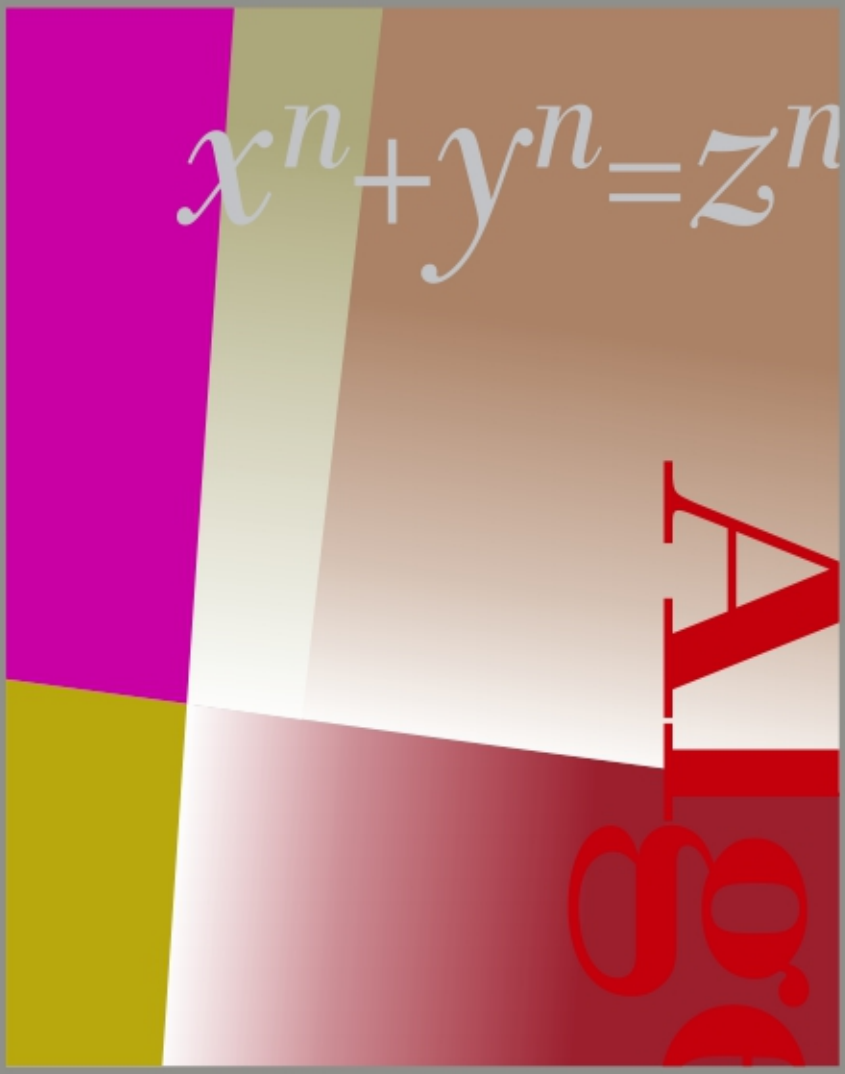
INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

Curso de Álgebra

volume 1



COLEÇÃO MATEMÁTICA UNIVERSITÁRIA

Abramo Hefez

Curso de Álgebra
volume 1

Hefez, Abramo
Curso de álgebra, volume 1 / Abramo Hefez. 1 ed. Rio de Janeiro : IMPA, 2014.
213 p. (Coleção matemática universitária)

Inclui bibliografia.
e-ISBN 978-85-244-0386-6

1. Álgebra. 2. Teoria dos Números. I. Título. II. Série.

CDD-512

COLEÇÃO MATEMÁTICA UNIVERSITÁRIA

Curso de Álgebra
volume 1

Abramo Hefez

impa

INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

Impresso no Brasil / Printed in Brazil

Capa: Sérgio R. Vaz e Noni Geiger

Coleção Matemática Universitária
Comissão Editorial:

Elon Lages Lima
S. Collier Coutinho
Paulo Sad

Títulos Publicados:

- Análise Real, vol. 1: Funções de uma Variável – Elon Lages Lima
- EDP. Um Curso de Graduação – Valéria Iório
- Curso de Álgebra, Volume 1 – Abramo Hefez
- Álgebra Linear – Elon Lages Lima
- Introdução às Curvas Algébricas Planas – Israel Vainsencher
- Equações Diferenciais Aplicadas – Djairo G. de Figueiredo e Aloisio Freiria Neves
- Geometria Diferencial – Paulo Ventura Araújo
- Introdução à Teoria dos Números – José Plínio de Oliveira Santos
- Cálculo em uma Variável Complexa – Marcio G. Soares
- Geometria Analítica e Álgebra Linear – Elon Lages Lima
- Números Primos: Mistérios e Recordes – Paulo Ribenboim
- Análise no Espaço R^n – Elon Lages Lima
- Análise Real, vol. 2: Funções de n Variáveis – Elon Lages Lima
- Álgebra Exterior – Elon Lages Lima
- Equações Diferenciais Ordinárias – Claus Ivo Doering e Artur Oscar Lopes
- Análise Real, vol. 3: Análise Vetorial – Elon Lages Lima
- Álgebra Linear. Exercícios e Soluções – Ralph Costa Teixeira
- Números Primos. Velhos Mistérios e Novos Recordes – Paulo Ribenboim

Distribuição:

IMPA
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ
e-mail: ddic@impa.br
http://www.impa.br

Este livro é dedicado a
Maria Lúcia, Felipe, Gabriel
e Júlia (in memoriam)

Prefácio

Curso de Álgebra, Volume 1, é o primeiro volume da uma trilogia destinada à formação básica em Álgebra dos alunos de graduação em Matemática e áreas afins. Este livro foi publicado pela primeira vez há cerca de 20 anos e, desde então, vem tendo uma boa acolhida, sendo utilizado em vários cursos pelo país e pela América Latina, justificando essa nova edição revisada. Ele é dedicado ao estudo dos números, começando com os inteiros e indo até os complexos, passando pelos racionais e os reais, dando ênfase às suas estruturas de anel e corpo e explorando a relação entre Álgebra e Aritmética.

A seguir, descrevemos a estrutura global dos três semestres do curso, correspondentes a cada um dos volumes.

No primeiro semestre, recomendamos os conteúdos dos Capítulos 1 a 7 e 9 deste livro. O Capítulo 8, por não fazer parte dos programas tradicionais de Álgebra, pode ser utilizado em turmas especiais ou para a realização de seminários com os alunos mais motivados.

No segundo semestre, estudam-se os polinômios e a sua álgebra, as equações algébricas, em especial as do terceiro e quarto graus, e as relações entre os coeficientes e as raízes de uma equação, onde aparecem os polinômios simétricos. Isso conduz naturalmente aos Grupos Simétricos, desembocando no método de Lagrange para a resolução das equações do terceiro e quarto graus, inspirador da teoria geral das equações devida a Abel e Galois. Em seguida, estudam-se as extensões de corpos e as suas relações com a Álgebra Linear, abordando os problemas clássicos da construtibilidade com régua e compasso de certas figuras geométricas. Um ponto culminante do curso é a prova do resultado de Abel que mostra que as equações gerais de grau maior do que quatro não são resolúveis por radicais. O Volume 2 finaliza com uma introdução aos números algébricos, através dos inteiros Gaussianos que, também, por não fazer parte dos programas, pode ser utilizada para realizar seminários com os alunos.

O terceiro semestre é dedicado ao estudo da Teoria dos Grupos e da Teoria de Galois, além de outros tópicos.

Esta presente edição é uma profunda revisão da 3ª edição da qual foi retirado o capítulo sobre os inteiros Gaussianos, que passa para o Volume 2, e foi acrescido um apêndice sobre noções de lógica, imprescindível para o aluno desejoso de aprimorar a sua formação matemática.

Niterói, fevereiro de 2010.
Abramo Hefez

Conteúdo

1

Conjuntos

A Teoria dos Conjuntos foi criada no final do século dezenove por Georg Cantor para abordar certas questões sutis da Teoria das Funções. As ideias revolucionárias de Cantor, de início incompreendidas por serem demasiado abstratas para a época, foram rapidamente se impondo como elemento unificador dos vários ramos da matemática, a ponto de se tornarem o meio pelo qual é formalizada toda a matemática contemporânea.

O nosso tratamento para a Teoria dos Conjuntos será deliberadamente ingênuo, não nos preocupando, portanto, em fundamentá-la com todo o rigor.

1 A linguagem dos conjuntos

Os termos *conjunto* e *elemento* e a relação de um elemento pertencer a um conjunto são conceitos primitivos; ou seja, não serão definidos.

Usa-se o termo *coleção* como sinônimo de conjunto. Os conjuntos são usualmente designados por letras maiúsculas do alfabeto latino ou grego, enquanto que os elementos o são por letras minúsculas. A afirmação de que o elemento a pertence ao conjunto A é simbolizada por

$$a \in A,$$

e a sua negação é simbolizada por

$$a \notin A.$$

Dois conjuntos são considerados *iguais*, se eles têm os mesmos elementos. Mais precisamente, temos que $A = B$ se, e somente se, todo elemento de A é elemento de B e todo elemento de B é elemento de A.

A condição de que todo elemento de um conjunto A pertence a um conjunto B, estabelece uma relação entre A e B, chamada de relação de *inclusão*. Quando existir uma tal relação entre A e B escreveremos

$$A \subset B \quad \text{ou} \quad B \supset A,$$

que se lê A está *contido* em B, ou A é *subconjunto* de B ou, ainda, B *contém* A.

A relação de inclusão possui claramente as seguintes propriedades:

1) $A \subset A$, para todo conjunto A.
2) $A = B$ se, e somente se, $A \subset B$ e $B \subset A$.
3) Se $A \subset B$ e $B \subset C$, então $A \subset C$.

A negação de $A \subset B$, ou seja, o fato de A não ser subconjunto de B, é simbolizada por $A \not\subset B$ e significa que existe pelo menos um elemento de A que não pertence a B. Se $A \subset B$ e $A \neq B$, diremos que A é *subconjunto próprio* de B. Neste caso, escrevemos

$$A \subsetneq B.$$

No que se segue, admitiremos o leitor familiarizado com o conjunto $\mathbb{N}$ dos *números naturais*:

$$0, 1, 2, 3, \ldots,$$

e com o conjunto $\mathbb{Z}$ dos *números inteiros*:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Um conjunto pode ser dado exibindo-se todos os seus elementos. Por exemplo, $\{a, b, c\}$ é o conjunto formado pelas três primeiras letras do nosso alfabeto; o conjunto $\{1\}$ é formado por apenas um elemento que é o número 1. Quando não houver risco de confusão, poderemos dar, por exemplo, um conjunto do seguinte modo:

$$\{1, 2, 3, \ldots, 1000\},$$

onde as reticências subentendem os inteiros de 4 a 999.

No que se segue, mostraremos como construir novos conjuntos a partir de conjuntos dados. Antes, porém, introduziremos a noção importante de sentença aberta.

Diremos que x é uma *indeterminada* para o conjunto A se x é uma letra que não representa nenhum elemento específico de A.

Uma *sentença aberta* $P(x)$ em um conjunto A é uma sentença que contém, como palavra, uma indeterminada x para A, tal que toda vez que se substitui x por um elemento específico a de A, obtém-se uma sentença $P(a)$ que é verdadeira ou falsa.

Exemplos

a. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta:

$$x \geq 0.$$

É claro que ao substituir x por um número inteiro, obtemos uma sentença que é verdadeira ou falsa. Em particular, $P(0)$, $P(1)$ e $P(8)$ são verdadeiras e $P(-1)$, $P(-2)$ e $P(-8)$ são falsas.

b. Sejam A um conjunto qualquer e $P(x)$ a sentença aberta:

$$x \in A.$$

É claro que $P(a)$ é verdadeira para todo $a \in A$ e falsa para todo $a \notin A$.

c. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta:

$$\text{Existe } n \in \mathbb{Z}, \quad \text{tal que} \quad x = 2 \cdot n.$$

Temos que $P(0)$, $P(2)$ e $P(-4)$ são verdadeiras, enquanto $P(1)$ e $P(-1)$ são falsas. É claro que $P(a)$ é verdadeira se, e somente se, a é um número par.

d. Sejam $A = \mathbb{Z}$ e $P(x)$ a sentença aberta:

$$\text{Existem } n \text{ e } m \text{ inteiros, tais que } x = m \cdot 4 + n \cdot 6.$$

Temos que $P(2)$ é verdadeira pois $2 = 2 \cdot 4 + (-1) \cdot 6$ ($m = 2$ e $n = -1$); $P(-6)$ é verdadeira ($m = 0$ e $n = -1$); $P(0)$ é verdadeira ($m = n = 0$); $P(3)$ é falsa (justifique).

e. Sejam A um conjunto e $P(x)$ uma sentença aberta em A. Forma-se uma nova sentença aberta em A tomando a negação (não $P(x)$) da

sentença aberta $P(x)$. Temos que (não $P(a)$) é verdadeira se, e somente se, $P(a)$ é falsa. Por exemplo, se $A = \mathbb{Z}$ e $P(x)$ é a sentença aberta $x < 0$, então (não $P(x)$) é a sentença aberta $x \geq 0$.

f. Sejam A um conjunto e $P(x)$ a sentença aberta em A:

$$x \neq x.$$

Temos que $P(a)$ é falsa para todo $a \in A$.

Como o conceito de conjunto não foi definido, não será possível provar a existência de certos conjuntos. Isto terá que ser estabelecido caso a caso por meio de um axioma específico, como faremos a seguir.

Dados um conjunto A e uma sentença aberta $P(x)$ em A, admitiremos a existência de um subconjunto de A formado pelos elementos a de A para os quais $P(a)$ é verdadeira. Este conjunto, chamado de *conjunto verdade de* $P(x)$, será denotado por:

$$\{x \in A;\ P(x)\}.$$

Exemplos

a′. O conjunto $\{x \in \mathbb{Z};\ x \geq 0\}$ é o conjunto $\mathbb{N}$ dos números naturais.

b′. Temos que $\{x \in A;\ x \in A\} = A$

c′. Temos que $\{x \in \mathbb{Z};$ existe $n \in \mathbb{Z}$, tal que $x = 2 \cdot n\}$ é o conjunto dos números inteiros pares.

d′. Pode-se mostrar (Problema 1.4) que o conjunto:

$$\{x \in \mathbb{Z};\ \text{ existem } n \text{ e } m \text{ inteiros, tais que } x = m \cdot 4 + n \cdot 6\}$$

coincide com o conjunto dos números pares. No Capítulo 4, estudaremos detalhadamente esse tipo de conjunto.

e′. Seja $P(x)$ uma sentença aberta num conjunto A. Considere os conjuntos $B = \{x \in A;\ P(x)\}$ e $B' = \{x \in A;\ \text{(não } P(x))\}$. É claro que B e B' não têm elementos em comum e que qualquer elemento de A pertence a um destes dois conjuntos.

f′. O conjunto $\{x \in A;\ x \neq x\}$ não possui qualquer elemento.

O último exemplo, acima, nos conduz a admitir a existência de um conjunto que não tem elementos. Tal conjunto será chamado de *conjunto vazio* e será simbolizado por $\emptyset$.

Afirmamos que $\emptyset \subset A$, qualquer que seja o conjunto A. Esta afirmação parece estranha à primeira vista, mas veja como é natural a

falsidade de sua negação (isto é, a sua veracidade). A afirmação $\emptyset \not\subset A$, para algum conjunto A, significa que existe pelo menos um $x \in \emptyset$ tal que $x \notin A$ e isto é claramente falso, visto que o conjunto $\emptyset$ não possui qualquer elemento.

Introduziremoa a seguir alguns conceitos de Lógica Matemática, remetendo o leitor ao Apêndice A para maiores detalhes.

Sejam $P(x)$ uma sentença aberta e A um conjunto. Usaremos as notações:

$$\forall\, x \in A,\ P(x),$$

para representar a sentença, *para todo* x *em* A*, a asserção* $P(x)$ *é verdadeira*, e

$$\exists\, x \in A,\ P(x),$$

para representar a sentença, *existe pelo menos um* x *em* A *tal que* $P(x)$ *é verdadeira*.

Os símbolos $\forall$ e $\exists$ são chamados *quantificadores universal e existencial*, respectivamente.

A negação da sentença $\forall\, x \in A,\ P(x)$ é a sentença

$$\exists\, x \in A,\ (\text{não } P(x)),$$

enquanto que a negação da sentença $\exists\, x \in A,\ P(x)$ é a sentença

$$\forall\, x \in A,\ \ (\text{não } P(x)).$$

Utilizaremos os conectivos *e* e *ou*, sendo que o conectivo *ou* terá sentido inclusivo; isto é, significando uma coisa ou outra, ou ambas. Se P e Q são sentenças, a negação de P *ou* Q é

$$(\text{não } P)\ \ e\ \ (\text{não } Q),$$

enquanto que a negação de P *e* Q é

$$(\text{não } P)\ \ ou\ \ (\text{não } Q).$$

Problemas

1.1 Falso ou verdadeiro:

a) $\{a, a, b, c\} = \{a, b, c\}$ b) $\{a\} = \{a, \{a\}\}$
c) $\{a\} \in \{a, \{a\}\}$ d) $\{a\} \subset \{a, \{a\}\}$
e) $\{\{a\}\} \subset \{a, \{a\}\}$ f) $\{a, b\} \subset \{a, \{a, b\}\}$

1.2 Falso ou verdadeiro:

a) $\emptyset \in \{\emptyset\}$ b) $\emptyset = \{\emptyset\}$ c) $\emptyset \subset \{\emptyset\}$
d) $\{\emptyset\} \subset \{\{\emptyset\}\}$ e) $\{\emptyset\} \in \{\{\emptyset\}\}$ f) $\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$

1.3 Quantos subconjuntos tem cada um dos seguintes conjuntos?

a) $\{1\}$ b) $\{1, 2\}$ c) $\{1, 2, 3\}$

Generalize.

1.4 Caracterize todos os inteiros x para os quais é verdadeira a sentença aberta $P(x)$ dada por:

a) Existem inteiros m e n, tais que $x = m \cdot 2 + n \cdot 3$.

b) Existem inteiros m e n, tais que $x = m \cdot 4 + n \cdot 6$.

2 Operações com conjuntos

2.1. União de conjuntos

Dada uma coleção qualquer de conjuntos, admitiremos a existência de um conjunto tal que cada um de seus elementos pertence a pelo menos um dos conjuntos da coleção. Tal conjunto será chamado de *união* dos conjuntos da coleção.

A união de dois conjuntos A e B é, portanto, o conjunto de todos os elementos que pertencem a A ou pertencem a B; esse será denotado por $A \cup B$.

Por exemplo, se $A = \{a, b, c\}$ e $B = \{b, c, d\}$, então $A \cup B = \{a, b, c, d\}$.

Quando numa discussão usarmos uma "sentença aberta" $P(x)$, sem especificar sobre que conjunto ela é definida, subentende-se que ela está definida sobre a união de todos os conjuntos envolvidos na discussão.

As propriedades a seguir decorrem imediatamente das definições.

Propriedades

Para todos os conjuntos A, B e C, temos que:

1) $A \cup \emptyset = A$ e $A \cup A = A$.

2) $A \subset A \cup B$ e $B \subset A \cup B$.

3) $A \cup B = B \cup A$.

4) $(A \cup B) \cup C = A \cup (B \cup C)$.

Proposição 1.2.1. *Dados conjuntos* A, A', B *e* B', *com* $A \subset B$ *e* $A' \subset B'$, *então* $A \cup A' \subset B \cup B'$.

Demonstração Se $A \cup A' = \emptyset$, a asserção é claramente verdadeira. Suponha que $A \cup A' \neq \emptyset$. Se $x \in A \cup A'$, temos que $x \in A$ ou $x \in A'$, e como $A \subset B$ e $A' \subset B'$, segue-se que $x \in B$ ou $x \in B'$, logo $x \in B \cup B'$. Isto prova que $A \cup A' \subset B \cup B'$. □

Corolário 1.2.2. $A \cup B = A$ *se, e somente se,* $B \subset A$.

Demonstração Suponhamos que $A \cup B = A$. Como $B \subset A \cup B$, segue-se que $B \subset A$.

Reciprocamente, suponha que $B \subset A$. Como $A \subset A$, segue-se da proposição que $A \cup B \subset A \cup A = A$, logo $A \cup B \subset A$. Como $A \subset A \cup B$, segue-se que $A \cup B = A$. □

2.2. Interseção de conjuntos

Dados dois conjuntos A e B, a *interseção* de A e B é o conjunto

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

Quando $A \cap B = \emptyset$, dizemos que os conjuntos A e B são *disjuntos*.

Por exemplo, se $A = \{a, b, c\}$, $B = \{b, c, d\}$ e $C = \{d, e, f\}$, então $A \cap B = \{b, c\}$ e A e C são disjuntos.

As propriedades a seguir decorrem imediatamente das definições.

Propriedades

Para todos os conjuntos A, B e C, temos que:

1) $A \cap \emptyset = \emptyset$ e $A \cap A = A$.

2) $A \cap B \subset A$ e $A \cap B \subset B$.

3) $A \cap B = B \cap A$.

4) $(A \cap B) \cap C = A \cap (B \cap C)$.

Proposição 1.2.3. *Dados conjuntos* A, B *e* C, *quaisquer, temos que:*

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

Demonstração Inicialmente, provaremos a inclusão

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C).$$

Se $A \cap (B \cup C) = \emptyset$, nada temos a provar. Suponha que $A \cap (B \cup C) \neq \emptyset$. Seja x um elemento qualquer de $A \cap (B \cup C)$. Logo, $x \in A$ e $x \in B \cup C$. Se $x \in B$, então $x \in A \cap B$. Se $x \in C$, então $x \in A \cap C$. Em qualquer caso, temos que $x \in (A \cap B) \cup (A \cap C)$.

Agora, provaremos a inclusão

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C).$$

Se o conjunto da esquerda for vazio, a inclusão é obviamente verificada. Suponha que tal conjunto é não vazio, e seja x um elemento qualquer dele. Logo, $x \in A \cap B$ ou $x \in A \cap C$. Em qualquer caso, $x \in A$ e temos que $x \in B$ ou $x \in C$. Portanto, $x \in A \cap (B \cup C)$. □

Proposição 1.2.4. *Dados conjuntos* A, B *e* C, *quaisquer, temos que:*

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

Demonstração Deixamos esta demonstração a cargo do leitor. □

2.3. Diferença de conjuntos

Dados dois conjuntos A e B, a *diferença* A menos B é o conjunto

$$A \setminus B = \{x;\ x \in A \ \text{ e } \ x \notin B\}.$$

Quando $B \subset A$, a diferença $A \setminus B$ é denotada por $C_A(B)$ e é chamada de *complementar* de B em A.

Por exemplo, se $A = \{a, b, c\}$ e $B = \{b, c, d\}$, então $A \setminus B = \{a\}$.

As seguintes propriedades decorem imediatamente das definições.

Propriedades

Para todos os conjuntos A e B, temos que:

1) $A \setminus \emptyset = A$ e $A \setminus A = \emptyset$.
2) Se $A \cap B = \emptyset$, então $A \setminus B = A$ e $B \setminus A = B$.
3) $C_A(\emptyset) = A$ e $C_A(A) = \emptyset$.

Proposição 1.2.5. *Sejam* B *e* B' *subconjuntos de* A. *Se* $B \subset B'$, *então*

$$C_A(B') \subset C_A(B).$$

Demonstração Suponha que $B \subset B'$. Se $C_A(B') = \emptyset$, nada temos a provar. Suponha $C_A(B') \neq \emptyset$ e seja x um elemento qualquer de $C_A(B')$. Logo $x \notin B'$. Segue-se que $x \notin B$, pois, caso contrário, como $B \subset B'$, teríamos $x \in B'$. Consequentemente, $x \in C_A(B)$. □

Proposição 1.2.6. *Sejam* B *e* B' *subconjuntos de* A. *Temos que*

$$C_A(B \cup B') = C_A(B) \cap C_A(B').$$

Demonstração A proposição decorre da seguinte cadeia de equivalências:

$$\begin{aligned} x \in C_A(B \cup B') &\iff x \notin B \cup B' \\ &\iff x \notin B \quad \text{e} \quad x \notin B' \\ &\iff x \in C_A(B) \cap C_A(B'), \end{aligned}$$

para todo elemento x de A. □

Proposição 1.2.7. *Sejam* B *e* B' *subconjuntos de* A. *Temos que*

$$C_A(B \cap B') = C_A(B) \cup C_A(B').$$

Demonstração Deixada a cargo do leitor. □

2.4. Conjuntos das partes e produto cartesiano

Dado um conjunto A, qualquer, admitiremos a existência de um conjunto $P(A)$ cujos elementos são todos os subconjuntos de A, chamado *conjunto das partes de* A.

Um *par ordenado* (a, b) de elementos de A é um elemento de $P(P(A))$ da forma

$$\{\{a\}, \{a, b\}\}.$$

Não é difícil convencer-se que $(a, b) = (a', b')$ se, e somente se, $a = a'$ e $b = b'$.

Dados dois conjuntos A e B, o *produto cartesiano* de A e B é o conjunto $A \times B$ de todos os pares ordenados (a, b) de elementos de $A \cup B$ tais que $a \in A$ e $b \in B$. Simbolicamente, escrevemos

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

Por exemplo, se $A = \{a, b\}$ e $B = \{c, d\}$, temos que

$$A \times B = \{(a, c), (a, d), (b, c), (b, d)\},$$

e

$$B \times A = \{(c, a), (c, b), (d, a), (d, b)\}.$$

Note que, em geral, $A \times B \neq B \times A$. Temos também que $A \times B = \emptyset$ se, e somente se, $A = \emptyset$ ou $B = \emptyset$.

Utilizaremos a notação A^n para representar o produto cartesiano do conjunto A por ele mesmo n vezes.

2.5. Famílias de conjuntos

Seja I um conjunto não vazio qualquer. Uma *família indexada* por I é uma coleção de conjuntos A_i com $i \in I$. Uma tal família será denotada por $(A_i)_{i\in I}$.

A união dos elementos da família é

$$\bigcup_{i\in I} A_i = \{x;\ x \in A_i \text{ para algum } i \in I\}$$

e a sua interseção é

$$\bigcap_{i\in I} A_i = \{x;\ x \in A_i \text{ para todo } i \in I\}.$$

É claro que, para todo $j \in I$,

$$A_j \subset \bigcup_{i\in I} A_i \quad \text{e} \quad \bigcap_{i\in I} A_i \subset A_j\,.$$

Problemas

2.1 Mostre que:

a) Se $A \subset B$ e $A' \subset B'$, então $A \cap A' \subset B \cap B'$.

b) $A \cap B = A$ se, e somente se, $A \subset B$.

2.2 Demonstre a Proposição 1.2.4.

2.3 Mostre que, se $B \subset A$, então

a) $B \cup C_A(B) = A$ b) $B \cap C_A(B) = \emptyset$.

2.4 Suponha que B e B' são subconjuntos de A. Mostre que:

a) $C_A(C_A(B)) = B$.

b) Se $C_A(B') \subset C_A(B)$, então $B \subset B'$.

c) $C_A(B \cap B') = C_A(B) \cup C_A(B')$.

2.5 Dados B e B' subconjuntos de A, mostre que:

a) $B \cup (C_A(B) \cap B') = B \cup B'$.

b) $B \cap (C_A(B) \cup B') = B \cap B'$.

c) $B \setminus B' = C_A(B') \setminus C_A(B)$.

d) $B \setminus B' = B \cap C_A(B')$.

2.6 Mostre que, para quaisquer conjuntos A, B e C, vale:

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

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

c) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

d) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

2.7 Suponha que $A \cap B = \emptyset$. Mostre que:

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

b) $A \setminus B = A$.

c) $A = (A \cup B) \setminus B$.

2.8 Diga se cada uma das seguintes asserções é falsa ou verdadeira. Prove-a quando verdadeira ou dê um contra-exemplo quando falsa.

a) Se $A \cup B = A \cup C$, então $B = C$.

b) Se $A \cap B = A \cap C$, então $B = C$.

c) Se $A \cup B = A \cup C$ e $A \cap B = A \cap C$, então $B = C$.

2.9 Demonstre as seguintes igualdades:

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

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

c) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) = (A \times D) \cap (C \times B)$.

d) $(A \times B) \setminus (C \times D) = [(A \setminus C) \times B] \cup [A \times (B \setminus D)]$.

2.10 Sejam A, B, C e D conjuntos tais que $A \neq \emptyset$ e $B \neq \emptyset$. Mostre que $A \subset$ e $C \subset D$ se, e somente se, $A \times C \subset B \times D$.

2.11 Sejam $(A_i)_{i\in I}$ uma família de conjuntos e A um conjunto. Mostre que:

a) $A \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I}(A \cap A_i)$.

b) $A \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I}(A \cup A_i)$.

c) $A \setminus \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I}(A \setminus A_i)$.

d) $A \setminus \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(A \setminus A_i)$.

3 Funções

3.1. O conceito de função

Uma *função* consiste de dois conjuntos não vazios X e Y e de uma lei f que associa a cada elemento $x \in X$ um único elemento $f(x) \in Y$.

Uma função será simbolizada por

$$\begin{aligned} f\colon X &\to Y \\ x &\mapsto f(x) \end{aligned}$$

Para abreviar, quando não quisermos explicitar a lei f, usaremos a notação $f\colon X \to Y$ e nos referiremos a f como sendo a função.

O conjunto X é chamado de *domínio* da função f e $f(x)$ de *imagem* de x por f. Usaremos também os nomes *aplicação* ou *correspondência* como sinônimos de função.

Para termos certeza que uma dada lei $x \mapsto f(x)$, que associa aos elementos de X elementos de Y, define uma função $f\colon X \to Y$, devemos verificar que, efetivamente, a cada elemento de X é associado um único elemento de Y. Deve-se então mostrar que se $a = b$, então $f(a) = f(b)$.

Duas funções,

$$\begin{aligned} f_1\colon X_1 &\longrightarrow Y_1 \\ x &\longmapsto f_1(x) \end{aligned} \qquad\qquad \begin{aligned} f_2\colon X_2 &\longrightarrow Y_2 \\ x &\longmapsto f_2(x) \end{aligned}$$

serão consideradas *iguais*, escrevendo-se, neste caso, $f_1 = f_2$, se $X_1 = X_2$, $Y_1 = Y_2$ e $f_1(x) = f_2(x)$ para todo $x \in X_1 = X_2$.

Exemplos

1. Seja

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z}. \\ x &\longmapsto x+1 \end{aligned}$$

Esta função associa a cada número inteiro x o número inteiro $f(x) = x+1$. Em particular, temos que $f(0) = 1$, $f(-1) = 0$ e $f(1) = 2$.

2. A função $f\colon X \to X$, que a cada elemento x associa o próprio x, recebe o nome de *função identidade* de X e é denotada por id_X.

3. Seja $f\colon X \to Y$ uma função tal que existe $b \in Y$ com $f(x) = b$ para todo x de X. Este tipo de função é chamado de *função constante.*

4. Toda função $s\colon \mathbb{N}\backslash\{0\} \to A$ é chamada de *sequência* em A. Costuma-se escrever s_n no lugar de $s(n)$.

5. Sejam $f\colon X \to Y$ uma função e A um subconjunto de X. Podemos definir uma nova função $g\colon A \to Y$ com a mesma lei de f, isto é, $g(x) = f(x)$ para todo $x \in A$. Esta função é chamada de *restrição* de f a A e é denotada por $f|_A$ ou, quando não houver risco de confusão, simplesmente por f.

6. Seja A um conjunto. Uma função qualquer $f\colon A \times A \to A$ é chamada de *operação* em A.

Diremos que a operação f é *comutativa* se, para todo par (a, b) em $A \times A$, tem-se que

$$f(a, b) = f(b, a).$$

A operação f será dita *associativa* se, para todos os elementos a, b e c de A, tem-se que

$$f(a, f(b, c)) = f(f(a, b), c).$$

Um elemento e de A será dito *elemento neutro* para a operação f, se para todo elemento a de A, tem-se que

$$f(a, e) = f(e, a) = a.$$

Se f possui um elemento neutro e, um elemento b de A será dito *elemento simétrico* ou *inverso* de a, se

$$f(a, b) = f(b, a) = e.$$

As funções

$$\begin{aligned} +\colon \mathbb{Z}\times\mathbb{Z} &\longrightarrow \mathbb{Z} & \qquad \cdot\colon \mathbb{Z}\times\mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a,b) &\longmapsto a+b & (a,b) &\longmapsto a\cdot b \end{aligned}$$

são exemplos de operações associativas, comutativas e com elementos neutros 0 e 1, respectivamente.

7. Sejam $X=\{a,b\}$ e $Y=\{1,2\}$. Damos abaixo todas as funções de X em Y.

$$f_1:\begin{cases} a\mapsto 1\\ b\mapsto 1\end{cases} \qquad f_2:\begin{cases} a\mapsto 2\\ b\mapsto 2\end{cases} \qquad f_3:\begin{cases} a\mapsto 1\\ b\mapsto 2\end{cases} \qquad f_4:\begin{cases} a\mapsto 2\\ b\mapsto 1\end{cases}$$

3.2. Composição de funções

Dadas duas funções $f\colon X\to Y$ e $g\colon Y\to Z$, define-se uma nova função $h\colon X\to Z$ com a regra

$$h(x)=g(f(x)).$$

A função h é chamada de *função composta* de g com f e é denotada por $g\circ f$. Temos portanto, por definição, que

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

Exemplos

1. Sejam

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z} & \qquad g\colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto x+1 & x &\longmapsto x^2 \end{aligned}$$

Considere as funções $f\circ g$ e $g\circ f$ de $\mathbb{Z}$ em $\mathbb{Z}$. Temos que

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

enquanto

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

Este exemplo mostra que, em geral, tem-se $f\circ g\neq g\circ f$, pois

$$f\circ g(-1)=2\neq 0=g\circ f(-1).$$

2. Seja $f\colon X\to Y$ uma função. Temos que

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

e que

$$\mathrm{id}_Y \circ f(x) = \mathrm{id}_Y(f(x)) = f(x).$$

Logo, qualquer que seja a função $f\colon X \to Y$, tem-se que

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

3. Sejam

$$\begin{array}{lll} f\colon \mathbb{Z} \longrightarrow \mathbb{Z} & & g\colon \mathbb{Z} \longrightarrow \mathbb{Z} \\ \quad x \longmapsto x+1 & & \quad x \longmapsto x-1 \end{array}$$

Temos que $f \circ g = g \circ f = \mathrm{id}_{\mathbb{Z}}$.

4. Seja $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^3$. Considere a função $f^2 = f \circ f$. Temos que $f^2(x) = f \circ f(x) = (x^3)^3 = x^9$. Atenção, não confundir $f^2(x)$ com $(f(x))^2$ que, neste caso, é x^6.

O processo de composição pode ser iterado. Dadas três funções, $f\colon X \to Y$, $g\colon Y \to Z$ e $h\colon Z \to W$, podemos compor estas funções de dois modos aparentemente distintos:

$$h \circ (g \circ f) \quad \text{e} \quad (h \circ g) \circ f.$$

Parece, portanto, ambíguo falar da composta $h \circ g \circ f$ das três funções. Mas, na verdade, esta ambiguidade inexiste pois os dois modos de compor as funções conduzem ao mesmo resultado, como mostra a seguinte cadeia de igualdades:

$$[h \circ (g \circ f)](x) = h(g \circ f(x)) = h(g(f(x))) = h \circ g(f(x)) = [(h \circ g) \circ f](x).$$

Está, portanto, bem definida a função $h \circ g \circ f\colon X \to W$, pois

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

3.3. Imagens diretas e inversas

Dada uma função $f\colon X \to Y$ e um subconjunto A de X, define-se a *imagem direta* de A por f como sendo

$$f(A) = \{y \in Y;\ y = f(x) \ \text{ para algum } x \text{ em } \ A\}.$$

Em particular, $f(X)$ é chamado simplesmente de *conjunto imagem* de f.

Se V é um subconjunto de Y, define-se a *imagem inversa* de V por f como sendo:

$$f^{-1}(V) = \{x \in X;\ f(x) \in V\}.$$

Decorre imediatamente das definições que $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$ e $f^{-1}(Y) = X$.

Para $x \in X$, denotaremos o conjunto $f^{-1}(\{x\})$ por $f^{-1}(x)$

Exemplo Seja $f\colon \mathbb{Z} \to \mathbb{Z}, \quad x \mapsto x^2$. Então

$$f(\{0,-1,2\}) = f(\{0,-1,1,-2,2\}) = \{0,1,4\}, \quad \text{e} \quad f(\mathbb{Z}) = \mathbb{N}.$$

$$f^{-1}(0) = \{0\}, \quad f^{-1}(1) = \{-1,1\}, \quad f^{-1}(4) = \{-2,2\}, \quad \text{e} \quad f^{-1}(\mathbb{N}) = \mathbb{Z}.$$

Problemas

3.1 Determine todas as funções de $X = \{a,b,c\}$ em $Y = \{1,2\}$.

3.2 Sejam f, g e h funções de $\mathbb{Z}$ em $\mathbb{Z}$ tais que $h(1) = 3$, $g(x) = 3$ e $f(2) = 5$, calcule $f \circ g(3)$, $g \circ h(1)$ e $f \circ g \circ h(1)$.

3.3 Sejam

$$\begin{array}{ccccc} f\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}, & g\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}, & h\colon \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & ax+b & x & \longmapsto & cx+d & x & \longmapsto & x^2+1 \end{array}$$

onde a, b, c e d são números inteiros. Determine as funções $f \circ g$, $g \circ f$, $h \circ f$, $f \circ h$, g^2, f^3, h^2 e $g \circ h \circ f$.

3.4 Seja $f\colon X \to Y$ uma função. Se $A \subset B \subset X$ e $V \subset W \subset Y$, mostre que $f(A) \subset f(B)$ e $f^{-1}(V) \subset f^{-1}(W)$.

3.5 Seja $f\colon X \to Y$ uma função. Se $A, B \subset X$, mostre que:

a) $f(A \cup B) = f(A) \cup f(B)$.

b) $f(A \cap B) \subset f(A) \cap f(B)$. Mostre com um exemplo que, em geral, não vale a igualdade.

c) $f(A \setminus B) \supset f(A) \setminus f(B)$. Mostre com um exemplo que, em geral, não vale a igualdade.

d) $f(f^{-1}(f(A))) = f(A)$.

3.6 Sejam $f\colon X \to Y$ uma função e $V, W \subset Y$. Mostre que:

a) $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$.

b) $f^{-1}(V \cap W) = f^{-1}(V) \cap f^{-1}(W)$.

c) $f^{-1}(V \setminus W) = f^{-1}(V) \setminus f^{-1}(W)$.

3.7 Sejam $f\colon X \to Y$ uma função, $A \subset X$ e $V \subset Y$. Mostre que vale: $A \subset f^{-1}(f(A))$ e $f(f^{-1}(V)) = V \cap f(X)$ (logo, $f(f^{-1}(V)) \subset V$).

3.8 Sejam $f\colon X \to Y$, $g\colon Y \to Z$, $A \subset X$ e $V \subset Z$. Mostre que:

a) $(g \circ f)(A) = g(f(A))$.

b) $(g \circ f)^{-1}(V) = f^{-1}(g^{-1}(V))$.

4 Funções inversas

4.1. Bijeções

Uma função $f\colon X \to Y$ será dita *injetora* se

$$\forall\, x_1, x_2 \in X, \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Pela formulação contrapositiva (cf. Seção 2.5, Apêndice A), isto equivale à seguinte implicação:

$$\forall\, x_1, x_2 \in X, \quad f(x_1) = f(x_2) \implies x_1 = x_2.$$

Uma função $f\colon X \to Y$ será dita *sobrejetora* se todo elemento de Y é imagem por f de algum elemento de X. Em outras palavras, f é sobrejetora se, para todo $y \in Y$, existir $x \in X$ tal que $y = f(x)$; ou, equivalentemente, se $f(X) = Y$.

Uma função é dita *bijetora* ou uma *bijeção* se ela e injetora e sobrejetora.

Exemplos

1. É bijetora a função

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto x + 1 \end{aligned}$$

2. A função

$$\begin{aligned} f\colon \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n^2 \end{aligned}$$

é injetora porém não sobrejetora.

3. Toda função $\mathrm{id}_X\colon X \to X$ é bijetora.

4. A função

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto 2 \end{aligned}$$

não é sobrejetora nem injetora.

4.2. Funções inversas

Dada uma função $f\colon X \to Y$, diremos que uma função $g\colon Y \to X$ é uma *inversa à esquerda* de f, se

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

Diremos que g é uma inversa à direita de f, se

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

Proposição 1.4.1. *Uma função é sobrejetora se, e somente se, ela admite inversa à direita.*

Demonstração Seja $f\colon X \to Y$ uma função sobrejetora. Então para cada y em Y é possível escolher pelo menos um x em X tal que $y = f(x)$; fixe um tal x para cada y. Defina $g\colon Y \to X$ tal que $g(y) = x$ (note que em geral tal função g não é unicamente determinada, ela o será se f é injetora). Segue-se então que, para todo $y \in Y$,

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

logo $f \circ g = \mathrm{id}_Y$ e, portanto, g é uma inversa à direita de f.

Reciprocamente, suponha que $f \circ g = \mathrm{id}_Y$ para alguma função $g\colon Y \to X$. Como id_Y é sobrejetora, segue-se que f é também sobrejetora. (Justifique, veja Problema 4.3, (b).) □

Proposição 1.4.2. *Uma função é injetora se, e somente se, ela admite uma inversa à esquerda.*

Demonstração Seja $f\colon X \to Y$ uma função injetora. Então cada $y \in f(X)$ determina um único x em X tal que $y = f(x)$. Defina $g\colon Y \to X$ como a seguir:

$$g(y) = \begin{cases} x & , \quad \text{se } y = f(x) \\ a & , \quad \text{se } y \notin f(X) \end{cases}$$

onde a é um elemento qualquer fixado de X. Note que em geral g não é unicamente determinada, ela o será se f for sobrejetora. Segue-se então que

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

para todo x em X. Logo, $g \circ f = id_X$ e, portanto, g é uma inversa à esquerda de f.

Suponha, reciprocamente, que existe $g\colon Y \to X$ tal que $g \circ f = id_X$. Como id_X é injetora, segue-se que f é injetora (veja Problema 4.2 (b)). □

Proposição 1.4.3. *Se uma função admite uma inversa à esquerda e uma inversa à direita, estas são iguais.*

Demonstração Sejam $g_1, g_2\colon Y \to X$ respectivamente uma inversa à direita e uma inversa à esquerda de uma função $f\colon X \to Y$. Segue-se que

$$g_1 = id_X \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ id_Y = g_2\,.$$

□

Uma função $g\colon Y \to X$ é dita *função inversa* de $f\colon X \to Y$ se ela for simultaneamente função inversa à direita e à esquerda de f. Decorre imediatamente da Proposição 1.4.3 que, se uma função admite função inversa, esta é única.

A proposição a seguir caracterizará as funções que admitem inversas.

Proposição 1.4.5. *Uma função admite função inversa se, e somente se, ela é bijetora.*

Demonstração Seja f uma função bijetora. Pelas Proposições 1.4.1 e 1.4.2, esta admite uma inversa à esquerda e uma inversa à direita. Logo, pela Proposição 1.4.3, estas são iguais, definindo uma função inversa para f. A recíproca também segue-se das Proposições 1.4.1 e 1.4.2. □

4.3. Conjuntos de funções

Dados dois conjuntos não vazios X e Y, podemos considerar o conjunto $\mathcal{F}(X, Y)$ de todas as funções de X em Y.

A composição de funções determina em $\mathcal{F}(X, X)$ uma operação que, segundo já vimos, é associativa.

Esta operação tem o elemento neutro id_X e não é comutativa, se X tem 2 ou mais elementos. De fato, sejam $a, b \in X$, com $a \neq b$, e definamos $f\colon X \to X$, tal que $f(x) = a,\ \forall x \in X$ e $g\colon X \to X$, tal que

$g(x) = b$, $\forall x \in X$. Agora observe que $f(g(a)) = a$ e $g(f(a)) = b$ e, portanto, $f \circ g \neq g \circ f$.

Em Matemática, frequentemente, o mesmo objeto vem apresentado de vários modos distintos. Por exemplo, quando $X = \{1, 2\}$ e $Y \neq \emptyset$, o conjunto $\mathcal{F}(X, Y)$ pode ser naturalmente identificado com o conjunto $Y^2 = Y \times Y$. De fato, para cada função $f\colon \{1, 2\} \to Y$, associamos o par $(f(1), f(2))$. Esta associação estabelece uma bijeção natural entre $\mathcal{F}(X, Y)$ e Y^2.

Problemas

4.1 Para quais valores de a, b e c, inteiros, a função $f\colon \mathbb{Z} \to \mathbb{Z}$, definida por $x \mapsto ax^2 + bx + c$, é bijetora?

4.2 Sejam $f\colon X \to Y$ e $g\colon Y \to Z$ funções. Demonstre que:

a) Se f e g são injetoras, então $g \circ f$ é injetora.

b) Se $g \circ f$ é injetora, então f é injetora.

c) Se $g \circ f$ é injetora e f é sobrejetora, então g é injetora.

4.3 Sejam $f\colon X \to Y$ e $g\colon Y \to Z$ funções. Demonstre que:

a) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora.

b) Se $g \circ f$ é sobrejetora, então g é sobrejetora.

c) Se $g \circ f$ é sobrejetora e g é injetora, então f é sobrejetora.

4.4 Sejam $f\colon X \to Y$ e $g\colon Y \to Z$ funções.

a) Mostre que se f e g são bijetoras, então $g \circ f$ é bijetora.

b) Construa um exemplo mostrando que a recíproca de (a) é falsa.

c) Mostre que se f é bijetora então f^{-1} é bijetora.

4.5 Seja $f\colon X \to Y$ uma função. Prove que f é sobrejetora se, e somente se, para todo conjunto Z e todo par de funções $g\colon Y \to Z$ e $h\colon Y \to Z$, $g \circ f = h \circ f$ implica $g = h$.

4.6 Seja $f\colon X \to Y$ uma função. Prove que f é sobrejetora se, e somente se, para todo conjunto Z e todo par de funções $g\colon Z \to X$ e $h\colon Z \to X$, $f \circ g = f \circ h$ implica $g = h$.

4.7 Seja dada uma função $f\colon X \to Y$. Mostre que:

a) f é sobrejetora se, e somente se, para todo $B \subset Y$, $f(f^{-1}(B)) = B$.

b) f é injetora se, e somente se, para todo $A \subset X$, $f^{-1}(f(A)) = A$.

4.8 Seja $f\colon X \to Y$ uma função. Mostre que f é injetora se, e somente se, para todo par de subconjuntos A e B de X, vale $f(A \setminus B) = f(A) \setminus f(B)$.

4.9 Seja $f\colon X \to Y$ uma função. Mostre que f é injetora se, e somente se, para todo par de subconjuntos A e B de X, vale $f(A \cap B) = f(A) \cap f(B)$.

4.10 Sejam $X = \{1, 2, 3\}$ e $Y \neq \emptyset$. Mostre que $\mathcal{F}(X, Y)$ identifica-se naturalmente com $Y^3 = Y \times Y \times Y$.

5 Relações binárias

Uma *relação binária* em um conjunto $X \neq \emptyset$ é uma sentença aberta xRy no conjunto $X \times X$.

São exemplos de relações binárias a igualdade $x = y$ entre elementos de um conjunto X e a relação de desigualdade $x \leq y$ em $\mathbb{Z}$.

Existem vários tipos de relações, sendo que as mais importantes são as duas que definiremos adiante.

5.1. Relações de equivalência

Uma relação binária xRy em um conjunto $X \neq \emptyset$ será chamada de *relação de equivalência*, se possuir as seguintes propriedades:

(i) Propriedade Reflexiva xRx é verdadeira para todo $x \in X$,

(ii) Propriedade Simétrica xRy é verdadeira se, e somente se, yRx é verdadeira,

(iii) Propriedade Transitiva Se xRy e yRz são verdadeiras, então xRz é verdadeira.

A noção de relação de equivalência é uma das noções mais fundamentais e importantes em toda a Matemática. Muitas vezes, uma relação de equivalência será denotada por $x \sim y$, ou por $x \equiv y$, ao invés de xRy. Em tal caso, designaremos a relação apenas por $\sim$ ou por $\equiv$.

Exemplos

1. A igualdade entre elementos de um conjunto qualquer X é uma relação de equivalência em X.

2. A relação de paralelismo entre retas no plano, considerando-se que uma reta é paralela a si mesma, é uma relação de equivalência no conjunto das retas do plano.

3. As relações de equipolência entre segmentos orientados no plano ou no espaço, são relações de equivalência nos conjuntos dos segmentos orientados no plano ou no espaço, respectivamente.

A relação de equipolência entre segmentos orientados é que permite definir a noção de vetor no plano ou no espaço.

4. Dada uma função $f\colon A \to B$, define-se uma relação de equivalência em A, associada a f, do seguinte modo:

$$x \sim y \iff f(x) = f(y).$$

Esta relação de equivalência é uma generalização da igualdade num conjunto X, onde a função $f\colon X \to X$ é a função identidade.

5. Um conjunto A será dito equipotente a um conjunto B, se existir uma bijeção entre A e B. É fácil verificar que a relação de equipotência é uma relação de equivalência.

A relação de equipotência é que permite definir a cadinalidade de um conjunto.

6. Em $\mathbb{R}$ define-se a seguinte relação de equivalência:

$$x \sim y \iff \exists\, n \in \mathbb{Z}, \text{ tal que } x - y = 2\pi n.$$

É esta relação de equivalência que permite definir a noção de ângulo.

As relações de equivalência são usadas quando se quer definir um novo ente matemático que possui uma determinada propriedade. O procedimento consiste em identificar entre si objetos que possuem tal propriedade. Isto é o que sugerem os Exemplos 3, 5 e 6.

