k \leq r$, com $\alpha_i \in \mathbb{N}$, para todo $i = 1, \ldots, k$ e números primos positivos $p_1 < p_2 < \cdots < p_k$, que é chamada a **decomposição canônica** de a.

6.8 Congruências e Aplicações

Você saberia responder as seguintes perguntas:

- O 264^o e o 118^o dias do ano ocorrem num mesmo dia da semana?
- Quais são os inteiros que deixam resto 3 quando divididos por 4?
- Qual é o resto da divisão de 7^{12} por 4?
- Qual é o critério de divisibilidade por 7?
- Em que dia da semana você nasceu?

A partir da noção de congruência, ou aritmética modular, vamos dar respostas a todas essas perguntas e mais algumas. Esta noção surgiu pela primeira vez no livro

Disquisitiones arithmeticae, escrito por *Carl Friedrich Gauss*, publicado em 1800. Até hoje é usada a mesma notação introduzida por Gauss.

O que vem a ser *congruência*? É uma linguagem na qual muitas abordagens acerca de divisibilidade de números inteiros podem ser simplificadas. Vejamos esta noção formalmente:

Definição 6.45. Seja $m \in \mathbb{Z}$, com $m > 0$ fixo. Para a e $b \in \mathbb{Z}$, dizemos que a **é côngruo a** b **módulo** m se $m \mid a - b$, ou equivalentemente, se $a - b$ for múltiplo de m. **Notação:** $a \equiv b \mod m$.

Exemplo 6.46. $5 \equiv 2 \mod 3$, pois $3 \mid (5 - 2)$.
$2 \equiv -1 \mod 3$, pois $3 \mid (2 - (-1))$.
$5 \equiv 17 \mod 3$, pois $3 \mid (5 - 17)$.

As propriedades abaixo da relação de congruência módulo m, nos mostram que esta é de fato uma relação de equivalência sobre $\mathbb{Z}$, para todo inteiro $m > 0$.

(i) *Reflexiva* - $a \equiv a \mod m$, para todo $a \in \mathbb{Z}$, pois $m \mid 0 = a - a$.

(ii) *Simétrica* - Se $a \equiv b \mod m$, então $b \equiv a \mod m$, pois para todo a, b e $m \in \mathbb{Z}$, temos $m \mid a - b$ se, e somente se $m \mid b - a$.

(iii) *Transitiva* - Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$. De fato, de $a \equiv b \mod m$ e $b \equiv c \mod m$, temos que $m \mid a - b$ e $m \mid b - c$. Logo $m \mid (a - b) + (b - c) = a - c$, ou seja, $a \equiv c \mod m$.

O próximo resultado relaciona congruência módulo m com o algoritmo da divisão.

Proposição 6.47. Sejam a e $b \in \mathbb{Z}$. Então $a \equiv b \mod m$ se, e somente se a e b fornecem os mesmos restos na divisão euclideana por m.

Prova: ($\Longrightarrow$) Desde que $a \equiv b \mod m$, temos que $a \mid a - b$, ou seja, existe $k \in \mathbb{Z}$ tal que $a - b = k\,m$ e, portanto, $a = k\,m + b$. Na divisão euclideana de a e b por m, temos que $b = q\,m + r$ e $a = p\,m + s$, para algum q, p, r e $s \in \mathbb{Z}$, com $0 \leq r, s < m$. Assim, $a = (k + q)\,m + r = p\,m + s$ e, pela unicidade do quociente e do resto temos que $k + q = p$ e $s = r$. Portanto os restos são iguais.

($\Longleftarrow$) Suponhamos que os restos sejam iguais, isto é, $a = p\,m + r$ e $b = q\,m + r$. Então $a - b = (p - q)\,m$, ou seja $m \mid a - b$ e, consequentemente, $a \equiv b \mod m$. ■

Já estamos em condições de responder as duas primeiras perguntas.

- O 264^o e o 118^o dias do ano ocorrem num mesmo dia da semana?

  Desde que a semana tem 7 dias, temos que eles ocorrem no mesmo dia da semana se, e somente se $264 \equiv 118 \mod 7$. De 6.47, isso ocorre se, e somente se eles tem o mesmo resto na divisão euclideana por 7. Como $264 = 37 \cdot 7 + 5$ e $118 = 16 \cdot 7 + 6$, temos que eles não correm no mesmo dia da semana e, sim em dias seguidos.

- Quais são os inteiros que deixam resto 3 quando divididos por 4?

  São os números inteiros a tais que $a \equiv 3 \mod 4$, ou seja, $4 \mid a-3$. Então existe $k \in \mathbb{Z}$, tal que $a - 3 = 4\,k$, isto é, $a = 4\,k + 3$, com $k \in \mathbb{Z}$.

Dado um número inteiro $m > 0$, desde que $\equiv$ é uma relação de equivalência sobre $\mathbb{Z}$, podemos considerar o conjunto quociente de $\mathbb{Z}$ por esta relação, que denotaremos por $\mathbb{Z}_m$, ou seja, $\mathbb{Z}_m = \{\overline{a};\ a \in \mathbb{Z}\}$, onde $\overline{a}$ é a classe de equivalência representada por a. De 6.47 temos que se $a = q\,m + r$, com $0 \leq r < m$, então $a \equiv r \mod m$ e, consequentemente, $\overline{a} = \overline{r}$. Assim,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\},$$

onde

$$\begin{aligned}
\overline{0} &= \{a \in \mathbb{Z};\ a \equiv 0 \mod m\} = \{a \in \mathbb{Z};\ m \mid a\} = \{m\,k;\ k \in \mathbb{Z}\} = m\,\mathbb{Z} \\
\overline{1} &= \{a \in \mathbb{Z};\ a \equiv 1 \mod m\} = \{a \in \mathbb{Z};\ m \mid a-1\} = \{m\,k+1;\ k \in \mathbb{Z}\} = m\,\mathbb{Z} + 1 \\
\overline{2} &= \{a \in \mathbb{Z};\ a \equiv 2 \mod m\} = \{a \in \mathbb{Z} : m \mid a-2\} == m\,\mathbb{Z} + 2 \\
&\vdots \\
\overline{m-1} &= \{a \in \mathbb{Z};\ a \equiv m-1 \mod m\} = \{a \in \mathbb{Z};\ m \mid a-(m-1)\} = m\,\mathbb{Z} + (m-1)
\end{aligned}$$

No próximo resultado apresentamos mais algumas propriedades da relação de congruência.