Dada a relação de equivalência $\sim$ em um conjunto X, definimos a *classe de equivalência* de um elemento $a \in X$ como sendo o conjunto

$$[a] = \{x \in X;\ \ x \sim a\},$$

e o elemento a será chamado de representante da classe $[a]$.

Por exemplo, se a relação de equivalência é a igualdade entre os elementos de um conjunto X, temos que $[a] = \{a\}$, para todo $a \in X$. Se a relação é a de paralelismo entre retas do plano ou do espaço, então a classe de uma dada reta r consiste de todas as retas que lhe são paralelas, incluindo a própria. A classe $[r]$ pode servir para definir o que é uma direção no plano ou no espaço.

Uma outra notação comum, mas que não utilizaremos, para a classe de equivalência de um elemento a é a seguinte: $\bar{a}$.

Dada uma relação de equivalência $\sim$ em um conjunto X, o conjunto das classes de equivalência dos elementos de X é um subconjunto do conjunto das partes de X, chamado de conjunto quociente de X pela relação $\sim$ e será denotado por $X/\sim$.

Portanto, se X é o conjunto das retas no plano e $\sim$ é a relação de paralelismo, o conjunto $X/\sim$ representa o conjunto das direções no plano.

Proposição 1.5.1. *Dado um conjunto X e uma relação de equivalência $\sim$ em X, temos que*

i) $[a] = [b]$ *se, e somente se,* $a \sim b$.

ii) *Se* $[a] \cap [b] \neq \emptyset$, *então* $[a] = [b]$.

iii) *A união dos conjuntos* $[a]$, *para* a *variando em* X, *é* X.

Demonstração (i) Suponhamos que $[a] = [b]$. Como $a \in [a] = [b]$, segue-se que $a \sim b$. Por outro lado, se $a \sim b$, temos, pelas propriedades simétrica e transitiva, que $x \sim a$ se, e somente se, $x \sim b$, seguindo-se daí o resultado.
(ii) Supondo que $[a] \cap [b] \neq \emptyset$, segue-se que existe $c \in [a]$ e $c \in [b]$. Logo, $c \sim a$ e $c \sim b$, seguindo-se, das propriedades simétrica e transitiva, que $a \sim b$ e, portanto, pelo item anterior, $[a] = [b]$.
(iii) Chamando de Y a união de todos os conjuntos $[a]$, temos que $Y \subset X$. Por outro lado, dado $a \in X$, tem-se que $a \in [a] \subset Y$, mostrando que $X \subset Y$ e, portanto, $Y = X$. □

Uma *partição* de um conjunto A é uma coleção de subconjuntos A_i de A, indexados por um conjunto I qualquer, tal que $A_i \cap A_j = \emptyset$, se $i \neq j$; e a união de todos os A_i é o conjunto A. A Proposição 1.5.1 nos diz que $A/\sim$ é uma partição de A.

Reciprocamente, dada uma partição A_i, $i \in I$, de A, podemos definir uma relação de equivalência em A, como a seguir:

$$a \sim b \iff \exists\, i \in I, \text{ tal que } a, b \in A_i.$$

É imediato verificar, neste caso, que $A/\sim = \{A_i;\ \ i \in I\}$.

Dada uma relação de equivalência $\sim$ em um conjunto A, temos uma função sobrejetora natural definida do seguinte modo:

$$\begin{array}{rccc} \pi\colon & A & \longrightarrow & A/\sim, \\ & a & \mapsto & [a] \end{array}$$

chamada de aplicação canônica.

É imediato verificar que qualquer relação $\sim$ de equivalência em um conjunto A é induzida pela sua aplicação canônica, no sentido que

$$a \sim b \iff \pi(a) = \pi(b).$$

5.2. Relações de ordem

Outras relações binárias de grande importância em Matemática são as chamadas relações de ordem.

Uma relação binária aRb em um conjunto $A \neq \emptyset$ será dita uma relação de ordem, se possuir as seguintes propriedades:

(i) Propriedade Reflexiva aRa é verdadeira para todo $a \in A$,

(ii) Propriedade Antissimétrica Se aRb e bRa são verdadeiras, então $a = b$.

(iii) Propriedade Transitiva Se aRb e bRc são verdadeiras, então aRc é verdadeira.

Por exemplo, a relação menor ou igual $\leq$ é uma relação de ordem em $\mathbb{Z}$.

Outro exemplo é dado pela relação de inclusão $\subset$ no conjunto das partes de um conjunto $A \neq \emptyset$.

Uma relação de ordem R em um conjunto A é dita *relação de ordem total*, se para quaisquer $a, b \in A$ se tenha aRb ou bRa. Caso contrário, diremos que a *relação de ordem é parcial*.

Por exemplo, a relação $\leq$ em $\mathbb{Z}$ é total, enquanto a relação $\subset$ no conjunto das partes de um conjunto A, com mais de um elemento, é parcial.

Problemas

5.1 Mostre que as relações descritas nos Exemplos 4 e 6 da Seção 5.1 são efetivamente relações de equivalência. Mostre que, em particular, a relação binária em $\mathbb{Z}$ dada por $a \equiv b$ se, e somente se, $a^2 = b^2$ é uma relação de equivalência.

5.2 Mostre que em $\mathbb{Z}$ a relação $a \equiv b$, dada por $b - a$ é par, é uma relação de equivalência. Caracterize as classes de equivalência de 0, 1, 2 e 3. Quantas classes existem em $\mathbb{Z}$? Descreva-as.

6 Cantor, o gênio injustiçado

Depois dos Elementos de Euclides, de 300 AC, poucos matemáticos influenciaram tanto o modo de apresentar a matemática quanto Georg Cantor (1845-1918), com a criação da Teoria dos Conjuntos. Cantor, filho de dinamarqueses, nascido na Russia, mas que viveu na Alemanha desde os 11 anos de idade, ao estudar as séries trigonométricas deparou-se com certas questões sutis de Análise Matemática que o conduziram a criar a Teoria dos Conjuntos e de toda uma teoria sobre o infinito. Entretanto, ao fazê-lo não suspeitava que iria provocar uma polêmica tão grande a ponto de prejudicar a própria carreira e, no final da vida, a sua saúde mental. A turbulenta polêmica teve como protagonista central Leopold Kronecker (1823-1891), um dos mais influentes matemáticos da sua época. Kronecker, não antevendo o potencial inovador da teoria do infinito de Cantor, foi seu acirrado crítico alegando que não se tratava de matemática mas de pura metafísica. A teoria de Cantor, revolucionária à época, introduziu os números transfinitos, um novo conceito de infinito com toda uma hierarquia, estabelecendo para esses números uma aritmética própria. As idéias de Cantor permitiram, entre outras coisas, mostrar que os números reais algébricos, isto é, os números reais que são raízes de polinômios em uma variável e coeficientes inteiros, são tão numerosos quanto os números racionais. Permitiram também mostrar que os números reais que não são algébricos, os chamados números transcendentes, são mais numerosos do que os números racionais, sem no entanto exibir um único número transcendente novo. Era esse tipo de argumento existencial que Kronecker criticava, pois acreditava que a prova da existência de um ente matemático deveria se basear em um algoritmo finito que permitisse a sua construção. Em consequência dessa polêmica, Kronecker nunca permitiu que Cantor conseguisse o posto que almejava, uma posição de professor em Berlim, onde ele próprio lecionava. Cantor teve que contentar-se com uma posição bem menos importante na Universidade de Halle e, talvez em consequência de toda essa história, passou os últimos anos de sua vida internado em um hospital de doenças mentais. A discussão levantada por Kronecker continuou acalorada entre a geração seguinte. Por um lado, na trilha de Kronecker, formou-se a escola intuicionista cujos expoentes foram H. Poincaré, L. E. J. Brouwer e H. Weyl que, levando o construtivismo ao extremo, não aceitavam tampouco as provas por redução ao absurdo. No ou-

tro extremo, a escola formalista liderada por David Hilbert (1862-1943) achava que de nada valia uma prova construtiva da existência de um objeto matemático se o algoritmo que o determinava não podia ser executado em tempo razoável devido à sua complexidade computacional. A matemática criada nos três primeiros quartos do Século 20 foi marcada pela influência de Hilbert que, em dada ocasião, chegou a afirmar que ninguem nos expulsaria do paraíso criado por Cantor. A patir do último quarto do Século 20, devido ao desenvolvimento dos computadores e da sofisticação dos programas computacionais, o nosso poder de cálculo aumentou drasticamente de modo que foi natural voltar a dar-se grande importância às provas construtivas, revivendo os ideais de Kronecker e de seus seguidores.

2

Os inteiros e racionais

Os números foram considerados durante milênios como entes intuitivos e algumas de suas propriedades, como, por exemplo, a comutatividade e a associatividade da adição e da multiplicação, eram consideradas inerentes à sua própria natureza e, portanto, não necessitando de demonstração.

O grande desenvolvimento da matemática a partir da criação do Cálculo Diferencial, no século dezessete, colocou diante dos matemáticos novos problemas que, para serem melhor compreendidos e solucionados, requeriam uma fundamentação mais rigorosa do conceito de número. Esta tarefa foi empreendida pelos matemáticos do século dezenove.

O primeiro a idealizar um método para a construção dos números inteiros negativos e dos números racionais a partir dos números naturais foi Karl Weierstrass. Bem mais sutil e profunda é a construção dos números irracionais, cuja descoberta de sua existência remonta à Grécia antiga, a partir dos números racionais. Isto foi conseguido independentemente por Georg Cantor e Richard Dedekind por volta de 1870.

Os números naturais ainda resistiram às investidas por algum tempo. Segundo vários matemáticos da época não seria possível construir tais números. Ficou célebre a seguinte frase de Leopold Kronecker a tal propósito: "Deus criou os inteiros, todo o resto é obra do homem". O grande capítulo da construção dos números ficou encerrado quando em 1888 Dedekind publicou um trabalho onde, a partir de noções básicas da teoria dos conjuntos, ele elabora um modelo para os números naturais,

definindo as operações de adição e multiplicação e demonstrando as suas propriedades básicas. A construção de Dedekind não teve muita difusão na época por ser bastante complicada. Ficou, entretanto, mais popular a axiomática que Giuseppe Peano deu em 1889. Trata-se de um conjunto de quatro axiomas que caracterizam totalmente os números naturais.

Não realizaremos toda a construção acima referida. Iniciaremos neste capítulo o estudo dos inteiros para os quais daremos um tratamento axiomático, tendo como ponto de partida uma lista de propriedades básicas que os caracterizarão completamente, para delas deduzir as demais propriedades. Em seguida, construiremos o conjunto dos números racionais a partir dos inteiros. Esta construção será feita no contexto mais geral dos domínios de integridade pois não irá requerer nenhum esforço adicional e evitará que no futuro tenhamos que repetí-la em outras situações análogas. Finalmente, a construção dos números reais será realizada no Capítulo 8.

1 Os inteiros

O conjunto $\mathbb{Z}$ dos números inteiros é munido de duas operações, uma adição $(+)$ e uma multiplicação $(\cdot)$, além de uma relação de ordem $(\leq)$. Estes objetos se relacionam através de várias propriedades que listaremos ao longo das três próximas subseções. Esta lista de propriedades caracterizará completamente os números inteiros de um modo que será precisado no Teorema 3.1.14.

1.1. Anéis

Sejam A um conjunto e $(+)$ e $(\cdot)$ duas operações em A, chamadas de adição e multiplicação. A terna $(A, +, \cdot)$ será chamada de *anel* se as operações gozarem das propriedades enunciadas a seguir.

A_1) A adição é associativa *Quaisquer que sejam* $a, b, c \in A$*, tem-se que* $(a + b) + c = a + (b + c)$.

A_2) A adição é comutativa *Quaisquer que sejam* $a, b \in A$*, tem-se que* $a + b = b + a$.

A_3) Existe um elemento neutro para a adição *Existe* $\alpha \in A$ *tal que* $\alpha + x = x$*, para todo* $x \in A$.

A_4) Todo elemento de A possui um simétrico *Para todo* $a \in A$*, existe* $a' \in A$ *tal que* $a + a' = \alpha$.

M_1) A multiplicação é associativa *Quaisquer que sejam* a, b, c *em* A*, tem-se que* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M_2) A multiplicação é comutativa *Quaisquer que sejam* $a, b \in A$*, tem-se que* $a \cdot b = b \cdot a$.

M_3) Existe um elemento neutro para a multiplicação *Existe* $e \in A$*, com* $e \neq \alpha$*, tal que* $x \cdot e = x$*, para todo* $x \in A$.

AM) A multiplicação é distributiva com relação à adição *Quaisquer que sejam* $a, b, c \in A$*, tem-se que*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Observações

1. O elemento neutro da adição é único. De fato, sejam α e α' elementos neutros para a adição. Como α' é neutro, temos que

$$\alpha = \alpha' + \alpha,$$

e como α é neutro, temos que

$$\alpha' = \alpha + \alpha'.$$

Por A_2, temos então que $\alpha = \alpha'$.

Usaremos o símbolo 0 para denotar o único elemento neutro da adição, que será chamado de *elemento zero*, ou de *elemento nulo*.

2. O elemento neutro da multiplicação é único. De fato, a demonstração acima, devidamente adaptada, nos fornece o resultado. Usaremos o símbolo 1 para denotar o único elemento neutro da multiplicação, que será chamado de *unidade*, ou apenas *um*.

3. O simétrico de um elemento $a \in A$ é único. De fato, se a' e a'' são dois simétricos de a, então, por A_2 e A_1, temos que

$$a'' = 0 + a'' = (a' + a) + a'' = a' + (a + a'') = a' + 0 = a'.$$

Este (único) simétrico de a será simbolizado por $-a$. Note que o simétrico de $-a$ é a.

Usaremos a notação $a - b$ para representar $a + (-b)$. Esta operação em A é chamada de *subtração*.

Um elemento $a \in A$ será dito *invertível*, se existir um elemento $b \in A$ tal que $a \cdot b = 1$. Um tal elemento b será chamado de *inverso* de a.

Note que a mesma prova da Observação 3, acima, mostra que o inverso de um elemento a, se existir, é único.

No caso em que a é invertível, o seu (único) inverso será denotado por a^{-1}.

Denotaremos por A^* o conjunto dos elementos invertíveis de um anel A. Note que se $x, y \in A^*$, então $x \cdot y \in A^*$ (veja Problema 1.3), isto é, A^* é fechado com respeito à multiplicação de A. Note também que $1 \in A^*$ e que se $x \in A^*$, então $x^{-1} \in A^*$ (pois decorre da definição que o inverso de x^{-1} é o próprio x).

Um anel A será chamado de *domínio de integridade*, ou simplesmente de *domínio* se for verificada a seguinte propriedade:

M_4) Integridade *Dados* $a, b \in A$*, se* $a \neq 0$ *e* $b \neq 0$*, então* $a \cdot b \neq 0$.

A propriedade, acima, é obviamente equivalente à seguinte propriedade, que é a sua contrapositiva:

M_4') *Dados* $a, b \in A$*, se* $a \cdot b = 0$*, então* $a = 0$ *ou* $b = 0$.

O seguinte axioma caracteriza parcialmente o conjunto dos inteiros e será complementado nas próximas duas subseções.

Axioma 1 (parcial). $(\mathbb{Z}, +, \cdot)$ *é um domínio de integridade.*

A seguir, enunciaremos e demonstraremos algumas propriedades dos anéis que decorrem das definições. A seguir, A designará um anel.

Proposição 2.1.1. *Para todo* $a \in A$*, temos que* $a \cdot 0 = 0$.

Demonstração Utilizando AM segue-se que

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Somando membro a membro $-(a \cdot 0)$ (que existe por A_4) na igualdade

$$a \cdot 0 = a \cdot 0 + a \cdot 0,$$

segue-se que

$$-(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0).$$

Por A_1 e A_2, temos que

$$0 = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.$$

Logo, $a \cdot 0 = 0$. □

Num anel A o elemento zero nunca é invertível, pois, se fosse, existiria $b \in A$ tal que $0 \cdot b = 1$. Logo, pela Proposição 2.1.1, teríamos $0 = 1$, o que é uma contradição pois, por definição, temos $1 \neq 0$.

Um anel A tal que todo elemento não nulo (i.e., diferente de zero) é invertível é chamado de *corpo*. Verifica-se facilmente que todo corpo é domínio de integridade (veja Problema 1.4).

Proposição 2.1.2. *Para todo* $a \in A$*, temos que* $(-1) \cdot a = -a$.

Demonstração Por M_3, AM, A_4 e pela Proposição 2.1.1, temos que

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0.$$

Somando $(-a)$ a ambos os membros da igualdade $(-1) \cdot a + a = 0$ e usando A_1, A_4 e A_3, obtemos o resultado. □

Usando a Proposição 2.1.2, M_1 e M_3 é fácil mostrar que

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

Das igualdades, acima, segue-se a distributividade da multiplicação com relação à subtração, isto é, para todos $a, b, c \in A$, temos que

$$a \cdot (b - c) = a \cdot b - a \cdot c.$$

Proposição 2.1.3 (Lei do Cancelamento). *Seja* A *um domínio de integridade. Para todos* $a, x, y \in A$*, com* $a \neq 0$*, se* $a \cdot x = a \cdot y$*, então* $x = y$.

Demonstração Somando $-(a \cdot x)$ a ambos os lados da igualdade $a \cdot x = a \cdot y$, e usando a observação após a Proposição 2.1.2 e AM, segue-se que

$$0 = a \cdot (y - x).$$

Como $a \neq 0$, por M_4', segue-se que $y - x = 0$ e, consequentemente, $x = y$. □

1.2. Anéis ordenados

Um anel A será chamado de *anel ordenado* se existir uma relação de ordem total $\leq$ em A que possui as seguintes propriedades adicionais:

OA) Compatibilidade com a adição *Para todos* a, b, c *em* A*, se* $a \leq b$*, então* $a + c \leq b + c$.

OM) Compatibilidade com a multiplicação *Para todos* a, b, c *em* A*, se* $a \leq b$ *e* $0 \leq c$*, então* $a \cdot c \leq b \cdot c$.

Quando $a \leq b$, diremos que a *menor do que ou igual* a b, ou abreviadamente, a é menor ou igual a b. Usaremos a notação $a < b$, que se lê a é *menor do que* b, para indicar que $a \leq b$ com $a \neq b$. Note que se $a < b$, então $a \leq b$. Usaremos também as notações $b > a$, que se lê b é *maior do que* a, e $b \geq a$, que se lê b é *maior do que ou igual a* a, significando $a < b$ e $a \leq b$, respectivamente.

Daremos, a seguir, mais um passo na axiomatização do conjunto $\mathbb{Z}$ dos inteiros, complementando o Axioma 1.

Axioma 2 (parcial). $(\mathbb{Z}, +, \cdot, \leq)$ *é um domínio ordenado.*

Num anel ordenado define-se o *valor absoluto* de um elemento $a \in A$ como sendo,

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

Decorre imediatamente desta definição que $|a| \geq 0$, para todo $a \in A$, valendo a igualdade se, e somente se, $a = 0$.

Proposição 2.1.4. *Se* A *é um anel ordenado e* $a, b, r \in A$*, então:*

i) $|a \cdot b| = |a| \cdot |b|$;

ii) $-|a| \leq a \leq |a|$;

iii) $|a| \leq r$ *se, e somente se,* $-r \leq a \leq r$;

iv) $|a + b| \leq |a| + |b|$.

Demonstração (i) Se $a \geq 0$ e $b \geq 0$, então de OM segue-se que $a \cdot b \geq 0$ e a igualdade decorre imediatamente da definição. Se $a \geq 0$ e $b \leq 0$, então $a \cdot b \leq 0$ (veja Problema 1.8 (c)) e neste caso temos, da observação após a Proposição 2.1.2, que

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

Os casos $a \leq 0$, $b \geq 0$ e $a \leq 0$, $b \leq 0$ são tratados de modo semelhante.
(ii) Decorre imediatamente da definição.
(iii) Suponha que $|a| \leq r$. Segue-se então que $-|a| \geq -r$ (veja Problema 1.6 (c)). Logo, de (ii), temos que

$$-r \leq -|a| \leq a \leq |a| \leq r.$$

Reciprocamente, suponha que $-r \leq a \leq r$. Se $a \geq 0$, então $|a| = a \leq r$. Se $a < 0$, então $|a| = -a \leq r$ (a última desigualdade pode ser obtida somando a ambos os membros de $-r \leq a$ o elemento $r - a$).
(iv) Somando membro a membro as desigualdades

$$-|a| \leq a \leq |a| \quad \text{e} \quad -|b| \leq b \leq |b|,$$

obtemos (veja Problemas 1.6 (b) e 1.1 (c))

$$-(|a| + |b|) \leq a + b \leq |a| + |b|,$$

logo de (iii) decorre que $|a + b| \leq |a| + |b|$. □

Corolário 2.1.5. *Sejam* A *um anel ordenado e* $a, b \in A$. *Temos que*

$$||a| - |b|| \leq |a \pm b| \leq |a| + |b|.$$

Demonstração A desigualdade $|a + b| \leq |a| + |b|$ foi provada na proposição. Novamente, pela proposição, temos

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

Temos também,

$$|a| = |a + b - b| \leq |a + b| + |-b| = |a + b| + |b|,$$

logo,

$$|a| - |b| \leq |a + b|.$$

Por outro lado,

$$|b| = |b + a - a| \leq |b + a| + |-a| = |a + b| + |a|,$$

logo,

$$-|a + b| \leq |a| - |b|.$$

Portanto,

$$-|a + b| \leq |a| - |b| \leq |a + b|,$$

e, consequentemente, pelo item (iii) da proposição, temos que

$$||a| - |b|| \leq |a + b|.$$

A desigualdade $|a - b| \geq ||a| - |b||$ decorre facilmente da desigualdade acima. □

1.3. Anéis bem ordenados

Um subconjunto S de um anel ordenado A será dito *limitado inferiormente* (respectivamente, *superiormente*), se existir um elemento $a \in A$ tal que para todo $x \in S$ se tenha $x \geq a$ (respectivamente, $x \leq a$). O conjunto vazio é considreado limitado inferiormente e superiormente.

Diremos que S tem um *menor elemento* (respectivamente, *maior elemento*), se existir $b \in S$ tal que para todo $x \in S$ se tenha $x \geq b$ (respectivamente, $x \leq b$). Se existir um menor elemento de um subonjunto S de um anel ordenado A, ele é único. De fato, se b e b' são menores elementos de S, temos que $b \leq b'$ e $b' \leq b$. Logo, pela antissimetria da relação de ordem $\leq$, segue-se que $b = b'$. No caso em que existe o menor elemento de S, ele é denotado por $\min S$. A mesma observação vale para o maior elemento que será denotado por $\max S$.

Um domínio ordenado A será chamado de *domínio bem ordenado*, se gozar da seguinte propriedade:

PBO) Princípio da Boa Ordenação *Todo subconjunto não vazio de A e limitado inferiormente possui um menor elemento.*

A propriedade acima é equivalente à seguinte propriedade:

PBO′) *Todo subconjunto não vazio de A e limitado superiormente possui um maior elemento.*

De fato, isto decorre das seguintes observações fáceis de verificar. Seja $\emptyset \neq S \subset A$, defina $S' = \{-b\,;\ b \in S\}$. Então S é limitado inferiormente se, e somente se, S' é limitado superiormente. Tem-se também que S possui um menor elemento se, e somente se, S' possui um maior elemento (neste caso tem-se que $\min S = -\max S'$).

Daremos a seguir a axiomática completa para os números inteiros.

Axioma dos números inteiros. $(\mathbb{Z}, +, \cdot, \leq)$ *é um domínio bem ordenado.*

Demonstraremos no Capítulo 3 que existe essencialmente um único domínio bem ordenado (num sentido que precisaremos na próxima subseção).

A seguir, daremos alguns resultados característicos dos domínios bem ordenados.

Proposição 2.1.6. *Sejam* A *um domínio bem ordenado e* $a \in A$. *Se* $a > 0$, *então* $a \geq 1$.

Demonstração Suponha por absurdo que exista $a \in A$ tal que $0 < a < 1$, logo o conjunto

$$S = \{x \in A\,;\ 0 < x < 1\}$$

é não vazio e limitado inferiormente. Portanto, S possui um menor elemento b tal que $0 < b < 1$. Segue-se então que $0 < b^2 < b < 1$ e, consequentemente, $b^2 \in S$ e $b^2 < b$; absurdo. □

Corolário 2.1.7. *Sejam* A *um domínio bem ordenado e* $a, b \in A$. *Se* $a > b$, *então* $a \geq b + 1$.

Demonstração Aplique a proposição com $a - b$ no lugar de a. □

Corolário 2.1.8. *Sejam* A *um domínio bem ordenado e* $a, b \in A$, *com* $b \neq 0$. *Então* $|a \cdot b| \geq |a|$.

Demonstração Como $b \neq 0$, pela Proposição 2.1.6, temos que $|b| \geq 1$. Multiplicando ambos os membros desta desigualdade por $|a|$, segue-se, da Proposição 2.1.4 (i), que

$$|a \cdot b| = |a| \cdot |b| \geq |a|.$$

□

Proposição 2.1.9. *Seja* A *um domínio bem ordenado e* $a, b \in A$. *Se* $a \cdot b = 1$, *então* $a = b = 1$. *ou* $a = b = -1$.

Demonstração Se $a \cdot b = 1$, segue-se, da Proposição 2.1.1, que $a \neq 0$ e $b \neq 0$. Logo, pelo Corolário 2.1.8, acima, e do fato de $1 > 0$ (veja Problema 1.9 (b)), temos que $1 = |a \cdot b| \geq |a|$ e $1 = |a \cdot b| \geq |b|$. Como $|a| > 0$ e $|b| > 0$, segue-se, da Proposição 2.1.6, que $|a| = |b| = 1$ e, portanto, $a = \pm 1$ e $b = \pm 1$. Da hipótese, $a \cdot b = 1$, segue-se que $a = b = 1$ ou $a = b = -1$. □

A proposição acima mostra que os únicos elementos invertíveis de um domínio bem ordenado são 1 e -1.

Proposição 2.1.10 (Propriedade Arquimediana). *Dados elementos* a *e* b *de um domínio bem ordenado* A, *com* $b \neq 0$, *existe um elemento* $n \in A$ *tal que* $n \cdot b \geq a$.

Demonstração Como $b \neq 0$, temos, pela Proposição 2.1.4 (i) e pelo Corolário 2.1.8, que

$$|b| \cdot |a| = |b \cdot a| \geq |a| \geq a.$$

Se $b > 0$, tome $n = |a|$, e o resultado decorre da desigualdade acima. Se $b < 0$, tome $n = -|a|$, e o resultado também decorre da desigualdade acima. □

1.4. Homomorfismos

As funções naturais no âmbito dos anéis são aquelas que preservam as operações. Tais funções serão chamadas de homomorfismos. Precisamente, dados dois anéis A e B, uma função $f\colon A \to B$ será chamada de *homomorfismo*, se valerem, para todos os elementos a e b de A, as igualdades:

1) $f(a + b) = f(a) + f(b)$,
2) $f(a \cdot b) = f(a) \cdot f(b)$,
3) $f(1) = 1$.

Note que as operações nos primeiros membros das igualdades acima são efetuadas em A, enquanto que as dos segundos membros são efetuadas em B.

Um homomorfismo bijetor será chamado de *isomorfismo.* É fácil verificar que a função inversa de um isomorfismo é um homomorfismo (veja Proposição 2.1.11 (iv), abaixo). Dois anéis que admitem entre si um isomorfismo são ditos *isomorfos* e, no que diz respeito à estrutura de anel, eles são considerados iguais. Quando existir um isomorfismo entre dois anéis A e B escreveremos $A \simeq B$.

Se A e B são anéis ordenados e $f\colon A \to B$ é um homomorfismo tal que se $a \leq b$, então $f(a) \leq f(b)$, diremos que f é um *homomorfismo de anéis ordenados.* Se o homomorfismo de anéis ordenados $f\colon A \to B$ for um isomorfismo, diremos que A e B são *isomorfos como anéis ordenados.* Provaremos no Capítulo 3 (Teorema 3.1.14) que dois domínios bem ordenados, quaisquer, são sempre isomorfos como anéis ordenados.

Um subconjunto A' de um anel A será chamado de *subanel* de A se A', juntamente com as restrições a ele das operações de adição e de multiplicação de A, é um anel cujo elemento unidade é o elemento unidade de A.

Para provar que um subconjunto A' de A é um subanel de A é preciso verificar que 0 e 1 são elementos de A', que a soma e o produto de dois elementos quaisquer de A' estão em A' e que o simétrico de todo elemento de A' está em A'. As demais propriedades de um anel são automaticamente satisfeitas para os elementos de A' pois o são para os elementos de A.

Proposição 2.1.11. *Se* $f\colon A \to B$ *é um homomorfismo de anéis, então:*

i) $f(0) = 0$.

ii) *Quaisquer que sejam* $a, b \in A$*, temos que* $f(a - b) = f(a) - f(b)$.
Em particular, $f(-a) = -f(a)$.

iii) $f(A)$ *é um subanel de* B.

iv) *Se* f *é bijetora, então* $f^{-1}\colon B \to A$ *é um homomorfismo de anéis.*

Demonstração (i) Note que

$$f(0) = f(0 + 0) = f(0) + f(0).$$

Logo, somando $-f(0)$ a ambos os lados da igualdade acima, temos que $f(0) = 0$.
(ii) Observe inicialmente que

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a),$$

logo $f(-a) = -f(a)$. Agora,

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b).$$

(iii) De (i) temos que $0 \in f(A)$ e da definição, $1 = f(1) \in f(A)$. Que somas e produtos de elementos de $f(A)$ estão em $f(A)$, seguem-se das condições (1) e (2) da definição de homomorfismo. Que o simétrico de um elemento de $f(A)$ está em $f(A)$, decorre de (ii).
(iv) Suponha f bijetora e sejam $y, y' \in B$. Logo, existem $x, x' \in A$, univocamente determinados, tais que $f(x) = y$ e $f(x') = y'$. Temos então que

$$\begin{aligned} f^{-1}(y + y') = \quad & f^{-1}(f(x) + f(x')) = \quad f^{-1}(f(x + x')) = \\ & x + x' = \quad f^{-1}(y) + f^{-1}(y'). \end{aligned}$$

Temos também que

$$\begin{aligned} f^{-1}(y \cdot y') = \quad & f^{-1}(f(x) \cdot f(x')) = \quad f^{-1}(f(x \cdot x')) = \\ & x \cdot x' = \quad f^{-1}(y) \cdot f^{-1}(y'). \end{aligned}$$

Finalmente, é claro que $f^{-1}(1) = 1$. □

Proposição 2.1.12. *Sejam* $f\colon A \to B$ *e* $g\colon B \to C$ *homomorfismos de anéis. Então,* $g \circ f\colon A \to C$ *é um homomorfismo de anéis. Se* f *e* g *são isomorfismos, então* $g \circ f$ *é um isomorfismo.*

Demonstração A prova deste resultado não contém nenhuma dificuldade e a deixamos como exercício. □

Problemas

1.1 Mostre que num anel valem as seguintes propriedades:

a) Se $a + c = b + c$, então $a = b$.

b) Se $a + b = a$, para algum a, então $b = 0$.

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

d) -1 é invertível.

1.2 Mostre que num domínio de integridade valem as seguintes propriedades:

a) $a^2 = 0$ se, e somente se, $a = 0$.

b) $a \cdot b = a$ se, e somente se, $a = 0$ ou $b = 1$.

c) $a^2 = a$ se, e somente se, $a = 0$ ou $a = 1$.

1.3 Mostre que a e b são invertíveis se, e somente se, $a \cdot b$ é invertível. Mostre que, neste caso, tem-se $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

1.4 Mostre que todo corpo é domínio de integridade.

1.5 Sejam A um anel e $a \in A \setminus \{0\}$. Defina a função $f_a\colon A \to A$ pela lei $f_a(x) = a \cdot x$.

a) Mostre que f_a é sobrejetora se, e somente se, a é invertível.

b) Mostre que se A é um domínio, então f_a é injetora.

1.6 Mostre que num anel ordenado valem as seguintes propriedades:

a) Se $a + c \leq b + c$, então $a \leq b$.

b) Se $a \leq b$ e $c \leq d$, então $a + c \leq b + d$.

c) Se $a \leq b$ e $c \leq 0$, então $a \cdot c \geq b \cdot c$.

1.7 Mostre que num anel ordenado vale o seguinte:

a) Se $a < b$ e $b < c$, então $a < c$.

b) Se $a < b$ e $b \leq c$, então $a < c$.

c) Se $a < b$, então $a + c < b + c$ para todo c.

1.8 Mostre que num anel ordenado vale o seguinte:

a) Se $a \geq 0$, então $-a \leq 0$.

b) Se $a \leq 0$, então $-a \geq 0$.

c) Se $a \geq 0$ e $b \leq 0$, então $a \cdot b \leq 0$.

d) Se $a \leq 0$ e $b \leq 0$, então $a \cdot b \geq 0$.

1.9 Mostre que num anel ordenado vale o seguinte:

a) Para todo a, tem-se que $a^2 \geq 0$.

b) $1 > 0$.

c) $-1 < 0$.

1.10 Mostre que num domínio ordenado se $a < b$ e $c > 0$, então $a \cdot c < b \cdot c$.

1.11 Mostre que num domínio ordenado vale o seguinte:

a) Se $a \cdot c \leq b \cdot c$ e $c > 0$, então $a \leq b$.

b) Se $a \cdot c \leq b \cdot c$ e $c < 0$, então $a \geq b$.

1.12 Seja $f\colon A \to B$ um homomorfismo de anéis. Mostre que se $a \in A$ é invertível, então $f(a)$ é invertível e $(f(a))^{-1} = f(a^{-1})$.

2 Os racionais

O que é um número racional? Usualmente define-se um número racional como sendo uma fração $\frac{a}{b}$ com a e b números inteiros e $b \neq 0$.

Mas o que é uma fração? O essencial numa fração $\frac{a}{b}$ é o par ordenado (a, b) e a relação de igualdade:

$$\frac{a}{b} = \frac{a'}{b'} \iff a \cdot b' = a' \cdot b.$$

Isto é o ponto inicial para construir o corpo dos números racionais a partir do anel dos inteiros. Como esta construção pode ser feita sem

custo adicional no contexto mais geral dos domínios de integridade, assim o faremos, pois isso evitará que tenhamos de repetí-la em outras situações análogas.

Em particular, quando a nossa constução for aplicada ao domínio $\mathbb{Z}$, obteremos o corpo dos números racionais.

2.1. Corpo de frações de um domínio de integridade

Seja A um domínio de integridade. Considere o seguinte conjunto:

$$B = \{(a, b) \in A \times A\,;\ b \neq 0\}.$$

Defina em B a seguinte relação de equivalência:

$$(a, b) \sim (a', b') \iff a \cdot b' = a' \cdot b.$$

De fato, a reflexividade e a simetria dessa relação são de verificação imediata. A transitividade será provada a seguir.

Se $(a, b) \sim (a', b')$ e $(a', b') \sim (a'', b'')$, então $a \cdot b' = a' \cdot b$ e $a' \cdot b'' = a'' \cdot b'$. Multiplicando a primeira igualdade por b'' e a segunda por b, segue-se que

$$a \cdot b' \cdot b'' = a' \cdot b \cdot b'' = a'' \cdot b' \cdot b,$$

logo

$$(a \cdot b'' - a'' \cdot b) \cdot b' = 0.$$

Como A é um domínio de integridade e $b' \neq 0$, segue-se que

$$a \cdot b'' - a'' \cdot b = 0$$

e, consequentemente, $(a, b) \sim (a'', b'')$.

A *classe de equivalência* de um elemento (a, b) de B, isto é, o conjunto $\{(x, y) \in B\,;\ (x, y) \sim (a, b)\}$, será denotada por $\frac{a}{b}$.

Denotaremos por K o conjunto $B/\sim$ de todas as classes de equivalência de elementos de B:

$$K = \left\{ \frac{a}{b}\,;\ \ a, b \in A \text{ com } b \neq 0 \right\}.$$

Portanto,

$$\frac{a}{b} = \frac{c}{d} \iff (a, b) \sim (c, d) \iff a \cdot d = b \cdot c.$$

Definimos em K as seguintes operações:

Adição: $$\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+c\cdot b}{b\cdot d}$$

Multiplicação: $$\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}\,.$$

Antes de mais nada, é preciso verificar que estas leis efetivamente definem duas operações. Para isto, é necessário mostrarmos que os resultados, além de pertencerem a K, independem dos particulares elementos (a,b) e (c,d) de B utilizados para representar as classes de equivalência $\frac{a}{b}$ e $\frac{c}{d}$.

De fato, sendo A um domínio de integridade e como $b\neq 0$ e $d\neq 0$, segue-se que $b\cdot d\neq 0$, logo os resultados da adição e da multiplicação pertencem a K. Por outro lado, se

$$\frac{a}{b}=\frac{a'}{b'}\quad\text{e}\quad\frac{c}{d}=\frac{c'}{d'},$$

não é difícil verificar (faça-o) que $(ad+bc,bd)\sim(a'd'+b'c',b'd')$ e que $(ac,bd)\sim(a'c',b'd')$, provando assim as igualdades:

$$\frac{a\cdot d+b\cdot c}{b\cdot d}=\frac{a'\cdot d'+b'\cdot c'}{b'\cdot d'}\quad\text{e}\quad\frac{a\cdot c}{b\cdot d}=\frac{a'\cdot c'}{b'\cdot d'}\,.$$

Isto mostra que os resultados dessas operações independem dos particulares representantes de $\frac{a}{b}$ e $\frac{c}{d}$.

Teorema 2.2.1. *Com as operações acima definidas,* K *é um corpo.*

Demonstração Levando em conta que o elemento zero em K é $\frac{0}{1}$, que o simétrico de $\frac{a}{b}$ é $\frac{-a}{b}$ e que a unidade é $\frac{1}{1}$, a demonstração de que K é um anel é só uma série de verificações diretas que deixamos a cargo do leitor.

Para provar que K é um corpo, seja $\frac{a}{b}$ um elemento não nulo de K. Sendo $b\neq 0$ e sendo a não nulo, por ser $\frac{a}{b}$ não nulo, temos que $\frac{b}{a}\in K$ e

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{a\cdot b}{b\cdot a}=\frac{1}{1}.$$

Portanto, $\frac{a}{b}$ é invertível e $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. □

O corpo K é chamado de *corpo de frações* de A. O corpo de frações de $\mathbb{Z}$ é, por definição, o *corpo dos números racionais* $\mathbb{Q}$.

Considere a função

$$\begin{aligned} j\colon A &\longrightarrow K\,. \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

Esta função é um homomorfismo injetor de anéis (verifique). Portanto, temos um isomorfismo de A com o subanel $j(A)$ de K. Identificaremos o elemento a de A com $j(a) = \frac{a}{1} \in K$, que passa a ser denotado simplesmente por a.

Proposição 2.2.2. *Seja A um domínio com corpo de frações K. Se K' é um corpo e $f\colon A \to K'$ é um homomorfismo injetor de anéis, então existe um único homomorfismo de anéis $\tilde{f}\colon K \to K'$ tal que $\tilde{f} \circ j = f$.*

Demonstração Para se ter uma idéia de como definir $\tilde{f}$, vamos, por um momento, supor que exista tal homomorfismo satisfazendo à condição $\tilde{f} \circ j = f$. Teríamos, portanto, para $\frac{a}{b} \in K$,

$$\tilde{f}\left(\frac{a}{b}\right) = \tilde{f}\left(\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}\right) = \tilde{f}\left(\frac{a}{1}\right) \cdot \tilde{f}\left(\left(\frac{b}{1}\right)^{-1}\right) = \tilde{f}\left(\frac{a}{1}\right)\left(\tilde{f}\left(\frac{b}{1}\right)\right)^{-1}$$

$$= f(a) \cdot (f(b))^{-1},$$

onde a igualdade

$$\tilde{f}\left(\left(\frac{b}{1}\right)^{-1}\right) = \left(\tilde{f}\left(\frac{b}{1}\right)\right)^{-1}$$

decorre do Problema 1.12.

Isto toma conta da unicidade de $\tilde{f}$. Agora, basta mostrar que a aplicação

$$\begin{aligned} \tilde{f}\colon K &\longrightarrow K' \\ \frac{a}{b} &\longmapsto f(a)(f(b))^{-1} \end{aligned}$$

é efetivamente um homomorfismo de anéis.

De fato, a função $\tilde{f}$ é bem definida pois, como f é injetora tem-se que se $b \neq 0$, então $f(b) \neq 0$ e, portanto, $f(a)(f(b))^{-1}$ está bem definido como elemento de K'.

Para mostrar que a expressão $f(a)(f(b))^{-1}$ independe dos representantes de $\frac{a}{b}$, suponha que $\frac{a}{b} = \frac{a'}{b'}$. Então, $a'b = b'a$ e, portanto,

$$f(a')f(b) = f(a'b) = f(b'a) = f(b')f(a).$$

Consequentemente,

$$f(a')(f(b'))^{-1} = f(a)(f(b))^{-1}.$$

Por outro lado, temos que

$$\begin{aligned} f\left(\frac{a}{b} + \frac{a'}{b'}\right) = f\left(\frac{ab' + a'b}{bb'}\right) = f(ab' + a'b)(f(bb'))^{-1} = \\ [f(a)f(b') + f(a')f(b)](f(b))^{-1}(f(b'))^{-1} = \\ f(a)(f(b))^{-1} + f(a')(f(b'))^{-1} = \\ \tilde{f}\left(\frac{a}{b}\right) + \tilde{f}\left(\frac{a'}{b'}\right), \end{aligned}$$

e que

$$\begin{aligned} \tilde{f}\left(\frac{a}{b} \cdot \frac{a'}{b'}\right) = \tilde{f}\left(\frac{a \cdot a'}{b \cdot b'}\right) = f(a \cdot a')(f(b \cdot b'))^{-1} = \\ f(a)(f(b))^{-1} \cdot f(a')(f(b'))^{-1} = \\ \tilde{f}\left(\frac{a}{b}\right) \cdot \tilde{f}\left(\frac{a'}{b'}\right). \end{aligned}$$

Como $\tilde{f}\left(\frac{1}{1}\right) = f(1)(f(1))^{-1} = 1$, temos que $\tilde{f}$ é um homomorfismo de anéis. □

2.2. Corpo de frações de um domínio ordenado

Sejam a e b elementos de um domínio ordenado A e seja K o corpo de frações de A. Devido à igualdade $\frac{a}{-b} = \frac{-a}{b}$ (verifique), todo elemento de K pode ser escrito sob a forma $\frac{a}{b}$ com $b > 0$. Nesta seção, vamos sempre supor que todos os elementos de K estão sob esta forma.

Sejam dados $\frac{a}{b}$ e $\frac{c}{d}$ em K, com $b > 0$ e $d > 0$. A relação

$$\frac{a}{b} \leq \frac{c}{d} \iff a \cdot d \leq b \cdot c$$

está bem definida em K (leitor, verifique que ela independe de representantes).

Suponha que $a \leq b$, logo $\frac{a}{1} \leq \frac{b}{1}$ e, portanto, $j(a) \leq j(b)$. Isto significa que a relação $\leq$ em K, acima definida, estende a relação $\leq$ de A.

Teorema 2.2.3. *Se A é um domínio ordenado, então o seu corpo de frações K é um anel ordenado, com uma relação de ordem que estende a de A.*

Demonstração A relação de ordem de K é a relação $\leq$ que definimos acima. Deixamos a cargo do leitor a verificação da reflexividade e da antissimetria de $\leq$, enquanto que a transitividade se demonstra como se segue:

Suponha que $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{e}{f}$. Segue-se que $a \cdot d \leq b \cdot c$ e $c \cdot f \leq d \cdot e$. Multiplicando ambos os lados da primeira desigualdade por f e da segunda por b (lembre-se que $b > 0$ e $f > 0$), obtemos que $a \cdot d \cdot f \leq b \cdot c \cdot f$ e $b \cdot c \cdot f \leq b \cdot d \cdot e$. Pela transitividade da relação $\leq$ em A, temos que $a \cdot d \cdot f \leq b \cdot d \cdot e$. Como $d > 0$, segue-se que $a \cdot f \leq b \cdot e$ (veja Problema 1.11 (a)), logo $\frac{a}{b} \leq \frac{e}{f}$.

Para provar a totalidade, considere a, b, c e d elementos de A, com $b > 0$ e $d > 0$. Pela totalidade da relação $\leq$ em A, segue-se que $a \cdot d \leq b \cdot c$ ou $b \cdot c \leq a \cdot d$, logo uma das seguintes possibilidades é verificada:

$$\frac{a}{b} \leq \frac{c}{d} \quad \text{ou} \quad \frac{c}{d} \leq \frac{a}{b}.$$

A seguir, demonstraremos a compatibilidade da relação $\leq$ com a adição, deixando a verificação da propriedade análoga para a multiplicação a cargo do leitor.

Sejam $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d} \in K$, tais que $\frac{a}{b} \leq \frac{a'}{b'}$. Segue-se que $a \cdot b' \leq a' \cdot b$. Multiplicando ambos os lados desta última desigualdade por d^2 e somando $c \cdot d \cdot b' \cdot b$ a ambos os lados da desigualdade obtida, temos que

$$b' \cdot d \cdot (a \cdot d + b \cdot c) \leq b \cdot d \cdot (a' \cdot d + b' \cdot c),$$

donde segue-se que $\frac{a}{b} + \frac{c}{d} \leq \frac{a'}{b'} + \frac{c}{d}$. □

Um corpo que é ordenado como anel será chamado de *corpo ordenado.*

O corpo dos números racionais é uma extensão do anel dos números inteiros. O que ganhamos e o que perdemos com esta extensão? Inicialmente, ganhamos o fato de termos preservado a estrutura de anel ordenado de $\mathbb{Z}$, obtendo, além disso, a propriedade adicional de corpo,

isto é, todo elemento não nulo de $\mathbb{Q}$ passa a ser invertível em $\mathbb{Q}$. Esta propriedade é mais forte do que a de integridade (veja o Problema 1.4). Perde-se porém a propriedade característica de $\mathbb{Z}$, que é o Princípio da Boa Ordenação, como pode-se verificar no seguinte exemplo:

O conjunto $S = \{x \in \mathbb{Q};\ 0 < x < 1\}$ é não vazio e limitado inferiormente, porém não possui menor elemento.

Problemas

2.1 Demonstre o Teorema 2.2.1.

2.2 Seja K' o corpo de frações de um corpo K. Mostre que a aplicação

$$\begin{aligned} \varphi\colon K' &\longrightarrow K \\ \frac{a}{b} &\longmapsto a \cdot b^{-1} \end{aligned}$$

é um isomorfismo.

2.3 Faça as verificações deixadas a cargo do leitor na demonstração do Teorema 2.2.3.

2.4 Sejam a, b, c e d elementos de um corpo K com $b, d \neq 0$. Mostre que se $\frac{a}{b} = \frac{c}{d}$, então

a) $\dfrac{a+c}{b+d} = \dfrac{a}{b}$, se $b + d \neq 0$.

b) $\dfrac{a+b}{b} = \dfrac{c+d}{d}$.

c) $\dfrac{a}{c} = \dfrac{b}{d}$, se $c \neq 0$.

d) $\dfrac{a-b}{b} = \dfrac{c-d}{d}$.

e) $\dfrac{a+b}{a-b} = \dfrac{c+d}{c-d}$, se $a \neq b$ e $c \neq d$.

2.5 Sejam $a, b \in \mathbb{Q}$. Mostre que $a > b > 0$ se, e somente se, $0 < \frac{1}{a} < \frac{1}{b}$.

2.6 Prove a seguinte propriedade de $\mathbb{Q}$ (Propriedade Arquimediana): Dados $a, b \in \mathbb{Q}$ com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $n \cdot b \geq a$.

2.7 Sejam A um domínio ordenado, K' um corpo ordenado e $f\colon A \to K'$ um homomorfismo injetor de anéis ordenados. Mostre que o homomorfismo $\tilde{f}$ da Proposição 2.2.2 é um homomorfismo de anéis ordenados onde a ordenação de K é a do Teorema 2.2.3.

3

Propriedades dos inteiros

1 Indução Matemática

O Princípio da Indução Matemática é um poderoso instrumento para demonstrar teoremas envolvendo os números inteiros e que vem sendo utilizado de uma forma implícita desde a antiguidade. Foi utilizado pela primeira vez de forma explícita por Francesco Maurolycus em 1575 para provar a fórmula da soma dos n primeiros números naturais ímpares (cf. Problema 1.1 (a)). O método tornou-se popular após a publicação em 1665 do *Traité du triangle arithmétique* por Blaise Pascal onde também era utilizado.

1.1. Princípio de Indução Matemática

Teorema 3.1.1 (Princípio de Indução Matemática). *Seja* $P(n)$ *uma sentença aberta em* $\{n \in \mathbb{Z};\ n \geq n_0\}$*, tal que*

i) $P(n_0)$ *é verdadeira.*

ii) *Para todo* $n \geq n_0$ *, se* $P(n)$ *é verdadeira, então* $P(n+1)$ *é verdadeira.*

Então $P(n)$ *é verdadeira para todo* $n \geq n_0$ *.*

Demonstração Seja $F = \{n \in \mathbb{Z};\ n \geq n_0$ e $P(n)$ é falso$\}$. Queremos provar que F é vazio.

Suponha, por absurdo, que $F \neq \emptyset$. Como F é limitado inferiormente (por n_0), pelo Princípio da Boa Ordenação, temos que F possui um menor elemento b. Como $b \in F$ temos que $b \geq n_0$, mas, por (i), temos

que $n_0 \notin F$, logo $b \neq n_0$ e, portanto, $b > n_0$. Sendo b o menor elemento de F, temos que $b - 1 \notin F$, logo $P(b-1)$ é verdadeira. De (ii) segue-se então que $P(b)$ é verdadeira e, portanto, $b \notin F$, contradição. □

Chamamos a atenção do leitor para não confundir indução matemática com indução empírica. Nas ciências naturais é comum, após um certo número (sempre finito) de experimentos, enunciar leis gerais que governam o fenômeno em estudo. Tais leis são tidas como verdades até prova em contrário. A indução matemática serve para estabelecer verdades matemáticas, válidas em conjuntos infinitos. Não se trata de mostrar que uma certa sentença aberta é verdadeira para um grande número de inteiros mas, trata-se de provar que uma tal sentença é verdadeira para todo inteiro n com $n \geq n_0$.