Proposição 6.48. Sejam $m > 0$ um inteiro fixo e $a,\ b,\ c$ e $d \in \mathbb{Z}$. Então valem as seguintes propriedades:

(a) Se $a \equiv b \mod m$, então $a \pm c \equiv b \pm c \mod m$ e $ac \equiv bc \mod m$.

(b) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a \pm c \equiv b \pm d \mod m$ e $ac \equiv bd \mod m$.

(c) Se $a \equiv b \mod m$ e $r \geq 1$ um inteiro, então $ra \equiv rb \mod m$ e $a^r \equiv b^r \mod m$.

Prova: (a) Se $a \equiv b \mod m$, então $m \mid a - b$. Mas $a - b = (a \pm c) - (b \pm c)$, o que implica que $a \pm c \equiv b \pm c \mod m$. Como $m \mid a - b$, temos que existe $k \in \mathbb{Z}$ tal que $a - b = m\,k$, o que implica que $ac - bc = (a - b)c = m\,kc = m\,(kc)$, ou sejam $m \mid ac - bc$ e, consequentemente $ac \equiv bc \mod m$.

(b) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então do ítem (a) temos que $a \pm c \equiv b \pm c \mod m$ e $b \pm c \equiv b \pm d \mod m$. Da transitividade obtemos $a \pm c \equiv b \pm d \mod m$.

De maneira análoga, usando o ítem (a) e a transitividade da relação, obtemos $ac \equiv bd \mod m$.

(c) Se $a \equiv b \mod m$ e $r \geq 1$ um inteiro, então aplicando o resultado do ítem (b) para $a = c$ e $b = d$, r vezes, obtemos $ra \equiv rb \mod m$ e $a^r \equiv b^r \mod m$. ■

Estamos aptos a responder mais uma das perguntas do início da seção.

- Qual é o resto da divisão de 7^{12} por 4?

  Podemos calcular diretamente $7^{12} = 13.841.287.201$, depois dividir por 4 e verificar que o resto é 1.

  Usando a congruências, podemos resolver de uma maneira mais simples. Desde que $7 \equiv 3 \mod 4$ e $3 \equiv -1 \mod 4$, por transitividade temos $7 \equiv -1 \mod 4$ e de 6.48 (c), obtemos $7^{12} \equiv (-1)^{12} \mod 4$, ou seja $7^{12} \equiv 1 \mod 4$. De 6.47, temos que o resto da divisão de 7^{12} por 4 é 1.

No restante do capítulo, apresentaremos algumas aplicações da relação de congruência e, responderemos as perguntas que faltam.

6.8.1 Critérios de Divisibilidade

Nesta seção deduziremos e/ou demonstraremos a validade dos critérios de divisibilidade conhecidos desde o ensino básico.

Dado um número inteiro positivo n, podemos escrevê-lo na forma

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r,$$

onde $r \geq 0$ e $0 \leq a_i \leq 9$, para cada $i = 0, 1, \ldots, r$, são os seus algarismos.

No que segue, usaremos esta notação e, os resultados contidos em 6.47 e 6.48, sem mencioná-los.

(a) Divisibilidade por 2 **-** O número n é divisível por 2 se, e somente se a_0 é divisível por 2.

De fato, n é divisível por 2 se, e somente se $n \equiv 0 \mod 2$.

Como $10 \equiv 0 \mod 2$, temos que $10^i \equiv 0 \mod 2$, para todo $i = 1, \ldots, r$. Assim, obtemos

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdot 0 + \cdots + a_r \cdot 0 \mod 2,$$

o que mostra que $2 \mid n$ se, e somente se $2 \mid a_0$.

(b) Divisibilidade por 3 **-** O número n é divisível por 3 se, e somente se $a_0 + a_1 + \cdots + a_r$ é divisível por 3.

De fato, n é divisível por 3 se, e somente se $n \equiv 0 \mod 3$.

Como $10 \equiv 1 \mod 3$, temos que $10^i \equiv 1 \mod 3$, para todo $i = 1, \ldots, r$. Assim,

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdot 1 + \cdots + a_r \cdot 1 \mod 3,$$

o que mostra que $3 \mid n$ se, e somente se $3 \mid (a_0 + a_1 + \cdots + a_r)$.

(c) Divisibilidade por 4 **-** O número n é divisível por 4 se, e somente se o número formado por seus dois últimos algarismos é divisível por 4, isto é, $a_0 + a_1 \cdot 10$ é divisível por 4.

De fato, n é divisível por 4 se, e somente se $n \equiv 0 \mod 4$.

Como $100 \equiv 0 \mod 4$, temos que $10^i \equiv 1 \mod 4$, para todo $i = 2, \ldots, r$. Assim,

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdot 10 \mod 4,$$

o que mostra que $4 \mid n$ se, e somente se $4 \mid (a_0 + a_1 \cdot 10)$.

(d) Divisibilidade por 5 **-** O número n é divisível por 5 se, e somente se é terminado em 0 ou 5, isto é a_0 é divisível por 5.

De fato, n é divisível por 5 se, e somente se $n \equiv 0 \mod 5$.

Como $10 \equiv 0 \mod 5$, temos que $10^i \equiv 0 \mod 5$, para todo $i = 1, \ldots, r$. Assim,

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 \mod 5,$$

o que mostra que $5 \mid n$ se, e somente se $5 \mid a_0$.

(e) Divisibilidade por 9 **-** O número n é divisível por 9 se, e somente se $a_0+a_1+\cdots+a_r$ é divisível por 9.

De fato, n é divisível por 9 se, e somente se $n \equiv 0 \mod 9$. Como $10 \equiv 1 \mod 9$, temos que $10^i \equiv 1 \mod 9$, para todo $i = 1, \ldots, r$. Assim,

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdot 1 + \cdots + a_r \cdot 1 \mod 9,$$

o que mostra que $9 \mid n$ se, e somente se $9 \mid (a_0 + a_1 + \cdots + a_r)$.