A título de exemplo, considere a sentença aberta em $\mathbb{N}$:

$$P(n): \quad n = n + (n-1)\cdot(n-2)\cdots(n-1000).$$

É claro que $P(1), P(2), P(3), \ldots, P(1000)$ são verdadeiras. O leitor mais afoito poderia considerar que estes experimentos são suficientes para concluir que $P(n)$ é verdadeira para todo número natural $n > 0$. Isto porém não é indução matemática. A conclusão seria falsa pois $P(1001)$ é falso.

Exemplo Vamos provar que a seguinte sentença aberta $P(n)$ é verdadeira para todo natural $n > 0$.

$$P(n): \quad 1 + \cdots + n = \frac{n(n+1)}{2}\cdot$$

(i) $P(1)$ é verdadeira pois $1 = 1(1+1)/2$.
(ii) Supondo $P(n)$ verdadeira, temos que

$$1 + \cdots + n = \frac{(n+1)}{2}\,.$$

Somando $n+1$ a ambos os membros da igualdade acima, obtemos

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

logo $P(n+1)$ é verdadeira. Pelo Princípio de Indução Matemática $P(n)$ é verdadeira para todo $n \geq 1$.

A seguir, daremos várias aplicações do Princípio de Indução Matemática.

1.2. Conjuntos finitos e infinitos

Seja $m \in \mathbb{N}$, com $m \neq 0$. Definimos I_m como sendo o conjunto

$$I_m = \{x \in \mathbb{N};\ 1 \leq x \leq m\} = \{1, \ldots, m\}.$$

Diremos que um conjunto A é *finito*, se $A = \emptyset$ ou se existirem $m \in \mathbb{N} \setminus \{0\}$ e uma bijeção de I_m em A. Se A não é finito, diremos que é *infinito*.

A questão que se coloca naturalmente é saber se o número natural m é univocamente determinado por A e pela existência de uma bijeção de I_m em A. A resposta é positiva e decorre do resultado a seguir.

Teorema 3.1.2. *Sejam m e n dois números naturais. Se $m > n > 0$, então não existe nenhuma função injetora de I_m em I_n.*

Demonsração: Afirmamos que basta provar o teorema quando $m = n + 1$. De fato, suponha a asserção do teorema válida para $m = n + 1$. Se $m > n + 1$ e se existisse uma função injetora de I_m em I_n, a sua restrição a I_{n+1} seria também injetora, o que seria uma contradição.

Para provar o teorema, basta então mostrar, por indução sobre n, que é verdadeira para todo $n \geq 1$ a seguinte asserção:

$P(n)$: Não existe nenhuma função injetora de I_{n+1} em I_n.

É claro que $P(1)$ é verdadeira. Supondo agora $P(n)$ verdadeira, queremos mostrar que $P(n + 1)$ é verdadeira.

Suponha por absurdo $P(n + 1)$ falso. Logo, existe $f\colon I_{n+2} \to I_{n+1}$ injetora. Duas possibilidades podem ocorrer:

a) $n + 1 \notin f(I_{n+2})$. Neste caso, a função $g\colon I_{n+1} \to I_n$, definida por $g(x) = f(x)$ para todo $x \in I_{n+1}$ é injetora, o que é uma contradição.

b) $n+1 \in f(I_{n+2})$. Seja x' o único elemento de I_{n+2} tal que $f(x') = n+1$. Consideraremos dois subcasos:

b′) $x' = n + 2$. Neste caso, $g\colon I_{n+1} \to I_n$ definida por $g(x) = f(x)$, $\forall\, x \in I_{n+1}$ é bem definida e injetora, absurdo.

b″) $x' \neq n+2$. Como f é injetora, temos que $f(n+2) \neq f(x') = n+1$.

Logo, a função $g\colon I_{n+1} \to I_n$ definida por

$$g(x) = \begin{cases} f(x) & \text{se} \quad x \neq x' \\ f(n+2) & \text{se} \quad x = x' \end{cases}$$

é bem definida e injetora, contradição. □

Suponha agora que dado um conjunto A, existam números naturais m e n com $m > n > 0$ e duas bijeções $f\colon I_m \to A$ e $g\colon I_n \to A$. Segue-se então que $g^{-1} \circ f\colon I_m \to I_n$ é uma bijeção, portanto injetora o que não é possível pelo teorema. Consequentemente, dado um conjunto finito A, o número natural m para o qual existe uma bijeção $I_m \to A$ é univocamente determinado por A e é chamado de *cardinalidade* de A ou o *número de elementos* de A. Diremos, neste caso, que A tem m elementos. A cardinalidade do conjunto $\emptyset$ é 0 (zero), por definição.

Corolário 3.1.3 (Princípio de Dirichlet). *Dados dois conjuntos X e Y respectivamente com m e n elementos, se $m > n > 0$, então não existe nenhuma função injetora de X em Y.*

Demonstração Existem bijeções $f\colon I_m \to X$ e $g\colon I_n \to Y$. Se existisse uma função injetora $h\colon X \to Y$, teríamos que $f^{-1} \circ h \circ f\colon I_m \to I_n$ é injetora, o que não é possível pelo teorema. □

O Princípio de Dirichlet é também chamado de *princípio das gavetas*, pois admite a seguinte formulação:

Princípio das Gavetas: Dados m objetos a serem distribuidos em n gavetas e se $m > n > 0$, então uma das gavetas deverá conter mais de um objeto.

Este princípio é chamado por alguns autores de *Princípio da Casa dos Pombos* (tente imaginar o porquê desse nome).

Corolário 3.1.4. *Sejam X um conjunto com m elementos e Y um conjunto com n elementos. Se $m < n$, então não existe nenhuma sobrejeção de X em Y.*

Demonstração Suponha $m > 0$ e que exista uma sobrejeção f de X em Y, logo pela Proposição 1.4.1, a função f admitiria uma inversa à direita $g\colon Y \to X$. Portanto, $f \circ g = \mathrm{id}_Y$. Segue-se então que g admite uma inversa à esquerda. Pela Proposição 1.4.2, tem-se que g é injetora. Isto contradiz o Princípio de Dirichlet.

Se $m = 0$, o resultado vale por vacuidade, pois não existem sequer funções de $\emptyset$ em Y. □

Corolário 3.1.5. *Sejam X e Y dois conjuntos finitos com o mesmo número de elementos. Uma função $f\colon X \to Y$ é injetora se, e somente se, ela é sobrejetora.*

Demonstração Suponha que f seja injetora e suponha por absurdo que não seja sobrejetora. Seja $y' \in Y$ não pertencente a $f(X)$. Logo é bem definida e injetora a função:

$$\begin{aligned} f_1 \colon X &\longrightarrow Y \setminus \{y'\} \\ x &\longmapsto f(x) \end{aligned}$$

Isto é uma contradição pelo Princípio de Dirichlet.

Suponha agora que f seja sobrejetora mas não injetora. Logo existem x' e x'' em X tais que $f(x') = f(x'')$. Portanto é bem definida e sobrejetora a função:

$$\begin{aligned} f_2 \colon X \setminus \{x'\} &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned}$$

Isto contradiz o Corolário 3.1.4. □

Corolário 3.1.6. *Todo domínio de integridade finito é um corpo.*

Demonstração Seja A um tal domínio. Para $a \neq 0$, considere a função

$$\begin{aligned} f \colon A &\longrightarrow A \\ x &\longmapsto a \cdot x \end{aligned}$$

Esta função é injetora (veja Problema 1.5, Capítulo 2). Logo, pelo Corolário 3.1.5, esta função é sobrejetora. Portanto, existe um elemento b em A tal que $a \cdot b = f(b) = 1$. Com isto fica provado que todo elemento $a \neq 0$ possui um inverso. Portanto, A é um corpo. □

Para $n \in \mathbb{N}$, define-se o *fatorial* de n como sendo

$$n! = \begin{cases} 1 & , \quad \text{se} \quad n = 0 \text{ ou } n = 1 \\ 1 \cdot 2 \cdots n & , \quad \text{se} \quad n > 1 \end{cases}$$

Proposição 3.1.7. *Dados dois conjuntos A e B, não vazios, com n elementos, então o conjunto de todas as bijeções de A em B tem $n!$ elementos.*

Demonstração Considere a sentença aberta:
$P(n)$: O número de bijeções entre dois conjuntos, cada um contendo $n > 0$ elementos, é $n!$.

$P(1)$ é claramente verdadeira, pois só existe uma bijeção entre dois conjuntos com 1 elemento cada.

Suponha $P(n)$ verdadeira e sejam A e B dois conjuntos com $n+1$ elementos cada. Fixe um elemento a de A. Existem $n+1$ possibilidades para escolher a imagem de a em B por uma bijeção. Para cada escolha dessas, por exemplo $a \mapsto b$, as bijeções que têm essa propriedade são tantas quantas são as bijeções de $A \setminus \{a\}$ em $B \setminus \{b\}$, logo são em número $n!$. Portanto, o número total de possibilidades de definir uma bijeção de A em B é

$$(n+1) \cdot n! = (n+1)!.$$

□

Daremos agora um exemplo de conjunto infinito.

Proposição 3.1.8. *$\mathbb{Z}$ é infinito.*

Demonstração Se existissem um número natural m e uma bijeção $f\colon I_m \to \mathbb{Z}$, teríamos uma função injetora $f^{-1}\colon \mathbb{Z} \to I_m$ e, portanto, a restrição $f^{-1}\big|_{I_{m+1}}\colon I_{m+1} \to I_m$ seria injetora, o que é impossível pelo Teorema 3.1.2. □

1.3. O homomorfismo característico

Sejam dados um anel A, um elemento a de A e um inteiro n. Definimos

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

Proposição 3.1.9. *Para todo $a \in A$ e todos $m, n \in \mathbb{Z}$, temos*

i) $m(a+b) = ma + mb$;

ii) $m(a \cdot b) = (ma) \cdot b$;

iii) $(m+n)a = ma + na$;

iv) $(mn)a = m(na)$;

v) $(-m)a = -(ma)$.

Demonstração A demonstração destes fatos é deixada a cargo do leitor, veja Problema 1.9. □

Das propriedades acima segue-se imediatamente que a aplicação natural

$$\begin{aligned} \rho\colon \mathbb{Z} &\longrightarrow A \\ n &\longmapsto n1 \end{aligned}$$

é um homomorfismo de anéis, chamado de *homomorfismo característico*. O próximo resultado nos garantirá que este é o único homomorfismo de $\mathbb{Z}$ em A.

Proposição 3.1.10. *Se* $h\colon \mathbb{Z} \to A$ *é um homomorfismo de anéis, então* $h = \rho$.

Demonstração Note que, pela Proposição 2.1.11 (i), temos que $h(0) = \rho(0) = 0$. Vamos provar, por indução sobre n, que, para todo $n > 0$, temos que

$$h(n) = n1. \tag{1}$$

Para $n = 1$, isto é claro, pois $h(1) = 1$. Suponha que para algum valor de $n > 0$, a igualdade (1) é verificada, logo

$$h(n+1) = h(n) + h(1) = n1 + 1 = (n+1)1,$$

o que demonstra, pelo Princípio de Indução Matemática, a igualdade (1) para todo $n > 0$.

Por outro lado, pela Proposição 2.1.11 (ii), e pelo caso $n > 0$ que acabamos de provar, temos que se $n < 0$, então

$$h(n) = -h(-n) = -(-n)1 = n1.$$

Com isto acabamos de provar que

$$h(n) = n1 = \rho(n), \quad \forall\, n \in \mathbb{Z}.$$

□

Corolário 3.1.11. *Seja* K *um corpo tal que o homomorfismo característico* $\rho\colon \mathbb{Z} \to K$ *é injetor. Então existe um único homomorfismo* $\tilde{\rho}\colon \mathbb{Q} \to K$ *e este é tal que* $\tilde{\rho} \circ j = \rho$, *onde* $j\colon \mathbb{Z} \to \mathbb{Q}$ *é o homomorfismo característico.*

Demonstração A existência de $\tilde{\rho}$ é garantida pela Proposição 2.2.2. Para provar a unicidade, suponha que tenhamos um homomorfismo

$$h\colon \mathbb{Q} \to K.$$

Logo temos dois homomorfismos ρ e $h \circ j$ de $\mathbb{Z}$ em K e portanto pela Proposição 3.1.10, segue-se que $h \circ j = \rho$. Novamente, a Proposição 2.2.2 nos diz que $h = \tilde{\rho}$. □

O homomorfismo característico ρ desempenha papel importante na teoria dos anéis. Para anéis ordenados, ρ tem uma propriedade adicional que damos a seguir.

Proposição 3.1.12. *Se A é um anel ordenado, então ρ é um homomorfismo injetor de anéis ordenados.*

Demonstração Inicialmente provaremos por indução que se $n \in \mathbb{Z}$, com $n > 0$, então $n1 > 0$.

Para $n = 1$, isto é claro já que em qualquer anel ordenado temos $1 > 0$ (veja Problema 1.9 (b), Capítulo 2). Suponha agora que para um determinado $n > 0$ tenhamos $n1 > 0$. Somando o elemento 1 de A a ambos os membros da última desigualdade acima, temos

$$(n+1)1 = n1 + 1 > 1 > 0,$$

obtendo $(n+1)1 > 0$. Consequentemente, para todo $n > 0$, temos que $n1 > 0$. Disto decorre que se $n < 0$, então $n1 < 0$.

Suponha que $m < n$, logo $n - m > 0$ e portanto $(n-m)1 > 0$, obtendo

$$\rho(n) - \rho(m) = n1 - m1 = (n-m)1 > 0.$$

Logo, $\rho(m) < \rho(n)$. Isto mostra que ρ é um homomorfismo injetor de anéis ordenados. □

Corolário 3.1.13. *Seja K um corpo ordenado. Existe um único homomorfismo $\tilde{\rho}\colon \mathbb{Q} \to K$. Além disso, $\tilde{\rho}$ é um homomorfismo de anéis ordenados.*

Demonstração Parte decorre imediatamente da Proposição 3.1.12 e do Corolário 3.1.11. Resta apenas provar que $\tilde{\rho}$ é um homomorfismo de anéis ordenados, o que decorre do Problema 2.7, Capítulo 2. □

Teorema 3.1.14. *Se A é um domínio bem ordenado, então ρ é um isomorfismo de anéis ordenados.*

Demonstração Pela Proposição 3.1.12, temos que ρ é um homomorfismo injetor de anéis ordenados. Falta apenas provar que ρ é sobrejetor, o que equivale a mostrar que todo elemento $a \in A$ é da forma $n1$ para

algum $n \in \mathbb{Z}$. Suponha por absurdo que existe $a \in A$ tal que $n1 \neq a$ para todo $n \in \mathbb{Z}$. Considere os seguintes subconjuntos de A:

$$S_1 = \{n1\,;\ n \in \mathbb{Z} \ \text{ e } \ n1 > a\} \quad \text{e} \quad S_2 = \{n1\,;\ n \in \mathbb{Z} \ \text{ e } \ n1 < a\}.$$

Mostraremos que $S_1 = S_2 = \emptyset$, o que é uma contradição.

Suponha que $S_1 \neq \emptyset$. Sendo S_1 limitado inferiormente, pelo Princípio da Boa Ordenação, ele possui um menor elemento $m1$, logo $m1 > a$ e $(m-1)1 \leq a$. Como $(m-1)1 \neq a$ (pela nossa hipótese sobre a), temos que $(m-1)1 < a$ e, consequentemente, pelo Corolário 2.1.7, temos que

$$m1 = (m-1)1 + 1 \leq a,$$

contradição.

De modo análogo prova-se que $S_2 = \emptyset$, usando porém a formulação (PBO′) do Princípio da Boa Ordenação. □

O teorema acima nos garante que:

A menos de isomorfismo, $\mathbb{Z}$ é o único anel bem ordenado.

2.4. Binômio de Newton

Sejam A um anel, $a \in A$ e $n \in \mathbb{N} \setminus \{0\}$. Definimos

$$a^n = \begin{cases} a & , \quad \text{se} \quad n = 1 \\ a \cdot a^{n-1} & , \quad \text{se} \quad n > 1 \end{cases}$$

Se $a \neq 0$, definimos $a^0 = 1$ e se a é invertível e $n < 0$, definimos $a^n = (a^{-1})^{-n}$.

Usando a definição acima é possível verificar (veja Problema 1.10) que para todos $a, b \in A \setminus \{0\}$ e todos $m, n \in \mathbb{N}$, temos que

i) $a^m \cdot a^n = a^{n+m}$,

ii) $(a^m)^n = a^{m \cdot n}$,

iii) $a^n \cdot b^n = (a \cdot b)^n$.

E se a é invertível, as igualdades acima se estendem para $n, m \in \mathbb{Z}$.

Para $n, i \in \mathbb{N}$, definimos

$$\binom{n}{i} = \begin{cases} \dfrac{n!}{i!(n-i)!} & , \quad \text{se} \quad n \geq i \\ 0 & , \quad \text{se} \quad n < i \end{cases}$$

Exemplo Temos, para todos n e $i \neq 0$ que

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{2} = \frac{n(n-1)}{2}, \quad \binom{n}{n} = 1, \quad \binom{0}{i} = 0.$$

Somente pela definição destes números, não é claro que se trata de números inteiros. Os próximos lemas nos mostrarão que este é o caso.

Lema 3.1.15 (Relação de Stifel). *Para todo par n e i, de números naturais não nulos, tem-se que*

$$\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$$

Demonstração Se $1 \leq i \leq n$, temos que

$$\binom{n}{i-1} + \binom{n}{i} = \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} =$$

$$\frac{i \cdot n! + (n-i+1) \cdot n!}{i!(n-i+1)!} =$$

$$\frac{(n+1) \cdot n!}{i!(n-i+1)!} = \frac{(n+1)!}{i!(n-i+1)!} = \binom{n+1}{i}$$

Se $i > n$, o resultado é trivialmente verificado. □

Lema 3.1.16. *Dado um par n e i de números naturais quaisquer, o número $\binom{n}{i}$ é natural.*

Demonstração A proposição é claramente válida para $n = 0$ e $n = 1$ e i qualquer, e para $i = 0$ e n qualquer. Vamos proceder por indução sobre n, para $n \geq 1$ e $i \geq 1$. Suponha que seja verdadeira para um determinado n e para i qualquer, nas condições acima.

Pelo Lema 3.1.15 temos que

$$\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i},$$

logo inteiro pela hipótese de indução. Isto conclui a prova. □

Teorema 3.1.17 (Binômio de Newton). *Dados dois elementos a e b de um anel e um número natural $n > 0$, tem-se que*

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} \cdot b + \cdots + \binom{n}{i} a^{n-i} \cdot b^i + \cdots + b^n.$$

Demonstração Seja $P(n)$ a igualdade acima. $P(1)$ é obviamente verdadeira. Suponhamos que $P(n)$ seja verdadeira. Temos que

$$(a+b)^{n+1} = (a+b)\cdot(a+b)^n = a\cdot(a+b)^n + b\cdot(a+b)^n.$$

Pela hipótese de que $P(n)$ é verdadeira, segue-se que

$$\begin{aligned} a\cdot(a+b)^n &= a^{n+1} + \binom{n}{1}a^n\cdot b + \binom{n}{2}a^{n-1}\cdot b^2 + \\ &\quad + \cdots + \binom{n}{n-1}a^2\cdot b^{n-1} + \binom{n}{n}a\cdot b^n \\ b\cdot(a+b)^n &= a^n b + \binom{n}{1}a^{n-1}\cdot b^2 + \\ &\quad + \cdots + \binom{n}{n-2}a^2\cdot b^{n-1} + \binom{n}{n-1}a\cdot b^n + b^{n+1} \end{aligned}$$

Somando membro a membro estas igualdades e usando as relações do Lema 3.1.15, segue-se que $P(n+1)$ é verdadeira. □

Corolário 3.1.18. *Para todo número natural* n*, tem-se que*

$$\begin{aligned} (a-b)^n = a^n + \binom{n}{1}(-1)a^{n-1}\cdot b + \cdots + \\ + \binom{n}{i}(-1)^i a^{n-i}\cdot b^i + \cdots + (-1)^n b^n. \end{aligned}$$

Exemplos Aplicando a fórmula do binômio de Newton, segue-se que

$(a+b)^2 = a^2 + 2a\cdot b + b^2$
$(a+b)^3 = a^3 + 3a^2\cdot b + 3a\cdot b^2 + b^3$
$(a+b)^4 = a^4 + 4a^3\cdot b + 6a^2\cdot b^2 + 4a\cdot b^3 + b^4$

1.5. Desigualdade de Bernoulli

Teorema 3.1.19 (Desigualdade de Bernoulli). *Seja* A *um domínio ordenado e seja* $c \in A$ *tal que* $c \geq -1$*, então para todo número natural* $n > 0$ *vale a seguinte desigualdade*:

$$(1+c)^n \geq 1 + nc.$$

Demonstração Seja $P(n)$ a desigualdade acima. $P(1)$ é claramente verdadeira.

Suponhamos $P(n)$ verdadeira. Multiplicando ambos os lados da desigualdade acima por $1+c$ (que é ≥ 0), obtemos

$$(1+c)^{n+1} \geq (1+n\cdot c)(1+c) = 1+(n+1)c+nc^2 \geq 1+(n+1)c,$$

donde concluímos que $P(n+1)$ é verdadeira.

Pelo Princípio de Indução Matemática, segue-se que $P(n)$ é verdadeira para todo número natural $n > 0$. □

Corolário 3.1.20. *Dados* $b, c \in \mathbb{Q}$ *com* $b > 1$, *existe* $n \in \mathbb{N}$ *tal que* $b^n > c$.

Demonstração Se $c \leq 0$, a desigualdade acima é claramente satisfeita para todo n. Suponha que $c > 0$. De $b > 1$, segue-se que $b-1 \neq 0$, logo, pela propriedade arquimediana de $\mathbb{Q}$ (veja Problema 2.6, Capítulo 2), existe $n \in \mathbb{Z}$ tal que $n(b-1) \geq c$. Como $c > 0$ e $b-1 > 0$, segue-se que $n \in \mathbb{N} \setminus \{0\}$. Temos então pela desigualdade de Bernoulli que

$$b^n = (1+(b-1))^n \geq 1+n(b-1) > n(b-1) \geq c. \quad \square$$

O corolário acima nos afirma que as potências de expoente inteiro positivo de um número racional maior do que 1 formam um conjunto que não é limitado superiormente.

Problemas

1.1 Prove por indução as seguintes fórmulas:

a) $1+3+5+\cdots+(2n-1) = n^2$.

b) $1^2+2^2+3^2+\cdots+n^2 = n(n+1)(2n+1)/6$.

c) $1^3+2^3+3^3+\cdots+n^3 = [n(n+1)/2]^2$.

d) $1^4+2^4+3^4+\cdots+n^2 = n(n+1)(2n+1)(3n^2+3n-1)/30$.

1.2 Prove por indução que:

a) $n! \geq 2^n$ para todo $n \geq 4$.

b) $n! \geq 3^n$ para todo $n \geq 7$.

c) $n! \geq 4^n$ para todo $n \geq 9$.

1.3 Ache o erro na "demonstração"da seguinte afirmação obviamente falsa: Todos os números inteiros positivos são iguais, ou seja, para todo $n \in \mathbb{N} \setminus \{0\}$ é verdadeira a asserção $P(n) : 1 = \cdots = n$.

i) $P(1)$ é verdadeira pois $1 = 1$.

ii) Suponha $P(n)$ verdadeira, logo $1 = \cdots = n - 1 = n$. Somando 1 a cada membro da última igualdade, segue-se que $n = n + 1$, logo $1 = \cdots = n - 1 = n = n + 1$ e, portanto, $P(n + 1)$ é verdadeira.

Pelo Princípio da Indução Matemática, segue-se que $P(n)$ é verdadeira para todo $n \in \mathbb{N} \setminus \{0\}$.

1.4 Dada a sentença aberta $P(n) : 1 + 2 + \cdots + n = [n(n + 1)/2] + 1$, em $\mathbb{N} \setminus \{0\}$, mostre que:

i) Para todo $n \in \mathbb{N}\setminus\{0\}$, se $P(n)$ é verdadeira, então $P(n+1)$ é verdadeira.

ii) $P(n)$ não é verdadeira para nenhum n.

1.5 Seja $f\colon \mathbb{Z} \to \mathbb{Z}$ uma função tal que, quaisquer que sejam a e b em $\mathbb{Z}$, tem-se que $f(a + b) = f(a) + f(b)$.

a) Mostre que $f(0) = 0$.

b) Mostre, por indução, que $f(n) = n \cdot f(1)$ para todo $n \in \mathbb{N}$.

c) Mostre que $f(-n) = -f(n)$ para todo $n \in \mathbb{Z}$.

d) Conclua que $f(n) = n \cdot f(1)$ para todo $n \in \mathbb{Z}$.

1.6 Uma *Progressão Aritmética* (P.A.) com primeiro termo a_1 e razão r é uma sequência de números cujo primeiro elemento é a_1 e tal que cada elemento, a partir do segundo, é igual ao anterior mais a razão. Em símbolos, se $n \geq 2$, $a_n = a_{n-1} + r$

a) Prove por indução sobre n que $a_n = a_1 + (n - 1)r$.

b) Se $S_n = a_1 + a_2 + \cdots + a_n$, prove por indução sobre n que

$$S_n = \frac{n(a_1 + a_n)}{2}.$$

1.7 Uma *Progressão Geométrica* (P.G.) com primeiro termo a_1 e razão q ($q \neq 0$ e $q \neq 1$) é uma sequência de números cujo primeiro elemento é a_1 e tal que, cada elemento, a partir do segundo, é igual ao anterior multiplicado pela razão. Em símbolos, se $n \geq 2$, $a_n = a_{n-1} \cdot q$

a) Prove por indução sobre n que $a_n = a_1 \cdot q^{n-1}$.

b) Se $S_n = a_1 + a_2 + \cdots + a_n$, prove por indução sobre n que

$$S_n = \frac{a_n \cdot q - a_1}{q - 1}.$$

1.8 Este é um jogo chamado Torre de Hanói. Dispõe-se de n discos perfurados de diâmetros decrescentes enfiados numa haste A, e de suas outras hastes B e C. O problema consiste em transferir toda a pilha de discos para a haste C, deslocando um disco de cada vez para qualquer haste, de modo que nenhum disco seja colocado sobre um outro de diâmetro menor.

a) Se a_n é o menor número de jogadas que resolve o jogo com n discos, mostre que $a_1 = 1$ e se $n \geq 2$, então $a_n = 2a_{n-1} + 1$.

b) Mostre, por indução sobre n, que se $n \geq 1$, então $a_n = 2^n - 1$.

1.9 Sejam A um anel, a e b elementos de A e n e m inteiros. Verifique que:

a) $(mn)a = m(na)$ b) $m(a \cdot b) = (ma) \cdot b$

c) $(m+n)a = ma + na$ d) $m(a+b) = ma + mb$

e) $(-m)a = -(ma)$

1.10 Sejam A um anel, a e b elementos de $A \setminus \{0\}$ e m e n números naturais. Mostre que:

a) $a^n \cdot a^m = a^{n+m}$ b) $(a^n)^m = a^{n \cdot m}$ c) $a^n \cdot b^n = (a \cdot b)^n$.

Mostre que se a e b são invertíveis, então as igualdades acima se estendem para $n, m \in \mathbb{Z}$.

1.11 Mostre que se A é um domínio ordenado e se $c \in A$, com $c > -1$, e $n \in \mathbb{N}$, então $(1+c) > n > 1 + cn$.

2 Divisão com resto

A divisão nos inteiros nem sempre é exata. Poder efetuar a divisão de dois inteiros com resto pequeno é uma propriedade importante responsável por propriedades algébricas notáveis que os inteiros possuem.

Teorema 3.2.1 (Divisão Euclidiana). *Dados inteiros* d *e* D *com* $d \neq 0$, *existem inteiros* q *e* r *tais que*

$$D = d \cdot q + r \quad e \quad 0 \leq r < |d|.$$

Além disso, q *e* r *são unicamente determinados pelas condições acima.*

Demonstração Considere o conjunto

$$S = \{x \in \mathbb{N};\ x = D - d \cdot n \text{ para algum } n \in \mathbb{Z}\}.$$

Este conjunto é limitado inferiormente (por 0) e não vazio, pois pela Propriedade Arquimediana dos inteiros, Proposição 2.1.10, existe um inteiro n tal que $n \cdot (-d) \geq -D$. Portanto, $x = D - n \cdot d \in S$.

Pelo Princípio da Boa Ordenação, segue-se que S posui um menor elemento r. Logo $r = D - d \cdot q$, para algum $q \in \mathbb{Z}$. É claro que $r \geq 0$ pois $r \in S$. Vamos agora provar que $r < |d|$.

Suponha por absurdo que $r \geq |d|$, logo $r = |d| + s$ para algum inteiro s tal que $0 \leq s < r$. Portanto,

$$D = d \cdot q + |d| + s = d(q \pm 1) + s,$$

e, consequentemente,

$$s = D - d \cdot (q \pm 1) \in S.$$

Como $s \in S$ e $s < r$, temos uma contradição, pois r era o menor elemento de S.

Para provar a unicidade, suponha que

$$D = d \cdot q_1 + r_1 = d \cdot q_2 + r_2\,,$$

com $0 \leq r_1 < |d|$ e $0 \leq r_2 < |d|$. Por estas últimas desigualdades segue-se que

$$-|d| < -r_2 \leq r_1 - r_2 \quad \text{e} \quad r_1 - r_2 < |d| - r_2 \leq |d|,$$

e, portanto,

$$-|d| < r_1 - r_2 < |d|.$$

Consequentemente, pela Proposição 2.1.4 (iii), temos que $|r_1 - r_2| < |d|$. Como

$$d(q_1 - q_2) = r_2 - r_1\,,$$

segue-se da Proposição 2.1.4 (i), que

$$|d| \cdot |q_1 - q_2| = |r_2 - r_1| < |d|.$$

Isto só é possível se $q_1 = q_2$ e $r_2 - r_1$. □

Portanto, o teorema nos garante que em $\mathbb{Z}$ é sempre possível efetuar a divisão de um número D por outro número $d \neq 0$ com resto pequeno.

Os números d, d, q e r são chamados, respectivamente, de *dividendo*, *divisor*, *quociente* e *resto*.

A seguir, introduzimos a *função parte inteira* que desempenha papel importante em Teoria dos Números e é definida como a seguir:

$$\begin{aligned}[\ \ ]: \mathbb{Q} &\longrightarrow \mathbb{Z} \\ x &\longmapsto [x] = \text{ maior inteiro } \leq x\end{aligned}$$

Por exemplo, $[1/2] = 0$, $[-1/2] = -1$, $[3/2] = 1$ e $[-3/2] = -2$.

Observações

3.2.2. Na divisão euclidiana, se $D \geq 0$ e $d > 0$, então $q \geq 0$.

De fato, se valesse $q < 0$, teríamos

$$D = d \cdot q + r < d \cdot q + d = d(q+1) \leq 0,$$

logo, $D < 0$, absurdo.

3.2.3. Na divisão euclidiana, se $D \geq d > 0$, então $r < D/2$.

De fato, como $D = d \cdot q + r$ com $0 \leq r < d$. É claro que $q \neq 0$ pois caso contrário, teríamos $D = r < d$, contrário à hipótese de que $D \geq d$. Logo, pela Observação 3.2.2 temos que $q > 0$ e, consequentemente, $q \geq 1$. Disto e da desigualdade $r < d$, obtemos $r \leq rq < dq$, portanto, $D = d \cdot q + r > 2r$, consequentemente, $r < D/2$.

3.2.4. O Teorema 3.2.1 admite a seguinte generalização: Dados inteiros D, d, n e m com $d \neq 0$ e $n \neq 0$, existem inteiros q e r unicamente determinados pelas condições

$$D = d \cdot q + r \quad \text{e} \quad \frac{m}{n} \leq r < \frac{m}{n} + |d|.$$

O Teorema 3.2.1 corresponde ao caso $\frac{m}{n} = 0$. Quando $\frac{m}{n} = -\frac{|d|}{2}$, esta divisão se chama de *algoritmo do menor resto*. Neste caso, tem-se que

$$-\frac{|d|}{2} \leq r < \frac{|d|}{2}\,.$$

3.2.5. Sejam $a, b \in \mathbb{Z}$ com $b > 0$ e q o quociente da divisão de a por b. Então $q = \left[\frac{a}{b}\right]$.

De fato, sendo $a = b \cdot q + r$ com $0 \leq r < b$, segue-se que $\frac{a}{b} = q + \frac{r}{b}$ com $\frac{r}{b}$ um número racional tal que $0 \leq \frac{r}{b} < 1$. Portanto,

$$q \leq \frac{a}{b} = q + \frac{r}{b} < q + 1,$$

logo $q = \left[\frac{a}{b}\right]$.

3.2.6. Dado um número racional c, existe um número inteiro no intervalo

$$(c, c+1] = \{x \in \mathbb{Q};\ c < x \leq c+1\}.$$

De fato, suponha $c = \frac{a}{b}$ com $a, b \in \mathbb{Z}$ e $b > 0$. Pela Observação acima,

$$[c] = \frac{a}{b} - \frac{r}{b},$$

com $0 \leq \frac{r}{b} < 1$ e portanto,

$$0 < ([c] + 1) - c \leq 1,$$

logo $[c] + 1 \in (c, c+1]$.

Note que existe um único inteiro no intervalo $(c, c+1]$. Vale um resultado análogo para o intervalo $[c, c+1)$.

Problemas

2.1 Ache q e r na divisão euclidiana quando:

a) $D = 25,\ \ d = 7$ b) $D = -25,\ d = 7$ c) $D = 25,\ \ d = -7$
d) $D = -25,\ \ d = -7$ e) $D = 8,\ d = 10$ f) $D = -8,\ \ d = 10$
g) $D = 8,\ \ d = -10$ h) $D = -8,\ \ d = -10$

2.2 Se o quociente e o resto da divisão de a por b são respectivamente q e r, quais são o quociente e o resto da divisão de a por $-b$? E de $-a$ por b?

2.3 Quais são os números inteiros que quando divididos por 4 dão um resto igual

a) à metade do quociente?

b) ao quociente?

c) ao dobro do quociente?

d) ao triplo do quociente?

2.4 A soma dos quocientes na divisão euclidiana de dois números D e D' por um número $d > 0$, é sempre igual ao quociente da divisão de $D + D'$ por d? Se não for igual de quanto difere?

2.5 Usando a divisão euclidiana, mostre que todo número inteiro é da forma $2n$ ou $2n+1$ com $n \in \mathbb{Z}$. Os números da forma $2n$ são chamados *pares* e os da forma $2n+1$ são chamados *ímpares*. Mostre que:

a) a soma de dois números pares é par.

b) a soma de dois números ímpares é par.

c) a soma de um número par com um ímpar é ímpar.

d) o produto de dois números é par se um deles é par.

e) o produto de dois números ímpares é ímpar.

f) de dois inteiros consecutivos um deles é par.

2.6 Seja a um número inteiro qualquer. Mostre que exatamente um número de cada terna dada é divisível por 3

a) a, $a+1$, $a+2$ b) a, $a+2$, $a+4$

c) a, $a+5$, $a+10$ d) a, $a+10$, $a+20$

2.7 Seja a um número inteiro. Mostre que:

a) Se a^2 é par, então a é par.

b) Se a^2 é divisível por 3, então a é divisível por 3.

2.8 Sejam $m, n, a \in \mathbb{N}$, com $n > m > 1$.

a) Quantos inteiros divisíveis por a existem entre 1 e n?

b) Quantos existem entre m e n?

c) Quantos inteiros divisíveis por 7 existem entre 112 e 1328?

3 Sistemas de numeração

Nesta seção vamos nos ocupar com a representação dos números inteiros. Há vários modos de se representar números inteiros e a cada um desses chamamos de *sistema de numeração*. A maioria dos sistemas de numeração têm em comum o fato dos números serem representados pelo uso de um número reduzido de símbolos chamados *algarismos*. Os sistemas de numeração mais utilizados são os sistemas de base constante e baseiam-se no seguinte resultado:

Teorema 3.3.1. *Dados inteiros* a *e* b *com* $a \geq 0$ *e* $b > 1$*, existem inteiros* $c_0, c_1, \ldots, c_n, \ldots$*, univocamente determinados pelas seguintes condições:*

i) *Existe um número natural* m *tal que* $c_n = 0$ *para todo* $n \geq m$.

ii) *Para todo* n*, temos que* $0 \leq c_n < b$.

iii) $a = c_0 + c_1 \cdot b + \cdots + c_m \cdot b^m$.

Demonstração Fixe um inteiro $b > 1$. Seja S o conjunto dos elementos de $\mathbb{N}$ para os quais são satisfeitas as condições do teorema. Queremos provar que o complementar S' de S em $\mathbb{N}$ é vazio. Caso $S' \neq \emptyset$, como ele é limitado inferiormente, ele possui um menor elemento c distinto de 0, pois $0 \in S$. Pela Divisão Euclidiana, temos que

$$c = b \cdot q + r, \quad 0 \leq r < b.$$

Como $c, b > 0$, temos que $q \geq 0$ (veja Observação 3.2.2). Claramente, $q < c$, logo $q \in S$ e, portanto,

$$q = c_1 + c_2 \cdot b + \cdots + c_m \cdot b^{m-1},$$

com c_i únicos tais que $0 \leq c_i < b$, para todo $i = 1, \ldots, m$.

Se tomamos $c_0 = r$, temos que

$$c = c_0 + c_1 \cdot b + \cdots + c_m \cdot b^m,$$

com c_i tais que $0 \leq c_i < b$, para todo $i = 0, \ldots, m$.

Suponha agora que $c = c_0' + q' \cdot b$, com $0 \leq c_0' < b$ e

$$q' = c_1' + c_2' \cdot b + \cdots + c_{m'}' b^{m'-1},$$

com $0 \leq c_i' < b$, para $i = 1, \ldots, m'$.

Pela unicidade do quociente e do resto na divisão euclidiana, temos que $c_0' = c_0$ e $q' = q$. Como $q \in S$, temos garantida a unicidade de $c_1, \ldots, c_{m'}$, logo $m' = m$ e $c_i' = c_i$ para todo $i = 1, \ldots, m$. Portanto, $c \in S$, contradição.

Com isto provamos que $S' = \emptyset$. □

A expressão $a = c_0 + c_1 \cdot b + \cdots + c_m \cdot b^m$ com $0 \leq c_i < b$ para $i = 0, \ldots, m$, é chamada de *expansão* b*-ádica* do inteiro a.

Analisando com cuidado a demonstração acima obtemos o seguinte algoritmo para calcular a expansão b-ádica de um inteiro não negativo a:

$$\begin{aligned}
a &= bq_0 + c_0, && 0 \leq c_0 < b \\
q_0 &= bq_1 + c_1, && 0 \leq c_1 < b \\
&\vdots \\
q_{n-2} &= bq_{n-1} + c_{n-1}, && 0 \leq c_{n-1} < b \quad \text{e } q_{n-1} < b
\end{aligned}$$

Pondo $c_n = q_{n-1}$, temos que

$$a = c_0 + c_1 \cdot b + \cdots + c_n \cdot b^n.$$

Exemplo Vamos determinar a expansão 5-ádica de 723:

$$\begin{aligned}
723 &= 144 \cdot 5 + 3 \\
144 &= 28 \cdot 5 + 4 \\
28 &= 5 \cdot 5 + 3 \\
5 &= 1 \cdot 5 + 0 \qquad (1 < 5)
\end{aligned}$$

logo $723 = 3 + 4 \cdot 5 + 3 \cdot 5^2 + 0 \cdot 5^3 + 1 \cdot 5^4$.

O sistema de numeração de base $b > 1$ obtém-se escolhendo um conjunto com b símbolos:

$$S = \{s_0, \ldots, s_{b-1}\},$$

onde $s_0 = 0$, que simbolizam os inteiros de 0 a $b-1$ e representando um inteiro não negativo s como

$$s = x_n x_{n-1} \ldots x_0\,, \quad \text{com } x_i \in S,\ i = 0, \ldots, n.$$

Identificam-se

$$0x_n x_{n-1} \ldots x_0 \quad \text{e} \quad x_n x_{n-1} \ldots x_0;$$

ou seja, em qualquer sistema de numeração os zeros à esquerda são desprezados.

Os inteiros negativos são representados pelos inteiros positivos precedidos do sinal $(-)$.

A justificativa da validade da representação acima se apoia no Teorema 3.3.1 que nos garante ser bijetora a função

$$\begin{aligned} \mathbb{Z}_b^+ &\longrightarrow \mathbb{N} \\ x_n \cdots x_0 &\longmapsto c_0 + \cdots + c_n \cdot b^n \end{aligned}$$

onde $\mathbb{Z}_b^+$ é o conjunto dos elementos da forma $x_n \ldots x_0$, com $x_n \neq 0$ se $n > 0$ e onde, para cada i, tem-se que c_i é o inteiro correspondente ao símbolo x_i.

No sistema de base 10, chamado de *sistema decimal*, toma-se

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

O sistema de base $b = 2$ é utilizado na aritmética dos computadores, onde os números são representados por sequências ou vetores $(a_0, a_1, a_2, \ldots)$, compostos dos algarismos 0 ou 1, correspondendo à escrita de um número na forma $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots$. Esse sistema é chamado de *sistema binário*.

Se $b \leq 10$, utilizam-se os símbolos $0, 1, \ldots, b-1$ e se $b > 10$ utilizam-se os símbolos $0, 1, \ldots, 9$ e introduzem-se símbolos adicionais para representar $10, \ldots, b-1$.

Problemas

3.1 Mostre que o algarismo das unidades do quadrado de um inteiro no sistema decimal só pode ser 0, 1, 4, 5, 6 ou 9.

3.2 Um certo número de três algarismos no sistema decimal aumenta de 36 quando se invertem os dois algarismos da direita e diminui de 270 quando se invertem os dois algarismos da esquerda. O que acontece ao número quando se invertem os dois algarismos extremos?

3.3 Prove que é válida a seguinte regra para calcular o quadrado de um número no sistema decimal cujo algarismo das unidades é 5:

$$(\bar{n}\,5)^2 = \overline{n(n+1)}25,$$

onde a notação $\bar{x}y$ significa o número $x \cdot 10^r + y$, onde r é o número de algarismos de y. Calcule mentalmente os quadrados de 25, 45, 95 e 105.

3.4 Escolha um número de três algarismos abc no sistema decimal de modo que os algarismos das centenas e o das unidades difiram de

pelo menos duas unidades, isto é, $|a - c| \geq 2$. Considere o número $xyz = |abc - cba|$ e efetue a soma de xyz com zyx. O resultado é 1089.

a) Justifique o fato de que o resultado independe do número inicialmente escolhido.

b) O que aconteria se os algarismos das unidades e o das centenas diferissem de uma unidade? E se fossem iguais?

3.5 Seja dado um número 5283 na base 10, escreva-o nas bases 2, 3, 4, 5, 8 e 15.

3.6 O número 6232 está escrito na base 7, escreva-o na base 5.

3.7 Escreva a tabuada da base 5. Dados os números $a = 23142$ e $b = 43210$, na base 5, ache por meio de um algoritmo os números $a + b$, $b - a$ e $a \cdot b$.

3.8 Por meio de um algoritmo análogo ao usado na base 10, efetue as seguintes operações na base 2:

a) $1011 + 1101$ b) $10011 + 11101101$

c) 1101×110 d) 101100×101

3.9 a) Considere 36 na base 10, em que base será representado por 51?

b) Idem para 73 e 243.

c) Idem para 73 e 242.

d) Considere o número 21378 na base 9, escreva-o na base 7.

3.10 Utilizando os sistemas decimal e binário, justifique o seguinte algoritmo utilizado por alguns povos para efetuar a multiplicação de dois inteiros positivos a e b representados no sistema decimal.

Ponha a e b no alto de duas colunas. Abaixo de a ponha o quociente q_1 da divisão de a por 2, abaixo de q_1 ponha o quociente q_2 da divisão de q_1 por 2, etc. Abaixo de b ponha $2b$, abaixo de $2b$ ponha $4b$, etc. Toda vez que o número na coluna do a for ímpar, coloque um sinal $+$ ao lado do número da mesma linha na coluna do b. Some todos os números assinalados com $+$. Este é o produto de a por b.

Exemplo $a = 35$ e $b = 47$:

$$
\begin{array}{lrll}
35 & 47 & & + \\
17 & 94 & & + \\
8 & 188 & & \\
4 & 376 & & \\
2 & 752 & & \\
1 & \underline{1504} & & + \\
 & 1645 & = & 35 \times 47
\end{array}
$$

4 Euclides

Euclides foi um eminente matemático grego. Presume-se que tenha vivido de 330 a 275 A.C. na cidade de Alexandria, durante o reinado de Ptolomeu I. A contribuição de Euclides à matemática foi considerável, tendo sido o primeiro matemático a apresentar a Geometria e a Aritmética como ciências dedutivas. Sua principal obra são os *Elementos*, um conjunto de treze livros onde é exposta de maneira sistemática e primorosa a matemática de sua época. Partindo de definições, postulados e axiomas e com regras lógicas bem determinadas, as proposições são demonstradas. Este método foi tão marcante que é utilizado até hoje para expor a matemática.

A Aritmética de Euclides tem início no livro VII dos Elementos, onde é usada sistematicamente, sem menção explícita e sem demonstração, a divisão com resto do Teorema 3.2.1 que denominamos de Divisão Euclidiana.

Os Elementos de Euclides é, sem dúvida, após a Bíblia, a segunda obra mais lida pela humanidade.

4

Álgebra dos inteiros

Como num anel nem sempre é posssível dividir de modo exato um elemento por outro, a noção de divisibilidade assume um papel importante. O conceito de máximo divisor comum é natural neste contexto e se relaciona com objetos algébricos chamados ideais. Neste capítulo introduzimos estes conceitos e deduzimos algumas relações entre eles. Em particular, mostramos como consequência da divisão euclidiana nos inteiros que, do ponto de vista da complexidade dos seus ideais, o anel dos inteiros tem uma estrutura bem simples, fato este que tem consequências algébricas notáveis. Por exemplo, em um anel com estrutura de ideais semelhante à dos inteiros, temos garantida a existência de máximo divisor comum e os seus elementos possuem a propriedade de fatoração única. Esta última propriedade no anel dos inteiros é chamada de Teorema Fundamental da Aritmética e já se encontra parcialmente nos Elementos de Euclides.

1 Divisibilidade

Sejam a e b elementos de um anel A. Se existir um elemento c de A tal que $b = a \cdot c$, diremos que a *divide* b. Neste caso, diremos também que a *é um divisor de* b, ou que b *é um múltiplo de* a, ou ainda, que b *é divisível por* a.

A afirmação a divide b será simbolizada por $a \mid b$ e a sua negação por $a \nmid b$.

Num anel A, a divisibilidade goza das seguintes propriedades:

Proposição 4.1.1. *Sejam* $a, b, c, d, b_1, \ldots, b_n, c_1, \ldots, c_n$ *elementos de* A. *São verdadeiras as seguintes afirmações:*

i) $a \mid 0$ *e* $a \mid a$.

ii) *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

iii) *Se* $a \mid b$ *e* $c \mid d$, *então* $a \cdot c \mid b \cdot d$.

iv) *Se* $a \mid (b + c)$ *e* $a \mid b$, *então* $a \mid c$.

v) *Se* $a \mid b_1, \ldots, a \mid b_n$, *então* $a \mid (c_1 \cdot b_1 + \cdots + c_n \cdot b_n)$.

vi) *Se* u *é invertível em* A, *então* $u \mid a$.

Demonstração (i) $a \mid 0$ pois $0 = a \cdot 0$ e $a \mid a$ pois $a = a \cdot 1$.
(ii) Se $a \mid b$ e $b \mid c$, existem elementos f e g de A tais que $b = a \cdot f$ e $c = b \cdot g$. Segue-se que $c = a \cdot f \cdot g$. Logo, $a \mid c$.
(iii) Se $a \mid b$ e $c \mid d$, existem elementos f e g de A tais que $b = a \cdot f$ e $d = c \cdot g$. Segue-se que $b \cdot d = a \cdot f \cdot c \cdot g = a \cdot c \cdot f \cdot g$ e, portanto, $a \cdot c \mid b \cdot d$.
(iv) Se $a \mid (b+c)$ e $a \mid b$, existem elementos f e g de A tais que $b+c = a \cdot f$ e $b = a \cdot g$. Segue-se que $c = a \cdot f - b = a \cdot f - a \cdot g = a \cdot (f - g)$. Logo, $a \mid c$.
(v) $a \mid b_i$ significa que existe $d_i \in A$ tal que $b_i = a \cdot d_i$, portanto, $c_1 \cdot b_1 + \cdots + c_n \cdot b_n = a \cdot (c_1 \cdot d_1 + \cdots + c_n \cdot d_n)$ e, consequentemente, $a \mid (c_1 \cdot b_1 + \cdots + c_n \cdot b_n)$.
(vi) Seja u um elemento invertível de A, logo $a = u(u^{-1} \cdot a)$ e, portanto, $u \mid a$. □

Proposição 4.1.2. *Sejam* A *um domínio de integridade e* $a, b \in A$. *Temos que* $a \mid b$ *e* $b \mid a$ *se, e somente se, existe um elemento invertível* u *de* A *tal que* $b = u \cdot a$.

Demonstração Se $a \mid b$ e $b \mid a$, então existem elementos u e v de A tais que $b = a \cdot u$ e $a = b \cdot v$, logo $b = b \cdot v \cdot u$ e, portanto, $b \cdot 1 = b \cdot v \cdot u$. Se $b \neq 0$, pela lei do cancelamento (Proposição 2.1.3), segue-se que $1 = v \cdot u$, logo u é invertível. Como $b = a \cdot u$, o resultado decorre. Se $b = 0$, de $b \mid a$ segue-se que $a = 0$ e neste caso vale também o resultado, já que $b = 1 \cdot a$.

Reciprocamente, se $b = u \cdot a$, então $a \mid b$. Se u é invertível, então $u^{-1} \cdot b = a$ e, consequentemente, $b \mid a$. □

Corolário 4.1.3. *Se* a *e* b *são inteiros tais que* $a \mid b$ *e* $b \mid a$*, então* $a = b$ *ou* $a = -b$.

Demonstração Da proposição acima, segue-se que $b = u \cdot a$ com u invertível em $\mathbb{Z}$, logo pela Proposição 2.1.9, tem-se que $u = \pm 1$. □

Dois elementos a e b de um anel A são ditos *associados* se existir um elemento invertível u de A tal que $a = u \cdot b$.

A noção de elementos associados é fundamental, pois, no que diz respeito à divisibilidade, dois elementos associados comportam-se exatamente do mesmo modo (veja Problema 1.2).

A relação binária, a é associado de b, em A é uma relação de equivalência em A (veja Problema 1.1).

A Proposição 4.1.2 nos diz que num domínio de integridade, a e b são associados se, e somente se, $a \mid b$ e $b \mid a$.

Proposição 4.1.4. *Se* a *e* b *são inteiros, com* $b \neq 0$ *e* $a \mid b$*, então* $|a| \leq |b|$.

Demonstração Se $a \mid b$, então existe um inteiro c tal que $b = a \cdot c$. Como $b \neq 0$, segue-se que $c \neq 0$, logo pelo Corolário 2.1.8, temos que

$$|b| = |a \cdot c| \geq |a|.$$

□

Sejam $a_1, \ldots, a_s$ elementos de um anel A. Diremos que $d \in A$ é um *máximo divisor comum* (mdc) de $a_1, \ldots, a_s$, se são verificadas as seguintes condições:

i) O elemento d é um divisor comum de $a_1, \ldots, a_s$.

ii) Todo divisor comum de $a_1, \ldots, a_s$ divide d.

Com este grau de generalidade, não podemos garantir a existência de um mdc de elementos de A. Antes de discutirmos o problema da existência de mdc, o que será feito na próxima seção, vejamos que relações guardam entre si, quando existem, os vários máximos divisores comuns de dados elementos de A.

Proposição 4.1.5. *Seja* d *um* mdc *de* $a_1, \ldots, a_s$. *Temos que* d' *é um* mdc *destes elementos se, e somente se,* $d \mid d'$ *e* $d' \mid d$.

Demonstração Suponha que d e d' sejam dois máximos divisores comuns de $a_1, \ldots, a_s$. Logo, pelo item (i) da definição acima, temos que

d e d' são divisores de $a_1, \ldots, a_s$ e, portanto, pelo item (ii) da definição, segue-se que $d \mid d'$ e $d' \mid d$.

Reciprocamente, suponha que d seja um mdc de $a_1, \ldots, a_s$ e que $d \mid d'$ e $d' \mid d$. Como $d \mid a_i$, para todo $i = 1, \ldots, s$, e $d' \mid d$, segue-se, do item (ii) da Proposição 4.1.1, que $d' \mid a_i$, para todo $i = 1, \ldots, s$. Seja agora $c \in A$ um divisor comum de $a_1, \ldots, a_s$, logo pelo item (ii) da definição, temos que $c \mid d$ e como $d \mid d'$, segue-se, novamente do item (ii) da Proposição 4.1.1, que $c \mid d'$. Temos, portanto, que d' é um mdc de $a_1, \ldots, a_s$. □

Corolário 4.1.6. *Num domínio de integridade dois máximos divisores comuns de dados elementos são associados e todo associado de um* mdc *destes elementos é também um* mdc *deles.*

Demonstração Este resultado é uma consequência direta das Proposições 4.1.2 e 4.1.5. □

Em particular, quando $A = \mathbb{Z}$, o corolário acima e o corolário 4.1.3 nos garantem que se d é um mdc de certos inteiros, então $-d$ também o é, e estes são os seus únicos máximos divisores comuns. Portanto, se existir um mdc não nulo dos inteiros $a_1, \ldots, a_s$, existirão dois, um positivo e outro negativo. Usaremos a notação mdc $(a_1, \ldots, a_s)$ para representar o mdc positivo de $a_1, \ldots, a_s$, o qual será chamado de *o máximo divisor comum.*

Se c é um divisor comum de inteiros $a_1, \ldots, a_s$, não todo nulos, então $c \neq 0$, $\text{mdc}(a_1, \ldots, a_s) \neq 0$ e $c \mid \text{mdc}(a_1, \ldots, a_s)$. Logo, pela Proposição 4.1.4, temos que

$$c \leq |c| \leq \text{mdc}(a_1, \ldots, a_s),$$

e, portanto, o máximo divisor comum de dados inteiros não todos nulos é o maior dos divisores comuns destes inteiros.

Um elemento m de um anel A é um *mínimo múltiplo comum* (mmc) de elementos $a_1, \ldots, a_s$ se são verificadas as seguintes condições:

i) O elemento m é múltiplo comum de $a_1, \ldots, a_s$.

ii) O elemento m divide qualquer múltiplo comum de $a_1, \ldots, a_s$.

Nesta situação, prova-se também que, num domínio de integridade, dois mínimos múltiplos comuns de dados elementos são associados e que todo associado de um mmc destes elementos é também um mmc deles (veja Problema 1.10). Segue-se, então, que se existir um mmc não

nulo de inteiros $a_1, \ldots, a_s$, existirão dois, um positivo e outro negativo. O mmc positivo será denotado por mmc $(a_1, \ldots, a_s)$ e será chamado de *o mínimo múltiplo comum*. Se c é um múltiplo comum positivo de $a_1, \ldots, a_s$, temos que mmc $(a_1, \ldots, a_x) \mid c$, logo, da Proposição 4.1.4, segue-se que

$$\text{mmc}(a_1, \ldots, a_s) \leq c.$$

Portanto, o mmc de dados números inteiros não nulos é o menor dos múltiplos comuns positivos destes números.

Problemas

1.1 Mostre que num anel qualquer, a relação de associado entre elementos é de equivalência.

1.2 Sejam a e b elementos de um anel. Mostre que são equivalentes as afirmações:

i) a divide b.

ii) Todo associado de a divide todo associado de b.

iii) Existe um associado de a que divide um associado de b.

1.3 Sejam a, b e c elementos de um domínio de integridade com $c \neq 0$. Mostre que $a \mid b$ se, e somente se, $a \cdot c \mid b \cdot c$.

1.4 Seja n um número inteiro positivo ímpar. Mostre que a soma de n temos consecutivos de uma progressão aritmética com elementos em $\mathbb{Z}$ é divisível por n.

1.5 Dados n números naturais consecutivos, mostre que um e apenas um destes números é divisível por n.

1.6 Sejam m e n inteiros ímpares. Mostre que:

a) $8 \mid (m^2 - n^2)$. b) $8 \mid (m^4 + n^4 - 2)$.

1.7 Mostre que para todo inteiro não negativo n, tem-se que

$$9 \mid (10^n + 3 \cdot 4^{n+2} + 5).$$

Sugestão: Por indução sobre n.

1.8 Sejam A um anel, a e b elementos de A e n um número natural. Mostre que:

a) Para todo n tem-se que $(a - b) \mid (a^n - b^n)$.

b) Para todo n ímpar tem-se que $(a+b) \mid (a^n + b^n)$.

c) Para todo n par tem-se que $(a+b) \mid (a^n - b^n)$.

Sugestão: Mostre que, para todos os números naturais n e m, valem as identidades:

$$a^n - b^n = (a-b)\cdot(a^{n-1} + a^{n-2}\cdot b + \cdots + a\cdot b^{n-2} + b^{n-1}).$$
$$a^{2m+1} + b^{2m+1} = (a+b)\cdot(a^{2m} - a^{2m-1}b + \cdots - ab^{2m-1} + b^{2m}).$$
$$a^{2m} - b^{2m} = (a+b)\cdot(a^{2m-1} - a^{2m-2}\,b + \cdots + ab^{2m-2} - b^{2m-1}).$$

1.9 Mostre que para todo número inteiro positivo n, tem-se que:

a) $9 \mid (10^n - 1)$ b) $3 \mid (10^n - 7^n)$ c) $8 \mid (3^{2n} - 1)$

d) $6 \mid (5^{2n+1} + 1)$ e) $17 \mid (10^{2n+1} + 7^{2n+1})$ f) $19 \mid (3^{2n+1} + 4^{4n+2})$

g) $6 \mid (5^{2n} - 1)$ h) $13 \mid (9^{2n} - 4^{2n})$ i) $53 \mid (7^{4n} - 2^{4n})$

1.10 Seja A um domínio de integridade. Mostre que:

a) Dois mínimos múltiplos comuns de dados elementos são associados.

b) Se um elemento é associado de um mmc de dados elementos, ele também é um mmc destes elementos.

1.11 a) Mostre que 0 é um mdc de $a_1, \ldots, a_s$ se, e somente se, $a_i = 0$ para todo $i = 1, \ldots, s$.

b) Mostre que 0 é um mmc de $a_1, \ldots, a_s$ se, e somente se, $a_i = 0$ para algum $i = 1, \ldots, s$.

2 Ideais

A definição de ideal foi introduzida no final do século dezenove por Kummer e Dedekind a fim de estudar certas questões em Teoria dos Números. Essa noção tornou-se um objeto central na teoria dos anéis. Nesta seção teremos a oportunidade de ver como essa noção se relaciona com as noções de máximo divisor comum e de mínimo múltiplo comum.

Um subconjunto I de um anel A será chamado de *ideal* de A se possuir as seguintes propriedades:

(i) $I \neq \emptyset$;

(ii) Se $a, b \in I$, então $a + b \in I$;

(iii) Se $a \in A$ e $b \in I$, então $a \cdot b \in I$.

Das propriedades (i) e (iii) segue-se claramente que $0 \in I$. Note que da definição decorre que $I = \{0\}$ é um ideal de A. Este ideal será chamado de ideal nulo e será simbolizado por (0).

Da propriedade (iii) da definição segue-se que se $a \in I$, então $-a = (-1) \cdot a \in I$. Disto e de (ii), segue-se que se $a, b \in I$, então $a - b \in I$.

Das propriedades (ii) e (iii) temos que se $a_1, \ldots, a_s \in I$ e $n_1, \ldots, n_s \in A$, então $n_1 \cdot a_1 + \cdots + n_s a_s \in I$.

Exemplos

1. Seja $a \in A$. Definimos $I(a) = \{n \cdot a\,;\ n \in A\}$. É fácil verificar (faça-o) que $I(a)$ é um ideal de A. Neste caso, diremos que o ideal $I(a)$ é gerado por a ou que a é um gerador do ideal $I(a)$. Por exemplo, se $A = \mathbb{Z}$, então o ideal gerado por 2 é o conjunto dos números inteiros pares e o ideal gerado por 1 é todo $\mathbb{Z}$.

2. Sejam $a, b \in A$. Definimos

$$I(a, b) = \{n \cdot a + m \cdot b\,;\ m, n \in A\}$$

É também fácil verificar que $I(a, b)$ é um ideal de A. Neste caso, diremos que o ideal $I(a, b)$ é gerado por a e b ou que a e b são geradores de $I(a, b)$.

3. Mais geralmente, sejam $a_1, \ldots, a_s \in A$, definimos

$$I(a_1, \ldots, a_s) = \{n_1 \cdot a_1 + \cdots + n_s \cdot a_s\,;\ n_1, \ldots, n_s \in A\}.$$

Este conjunto é um ideal de A, ideal este gerado por $a_1, \ldots, a_s$. É claro que $a_i \in I(a_1, \ldots, a_s)$ para todo $i = 1, \ldots, s$.

Um ideal I de um anel A que é da forma $I(a)$ para algum $a \in A$ será chamado de *ideal principal*.

Lema 4.2.1. *Dados um ideal J de A e $a_1, \ldots, a_s \in A$, temos que*

$$I(a_1, \ldots, a_s) \subset J \quad \textit{se, e somente se,} \quad a_1, \ldots, a_s \in J.$$

Demonstração ($\Rightarrow$) Como $a_1, \ldots, a_s \in I(a_1, \ldots, a_s) \subset J$, segue-se que $a_1, \ldots, a_s \in J$.

($\Leftarrow$) Suponha que $a_1, \ldots, a_s \in J$. Como J é um ideal de A, temos que $n_1 \cdot a_1 + \cdots + n_s \cdot a_s \in J$ para todos os $n_1, \ldots, n_s$ em A, logo $I(a_1, \ldots, a_s) \subset J$. □

Note que o Lema 4.2.1 nos diz que $I(a_1, \ldots, a_s)$ é o menor ideal de A que contém $\{a_1, \ldots, a_s\}$.

Lema 4.2.2. *Sejam* $a_1, \ldots, a_s \in A$. *Valem as seguintes igualdades:*

i) $I(a_1, \ldots, a_s, 0) = I(a_1, \ldots, a_s)$;

ii) $I(a_1, \ldots, a_i, \ldots, a_j, \ldots, a_s) = I(a_1, \ldots, a_j, \ldots, a_i, \ldots, a_s)$;

iii) *Quaisquer que sejam* $u_1, \ldots, u_s$, *elementos invertíveis de* A,

$$I(u_1 \cdot a_1, \ldots, u_s \cdot a_s) = I(a_1, \ldots, a_s);$$

iv) *Para todo* t *em* A,

$$I(a_1, \ldots, a_{s-1}, a_s) = I(a_1, \ldots, a_{s-1}, a_s - t \cdot a_{s-1}).$$

Demonstração (i) e (ii) são imediatas.
(iii) Em vista do Lema 4.2.1, basta mostrar que $u_1 \cdot a_1, \ldots, u_s \cdot a_s$ pertencem a $I(a_1, \ldots, a_s)$, o que é óbvio; e que $a_1, \ldots, a_s$ pertencem a $I(u_1 \cdot a_1, \ldots, u_s \cdot a_s)$, o que decorre das igualdades

$$a_i = 1 \cdot a_i = (u_i^{-1} \cdot u_i) \cdot a_i = u_i^{-1} \cdot (u_i \cdot a_i),$$

e do fato de que o último membro destas igualdades pertence a $I(u_1 \cdot a_1, \ldots, u_s \cdot a_s)$.
(iv) Pelo Lema 4.2.1 é claro que

$$I(a_1, \ldots, a_{s-1}, a_s - t \cdot a_{s-1}) \subset I(a_1, \ldots, a_{s-1}, a_s).$$

Por outro lado,

$$a_s = (a_s - t \cdot a_{s-1}) + t \cdot a_{s-1} \in I(a_1, \ldots, a_{s-1}, a_s - t \cdot a_{s-1}),$$

e a outra inclusão decorre novamente do Lema 4.2.1. □

Exemplos Seja $A = \mathbb{Z}$. Aplicando o Lema 4.2.2 repetidas vezes, temos

1) $I(2,3) = I(2, 3 - 1 \cdot 2) = I(2,1) = I(1, 2 - 2 \cdot 1) = I(1,0) = I(1) = \mathbb{Z}$.

2) $I(4,6) = I(4, 6{-}4{\cdot}1) = I(4,2) = I(2,4) = I(2, 4{-}2{\cdot}2) = I(2,0) = I(2)$.

3) $I(a,b) = I(-a,b) = I(a,-b) = I(-a,-b) = I(|a|,|b|)$.

A variedade dos tipos de ideais de um anel, de certo modo, mede a complexidade do anel. O anel dos inteiros é bastante simples desse ponto

de vista, como mostra o seguinte teorema, consequência da existência da divisão euclidiana em $\mathbb{Z}$.

Teorema 4.2.3. *Dado um ideal* $I \neq (0)$ *de* $\mathbb{Z}$*, temos que* $I = I(d)$*, onde* $d = \min(I \cap \mathbb{N} \setminus \{0\})$.

Demonstração Seja $I \neq (0)$ um ideal de $\mathbb{Z}$. O conjunto $I \cap \mathbb{N} \setminus \{0\}$ é não vazio. De fato, existe $a \neq 0$ em I, como a e $-a$ são elementos de I, segue-se que $I \cap \mathbb{N} \setminus \{0\} \neq \emptyset$. Como $I \cap \mathbb{N} \setminus \{0\}$ é limitado inferiormente, pelo Princípio de Boa Ordenação, ele admite um menor elemento d. Vamos agora provar que $I = I(d)$.

É claro, pelo Lema 4.2.1, que $I(d) \subset I$. Por outro lado, seja x um elemento de I. Pela divisão euclidiana em $\mathbb{Z}$, existem q e r em $\mathbb{Z}$ tais que $x = d \cdot q + r$ com $0 \leq r < d$. Suponha que $r \neq 0$, logo $r = x - d \cdot q \in I \cap \mathbb{N} \setminus \{0\}$, o que contradiz o fato de d ser o menor elemento de $I \cap \mathbb{N} \setminus \{0\}$ e, portanto, $r = 0$. Consequentemente, $x = d \cdot q \in I(d)$, o que prova que $I \subset I(d)$. Está portanto provado que $I = I(d)$. □

Um domínio de integridade A tal que todo ideal é principal é chamado de *domínio principal*. O teorema acima nos diz que $\mathbb{Z}$ é um domínio principal. Esse teorema é um típico teorema de existência, não fornecendo nenhum método para o cálculo do gerador d do ideal. O cálculo efetivo de d será abordado no próximo capítulo.

Proposição 4.2.4. *Sejam* A *um anel e* a *e* b *elementos de* A*. Valem as seguinte afirmações:*

i) $I(a) = I(b)$ *se, e somente se,* $a \mid b$ *e* $b \mid a$.

ii) *Se* A *é um domínio de integridade, então* $I(a) = I(b)$ *se, e somente se,* a *e* b *são associados.*

iii) *Suponha* $A = \mathbb{Z}$*. Temos que* $I(a) = I(b)$ *se, e somente se,* $a = \pm b$.

Demonstração (i) Do Lema 4.2.1 temos que $I(b) \subset I(a)$ e $I(a) \subset I(b)$ se, e somente se, $b \in I(a)$ e $a \in I(b)$ e isto por sua vez é equivalente a $a \mid b$ e $b \mid a$.

(ii) Essa afirmação decorre de (i) e da Proposição 4.1.2.

(iii) Essa afirmação decorre de (ii) e do fato que os elementos invertíveis de $\mathbb{Z}$ são 1 e -1 (veja Proposição 2.1.9). □

Segue-se do Teorema 4.2.3 e do item (iii) da Proposição 4.2.4, que todo ideal não nulo de $\mathbb{Z}$ tem exatamente dois possíveis geradores, um positivo e outro negativo.

O gerador positivo ou nulo do ideal $I(a_1, \ldots, a_s)$ será simbolizado por $(a_1, \ldots, a_s)$.

Proposição 4.2.5. *Sejam* A *um anel e* $a_1, \ldots, a_s$ *elementos de* A. *Se* $d \in A$ *é tal que* $I(a_1, \ldots, a_s) = I(d)$, *então* d *é um* mdc *de* $a_1, \ldots, a_s$.

Demonstração Temos por hipótese que $I(a_1, \ldots, a_s) = I(d)$, logo $a_i \in I(d)$, $i = 1, \ldots, s$, e, portanto, $d \mid a_1, \ldots, d \mid a_s$.

Suponha agora que c seja um divisor de $a_1, \ldots, a_s$, logo $I(d) = I(a_1, \ldots, a_s) \subset I(c)$, portanto $d \in I(c)$ e, consequentemente, $c \mid d$.

Isto prova que d é um mdc de $a_1, \ldots, a_s$. □

A proposição acima admite os seguintes corolários cujas demonstrações são imediatas e por isso serão omitidas.

Corolário 4.2.6. *Sejam* A *um domínio principal e* $a_1, \ldots, a_s$ *elementos de* A. *Então existe um* mdc *destes elementos e todo* mdc *é da forma* $n_1 \cdot a_1 + \cdots + n_s \cdot a_s$ *para alguns elementos* $n_1, \ldots, n_s \in A$.

Dois elementos de um anel A são ditos *primos entre si*, se os únicos divisores comuns destes elementos são os elementos invertíveis de A.

Quando A é um domínio principal, dois elementos a e b são primos entre si se e somente se a e b possuem um mdc invertível.

Corolário 4.2.7. *Seja* A *é um domínio principal. Os elementos* a *e* b *de* A *são primos entre si se e somente se existem* $n, m \in A$ *tais que* $na + mb = 1$.

Corolário 4.2.8. *Dados* $a_1, \ldots, a_s \in \mathbb{Z}$, *não todos nulos, existe um* mdc *destes elementos e temos que* mdc $(a_1, \ldots, a_s) = (a_1, \ldots, a_s)$.

A seguir, utilizaremos indistintamente em $\mathbb{Z}$ as notações mdc $(a_1, \ldots, a_s)$ e $(a_1, \ldots, a_s)$.

Problemas

2.1 Sejam A um anel e I um ideal de A. Mostre que:

a) $I = A$ se, e somente se, I contém um elemento invertível de A.

b) A é um corpo se, e somente se, os seus únicos ideais são (0) e A.

2.2 Supondo $A = \mathbb{Z}$ e $n \in \mathbb{Z}$, mostre que:

a) $I(2, 3) = \mathbb{Z}$ b) $I(n, n + 1) = \mathbb{Z}$ c) $I(n, n^2 + 1) = \mathbb{Z}$

2.3 Mostre que todo subconjunto não vazio I de $\mathbb{Z}$, fechado para a subtração, é um ideal.

Sugestão: Para mostrar que $n \cdot a \in I$ para todo n em $\mathbb{N}$ e a em I, use indução matemática.

2.4 Sejam a, b, a', b', m, n, r e s inteiros tais que $m \cdot s - n \cdot r = \pm 1$, $a' = m \cdot a + n \cdot b$ e $b' = r \cdot a + s \cdot b$, mostre que $I(a, b) = I(a', b')$.

2.5 Sejam I e J ideais de um anel A. Mostre que:

a) $I \cap J$ é um ideal de A.

b) $I + J = \{x + y\,;\ x \in I, y \in J\}$ é um ideal de A.

c) $I + J = I$ se, e somente se, $J \subset I$.

2.6 Mostre que se $a_1, \ldots, a_s \in \mathbb{Z}$, então:

a) $I(a_1, \ldots, a_s) = I(a_1) + \cdots + I(a_s)$.

b) $(a_1, \ldots, a_{s-2}, a_{s-1}, a_s) = (a_1, \ldots, a_{s-2}, (a_{s-1}, a_s))$.

Observação: Esta última fórmula permite calcular o mdc de vários inteiros iteradamente, sabendo calcular o mdc de dois elementos.

2.7 Seja $(I_n)_{n\in\mathbb{N}}$ uma família de ideais de um anel A. Mostre que:

a) $\bigcap_{n\in\mathbb{N}} I_n$ é um ideal de A.

b) Se $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$, então $\bigcup_{n\in\mathbb{N}} I_n$ é um ideal de A.

2.8 Sejam A um anel e $a_1, \ldots, a_s$ elementos não nulos de A. Mostre que se o ideal $I(a_1) \cap \cdots \cap I(a_s)$ (veja Problema 2.7 (a)) é gerado por um elemento m de A, então m é um mmc de $a_1, \ldots, a_s$. Conclua que num domínio principal, sempre existe um mmc de dados elementos. Mostre que se $A = \mathbb{Z}$, então

$$\mathrm{mmc}(a_1, \ldots, a_s) = \min(I(a_1) \cap \cdots \cap I(a_s) \cap \mathbb{N} \setminus \{0\}).$$

2.9 Sejam $a_1, \ldots, a_s$ e n inteiros. Mostre que

$$(n \cdot a_1, \ldots, n \cdot a_s) = |n| \cdot (a_1, \ldots, a_s).$$

3 Fatoração

Um elemento não nulo e não invertível de um anel é dito *irredutível* se os seus únicos divisores são os elementos invertíveis do anel e os seus próprios associados. Um elemento não irredutível será dito *redutível*. Note que todo associado de um elemento irredutível (respectivamente, redutível) é também irredutível (respectivamente, redutível).

Exemplos

1. O número 2 é irredutível em $\mathbb{Z}$, pois os seus únicos divisores são ± 1 e ± 2.

2. O número 4 não é irredutível em $\mathbb{Z}$ pois $2 \mid 4$ e 2 não é invertível nem associado de 4.

O lema a seguir será útil na demonstração da próxima proposição.

Lema 4.3.1. *Num domínio principal* A*, toda cadeia ascendente de ideais*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$$

é estacionária; isto é, existe um índice m *tal que*

$$I_m = I_{m+1} = \cdots$$

Demonstração Verifica-se facilmente que

$$\bigcup_{j \geq 1} I_j$$

é um ideal de A (veja Problema 2.7). Como A é um domínio principal, existe $a \in A$ tal que

$$\bigcup_{j \geq 1} I_j = I(a).$$

Segue-se daí que

$$a \in \bigcup_{j \geq 1} I_j$$

e, portanto, $a \in I_m$ para algum m. Logo, $a \in I_n$ para todo $n \geq m$ e, consequentemente, $I(a) \subset I_n$ para todo $n \geq m$. Como para todo n, temos que

$$I_n \subset \bigcup_{j \geq 1} I_j = I(a),$$

segue-se que $I_n = I(a)$ para todo $n \geq m$. □

Proposição 4.3.2. *Todo elemento não nulo e não invertível de um domínio principal possui pelo menos um divisor irredutível.*

Demonstração Sejam A um domínio principal e a um elemento de A não nulo e não invertível. Se a é irredutível, nada temos a provar. Suponha agora que a seja redutível, logo pela definição, a tem um divisor a_1 que não é invertível nem associado de a. Portanto,

$$I(a) \subsetneqq I(a_1) \subsetneqq A,$$

onde $I(a) \neq I(a_1)$ pois a e a_1 não são associados (veja Proposição 4.2.4, (ii)) e $I(a_1) \neq A$ pois a_1 é não invertível (justifique).

Se a_1 é irredutível, o resultado fica estabelecido. Se a_1 é redutível, ele possui um divisor a_2 que não é invertível nem é associado de a_1. Logo, temos que

$$I(a) \subsetneqq I(a_1) \subsetneqq I(a_2) \subsetneqq A.$$

E assim, sucessivamente, até que, ou para algum n tenhamos que a_n é irredutível e, portanto, é um divisor irredutível de a; ou tenhamos uma cadeia infinita de ideais:

$$I(a) \subsetneqq I(a_1) \subsetneqq I(a_2) \subsetneqq \cdots \subsetneqq I(a_n) \subsetneqq \cdots,$$

o que não é possível tendo em vista o Lema 4.3.1. □

Um domínio de integridade A é um *domínio de fatoração única* (DFU), se todo elemento não nulo e não invertível de A se fatora como produto de um número finito de elementos irredutíveis. Além disso, tal fatoração é única a menos da ordem dos fatores e de elementos associados, isto é, se $p_1, \ldots, p_n$, $q_1, \ldots, q_m$ são elementos irredutíveis de A e se

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

então $n = m$ e após um reordenamento de $q_1, \ldots, q_n$, se necessário, temos que p_i e q_i são associados para todo $i = 1, \ldots, n$.

Todo corpo, por ter todos os seus elementos não nulos invertíveis, é um DFU (pela vacuidade da condição de fatoração).

Um elemento a não nulo e não invertível de um anel A é dito *primo*, se toda vez que a divide o produto de dois elementos de A, ele divide um dos fatores. Vê-se facilmente que se a é primo, então todo associado de a é primo.

Exemplos

1. O número 2 é primo em $\mathbb{Z}$. De fato, se $2 \mid b \cdot c$, então b ou c tem que ser par (pois o produto de dois números ímpares é ímpar).

2. O número 3 é primo em $\mathbb{Z}$. De fato, suponha que $3 \mid b \cdot c$. Dividindo b e c por 3 temos que

$$b = 3q_1 + r_1\,, \quad c = 3q_2 + r_2\,,$$

com $0 \leq r_1 < 3$ e $0 \leq r_2 < 3$. Logo

$$b \cdot c = 3(3q_1 \cdot q_2 + q_1 \cdot r_2 + q_2 \cdot r_1) + r_1 \cdot r_2\,,$$

portanto, $3 \mid r_1 \cdot r_2$. Isto implica, em face das desigualdades acima envolvendo r_1 e r_2, que $r_1 \cdot r_2 = 0$, ou seja, $3 \mid b$ ou $3 \mid c$.

3. O número 4 não é primo em $\mathbb{Z}$ pois $4 \mid 2 \cdot 6$ e no entanto, temos que $4 \nmid 2$ e $4 \nmid 6$.

A relação entre elementos primos e irredutíveis é dada nas três proposições a seguir.

Proposição 4.3.3. *Num domínio de integridade, todo elemento primo é irredutível.*

Demonstração Seja p um elemento primo de um domínio A e suponha que para algum $a \in A$ tenhamos $a \mid p$. Queremos provar que a é invertível ou que a é um associado de p.

Com efeito, se $a \mid p$, então $p = a \cdot b$ para algum b. Logo $p \mid a \cdot b$ e como p é primo, temos que $p \mid a$ ou $p \mid b$. Suponhamos inicialmente que $p \mid a$. Como por hipótese $a \mid p$, segue-se da Proposição 4.1.2 que a é um associado de p. Em seguida suponhamos que $p \mid b$. Da igualdade $p = a \cdot b$, segue-se que $b \mid p$, logo pela Proposição 4.1.2, existe u invertível tal que $p = u \cdot b$. Segue-se então que $u \cdot b = p = a \cdot b$ e portanto, pela lei do cancelamento, tem-se que $a = u$ e, consequentemente, a é invertível. □

Corolário 4.3.4. *Sejam $p, p_1, \ldots, p_n$ elementos primos de um domínio de integridade. Se $p \mid p_1 \ldots p_n$, então p é associado de p_i para algum $i = 1, \ldots, n$.*

Demonstração Se $p \mid p_1 \cdots p_n$, então pela definição de elemento primo, juntamente com um argumento simples de indução, segue-se que $p \mid p_i$

para algum $i = 1, \ldots, n$. Agora, como p_i é primo, pela proposição acima ele é irredutível e como $p \mid p_i$ e p não é invertível (por ser primo), segue-se que p é associado de p_i. □

A recíproca da Proposição 4.3.3 nem sempre é verdadeira. Veremos no Volume 2 exemplos de anéis onde nem todo elemento irredutível é primo. Entretanto, o resultado pode valer com hipóteses adicionais como se poderá ver na próxima proposição.

Proposição 4.3.5. *Num domínio principal, todo elemento irredutível é primo.*

Demonstração Seja p um elemento irredutível de um domínio principal A. Suponha que $p \mid a \cdot b$ e que $p \nmid a$, vamos provar que $p \mid b$.

Com efeito, sendo A principal, existe $c \in A$ tal que $I(a, p) = I(c)$, logo $c \mid a$ e $c \mid p$. Como os únicos divisores de p são os elementos invertíveis de A e os associados de p, segue-se que c é associado de p ou c é invertível. Note que c não é associado de p pois se fosse, teríamos $p \mid c$ e como $c \mid a$, seguiria então que $p \mid a$, o que é uma contradição. Temos portanto que c é invertível e, consequentemente (veja Problema 2.1),

$$I(a, p) = I(c) = A.$$

Segue-se daí que existem elementos m e n em A tais que

$$1 = n \cdot a + m \cdot p.$$

Multiplicando por b ambos os membros da igualdade acima, temos que

$$b = n \cdot a \cdot b + m \cdot p \cdot b,$$

e como $p \mid a \cdot b$, segue-se que $p \mid b$, como queríamos demonstrar. □

Proposição 4.3.6. *Em $\mathbb{Z}$ um elemento é primo se, e somente se, ele é irredutível.*

Demonstração Isto decorre das Proposições 4.3.3 e 4.3.5 e do fato de $\mathbb{Z}$ ser domínio principal (Teorema 4.2.3). □

Teorema 4.3.7. *Todo domínio principal é domínio de fatoração única.*

Demonstração Sejam A um domínio principal e a um elemento não nulo e não invertível de A. Pela Proposição 4.3.2, o elemento a tem pelo menos um divisor irredutível p_1, logo existe $a_1 \neq 0$ tal que

$$a = a_1 \cdot p_1.$$

Se a_1 não é invertível, então ele possui um divisor irredutível p_2, logo

$$a = a_2 \cdot p_2 \cdot p_1 .$$

Assim, sucessivamente, determinando uma sequência de pares de elementos (a_i, p_i) com os p_i irredutíveis e tais que $a_i = a_{i+1} \cdot p_{i+1}$. Vamos mostrar que este procedimento tem que parar após um número finito de passos, isto é, para algum n temos que a_n é invertível.

Com efeito, se nenhum dos elementos $a_1, \ldots, a_n, \ldots$ fosse invertível, teríamos para todo i que $a_{i+1} \mid a_i$ e a_i não é associado de a_{i+1}, logo teríamos a seguinte cadeia infinita

$$I(a) \subsetneqq I(a_1) \subsetneqq I(a_2) \subsetneqq \cdots \subsetneqq I(a_n) \subsetneqq \cdots ,$$

o que é absurdo em vista do Lema 4.3.1. Portanto, para algum n temos que a_n é invertível. Pondo $a_n = u$, temos que

$$a = p_1 \cdots p_{n-1} \cdot (up_n)$$

com $p_1, \ldots, p_{n-1}$, up_n irredutíveis (portanto, pela Proposição 4.3.5, também primos).

Provaremos agora, por indução sobre n, a unicidade de tal escrita. Suponha que $n = 1$ e que

$$p_1 = q_1 \cdots q_m ,$$

com $p_1, q_1, \ldots, q_m$ irredutíveis (e portanto primos). Como da equação acima decorre que $p_1 \mid q_1 \cdots q_m$, pelo Corolário 4.3.4 temos que p_1 é associado de q_i para algum i. Reordenando os q_j, se necessário, podemos supor que $i = 1$, logo $p_1 = w \cdot q_1$, onde w é invertível. Se $m > 1$, seguiria que

$$w = q_2 \cdots q_m ,$$

o que é impossível pois nenhum elemento irredutível pode dividir um elemento invertível (justifique). Portanto $m = 1$ e p_1 é associado de q_1.

Suponha agora a unicidade válida para $n - 1$ e suponha que

$$p_1 \cdots p_n = q_1 \cdots q_m ,$$

com $p_1, \ldots, p_n$ e $q_1, \ldots, q_m$ irredutíveis, logo primos. Segue-se que $p_n \mid q_1 \cdots q_m$ e novamente, pelo Corolário 4.3.4, temos para algum i

que p_n e q_i são associados. Novamente, a menos da reordenação dos q_j podemos supor que $i = m$ e portanto $p_n = w \cdot q_m$ com w invertível. Segue-se então que

$$w \cdot p_1 \cdots p_{n-1} = q_1 \cdot q_{m-1} .$$

Pela hipótese de indução segue-se que $n - 1 = m - 1$, portanto $n = m$, e após reordenação dos q_j , se necessário, temos que cada p_i é associado de q_i para todo $i = 1, \ldots, n-1$. Como já mostramos acima que p_n e q_n são associados, fica demonstrada a unicidade no nível n. □

Corolário 4.3.8. *O anel $\mathbb{Z}$ dos inteiros é um Domínio de Fatoração Única.*

Corolário 4.3.9 (Teorema Fundamental da Aritmética). *Todo inteiro $a \neq 0$, ± 1, pode ser escrito sob a forma*

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n} ,$$

com os p_i números primos positivos distintos e os α_i inteiros positivos. Além disso, esta escrita é única a menos da ordem dos fatores.

Dados dois inteiros quaisquer a e b podemos representá-los do seguinte modo

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n} , \quad b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n} ,$$

com $p_1, \ldots, p_n$ primos positivos distintos mas com $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ inteiros positivos ou nulos. Nesta representação poderíamos facilmente mostrar (veja Problema 3.9) que

$$\text{mdc } (a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} ,$$

com $\gamma_1 = \min\{\alpha_i, \beta_i\}$, $i = 1, \ldots, n$, e que

$$\text{mmc } (a, b) = p_1^{\delta_1} \cdots p_n^{\delta_n} ,$$

com $\delta_i = \max\{\alpha_i, \beta_i\}$, $i = 1, \ldots, n$.

Neste contexto, temos que, se

$$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n} \quad \text{e} \quad b = \pm q_1^{\beta_1} \cdots q_m^{\beta_m}$$

com $p_1, \ldots, p_n$ primos positivos distintos, $q_1, \ldots, q_m$ primos positivos distintos e $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_m$ inteiros positivos, então a e b são primos entre si se, e somente se, $p_i \neq q_j$ para todo i e j.

O seguinte resultado é importante.

Proposição 4.3.10. *Todo número racional não nulo se escreve de modo único na forma* $\frac{a}{b}$ *com* a *e* b *primos entre si e* $b > 0$.

Demonstração Represente o número racional como $\frac{a'}{b'}$ com a' e b' inteiros e $b' \neq 0$. Se b' é negativo, transfira o seu sinal para o numerador. Decomponha a' e b' em produtos de primos e simplifique os seus fatores comuns, daí resulta que $\frac{a'}{b'} = \frac{a}{b}$ com $b > 0$ e a e b primos entre si. □

Proposição 4.3.11. *O "número"* $\sqrt{2}$ *não é racional.*

Demonstração Suponha por absurdo que $\sqrt{2} = \frac{a}{b}$ com a e b inteiros primos entre si. Desta equação, elevando ambos os membros ao quadrado, obtemos que

$$2b^2 = a^2.$$

Segue-se daí que $2 \mid a^2$ e como 2 é primo, devemos ter $2 \mid a$ e portanto $a = 2 \cdot c$ para algum inteiro c. Temos então que

$$2b^2 = a^2 = 4 \cdot c^2,$$

logo $b^2 = 2c^2$ e portanto $2 \mid b^2$ e, consequentemente, $2 \mid b$. Temos portanto que $2 \mid a$ e $2 \mid b$, o que é uma contradição pois a e b são primos entre si. □

A Proposição 4.3.11, com a demonstração que apresentamos, encontra-se nos *Elementos* de Euclides. Os gregos antigos haviam portanto detectado a existência de "números"que não são racionais. No Capítulo 8 construiremos o corpo dos números reais $\mathbb{R}$ como extensão do corpo $\mathbb{Q}$ dos números racionais onde $\sqrt{2}$ terá o seu lugar.

Problemas

3.1 Mostre que num DFU todo elemento irredutível é primo.

3.2 Sejam A um DFU e a, b e c elementos de A. Suponha a e b primos entre si. Mostre que:

a) Se $a \mid b \cdot c$, então $a \mid c$; b) Se $a \mid c$ e $b \mid c$, então $a \cdot b \mid c$.

3.3 Sejam A um domínio principal e a e b elementos de A não ambos nulos. Mostre que são equivalentes as afirmações:

i) a e b são primos entre si.

ii) a e b possuem um mdc invertível.

iii) $I(a, b) = A$;

iv) Existem elementos m e n de A tais que $m \cdot a + n \cdot b = 1$.

3.4 Se a e b são inteiros não ambos nulos, mostre que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

3.5 Sejam a, b e c inteiros e m e n naturais. Mostre que:

i) Se $(a, c) = 1$, então $(a \cdot b, c) = (b, c)$.

ii) Se $(a, b) = 1$, então $(a^m, b^n) = 1$.

3.6 Sejam m e n inteiros positivos. Mostre que se $\sqrt[n]{m}$ não é inteiro, então ele é irracional.

3.7 Mostre que se a é um inteiro positivo que não é uma potência de 10, então $\log_{10} a$ é irracional.

3.8 Sejam b e m inteiros com $m > 1$.

i) Mostre que na sequência $b, 2b, \ldots, mb$ há exatamente (m, b) números divisíveis por m.

ii) Se $(m, b) = 1$, mostre que os restos da divisão de $b, 2b, \ldots, mb$ por m são os números $0, 1, \ldots, m - 1$, em alguma ordem.

iii) Se $(m, b) = 1$, mostre que de m termos consecutivos quaisquer de uma progressão aritmética de razão b, um e somente um desses termos é divisível por m.

3.9 Sejam A um DFU, $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = vp_1^{\beta_1} \cdots p_n^{\beta_n}$ com u e v invertíveis, os p_i irredutíveis dois a dois não associados e $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ números naturais. Mostre que $p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ e $p_1^{\delta_1} \cdots p_n^{\delta_n}$ com $\gamma_i = \min\{\alpha_i, \beta_i\}$ e $\delta_i = \max\{\alpha_i, \beta_i\}$, para $i = 1, \ldots, n$, são respectivamente o mdc e o mmc de a e b.

3.10 Sejam A um DFU e a e b elementos não nulos de A. Sejam d um mdc e m um mmc de a e b. Mostre que os elementos $m \cdot d$ e $a \cdot b$ são associados. Mostre que em $\mathbb{Z}$ vale a relação

$$\text{mmc } (a, b) = \frac{|a \cdot b|}{\text{mdc } (a, b)} \cdot$$

3.11 Seja p um número primo positivo. Mostre que todo número racional não nulo x se escreve de modo único na forma

$$x = p^n \cdot \frac{a}{b},$$

com $a, b, n \in \mathbb{Z}$, $b > 0$ e $(a, b) = (a, p) = (b, p) = 1$. Define-se o *valor absoluto* p*-ádico* como se segue:

$$|0|_p = 0 \quad \text{e} \quad |x|_p = \frac{1}{p^n}.$$

Mostre que para todo $x, y \in \mathbb{Q}$ e $n \in \mathbb{Z}$ tem-se que:

i) $|x \cdot y|_p = |x|_p \cdot |y|_p$.

ii) $|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$.

iii) $|n|_p \leq 1$.

5

Aritmética dos inteiros

Em Matemática, há vários tipos de teoremas de existência. Alguns destes teoremas são de natureza construtiva, isto é, a demonstração da existência de um determinado objeto matemático consiste em exibir um algoritmo que permite, pelo menos em teoria, calculá-lo. Outros, são de natureza mais conceitual, apenas garantindo a existência e eventualmente caracterizando o objeto mas não fornecendo nenhum método para calculá-lo.

O capítulo anterior contém vários resultados deste último tipo. Por exemplo, o Teorema 4.2.3 garante que todo ideal de $\mathbb{Z}$ pode ser gerado por um único elemento e que ainda este elemento pode ser caracterizado como o mínimo de um determinado conjunto, mas a demonstração deste teorema não nos fornece nenhuma indicação de como este elementto pode ser calculado. Este último tipo de prova tornou-se muito popular desde o final do século dezenove e um dos argumentos a seu favor até muito recentemente era de que mesmo de posse de um algoritmo, a complexidade dos cálculos pode tornar a execução do mesmo impraticável. Com o desenvolvimento recente da Ciência da Computação, aumentando a nossa capacidade computacional, voltou naturalmente o interesse pelos algoritmos.

No presente capítulo, estudaremos algumas propriedades específicas dos inteiros, chamadas de propriedades aritméticas, dando ênfase aos aspectos computacionais. Inicialmente, discutiremos algumas questões relativas à distribuição dos números primos que nos conduzem rapida-

mente a problemas muito difíceis ou a questões ainda em aberto. Em seguida, descrevemos o algoritmo de Euclides para o cálculo efetivo do mdc de dois inteiros. Este algoritmo, apesar de sua venerável idade, continua sendo um dos mais eficientes do ponto de vista computacional para o cálculo do mdc. A questão da eficiência ou "custo" de um determinado algoritmo é central em Computação Científica, pois o seu sucesso é função da rapidez com a qual uma máquina pode efetuar os cálculos. Finalmente, mostramos como se resolvem certas equações envolvendo inteiros usando o algoritmo de Euclides.

1 Números primos

Tivemos oportunidade no capítulo anterior de verificar que os números primos são, do ponto de vista da divisibilidade, os mais simples, pois são irredutíveis, e pelo Teorema Fundamental da Aritmética são suficientes para gerar todos os inteiros diferentes de 0 e ± 1 por meio de multiplicações. A primeira pergunta natural que surge é, quantos são os números primos? A resposta foi dada por Euclides nos Elementos e é a seguinte

Teorema 5.1.1 (Euclides). *Em $\mathbb{Z}$ existem infinitos números primos.*

Demonstração Suponhamos por absurdo que os números primos sejam em número finito. Seja p o maior número primo positivo e considere o número a formado pelo produto de todos os primos positivos diminuído de 1, portanto

$$a = (2 \cdot 3 \cdots p) - 1. \tag{1}$$

Como $a \neq 0, \pm 1$, pelas Proposições 4.3.2 e 4.3.6, temos que a possui um divisor primo q, que podemos supor positivo. Como q é um número primo positivo, ele é um dos fatores de $2 \cdot 3 \cdots p$, logo de (1) segue-se que $p \mid (-1)$, o que é absurdo. □

O teorema acima é um típico teorema de existência, não nos dando nenhum método para determinar números primos. O problema de determinar números primos continua sem solução satisfatória.

Damos a seguir um método bem antigo para a elaboração de tabelas de números primos até a ordem que se desejar. O método é conhecido pelo nome de *Crivo de Eratóstenes* e se baseia no resultado a seguir.

Lema 5.1.2. *Se um número inteiro* n *maior do que* 1 *não é divisível por nenhum primo positivo* p *tal que* $p^2 \leq n$*, então ele é primo.*

Demonstração Suponha por absurdo que n não é primo e seja q o menor número primo positivo que divide n (q existe em virtude das Proposições 4.3.2 e 4.3.6 e do princípio da boa ordenação em $\mathbb{Z}$). Temos então que

$$n = q \cdot m \quad \text{com} \quad q \leq m,$$

logo,

$$q^2 \leq q \cdot m = n.$$

Portanto, n é divisível por um número primo positivo q tal que $q^2 \leq n$, absurdo. □

Vamos agora elaborar a tabela (Tabela 1) dos números primos positivos inferiores a 250. Para isso, escrevamos todos os inteiros de 1 a 250. Riscaremos de modo sistemático todos os inteiros compostos, isto é, os inteiros não primos, que figuram nesta tabela seguindo o roteiro abaixo.

i) 2 é primo, risque todos os números pares maiores do que 2 pois não são primos;

ii) Todos os números não riscados inferiores a 4, isto é, o número 3, são primos. Risque todos os múltiplos de 3 maiores do que 3 pois não são primos;

iii) Todos os números não riscados inferiores a 9, pelo Lema 5.1.2, são primos, estes são, $2, 3, 5$ e 7. Risque todos os seus múltiplos que ainda não foram riscados;

iv) Todos os números não riscados inferiores a $7^2 = 49$ são primos, estes são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47. Risque todos os seus múltiplos que ainda não foram riscados;

v) Como $47^2 > 250$, todos os números não riscados na tabela são primos.

O Crivo de Eratóstenes tem um custo computacional muito elevado tornando-se por isto um método inviável na prática. Até o momento continuamos sem métodos eficazes para elaborar tabelas de números primos.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230
231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250

Tabela 1 - Os números primos positivos menores do que 250

As duas proposições seguintes caracterizarão certos números primos famosos.

Proposição 5.1.3. *Sejam* a *e* n *inteiros maiores do que* 1. *Se* $a^n - 1$ *é primo, então* $a = 2$ *e* n *é primo.*

Demonstração Suponha que $a^n - 1$ seja primo. Como $a \neq 1$, temos que $(a-1) \mid (a^n-1)$ (veja Problema 1.8 (a), Capítulo 4), logo $a-1 = \pm 1$ ou $a - 1 = \pm(a^n - 1)$. Segue-se daí que a única possibilidade é $a = 2$.

Suponha agora que n não seja primo, logo $n = n_1 \cdot n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Como $2^{n_1} - 1$ divide $2^n - 1 = (2^{n_1})^{n_2} - 1$ (veja Problema 1.8 (a), Capítulo 4) e $1 < 2^{n_1} - 1 < 2^n - 1$, segue-se que $2^n - 1$ não é primo. □

Os números primos da forma

$$M_p = 2^p - 1,$$

com p primo positivo são chamados de *números de Mersenne* em homenagem a Marin Mersenne (1588-1648) que se interessou pelo problema de determinar números primos p para os quais M_p é um número primo. Mersenne calculou alguns destes primos. No intervalo $2 \leq p \leq 5000$ os números de Mersenne correspondem aos seguintes valores de p: 2, 3, 5, 7, 3, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423.

Proposição 5.1.4. *Sejam* a *e* n *inteiros maiores do que* 1. *Se* $a^n + 1$ *é primo, então* a *é par e* $n = 2^m$ *com* $m \in \mathbb{N}$.

Demonstração Suponha que a^n+1 seja primo. Segue-se que a tem que ser par pois, caso contrário, teríamos que $2 \mid (a^n + 1)$ e $a^n + 1 > 2$, que é absurdo. Escreva agora $n = 2^m \cdot r$ com $m, r \in \mathbb{N}$, e $2 \nmid r$. Queremos provar que $r = 1$. Sendo r ímpar, segue-se que $a^{2^m}+1$ divide $a^n+1 = (a^{2^m})^r+1$ (veja Problema 1.8 (b), Capítulo 4). Como estamos supondo $a^n + 1$ primo, isto só é possível se $a^{2^m}+1 = a^n+1$, logo $r = 1$, como queríamos demonstrar. □

Os números da forma

$$F_m = 2^{2^m} + 1,$$

com $m \in \mathbb{N}$ são chamados de números de Fermat, em homenagem a Pierre de Fermat (1601-1655). Fermat havia conjecturado que F_m era primo para todo $m \geq 0$. Leonhard Euler (1707-1783) mostrou que $F_5 = 2^{32} + 1 = 4.294.967.297$ é divisível por 641, derrubando assim a conjectura de Fermat (veja Problema 1.15, Capítulo 6).