(f) Divisibilidade por 11 **-** O número n é divisível por 11 se, e somente se $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^r a_r$ é divisível por 11.

Como n é divisível por 11 se, e somente se $n \equiv 0 \mod 11$, e $10 \equiv -1 \mod 11$, temos que $10^i \equiv (-1)^i \mod 11$, para todo $i = 1, \ldots, r$. Assim,

$$n = a_0 + a_1 \cdot 10 + \cdots + a_r \cdot 10^r \equiv a_0 + a_1 \cdot (-1) + \cdots + a_r \cdot (-1)^r \mod 11,$$

o que mostra o critério.

(g) Divisibilidade por 7 **-** Quais as condições sobre os algarismos de n para que n seja divisível por 7?

Vejamos, n é divisível por 7 se, e somente se $n \equiv 0 \mod 7$. Como

$10^0 \equiv 1 \mod 7$
$10^1 \equiv 3 \mod 7$
$10^2 \equiv 3^2 \mod 7 \Rightarrow 10^2 \equiv 2 \mod 7$
$10^3 \equiv 2 \cdot 3 \mod 7 \Rightarrow 10^3 \equiv -1 \mod 7$
$10^4 \equiv 2^2 \mod 7 \Rightarrow 10^3 \equiv -3 \mod 7$
$10^5 \equiv (-1) \cdot 2 \mod 7 \Rightarrow 10^5 \equiv -2 \mod 7$
$10^6 \equiv (-1)^2 \mod 7 \Rightarrow 10^3 \equiv 1 \mod 7$

temos que

$$n \equiv (a_0 + a_1 \cdot 3 + a_2 \cdot 2) - (a_3 + a_4 \cdot 3 + a_5 \cdot 2) + (a_6 + a_7 \cdot 3 + a_8 \cdot 2) + \cdots \mod 7,$$

o que mostra que

$$7 \mid n \iff 7 \mid (a_0 + a_1 \cdot 3 + a_2 \cdot 2) - (a_3 + a_4 \cdot 3 + a_5 \cdot 2) + (a_6 + a_7 \cdot 3 + a_8 \cdot 2) + \cdots .$$

6.8.2 A validade de um número de CPF

O CPF (**Cadastro de Pessoa Física**), emitido pela Receita Federal, é caracterizado por uma função bijetora entre o conjunto das pessoas físicas cadastradas e o conjunto dos números emitidos.

O número de um CPF tem exatamente 9 algarismos em sua raiz e mais dois algarismos **dígitos verificadores**, que são indicados por último, ou seja, um CPF tem 11 algarismos e é escrito na forma $abcdefghi - jk$, ou diretamente como $abcdefghijk$, onde os algarismos não podem ser todos iguais entre si. O algarismo j é chamado o **primeiro digito verificador do número do CPF** e k é chamado o **segundo digito verificador do número do CPF.**

- **Regra para determinar o primeiro dígito verificador**

  Começamos calculando

  $$S_1 = 10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i.$$

  Encontramos r, onde $S_1 \equiv r \mod 11$.

  Se $r = 0$ ou $r = 1$, o dígito j é 0 (zero).

  Se $r \neq 0$ e $r \neq 1$, o dígito j é $11 - r$.

- **Regra para determinar o segundo dígito verificador**

  Para obtermos k, começamos calculando

  $$S_2 = 11a + 10b + 9c + 8d + 7e + 6f + 5g + 4h + 3i + 2j.$$

  Encontramos r, onde $S_2 \equiv r \mod 11$.

  Se $r = 0$ ou $r = 1$, o dígito k é 0 (zero).

  Se $r \neq 0$ e $r \neq 1$, o dígito j é $11 - r$.

Exercício 6.49. Verifique se o número de seu CPF é válido.

6.8.3 Em que dia da semana você nasceu?

Para responder essa pergunta, começamos associando um número a cada dia da semana da seguinte forma

Número	Dia da semana
0	sábado
1	domingo
2	segunda-feira
3	terça-feira
4	quarta-feira
5	quinta-feira
6	sexta-feira

A cada mês associamos uma constante M, chamada a **constante do mês**, entre 0 e 6 correspondente ao dia da semana do último dia do mês anterior. Por exemplo, no mês de setembro de 2010, o dia primeiro foi quarta-feira, o dia anterior foi terça-feira e, portanto $M = 3$.

Para tal constante temos a seguinte propriedade de demonstração imediata:

Lema 6.50. $(M +$ dia $) \equiv (\,$ dia da semana $)\mod 7$.

Por exemplo, para o dia 14 de setembro de 2010, temos $3 + 14 = 17 \equiv 3 \mod 7$. Portanto, dia 14 de setembro de 2010 foi uma terça-feira.

Com a fórmula de 6.50, o problema de descobrir o dia da semana de alguma data se reduz a descobrir a constante M do mês correspondente.

- Como calcular a constante do mês seguinte?

Note que, por definição, a constante do mês seguinte (outubro/2010) é o dia da semana do último dia de setembro/2010. Como setembro tem 30 dias e $3+30 = 33 \equiv 5 \mod 7$, temos 6.50 que dia 30/09/2010 foi em uma quinta-feira. Portanto a constante do mês de outubro de 2010 é $M = 5$.

- Como calcular as constantes dos meses futuros a setembro/2010?

Note que $30 \equiv 2 \mod 7$ e $31 \equiv 3 \mod 7$. Com isso obtemos:

N: Número de dias no mês	30	31	30	31
$N \equiv 3$ ou $2 \mod 7$	2	3	2	3
Mês	S	O	N	D
M	5	0	3	5

Observe que para obtermos a constante do mês seguinte, somamos a constante ao número acima e tomamos a congruência módulo 7.

- Como calcular as constantes dos meses anteriores a setembro/2010?

Como o mês de fevereiro é anterior a setembro, é preciso saber se o ano em questão é ou não um ano bissexto.

São considerados **anos bissextos** aqueles que são múltiplos de 4 e que não sejam múltiplos de 100, com exceção dos múltiplos de 400.