Problemas

1.1 Considere a função $\nu\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $a \mapsto \nu(a)$, onde $\nu(a)$ é o número de divisores positivos de a. Mostre que:

i) Para todo $a \in \mathbb{Z} \setminus \{0\}$, tem-se que $\nu(-a) = \nu(a)$.

ii) Se $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ com $p_1, \dots, p_n$ primos distintos e $\alpha_1, \dots, \alpha_n$ inteiros positivos, então $\nu(a) = (\alpha_1 + 1) \cdots (\alpha_n + 1)$.

iii) Se $a, b \in \mathbb{Z} \setminus \{0\}$ com $(a, b) = 1$, então $\nu(a \cdot b) = \nu(a) \cdot \nu(b)$.

1.2 Mostre que um inteiro positivo a é um quadrado perfeito se, e somente se, $\nu(a)$ é ímpar.

1.3 Qual é a expressão geral dos números inteiros que admitem um número primo de divisores positivos?

1.4 Seja p um número primo positivo. Mostre que:

i) Se $i \in \mathbb{N}$ é tal que $1 \leq i < p$, então $\binom{p}{i}$ é divisível por p.

ii) Se $a, b \in \mathbb{Z}$, então p divide $(a+b)^p - (a^p + b^p)$.

iii) Para todo $a \in \mathbb{Z}$, tem-se $p \mid (a^p - a)$.

iv) Se $a, b \in \mathbb{Z}$, então ou $a^p - b^p$ é primo com p ou $p^2 \mid (a^p - b^p)$.

Sugestão para (iii): Demonstre o resultado por indução sobre a. Este resultado é chamado de *Pequeno Teorema de Fermat*.

1.5 Mostre que para $n \in \mathbb{N}$, não são primos os números

i) $2^{4n+2} + 1$ ii) $8^n + 1$

iii) $2^{4n+2} - 1$ iv) $8^{n+1} - 1$

1.6 Sejam a, m e n inteiros tais que $m > n \geq 0$.

i) Mostre que $a^{2n} + 1$ divide $a^{2^m} - 1$.

ii) Mostre que

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & , \text{ se } a \text{ é par} \\ 2 & , \text{ se } a \text{ é ímpar} \end{cases}$$

iii) Como aplicação de (ii) deduza que $(F_n, F_m) = 1$. Mostre com isto que existem infinitos números primos.

iv) Mostre que $2^{2^m} - 1$ tem pelo menos m divisores primos positivos distintos.

v) Mostre que se p_n representa o n-ésimo número primo positivo, então

$$p_{n+1} \leq F_n = 2^{2^n} + 1.$$

2 Distribuição dos números primos

Com os números primos estão relacionados alguns dos problemas mais famosos da Matemática. Alguns destes problemas ainda não foram resolvidos enquanto que outros só foram resolvidos com a utilização de

técnicas matemáticas sofisticadas de áreas como a Álgebra, a Análise Real e a Análise Complexa.

Consultando a Tabela 1, note que existem vários pares de números primos que diferem de duas unidades, como por exemplo $(3,5)$, $(5,7)$, $(11,13)$, $(41,43)$, $(107,109)$, $(239,241)$, entre outros. Pares de primos como estes são chamados de *primos gêmeos*. Até o presente momento ainda não se sabe se os primos gêmeos são em número finito ou infinito, enquanto que o problema análogo para ternas de primos trigêmeos é de fácil resolução (veja o Problema 2.1).

A distribuição dos números primos é tão irregular que dois primos consecutivos podem ser gêmeos ou, dado um natural n arbitrário, podem diferir por um número maior do que n, como decorre da observação de que não são primos os números

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

Por outro lado, um resultado chamado de *Postulado de Bertrand*, conjecturado por Bertrand em 1845 e demonstrado por Chebichev em 1852, afirma que dado um inteiro positivo n, existe sempre um número primo entre n e $2n$. Este é um dos poucos resultados sobre números primos que tem uma demonstração elementar. O leitor interessado neste assunto está convidado a consultar o livro de LeVeque listado na literatura.

Um famoso resultado sobre números primos, diz respeito à função $\pi\colon \mathbb{N} \to \mathbb{N}$, definida por $\pi(n) =$ *número de primos positivos menores ou iguais a* n. O Teorema de Euclides (Teorema 4.2.3) nos diz que

$$\lim_{n\to\infty} \pi(n) = \infty,$$

e o problema que vinha desafiando os matemáticos, desde o tempo de Gauss, era comparar o crescimento da função π com o crescimento de funções conhecidas. Consultando tabelas de primos pode-se ver que a função π assume valores bastante irregulares e que os números primos são esparsos em $\mathbb{N}$, isto é, dado um inteiro positivo n, a probabilidade de um número inteiro entre 1 e n ser um número primo, medida pelo número $\pi(n)/n$, se torna pequena à medida que n aumenta. A partir da tabela dos primos menores do que 102.000 publicada por J. Lambert, Gauss determinou empiricamente algo equivalente à seguinte relação:

$$\frac{\pi(n)}{n} \sim \frac{1}{L(n)},$$

onde $L(n)$ significa o logaritmo Neperiano de n e onde o símbolo $f(n) \sim g(n)$ significa que

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

O primeiro passo na direção da demonstração deste resultado foi dado por Chebichev em 1852, que demonstrou de modo elementar que existem números reais positivos a e b próximos de 1 com $a < 1$ e $b > 1$, tais que

$$\frac{a}{L(n)} < \frac{\pi(n)}{n} < \frac{b}{L(n)}.$$

A relação de Gauss foi demonstrada em 1896 independentemente por J. Hadamard e C. de La Vallée Poussin, utilizando técnicas de cálculo diferencial e integral. Este resultado constitui-se num importante e difícil teorema de Teoria dos Números, chamado de *Teorema dos Números Primos* e que foi redemonstrado em 1949 por A. Selberg com a utilização de métodos algébricos.

Outro resultado profundo sobre números primos, devido a Dirichlet, provado em 1837 usando técnicas de análise e cuja demonstração está também além do nível deste texto, é o seguinte:

Teorema (Dirichlet). *Dados* a *e* r *inteiros positivos primos entre si, existe pelo menos um número primo na progressão aritmética de primeiro termo* a *e razão* r.

Problemas

2.1 Mostre que $(3, 5, 7)$ é a única terna de primos trigêmeos.

Sugestão Mostre que, dado n, um dos números n, $n+2$ ou $n+4$ é divisível por 3.

2.2 Assumindo o Postulado de Bertrand mostre que para $n > 1$, o n-ésimo número primo positivo p_n satisfaz a desigualdade $p_n < 2^n$.

2.3 Usando a desigualdade de Chebichev mostre que

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0.$$

2.4 Usando o teorema dos números primos calcule valores aproximados para $\pi(10^5)$ e para $\pi(10^7)$. Compare os valores obtidos com os seguintes valores exatos: $\pi(10^5) = 9592$ e $\pi(10^7) = 664579$.

2.5 Mostre usando o teorema de Dirichlet que se a e r são inteiros primos entre si, então na progressão aritmética de primeiro termo a e razão r existem infinitos números primos. O que acontece quando a e r não são primos entre si?

2.6 Prove que existem infinitos números primos da forma $4n + 3$.

Sugestão (i) mostre que todo primo $p \geq 3$ é da forma $4n+1$ ou $4n+3$; (ii) mostre que o produto de dois números da forma $4n + 1$ é da mesma forma; (iii) suponha por absurdo que p_k é o último primo positivo da forma $4n + 3$. Considere o número $n = 4(7 \cdot 11 \cdots p_k) + 3$, mostre que ele deveria ser também da forma $4n + 1$ o que é absurdo.

3 Algoritmo de Euclides

Nesta seção apresentaremos o *Algoritmo de Euclides* que permite calcular efetivamente o máximo divisor comum de dois inteiros. Este método encontra-se nos *Elementos de Euclides* (Livro VII, Proposição 2) e nos permitirá também calcular o mdc de vários inteiros (veja o Problema 3.3).

Recorde que dados inteiros a e b, temos que mdc $(a, b) = (a, b)$, onde (a, b) representa o gerador positivo de $I(a, b)$. O seguinte lema nos será útil

Lema 5.3.1. *Sejam* a, b *e* m *inteiros. Temos então que* $(a, 0) = |a|$ *e que*

$$(a, b) = (b, a) = (|a|, |b|) = (a - mb, b).$$

Demonstração As afirmações decorrem das seguintes igualdades que se obtêm usando o Lema 4.2.2: $I(a, 0) = I(|a|)$ e

$$I(a, b) = I(b, a) = I(|a|, |b|) = I(a - mb, b).$$

□

Para calcular (a, b), tendo em vista o lema acima, podemos supor que a e b são não negativos. Se $b = 0$ ou $a = b$, então $(a, b) = a$, nada tendo que calcular. Suponhamos que $a \neq b$, como $(a, b) = (b, a)$, podemos finalmente supor que $a > b > 0$.

Pela divisão euclidiana, temos que

$$a = b \cdot q_1 + r_2\,, \quad 0 \leq r_2 < b.$$

Da igualdade acima e do Lema 5.3.1 segue-se que

$$(a, b) = (a - b \cdot q_1, b) = (r_2, b) = (b, r_2).$$

Dois casos podem se apresentar:

1) $r_2 = 0$. Neste caso, temos $(a, b) = (b, r_2) = (b, 0) = b$.

2) $r_2 \neq 0$. Neste caso efetuamos a divisão euclidiana de b por r_2, obtendo
$$b = r_2 \cdot q_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Argumentando como acima, segue-se que $(a, b) = (b, r_2) = (r_2, r_3)$. Novamente, dois casos podem se apresentar

1′) $r_3 = 0$. Neste caso, $(a, b) = (r_2, 0) = r_2$;

2′) $r_3 \neq 0$. Neste caso efetuamos a divisão euclidiana r_2 por r_3, obtendo
$$r_2 = r_3 \cdot q_3 + r_4, \quad 0 \leq r_4 < r_3.$$

Novamente, procedendo como acima, temos que

$$(a, b) = (b, r_2) = (r_2, r_3) = (r_3, r_4),$$

e assim sucessivamente.

Definindo $r_1 = b$, segue-se da argumentação acima que existe um valor de n tal que $r_{n+1} = 0$ e $r_n \neq 0$. De fato, se para todo n, tivessemos $r_n \neq 0$, teríamos uma sequência infinita $r_1, r_2, r_3, \ldots$ tal que

$$r_1 > r_2 > r_3 > \cdots > 0,$$

contrariando o Princípio da Boa Ordenação.

Segue-se então que

$$(a, b) = (b, r_2) = \cdots = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

Portanto, o último resto não nulo r_n neste processo nos fornece o valor de (a, b).

Note que o procedimento acima é uma outra demonstração, desta vez construtiva, da existência de mdc em $\mathbb{Z}$.

Calcularemos efetivamente o número (a, b) com a ajuda do seguinte dispositivo prático que decorre imediatamente do procedimento acima que chamamos de *Algoritmo de Euclides*:

	q_1	q_2	q_3	...	q_{n-2}	q_{n-1}	q_n
a	b	r_2	r_3	...	r_{n-2}	r_{n-1}	r_n
r_2	r_3	r_4	r_5	...	r_n	0	

Exemplos

1. Calculemos $(330, 240)$.

	1	2	1	2
330	240	90	60	30
90	60	30	0	

$(330, 240) = 30$.

2. Calculemos $(484, 1521)$.

	3	7	69
1521	484	69	1
69	1	0	

$(484, 1521) = 1$.

Como, em particular, $(a, b) \in I(a, b)$, existem inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$. O algoritmo de Euclides usado de trás para frente permite calcular tais inteiros m_0 e n_0. De fato, considere as seguintes igualdades:

$$\begin{array}{ll}
(1) & r_n = r_{n-2} - q_{n-1} \cdot r_{n-1} \\
(2) & r_{n-1} = r_{n-3} - q_{n-2} \cdot r_{n-2} \\
(3) & r_{n-2} = r_{n-4} - q_{n-3} \cdot r_{n-3} \\
\vdots & \vdots \\
(n-2) & r_3 = b - q_2 \cdot r_2 \\
(n-1) & r_2 = a - q_1 \cdot b.
\end{array}$$

Substituindo o valor de r_{n-1} de (2) em (1), obtemos

$$r_n = (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-2} - q_{n-1} \cdot r_{n-3}\,,$$

substituindo nesta igualdade o valor de r_{n-2} de (3), obtemos

$$r_n = -(q_{n-3} + q_{n-1} \cdot q_{n-2} \cdot q_{n-3} + q_{n-1}) \cdot r_{n-3} + (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-4}\,.$$

Assim, sucessivamente, até obter no final os inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$.

3. No Exemplo 1, acima, temos

$$\begin{aligned} 30 &= 90 - 1 \cdot 60 \\ 60 &= 240 - 2 \cdot 90 \\ 90 &= 330 - 1 \cdot 240 \end{aligned}$$

Efetuando as substituições mencionadas acima, temos:

$$\begin{aligned} 30 &= 90 - 1 \cdot (240 - 2 \cdot 90) = 3 \cdot 90 - 240 \\ &= 3 \cdot (330 - 240) - 240 = 3 \cdot 330 - 4 \cdot 240 \end{aligned}$$

Logo $m_0 = 3$ e $n_0 = -4$.

4. No Exemplo 2, acima, temos

$$\begin{aligned} 1 &= 484 - 7 \cdot 69 \\ 69 &= 1521 - 3 \cdot 484 \end{aligned}$$

Fazendo substituições sucessivas, temos:

$$1 = 484 - 7 \cdot 69 = 484 - 7 \cdot (1521 - 3 \cdot 484) = 22 \cdot 484 - 7 \cdot 1521.$$

Logo, $m_0 = 22$ e $n_0 = -7$.

O algoritmo de Euclides é um dos primeiros exemplos na história da Matemática de método de cálculo recursivo. Este método por ser um importante instrumento de cálculo em computação, ganhou nos nossos dias maior destaque. O leitor, a título de exercício, poderá escrever um programa na linguagem de sua preferência para calcular o número (a, b) e os inteiros m_0 e n_0 tais que $(a, b) = m_0 \cdot a + n_0 \cdot b$.

Uma questão muito importante para os interessados nos aspectos computacionais é a eficiência ou o custo de um dado algoritmo. Vejamos agora qual é o custo do algoritmo de Euclides.

Na demonstração do próximo teorema utilizaremos o fato da função logaritmo na base 2 ser monótona crescente e a seguinte desigualdade simples de verificar:

$$\forall m \in \mathbb{N}, \qquad \left[\frac{m}{2}\right] \geq \frac{m}{2} - \frac{1}{2}.$$

Teorema 5.3.2. *O número de iterações no algoritmo de Euclides para calcular o* mdc *de dois inteiros positivos* a *e* b *com* $a > b$*, é inferior a* $2(1 + \log_2 b)$.

Demonstração O algoritmo de Euclides se escreve

$$\begin{aligned}
a &= bq_1 + r_2, && 0 \le r_2 < b \\
b &= r_2q_2 + r_3, && 0 \le r_3 < r_2 \\
r_2 &= r_3q_3 + r_4, && 0 \le r_4 < r_3 \\
&\vdots \\
r_{n-1} &= r_nq_n + r_{n+1}\ , && r_{n+1} = 0
\end{aligned}$$

Pela Observação 3.2.3, temos, para $i = 1, 2, \ldots, n-1$, que

$$r_{i+2} < \frac{r_i}{2}\,,$$

onde colocamos $r_1 = b$. Logo,

$$1 \le r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{2^2} < \cdots < \frac{r_{n-2\left[\frac{n-1}{2}\right]}}{2^{\left[\frac{n-1}{2}\right]}} \le \frac{b}{2^{\left[\frac{n-1}{2}\right]}}\,.$$

Portanto,

$$2^{\left[\frac{n-1}{2}\right]} < b,$$

e, consequentemente,

$$\left[\frac{n-1}{2}\right] < \log_2 b.$$

Como $\left[\frac{n-1}{2}\right] \ge \frac{n-1}{2} - \frac{1}{2}$, segue-se que

$$n < 2(1 + \log_2 b).$$

Como n é o número de iterações para calcular o mdc, o resultado está provado. □

Com um pouco mais de trabalho, é possível mostrar que o número de iterações é de fato não superior a $5\log_{10} b$.

Um resultado curioso relacionado com a noção de mdc é o seguinte teorema de Cesaro demonstrado em 1881 e que apenas enunciamos

Teorema (Cesaro). *Se* a *e* b *são inteiros positivos escolhidos ao acaso, então a probabilidade de que* $(a, b) = 1$ *é* $6/\pi^2$ (*aproximadamente* 61%).

Problemas

3.1 Para cada par de inteiros a e b dados abaixo ache os inteiros (a, b), e mmc (a, b) além de inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$.

i) $637, 3887$ ii) $648, -1218$

iii) $-551, -874$ v) $7325, 8485$

3.2 Dado um inteiro n, positivo em (iii), mostre que:

i) $(n, 2n+1) = 1$ ii) $(2n+1, 3n+1) = 1$ iii) $(n!+1, (n+1)!+1) = 1$

3.3 Calcule $(325, 275, 450)$.

Sugestão Use o resultado do Problema 2.6 (b), Capítulo 4 e o Algoritmo de Euclides.

3.4 Sejam $a \in \mathbb{Z} \setminus \{-1, 1\}$ e $m, n \in \mathbb{N}$ e seja $d = (m, n)$. Mostre que

$$(a^m - 1, a^n - 1) = a^d - 1.$$

4 Equações Diofantinas

Diofanto viveu presumivelmente no século III em Alexandria, já sob o domínio de Roma. Foi praticamente o único matemático de renome na Grécia antiga que se dedicou predominantemente à teoria dos números. Interessou-se por uma grande variedade de equações para as quais procurava soluções racionais e eventualmente inteiras.

O tratamento algébrico dado por Diofanto à teoria dos números difere do de seus predecessores que utilizavam métodos geométricos para deduzir as suas asserções.

Hoje chamam-se de *Equações Diofantinas* às equações polinomiais com coeficientes inteiros (para as quais só se está interessado em soluções inteiras ou racionais).

As equações Diofantinas das quais nos ocuparemos aqui são de um tipo especial, a saber, são da forma $ax + by = n$, com a, b e n inteiros.

Dada uma tal equação, é natural formular as seguintes perguntas:

a) Sob quais condições a equação admite soluções?

b) Quando existem soluções, como determiná-las?

Os próximos dois teoremas nos darão respostas a essas perguntas.

Teorema 5.4.1. *A equação* $ax + by = n$ *admite solução se, e somente se,* $(a, b) \mid n$.

Demonstração Suponha que a equação admita uma solução x_0, y_0, isto é, $a \cdot x_0 + b \cdot y_0 = n$. Como (a, b) divide a e divide b, segue-se que divide $a \cdot x_0 + b \cdot y_0 = n$.

Reciprocamente, suponha que $(a, b) \mid n$. Então existe um inteiro t tal que $n = t \cdot (a, b)$. Como existem inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$, segue-se que $n = t \cdot (a, b) = (t \cdot m_0) \cdot a + (t \cdot n_0) \cdot b$. Logo os inteiros $x_0 = t \cdot m_o$ e $y_0 = t \cdot n_0$ são uma solução da equação. □

Teorema 5.4.2. *Seja* x_0, y_0 *uma solução particular da equação* $ax + by = n$. *Tem-se que* x, y *é uma solução da equação se, e somente se,*

$$x = x_0 + t \cdot \frac{b}{(a, b)} \quad e \quad y = y_0 - t \cdot \frac{a}{(a, b)},$$

para algum t *em* $\mathbb{Z}$.

Demonstração Substituindo x e y da forma acima, na equação, vê-se facilmente que se trata de uma solução.

Reciprocamente, se $a = 0$ e $b = 0$, é claro que toda solução é da forma acima.

Suponha $a \cdot b \neq 0$ e x, y é uma solução, então

$$n = a \cdot x + b \cdot y = a \cdot x_0 + b \cdot y_0 .$$

Decorre daí que

$$a \cdot (x - x_0) = b \cdot (y_0 - y). \tag{1}$$

Portanto,

$$\frac{a}{(a, b)} \cdot (x - x_0) = \frac{b}{(a, b)} \cdot (y_0 - y).$$

Como $(a/(a, b), b/(a, b)) = 1$ (veja Problema 3.4, Capítulo 4), segue-se que $(a/(a, b)) \mid (y_0 - y)$ e $(b/(a, b)) \mid (x - x_0)$. Portanto, existem inteiros m e t tais que $y_0 - y = t \cdot (a/(a, b))$ e $x - x_0 = m \cdot (b/(a, b))$. Substituindo esses valores em (1), obtém-se $m = t$, logo

$$x = x_0 + t \cdot \frac{b}{(a, b)} \quad e \quad y = y_0 - t \cdot \frac{a}{(a, b)}.$$

□

Segue-se do teorema que se a equação admite uma solução, ela admitirá uma infinidade de soluções. Qualquer uma destas soluções determina todas as outras.

Para determinar uma solução particular da equação, quando a e b são números pequenos, procede-se por inspeção. Se não for possível por este método achar uma solução, o método a seguir é efetivo.

Ache com o algoritmo de Euclides inteiros m_0 e n_0 tais que $m_0 \cdot a + n_0 \cdot b = (a, b)$. Multiplique ambos os lados desta igualdade por $n/(a, b)$, obtendo $(n/(a, b)) \cdot m_0 \cdot a + (n/(a, b)) \cdot n_0 \cdot b = n$. Portanto $x_0 = (n/(a, b)) \cdot m_0$ e $y_0 = (n/(a, b)) \cdot n_0$ é uma solução particular da equação.

Exemplos

1. A equação $9x = 12y = 1$ não admite solução pois $(9, 12) = 3$ e $3 \nmid 1$.

2. Resolvamos a equação $28x + 90y = 22$. Inicialmente temos que calcular $(18, 90)$.

	3	4	1	2
90	28	6	4	2
6	4	2	0	

Visto que $(18, 90) = 2$ e $2 \mid 22$, a equação admite soluções. Usando o algoritmo de trás para frente, temos

$$\begin{aligned} 2 &= 666 - 1 \cdot 4 \\ 4 &= 28 - 4 \cdot 6 \\ 6 &= 90 - 3 \cdot 28 \end{aligned}$$

Segue-se que

$$\begin{aligned} 2 = 6 - 1 \cdot (28 - 4 \cdot 6) &= (-1) \cdot 28 + 5 \cdot 6 \\ &= (-1) \cdot 28 + 5 \cdot (90 - 3 \cdot 28) \\ &= (-16) \cdot 28 + 5 \cdot 90 \end{aligned}$$

Logo, $2 = (-16) \cdot 28 + 5 \cdot 90$.

Multiplicando ambos os membros desta igualdade por 11, temos

$$22 = (-176) \cdot 28 + 55 \cdot 99.$$

Portanto, uma solução particular da equação é dada por $(x_0, y_0) = (-176, 55)$. Pelo Teorema 4, a solução geral é

$$x = -176 + t \cdot 45 \quad \text{e} \quad y = 55 - t \cdot 14, \quad t \in \mathbb{Z}.$$

A equação $ax + by = n$ foi resolvida pelo matemático hindú, Brahmagupta, do século VII.

Muitas outras equações Diofantinas foram estudadas. Algumas, como, por exemplo, as que consideramos, resolvem-se utilizando métodos ele-mentares, outras requerem métodos mais sofisticados. Uma equação estudada desde a antiguidade, é a *equação pitagórica*:

$$x^2 + y^2 = z^2.$$

Esta equação, que será estudada no Volume 2, possui infinitas soluções e existem fórmulas que permitem gerar todas elas. Pierre de Fermat afirmou, sem dar uma demonstração, que a equação

$$x^n + y^n = z^n,$$

para $n > 2$, não admitia soluções em inteiros positivos. Esta afirmação chama-se impropriamente de o *Último Teorema de Fermat* .

Observe também que os Teoremas 5.4.1 e 5.4.2 são válidos no contexto mais geral dos domínios principais.

Problemas

4.1 Resolva as equações:

a) $7x - 9y = 1$ b) $4x - 3y = 2$ c) $6x + 4y = 3$
d) $6x + 4y = 6$ e) $12x - 18y = 360$ f) $144x + 125y = 329$
g) $36x - 21y = 31$ h) $350x - 91y = 731$

4.2 Dada a equação $ax + by = n$ com a e b positivos, mostre que o número de soluções positivas desta equação é no máximo finito.

4.3 Sejam $a, b, c, d, n, m \in \mathbb{Z}$ com $D = a \cdot d - b \cdot c \neq 0$. Mostre que o sistema de equações simultâneas

$$\begin{cases} ax + by = n \\ cx + cy = m \end{cases}$$

admite solução se, e somente se, D divide $n \cdot d - m \cdot b$ e $m \cdot a - n \cdot c$. Neste caso, o sistema admite uma única solução. Determine esta solução.

4.4 Mostre que a equação $a_1x_1+\cdots+a_nx_n = b$ com $a_1,\ldots,a_n,\ b \in \mathbb{Z}$, admite solução em inteiros se, e somente se, $(a_1,\ldots,a_n) \mid b$.

5 O despertar da Aritmética

Após os trabalhos de Diofanto seguiram-se muitos séculos sem que a Aritmética registrasse um grande salto qualitativo do ponto de vista teórico. Houve, neste interim, a criação do sistema de numeração decimal posicional e a introdução do zero pelos hindús, a sua adoção pelos árabes e a sua utilização ainda que tardia na Europa. Durante este longo período foram aperfeiçoados os algoritmos para efetuar as operações, as frações e a Aritmética Financeira.

A Aritmética Teórica teve o seu despertar no século 17 por obra do jurista francês e matemático amador Pierre de Fermat (1601-1665). Fermat enunciou vários teoremas dos quais raramente dava as demonstrações. Muitas delas foram dadas posteriormente por outros matemáticos ficando porém em aberto até recentemente o já citado Último Teorema de Fermat.

Nas suas leituras de uma tradução da Aritmética de Diofanto, Fermat anotava as suas observações nas margens do livro. No seu comentário ao oitavo problema do segundo livro que trata da resolução da equação pitagórica $x^2 + y^2 = z^2$, Fermat escreveu:

> "*Ao contrário, é impossível separar um cubo em dois cubos, uma potência quarta em duas potências quartas, ou em geral, qualquer potência acima da segunda em duas potências do mesmo grau. Eu descobri uma demonstração verdadeiramente maravilhosa que esta margem é muito estreita para conter*".

Quase três séculos e meio se passsaram até que se tenha conseguido provar esta afirmação. Foram produzidas ao longo do tempo provas da veracidade da asserção para vários valores de n e inúmeras vezes foram anunciadas e publicadas falsas demonstrações do teorema.

Finalmente, em 1993 Andrew Wiles anunciou que havia demonstrado o Último Teorema de Fermat exibindo um manuscrito de cerca de 200 páginas contendo o que afirmava ser a demonstração do teorema. Foram necessários dois anos para que os especialistas analisassem este trabalho e que o próprio Wiles esclarecesse vários pontos para que a prova fosse

reconhecida como correta e completa. Foi assim vencido um dos maiores desafios da Matemática, sendo difícil acreditar que Fermat tivesse realmente a demosntração deste teorema.

Grande parte dos teoremas enunciados por Fermat foram posteriormente provados pelo matemático suíço Leonhard Euler (1707-1783). Euler teve uma produção científica fabulosa, tendo sido o matemático mais produtivo de todos os tempos. Estima-se que ao longo de 55 anos de atividades ele tenha escrito trabalhos que não caberiam em 80 grossos volumes. Esta produtividade sequer baixou nos últimos 17 anos de sua vida passados em estado de cegueira total.

Grandes matemáticos como Legendre, Gauss, Dirichlet, Dedekind, Riemann e Hilbert, só para citar alguns, contribuiram para o desenvolvimento posterior da Teoria dos Números, considerada por muitos a área mais nobre da Matemática.

6

Congruências

As congruências são o instrumento adequado quando se quer dar ênfase ao resto na divisão euclidiana. Elas foram introduzidas e extensivamente estudadas por Gauss no seu famoso *Disquisitiones Arithmeticae*, publicado em 1801. As noções introduzidas por Gauss e suas notações foram imediatamente adotadas pelos matemáticos da época e ainda são usadas atualmente. Este capítulo destina-se a introduzir a noção de congruência, apresentar as suas propriedades básicas e oferecer algumas aplicações.

1 Propriedades das congruências

Seja m um inteiro não nulo. Dois inteiros a e b serão ditos *congruentes módulo* m se os restos da divisão de a e b por m forem iguais. Quando a e b são congruentes módulo m, escrevemos $a \equiv b \bmod m$.

Exemplos $12 \equiv 17 \bmod 5$, $15 \equiv 0 \bmod 3$, $15 \equiv -1 \bmod 4$.

Note que $a \equiv b \bmod m$ se, e somente se, $a \equiv b \bmod(-m)$ pois de $a = m \cdot q + r$ e $b = m \cdot q' + r$ com $0 \leq r < |m|$, decorre que $a = (-m)(-q) + r$ e $b = (-m)(-q') + r$ com $0 \leq r < |-m|$ e vice-versa. Portanto, no que diz respeito aos restos, basta considerarmos congruências módulos inteiros positivos.

Como $a \equiv b \bmod 1$, quaisquer que sejam os inteiros a e b, é portanto sem interesse a noção de congruência neste caso. A seguir vamos sempre supor $m > 1$.

Dois números a e b não congruentes módulo m serão ditos *incongruentes* módulo m. Nesse caso, escreveremos $a \not\equiv b \bmod m$.

Uma maneira mais simples de verificar se dois números são congruentes é dada pela seguinte proposição.

Proposição 6.1.1. *Tem-se que* $a \equiv b \bmod m$ *se, e somente se,* m *divide* $a - b$.

Demonstração Se $a \equiv b \bmod m$, então existem inteiros r, q e q' tais que $a = m \cdot q + r$ e $b = m \cdot q' + r$, logo $a - b = m(q - q')$ e, consequentemente, $m \mid (a - b)$.

Reciprocamente, suponha que $m \mid (a - b)$. Pela divisão euclidiana, temos que $a = m \cdot q + r$ e $b = m \cdot q' + r'$ com $0 \leq r < m$ e $0 \leq r' < m$. Logo, $a - b = m(q - q') + r - r'$. Como $m \mid m(q - q')$, segue-se que $m \mid (r - r')$ e isto só é possível se $r = r'$, pois $|r - r'| < m$. Portanto, $a \equiv b \bmod m$. □

Proposição 6.1.2. *Sejam* a, b, c, d, m *e* n *inteiros com* $m > 1$ *e* $n \geq 1$. *Temos que:*

i) $a \equiv a \bmod m$ *;*

ii) *Se* $a \equiv b \bmod m$, *então* $b \equiv a \bmod m$ *;*

iii) *Se* $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$, *então* $a \equiv c \bmod m$ *;*

iv) *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $a + c \equiv b + d \bmod m$ *;*

v) *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $a \cdot c \equiv b \cdot d \bmod m$ *;*

vi) *Se* $a \equiv b \bmod m$, *então* $a^n \equiv b^n \bmod m$.

Demonstração (i) e (ii) são imediatas.
(iii) Se $a \equiv m \bmod m$ e $b \equiv c \bmod m$, então $m \mid (a - b)$ e $m \mid (b - c)$, logo $m \mid (a - b + b - c)$, donde $m \mid (a - c)$ e, portanto, $a \equiv c \bmod m$.
(iv) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, segue-se que $m \mid (a - b)$ e $m \mid (c - d)$, logo $m \mid (a - b + c - d)$ e, portanto, $a + c \equiv b + d \bmod m$.
(v) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, segue-se que $m \mid (a-b)$ e $m \mid (c-d)$. Como

$$ac - bd = a(c - d) + d(a - b),$$

segue-se que $m \mid (ac - bd)$ e, consequentemente, $ac \equiv bd \bmod m$.
(vi) Isto decorre de (v), por indução sobre n. □

As propriedades (i), (ii) e (iii) na proposição acima nos dizem que a relação de congruência módulo m em $\mathbb{Z}$ é uma relação de equiva-

lência, enquanto que as propriedades (iv) e (v) são de compatibilidade da relação com as operações de adição e multiplicação.

Vejamos agora alguns exemplos que nos revelarão a riqueza do campo de aplicações da noção de congruência.

Exemplos

1. Para achar o resto da divisão de a por m, basta achar um inteiro r tal que $a \equiv r \bmod m$ e $0 \leq r < m$. Para acharmos o resto da divisão de 2^{30} por 17, sem usar nenhum resultado especial, deveríamos calcular inicialmente o valor de 2^{30} para posteriormente dividí-lo por 17, o que representaria um trabalho considerável. Vejamos como a noção de congruência torna mais suave esta tarefa.

Note que $2^4 \equiv -1 \bmod 17$, elevando ambos os membros à potência 7 temos pela Proposição 6.1.2, (vi), que $2^{28} \equiv -1 \bmod 17$. Multiplicando ambos os membros desta igualdade por 4, pela Proposição 6.1.2 (v), segue-se que $2^{30} \equiv -4 \bmod 17$. Como $-4 \equiv 13 \bmod 17$, segue-se da Proposição 6.1.2 (iii), que $2^{30} \equiv 13 \bmod 17$. Concluímos com isto que o resto da divisão de 2^{30} por 17 é 13.

2. Critérios de divisibilidade por 2, 5 e 10.

Observe que $10 \equiv 0 \bmod 2$, $10 \equiv 0 \bmod 5$ e $10 \equiv 0 \bmod 10$. Consequentemente, para todo $i \in \mathbb{N} \setminus \{0\}$, temos que $10^i \equiv 0 \bmod 2$, $\bmod 5$ e $\bmod 10$. Se $a = a_n a_{n-1} \cdots a_2 a_1 a_0$ é um inteiro representado na base 10, temos que $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$, logo $a \equiv a_0 \bmod 2$, $\bmod 5$ e $\bmod 10$. Portanto, a é divisível por 10, por 5 ou por 2 se, e somente se, $a_0 \equiv 0 \bmod 10$, $\bmod 5$ ou $\bmod 2$, respectivamente.

Deduzimos daí os seguintes critérios, para números representados na base 10:

(a) Um número é divisível por 10 se, e somente se, o seu algarismo da unidade é zero;

(b) Um número é divisível por 5 se, e somente se, o seu algarismo da unidade é zero ou 5;

(c) Um número é divisível por 2 se, e somente se, o seu algarismo da unidade é par.

3. Critérios de divisibilidade por 9 e por 3.

De $10 \equiv 1 \bmod 9$ ou $\bmod 3$, segue-se da Proposição 6.1.2 (vi), que $10^i \equiv 1 \bmod 9$ ou $\bmod 3$ para todo $i \in \mathbb{N}$. Seja $a = a_n a_{n-1} \cdots a_1 a_0$ um inteiro positivo representado na base 10, temos então que

$$a \equiv a_0 + a_1 + \cdots + a_n \mod 9, \bmod 3.$$

Deduzimos daí os seguintes critérios:

Um inteiro é divisível por 9 (respectivamente por 3) se e somente se a soma dos algarismos de sua representação na base 10 for divisível por 9 (respectivamente por 3).

Na soma $a_0 + a_1 + \cdots + a_n$ cada parte igual a nove se elimina pois é congruente a zero módulo 9. Isto é a regra dos *noves fora*.

4. Neste exemplo discutimos a *prova dos nove*.

A *prova dos nove* é um teste para detectar erros nas quatro operações. A título de exemplo, vejamos como ela funciona no caso da multiplicação.

Sejam

$$\begin{aligned} a &= a_n a_{n-1} \cdots a_1 a_0\,, \\ b &= b_m b_{m-1} \cdots b_1 b_0\,, \text{ e} \\ c &= c_r c_{r-1} \cdots c_1 c_0\,, \end{aligned}$$

três inteiros representados na base 10 e suponha que se tenha efetuado a operação $a \cdot b = c$. Seja a' o valor de $a_0 + a_1 + \cdots + a_n$ após ter posto os noves fora, analogamente para b' e c'. Seja d' o valor de $a' \cdot b'$ após ter posto os noves fora, devemos então ter $c' = d'$. Se $d' \neq c'$, então certamente houve um erro na conta. Caso $d' = c'$, não podemos concluir que a conta esteja correta, mas ela se torna mais confiável por ter passado por um teste.

5. Critério de divisibilidade por 11.

Note que $10 \equiv -1 \bmod 11$, logo

$$10^i = \begin{cases} 1 \bmod 11 & , \quad \text{se} \quad i \text{ é par} \\ -1 \bmod 11 & , \quad \text{se} \quad i \text{ é ímpar} \end{cases}$$

Seja $a = a_n a_{n-1} \cdots a_1 a_0$ um número inteiro representado na base 10. Temos que

$$a = a_0 + a_1 \cdot 10 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n,$$

logo

$$a \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \bmod 11.$$

Deduzimos daí o seguinte critério:

Um inteiro é divisível por 11 se, e somente se, a diferença entre a soma dos algarismos de ordem par e a soma dos algarismos de ordem ímpar na sua representação decimal for divisível por 11.

Vejamos agora algumas propriedades das congruências relacionadas com a divisão.

Proposição 6.1.3. *Sejam* $a, b, c, m, n \in \mathbb{Z}$ *com* $m > 1$ *e* $n > 1$.

i) *Se* $a \equiv b \bmod m$ *e se* $n \mid m$, *então* $a \equiv b \bmod n$.

ii) $a \equiv b \bmod m$ *e* $a \equiv b \bmod n$ *se, e somente se,* $a \equiv b \bmod \operatorname{mmc}(m, n)$.

iii) *Se* $a \cdot c \equiv b \cdot c \bmod m$ *e* $(c, m) = 1$, *então* $a \equiv b \bmod m$.

iv) *Se* $d = (c, m)$, *então* $a \cdot c \equiv b \cdot c \bmod m$ *se, e somente se,* $a \equiv b \bmod \frac{m}{d}$.

Demonstração (i) Se $a \equiv b \bmod m$, então $m \mid (a - b)$ e como $n \mid m$, segue-se que $n \mid (a - b)$. Logo, $a \equiv b \bmod n$.
(ii) Se $a \equiv b \bmod m$ e $a \equiv b \bmod n$, temos que $m \mid (a - b)$ e $n \mid (a - b)$, logo pela definição de mmc temos que mmc $(m, n) \mid (a - b)$ e, portanto, $a \equiv b \bmod$ mmc (m, n).

Reciprocamente, se $a \equiv b \bmod$ mmc (m, n), temos de (i) que $a \equiv b \bmod m$ e $a \equiv b \bmod n$ pois $m \mid$ mmc (m, n) e $n \mid$ mmc (m, n).
(iii) Se $a \cdot c \equiv b \cdot \bmod m$, então $m \mid [c \cdot (a - b)]$ e como $(c, m) = 1$, segue-se que $m \mid (a - b)$ e, portanto, $a \equiv b \bmod m$.
(iv) Se $a \cdot c \equiv b \cdot c \bmod m$, segue-se que $m \mid [c \cdot (a - b)]$, donde $c \cdot (a - b) = t \cdot m$, para algum $t \in \mathbb{Z}$. Sendo $d = (c, m)$, temos que

$$\frac{c}{d} \cdot (a - b) = t \cdot \frac{m}{d},$$

com

$$\left(\frac{c}{d}, \frac{m}{d}\right) = 1.$$

Como

$$\frac{c}{d} \cdot a \equiv \frac{c}{d} \cdot b \bmod \frac{m}{d},$$

segue-se, de (iii) acima, que $a \equiv b \bmod \frac{m}{d}$.

Reciprocamente, sejam $c_0, m_0 \in \mathbb{Z}$ tais que $c = c_0 \cdot d$ e $m = m_0 \cdot d$. Por hipótese, $a \equiv b \bmod m_0$, logo $a - b = t \cdot m_0$ para algum $t \in \mathbb{Z}$. Portanto, $c\cdot(a-b) = t\cdot m_0\cdot c = t\cdot m_0\cdot c_0\cdot d = t\cdot c_0\cdot m$ e, consequentemente, $ac \equiv bc \bmod m$. □

Corolário 6.1.4. *Sejam* $a, b, m, m_1, \ldots, m_r$ *números inteiros, com* $m, m_1, \ldots, m_r > 1$. *Suponha que* $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ *seja a decomposição de* m *em fatores primos distintos. Temos que*

i) *Se* $a \equiv b \bmod m_i$, $i = 1, \ldots, r$, *então* $a \equiv b \bmod \operatorname{mmc}(m_1, \ldots, m_r)$.

ii) $a \equiv b \bmod m$ *se, e somente se,* $a \equiv b \bmod p_1^{\alpha_1}, \ldots, a \equiv b \bmod p_s^{\alpha_s}$.

iii) *Se* $a \equiv b \bmod p_i^{\alpha_i}$, *então* $a \equiv b \bmod p_i$.

Demonstração As demonstrações são imediatas e serão omitidas. □

Problemas

1.1 Verifique a veracidade ou falsidade das seguintes afirmações:

a) $7 \equiv 24 \bmod 5$ b) $33 \equiv 57 \bmod 6$

c) $529 \equiv -8 \bmod 3$ d) $-12 \equiv -72 \bmod 8$

1.2 Ache a solução geral e a menor solução positiva de cada uma das congruência abaixo:

a) $x \equiv 7 \bmod 3$ b) $x \equiv -1 \bmod 6$

c) $3x + 2 \equiv 0 \bmod 7$ d) $14x + 3 \equiv 0 \bmod 21$

1.3 Seja $n \in \mathbb{N}$, mostre que:

a) $19^{8n} - 1$ é divisível por 17 para todo n.

b) $13^{3n} + 17^{3n}$ é divisível por 45 para todo n ímpar.

1.4 Mostre que se $n \in \mathbb{N}$, o algarismo das unidades na representação na base 10 de 3^n só pode ser 1, 3, 7 e 9. Ache os algarimos das unidades 3^{400}, 3^{401}, 3^{402} e 3^{403}.

1.5 Ache, na base 10, critérios de divisibilidade por

a) 4, 25 e 100.

b) 8, 125 e 1000.

c) generalize.

1.6 Determine os algarismos x, y e z, em cada caso, para que os números abaixo, representados na base 10, tenham a propriedade mencionada.

a) $2x7y$ é divisível por 11 e por 4.

b) $28x75y$ é divisível por 3 e por 11.

c) $45xy$ é divisível por 4 e 9.

d) $13xy45z$ é divisível por 8, por 9 e por 11.

1.7 Mostre que, para que um número seja divisível por 6, é necessário e suficiente que na sua representação na base 10, a soma do algarismo da unidade com quatro vezes cada um dos outros algarismos seja divisível por 6.

1.8 Da igualdade $1001 = 7 \cdot 11 \cdot 13$, deduza os seguintes critérios de divisibilidade por 7, 11 e 13:

Dado $a = a_n a_{n-1} \cdots a_1 a_0$ *, escrito na base* 10*, então* a *é divisível por* 7*, por* 11 *ou por* 13 *se, e somente se,* $a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - \cdots$ *é divisível poor* 7 *por* 11 *ou por* 13*, respectivamente.*

1.9 Mostre que dado um número qualquer representado na base 10,

a) Se subtrairmos do número a soma dos seus algarismos, o resultado é divisível por 9 .

b) Se subtrairmos do número outro qualquer formado por uma permutação dos seus algarismos, o resultado é divisível por 9.

1.10 (**O Pequeno Teorema de Fermat**). Seja p um número primo positivo, mostre que:

a) Se a é um inteiro qualquer, então $a^p \equiv a \bmod p$.

b) Se a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \bmod p$.

Sugestão (Para (a)). Por indução sobre a ou, senão, veja Problema 1.4, Capítulo 5.

1.11 Ache o resto da divisão

a) de 11^{p-1} por p, se p é primo .

b) de 2^{100} por 11 .

Sugestão Use o Pequeno Teorema de Fermat.

1.12 Ache o menor inteiro positivo que deixa restos 5, 4, 3 e 2 quando dividido, respectivamente, por 6, 5, 4 e 3.

Sugestão Note que $5 \equiv -1 \bmod 6$, $4 \equiv -1 \bmod 5$, etc. Use então o item (ii) da Proposição 6.1.3.

1.13 Ache o menor múltiplo positivo de 7 que tem resto 1 quando dividido por 2, 3, 4, 5 e 6.

2 As classes residuais e a sua aritmética

Seja dado um inteiro $m > 1$. Define-se a *classe residual módulo* m do elemento a de $\mathbb{Z}$ como sendo a classe de equivalência de a segundo a relação de equivalência dada pela congruência módulo m:

$$[a] = \{x \in \mathbb{Z};\ x \equiv a \bmod m\}.$$

Exemplos

1. Seja $m = 2$. Então,

$[0] = \{x \in \mathbb{Z};\ x \equiv 0 \bmod 2\} = \{x \in \mathbb{Z};\ x \text{ é par}\}$, e

$[1] = \{x \in \mathbb{Z};\ x \equiv 1 \bmod 2\} = \{x \in \mathbb{Z};\ x \text{ é ímpar}\}$.

Temos também que $[a] = [0]$, se a é par e $[a] = [1]$, se a é ímpar.

2. Seja $n = 3$. Então

$$[0] = \{3\lambda;\ \lambda \in \mathbb{Z}\}$$
$$[1] = \{3\lambda + 1;\ \lambda \in \mathbb{Z}\}$$
$$[2] = \{3\lambda + 2;\ \lambda \in \mathbb{Z}\}$$

Tem-se que

$$a \in \begin{cases} [0] & , \text{ se } a \text{ é múltiplo de } 3 \\ [1] & , \text{ se } a \text{ tem resto } 1 \text{ quando dividido por } 3 \\ [2] & , \text{ se } a \text{ tem resto } 2 \text{ quando dividido por } 3 \end{cases}$$

As classes residuais, por serem classes de equivalência, possuem as propriedades expressas na Proposição 1.5.1, ou seja,

(i) $[a] = [b]$ se e somente se $a \equiv b \bmod m$;

(ii) Se $[a] \cap [b] \neq \emptyset$, então $[a] = [b]$;

(iii) $\bigcup_{a \in \mathbb{Z}} [a] = \mathbb{Z}$.

Recorde que um inteiro qualquer b tal que $[b] = [a]$ é dito *representante* da classe residual $[a]$.

Exemplos

1. Se $m = 2$, então qualquer inteiro par é representante da classe residual $[0]$ e qualquer inteiro ímpar é representantes da classe residual $[1]$.

2. Se $m = 3$, então qualquer múltiplo de 3 é representante da classe residual $[0]$. Temos que 1, 4, 7, 10, -2, -5, -8, -11, etc, são representantes da classe residual $[1]$, enquanto 2, 5, -1, -4, etc, são representantes da classe residual $[2]$.

Proposição 6.2.1. *Para cada* $a \in \mathbb{Z}$ *existe um, e somente um* $r \in \mathbb{Z}$, *com* $0 \leq r < m$, *tal que* $[a] = [r]$.

Demonstração Seja $a \in \mathbb{Z}$. Pela divisão euclidiana, existem dois únicos inteiros q e r, com $0 \leq r < m$, tais que $a = m \cdot q + r$. Portanto, é único o inteiro r tal que $0 \leq r < m$ e $a \equiv r \bmod m$. Consequentemente, é único o inteiro r tal que $0 \leq r < m$ e $[a] = [r]$. □

Corolário 6.2.2. *Existem exatamente* m *classes residuais módulo* m *distintas, a saber,* $[0], [1], \ldots, [m-1]$.

Um conjunto $\{a_1, \ldots, a_n\}$ é chamado de *sistema completo de resíduos módulo* m se para todo $a \in \mathbb{Z}$ existir um i, com $i = 0, \ldots, m$, tal que $a \equiv a_i \bmod m$.

Em outras palavras, $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo m se, e somente se, $[a_1], \ldots, [a_m]$ são as m classes residuais módulo m. Os conjuntos $\{0, 1, \ldots, m-1\}$ e $\{1, 2, \ldots, m\}$ são sistemas completos de resíduos módulo m. É fácil verificar que m inteiros formam um sistema completo de resíduos módulo m, se, e somente se, eles são dois a dois incongruentes módulo m.

O conjunto de todas as classes residuais módulo m é representado por $\mathbb{Z}_m$. Esse conjunto possui m elementos que podem ser representados por $[0], [1], \ldots, [m-1]$. Uma vantagem das classes residuais é que transformam a congruência $a \equiv b \bmod m$ na igualdade $[a] = [b]$.

Em $\mathbb{Z}_m$ definimos as seguintes operações:

Adição: $[a] + [b] = [a + b]$

Multiplicação: $[a] \cdot [b] = [a \cdot b]$

Note que, tendo sido definidas estas operações usando os representantes a e b para as classes residuais $[a]$ e $[b]$, respectivamente, temos que verificar que ao mudarmos os representantes das classes $[a]$ e $[b]$, não mudam os valores de $[a + b]$ e de $[a \cdot b]$. Para verificar que isto acontece, basta notar que se $a \equiv a' \bmod m$ e $b \equiv b' \bmod m$, então $[a + b] = [a' + b']$ e $[a \cdot b] = [a' \cdot b']$, o que se segue diretamente dos itens (iv) e (v) da Proposição 6.1.2.

As operações que acabamos de definir, acima, gozam das seguintes propriedades:

Propriedades da Adição

Para todos $[a], [b], [c] \in \mathbb{Z}_m$, temos

A_1) Associatividade $([a] + [b]) + [c] = [a] + ([b] + [c])$;

A_2) Comutatividade $[a] + [b] = [b] + [a]$;

A_3) Existência de zero $[a] + [0] = [a]$ para todo $[a] \in \mathbb{Z}_m$;

A_4) Existência de simétrico $[a] + [-a] = [0]$.

Propriedades da Multiplicação

Para todos $[a], [b], [c] \in \mathbb{Z}_m$, temos

M_1) Associatividade $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$;

M_2) Comutatividade $[a] \cdot [b] = [b] \cdot [a]$;

M_3) Existência de unidade $[a] \cdot [1] = [a]$.