Em termos de congruências, se A é o ano em questão, então A é bissexto se, e somente se $A \equiv 0 \mod 4$ e $A \not\equiv 0 \mod 100$, ou $A \equiv 0 \mod 400$. Como $2010 \equiv 2 \mod 4$, temos que 2010 não é bissexto.

Note que $28 \equiv 0 \mod 7$ e $29 \equiv 1 \mod 7$. Usando este fato e o fato que 2010 não é bissexto, obtemos

N	31	28/**29**	31	30	31	30	31	31	30
$3, 2$ ou $0/1$	3	0/**1**	3	2	3	2	3	3	2
Mês	J	F	M	A	M	J	J	A	S
M	0	3	3	6	1	4	6	2	5

Observe que para obter as constantes dos meses anteriores, subtrai-se à constante o número acima do mês anterior e toma-se a congruência módulo 7. para obter a constante do mês anterior.

Em uma só tabela as constantes referentes ao ano de 2010.

$3, 2$ ou $0/1$	3	0/**1**	3	2	3	2	3	3	2	3	2	3
Mês	J	F	M	A	M	J	J	A	S	O	N	D
M 0	3	3	6	1	4	6	2	5	0	3	5	

Juntando as constantes para 2009 e 2011, obtemos:

3, 2 ou 0/1	3	0/**1**	3	2	3	2	3	3	2	3	2	3
Mês	J	F	M	A	M	J	J	A	S	O	N	D
2009	4	0	0	3	5	1	3	6	2	4	0	2
2010	0	3	3	6	1	4	6	2	5	0	3	5
2011	1	1	4	6	2	4	0	3	6	1	4	6

- Como saber o dia da semana em uma data qualquer, passada ou futura?

Como $365 \equiv 1 \mod 7$ e $366 \equiv 2 \mod 7$, temos que irmos para um ano A futuro (resp. passado) precisamos somar (resp. subtrair) o número de anos da diferença $(2010 - A)$ adicionado do número de 29's de fevereiro entre estas datas.

Exemplo 6.51. Eu (Ires) nasci no dia 19 de junho de 1959. Em que dia da semana eu nasci?

Queremos saber a constante M do mês de junho de 1959. Portanto $A = 1959$. Assim $(2010 - A)+$ (o número de 29 de fevereiro entre as datas) é $51 + 13 = 64$ e $64 \equiv 1 \mod 7$.

Como a constante do mês junho de 2010 é $M = 4$, temos que a constante do mês junho de 1959 é $4 - 1 \equiv 3 \mod 7$, ou seja $M = 3$.

Assim, de 6.50, obtemos $M + 19 = 3 + 19 = 22 \equiv 1 \mod 7$, ou seja, eu nasci em uma **segunda-feira**.

Exercício 6.52. Em que dia da semana você nasceu?

6.9 Exercícios

1. (a) Prove que a soma de dois números inteiros pares é par e que a soma de dois números inteiros ímpares também é par.

   (b) O produto de dois números inteiros é ímpar se, e somente se, ambos são ímpares.

2. Se a e b são números inteiros, com $a \neq 0$ e $b \neq 0$, mostre que

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}\, b + ... + a\, b^{n-2} + b^{n-1}), \quad \forall n \geq 1.$$

3. Sejam x e y números inteiros tais que $xy = 1$. Mostre que $x = y = 1$ ou $x = y = -1$.

4. Para $a,\ b$ e $c \in \mathbb{Z}$, mostre que $a < b + c$ se, e somente se $a - b < c$.

5. Para $a,\ b$ e $c \in \mathbb{Z}$, com $a < b$ e $c < d$, mostre que:

   (a) $a - d < b - c$.

   (b) $bc + ad < ac + bd$.

6. Mostre que, para todo $n \in \mathbb{Z}$, o conjunto $\{x \in \mathbb{Z};\ n < x < n + 1\}$ é vazio.

7. Considerando a relação $\leq$ definida em $\mathbb{Z}$, mostre que ela é transitiva e a compatibilidade com a adição.

8. Sejam $a,\ b \in \mathbb{Z}$ e $d = \text{mdc}(a, b)$. Mostre que:

   (a) $\text{mdc}(sa, sb) = sd$.

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

9. Se $n > 0$ não é múltiplo de 3, mostre que $a = 3^{2n} + 3^n + 1$ é divisível por 13.

10. Encontre o quociente e o resto na divisão euclidiana de a por b nos seguintes casos:

    $a = 390,\ b = 74$ $\qquad$ $a = -124,\ b = 18$ $\qquad$ $a = -420,\ b = 58$.

11. Na divisão euclidiana de 326 pelo inteiro $b > 0$, o quociente é 14 e o resto é r. Ache os possíveis valores de b e r.

12. Seja m um inteiro ímpar. Mostre que o resto da divisão de m por 4 é 1 ou 3.

13. Seja a um inteiro. Mostre que:

    (a) Um dos inteiros a, $a + 1$ ou $a + 2$ é divisível por 3.

    (b) Um dos inteiros a, $a + 2$ ou $a + 4$ é divisível por 3.

    (c) Um dos inteiros a, $a + 1$, $a + 2$ ou $a + 3$ é divisível por 4.

14. Seja m um inteiro.

    (a) Mostre que o resto da divisão de m^2 por 3 é 0 ou 1.

    (b) Se m é um inteiro ímpar, mostre que o resto da divisão de m^2 por 4 é 1.

15. (a) Se n é um inteiro par, mostre que $\text{mdc}(n, n + 2) = 2$.

    (b) Se n é ímpar, mostre que $\text{mdc}(n, n + 2) = 1$.

16. Sejam a e $b, \in \mathbb{Z}$. Mostre que $\text{mdc}(a, b) = 1$ se, e somente se $\text{mdc}(a + b, b) = 1$.

17. Encontre os restos nas seguintes divisões:

    (a) 2^{45} por 7.

    (b) 11^{10} por 100.

    (c) $5^2 \cdot 4841 + 28^5$ por 3.

18. Qual é o resto na divisão euclidiana de $s = 1^5 + 2^5 + 3^5 + ... + 99^5 + 100^5$ por 4? Justifique.

19. (a) Se a é um cubo perfeito ($a = t^3$, para algum $t \in \mathbb{Z}$), então mostre que $a \equiv 0, 1$ ou $-1 \mod 9$.

    (b) Se a é um quadrado perfeito ($a = t^2$, para algum $t \in \mathbb{Z}$) e também um cubo perfeito ($a = s^3$, para algum $s \in \mathbb{Z}$), mostre que $a \equiv 0$, 1, 9 ou 28 $\mod 36$.

20. (a) Mostre que todo número inteiro primo é da forma $4k + 1$ ou $4k + 3$, com $k \in \mathbb{Z}$.

    (b) Mostre que todo número primo (é da forma $6k + 1$ ou $6k + 5$, com $k \in \mathbb{Z}$.

21. Sejam a e b números inteiros e p um número primo. Verificar se as afirmações abaixo são verdadeiras ou falsas.

    (a) Se p divide $a^2 + b^2$ e p divide a, então p divide b.

    (b) Se p divide ab, então p divide a e p divide b.

    (c) Se p divide $a + b$, então p divide a e p divide b.

    (d) Se a divide p, então a é primo.

    (e) Se a divide b e p divide b, então p divide a.

7
Números Racionais

No conjunto dos números inteiros, temos que a equação $a \cdot X = b$, com a e $b \in \mathbb{Z}$, tem solução se, e somente se $a \mid b$. Podemos sempre assumir que $a \neq 0$, pois caso contrário, b também seria igual a zero e a equação seria $0 = 0$. Mais ainda, usando a lei do cancelamento para o produto, temos que quando esta equação tem solução, ela é única. Queremos ampliar o conjunto dos números inteiros, construindo um conjunto onde esta equação sempre tenha solução única, mesmo quando $a \nmid b$. Note que a solução será $X = \dfrac{b}{a}$, com $a \neq 0$ e $b \in \mathbb{Z}$. Assim, queremos construir um conjunto, "contendo" $\mathbb{Z}$, onde faça sentido este "quociente" e que contenha todos os quocientes deste tipo.

Observe, por exemplo, que expressões do tipo $\dfrac{4}{2}$, $\dfrac{6}{3}$, $\dfrac{10}{5}$, $\dfrac{90}{45}$, representam, todas, o número inteiro 2. Mas, seria muito bom se tivéssemos uma certa unicidade de representação.

Note que a igualdade $\dfrac{4}{2} = \dfrac{10}{5}$ em $\mathbb{Z}$ é equivalente a $4 \cdot 5 = 2 \cdot 10$. Isso nos ajuda a entender a construção que faremos a seguir.

Seja $\mathbb{Z}^* = \{n \in \mathbb{Z};\ n \neq 0\}$. Em $\mathbb{Z} \times \mathbb{Z}^*$ definimos a relação $\sim$ por:

$$(m, n) \sim (p, q) \Longleftrightarrow m\,q = n\,p,$$

para todo (m, n) e $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$.

A relação $\sim$ acima é uma relação de equivalência sobre $\mathbb{Z} \times \mathbb{Z}^*$. (Verifique este fato como exercício)

Portanto, determina em $\mathbb{Z} \times \mathbb{Z}^*$ uma partição em classes de equivalência. Para cada par $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$, a classe de equivalência representada por esse elemento, será

indicada por $\overline{(m,n)} = \dfrac{m}{n}$, ou seja

$$\frac{m}{n} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^*;\ (x,y) \sim (m,n)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^*;\ x\,n = y\,m\}.$$

Por exemplo:

$$\begin{aligned}\frac{5}{6} &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^*;\ (x,y) \sim (5,6)\} \\ &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^*;\ 6x = 5y\} \\ &= \{(5,6), (-5,-6), (10,12), (-10,-12), \cdots\}.\end{aligned}$$

Observe que $\dfrac{m}{n} = \dfrac{r}{s}$ se, e somente se $(m,n) \sim (r,s)$ isto é,

$$\frac{m}{n} = \frac{r}{s} \Longleftrightarrow ms = nr.$$

O conjunto quociente $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$, de todas as classes de equivalência determinadas pela relação $\sim$ sobre $\mathbb{Z} \times \mathbb{Z}^*$, será denotado por $\mathbb{Q}$, ou seja,

$$\mathbb{Q} = \left\{\frac{m}{n};\ (m,n) \in \mathbb{Z} \times \mathbb{Z}^*\right\}.$$

Observe que cada $x \in \mathbb{Q}$ admite infinitas representações $\dfrac{m}{n}$, com $m \in \mathbb{Z}$ e $n \in \mathbb{Z}^*$. Em cada uma das representações, o número m é o **numerador** e n o **denominador**. Mais ainda, dois elementos x e y no conjunto $\mathbb{Q}$ sempre admitem representações com denominadores iguais, pois se $x = \dfrac{m}{n}$ e $y = \dfrac{r}{s}$, então temos que $\dfrac{m}{n} = \dfrac{ms}{ns}$ e $\dfrac{r}{s} = \dfrac{rn}{sn}$, pois $(m,n) \sim (ms,ns)$ e $(r,s) \sim (rn,sn)$.

Os elementos de $\mathbb{Q}$ são ditos serem **números racionais** uma vez que definamos uma operação de adição, uma de multiplicação e uma relação de ordem, satisfazendo certas propriedades, como faremos a seguir.

7.1 A adição em $\mathbb{Q}$

Definição 7.1. Sejam $x = \dfrac{m}{n}$ e $y = \dfrac{r}{s}$ elementos de $\mathbb{Q}$. Definimos a **adição** de x com y, e indicamos por $x + y$, como sendo o elemento de $\mathbb{Q}$

$$x + y = \frac{m}{n} + \frac{r}{s} = \frac{ms}{ns} + \frac{nr}{ns} = \frac{ms + nr}{ns}.$$

Como nesta definição envolve a escolha de representantes das classes de equivalência, devemos mostrar que esta definição não depende da escolha de tais representantes, ou seja que a adição está bem definida em $\mathbb{Q}$.