AM) Distributividade $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$.

Todas estas propriedades são fáceis de verificar. Por exemplo, prova-se AM como se segue:

$$\begin{aligned}[a] \cdot ([b] + [c]) &= [a] \cdot [b + c] = [a \cdot (b + c)] \\ &= [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c]\end{aligned}$$

Portanto, $\mathbb{Z}_m$, com as operações acima, é um anel, chamado *anel das classes residuais módulo* m.

Por outro lado, como a aplicação

$$\begin{aligned}\psi \colon \mathbb{Z} &\longrightarrow \mathbb{Z}_m \\ a &\longmapsto [a]\end{aligned}$$

é claramente um homomorfismo de anéis, trata-se do homomorfismo característico ρ que definimos no Capítulo 3.

Exemplos

1. As tabelas da adição e da multiplicação em $\mathbb{Z}_2 = \{[0], [1]\}$ são

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

2. As tabelas da adição e da multiplicação em $\mathbb{Z}_3 = \{[0], [1], [2]\}$ são

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

3. Em $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ temos

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

É interessante notar que $\mathbb{Z}_4$ não é um domínio de integridade, pois $[2] \neq [0]$ e, no entanto, $[2] \cdot [2] = [0]$.

4. Em $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ temos

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Note que $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$, com as operações acima definidas, são corpos. A seguir, caracterizaremos os elementos invertíveis de $\mathbb{Z}_m$.

Proposição 6.2.3. *Um elemento* $[a] \in \mathbb{Z}_m$ *é invertível se, e somente se,* $(a, m) = 1$.

Demonstração Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a] \cdot [b] = [a \cdot b]$. Logo, $a \cdot b \equiv 1 \bmod m$, isto é, existe um inteiro t tal que $a \cdot b + t \cdot m = 1$ e, consequentemente, $(a, m) = 1$.

Reciprocamente, se $(a, m) = 1$, existem inteiros b e t tais que $a \cdot b + m \cdot t = 1$ e, consequentemente, $[1] = [a \cdot b + m \cdot t] = [a \cdot b] + [m \cdot t] = [a] \cdot [b] + [0] = [a] \cdot [b]$. Portanto, $[a]$ é invertível. □

Corolário 6.2.4. $\mathbb{Z}_m$ *é um corpo se, e somente se,* m *é primo.*

Demonstração Suponha por absurdo que $\mathbb{Z}_m$ é um corpo e m não é primo, então $m = m_1 \cdot m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$. Logo, $[0] = [m] = [m_1] \cdot [m_2]$ com $[m_1] \neq 0$ e $[m_2] \neq 0$, contradição.

Reciprocamente, suponha m primo. Como $(i, m) = 1$ para $i = 1, \ldots, m-1$, segue-se da Proposição 6.2.3 que $[1], [2], \ldots, [m-1]$ são invertíveis. Logo, $\mathbb{Z}_m$ é um corpo. □

A função aritmética definida a seguir desempenha um papel importante na teoria dos números:

$$\begin{array}{rccl} \Phi\colon & \mathbb{Z} \setminus \{0, \pm 1\} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \textit{número de inteiros positivos} \\ & & & \textit{menores do que } |n| \textit{ e primos com } n \end{array}$$

Esta função é chamada de *função* Φ *de Euler*. Pela Proposição 6.2.3, temos que $\Phi(n) =$ número de elementos invertíveis de $\mathbb{Z}_{|n|}$. Estudaremos esta função com mais detalhes na Seção 4.

Um conjunto $\{a_1, \ldots, a_{\Phi(m)}\} \subset \mathbb{Z}$ é chamado de *sistema reduzido de resíduos módulo* m se $[a_1], \ldots, [a_{\Phi(m)}]$ são os elementos invertíveis de $\mathbb{Z}_m$.

Sendo $\mathbb{Z}_m^*$ o conjunto dos elementos invertíveis de $\mathbb{Z}_m$, temos então que $\mathbb{Z}_m^* = \{[a_1], \ldots, [a_{\Phi(m)}]\}$, onde $\{a_1, \ldots, a_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulos m.

Recorde que $\mathbb{Z}_m^*$ é multiplicativamente fechado e que o inverso de todo elemento de $\mathbb{Z}_m^*$ é um elemento de $\mathbb{Z}_m^*$.

No caso em que p é primo, temos, pelo Corolário 6.2.4, que $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$. Sejam $[1], \ldots, [p-1]$ os elementos de $\mathbb{Z}_p^*$. Os elementos $[1]$ e $[-1]$ são os únicos elementos de $\mathbb{Z}_p^*$ que são auto-inversos, isto é, são as únicas soluções da equação $x^2 = [1]$. De fato, de $0 = x^2 - [1] = (x - [1])(x + [1])$, e do fato de $\mathbb{Z}_p$ ser um corpo, portanto um domínio de integridade, segue-se que $x - [1] = 0$ ou $x + [1] = 0$ e, consequentemente, $x = [1]$ ou $x = [-1]$.

Teorema 6.2.5 (Teorema de Wilson). *Se* p *é um número primo positivo, então* $(p-1)! \equiv -1 \bmod p$.

Demonstração No produto $[1] \cdot [2] \cdots [p-2] \cdot [p-1]$, em $\mathbb{Z}_p$, para cada fator diferente de $[1]$ e de $[-1] = [p-1]$, existe um fator distinto do mesmo que é o seu inverso, logo $[1] \cdot [2] \cdots [p-2] \cdot [p-1] = [1] \cdot [p-1] = [-1]$. Daí segue-se que $[(p-1)!] = [-1]$, donde $(p-1)! \equiv -1 \bmod p$. □

Problemas

2.1 Seja $\{a_1, \ldots, a_m\}$ um sistema completo de resíduos módulo m.

a) Mostre que se a é um inteiro, então $\{a_1 + a, \ldots, a_m + a\}$ é um sistema completo de resíduos módulo m.

b) Se $(a, m) = 1$, então $\{a \cdot a_1, \ldots, a \cdot a_m\}$ é um sistema completo de resíduos módulo m. Mostre que vale a recíproca.

c) Se p é primo e a um inteiro que não é múltiplo de p, mostre que $a^{p-1} \equiv 1 \bmod p$ (Pequeno Teorema de Fermat).

Sugestão Considere os dois sistemas completos de resíduos mod p: $\{0, 1, \ldots, p-1\}$ e $\{0, a \cdot 1, \ldots, a(p-1)\}$ e note que

$$1 \cdots (p-1) \equiv a^{p-1} \cdot 1 \cdots (p-1) \bmod p.$$

d) Mostre que se $(r, m) = 1$, então $\{a, a + r, \ldots, a + (m-1)r\}$ é um sistema completo de resíduos módulo m.

2.2 Construa as tabelas da adição e da multiplicação para $\mathbb{Z}_6$ e $\mathbb{Z}_7$.

2.3 Ache os elementos invertíveis de $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ e $\mathbb{Z}_9$.

2.4 Ache os inversos de

a) $[5]$ em $\mathbb{Z}_6$ b) $[3], [4]$ e $[5]$ em $\mathbb{Z}_7$

c) $[3], [5]$, e $[7]$ em $\mathbb{Z}_8$ d) $[5], [4]$ e $[8]$ em $\mathbb{Z}_9$

e) $[1951]$ em $\mathbb{Z}_{2431}$ f) $[3], [5]$ e $[7]$ em $\mathbb{Z}_8$

2.5 a) Seja $\{a_1, \ldots, a_{\Phi(m)}\}$ um sistema reduzido de resíduos módulo m. Mostre que se $(a, m) = 1$, então $\{a \cdot a_1, \ldots, a \cdot a_{\Phi(m)}\}$ é um sistema reduzido de resíduos módulo m.

b) Mostre a seguinte generalização do Pequeno Teorema de Fermat, devida a Euler. Se $(a, m) = 1$, então $a^{\Phi(m)} \equiv 1 \bmod m$.

2.6 a) Mostre que se n não é primo e $n > 4$, então $(n-1)! \equiv 0 \bmod n$.

b) E se $n = 4$, o que acontece?

c) Mostre a recíproca do Teorema de Wilson: Se $(n-1)! \equiv -1 \bmod n$, então n é primo.

2.7 Seja p um número primo positivo, calcule:

a) $(p!, (p-1)! - 1)$ b) $(p!, (p-1)! + 1)$

Sugestão Use o Teorema de Wilson.

3 Congruências lineares

Seja $m > 1$ um inteiro e sejam $[a], [b] \in \mathbb{Z}_m$, queremos resolver em $\mathbb{Z}_m$ equações do tipo

$$[a] \cdot [x] = [b], \tag{1}$$

ou seja, resolver em $x \in \mathbb{Z}$ a congruência

$$ax \equiv b \bmod m. \tag{2}$$

Se x_0 é uma solução de (2) e se $x_1 \equiv x_0 \bmod m$, então x_1 é também uma solução de (2). Portanto, as soluções da congruência (2) se repartem em classes residuais módulo m. Cada classe residual de soluções da congruência (2) é chamada de *solução módulo* m e corresponde a uma solução da equação (1).

Se $(a, m) = 1$, da Proposição 6.2.3, segue-se que $[a]$ é invertível em $\mathbb{Z}_m$. Portanto, neste caso, a equação (1) tem uma única solução dada por

$$[x] = [a]^{-1} \cdot [b].$$

Em outras palavras, se $(a, m) = 1$, então a congruência (2) tem uma única solução módulo m.

Teorema 6.3.1. *Sejam* a, b *e* m *inteiros, com* $m > 1$, *e* $d = (a, m)$.

i) *A congruência* (2) *tem solução se, e somente se,* $d \mid b$.

ii) *Se* $d \mid b$, *existem exatamente* d *soluções distintas módulo* m, *com representantes*

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d},$$

onde x_0 *é uma solução particular qualquer de* (2).

Demonstração (i) A congruência $ax \equiv b \bmod m$ admite solução em x se, e somente se, a equação diofantina $ax + my = b$ admite solução em x e y e isto é equivalente, pelo Teorema 5.4.1, à condição $d \mid b$.
(ii) Seja x_0 uma solução qualquer da congruência $ax \equiv b \bmod m$, logo existe y_0 tal que x_0, y_0 é uma solução particular da equação diofantina $ax + my = b$. Pelo Teorema 5.4.2, temos que toda solução da equação diofantina $ax + my = b$ é, para algum $t \in \mathbb{Z}$, da forma

$$x = x_0 + t\frac{m}{d}, \quad y = y_0 - t\frac{a}{d}.$$

Portanto, toda solução da congruência $ax \equiv b \bmod m$ é da forma

$$x = x_0 + t\,\frac{m}{d}, \quad t \in \mathbb{Z}.$$

As seguintes soluções de (2)

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\,\frac{m}{d} \ldots, x_0 + (d-1)\,\frac{m}{d}, \tag{3}$$

são claramente duas a duas incongruentes módulo m. Por outro lado, se $x = x_0 + t\,\frac{m}{d}$ é uma solução qualquer de (2), pondo $t = dq + r$ com $0 \leq r < d$, temos que

$$x \equiv x_0 + t\,\frac{m}{d} \;\equiv\; x_0 + r\frac{m}{d} \bmod m.$$

Portanto, x é congruente módulo m a uma e somente uma das soluções em (3). □

Exemplos

1. Considere a congruência $12x \equiv 28 \bmod 8$.

Como $d = (12, 8) = d$ e $4 \mid 28$, temos, pelo Teorema 6.3.1 (i), que as soluções módulo 8 têm como representantes 3, 5, 7 e 9. Qualquer outra solução da congruência é congruente módulo 8 a uma dessas.

2. Considere a congruência $245x \equiv 95 \bmod 180$.

Como $d = (245, 180) = 5$ e $5 \mid 95$, segue-se que a congruência admite cinco soluções distintas módulo 180. A nossa congruência, tendo em vista a Proposição 6.1.3 (iv), é equivalente a $49x \equiv 19 \bmod 36$ (as congruências são equivalentes porém as soluções da congruência original são consideradas módulo 180, enquanto que as da outra são módulo 36), da qual devemos achar uma solução particular que pode ser obtida resolvendo a equação diofantina

$$49x - 36y = 19.$$

Pelo método desenvolvido no Capítulo 5, temos

	1	2	1	3	3
49	36	13	10	3	1
13	10	3	1	0	

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ 3 &= 13 - 1 \cdot 10 \\ 10 &= 36 - 2 \cdot 13 \\ 13 &= 49 - 1 \cdot 36 \end{aligned}$$

logo

$$\begin{aligned} 1 &= 10 - 3 \cdot (13 - 1 \cdot 10) = -3 \cdot 13 + 4 \cdot 10 \\ &= -3 \cdot 13 + 4 \cdot (36 - 2 \cdot 13) = 4 \cdot 36 - 11 \cdot 13 \\ &= 4 \cdot 36 - 11 \cdot (49 - 1 \cdot 36) = -11 \cdot 49 + 15 \cdot 36. \end{aligned}$$

Segue-se então que

$$19 = -209 \cdot 49 + 285 \cdot 36.$$

Portanto, uma solução particular da equação diofantina é $x_0 = -209$ e $y_0 = -285$. Temos então que $x_0 = -209$ é uma solução particular da congruência $245x \equiv 95 \bmod 180$. Consequentemente, as soluções da congruência módulo 180 têm como representantes

$$-209 + r \cdot 36, \quad r = 0, 1, 2, 3, 4,$$

ou seja,

$$-209, -173, -137, -101, -65,$$

ou, ainda,

$$151, 7, 53, 79, 115.$$

Problemas

3.1 Resolva as congruências:

a) $3x \equiv 5 \bmod 7$ b) $4x \equiv 2 \bmod 3$
c) $7x \equiv 21 \bmod 49$ d) $3x \equiv 1 \bmod 6$
e) $18x \equiv 12 \bmod 42$ f) $12x \equiv 9 \bmod 15$
g) $240x \equiv 148 \bmod 242$ h) $6125x \equiv 77 \bmod 189$

3.2 Resolva os seguintes sistemas de congruências:

a) $\begin{cases} x \equiv 6 \mod 11 \\ x \equiv 3 \mod 7 \end{cases}$ b) $\begin{cases} x \equiv 4 \mod 8 \\ x \equiv 1 \mod 4 \end{cases}$

3.3 Em quais condições o sistema de congruências abaixo admite solução?

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \end{cases}$$

3.4 Sob quais condições as progressões aritméticas $a_n = a + n \cdot r$ e $b_n = b + n \cdot s$, com $a, b, r, s \in \mathbb{Z}$, têm interseção não vazia?

Sugestão Use o Problema 3.3.

3.5 Resolva o sistema de congruências

$$\begin{cases} 2x + 7y \equiv 2 \mod 5 \\ 3x - y \equiv 1 \mod 5 \end{cases}$$

3.6 Ache o menor inteiro positivo que deixa restos 2, 3 e 2 quando dividido respectivamente por 3, 5 e 7.

4 A função Φ de Euler

Note que a definição da função Φ de Euler, dada na Seção 2, nos fornece que $\Phi(n) = \Phi(-n)$, para todo $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. É fácil deduzir da definição que $\Phi(p) = p - 1$ se, e somente se, p é um primo positivo.

Proposição 6.4.1. *Se p é um número primo positivo e $n \in \mathbb{N} \setminus \{0\}$, então $\Phi(p^n) = p^{n-1}(p-1)$.*

Demonstração O ponto crucial da demonstração é notar que se p é primo, então $(m, p^n) \neq 1$ se, e somente se, m é um múltiplo de p.

Considere agora a sequência:

$$1, 2, \ldots, p, p+1, \ldots, 2p, \ldots, 3p, \ldots, p^{n-1} \cdot p.$$

Devido à observação acima, os inteiros não primos com p^n nesta sequência são os p^{n-1} números: $p,\ 2p,\ 3p, \ldots, p^{n-1} \cdot p$.

Logo, existem exatamente $p^n - p^{n-1} = p^{n-1}(p-1)$ números naturais menores do que p^n e primos com p^n. □

Proposição 6.4.2. *Se m e n são inteiros em $\mathbb{Z} \setminus \{0, \pm 1\}$ tais que $(n, m) = 1$, então $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$.*

Demonstração Basta claramente demonstrar o resultado para n e m maiores do que 1. Considere a seguinte tabela formada com os inteiros de 1 a $n \cdot m$

$$\begin{array}{ccccccc} 1 & 2 & \dots & k & \dots & m \\ m+1 & m+2 & \dots & m+k & \dots & 2m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+k & \dots & n\cdot m \end{array}$$

Como $(t, n\cdot m) = 1$ se, e somente se, $(t, m) = 1$ e $(t, n) = 1$ (verifique), devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e com n, para determinar os que são primos com $n\cdot m$.

Se o primeiro elemento de uma coluna não for primo com m, então todos os elementos da coluna não são primos com m. Portanto, os elementos primos com m estão necessariamente nas colunas restantes que são $\Phi(m)$ em número e é fácil ver que são primos com m todos os elementos destas colunas. Vejamos agora quais são os elementos primos com n em cada uma destas $\Phi(m)$ colunas.

Como $(n, m) = 1$, a sequência $k, m+k, \dots, (n-1)m+k$ forma um sistema completo de resíduos módulo n (veja Problema 2.1 (d)) e, portanto, $\Phi(n)$ desses elementos são primos com n. Logo, o número de elementos simultaneamente primos com m e n é $\Phi(n)\cdot\Phi(m)$. □

Corolário 6.4.3. *Se* $m = \pm p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, *com* $p_1, \dots, p_r$ *primos distintos e* $\alpha_1, \dots, \alpha_r \in \mathbb{N}\setminus\{0\}$, *então*

$$\Phi(m) = p_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1}(p_1-1)\cdots(p_r-1) = m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Exemplos

1. $\Phi(100) = \Phi(2^2\cdot 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$
2. $\Phi(725) = \Phi(5^2\cdot 29) = 725\left(1-\frac{1}{29}\right)\left(1-\frac{1}{5}\right) = 560$
3. $\Phi(7^3) = 7^2(7-1) = 49\cdot 6 = 294$

Do corolário acima, é fácil verificar que se $m \neq 0, \pm 1, \pm 2$, então $\Phi(m)$ é par. Os números m para os quais $\Phi(m) = 2^r$, para algum $r \in \mathbb{N}$, são muito importantes e se relacionam, via resultados de Gauss, com a construção com régua e compasso dos polígonos regulares que abordaremos no Volume. A proposição a seguir nos permitirá caracterizar tais números.

Proposição 6.4.4. *Se* $\Phi(m) = 2^r$, *para algum* $r \in \mathbb{N} \setminus \{0\}$, *então a decomposição de* m *em fatores primos é dada por*

$$m = \pm 2^s \cdot \left(2^{2^{n_1}} + 1\right) \cdots \left(2^{2^{n_k}} + 1\right),$$

com $s, n_1, \ldots, n_k \in \mathbb{N}$, *onde os* $\left(2^{2^{n_i}} + 1\right)$, *com* $i = 1, \ldots, k$, *são primos distintos.*

Demonstração Seja $m = \pm p_0^{\alpha_0} \cdots p_k^{\alpha_k}$, com $p_0, \ldots, p_k$ primos positivos distintos, $\alpha_0 \in \mathbb{N}$ e $\alpha_1, \ldots, \alpha_k \in \mathbb{N} \setminus \{0\}$. Vamos supor

$$2 = p_0 < p_1 < \cdots < p_k .$$

Temos então que

$$\Phi(m) = p_0^{\alpha_0 - 1} p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1} (p_0 - 1) \cdots (p_k - 1) = 2^r.$$

Como $p_1, \ldots, p_k$ são diferentes de 2, devemos ter $\alpha_1 = 1, \ldots, \alpha_k = 1$. Além disso, $p_i - 1 = 2^{\beta_i}$, para algum β_i, $i = 1, \ldots, k$, logo $p_i = 2^{\beta_i} + 1$ e como p_i é primo segue-se, da Proposição 5.1.4, que $\beta_i = 2^{n_i}$, com $n_i \in \mathbb{N}$. Logo, pondo $s = \alpha_0$, temos que

$$m = \pm 2^s \left(2^{2^{n_1}} + 1\right) \cdots \left(2^{2^{n_k}} + 1\right).$$

□

Problemas

4.1 Calcule

a) $\Phi(125)$ b) $\Phi(16200)$ c) $\Phi(2097)$

4.2 Ache os valores de m sabendo que

a) $\Phi(m) = 2^2$ b) $\Phi(m) = 2^3$ c) $\Phi(m) = 2^4$

d) $\Phi(m) = 2^5$ e) $\Phi(m) = 3^2 \cdot 2$ f) $\Phi(m) = 10$

5 O legado de um gigante

Carl Friedrich Gauss (1777-1855) foi um dos maiores matemáticos de todos os tempos, legando-nos uma imponente obra matemática.

Ainda adolescente, Gauss ficou intrigado com o paradoxo do binômio de Newton. A fórmula do binômio,

$$(1 + x)^\alpha = 1 + \frac{\alpha}{1} x + \frac{\alpha(\alpha - 1)}{2!} x^2 + \cdots ,$$

estendida pelo próprio Newton para valores de α não necessariamente inteiros positivos tem no seu segundo membro uma soma infinita. Estas somas eram tratadas pelos predecessores de Gauss, entre eles o próprio Newton, Leibniz e Euler como se fossem finitas, gerando paradoxos. Por exemplo, pondo $x = -2$ e $\alpha = -1$ na expressão acima obtém-se a igualdade

$$-1 = 1 + 2 + 2^2 + \cdots,$$

o que é absurdo. Gauss então introduziu o conceito de convergência para as somas infinitas, chamadas séries, provando por exemplo que se α e x são reais com $|x| < 1$, então a série do binômio de Newton é convergente. O trabalho de Gauss nesta direção teve grande influência sobre seus contemporâneos Abel e Cauchy e sobre os seus sucessores Weierstrass e Dedekind, responsáveis pelo desenvolvimento da Análise Matemática. Este trabalho sobre séries inclui a série hipergeométrica que contém como casos particulares muitas séries importantes e pode ser considerado como divisor de águas entre o Cálculo Diferencial intuitivo de Newton e Leibniz e o rigor da Análise Matemática.

Aos dezessete anos, Gauss estabeleceu-se como meta corrigir e completar o que os seus predecessores haviam feito em Aritmética. Aos 21 anos, como fruto deste projeto, ele produziu a sua obra prima, o livro *Disquisitiones Arithmeticae*, publicado em 1801, três anos após a sua conclusão, que contém grandes contribuições à Aritmética e à Álgebra.

No livro, Gauss introduz e estuda as congruências e as equações do tipo

$$x^n \equiv a \bmod p,$$

isto é, as equações $x^n = [a]$ em $\mathbb{Z}_p$. Um problema natural neste contexto é saber para quais valores de $a \in \mathbb{Z}$, a equação acima possui solução. Este é um problema difícil e até hoje sem solução. Em busca da solução, Gauss se restringiu ao caso $n = 2$ e elaborou tabelas para compreender o problema. Gauss não conseguiu resolver o problema mas descobriu e demonstrou uma propriedade maravilhosa, detectada anteriormente por Euler, o *Teorema da Reciprocidade Quadrática*[1], cujo enunciado é o seguinte:

[1] O leitor desejoso de ver uma demonstração desse teorema e outros tópicos relacionados é convidado a consultar o livro *Elementos de Aritmética* do autor, citado na bibliografia.

Se p e q são números primos positivos distintos, então as congruências

$$x^2 \equiv q \bmod p \quad \text{e} \quad x^2 \equiv p \bmod q,$$

são ambas resolúveis ou ambas não resolúveis exceto quando $p \equiv 3 \bmod 4$, e neste caso uma e somente uma das congruências admite solução.

Gauss obteve este resultado aos 19 anos e ficou tão intrigado com ele que posteriormente produziu 5 outras demonstrações e estudou os casos $n = 3$ e $n = 4$.

No final do Disquisitiones, Gauss aplica a teoria que desenvolveu para atacar a *ciclotomia*, isto é, o estudo das raízes n-ésimas da unidade, e apresenta o seu belo resultado sobre a construtibilidade com régua e compasso de polígonos regulares.

Outra famosa contribuição do Gauss é o chamado Teorema Fundamental da Álgebra, que estabelece que toda equação algébrica com coeficientes reais (ou complexos) admite pelo menos uma raiz complexa. Este é outro teorema que fascinou Gauss dando-lhe ao longo da vida quatro provas distintas.

Outras áreas onde Gauss deixou contribuições relevantes foram: Estatística (distribuição normal de Gauss), Geometria (geometria das superfícies e geometrias não euclidianas) e Física (magnetismo). Mas de todo este universo, Gauss nunca escondeu a sua preferência sintetizada na seguinte frase:

"*A matemática é a rainha das ciências e a aritmética é a rainha da matemática*".

7

Anéis

A teoria dos Anéis é um dos principais assuntos do vasto campo da álgebra abstrata. A origem da Álgebra remonta aos babilônios e o seu desenvolvimento percorreu um longo caminho que não pretendemos retraçar aqui, mas que teve, no século 16, um momento importante com os matemáticos da chamada Escola de Bolonha que se ocuparam da resolução das equações algébricas do terceiro e do quarto grau. Em seguida, Bombelli deu um passo decisivo introduzindo o simbolismo apropriado para as operações permitindo a manipulação de expressões e fórmulas. Um outro momento importante para a Álgebra ocorreu na primeira metade do século 19 com os trabalhos do irlandês Hamilton e de seus contemporâneos ingleses. Hamilton introduziu o formalismo dos números complexos, até hoje usado, e, posteriormente, definiu formalmente os quatérnios, dando mais um passo decisivo para o desenvolvimento da álgebra abstrata. Importante para o desenvolvimento da teoria, foi o estudo dos anéis de inteiros algébricos, iniciado por Gauss e desenvolvido por Kummer, Dedekind, Kronecker, Dirichlet e Hilbert, no final do século 19, início do século 20. Finalmente, a noção abstrata de anel foi introduzida na segunda década do século 20.

1 Anéis

Retomamos aqui os conceitos de anel, subanel e homomorfismo introduzidos no Capítulo 2. O próximo resultado nos fornece um modo ligei-

ramente mais econômico do que usar a definição para verificar que um dado subconjunto A' de A é um subanel de A.

Proposição 7.1.1. *Sejam A um anel e A' um subconjunto de A. Temos que A' é um subanel de A se, e somente se, são satisfeitas as condições:*

i) $1 \in A'$;

ii) *Quaisquer que sejam $a, b \in A'$, tem-se que $a - b \in A'$ e $a \cdot b \in A'$.*

Demonstração É claro que se A' é um subanel de A, então as condições (i) e (ii) são satisfeitas.

Suponha agora que tais condições sejam verificadas. Como $1 \in A'$, segue-se que $0 = 1 - 1 \in A'$. Se $a \in A'$, então $-a = 0 - a \in A'$.

Sejam agora a e b elementos de A', logo $-b \in A'$ e, consequentemente,

$$a + b = a - (-b) \in A'.$$

Como $a \cdot b \in A'$ e as demais condições que definem um anel são verificadas em A', pois o são em A, segue-se que A' é um subanel de A. □

Proposição 7.1.2. *Sejam A um anel e $\{A_i\}_{i\in I}$ uma família de subanéis de A. Então, $\bigcap_{i\in I} A_i$ é um subanel de A.*

Demonstração Como $1 \in A_i$, para todo $i \in I$, segue-se que $1 \in \bigcap_{i\in I} A_i$. Sejam agora $a, b \in \bigcap_{i\in I} A_i$, logo $a, b \in A_i$, para todo $i \in I$, e, portanto, $a - b \in A_i$ e $a \cdot b \in A_i$, para todo $i \in I$. Consequentemente,

$$a - b \in \bigcap_{i\in I} A_i \quad \text{e} \quad a \cdot b \in \bigcap_{i\in I} A_i ,$$

e o resultado decorre da Proposição 7.1.1. □

Proposição 7.1.3. *Sejam B um anel, A um subanel de B e $b_1, \ldots, b_n \in B \setminus \{0\}$. O conjunto $A[b_1, \ldots, b_n]$ de todos os elementos de B que são somas de elemento da forma $a \cdot b_1^{r_1} \cdots b_n^{r_n}$, com $a \in A$ e $r_1, \ldots, r_n \in \mathbb{N}$, é um subanel de B que contém A e $b_1, \ldots, b_n$.*

Demonstração É claro que $1 \in A[b_1, \ldots, b_n]$ pois $1 = 1 \cdot b_1^0 \cdots b_n^0$. Por outro lado, é claro que se $x, y \in A[b_1, \ldots, b_n]$, então $x - y$ e $x \cdot y$ estão em $A[b_1, \ldots, b_n]$. Consequentemente, pela Proposição 7.1.1, temos que $A[b_1, \ldots, b_n]$ é um subanel de B. Como para todo $a \in A$, temos

que $a = a \cdot b_1^0 \cdots b_n^0$ e que $b_i = 1 \cdot b_1^0 \cdots b_i^1 \cdots b_n^0$, para todo i, então $A[b_1, \ldots, b_n]$ contém A e $b_1, \ldots, b_n$. □

O anel $A[b_1, \ldots, b_n]$ é chamado de *subanel* de B *gerado* por A e por $b_1, \ldots, b_n$. É fácil verificar que $A[b_1, \ldots, b_n]$ é o menor subanel de B que contém A e $b_1, \ldots, b_n$, no sentido que todo subanel de B que contém A e $b_1, \ldots, b_n$, também contém $A[b_1, \ldots, b_n]$. É também fácil verificar que $A[b_1, \ldots, b_n]$ é a interseção de todos os subanéis de B que contêm A e $b_1, \ldots, b_n$.

Um subconjunto K' de um corpo K será chamado de *subcorpo* de K, se K' é um subanel de K e é um corpo. Portanto, K' é um subanel de K tal que o inverso de todo elemento de $K' \setminus \{0\}$ pertence a K'. Quando K' é um subcorpo de K dizemos também que K é uma extensão de K'.

Seja K' um subcorpo de um corpo K. Se $b_1, \ldots, b_n \in K \setminus \{0\}$, então $K'[b_1, \ldots, b_n]$ é um subanel de K e, portanto, também domínio de integridade, logo possuindo um corpo de frações que se identifica naturalmente com o conjunto $K'(b_1 \ldots, b_n)$ de todos os elementos de K que são frações com numerador em $K'[b_1, \ldots, b_n]$ e denominador em $K'[b_1, \ldots, b_n] \setminus \{0\}$. Temos claramente que $K'(b_1, \ldots, b_n)$ é o menor subcorpo de K que contém K' e $b_1, \ldots, b_n$.

Dados dois anéis A e B é possível dotar o produto cartesiano $A \times B$ de uma estrutura natural de anel onde as operações de adição e de multiplicação são dadas por

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$$

Proposição 7.1.4. *Se A e B são anéis, então o conjunto $A \times B$ com as operações acima definidas é um anel.*

Demonstração A comutatividade e a associatividade da adição e da multiplicação são de verificação fácil a partir das definições, o mesmo ocorrendo com a distributividade da multiplicação com relação à adição. O elemento zero da adição é $(0, 0)$, o simétrico de (a, b) é $(-a, -b)$ e $(1, 1)$ é o elemento identidade da multiplicação. □

Proposição 7.1.5. *Um elemento $(a, b) \in A \times B$ é invertível se, e somente se, a é invertível em A e b é invertível em B. Neste caso, temos que $(a, b)^{-1} = (a^{-1}, b^{-1})$.*

Demonstração Suponha (a, b) invertível com inverso (c, d), logo

$$(1, 1) = (a, b) \cdot (c, d) = (a \cdot c, b \cdot d).$$

Portanto, $a \cdot c = 1$ e $b \cdot d = 1$. Consequentemente, a e b são invertíveis com $c = a^{-1}$ e $d = b^{-1}$.

Reciprocamente, se a e b são invertíveis, então

$$(a, b) \cdot (a^{-1}, b^{-1}) = (a \cdot a^{-1}, b \cdot b^{-1}) = (1, 1),$$

e, consequentemente, (a, b) é invertível, com $(a, b)^{-1} = (a^{-1}, b^{-1})$. □

Note que o anel $A \times B$ nunca é um domínio, pois $(1, 0) \cdot (0, 1) = (0, 0)$.

Usando a notação A^* para representar o conjunto dos elementos invertíveis do anel A, a Proposição 7.1.5 nos afirma que

$$(A \times B)^* = A^* \times B^*.$$

Sejam A um anel e S um conjunto não vazio. Recorde que, no Capítulo 1, definimos $\mathcal{F}(S, A)$ como sendo o conjunto de todas as funções de S em A. Nesse conjunto, consideramos as seguintes operações de adição e de multiplicação:

$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Proposição 7.1.6. *Sejam A um anel e S um conjunto não vazio qualquer. O conjunto $\mathcal{F}(S, A)$, com as operações acima definidas, é um anel.*

Demonstração A associatividade e comutatividade da adição e da multiplicação, bem como a distributividade da multiplicação com relação à adição, são fáceis de verificar. O elemento zero da adição é a função constante $0\colon S \to A$, que associa a cada $x \in S$ o elemento $0 \in A$, enquanto que o elemento identidade da multiplicação é a função constante $1\colon S \to A$, que associa a cada $x \in S$ o elemento $1 \in A$. O simétrico de $f\colon S \to A$ é a função $-f\colon S \to A$ tal que $(-f)(x) = -f(x)$. □

Exemplo Seja A um anel, o conjunto $\mathcal{F}(\mathbb{N}\backslash\emptyset, A)$, de todas as sequências de A, é um anel com as operações acima definidas. Este anel será denotado também por $S(A)$.

Problemas

1.1 Mostre que o subanel $\mathbb{Z}[1/2]$ de $\mathbb{Q}$ é igual a $\left\{\frac{a}{2^n};\ a \in \mathbb{Z} \text{ e } n \in \mathbb{N}\right\}$, juntamente com a adição e multiplicação de números racionais.

1.2 Sejam A um subanel de B e $b_1, \ldots, b_n \in B \setminus \{0\}$. Mostre que $A[b_1, \ldots, b_n]$ é o menor subanel de B que contém A e $b_1, \ldots, b_n$. Mostre também que $A[b_1, \ldots, b_n]$ é a interseção de todos os subanéis de B que contém A e $b_1, \ldots, b_n$.

1.3 Demonstre com detalhes as Proposições 7.1.4 e 7.1.6.

1.4 Mostre que o único subanel de $\mathbb{Z}$ é ele próprio.

1.5 Sejam S um conjunto com um único elemento e A um anel. Mostre que $\mathcal{F}(S, A)$ é isomorfo a A.

1.6 Sejam S um conjunto com dois elementos e A um anel. Mostre que $\mathcal{F}(S, A)$ é isomorfo a $A \times A$.

1.7 Seja p um número primo. Mostre que

$$\mathbb{Z}_{(p)} = \left\{\frac{m}{n};\ m, n \in \mathbb{Z}, p \nmid n\right\}$$

é um subanel de $\mathbb{Q}$. Quais são os elementos invertíveis de $\mathbb{Z}_{(p)}$? Determine o corpo quociente de $\mathbb{Z}_{(p)}$.

1.8 Sejam A um anel e S um conjunto não vazio. Determine os divisores de zero de $\mathcal{F}(S, A)$ (isto é, os elementos $f \in \mathcal{F}(S, A)$ para os quais existem $g \in \mathcal{F}(S, A)\setminus\{0\}$ tais que $f \cdot g = 0$).

2 Homomorfismos

As próximas proposições nos relacionarão os subanéis e ideais de dois anéis A e B em presença de um homomorfismo $f\colon A \to B$.

Proposição 7.2.1. *Seja* $f\colon A \to B$ *um homomorfismo de anéis.*

i) *Se* A' *é um subanel de* A*, então* $f(A')$ *é um subanel de* $f(A)$*.*

ii) *Se* B' *é um subanel de* B*, então* $f^{-1}(B')$ *é um subanel de* A*.*

Demonstração (i) Isto decorre da Proposição 2.1.11 (iii),tomando no lugar de f a restrição de f a A'.

(ii) Seja B' um subanel de B. Como $f(1) = 1 \in B'$, segue-se que $1 \in f^{-1}(B')$. Além disso, se $a, b \in f^{-1}(B')$, segue-se que $f(a), f(b) \in B'$. Portanto,

$$f(a - b) = f(a) - f(b) \in B', \text{ e}$$

$$f(a \cdot b) = f(a) \cdot f(b) \in B'.$$

Logo, $a - b \in f^{-1}(B')$ e $a \cdot b \in f^{-1}(B')$. Portanto, pela Proposição 7.1.1, temos que $f^{-1}(B')$ é um subanel de A. □

Proposição 7.2.2. *Seja* $f\colon A \to B$ *um homomorfismo de anéis.*

i) *Se* I *é um ideal de* A*, então* $f(I)$ *é um ideal de* $f(A)$*.*

ii) *Se* J *é um ideal de* B*, então* $f^{-1}(J)$ *é um ideal de* A*.*

Demonstração (i) Se I é um ideal de A, então $I \neq \emptyset$. Logo, $f(I) \neq \emptyset$.

Suponha agora que $a', b' \in f(I)$, logo $a' = f(a)$ e $b' = f(b)$, com $a, b \in I$. Consequentemente,

$$a' + b' = f(a) + f(b) = f(a + b) \in f(I).$$

Agora, se $a' \in f(I)$ e $b' \in f(A)$, temos que $a' = f(a)$ e $b' = f(b)$ com $a \in I$ e $b \in A$, logo $a \cdot b \in I$ e, consequentemente,

$$a' \cdot b' = f(a) \cdot f(b) = f(a \cdot b) \in f(I).$$

Temos, portanto, que $f(I)$ é um ideal de $f(A)$.

(ii) Como $0 \in J$ e $f(0) = 0$, segue-se que $0 \in f^{-1}(J)$ e, portanto, $f^{-1}(J) \neq \emptyset$.

Suponha agora que $a, b \in f^{-1}(J)$, logo $f(a), f(b) \in J$. Portanto,

$$f(a + b) = f(a) + f(b) \in J,$$

e, consequentemente, $a + b \in f^{-1}(J)$. Por outro lado, se $a \in A$ e $b \in f^{-1}(J)$, então

$$f(a \cdot b) = f(a) \cdot f(b) \in J,$$

e, portanto, $a \cdot b \in f^{-1}(J)$. Temos então que $f^{-1}(J)$ é um ideal de A. □

No caso em que $J = (0)$, o ideal $f^{-1}(J)$ é chamado de *núcleo* de f e denotado por $N(f)$. Em outras palavras,

$$N(f) = \{a \in A;\ f(a) = 0\}.$$

Quando A é um subanel de B e J é um ideal de B, a Proposição 7.2.2, aplicada ao homomorfismo inclusão $i\colon A \to B$, $i(x) = x$, nos diz que $J \cap A$ é um ideal de A.

Proposição 7.2.3. *Seja* $f\colon A \to B$ *um homomorfismo de anéis.*

i) $f(a') = f(a)$ *se, e somente se,* $a' - a \in N(f)$.

ii) f *é injetora se, e somente se,* $N(f) = (0)$.

Demonstração (i) $f(a') = f(a)$ se e somente se $f(a' - a) = f(a') - f(a) = 0$, o que é equivalente a $a' - a \in N(f)$.
(ii) Decorre imediatamente de (i). □

Corolário 7.2.4. *Seja* $f\colon K \to B$ *um homomorfismo de anéis, onde* K *é um corpo. Então* f *é injetora e o subanel* $f(K)$ *de* B *é um corpo.*

Demonstração Como $N(f)$ é um ideal de K e os únicos ideais de K são (0) e o próprio K (veja Problema 2.1, Capítulo 4) e como $N(f) \neq K$ pois $f(1) = 1 \neq 0$, segue-se que $N(f) = (0)$. Logo, pela proposição, f é injetora. Falta só mostrar que o anel $f(K)$ é um corpo. Seja $f(a) \neq 0$ um elemento de $f(K)$, logo, por ser f injetora, $a \neq 0$ e, Portanto, a é invertível sendo $f(a^{-1})$ é o inverso de $f(a)$. □

Um ideal I de um anel A, com $I \neq A$, é chamado de *ideal primo* se sempre que $a \cdot b \in I$, com $a, b \in A$, segue-se que $a \in I$ ou $b \in I$.

Um ideal M de A, com $M \neq A$, é chamado de *ideal maximal* se para todo ideal I tal que $M \subsetneqq I \subset A$, temos que $I = A$.

Proposição 7.2.5. *Todo ideal maximal é primo.*

Demonstração Seja M um ideal maximal de um anel A e sejam a e b elementos de A tais que $a \cdot b \in M$. Se $a \notin M$, então temos que o ideal $M + I(a)$ é tal que $M \subsetneqq M + I(a) \subset A$. Logo, $M + I(a) = A$. Portanto, existem $m \in M$ e $\lambda \in A$ tais que

$$1 = m + \lambda \cdot a.$$

Multiplicando ambos os membros da igualdade acima por b, temos que

$$b = m \cdot b + \lambda \cdot a \cdot b \in M,$$

pois $m, a \cdot b \in M$. Isto prova que M é primo. □

Proposição 7.2.6. *Para um domínio principal* A *e para um ideal* I, *com* $I \neq (0)$ *e* $I \neq A$, *as seguintes afirmações são equivalentes:*

i) I *é maximal.*

ii) I *é primo.*

iii) $I = I(p)$*, onde* p *é um elemento primo de* A*.*

Demonstração A implicação (i) $\Rightarrow$ (ii) decorre da Proposição 7.2.5.

Vamos provar (ii) $\Rightarrow$ (iii). Suponha que $I \neq (0)$ é um ideal primo de A. Como A é principal, existe $p \in A$ tal que $I = I(p)$. É claro que $p \neq 0$ e p não é invertível. Suponha que $p \mid a \cdot b$, logo $a \cdot b \in I(p)$ e como $I(p)$ é primo temos que $a \in I(p)$ ou $b \in I(p)$. Portanto, $p \mid a$ ou $p \mid b$. Consequentemente, p é primo.

Para provar que (iii) $\Rightarrow$ (i), seja $I = I(p)$ o ideal gerado por um elemento primo p de A. Suponha que $J = I(a)$ seja um ideal de A tal que $I(p) \subsetneqq J \subset A$. Temos que $a \mid p$ e a não é associado de p, logo a é invertível, pois p é primo. Portanto, $J = I(a) = A$. □

Problemas

2.1 Seja $h\colon A \to B$ uma função não nula de anéis tal que

$$h(a \cdot b) = h(a) \cdot h(b), \quad \forall a, b \in A.$$

Mostre que se B é um domínio então $h(1) = 1$.

2.2 Mostre que a função

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z}_{12} \\ x &\longmapsto [9x] \end{aligned}$$

é tal que, para todos $a, b \in \mathbb{Z}$, $f(a+b) = f(a)+f(b)$, $f(a\cdot b) = f(a)\cdot f(b)$ e $f(1) \neq 1$.

2.3 Sejam A um anel e $a \in A$.

a) Mostre que o ideal (0) é primo se, e somente se, A é um domínio.

b) Mostre que a é um elemento primo de A se, e somente se, $I(a)$ é um ideal primo de A.

2.4 Seja $f\colon A \to B$ um homomorfismo. Mostre que

a) Se J é um ideal primo de B, então $f^{-1}(J)$ é um ideal primo de A.

b) Se I é um ideal primo de A contendo $N(f)$, então $f(I)$ é um ideal primo de $f(A)$.

2.5 Seja $f\colon A \to B$ um homomorfismo de anéis e sejam I e J respectivamente ideais de A e B.

a) Mostre que $f(f^{-1}(J)) = J \cap f(A)$.

b) Mostre que $f^{-1}(f(I)) = I + N(f)$.

2.6 Dado um homomorfismo de anéis $f\colon A \to B$, mostre que a aplicação

$$\begin{array}{rccc} \psi_f\colon & \{\text{ideais de } A \text{ que contém } N(f)\} & \longrightarrow & \{\text{ideais de } f(A)\} \\ & I & \longmapsto & f(I) \end{array}$$

é uma bijeção que faz corresponder os ideais primos de cada conjunto.

Sugestão Use os Problemas 2.4 e 2.5.

2.7 Seja m um inteiro maior do que 1 e seja $\rho\colon \mathbb{Z} \to \mathbb{Z}_m$ o homomorfismo característico.

a) Mostre que $\mathbb{Z}_m$ é o único subanel dele próprio.

b) Seja $J \subset \mathbb{Z}_m$ um ideal e considere a aplicação inversa de ψ_ρ do Problema 2.6, relativa a ρ. Mostre que $J = I([\lambda])$ onde λ é um divisor de m. Isto prova que $\mathbb{Z}_m$ é um anel principal e que os seus ideais estão com correspondência bijetora com os divisores positivos de m.

2.8 Sejam S um conjunto não vazio e A um anel. Se $T \subset S$, mostre que $\{f \in \mathcal{F}(S, A)\,;\ \ f(T) \subset \{0\}\}$ é um ideal de $\mathcal{F}(S, A)$. Mostre que este ideal é primo se, e somente se, A é um domínio e T possui um só elemento.

2.9 Sejam S um subconjunto de um anel A e $a \in A$. Define-se

$$aS = \{a \cdot x\,;\ \ x \in S\}.$$

Mostre que $\{a \in A\,;\ \ aS = \{0\}\}$ é um ideal de A.

2.10 a) Sejam A um anel e I um ideal de A. Mostre que se todo elemento de $A \setminus I$ for invertível, então I é o único ideal maximal de A. Um anel que possui um único ideal maximal é chamado de *anel local*.

b) Mostre que o anel $\mathbb{Z}_{(p)}$ do Problema 1.7 é um anel local com ideal maximal

$$M_p \left\{ \frac{m}{n}\,;\ \ m, n \in \mathbb{Z},\ p \mid m \text{ e } p \nmid n \right\}.$$

3 Anéis quocientes

A relação de congruência em $\mathbb{Z}$, estudada no Capítulo 6, pode ser reinterpretada em termos de ideais como a seguir:

$$a \equiv b \bmod n \iff b - a \in I.$$

Usando isto como motivação, mais geralmente, dado um ideal I de um anel A, definimos a seguinte relação em A:

$$a \equiv b \bmod I \iff b - a \in I.$$

Prova-se facilmente (faça-o) que esta relação é uma relação de equivalência em A, possuindo a propriedade a seguir.

Proposição 7.3.1. *Se* $a \equiv b \bmod I$ *e* $c \equiv d \bmod I$*, então* $a + c \equiv b + d \bmod I$ *e* $a \cdot c \equiv b \cdot d \bmod I$.

Demonstração Semelhante à demonstração da Proposição 6.1.2 e a deixamos como exercício. □

Portanto, a classe de um elemento a por esta relação de equivalência, chamada *classe residual de* a *módulo* I, é o conjunto:

$$[a] = a + I = \{a + x;\ x \in I\}.$$

Tal como para as congruências (e, mais geralmente, para qualquer relação de equivalência, cf. Proposição 1.5.1), estas classes satisfazem às seguintes condições:

1) $[a] = [b] \Leftrightarrow a \equiv b \bmod I$.
2) $[a] \cap [b] \neq \emptyset \implies [a] = [b]$.
3) $\bigcup_{a \in A} [a] = A$.

Denotaremos por A/I o conjunto das classes residuais módulo I de todos os elementos de A.

Por exemplo, quando $A = \mathbb{Z}$ e $I = I(m)$, para algum inteiro m maior do que 1, temos que $A/I = \mathbb{Z}_m$.

Definem-se em A/I as seguintes operações:

Adição: $[a] + [b] = [a + b]$

Multiplicação: $[a] \cdot [b] = [a \cdot b]$

Novamente, tal como no caso das congruências, mostra-se facilmente com o uso da Proposição 7.3.1 (faça-o), que as leis acima definem efetivamente operações em A/I. Quando $I \neq A$, tem-se que A/I, com estas operações, é um anel, chamado *anel quociente* de A por I.

Neste anel, o elemento zero é $[0] = I$, o simétrico de $[a] = a + I$ é $[-a] = -a + I$, o elemento unidade é $[1] = 1 + I$. A aplicação

$$\begin{aligned} \varphi\colon A &\longrightarrow A/I \\ a &\longmapsto [a] \end{aligned}$$

define um homomorfismo sobrejetor cujo núcleo é I.

Proposição 7.3.2 (Teorema do Isomorfismo). *Seja dado um homomorfismo sobrejetor de anéis* $h\colon A \to B$. *Existe um único isomorfismo* $\tilde{h}\colon A/N(h) \to B$ *tal que* $h = \tilde{h} \circ \varphi$.

Demonstração Como a unicidade é clara, provemos a existência. Para $a \in A$, definimos $\tilde{h}([a]) = h(a)$. Temos que mostrar que o valor de $\tilde{h}([a])$ depende apenas da classe $[a]$ e não do representante a da classe. Suponha que $[a] = [b]$, logo $a - b \in N(h)$ e, portanto, pela Proposição 7.2.3, temos que $h(a) = h(b)$, mostrando que $\tilde{h}([a]) = \tilde{h}([b])$.

A função $\tilde{h}$ é um homomorfismo, pois

$\tilde{h}([a] + [b]) = \tilde{h}([a+b]) = h(a+b) = h(a) + h(b) = \tilde{h}([a]) + \tilde{h}([b])$,

$\tilde{h}([a] \cdot [b]) = \tilde{h}([a \cdot b]) = h(a \cdot b) = h(a) \cdot h(b) = \tilde{h}([a]) \cdot \tilde{h}([b])$, e

$\tilde{h}([1]) = h(1) = 1$.

A função $\tilde{h}$ é sobrejetora, pois se $y \in B$, existe $x \in A$ tal que $h(x) = y$ (pois h é sobrejetora), logo $\tilde{h}([x]) = h(x) = y$.