Para tanto, se $x = \frac{m}{n} = \frac{m'}{n'}$ e $y = \frac{r}{s} = \frac{r'}{s'}$, então temos que

$$mn' = nm', \qquad (*)$$

e

$$rs' = sr', \qquad (**)$$

Multiplicando (*) por ss' e (**) por nn' e somando membro a membro, obtemos

$$msn's' + rnm'r' = nsm's' + nsr'n'$$

ou seja, $(ms + rn)\, n's' = ns\,(m's' + r'n')$ e, portanto, $\frac{ms + rn}{ns} = \frac{m's' + r'n'}{n's'}$, o que mostra que a adição está bem definida.

No próximo resultado apresentamos as principais propriedades desta operação.

Teorema 7.2. Para x, y e $z \in \mathbb{Q}$, valem as seguintes propriedades:

(a) *Associativa* - $(x + y) + z = x + (y + z)$.

(b) *Comutativa* - $x + y = y + x$.

(c) *Elemento Neutro* - Existe $0 = \frac{0}{1} = \frac{0}{2} = \cdots$ em $\mathbb{Q}$, tal que $0 + x = x$, para todo $x \in \mathbb{Q}$.

(d) *Elemento Oposto* - Para cada $x \in \mathbb{Q}$, existe $y \in \mathbb{Q}$ tal que $x + y = 0$.

(e) *Lei do Cancelamento* - Se $x + y = x + z$, então $y = z$.

Prova: Exercício. ■

Observação 7.3. Usando a Lei do Cancelamento, pode-se mostrar que o elemento neutro é único e, que para cada $x \in \mathbb{Q}$, o elemento y satisfazendo a propriedade (d) também é único, o qual será denotado por $-x$ e dito ser o **oposto** ou **simétrico aditivo** de x.

Para x e $y \in \mathbb{Q}$, diremos ser a **diferença** entre x e y e indicaremos por $x - y$, ao número racional $x - y = x + (-y)$.

Tal como em $\mathbb{Z}$, com demonstrações análogas, temos algumas propriedades envolvendo adição e opostos.

Proposição 7.4. Sejam x, y e $z \in \mathbb{Q}$. Valem as seguintes propriedades:

(a) $-(x+y) = -x - y$.

(b) $(x-y)+y = x$.

(c) $x + a = y \Longleftrightarrow a = y - x$.

Prova: Exercício. ■

7.2 A Multiplicação em $\mathbb{Q}$

Definição 7.5. Sejam $x = \frac{m}{n}$ e $y = \frac{r}{s}$ elementos de $\mathbb{Q}$. O elemento de $\mathbb{Q}$ dado por $x\,y = x.y = \frac{mr}{ns}$ é dito ser o **produto** de x por y.

Mostre que essa definição não depende das particulares representações escolhidas para x e y, ou seja, que a operação de multiplicação em $\mathbb{Q}$ está bem definida.

Para tal operação temos as seguintes propriedades elementares:

Teorema 7.6. Sejam x, y e $z \in \mathbb{Q}$. Valem as seguintes propriedades:

(a) *Associativa* - $x\,(yz) = (xy)\,z$.

(b) *Comutativa* - $xy = yx$.

(c) *Elemento Neutro* - Existe $1 = \frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \cdots$ em $\mathbb{Q}$, tal que $1 \cdot x = x$, para todo $x \in \mathbb{Q}$.

(d) *Elemento Inverso* - Para cada $x \in \mathbb{Q}$, com $x \neq 0$, existe $y \in \mathbb{Q}$ tal que $xy = 1$.

(e) *Distributividade* - $x(y+z) = xy + xz$.

(f) *Lei do Cancelamento* - Se $xy = xz$ e $x \neq 0$, então $y = z$.

Prova: Vamos mostrar os ítens (c), (d) e (f), ficando a demonstração dos outros como exercício.
(c) Para $x = \frac{m}{n} \in \mathbb{Q}$, temos que $x \cdot 1 = \frac{m}{n} \cdot \frac{1}{1} = \frac{m \cdot 1}{n \cdot 1} = \frac{m}{n} = x$.
(d) Se $x = \frac{m}{n} \neq 0$ em $\mathbb{Q}$, então $m \neq 0$, e, consequentemente, $y = \frac{n}{m} \in \mathbb{Q}$. Mais ainda, $x \cdot y = \frac{m}{n} \cdot \frac{n}{m} = \frac{mn}{mn} = \frac{1}{1} = 1$, como queríamos mostrar.

(f) Se $xy = xz$ e $x \neq 0$, então de (b) temos que $yx = zx$. Mais ainda, como $x \neq 0$, então do ítem anterior, existe $x' \in \mathbb{Q}$ tal que $xx' = 1$. Assim, multiplicando a equação $yx = zx$ por x' e usando a associatividade, obtemos $y(xx') = z(xx')$, ou seja $y \cdot 1 = z \cdot 1$, o que implica que $y = z$. ■

Observação 7.7. Como na adição, usando a Lei do Cancelamento para a multiplicação, pode-se mostrar que o elemento neutro é único e, o elemento y satisfazendo a propriedade do ítem (d), também é único. Tal elemento será dito ser o **inverso** ou **simétrico multiplicativo** de x e denotado por x^{-1}.

Com relação à inversos temos:

Exercício 7.8. Para x e $y \in \mathbb{Q}$, mostre que:

(a) Se $x \neq 0$, então $(x^{-1})^{-1} = x$.

(b) $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$.

Mais ainda, ainda usando a noção de inverso, podemos definir a operação de divisão sobre $\mathbb{Q}$ como segue:

Definição 7.9. Sejam $x \in \mathbb{Q}$ e $y \in \mathbb{Q}^* = \{ x \in \mathbb{Q}, x \neq 0 \}$. A operação de $\mathbb{Q} \times \mathbb{Q}^*$ em $\mathbb{Q}$ que a cada par (x, y) associa o número racional $x \cdot y^{-1}$ é chamada de ***divisão*** em $\mathbb{Q}$. O elemento $x \cdot y^{-1}$ é dito ser o ***quociente*** de x por y e também poderá ser indicado por $x : y$.

Exercício 7.10. Mostre que $(x + y) : z = x : z + y : z$, para todo $x, y \in \mathbb{Q}$ e $z \in \mathbb{Q}^*$.

7.3 Relação de Ordem em $\mathbb{Q}$

Observe que dado $x \in \mathbb{Q}$ sempre poderemos considerar uma representação para x em que o denominador seja um número inteiro maior que zero. Isso segue do simples fato que $x = \frac{m}{n} = \frac{-m}{-n}$.

Definição 7.11. Sejam x e y números racionais com representações em que os respectivos numeradores sejam estritamente positivos,isto é, $x = \frac{m}{n}$ e $y = \frac{r}{s}$, com $n > 0$ e $s > 0$ em $\mathbb{Z}$. Dizemos que x é **menor ou igual** a y e escrevemos $x \leq y$ se $ms \leq nr$ em $\mathbb{Z}$. Neste caso, dizemos também que y é **maior ou igual** a x e escrevemos $y \geq x$.

Se $ms < nr$ em $\mathbb{Z}$, dizemos que x é **menor que** y $(x < y)$ ou que y é **maior que** x $(y > x)$.

Exemplo 7.12. Note que $\frac{-8}{7} < \frac{3}{4}$, pois $(-8) \cdot 4 < 3 \cdot 7$ e $\frac{5}{6} > \frac{4}{5}$, pois $5 \cdot 5 > 6 \cdot 4$.

Dizemos que um elemento $x = \frac{m}{n} \in \mathbb{Q}$, com $n > 0$ é **positivo** se $x \geq 0$, e, isto ocorre se, e somente se $m \geq 0$. Quando $x > 0$, ou seja, $m > 0$, dizemos que x é **estritamente positivo**. Se $x \leq 0$, isto é, $n > 0$ e $m \leq 0$, dizemos que x é **negativo**. Quando $m < 0$, dizemos que x é **estritamente negativo**.

A relação definida acima, é análoga a relação de ordem definida sobre $\mathbb{Z}$, ou seja, vale o seguinte resultado:

Proposição 7.13. Sejam x e y em $\mathbb{Q}$ tais que $x \leq y$. Então existe $z \in \mathbb{Q}$, positivo, tal que $y = x + z$.

Prova: Dados x e y em $\mathbb{Q}$, podemos escrever $x = \frac{m}{n}$ e $y = \frac{r}{n}$, com $n > 0$.

Se $x \geq y$ em $\mathbb{Q}$, então $mn \geq rn$ em $\mathbb{Z}$ e, como $n > 0$, obtemos $m \geq r$. Pela definição da relação de ordem sobre $\mathbb{Z}$, temos que existe $u \in \mathbb{Z}_+$ tal que $r = m + u$. Assim,

$$y = \frac{r}{n} = \frac{m+u}{n} = \frac{m}{n} + \frac{u}{n} = x + z,$$

onde $z = \frac{u}{n} \in \mathbb{Q}$ é positivo, pois $u \geq 0$ e $n > 0$, o que mostra o resultado. ■

No próximo resultado mostraremos que $\leq$, como definida acima, é uma relação de ordem total sobre $\mathbb{Q}$.

Teorema 7.14. A relação $\leq$ é uma relação de ordem total sobre $\mathbb{Q}$.

Prova: Assumiremos que todos os denominadores dos elementos considerados em $\mathbb{Q}$, sejam estritamente positivos.

Sejam $x = \frac{m}{n}$, $y = \frac{r}{s}$ e $z = \frac{p}{q}$ elementos de $\mathbb{Q}$.

(i) $\leq$ é reflexiva.

De fato, para todo $x \in \mathbb{Q}$, temos que

$$x \leq x \Longleftrightarrow \frac{m}{n} \leq \frac{m}{n} \Longleftrightarrow mn = nm,$$

pois o produto de números inteiros é comutativo.

(ii) $\leq$ é anti-simétrica.

Sejam x e y elementos de $\mathbb{Q}$ tais que $x \leq y$ e $y \leq x$, ou seja, $\frac{m}{n} \leq \frac{r}{s}$ e $\frac{r}{s} \leq \frac{m}{n}$. Então $ms \leq nr$ e $rn \leq sm$ em $\mathbb{Z}$.

Portanto, $ms = nr$, o que implica que $\frac{m}{n} = \frac{r}{s}$, isto é $x = y$.

(iii) $\leq$ é transitiva.

Sejam x, y e z elementos de $\mathbb{Q}$ tais que $x \leq y$ e $y \leq z$, ou seja, $\frac{m}{n} \leq \frac{r}{s}$ e $\frac{r}{s} \leq \frac{p}{q}$. Então $ms \leq nr$ e $rq \leq sp$ em $\mathbb{Z}$. Logo, $msq \leq nrq$ e $rqn \leq spn$. Usando a transitividade da relação de ordem em $\mathbb{Z}$ temos que $msq \leq spn$, e como $s > 0$, temos que $mq \leq pn$. Assim, $\frac{m}{n} \leq \frac{p}{q}$, ou seja $x \leq z$.

(iv) $\leq$ é uma ordem total.

Sejam x e y elementos de $\mathbb{Q}$. Queremos mostrar que $x \leq y$ ou $y \leq x$, ou seja $\frac{m}{n} \leq \frac{r}{s}$ ou $\frac{r}{s} \leq \frac{m}{n}$. Isso ocorre pois, em $\mathbb{Z}$, temos que $ms \leq nr$ ou $nr \leq ms$.

■

O próximo resultado mostra que esta relação de ordem é compatível com as operações de adição e multiplicação em $\mathbb{Q}$.

Proposição 7.15. Sejam x, y e $z \in \mathbb{Q}$.

(a) *Compatibilidade com a adição* - Se $x \leq y$, então $x + z \leq y + z$.

(b) *Compatibilidade com a multiplicação* - Se $x \leq y$ e $0 \leq z$, então $xz \leq yz$.

Prova: Exercício. ■

7.4 A imersão de $\mathbb{Z}$ em $\mathbb{Q}$

Como feito no capítulo anterior, com $\mathbb{N}$ e $\mathbb{Z}$, nesta seção estamos interessados em identificar $\mathbb{Z}$ com um subconjunto de $\mathbb{Q}$. Isto será feito através de uma imersão, ou seja, uma função injetora $f : \mathbb{Z} \to \mathbb{Q}$, que preserva as operações de adição e multiplicação e as relações de ordem.