É claro que

$$\tilde{h}([a]) = 0 \iff h(a) = 0 \iff a \in N() \iff [a] = [0].$$

Logo, $N(\tilde{h}) = \{[0]\}$ e, portanto, pela Proposição 7.2.3, $\tilde{h}$ é injetora. Temos então que $\tilde{h}$ é bijetora e verifica trivialmente a igualdade $h = \tilde{h} \circ \varphi$. □

Corolário 7.3.3. *Seja* $h\colon A \to B$ *um homomorfismo, então* $A/\mathbb{N}(h)$ *e* $h(A)$ *são anéis isomorfos.*

Demonstração Substitua B por $h(A)$ e use a proposição. □

Usando o homomorfismo identidade $\mathrm{id}\colon A \to A$, vê-se que $A/(0)$ é isomorfo a A.

Proposição 7.3.4. *Sejam* A *um anel e* I *um ideal de* A*, com* $I \neq A$.

i) A/I *é um domínio se, e somente se,* I *é ideal primo.*

ii) A/I *é um corpo se, e somente se,* I *é ideal maximal.*

Demonstração (i) Suponha que A/I seja um domínio. Suponha que $a \cdot b \in I$, logo $[a] \cdot [b] = [a \cdot b] = [0]$. Consequentemente, temos que $[a] = [0]$ ou $[b] = [0]$ e, portanto, $a \in I$ ou $b \in I$, ou seja, I é primo.

Reciprocamente, suponha que I seja um ideal primo. Sejam $[a], [b] \in A/I$ tais que $[a] \cdot [b] = [0]$, logo $a \cdot b \in I$ e, portanto, $a \in I$ ou $b \in I$, ou seja, $[a] = [0]$ ou $[b] = [0]$.
(ii) Suponha que A/I seja um corpo e suponha que J seja um ideal tal que $I \subsetneqq J \subset A$. Seja $a \in J \backslash I$, logo $[a] \neq [0]$ e, portanto, existe $[b] \in A/I$ tal que $[a] \cdot [b] = [1]$, isto é, $a \cdot b - 1 \in I$. Como $I \subset J$ e $a \cdot b \in J$ (pois $a \in J$), segue-se que $1 \in J$ e, consequentemente, $J = A$.

Reciprocamente, suponha que I seja um ideal maximal. Seja $[a] \neq [0]$, isto é, $a \notin I$. Portanto, $I \subsetneqq I + I(a)$ e, consequentemente, $I + I(a) = A$. Logo, $1 = b + \lambda \cdot a$, com $b \in I$, $\lambda \in A$, e, consequentemente, $I = [0] + [\lambda] \cdot [a] = [\lambda] \cdot [a]$. Isto prova que $[a]$ é invertível e portanto A/I é um corpo. □

Note que a proposição acima nos fornece outra prova de que todo ideal maximal é primo já que todo corpo é domínio.

Sejam A um anel e $\rho\colon \mathbb{Z} \to A$ o homomorfismo característico. Sendo $\mathbb{Z}$ principal temos que $N(\rho) = I(n)$ para algum $n \in \mathbb{N}$, $n \neq 1$. O inteiro n assim definido é chamado de *característica* de A e denotado por $\mathrm{car}(A)$.

Pelo Corolário 7.3.3, temos que $\rho(\mathbb{Z})$ é isomorfo a $\mathbb{Z}_n = \mathbb{Z}/I(n)$ (note que $\mathbb{Z}_0 = \mathbb{Z}/(0) = \mathbb{Z}$), logo $\mathbb{Z}_n$ pode ser visto como subanel de A, sendo o menor subanel de A. Se A é um domínio, então $\rho(\mathbb{Z})$ é um domínio e, portanto, $\mathbb{Z}/I(n)$ é um domínio. Isto só é verificado quando $n = 0$ ou n é um número primo (veja Proposição 7.3.4 e Problema 2.3). Portanto, a característica de um domínio ou é zero ou é um número primo.

Sejam $\rho\colon \mathbb{Z} \to A$ o homomorfismo característico e A' um subanel de A. Como $1 \in A'$, temos que $\rho(\mathbb{Z}) \subset A'$. Portanto, $\rho(\mathbb{Z})$ é o menor subanel de A. Daí segue-se, em particular, que a característica de qualquer subanel de A é igual à característica de A.

Seja K um corpo de característica > 0. Como K é um domínio de integridade, a sua característica é um número primo p, então K contém o corpo $\rho(\mathbb{Z}) \simeq \mathbb{Z}_p$. Além disso, $\rho(\mathbb{Z})$ é o menor subcorpo de K, chamado de corpo primo de K e denotado por K_0.

Se K é um corpo de característica zero, então o homomorfismo característico ρ é injetor e, portanto, pela Proposição 2.2.2, existe um homomorfismo de anéis

$$\tilde{\rho}\colon \mathbb{Q} \to K.$$

Como $\mathbb{Q}$ é um corpo, temos que $\tilde{\rho}$ é um homomorfismo injetor (veja o Corolário 7.2.4). Se K' é um subcorpo de K, então $\mathbb{Q} \simeq \tilde{\rho}(\mathbb{Q}) \subset K'$ e, portanto, $\tilde{\rho}(\mathbb{Q})$ é o menor subcorpo de K, chamado também, nesse caso, de corpo primo de K e denotado por K_0.

Exemplos

1. Como $\rho\colon \mathbb{Z} \to \mathbb{Z}$ e $\rho\colon \mathbb{Z} \to \mathbb{Q}$ são injetoras, temos que $\mathrm{car}(\mathbb{Z}) = \mathrm{car}(\mathbb{Q}) = 0$. Mais geralmente, se A é um anel ordenado, pela Proposição 3.1.12, temos que $\mathrm{car}(A) = 0$.

2. Seja $n \in \mathbb{N}$, com $n > 1$. Como $N(\rho) = I(n)$, onde ρ é o homomorfismo característico de $\mathbb{Z}$ em $\mathbb{Z}_n$, temos que $\mathrm{car}(\mathbb{Z}_n) = n$.

3. Seja $\rho\colon \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}$. É claro que ρ é injetora, logo $\mathrm{car}(\mathbb{Z}_2 \times \mathbb{Z}) = 0$.

4. Seja $\rho\colon \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$. Temos que $\rho(1)$, $\rho(2)$, $\rho(3)$, $\rho(4)$, $\rho(5) \neq 0$ e $\rho(6) = 0$, logo $N(\rho) = I(6)$ (justifique). Portanto, $\mathrm{car}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$.

O próximo resultado possui várias aplicações.

Teorema 7.3.5. *Sejam A um domínio principal e $a_1, \ldots, a_n \in A \setminus A^*$. Considere o homomorfismo*

$$\begin{array}{rccc} h\colon & A & \longrightarrow & A/I(a_1) \times \cdots \times A/I(a_n) \\ & a & \longmapsto & ([a_1], \ldots, [a_n]) \end{array}$$

Temos que

i) $N(h) = I(m)$, *onde m é um mínimo múltiplo comum de $a_1, \ldots, a_n$.*

ii) *Se a_i e a_j são primos entre si, para todos i, j, com $i \neq j$, então h é sobrejetora.*

Demonstração (i) Como $h(a) = 0 \iff a \in I(a_1) \cap \cdots \cap I(a_n)$, segue-se que $N(h) = I(a_1) \cap \cdots \cap I(a_n)$. Portanto, $N(h) = I(m)$ com m um mmc de $a_1, \ldots, a_n$ (veja Problema 2.8, Capítulo 4).
(ii) Ponha $b = a_1 \cdots a_n$. É claro que, sendo a_i e a_j primos entre si, para $i \neq j$, tem-se que b_i e a_i são primos entre si, onde $b_i = \frac{b}{a_i}$. Logo, existem $r_i, s_i \in A$ tais que

$$r_i a_i + s_i b_i = 1. \tag{1}$$

Dado $([c_1],\dots,[c_n]) \in A/I(a_1)\times\cdots\times A/I(a_n)$, como $a_i \mid b_j$ se $i \neq j$, temos que

$$a = c_1 s_1 b_1 + \cdots + c_n s_n b_n\,,$$

é tal que

$$a \equiv c_i s_i b_i \bmod a_i. \tag{2}$$

De (1) temos que

$$s_i b_i \equiv 1 \bmod a_i\,,$$

logo de (2) segue-se que

$$a \equiv c_i \bmod a_i\,.$$

Consequentemente,

$$h(a) = ([c_1],\dots,[c_n]),$$

provando assim que h é sobrejetora. □

Corolário 7.3.6. *Se* $a_1,\dots,a_n \in \mathbb{N}\setminus\{1\}$*, então*

$$\mathrm{car}(\mathbb{Z}_{a_1}\times\cdots\times\mathbb{Z}_{a_n}) = \mathrm{mmc}(a_1,\dots,a_n).$$

Corolário 7.3.7. *Se* A *é um domínio principal e* $a_1,\dots,a_n \in A\backslash A^*$ *são não nulos e dois a dois primos entre si, então*

$$A/I(a_1\cdots a_n) \simeq A/I(a_1)\times\cdots\times A/I(a_n).$$

Demonstração Note que a hipótese implica que $a_1\cdots a_n$ é um mmc de $a_1,\dots,a_n$ e o resultado segue-se dos Teoremas 7.3.5 e 7.3.2. □

O corolário acima chama-se *O Teorema Chinês dos Restos* e no caso de $A=\mathbb{Z}$ pode ser interpretado como a seguir:

Dados $a_1,\dots,a_n \in \mathbb{Z}\backslash\{0,-1,1\}$ dois a dois primos entre si e dados $x_i \in \mathbb{Z}$, $i=1,\dots,n$, existe um único $[x] \in \mathbb{Z}_{a_1\cdots a_n}$ tal que $[x]=[x_i]$ em $\mathbb{Z}_{a_i}$, para $i=1,\dots,n$.

Em outras palavras, o sistema de congruências

$$\begin{cases} x \equiv x_1 & \bmod a_1 \\ x \equiv x_2 & \bmod a_2 \\ \quad\cdots & \\ x \equiv x_n & \bmod a_n \end{cases}$$

admite uma única solução módulo $a_1 \cdots a_n$.

Temos o seguinte resultado envolvendo a função Φ de Euler, já provado anteriormente.

Corolário 7.3.8. *Se* $m, n \in \mathbb{Z}\backslash\{0, \pm 1\}$, *com* $(m, n) = 1$, *então*

$$\Phi(m \cdot n) = \Phi(m)\Phi(n).$$

Demonstração Pelo Corolário 7.3.7, temos um isomorfismo $\mathbb{Z}_{n \cdot m} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$. Como isomorfismos estabelecem uma bijeção entre os elementos inertíveis de cada anel e como os elementos invertíveis de $\mathbb{Z}_m \times \mathbb{Z}_n$ são os pares ordenados cujas primeiras componentes são elementos invertíveis de $\mathbb{Z}_m$ e as segundas componentes elementos invertíveis de $\mathbb{Z}_n$ (veja Proposição 7.1.5), segue-se que $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$. □

O Corolário 7.3.8 acima nos dá uma outra demonstração da Proposição 6.4.2.

Problemas

3.1 Sejam A um domínio, $a \in A$ e $n \in \mathbb{Z}$. Mostre que $na = 0$ se, e somente se, $a = 0$ ou $\mathrm{car}(A) \mid n$.

3.2 Sejam A um domínio de característica $p > 0$ e $q = p^\alpha$ para algum $\alpha \in \mathbb{N}$.

a) Mostre que para todo $x, y \in A$, temos que

$$(x + y)^q = x^q + y^q.$$

b) Mostre que

$$\begin{aligned} F_q \colon A &\longrightarrow A \\ x &\longmapsto x^q \end{aligned}$$

é um homomorfsimo injetor. Se A é finito, conclua que F_q é um isomorfismo.

Sugestão Use o Corolário 3.1.5 para provar a segunda parte de (b).

3.3 Seja A um domínio com corpo de frações K. Mostre que

$$\mathrm{car}(K) = \mathrm{car}(A).$$

3.4 Sejam A e B anéis de características respectivamente n e m. Mostre que

$$\mathrm{car}(A \times B) = \text{ mmc } (m, n).$$

3.5 Mostre que todo anel ordenado tem característica zero. Conclua que todo anel ordenado é infinito.

Sugestão Use a Proposição 3.1.12.

8

Os números reais

Aproximadamente dois milênios e meio passaram-se desde a descoberta pelos pitagóricos da irracionalidade de $\sqrt{2}$ até a construção rigorosa dos números reais realizada pela escola alemã na segunda metade do século dezenove.

Ao descobrir a existência dos números irracionais, os pitagóricos viram ruir a sua crença de que os números inteiros eram suficientes para tratar todos os problemas matemáticos. Cerca de um século depois, Eudoxo (408-355 A.C.) criava a sua teoria das proporções para fundamentar o uso das grandezas irracionais em geometria. Os trabalhos de Eudoxo foram expostos por Euclides nos Elementos, sendo praticamente tudo que existe na direção da conceituação dos números reais até o século dezenove.

A preocupação com os fundamentos dos números reais só voltou na primeira metade do século dezenove, motivada pelo desenvolvimento da Análise Matemática realizado principalmente por Gauss, Abel e Cauchy. A teoria foi ultimada na segunda metade daquele século com duas construções diferentes dos números reais realizadas por Dedekind e Cantor. Os dois métodos têm em comum apenas o ponto de partida, o corpo ordenado dos números racionais. O método de Dedekind baseia-se na noção de corte no corpo ordenado dos números racionais e não é passível de ser utilizado em outras situações. O método de Cantor, que aqui adotamos, é muito engenhoso e baseia-se no uso de sequências convergentes e de Cauchy de números racionais. A construção de Cantor tem a vantagem

de ser aplicável em muitos outros contextos, enquanto a de Dedekind só serve para construir os reais a partir dos racionais.

No final do capítulo, faremos a conexão com a Análise através do chamado Princípio do Supremo. A compreensão dos números reais propiciou o impressionante desenvolvimento da Análise Matemática registrado durante o século vinte.

1 Sequências convergentes

Nesta seção, introduziremos as definições e resultados básicos sobre as sequências convergentes num corpo ordenado, preparando o terreno para a construção dos números reais.

Daqui por diante, K será um corpo ordenado, portanto de característica zero (veja Problema 3.5, Capítulo 7).

Recorde que uma sequência $\mathbf{x} = (x_n)$ em K é um elemento do anel $S(K) = \mathcal{F}(\mathbb{N} \setminus \{0\}, K)$, das funções de $\mathbb{N} \setminus \{0\}$ em K, onde as operações de adição e multiplicação são dadas por

$$\mathbf{x} + \mathbf{y} = (x_n + y_n) \qquad \text{e} \qquad \mathbf{x} \cdot \mathbf{y} = (x_n \cdot y_n),$$

se $\mathbf{x} = (x_n)$ e $\mathbf{y} = (y_n)$.

Usaremos a seguinte notação:

$$K_+^* = \{x \in K;\ x > 0\}.$$

Uma sequência $\mathbf{x} = (x_n) \in S(K)$ será dita *convergente* em K quando existir um elemento $x \in K$ tal que, para todo $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ com a propriedade

$$|x_n - x| < \varepsilon\,, \quad \forall\, n > N.$$

Um elemento x como acima, se existir, será chamado de *limite* da sequência $\mathbf{x}$. Neste caso, diremos também que a sequência $\mathbf{x}$ *converge* para x.

Relacionado com esta definição, temos o seguinte resultado:

Proposição 8.1.1. *Uma sequência convergente possui um único limite.*

Demonstração Suponha, por absurdo, que x e y sejam dois limites distintos de uma sequência $\mathbf{x}$. Portanto, dado $\varepsilon = \frac{1}{2}|y - x| > 0$, pela definição de convergência, existem N_1 e N_2 em $\mathbb{N}$ tais que

$$|x_n - x| < \varepsilon, \quad \forall\, n > N_1 \quad \text{e} \quad |x_n - y| < \varepsilon, \quad \forall\, n > N_2\,.$$

Tomando $N > \max\{N_1, N_2\}$, temos que

$$|x_N - x| < \varepsilon \quad \text{e} \quad |x_N - y| < \varepsilon,$$

e a Proposição 2.1.4 fornece

$$|y - x| = |x_N - x + y - x_N| \leq |x_N - x| + |x_N - y| < 2\varepsilon = |y - x|,$$

o que é um absurdo. □

No caso em que $\mathbf{x}$ é uma sequência cujo limite é x, escrevemos

$$\lim \mathbf{x} = x,$$

ou ainda,

$$\lim_{n\to\infty} x_n = x.$$

Denotando por $S_c(K)$ o subconjunto de $S(K)$ das sequências convergentes, a proposição acima nos garante que é bem definida a aplicação

$$\begin{array}{rccc} \lim\colon & S_c(K) & \longrightarrow & K \\ & \mathbf{x} & \longmapsto & \lim \mathbf{x} \end{array}$$

Uma sequência que não é convergente será dita *divergente*.

Se $x \in K$, denotaremos por x^* a sequência constante $x_n = x$, para todo $n \in \mathbb{N}$. É claro que

$$\lim x^* = x.$$

Decorre imediatamente das definições que uma sequência $\mathbf{x}$ converge para x se, e somente se, a sequência $\mathbf{x} - x^*$ converge para zero.

Considerando a aplicação

$$\begin{array}{rccc} \psi\colon & K & \to & S(K) \\ & x & \mapsto & x^* \end{array}$$

que é um homomorfismo injetor de anéis (leitor, prove), concluímos que K é isomorfo ao subcorpo $\psi(K)$ de $S(K)$. Podemos, assim, identificar K com um subcorpo de $S(K)$, identificando $x \in K$ com $x^* \in S_c(K) \subset S(K)$.

Denotaremos por $S_0(K)$ o subconjunto de $S_c(K)$ das *sequências nulas*, isto é, das sequências que convergem para zero.

Exemplos

1. A sequência $\mathbf{x}$ em $S(\mathbb{Q})$ definida por $x_0 = 1$ e $x_n = \frac{1}{n}$, se $n > 0$, converge para zero. De fato, dado $\varepsilon \in \mathbb{Q}_+^*$, tome N um inteiro maior do que $\frac{1}{\varepsilon}$, o que é possível pela propriedade arquimediana de $\mathbb{Q}$ (veja Problema 2.6, Capítulo 2). Temos para $n > N$ que

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} < \frac{1}{N} < \varepsilon.$$

2. A sequência definida por $x_n = (-1)^n$ é divergente em qualquer corpo ordenado K (justifique).

Uma sequência $\mathbf{x} = (x_n) \in S(K)$ será dita *limitada superiormente* (respectivamente, *limitada inferiormente*) se existir $L \in K$ tal que para todo $n \in \mathbb{N}$ se tenha $x_n \leq L$ (respectivamente, $L \leq x_n$). Uma sequência limitada superiormente e inferiormente será dita *limitada*. Decorre facilmente da definição que $\mathbf{x} = (x_n)$ é limitada se, e somente se, existe $B \in K_+^*$ tal que $|x_n| \leq B$, para todo $n \in \mathbb{N}$. O subconjunto de $S(K)$ das sequências limitadas será denotado por $S_\ell(K)$.

Proposição 8.1.2. *Toda sequência convergente é limitada.*

Demonstração Suponha que $\lim \mathbf{x} = x$, logo dado $\varepsilon = 1$, existe um número natural N tal que se $n > N$, então $|x_n - x| < 1$. Como $|x_n| - |x| \leq |x_n - x|$ (cf. Corolário 2.1.5), temos que se $n > N$, então $|x_n| - |x| < 1$ e, consequentemente, $|x_n| < 1 + |x|$. Pondo

$$B = \max\{|x_0|, \ldots, |x_N|, 1 + |x|\},$$

temos, para todo $n \in \mathbb{N}$, que $|x_n| \leq B$. Portanto, $\mathbf{x}$ é limitada. □

Assim, temos a seguinte cadeia de inclusões:

$$K \subset S_0(K) \subset S_c(K) \subset S_\ell(K) \subset S(K).$$

Proposição 8.1.3. *Sejam* $\mathbf{x}, \mathbf{y} \in S_c(K)$. *Então* $\mathbf{x}+\mathbf{y}$ *e* $\mathbf{x}-\mathbf{y}$ *pertencem a* $S_c(K)$ *e*

$$\lim(\mathbf{x} \pm \mathbf{y}) = (\lim \mathbf{x}) \pm (\lim \mathbf{y}).$$

Demonstração Suponha que $\lim \mathbf{x} = x$ e $\lim \mathbf{y} = y$. Dado $\varepsilon \in K_+^*$, existem N_1 e N_2 em $\mathbb{N}$ tais que

$$|x_n - x| < \frac{\varepsilon}{2}, \quad \forall\, n > N_1, \quad \text{e}$$

$$|y_n - y| < \frac{\varepsilon}{2}, \quad \forall\, n > N_2\,.$$

Seja $N = \max\{N_1, N_2\}$. Logo, se $n > N$, temos que

$$|x_n \pm y_n - (x \pm y)| = |(x_n - x) \pm (y_n - y)| \leq |x_n - x| + |y_n - y| < \varepsilon,$$

provando o resultado. □

Da proposição, decorre imediatamente o seguinte corolário:

Corolário 8.1.4. *Se* $\mathbf{x}, \mathbf{y} \in S_c(K)$ *são tais que* $\lim \mathbf{x} = \lim \mathbf{y}$, *então* $\mathbf{x} - \mathbf{y}$ *é uma sequência nula.*

Proposição 8.1.5. *Sejam* $\mathbf{x}, \mathbf{y} \in S(K)$. *Se* $\mathbf{x}$ *é limitada e* $\mathbf{y}$ *é uma sequência nula, então* $\mathbf{x} \cdot \mathbf{y}$ *é uma sequência nula.*

Demonstração Como $\mathbf{x}$ é limitada, existe $B \in K_+^*$ tal que $|x_n| \leq B$, para todo $n \in \mathbb{N}$. Como $\lim \mathbf{y} = 0$, temos que dado $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que

$$|y_n| = |y_n - 0| < \frac{\varepsilon}{B}, \quad \forall\, n > N.$$

Portanto, para $n > N$, temos que

$$|x_n y_n - 0| = |x_n|\,|y_n| < B\,\frac{\varepsilon}{B} = \varepsilon,$$

provando assim o resultado. □

Proposição 8.1.6. *Sejam* $\mathbf{x}, \mathbf{y} \in S(K)$. *Se* $\mathbf{x}$ *e* $\mathbf{y}$ *são convergentes, então* $\mathbf{x} \cdot \mathbf{y}$ *é convergente e* $\lim(\mathbf{x} \cdot \mathbf{y}) = (\lim \mathbf{x}) \cdot (\lim \mathbf{y})$.

Demonstração Suponha que $\lim \mathbf{x} = x$ e $\lim \mathbf{y} = y$. Vamos provar que a sequência $\mathbf{x} \cdot \mathbf{y} - (x \cdot y)^*$ converge para zero. De fato, como $\mathbf{y}$ é convergente, pela Proposição 8.1.2 ela é limitada. Por outro lado, a sequência $\mathbf{x} - x^*$ converge para zero. Portanto, pela Proposição 8.1.5, temos que

$$\lim(\mathbf{x} - x^*) \cdot \mathbf{y} = 0.$$

De modo análogo, conclui-se que

$$\lim x^* \cdot (\mathbf{y} - y^*) = 0.$$

Usando as duas igualdades acima, a Proposição 8.1.3 e a igualdade

$$\mathbf{x} \cdot \mathbf{y} - (x \cdot y)^* = \mathbf{x} \cdot \mathbf{y} - x^* \cdot y^* = (\mathbf{x} - x^*) \cdot \mathbf{y} + x^* \cdot (\mathbf{y} - y^*),$$

segue-se que

$$\lim(\mathbf{x}\cdot\mathbf{y}-(x\cdot y)^*)=0.$$

□

Teorema 8.1.7. *O conjunto* $S_c(K)$ *é um subanel de* $S(K)$ *e a aplicação* $\lim\colon S_c(K)\to K$ *é um homomorfismo sobrejetor de anéis cujo núcleo é* $S_0(K)$.

Demonstração Os fatos de que $S_c(K)$ é um subanel de $S(K)$ e lim é um homomorfismo decorrem das Proposições 8.1.3 e 8.1.6. É claro que o núcleo de lim é $S_0(K)$ e que ele é sobrejetor, já que para $x\in K$, tem-se $\lim x^*=x$. □

Corolário 8.1.8. Tem-se um isomorfismo entre $S_c(K)/S_0(K)$ e K.

Demonstração Isto é consequência direta dos Teoremas 8.1.7 e 7.3.2. □

Uma sequência $\mathbf{x}=(x_n)\in S(K)$ será dita *monótona crescente* (respectivamente, *monótona decrescente*), se para todos n e m em $\mathbb{N}\setminus\{0\}$ tais que $n\geq m$, se tenha $x_n\geq x_m$ (respectivamente, $x_n\leq x_m$).

Uma sequência $\mathbf{y}\in S(K)$ será chamada de *subsequência* de uma sequência $\mathbf{x}\in S(K)$, se existir uma sequência injetora e monótona crescente $\mathbf{i}\colon\mathbb{N}\setminus\{0\}\to\mathbb{N}\setminus\{0\}$ tal que $\mathbf{y}=\mathbf{x}\circ\mathbf{i}$. Temos, portanto, que $y_n=x_{i_n}$. Uma classe especial de subsequências de $\mathbf{x}$ é dada pela composição com as translações

$$\begin{aligned}\tau_r\colon\mathbb{N}\setminus\{0\}&\longrightarrow\mathbb{N}\setminus\{0\},\\ n&\longmapsto n+r\end{aligned}$$

onde r é um número natural.

Proposição 8.1.9. *Seja* $\mathbf{x}\in S_c(K)$. *Então, para toda sequência injetora e monótona crescente* $\mathbf{i}\colon\mathbb{N}\to\mathbb{N}$, *tem-se que* $\mathbf{x}\circ\mathbf{i}\in S_c(K)$ *e*

$$\lim\mathbf{x}\circ\mathbf{i}=\lim\mathbf{x}.$$

Demonstração Suponha que $\lim\mathbf{x}=x$, logo dado $\varepsilon\in K_+^*$, existe N_1 tal que

$$|x_m-x|<\varepsilon,\quad\forall\, m>N_1\,.$$

Como $\mathbf{i}$ é injetora e monótona crescente, temos que existe $N\in\mathbb{N}$ tal que $i_n>N_1\,,\ \ \forall\, n>N$. Portanto, temos que

$$|x_{i_n}-x|<\varepsilon,\quad\forall\, n>N.$$

Assim, $\mathbf{x} \circ \mathbf{i} \in S_c(K)$ e $\lim \mathbf{x} \circ \mathbf{i} = \lim \mathbf{x}$. □

A proposição acima, nos diz que toda subsequência de uma sequência convergente é convergente e o seu limite é igual ao limite da sequência.

Problemas

1.1 Mostre que $S_\ell(K)$ é um subanel de $S(K)$.

1.2 Mostre que $S_0(K)$ é um ideal de $S_\ell(K)$.

1.3 Sejam $\mathbf{i}, \mathbf{j}\colon \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ duas sequências injetoras e monótonas crescentes. Considere

$$\begin{aligned} \mathbf{i}^*\colon S(K) &\longrightarrow S(K) \\ \mathbf{x} &\longmapsto \mathbf{x} \circ \mathbf{i} \end{aligned}$$

a) Mostre que $\mathbf{i}^*$ é um homomorfismo de anéis.

b) Determine o núcleo de $\mathbf{i}^*$.

c) Mostre que $\mathbf{i}^*(S_c(K)) = S_c(K)$ e que $\mathbf{i}^*(S_\ell(K)) = S_\ell(K)$.

d) Mostre que $(\mathbf{i} \circ \mathbf{j})^* = \mathbf{j}^* \circ \mathbf{i}^*$.

1.4 Seja $\mathbf{x} \in S_c(K)$ e seja $x = \lim \mathbf{x}$. Mostre que o isomorfismo do Corolário 8.1.8 é dado por

$$\mathbf{x} + S_0(K) \;\mapsto\; x,$$

e o seu inverso é

$$x \;\mapsto\; x^* + S_0(K).$$

1.5 Se $\mathbf{x} = (x_n) \in S_c(K)$, defina a sequência $\mathbf{y} = (|x_n|)$. Mostre que $\mathbf{y} \in S_c(K)$ e $\lim \mathbf{y} = |\lim \mathbf{x}|$.

1.6 Sejam $\mathbf{x}, \mathbf{y} \in S_c(K)$ e suponha que exista $N \in \mathbb{N}$ tal que

$$x_n \geq y_n\,, \quad \forall\, n > N.$$

Mostre que $\lim \mathbf{x} \geq \lim \mathbf{y}$.

2 Corpos Arquimedianos

A restrição a $\mathbb{N} \setminus \{0\}$ do homomorfismo característico ρ de um corpo (ordenado) K é uma sequência que também denotaremos por ρ. Diremos que K é um *corpo arquimediano* se a sequência ρ não for limitada.

Lema 8.2.1. *K é um corpo arquimediano se, e somente se, quaisquer que sejam $a, b \in K$, com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $nb > a$.*

Demonstração Suponha que K seja arquimediano e sejam $a, b \in K$ com $b \neq 0$. Então existe $m \in \mathbb{N}$ tal que $m1 > \left|\frac{a}{b}\right|$, logo $m|b| > |a| \geq a$. Portanto, $nb > a$, onde $n = \pm m$, segundo se $b > 0$ ou $b < 0$. A recíproca é imediata. □

Exemplos

1. O corpo ordenado $\mathbb{Q}$ é arquimediano (ver Problema 2.6, Capítulo 2).

2. Exemplo de um corpo ordenado não arquimediano. Este exemplo se destina ao leitor que tenha alguma familiaridade com os polinômios, os quais serão estudados detalhadamente no Volume 2.

Seja $\mathbb{Q}[x]$ o conjunto dos polinômios numa indeterminada x com coeficientes em $\mathbb{Q}$. Com a adição e multiplicação de polinômios, $\mathbb{Q}[x]$ é um domínio de integridade. Se

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[x] \setminus \{0\},$$

com $a_n \neq 0$, chamamos a_n de *coeficiente líder* de $p(x)$ e o denotamos por $cl(p(x))$. Define-se o coeficiente líder do polinômio zero como sendo zero, isto é, $cl(0) = 0$. É fácil verificar que a seguinte relação em $\mathbb{Q}[x]$:

$$p(x) \leq q(x) \iff cl(q(x) - p(x)) \geq 0,$$

é uma relação de ordem total, munindo $\mathbb{Q}[x]$ de uma estrutura de anel ordenado.

Seja $\mathbb{Q}(x)$ o corpo de frações do domínio $\mathbb{Q}[x]$, que pelo Teorema 2.2.3 sabemos ser um corpo ordenado. Observe agora que, para todo $n \in \mathbb{N}$, temos $n1 < x$ em $\mathbb{Q}(x)$. Logo, $\mathbb{Q}(x)$ não é arquimediano.

O seguinte resultado nos fornecerá uma caracterização importante dos corpos arquimedianos.

Proposição 8.2.2. *Sejam K um corpo ordenado e K_0 ($\simeq \mathbb{Q}$) o seu corpo primo. As asserções abaixo são equivalentes.*

i) K *é arquimediano.*

ii) *Dados* $a, b \in K$*, quaisquer, com* $a < b$*, existe* $r \in K_0$ *tal que*

$$a < r < b.$$

iii) *Todo elemento de* K *é limite de uma sequência em* K_0 *.*

Demonstração (i) $\Rightarrow$ (ii) Sendo K arquimediano e $b - a \neq 0$, pelo Lema 8.2.1, existe $n \in \mathbb{Z}$ tal que

$$n(b-a) > 1.$$

Como $b - a > 0$, é claro que $n > 0$ e, portanto,

$$\frac{1}{n1} < b - a. \tag{1}$$

Por outro lado, seja

$$S = \{x \in \mathbb{Z};\ x1 > na\}.$$

Pelo fato de K ser arquimediano, temos que $S \neq \emptyset$. Temos também que S é limitado inferiormente, pois se $\ell \in \mathbb{Z}$ é tal que $\ell 1 > -a$, então, para todo $x \in S$,

$$x1 > na > -n\ell 1,$$

e, portanto, $x > -n\ell$ (o homomorfismo característico é ordenado!). Seja $m = \min S$ (que existe pelo PBO). Temos então que $m1 > na$, isto é,

$$\frac{m1}{n1} > a, \tag{2}$$

e $(m-1)1 \leq na$, ou seja,

$$\frac{(m-1)1}{n1} \leq a. \tag{3}$$

De (1), (2) e (3) temos que

$$a < \frac{m1}{n1} = \frac{(m-1)1}{n1} + \frac{1}{n1} < a + b - a = b,$$

e o resultado segue-se tomando $r = \frac{m1}{n1}$.

(ii) $\Rightarrow$ (iii) Seja $a \in K$. Para cada $n \in \mathbb{N} \setminus \{0\}$, temos por hipótese que existe $r_n \in K_0$ tal que

$$a - \frac{1}{n1} < r_n < a + \frac{1}{n1},$$

isto é,

$$|a - r_n| < \frac{1}{n1}\,.$$

Seja $\varepsilon \in K_+^*$, logo de (ii) existe $\varepsilon' \in K_0$ tal que $0 < \varepsilon' < \varepsilon$. Como $\varepsilon' \in K_0$ e K_0 é ordenadamente isomorfo a $\mathbb{Q}$, que é arquimediano, temos que existe $N \in \mathbb{N}$ tal que

$$\frac{1}{n1} < \varepsilon', \quad \forall\, n > N.$$

Temos então que

$$|a - r_n| < \frac{1}{n1} < \varepsilon' < \varepsilon, \quad \forall\, n > N.$$

Definindo a sequência $\mathbf{r}$ com $r_0 = 1$ e r_n, para $n > 0$, como acima, temos que $\mathbf{r} \in S(K_0)$ e $\lim \mathbf{r} = a$.

(iii) $\Rightarrow$ (i) Dado $a \in K$, devemos mostrar que existe $m \in \mathbb{N}$ tal que

$$a < m1.$$

De fato, seja $(r_n) \in S(K_0)$ tal que

$$\lim_{n\to\infty} r_n = a + 1.$$

Agora, dado $\varepsilon = \frac{1}{2}$, existe $N \in \mathbb{N}$ tal que

$$|r_N - (a+1)| < \frac{1}{2}.$$

Portanto,

$$a < (a+1) - \frac{1}{2} < r_N\,. \tag{4}$$

Como $K_0\,(\simeq \mathbb{Q})$ é arquimediano, existe $m \in \mathbb{N}$ tal que $r_N < m1$, logo de (4) segue-se que $a < m1$, provando assim o resultado. □

Uma *série* num corpo ordenado K é uma soma infinita

$$a_1 + a_2 + \cdots + a_n + \cdots\,,$$

com os a_i em K. Diremos que a *série é convergente*, se for convergente a sequência $\mathbf{s} = (s_n)$, definida por

$$s_n = a_1 + a_2 + \cdots + a_n\,.$$

A *soma da série* é, por definição, o limite da sequência $\mathbf{s}$.

Problemas

2.1 Seja K um corpo arquimediano e sejam $a, b \in K_+^*$. Mostre que existe um, e somente um, inteiro positivo m tal que

$$(m-1)a \leq b < ma.$$

Sugestão Considere o conjunto $S = \{n \in \mathbb{N};\ na > b\}$. Mostre que $S \neq \emptyset$ e tome $m = \min S$.

2.2 Seja $\mathbf{x} = (x_n) \in S(K)$ a sequência definida por $x_0 = 1$ e

$$x_n = \frac{1}{n1}, \quad \forall\, n \in \mathbb{N} \setminus \{0\}.$$

a) Mostre que se K é arquimediano, então $\mathbf{x}$ converge para zero.

b) Mostre que se $K = \mathbb{Q}(x)$, então a sequência $\mathbf{x}$ não converge para zero.

2.3 Seja K um corpo arquimediano e sejam $b, c \in K$, com $b > 1$. Mostre que existe $n \in \mathbb{N}$ tal que $b^n > c$.

Sugestão Adapte a demonstração do Corolário 3.1.20.

2.4 Seja K um corpo arquimediano. Mostre que se $a \in K$ com $|a| < 1$, então $\lim_{n\to\infty} a^n = 0$.

Sugestão Analise separadamente os casos $a = 0$ e $a \neq 0$. Se $a \neq 0$, use o Problema 2.3 para mostrar que dado $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que $1/|a|^N > 1/\varepsilon$. Aplique a definição de limite, observando que a sequência $(|a|^n)$ é monótona decrescente.

2.5 Suponha que K seja arquimediano. Sejam $a, q \in K$ com $|q| < 1$. Mostre que a *série geométrica*

$$a + aq + aq^2 + \cdots$$

converge para $\frac{a}{1-q}$.

Sugestão Use o Problema 1.7, Capítulo 3, para escrever compactamente s_n e calcule $\lim_{n\to\infty} s_n$, usando o Problema 2.4.

2.6 Calcule a soma da seguinte série em $\mathbb{Q}$:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$

3 Sequências fundamentais

Um corpo ordenado L será dito uma *extensão ordenada* de um corpo ordenado K, se L é uma extensão de K, tal que a restrição da ordenação de L a K coincide com a ordenação de K.

Na primeira seção do presente capítulo, estabelecemos um isomorfismo entre um corpo K e o anel quociente $S_c(K)/S_0(K)$ (veja o Corolário 8.1.8).

Tomando $K = \mathbb{Q}$, isto permite identificar um número racional x com a classe residual módulo $S_0(\mathbb{Q})$ de x^* (ou de qualquer sequência $\mathbf{x}$ em $S_c(\mathbb{Q})$ que tenha por limite o número x). Mais precisamente, se $x \in \mathbb{Q}$, então identifica-se x com $[x^*] = x^* + S_0(\mathbb{Q})$. Desenvolvendo esta ideia, Cantor idealizou a seguinte estratégia para ampliar o corpo dos números racionais a fim de obter o corpo dos números reais. A idéia consiste em definir um número real como sendo uma classe residual módulo $S_0(\mathbb{Q})$ de uma sequência de $\mathbb{Q}$ de um tipo especial, mais precisamente, de uma sequência de $\mathbb{Q}$ que possa convergir em alguma extensão ordenada de $\mathbb{Q}$.

Seja L um corpo ordenado arbitrário. Uma sequência $\mathbf{x} = (x_n)$ em $S(L)$ será chamada de *sequência fundamental* ou *sequência de Cauchy* em L, se o valor absoluto da diferença entre dois termos da sequência tende a zero à medida que os seus índices aumentam. Formalmente, isto se expressa como a seguir:

$\mathbf{x} = (x_n) \in S(L)$ é uma sequência fundamental em L, se para todo $\varepsilon \in L_+^*$, existe $N \in \mathbb{N}$ tal que, para todos $m, n \in \mathbb{N}$ com $m, n > N$, se tenha

$$|x_m - x_n| < \varepsilon.$$

É claro que se $\mathbf{x} \in S(K)$ é fundamental em alguma extensão ordenada L de K, então ela é fundamental em K.

O próximo resultado nos fornecerá a relação entre sequências convergentes e sequências fundamentais.

Proposição 8.3.1. *Toda sequência convergente é fundamental.*

Demonstração Seja $\mathbf{x} = (x_n) \in S_c(K)$ e suponha que $\lim \mathbf{x} = x$. Temos que, para todo $\varepsilon \in K_+^*$, existe $N \in \mathbb{N}$ tal que se $n > N$, então

$$|x_n - x| < \frac{\varepsilon}{2}\,.$$

Segue-se que, se $m, n > N$, então

$$|x_n - x_m| = |x_n - x - (x_m - x)| \leq |x_n - x| + |x_m - x| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

logo $\mathbf{x}$ é fundamental em K. □

A proposição acima nos fornece uma condição necessária, em termos de propriedades intrínsecas, para que uma sequência $\mathbf{x} \in S(K)$ seja convergente em alguma extensão ordenada de K. A condição é a seguinte:

Se uma sequência em K *é convergente em alguma extensão ordenada* L*, então ela é fundamental em* K*.*

Exemplo. A sequência $\mathbf{x} = (x_n) \in S(\mathbb{Q})$ definida por $x_n = (-1)^n$, não é fundamental, logo não converge em nenhuma extensão de $\mathbb{Q}$.

O próximo resultado nos dará um critério útil para que uma sequência definida num corpo arquimediano seja fundamental.

Proposição 8.3.2. *Toda sequência monótona crescente e limitada superiormente em um corpo arquimediano é fundamental.*

Demonstração Seja $\mathbf{x} = (x_n) \in S(K)$ uma sequência monótona crescente e limitada superiormente, onde K é arquimediano. Seja $c \in K$ tal que

$$x_n \leq c, \quad \forall\, n \in \mathbb{N}.$$

Seja $\varepsilon \in K_+^*$ e considere o conjunto

$$S = \left\{ z \in \mathbb{N};\ \ z1 \leq \frac{c - x_n}{\varepsilon},\ \forall\, n \in \mathbb{N} \right\}.$$

Então S é limitado superiormente. De fato, como K é arquimediano, existe $l > 0$ tal que $l1 > \frac{c-x_1}{2}$, e daí resulta que $k \notin S$ para todo $k \geq l$. Como $0 \in S$, segue-se da formulação equivalente (PBO′) do Princípio da Boa Ordenação, que S possui um maior elemento, que denotaremos por r. Como $r \in S$ e $r + 1 \notin S$, temos que

$$r\varepsilon \leq c - x_n, \quad \forall\, n \in \mathbb{N}$$

e existe $N \in \mathbb{N}$ tal que

$$c - x_N < (r + 1)\varepsilon.$$

Portanto, se $n \geq m > N$, temos pelas desigualdades acima e pelo fato de que $\mathbf{x}$ é monótona crescente, que

$$c - x_m \leq c - x_N < (r + 1)\varepsilon \leq c - x_n + \varepsilon,$$

logo

$$|x_n - x_m| = x_n - x_m < \varepsilon,$$

e, portanto, a sequência $\mathbf{x}$ é fundamental em K. □

A fim de dar um exemplo de uma sequência fundamental que não é convergente, considere a sequência $\mathbf{r} = (r_n)$ de K, definida recorrentemente como a seguir:

$$r_1 = 1, \qquad r_{n+1} = \frac{4r_n}{2 + r_n^2}, \quad \forall\, n \geq 1.$$

Lema 8.3.3. *Para todo* $n \in \mathbb{N} \setminus \{0\}$*, temos que* $r_n^2 < 2$ *e* $r_n \geq 1$.

Demonstração Por indução sobre n. Para $n = 1$, o resultado vale trivialmente.

Suponha que $r_n^2 < 2$ e $r_n \geq 1$, logo

$$r_{n+1}^2 = \frac{16r_n^2}{(2 + r_n^2)^2} = \frac{16r_n^2}{(2 - r_n^2)^2 + 8r_n^2} < \frac{16r_n^2}{8r_n^2} = 2,$$

e

$$r_{n+1} = \frac{4r_n}{2 + r_n^2} \geq \frac{4}{2 + 2} = 1.$$

□

Proposição 8.3.4; *A sequência* $\mathbf{r}$ *é fundamental.*

Demonstração Pelo Lema 8.3.3, segue-se que $\mathbf{r}$ é limitada superiormente. De fato, $r_n^2 < 2 < 4$, logo $r_n < 2$. Além disso, $\mathbf{r}$ é monótona crescente, pois

$$r_{n+1} - r_n = \frac{r_n(2 - r_n^2)}{2 + r_n^2} > 0.$$

Segue-se então, pela Proposição 8.3.2, que $\mathbf{r}$ é fundamental. □

A sequência $\mathbf{r}$ não é convergente em $\mathsf{K} = \mathbb{Q}$, pois se fosse convergente, com $\lim \mathbf{r} = \alpha \in \mathbb{Q}$, teríamos

$$\lim[r_{n+1}(2 + r_n^2)] = \lim 4r_n\,,$$

logo, pelas Proposições 8.1.3, 8.1.6 e 8.1.9, seguiria que

$$\alpha(2 + \alpha^2) = 4\alpha.$$

Observando que $\alpha \neq 0$ (pois $r_n \geq 1$ para todo $n \in \mathbb{N}$), segue-se que $\alpha^2 = 2$, o que não é possível para $\alpha \in \mathbb{Q}$.

O nosso objetivo será o de ampliar o corpo $\mathbb{Q}$ de modo que a sequência $\mathbf{r}$ passe a ter limite, obtendo assim um corpo contendo $\sqrt{2}$.

Proposição 8.3.4. *Toda sequência fundamental é limitada.*

Demonstração Seja $\mathbf{x} = (x_n)$ uma sequência fundamental. Tomando $\varepsilon = 1$, existe $N \in \mathbb{N}$ tal que, para todo $n > N$, tem-se que

$$|x_n| - |x_{N+1}| \leq |x_n - x_{N+1}| < 1.$$

Logo,

$$|x_n| < 1 + |x_{N+1}|, \quad \forall\, n > N.$$

Pondo $B = \max\{|x_0|, \ldots, |x_N|, 1 + |x_{N+1}|\}$, segue-se que

$$|x_n| \leq B, \quad \forall\, n \in \mathbb{N},$$

logo $\mathbf{x}$ é limitada. □

O conjunto das sequências fundamentais em K será denotado por $S_f(K)$.

Proposição 8.3.5. $S_f(K)$ é um subanel de $S(K)$.

Demonstração Note que toda sequência constante é fundamental. Em particular, as sequências $a_n = 1$ e $b_n = 0$, $\forall\, n \in \mathbb{N}$, pertencem a $S_f(K)$.

Sejam $\mathbf{x}, \mathbf{y} \in S_f(K)$. Pela Proposição 8.3.4, as sequências $\mathbf{x}$ e $\mathbf{y}$ são limitadas, logo existe $B \in K_+^*$ tal que

$$|x_n| \leq B \quad \text{e} \quad |y_n| \leq B, \qquad \forall\, n \in \mathbb{N}.$$

Dado $\varepsilon \in K_+^*$, existe N tal que se $m, n > N$, então

$$|x_m - x_n| < \frac{\varepsilon}{2B} \quad \text{e} \quad |y_m - y_n| < \frac{\varepsilon}{2B}\,.$$

Segue-se então que, se $m, n > N$,

$$\begin{aligned} |x_m y_m - x_n y_n| &= |x_m(y_m - x_n) + y_n(x_m - x_n)| \\ &\leq |x_m|\,|y_m - y_n| + |y_n|\,|x_m - x_n| \\ &\leq B\,\frac{\varepsilon}{2B} + B\,\frac{\varepsilon}{2B} = \varepsilon. \end{aligned}$$

Temos então que $\mathbf{x} \cdot \mathbf{y} = (x_n \cdot y_n)$ é fundamental em K.
Por outro lado, dado $\varepsilon \in K_+^*$, existe N tal que se $m, n > N$, então

$$|x_m - x_n| \leq \frac{\varepsilon}{2} \quad \text{e} \quad |y_m - y_n| \leq \frac{\varepsilon}{2}.$$

Logo, se $m, n > N$, temos que

$$|x_m - y_m - (x_n - y_n)| \leq |x_m - x_n| + |y_n - y_m| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Temos então que $\mathbf{x} - \mathbf{y} = (x_n - y_n)$ é fundamental em K.

Pela Proposição 7.1.1, $S_f(K)$ é um subanel de $S(K)$. □

Proposição 8.3.6. *O conjunto* $S_0(K)$ *das sequências nulas de* K *forma um ideal de* $S_f(K)$.

Demonstração Isto decorre dos fatos de que a soma de duas sequências nulas é claramente uma sequência nula, o produto de uma sequência nula por uma sequência limitada é uma sequência nula (Proposição 8.1.5) e toda sequência fundamental é limitada (Proposição 8.3.4). □

A próxima proposição nos será de grande utilidade.

Proposição 8.3.7. *Seja* $\mathbf{x} = (x_n) \in S_f(K) \setminus S_0(K)$. *Então existem* $c \in K_+^*$ *e* $N \in \mathbb{N}$ *tais que* $|x_n| > c, \quad \forall n > N$.

Demonstração A afirmação $\mathbf{x} \notin S_0(K)$ significa que existe $a \in K_+^*$ tal que, para todo $N \in \mathbb{N}$, existe $\ell > N$ para o qual $|x_\ell| \geq a$.

Como $\mathbf{x} \in S_f(K)$, existe $N \in \mathbb{N}$ tal que se $m, n > N$, então

$$||x_n| - |x_m|| \leq |x_n - x_m| < \frac{a}{2}.$$

Sja l o inteiro maior do que N tal que $|x_l| \geq a$. Logo, para $n > N$, temos que

$$|x_n| > |x_l| - \frac{a}{2} \geq a - \frac{a}{2} = \frac{a}{2},$$

e basta tomar $c = \frac{a}{2}$. □

Teorema 8.3.8 *O anel quociente* $S_f(K)/S_0(K)$ *é um corpo, extensão do corpo* $S_c(K)/S_0(K)$ $(\simeq K)$.

Demonstração Para provar o resultado temos que mostrar que todo elemento $[\mathbf{x}]$ não nulo do anel quociente $S_f(K)/S_0(K)$ é invertível. Devemos então provar que dado $\mathbf{x} \in S_f(K) \setminus S_0(K)$, existe $\mathbf{y} \in S_f(K)$ tal que $\mathbf{x} \cdot \mathbf{y} - 1^* \in S_0(K)$.