Definimos $f : \mathbb{Z} \to \mathbb{Q}$, por $f(m) = \frac{m}{1}$, para todo $m \in \mathbb{Z}$. Temos então:

- $\text{Im}(f) = \left\{ \frac{m}{1};\ m \in \mathbb{Z} \right\}$.

- f é injetora, ou seja, se $f(m) = f(n)$, então $\frac{m}{1} = \frac{n}{1}$ em $\mathbb{Q}$, o que implica que $m \cdot 1 = n \cdot 1$ em $\mathbb{Z}$, ou seja $m = n$, para todo m e $n \in \mathbb{Z}$.

- f preserva as operações de adição, ou seja,

$$f(m+n) = \frac{m+n}{1} = \frac{m}{1} + \frac{n}{1} = f(m) + f(n),$$

para todo m e $n \in \mathbb{Z}$.

- f preserva as operações de multiplicação, ou seja,

$$f(m \cdot n) = \frac{m \cdot n}{1} = \frac{m}{1} \cdot \frac{n}{1} = f(m) \cdot f(n),$$

para todo m e $n \in \mathbb{Z}$.

- f preserva as relações de ordem, ou seja, se $m \leq n$ em $\mathbb{Z}$, então existe $u \in \mathbb{Z}_+$ tal que $n = m + u$. Logo,

$$f(n) = \frac{n}{1} = \frac{m+u}{1} = \frac{m}{1} + \frac{u}{1} = f(m) + \frac{u}{1},$$

com $\frac{u}{1} \geq 0$ em $\mathbb{Q}$, o que implica que $f(m) \leq f(n)$ em $\mathbb{Q}$.

Assim, no que se refere aos aspectos algébricos e quanto a ordenação, $\mathrm{Im}(f)\left\{\frac{m}{1};\ m \in \mathbb{Z}\right\}$ é uma cópia de $\mathbb{Z}$ dentro de $\mathbb{Q}$. É coerente portanto, identificarmos $\mathbb{Z}$ com $\mathrm{Im}(f)$ através de f e considerarmos que $\mathbb{Z} \subseteq \mathbb{Q}$. Mais ainda, como $\mathbb{N}$ pode ser visto como um subconjunto de $\mathbb{Z}$, temos $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$. Como era de se esperar, cada número inteiro m será identificado com $\frac{m}{1}$ em $\mathbb{Q}$ e, omitiremos o denominador 1 ao escrevê-lo.

Assumindo estas identificações, se m e $n \in \mathbb{Z}$, com $n \neq 0$, então

$$m : n = \frac{m}{1} : \frac{n}{1} = \frac{m}{1} \cdot \frac{1}{n} = \frac{m}{n} \in \mathbb{Q}.$$

Vamos agora responder a questão formulado no início do capítulo.

Dados números inteiros a e b, com $a \neq 0$, a equação $a \cdot X = b$ admite uma única solução em $\mathbb{Q}$, à saber, $X = a^{-1} \cdot b = b : a = \frac{b}{a}$, mesmo quando $a \nmid b$.

7.5 Exercícios

1. Prove que a relação $\sim$ definida em $\mathbb{Z} \times \mathbb{Z}^*$ por

$$(m, n) \sim (p, q) \Longleftrightarrow mq = np$$

é uma relação de equivalência.

2. Em relação às operações de adição e subtração definidas em $\mathbb{Q}$, prove que para quaisquer que sejam $a, b, c \in \mathbb{Q}$ valem as seguintes propriedades:

   a) Associativa: (a+b)+c = a+(b+c)

   b) Comutativa: $a + b = b + a$

   c) $-(a + b) = -a - b$

   d) $(a - b) + b = a$

   e) $a + x = b \Longleftrightarrow x = b - a$

   f) $a + b = a + c \Longleftrightarrow b = c$.

3. Para quaisquer $a, b, c \in \mathbb{Q}$ prove que valem:

   a) $(a^{-1})^{-1} = a$

   b)$(ab)^{-1} = a^{-1}b^{-1}$

   c) $a(b + c) = ab + ac$

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

   e) $a(-b) = (-a)b = -(ab)$

   f) $(-a)(-b) = ab$

4. a) Seja x um elemento de $\mathbb{Q}$ tal que $x + \alpha = \alpha$, para todo $\alpha \in \mathbb{Q}$. Mostre que $x = 0$.

   b) Demonstrar que o oposto de um racional é único.

5. Mostre que toda equação da forma $a\,x = b$, onde a, b são números racionais, $b \neq 0$, tem solução em $\mathbb{Q}$. Mostre também que essa solução é única.

6. Mostre que para toda terna x, y, z de racionais tem-se que:

   a) Se $x \leq y$, então $x + z \leq y + z$.

   b) Se $x \leq y$ e $0 \leq z$, então $xz \leq yz$.

7. Se x e y são racionais tais que $x < y$, então sempre existe um racional z tal que $x < z < y$.

8. Sejam x e y racionais positivos. Prove que existe um natural n tal que $nx > y$. (Propriedade Arquimediana em $\mathbb{Q}$.)

Referências Bibliográficas

[1] Bloch, E. D.; *Proofs and Fundamentals: a First Course in Abstract Mathematics*; Boston: Birkhäuser, 2000.

[2] Castrucci, B.; *Elementos de Teoria dos Conjuntos*; Série Professor n.3, São Paulo, 1976.

[3] Domingues, H. H.; *Fundamentos de Aritmética*; Editora Atual, São Paulo, 1991.

[4] Lipschutz, S.; *Teoria dos Conjuntos*; Mc-Graw-Hill do Brasil, 1978.

[5] Lipschutz, S.; *Topologia Geral*; Mc-Graw-Hill do Brasil, 1973.

[6] Monteiro, L. H. J.; *Álgebra Moderna*; LpM, São Paulo, 1966.

[7] Morash, R. P.; *Bridge to Abstract Mathematics*; The Handom House/Birkhäuser Mathematics Series, 1987.