De fato, sendo $\mathbf{x} \in S_f(K) \setminus S_0(K)$, temos pela Proposição 8.3.7 que existem $c \in K_+^*$ e $N' \in \mathbb{N}$ tais que

$$|x_n| > c, \quad \forall\, n > N'.$$

Tem-se, em particular, que $x_n \neq 0, \quad \forall\, n > N'$. Defina $\mathbf{y} \in S(K)$ tal que

$$y_n = \begin{cases} 1 & , \quad \text{se} \quad x_n = 0 \\ x_n^{-1} & , \quad \text{se} \quad x_n \neq 0 \end{cases}$$

É claro que o produto $x_n \cdot y_n$ vale 1, exceto para apenas um número finito de índices n, quando vale zero. Logo,

$$\mathbf{x} \cdot \mathbf{y} - 1^* \in S_0(K).$$

Só falta agora provar que $\mathbf{y} \in S_f(K)$. Sendo $\mathbf{x}$ fundamental, dado $\varepsilon \in K_+^*$, existe $N'' \in \mathbb{N}$ tal que se $m, n > N''$ então

$$|x_n - x_m| < \varepsilon c^2.$$

Tomando $N = \max\{N', N''\}$, tem-se

$$|y_n - y_m| = \left|\frac{1}{x_n} - \frac{1}{x_m}\right| = \left|\frac{x_m - x_n}{x_n x_m}\right| \leq \frac{|x_m - x_n|}{c^2} < \frac{\varepsilon c^2}{c^2} = \varepsilon,$$

para $m, n > N$. Portanto, $\mathbf{y}$ é fundamental em K. □

O corpo $S_f(K)/S_0(K)$ será denotado por $\widehat{K}$ e chamado o completamento de K. É claro que

$$\begin{aligned} S_c(K) &\longrightarrow \widehat{K} \\ \mathbf{x} &\longmapsto [\mathbf{x}] \end{aligned}$$

é um homomorfismo de anéis cujo núcleo é $S_0(K)$, logo existe um homomorfismo injetor

$$K \simeq S_c(K)/S_0(K) \longrightarrow \widehat{K},$$

que nos permite enxergar $\widehat{K}$ como uma extensão do corpo K. Um elemento x de K será indentificado com o elemento $[x^*]$ de $\widehat{K}$.

O completamento de $\mathbb{Q}$ será denotado por $\mathbb{R}$ e chamado de *corpo dos números reais*.

Problemas

3.1 Mostre que toda subsequência de uma sequência fundamental é uma sequência fundamental.

3.2 Mostre que se uma sequência fundamental tem uma subsequência convergente, então a sequência é convergente e tem o mesmo limite que o da subsequência.

3.3 Mostre que num corpo arquimediano toda sequência monótona decrescente e limitada inferiormente é fundamental.

Sugestão Se $\mathbf{x}$ possui as propriedades acima, então aplique a Proposição 8.3.2 à sequência $(-\mathbf{x})$.

3.4 Seja K um corpo ordenado e seja $a \in K$, com $a \geq 0$. Defina a sequência $\mathbf{s} = (s_n)$ recorrentemente como a seguir:

$$s_1 = 1, \qquad s_{n+1} = \frac{2as_n}{a + s_n^2}, \quad \forall\, n \in \mathbb{N}.$$

Mostre que $\mathbf{s}$ é monótona crescente e limitada superiormente. Conclua que se K é arquimediano, então $\mathbf{s}$ é fundamental. Se $\mathbf{s}$ fosse convergente qual seria o seu limite?

3.5 Determine os elementos invertíveis de $S(K)$, $S_f(K)$ e de $S_c(K)$. Mostre que se $\mathbf{x} \in S_c(K) \setminus S_0(K)$, então existe algum $r \in \mathbb{N}$ tal que $\mathbf{y} = \mathbf{x} \circ \tau_r$ é invertível e

$$\lim \mathbf{y}^{-1} = (\lim \mathbf{x})^{-1}.$$

4 Ordenação do completamento

Nesta seção, estenderemos a ordenação de K para $\widehat{K}$ e estudaremos as suas propriedades.

Proposição 8.4.1. *Seja* $\mathbf{x} = (x_n) \in S_f(K)$. *Então uma, e somente uma, das seguintes condições é satisfeita*

i) $\mathbf{x} \in S_0(K)$.

ii) *Existem* $c \in K_+^*$ *e* $N \in \mathbb{N}$ *tais que* $x_n \geq c, \quad \forall\, n > N$.

iii) *Existem* $c \in K_+^*$ *e* $N \in \mathbb{N}$ *tais que* $x_n \leq -c, \quad \forall\, n > N$.

Demonstração É claro que as condições acima são mutuamente exclusivas. Suponha que $\mathbf{x} \notin S_0(K)$, logo pela Proposição 8.3.7 existem $c \in K_+^*$ e $N \in \mathbb{N}$ tais que $|x_n| > c, \ \ \forall\, n > N$.

Assim, se $n > N$, temos que $x_n \geq c$, se $x_n > 0$ e $-x_n \geq c$, se $x_n < 0$. Vamos provar que o sinal de x_n é fixo para n grande. Suponha que para todo $N' \in \mathbb{N}$ tenhamos n e m inteiros com $m, n > N'$ tais que

$$x_n \geq c \quad \text{e} \quad -x_m \geq c.$$

Logo,

$$|x_n - x_m| = x_n - x_m \geq 2c > 0,$$

contradizendo o fato de $\mathbf{x}$ ser fundamental. □

As condições (i) e (ii) da Proposição 8.4.1 nos permitem definir um subconjunto notável de $S_f(K)$.

Definimos $S_f(K)^+$ como sendo o seguinte subconjunto de $S_f(K)$:

$$\left\{\mathbf{x} \in S_f(K)\,;\ \text{existem } c \in K_+^* \text{ e } N \in \mathbb{N} \text{ tais que } x_n \geq c,\ \forall\, n > N\right\} \cup S_0(K).$$

Lema 8.4.2. *Valem as seguintes afirmações:*

i) *Se* $\mathbf{x} \in S_f(K)^+$ *e* $(-\mathbf{x}) \in S_f(K)^+$, *então* $\mathbf{x} \in S_0(K)$.

ii) *Se* $\mathbf{x}, \mathbf{y} \in S_f(K)^+$, *então* $\mathbf{x} + \mathbf{y}$ *e* $\mathbf{x} \cdot \mathbf{y} \in S_f(K)^+$.

Demonstração É uma simples verificação deixada a cargo do leitor. □

Definimos agora a seguinte relação em $\widehat{K}$:

$$[\mathbf{x}] \leq [\mathbf{y}] \iff \mathbf{y} - \mathbf{x} \in S_f(K)^+.$$

Como a definição acima diz respeito a classes em $\widehat{K}$, porém é dada em termos de representantes destas classes, devemos verificar que ela é bem posta. Para isto, devemos mostrar que se $\mathbf{x}' - \mathbf{x}$, $\mathbf{y}' - \mathbf{y} \in S_0(K)$ e se $\mathbf{y} - \mathbf{x} \in S_f(K)^+$, então $\mathbf{y}' - \mathbf{x}' \in S_f(K)^+$. De fato, como $\mathbf{x}' = \mathbf{x} + \mathbf{x}''$ e $\mathbf{y}' = \mathbf{y} + \mathbf{y}''$, com $\mathbf{x}'', \mathbf{y}'' \in S_0(K)$ e $\mathbf{y} - \mathbf{x} \in S_f(K)^+$, então $\mathbf{y}'' - \mathbf{x}'' \in S_0(K) \subset S_f(K)^+$ e, portanto, pelo Lema 8.4.2 (ii), temos que

$$\mathbf{y}' - \mathbf{x}' = \mathbf{y} - \mathbf{x} + (\mathbf{y}'' - \mathbf{x}'') \in S_f(K)^+.$$

A relação, acima definida, é uma relação de ordem em $\widehat{K}$, conforme verificaremos abaixo.

Teorema 8.4.3. $(\widehat{\mathsf{K}}, +, \cdot, \leq)$ *com a relação* $\leq$ *acima definida é uma extensão ordenada do corpo ordenado* $(\mathsf{K}, +, \cdot, \leq)$.

Demonstração Já vimos no Teorema 8.3.8 que $(\widehat{\mathsf{K}}, +, \cdot)$ é uma extensão de $(\mathsf{K}, +, \cdot)$. Vamos mostrar agora que $(\widehat{\mathsf{K}}, +, \cdot, \leq)$ é um anel ordenado.

(Reflexividade:) Para todo $[\mathbf{x}] \in \widehat{\mathsf{K}}$, temos que $[\mathbf{x}] \leq [\mathbf{x}]$, pois

$$\mathbf{x} - \mathbf{x} = 0 \in \mathsf{S}_0(\mathsf{K}) \subset \mathsf{S}_f(\mathsf{K})^+.$$

(Antisimetria:) Se $[\mathbf{x}] \leq [\mathbf{y}]$ e $[\mathbf{y}] \leq [\mathbf{x}]$, então $[\mathbf{x}] = [\mathbf{y}]$. De fato, temos que $\mathbf{y}-\mathbf{x} \in \mathsf{S}_f(\mathsf{K})^+$ e $-(\mathbf{y}-\mathbf{x}) \in \mathsf{S}_f(\mathsf{K})^+$, logo, pelo Lema 8.4.2 (i), temos que $\mathbf{y} - \mathbf{x} \in \mathsf{S}_0(\mathsf{K})$ e, portanto, $[\mathbf{x}] = [\mathbf{y}]$.

(Transitividade:) Se $[\mathbf{x}] \leq [\mathbf{y}]$ e $[\mathbf{y}] \leq [\mathbf{z}]$, então $[\mathbf{x}] \leq [\mathbf{y}]$. De fato, como $\mathbf{y} - \mathbf{x}$ e $\mathbf{z} - \mathbf{y}$ pertencem a $\mathsf{S}_f(\mathsf{K})^+$, segue-se, do Lema 8.4.2 (ii), que

$$\mathbf{z} - \mathbf{x} = (\mathbf{y} - \mathbf{x}) + (\mathbf{z} - \mathbf{y}) \in \mathsf{S}_f(\mathsf{K})^+,$$

e, consequentemente, $[\mathbf{x}] \leq [\mathbf{z}]$.

(Totalidade:) Dados $[\mathbf{x}], [\mathbf{y}] \in \widehat{\mathsf{K}}$, então $[\mathbf{x}] \leq [\mathbf{y}]$ ou $[\mathbf{y}] \leq [\mathbf{x}]$. De fato, dados $\mathbf{x}, \mathbf{y} \in \mathsf{S}_f(\mathsf{K})$, então pela Proposição 8.4.1 temos que $\mathbf{y}-\mathbf{x} \in \mathsf{S}_f(\mathsf{K})^+$ ou $-(\mathbf{y} - \mathbf{x}) \in \mathsf{S}_f(\mathsf{K})^+$, daí segue-se que $[\mathbf{x}] \leq [\mathbf{y}]$ ou $[\mathbf{y}] \leq [\mathbf{x}]$.

(Compatibilidade com a Adição:) Sejam $[\mathbf{x}], [\mathbf{y}], [\mathbf{z}] \in \widehat{\mathsf{K}}$. Se $[\mathbf{x}] \leq [\mathbf{y}]$, então segue-se imediatamente da definição que $[\mathbf{x}] + [\mathbf{z}] \leq [\mathbf{y}] + [\mathbf{z}]$.

(Compatibilidade com a Multiplicação:) Sejam $[\mathbf{x}], [\mathbf{y}], [\mathbf{z}] \in \widehat{\mathsf{K}}$, com $[\mathbf{z}] \geq 0$ e $[\mathbf{x}] \leq [\mathbf{y}]$, então $[\mathbf{x}] \cdot [\mathbf{z}] \leq [\mathbf{y}] \cdot [\mathbf{z}]$. De fato, como $\mathbf{y}-\mathbf{x} \in \mathsf{S}_f(\mathsf{K})^+$ e $\mathbf{z} \in \mathsf{S}_f(\mathsf{K})^+$, do Lema 8.4.2 (ii), segue-se que $(\mathbf{y} - \mathbf{x})\mathbf{z} \in \mathsf{S}_f(\mathsf{K})^+$ e, portanto, $[\mathbf{x}] \cdot [\mathbf{z}] \leq [\mathbf{y}] \cdot [\mathbf{z}]$.

Só falta agora mostrar que a relação $\leq$ de $\widehat{\mathsf{K}}$ é uma extensão a $\widehat{\mathsf{K}}$ da relação $\leq$ de K. Isto se vê como se segue. Suponha $x, y \in \mathsf{K}$ com $x \leq y$. Identificando x e y com as sequências constantes x^* e y^*, é claro que $y^* - x^* = (y - x)^* \in \mathsf{S}_f(\mathsf{K})^+$ e, consequentemente, $[x^*] \leq [y^*]$. □

Proposição 8.4.4. *Se* K *é arquimediano, então* $\widehat{\mathsf{K}}$ *é arquimediano.*

Demonstração Seja $[\mathbf{x}] \in \widehat{\mathsf{K}}$. Como $\mathbf{x} \in \mathsf{S}_f(\mathsf{K})$, segue-se que $\mathbf{x}$ é limitada (Proposição 8.3.4), logo temos para algum $r \in \mathsf{K}_+^*$, que

$$x_n \leq r, \quad \forall\, n \in \mathbb{N}.$$

Como K é arquimediano, segue-se que existe $m \in \mathbb{N}$ tal que $m1 \geq r + 1$. Temos então que

$$m1 - x_n \geq 1, \quad \forall\, n \in \mathbb{N}.$$

Segue-se que

$$m1 - \mathbf{x} \in S_f(K)^+,$$

logo $m[1^*] \geq [\mathbf{x}]$. □

Lema 8.4.5. *Sejam* $\mathbf{x}, \mathbf{y} \in S_f(K)$. *Se existir* $N \in \mathbb{N}$ *tal que*

$$x_n \geq y_n, \quad \forall\, n > N,$$

então $[\mathbf{x}] \geq [\mathbf{y}]$.

Demonstração Em virtude da Proposição 8.4.1, a condição $x_n \geq y_n$, $\forall\, n > N$, , implica que $\mathbf{x} - \mathbf{y} \in S_f(K)^+$, logo $[\mathbf{x}] \geq [\mathbf{y}]$. □

Lema 8.4.6. *Seja* K *um corpo arquimediano e seja* $\mathbf{x} = (x_n) \in S_f(K)$. *Considerando a sequência* $([\mathbf{y}_n]) = ([(x_n)^*])$ *em* $\widehat{K}$, *temos que*

$$\lim_{n\to\infty} [\mathbf{y}_n] = [\mathbf{x}].$$

Demonstração Pela Proposição 8.4.4 temos que $\widehat{K}$ é arquimediano e portanto dado $\varepsilon \in \widehat{K}^*_+$, pela Proposição 8.2.2, existe $\varepsilon' \in K_0$ tal que $0 < [(\varepsilon')^*] < \varepsilon$. Para este ε', dado que $\mathbf{x}$ é fundamental em K, existe $N \in \mathbb{N}$ tal que

$$|x_n - x_m| < \varepsilon', \quad \forall\, m, n > N.$$

Para cada $m > N$ fixo, temos que

$$x_m - \varepsilon' < x_n < x_m + \varepsilon', \quad \forall\, n > N.$$

Olhando para $x_m - \varepsilon'$ como o n-ésimo termo da sequência $(x_m - \varepsilon')^*$ e para $x_m + \varepsilon'$ como o n-ésimo termo da sequência $(x_m + \varepsilon')^*$, temos pelo Lema 8.4.5 que

$$[(x_m - \varepsilon')^*] \leq [\mathbf{x}] \leq [(x_m + \varepsilon')^*], \quad \text{para} \quad m > N,$$

logo

$$[(x_m)^*] - [(\varepsilon')^*] \leq [\mathbf{x}] \leq [(x_m)^*] + [(\varepsilon')^*], \quad \text{para } m > N.$$

Consequentemente, para todo $m > N$, temos que

$$|[(x_m)^*] - [\mathbf{x}]| \leq [(\varepsilon')^*] < \varepsilon$$

e, portanto,

$$\lim_{m\to\infty}[\mathbf{y}_m] = [\mathbf{x}].$$

□

O resultado que se segue nos fornecerá uma propriedade fundamental do completamento $\widehat{K}$ de um corpo arquimediano K.

Teorema 8.4.7. *Seja K um corpo arquimediano e seja $\widehat{K}$ o seu completamento. Temos que toda sequência fundamental em $\widehat{K}$ é convergente em $\widehat{K}$, isto é,*

$$S_f(\widehat{K}) = S_c(\widehat{K}).$$

Demonstração Seja $\mathbf{X} = (X_n) \in S_f(\widehat{K})$. Pelo fato de $\widehat{K}$ ser arquimediano (Proposição 8.4.4) e, em vista da Proposição 8.2.2, para cada $n \in \mathbb{N}$ é possível encontrar $[(x_n)^*] \in \widehat{K}_0\,(\simeq K_0)$, tal que

$$X_n - \frac{1}{[(n1)^*]} \leq [(x_n)^*] \leq X_n + \frac{1}{[(n1)^*]},$$

isto é, tal que

$$|X_n - [(x_n)^*]| \leq \frac{1}{[(n1)^*]}\cdot$$

Como $\mathbf{X}$ é fundamental, dado $\varepsilon \in \widehat{K}_+^*$, existe N, tal que

$$|X_n - X_m| \leq \frac{\varepsilon}{3}, \quad \forall\, m, n > N.$$

Seja $N_1 \in \mathbb{N}$ tal que $N_1 \geq N$ e $[(N_1 1)^*] > \frac{3}{\varepsilon}\cdot$ Temos então, para todo $m, n \geq N_1$, que

$$\begin{aligned}|[(x_n)^*] - [(x_m)^*]| &\leq |[(x_n)^*] - X_n + X_n - X_m + X_m - [(x_m)^*]| \\ &\leq |[(x_n)^*] - X_n| + |X_n - X_m| + |X_m - [(x_m)^*]| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.\end{aligned}$$

Isto prova que $\mathbf{x} = (x_n) \in S(K_0)$ é fundamental. Logo, pelo Lema 8.4.6, temos que

$$\lim_{n\to\infty}[(x_n)^*] = [\mathbf{x}].$$

Temos então que, dado $\varepsilon \in \widehat{K}_+^*$, existe $N \in \mathbb{N}$ tal que

$$|X_n - [(x_n)^*]| < \frac{\varepsilon}{2} \quad \text{e} \quad |[(x_n)^*] - [\mathbf{x}]| < \frac{\varepsilon}{2}, \quad \forall\, n > N.$$

Logo, para $n > N$, temos que

$$|X_n - [\mathbf{x}]| \leq |X_n - [(x_n)^*]| + |[(x_n)^*] - [\mathbf{x}]| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

provando que

$$\lim \mathbf{X} = [\mathbf{x}],$$

e, portanto, $\mathbf{X}$ é convergente. □

Um corpo L tal que $S_f(L) = S_c(L)$ será dito *completo*. Portanto, o Teorema 8.4.7 nos garante que o completamento $\widehat{K}$ de um corpo arquimediano K é completo.

Em particular, temos que o completamento $\mathbb{R}$ de $\mathbb{Q}$ é um **corpo arquimediano completo**. Estas propriedades caracterizam totalmente o corpo dos números reais, como veremos mais adiante.

Uma vantagem de $\mathbb{R}$ sobre $\mathbb{Q}$ é que em $\mathbb{R}$ existe um número cujo quadrado é 2, isto é, existe $\sqrt{2}$. De fato, a sequência $\mathbf{r}$ que introduzimos na seção 3 é fundamental em $\mathbb{R}$ e, portanto, converge em $\mathbb{R}$ a um número α tal que $\alpha^2 = 2$. Isto é apenas uma pequena indicação de que $\mathbb{R}$ tem muitas propriedades não compartilhadas por $\mathbb{Q}$.

Note que em decorrência do Problema 3.4 temos que num corpo arquimediano completo K, todo elemento $a \geq 0$ possui raiz quadrada, isto é, existe $b \in K$ tal que $b^2 = a$.

Teorema 8.4.8. *Seja K um corpo arquimediano completo. Então existe um único homomorfismo de anéis de $\mathbb{R}$ em K. Além disso, este homomorfismo é um isomorfismo de anéis ordenados.*

Demonstração Vamos inicialmente mostrar que sendo $\mathbb{R}$ completo, qualquer homomorfismo f de $\mathbb{R}$ num corpo ordenado é monótono crescente. De fato, se $a, b \in \mathbb{R}$ com $a \leq b$, segue-se que $b - a \geq 0$, logo existe $c \in \mathbb{R}$ tal que $c^2 = b - a$. Temos então que

$$0 \leq [f(c)]^2 = f(c^2) = f(b - a) = f(b) - f(a),$$

logo $f(a) \leq f(b)$.

Vamos agora mostrar a unicidade. Sejam f e g dois homomorfismos de $\mathbb{R}$ num corpo arquimediano L. Considere o conjunto

$$M = \{x \in \mathbb{R}\,;\ f(x) = g(x)\}.$$

Queremos provar que $M = \mathbb{R}$. Suponha por absurdo que $M \neq \mathbb{R}$. Seja $a \in \mathbb{R} \setminus M$, que podemos supor positivo (justifique). Suponha que $f(a) < g(a)$. Temos pela Proposição 8.3.2 que existe $r \in L_0$ tal que

$$f(a) < r < g(a). \tag{1}$$

Como $L_0 = \tilde{\rho}(\mathbb{Q})$ e $\tilde{\rho}$ é o único homomorfismo de $\mathbb{Q}$ em L, segue-se que $f|_{\mathbb{Q}} = g|_{\mathbb{Q}} = \tilde{\rho}$ e, portanto, existe $s \in \mathbb{Q}$ tal que $r = \tilde{\rho}(s) = f(s) = g(s)$.

Vamos mostrar que isto gera uma contradição. Temos duas possibilidades: $a \leq s$ ou $s \leq a$. Se $a \leq s$, segue-se que $g(a) \leq g(s) = r$, contradição com (1). Se $s \leq a$, segue-se que $r = f(s) \leq f(a)$, contradição com (1).

Portanto, $M = R$, ou seja, $f = g$.

Agora, vamos mostrar a existência de um homomorfismo de $\mathbb{R}$ em K. Considere a seguinte lei:

$$\begin{aligned} \psi\colon S_f(\mathbb{Q}) &\longrightarrow K \\ (x_n) &\longmapsto \lim_{n\to\infty} \tilde{\rho}(x_n) \end{aligned}$$

Vamos mostrar que a lei acima está bem definida, ou seja, que o limite da direita existe. Como K é completo, bastará mostrar que $(\tilde{\rho}(x_n))$ é uma sequência fundamental.

De fato, seja dado $\varepsilon \in K_+^*$. Como K é arquimediano, pela Proposição 8.2.2, existe $\nu \in \mathbb{Q}_+$ tal que

$$0 < \tilde{\rho}(\nu) < \varepsilon.$$

Como (x_n) é fundamental, existe $N \in \mathbb{N}$ tal que

$$|x_n - x_m| < \nu, \quad \forall\, n, m > N.$$

Pelo fato de $\tilde{\rho}$ ser um homomorfismo ordenado, temos que

$$|\tilde{\rho}(x_n) - \tilde{\rho}(x_m)| < \tilde{\rho}(\nu) < \varepsilon, \quad \forall\, n, m > N.$$

Logo, $(\tilde{\rho}(x_n))$ é fundamental em K.

Por outro lado, é fácil verificar que ψ é um homomorfismo de anéis. Este homomorfismo é sobrejetor pois, dado $\alpha \in K$, existe pela Proposição 8.2.2 uma sequência $(s_n) \in S(\mathbb{Q})$ tal que $\lim_{n\to\infty} \tilde{\rho}(s_n) = \alpha$. Basta agora provar que $(s_n) \in S_f(\mathbb{Q})$. Este fato decorre de sabermos que $\tilde{\rho}(s_n) \in S_f(K_0)$ e $\tilde{\rho}\colon \mathbb{Q} \to K_0$ é um isomorfismo ordenado de anéis.

É claro também que o núcleo de ψ é $S_0(\mathbb{Q})$. Pelo Teorema do isomorfismo, temos um isomorfismo

$$\mathbb{R} = S_f(\mathbb{Q})/S_0(\mathbb{Q}) \simeq K.$$

□

Corolário 8.4.9. *Todo corpo arquimediano completo* K *é ordenadamente isomorfo ao corpo dos números reais, através de um único isomorfismo* $\hat{\rho}\colon \mathbb{R} \to K$.

Corolário 8.4.10. *O homomorfismo identidade é o único homomorfismo de anéis de* $\mathbb{R}$ *em* $\mathbb{R}$.

Corolário 8.4.11. *Todo corpo arquimediano é ordenadamente isomorfo a um subcorpo de* $\mathbb{R}$.

Demonstração Seja K um corpo arquimediano. Então K é ordenadamente isomorfo a um subcorpo de $\widehat{K}$, que pelo Corolário 8.4.9 é ordenadamente isomorfo a $\mathbb{R}$. □

5 Relação com a Análise

Usualmente, um curso de Análise Matemática inicia-se admitindo o Princípio do Supremo em $\mathbb{R}$ (veja por exemplo o livro Análise Real, Volume I, de Elon Lages Lima nesta mesma coleção).

Para enunciarmos este princípio necessitaremos das definições a seguir. Sejam K um corpo ordenado e A um subconjunto de K.

Um elemento $b \in K$ será chamado de *supremo* de A se são satisfeitas as condições:

i) Para todo $x \in A$, tem-se que $x \leq b$.

ii) Para todo $\varepsilon \in K_+^*$, existe $x \in A$ tal que $b - \varepsilon < x \leq b$.

O supremo de um conjunto A, se existir, é único. De fato, sejam b e b' dois supremos de A. Se $b \neq b'$, digamos $b < b'$, então por (ii) acima, temos que existe $x \in A$ tal que

$$b = b' - (b' - b) < x,$$

o que é um absurdo, pois por (i) temos que $x \leq b, \quad \forall\, x \in A$.

O supremo de A, caso exista, será denotado por $\operatorname{Sup} A$.

Recorde que o conjunto A é dito *limitado superiormente*, se existir $b \in K$ tal que $x \leq b, \ \ \forall\, x \in A$.

Teorema 8.5.1 (Princípio do Supremo). *Todo subconjunto de* $\mathbb{R}$*, não vazio e limitado superiormente, admite um supremo.*

Demonstração Seja A um subconjunto de $\mathbb{R}$, não vazio e limitado superiormente. Para cada $n \in \mathbb{N}$ defina

$$S_n = \{x \in \mathbb{Z};\ \frac{x}{n} \geq a, \forall\, a \in A\}.$$

Pela propriedade arquimediana de $\mathbb{R}$, temos que S_n é não vazio. É claro também que S_n é limitado inferiormente. Logo, pelo Princípio da Boa Ordenação, S_n tem um menor elemento que denotaremos por x_n. Pela definição de x_n, temos que existe $a_n \in A$ tal que

$$\frac{x_n}{n} - \frac{1}{n} = \frac{x_n - 1}{n} < a_n \leq \frac{x_n}{n}\cdot \tag{1}$$

Considere a sequência definida por

$$z_n = \frac{x_n}{n}\cdot$$

Sejam m e n inteiros positivos. Suponhamos que $\frac{x_n}{n} \geq \frac{x_m}{m}$ (o outro caso é análogo). Temos de (1) que

$$\frac{x_n}{n} - \frac{1}{n} < a_n \leq \frac{x_m}{m} \leq \frac{x_n}{n} < \frac{x_n}{n} + \frac{1}{n},$$

logo

$$|z_n - a_n| < \frac{1}{n} \tag{2}$$

e

$$|z_m - z_n| < \frac{1}{n}. \tag{3}$$

De (3) segue-se facilmente que (z_n) é uma sequência fundamental.

Como $\mathbb{R}$ é completo, segue-se que (z_n) é convergente. Digamos que

$$\lim_{n\to\infty} z_n = z.$$

Como $z_n \geq a, \ \ \forall\, a \in A$, segue-se (veja Problema 1.6) que

$$z = \lim_{n\to\infty} z_n \geq a, \quad \forall\, a \in A.$$

Vamos mostrar que $z = \text{ Sup } A$. Seja $\varepsilon \in \mathbb{R}_+$ e tome $N' > \frac{2}{\varepsilon}$, logo de (2) temos que se $n > N'$, então

$$|z_n - a_n| < \frac{\varepsilon}{2}\cdot$$

Por outro lado, existe N'' tal que se $n > N''$, então

$$|z - z_n| < \frac{\varepsilon}{2}\cdot$$

Tomando $N = \max\{N', N''\}$ temos que se $n > N$, então

$$z - a_n = |z - a_n| \leq |z - z_n| + |z_n - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto, existe $a_n \in A$ tal que $z - \varepsilon < a_n$, provando que $z = \text{ Sup } A$. □

O próximo resultado nos garantirá a existência em $\mathbb{R}$ da raiz n-ésima de um número real positivo qualquer, para todo $n \in \mathbb{N}$.

Teorema 8.5.2. *Dados* $a \in \mathbb{R}^+$ *e* $n \in \mathbb{N} \setminus \{0\}$, *existe* $b \in \mathbb{R}$ *tal que* $b^n = a$.

Demonstração Como o resultado é claro para $a = 0$, admitamos $a > 0$. Considere o conjunto

$$A = \{x \in \mathbb{R};\ x^n \leq a\}.$$

O conjunto A é não vazio e limitado superiormente, logo pelo Teorema 8.5.1, admite um supremo. Ponhamos $b = \text{ Sup } A$. Vamos mostrar que $b^n = a$.

Suponha que $b^n < a$ e escolha $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1$ e $\varepsilon < \frac{a-b^n}{(1+b)^n - b^n}$. Usando o binômio de Newton, obtemos

$$(b+\varepsilon)^n = b^n + \binom{n}{1} b^{n-1}\varepsilon + \binom{n}{2} b^{n-2}\varepsilon^2 + \cdots + \varepsilon^n \leq$$

$$b^n + \varepsilon\left[\binom{n}{1} b^{n-1} + \binom{n}{2} b^{n-2} + \cdots + 1\right] =$$

$$b^n + \varepsilon\left[(1+b)^n - b^n\right] < b^n + a - b^n = a.$$

Portanto, $b + \varepsilon \in A$, contradizendo o item (i) da definição de supremo.

Suponha agora que $b^n > a$ e escolha $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1$, $\varepsilon < b$ e $\varepsilon < \frac{b^n - a}{(1+b)^n - b^n}$. Então, para todo $x \geq b - \varepsilon$, temos

$$x^n \geq (b-\varepsilon)^n = b^n - \binom{n}{1} b^{n-1}\varepsilon + \binom{n}{2} b^{n-2}\varepsilon^2 + \cdots + (-1)^n \varepsilon^n =$$

$$b^n - \varepsilon \left[\binom{n}{1} b^{n-1} - \binom{n}{2} b^{n-2} + \cdots - (-1)^n \varepsilon^{n-1} \right] \geq$$

$$b^n - \varepsilon \left[\binom{n}{1} b^{n-1} + \binom{n}{2} b^{n-2} + \cdots + 1 \right] =$$

$$b^n - \varepsilon \left[(1+b)^n - b^n \right] > b^n + (b^n - a) = a,$$

ou seja, $x \notin A$. Mas isto contraria o item (ii) da definição de supremo. □

O número real não negativo b tal que $b^n = a$ é denotado por $\sqrt[n]{a}$ e chamado de *raiz* n*-ésima* de a. Sejam $a, c \in \mathbb{R}_+$ e sejam b e d tais que $b^n = a$ e $d^n = c$, logo

$$a \cdot c = b^n \cdot d^n = (b \cdot d)^n$$

e, consequentemente,

$$\sqrt[n]{a \cdot c} = b \cdot d = \sqrt[n]{a} \cdot \sqrt[n]{c},$$

ou seja,

$$\sqrt[n]{a \cdot c} = \sqrt[n]{a} \cdot \sqrt[n]{c}.$$

9

Os números complexos

O corpo dos números reais foi criado com o objetivo de completar o corpo dos números racionais de modo que equações do tipo $x^2 = 2$ tivessem soluções. Com isto muitas lacunas dos racionais, mas não todas, foram preenchidas. Por exemplo, equações como $x^2 = -1$ continuam sem solução em $\mathbb{R}$. A fim de sanar esta lacuna é que se resolveu após muitas hesitações ampliar o corpo dos números reais, criando o corpo dos números complexos $\mathbb{C}$. É curioso observar que historicamente a construção formal dos números complexos precedeu a dos números reais.

Desde a antiguidade, os matemáticos se depararam com o problema de extrair raízes quadradas de números negativos, o que era considerado impossível. Cardan em 1545 foi o primeiro matemático que efetuou operações com os números complexos apesar de não compreendê-los. Por exemplo, na procura de dois números cuja soma é 10 e cujo produto é 40, ele encontrou os "números" $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$, que somados e multiplicados nos dão respectivamente 10 e 40.

O primeiro matemático a olhar os números complexos com mais naturalidade foi Walis que em 1675 teve a idéia de representá-los geometricamente, não indo porém além disso. Sustentava ele que se as raízes quadradas de números negativos fossem consideradas como absurdas, absurdo também seria aceitar as quantidades negativas que na época eram totalmente aceitas. A sua argumentação era a seguinte: não há razão para aceitar comprimentos negativos e rejeitar áreas negativas!

Em seguida, foi Leibniz quem considerou os números complexos mos-

trando em 1676 que

$$\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}=\sqrt{6}$$

e em 1702 que

$$x^4+a^4=\left(x+a\sqrt{-\sqrt{-1}}\right)\left(x-a\sqrt{-\sqrt{-1}}\right)\left(x+a\sqrt{\sqrt{-1}}\right)\left(x-a\sqrt{\sqrt{-1}}\right).$$

O passo seguinte foi dado no século 18 por De Moivre e Euler que relacionaram, por meio dos números complexos, a função exponencial com as funções trigonométricas.

A teoria consolidou-se com a representação geométrica das operações de adição e multiplicação de números complexos elaborada no final do século 18 por Wessel, Argand e Gauss, culminando com o chamado Teorema Fundamental da Álgebra demonstrado por Gauss e que afirma que toda equação algébrica definida sobre $\mathbb{C}$ admite pelo menos uma raiz.

Os fatos que utilizaremos aqui e que não foram abordados no texto são a existência e propriedades básicas das funções trigonométricas seno e coseno.

1 O corpo dos complexos

Consideremos o conjunto $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$ dos pares de números reais (x,y) e nele definamos as seguintes operações de adição e multiplicação:

$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$.

$(a_1,b_1)\cdot(a_2,b_2)=(a_1\cdot a_2-b_1\cdot b_2,a_1\cdot b_2+b_1\cdot a_2)$.

A adição acima é simplesmente a adição de vetores em $\mathbb{R}^2$, enquanto a multiplicação tem uma interpretação geométrica mais elaborada que veremos na seção 3. O conjunto $\mathbb{R}^2$, com as operações acima definidas, será denotado por $\mathbb{C}$.

Teorema 9.1.1. $\mathbb{C}$ *é um corpo.*

Demonstração A associatividade e a comutatividade da adição são óbvias. O elemento zero é $(0,0)$, pois para todo $(a,b)\in\mathbb{C}$, temos

$$(a,b)+(0,0)=(a,b).$$

O simétrico de (a, b) é $(-a, -b)$, pois

$$(a, b) + (-a, -b) = (0, 0).$$

A associatividade e comutatividade da multiplicação, bem como a distributividade da multiplicação com relação à adição são de verificação direta. A unidade da multiplicação é $(1, 0)$, pois para todo $(a, b) \in \mathbb{C}$,

$$(a, b) \cdot (1, 0) = (a, b).$$

O inverso de $(a, b) \neq (0, 0)$ é $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$, pois

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) = (1, 0).$$

□

Chamaremos $\mathbb{C}$ de *corpo dos números complexos*, e os seus elementos de *números complexos*.

Seja $(a, b) \in \mathbb{C}$, podemos escrever

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1). \tag{1}$$

Portanto, todo número complexo pode ser representado usando somente os números da forma $(x, 0)$ e o número $(0, 1)$.

Considere a função

$$\begin{aligned} \varphi \colon \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\longmapsto (x, 0). \end{aligned}$$

Verifica-se facilmente que φ é um homomorfismo injetor de anéis. Portanto, φ permite identificar $\mathbb{R}$ com o subcorpo $\varphi(\mathbb{R})$ de $\mathbb{C}$. Se, por abuso de notação, escrevermos x no lugar de $(x, 0)$ e i no lugar de $(0, 1)$, temos de (1) que

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + b \cdot i.$$

A forma acima, que também escreve-se $a + bi$, é chamada *forma normal* do número complexo (a, b). Observe que

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

Portanto, acabamos de construir um corpo que contém o corpo $\mathbb{R}$ e no qual a equação $z^2 + 1 = 0$ admite uma raiz (o número i).

Na forma normal, é claro que $a_1 + b_1 i = a_2 + b_2 i$ se, e somente se, $a_1 = a_2$ e $b_1 = b_2$. Além disso, opera-se usando as propriedades de corpo e a informação adicional de que $i^2 = -1$. Por exemplo,

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i,$$

$$(a_1 + b_1 i) - (a_2 + b_2 i) = (a_1 - a_2) + (b_1 - b_2)i,$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = a_1 a_2 + b_1 a_2 i + a_2 b_2 i + b_1 b_2 i^2 = (a_1 a_2 - b_1 b_2) + (b_1 a_2 + a_1 b_2)i,$$

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi) \cdot (a - bi)} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\, i.$$

O corpo $\mathbb{C}$ nos forneceu uma solução para a equação $z^2 = -1$. Vamos agora mostrar que dado um número complexo qualquer $a+bi$, a equação $z^2 = a + bi$ admite solução em $\mathbb{C}$.

Ponha $z = x + yi$, temos então que

$$(x + yi)^2 = a + bi,$$

logo

$$x^2 - y^2 + 2xyi = a + bi,$$

portanto

$$\begin{cases} x^2 - y^2 = 0 \\ 2xy = b \end{cases} \tag{2}$$

Considere agora a seguinte identidade, válida para todos $x, y \in \mathbb{R}$,

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + 4x^2y^2. \tag{3}$$

Substituindo os valores de (2) e (3), temos que

$$(x^2 + y^2)^2 = a^2 + b^2,$$

logo

$$x^2 + y^2 = \sqrt{a^2 + b^2}. \tag{4}$$

Temos de (2) e (4) o sistema,

$$\begin{cases} x^2 - y^2 = a \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases}$$

que implica

$$x = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}$$
$$y = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$$

Ao combinarmos estes duplos sinais obtemos quatro possibilidades para as soluções. Mas de (2) temos que $2xy = b$ e, portanto, x e y devem ser tais que o seu produto tenha o sinal de b, dando assim duas soluções para a equação $z^2 = a + bi$.

É preciso tomar cuidado com o símbolo $\sqrt{a+bi}$, pois, em contraste com o que ocorre no campo real, aqui não há nenhuma preferência em denotar $\sqrt{a+bi}$ uma ou outra solução da equação $z^2 = a + bi$. No caso real, dado $a > 0$, existem duas soluções para $x^2 = a$, uma positiva e outra negativa, sendo que a raiz positiva é simbolizada por $\sqrt{a}$. Já em $\mathbb{C}$ não se adota nenhuma convenção para dar sentido ao símbolo $\sqrt{a+bi}$, a não ser quando se disser explicitamente, caso a caso, qual das soluções da equação $z^2 = a+bi$ convenciona-se chamar de $\sqrt{a+bi}$. Por exemplo, o símbolo $\sqrt{-1}$ é reservado para o número i, sendo que a outra solução da equação $z^2 = -1$ é $-i$.

Exemplos

1. Vamos resolver a equação $z^2 = -i$.
Como $a = 0$ e $b = -1$, temos que

$$x = \pm\sqrt{\frac{1}{2}}, \quad y = \pm\sqrt{\frac{1}{2}}.$$

Como $b < 0$, então as soluções da equação são

$$z_1 = \sqrt{\frac{1}{2}} - \sqrt{\frac{1}{2}}\,i, \qquad z_2 = -\sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2}}\,i.$$

2. Resolvamos a equação $x^2 = 1 + i$.
Usando as fórmulas, temos que

$$x = \pm\sqrt{\frac{\sqrt{2}+1}{2}}, \qquad y = \pm\sqrt{\frac{\sqrt{2}-1}{2}}.$$

Como $b > 0$, as soluções são

$$z_1 = \sqrt{\frac{\sqrt{2}+1}{2}} + \sqrt{\frac{\sqrt{2}-1}{2}}\,i$$
$$z_2 = -\sqrt{\frac{\sqrt{2}+1}{2}} - \sqrt{\frac{\sqrt{2}-1}{2}}\,i$$

Problemas

1.1 Mostre que $\mathbb{C}$ não é um corpo ordenado.

Sugestão Num corpo ordenado, para todo $a \neq 0$, tem-se que $a^2 > 0$. Mas, $0 < i^2 = -1 < 0$, contradição.

1.2 Coloque na forma normal os seguintes números complexos:

a) $(3+i)^2 \cdot (2-i)$ b) $(4-3i)^3$ c) $\dfrac{1}{i}$

d) $\dfrac{1+i}{1-i}$ e) $\dfrac{2+i}{1-i} + \dfrac{3-i}{1+i}$

1.3 Ache os inversos dos seguintes números complexos, na forma normal

a) $2+3i$ b) $\dfrac{5+i}{3+i} + \dfrac{3+2i}{1+3i}$ c) $\dfrac{2+3i}{1+i} + 1 + i$

d) $(1+i)^3$

1.4 Mostre que

$$i^n = \begin{cases} 1 & , \text{ se } n \equiv 0 \bmod 4 \\ i & , \text{ se } n \equiv 1 \bmod 4 \\ -1 & , \text{ se } n \equiv 2 \bmod 4 \\ -i & , \text{ se } n \equiv 3 \bmod 4 \end{cases}$$

1.5 Calcule o valor de

$$3 \cdot i^{27} + 4 \cdot i^{37} - i^{30}.$$

1.6 Para $n \in \mathbb{N}$, calcule o valor de $1 + i + i^2 + \cdots + i^{n-1}$.

1.7 Resolva em $\mathbb{C}$ as seguintes equações:

a) $z^2 = 1 - i$ b) $z^2 = 1 + \sqrt{3}i$ c) $z^2 = 1 - \sqrt{3}i$

d) $z^4 = 1 + i$ e) $z^4 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ f) $z^4 = 3 + 4i$

1.8 Escolhendo convenientemente $\sqrt{1+\sqrt{3}i}$ e $\sqrt{1-\sqrt{3}i}$, mostre que

$$\sqrt{1+\sqrt{3}i} + \sqrt{1-\sqrt{3}i} = \sqrt{6}.$$

1.9 Sejam $a, b, c \in \mathbb{C}$, com $a \neq 0$. Mostre que as soluções da equação

$$az^2 + bz + c = 0,$$

são

$$z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{e} \quad z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

onde $\sqrt{b^2 - 4ac}$ é uma das soluções da equação $u^2 = b^2 - 4ac$.

1.10 Resolva as equações:

a) $iz^2 - (2+2i)z + 2 - i = 0$ b) $z^2 + z + 1 = 0$.

2 Conjugação e módulo

Seja $z = a + bi \in \mathbb{C}$, com $a, b \in \mathbb{R}$. Define-se o *conjugado* de z como sendo $\overline{a} = a - bi$ e o *módulo* de z como sendo o número real $|z| = \sqrt{a^2 + b^2}$. A *parte real* e a *parte imaginária* de z são, respectivamente, os números reais $\operatorname{Re} z = a$ e $\operatorname{Im} z = b$.

Damos a seguir uma lista de propriedades que estes conceitos possuem.

1) $\overline{z} = 0$ se, e somente se, $z = 0$.

2) $\overline{z} = z$ se, e somente se, $z \in \mathbb{R}$.

3) $\overline{\overline{z}} = z$, para todo $z \in \mathbb{C}$.

4) $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$.

5) $\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2$.

6) Se $z_2 \neq 0$, então $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z}_1}{\overline{z}_2}$.

7) Se $z \neq 0$, então $(\overline{z})^n = \overline{(z^n)}$ para todo $n \in \mathbb{Z}$.

8) $z \cdot \overline{z} = |z|^2$, para todo $z \in \mathbb{C}$.

9) $|z| = |\overline{z}| = |-z|$, para todo $z \in \mathbb{C}$.

10) $\operatorname{Re} z = \frac{z+\overline{z}}{2}$ e $\operatorname{Im} z = \frac{z-\overline{z}}{2i}$.

11) $\operatorname{Re} z \leq |\operatorname{Re} z| \leq |z|$ e $\operatorname{Im} z \leq |\operatorname{Im} z| \leq |z|$.

Estas propriedades são fáceis de verificar. A título de ilustração, provaremos a propriedade (5).

Sejam $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$, a propriedade (5) é consequência das seguintes igualdades:

$$\begin{aligned}\overline{z_1 \cdot z_2} &= \overline{(a_1 + b_1 i) \cdot (a_2 + b_2 i)} = \overline{(a_1 a_2 - b_1 b_2) + (b_1 a_2 + a_1 b_2)i} \\ &= (a_1 a_2 - b_1 b_2) - (b_1 a_2 + a_1 b_2)i\end{aligned}$$

e

$$\overline{z}_1 \cdot \overline{z}_2 = (a_1 - b_1 i) \cdot (a_2 - b_2 i) = a_1 a_2 - b_1 b_2 - (b_1 a_2 + a_1 b_2)i.$$

As seguintes proposições nos fornecerão alguns resultados básicos.

Proposição 9.2.1. *Quaisquer que sejam $z_1, z_2 \in \mathbb{C}$, temos que*

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|.$$

Demonstração Usando as propriedades (5) e (8), acima, temos que

$$|z_1 \cdot z_2|^2 = (z_1 \cdot z_2)\overline{(z_1 \cdot z_2)} = z_1 \cdot \overline{z}_1 \cdot z_2 \cdot \overline{z}_2 = |z_1|^2 \cdot |z^2|^2 = (|z_1| \cdot |z_2|)^2.$$

Como $|z_1 \cdot z_2|$ e $|z_1| \cdot |z_2|$ são ambos números reais não negativos, extraindo a raiz quadrada de ambos os membros da igualdade $|z_1 \cdot z_2|^2 = (|z_1| \cdot |z_2|)^2$, obtemos que $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$. □

Proposição 9.2.2. *Quaisquer que sejam $z_1, z_2 \in \mathbb{C}$, temos que*

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Demonstração Usando as propriedades (5) e (3) acima, verifica-se que $z_1 \cdot \overline{z}_2$ e $z_2 \cdot \overline{z}_1$ são conjugados, logo pela propriedade (10) temos que $z_1 \cdot \overline{z}_2 + z_2 \cdot \overline{z}_1 = 2\operatorname{Re}(z_1 \cdot \overline{z}_2)$. Como, pelas propriedades (11) e (9) e

pela Proposição 9.2.1, temos que $z_1 \cdot \bar{z}_2 + z_2 \cdot \bar{z}_1 \leq 2|z_1| \cdot |z_2|$, decorre das propriedades (8) e (4) que

$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2) \cdot \overline{(z_1 + z_2)} = z_1 \cdot \bar{z}_1 + z_1 \cdot \bar{z}_2 + z_2\bar{z}_1 + z_2 \cdot \bar{z}_2 \\ &= |z_1|^2 + 2\mathrm{Re}(z_1 \cdot \bar{z}_2) + |z_2|^2 \leq |z_1|^2 + 2|z_1| \cdot |z_2| + |z_2|^2 \\ &= (|z_1| + |z_2|)^2. \end{aligned}$$

Extraindo a raiz quadrada dos dois extremos das desigualdades acima, obtemos o resultado. □

Problemas

2.1 Demonstre as propriedades de (1) a (11) da conjugação e do módulo.

2.2 Ache uma condição necessária e suficiente para que valha a igualdade na Proposição 9.2.2.

2.3 Seja $S^1 = \{z \in \mathbb{C};\ |z| = 1\}$. Mostre que

a) Se $z \in S^1$ então z é invertível e $z^{-1} = \bar{z}$.

b) Se $z_1, z_2 \in S^1$, então $z_1 \cdot z_2 \in S^1$.

c) Se $z \in S^1$, então $z^{-1} \in S^1$.

d) Se para algum $n \in \mathbb{Z}\backslash\{0\}$ tem-se $z^n = 1$, então $z \in S^1$.

2.4 Mostre que qualquer que seja $z \in \mathbb{C}$, tem-se

$$\frac{1}{\sqrt{2}}\,(\mathrm{Re}\, z + \mathrm{Im}\, z) \leq |z| \leq |\mathrm{Re}\, z| + |\mathrm{Im}\, z|.$$

3 Forma trigonométrica

Nesta seção, daremos a representação dos números complexos em coordenadas polares. A relação entre coordenadas cartesianas e polares resultou num dos instrumentos mais poderosos na teoria dos números complexos, sem o qual seria praticamente impossível operar com estes números, especialmente no que diz respeito à extração de raízes.

Seja $z = a + bi$ um número complexo não nulo e sejam r o módulo de z e θ o ângulo orientado (módulo 2π radianos) que o vetor (a, b) forma com o eixo $\mathbb{R} \times \{0\}$. Com estas notações, temos que

$$\begin{cases} a = r\cos\theta \\ b = r\,\mathrm{sen}\,\theta \end{cases}$$

Podemos então escrever

$$z = r(\cos\theta + i\,\mathrm{sen}\,\theta),$$

a qual é chamada de *forma trigonométrica* do número complexo z. Temos, portanto, que $r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1) = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2)$ se, e somente se, $r_1 = r_2$ e $\theta_1 = \theta_2 + 2m\pi$, para algum $m \in \mathbb{Z}$.

Exemplos

1) $1 = \cos 0 + i\,\mathrm{sen}\,0$.
2) $-1 = \cos\pi + i\,\mathrm{sen}\,\pi$.
3) $i = \cos\frac{\pi}{2} + i\,\mathrm{sen}\,\frac{\pi}{2}$.
4) $-i = \cos\frac{3\pi}{2} + i\,\mathrm{sen}\,\frac{3\pi}{2}$.
5) $1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4}\right)$.
6) $1 + \sqrt{3}i = 2\left(\cos\frac{\pi}{3} + i\,\mathrm{sen}\,\frac{\pi}{3}\right)$.

Proposição 9.3.1. *Sejam dados os números* $z_1 = r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1)$ *e* $z_2 = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2)$. *Tem-se que*

$$z_1 \cdot z_2 = r_1 \cdot r_2[\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)].$$

Demonstração Efetuando o produto, temos que

$$\begin{aligned} z_1 \cdot z_2 &= r_1 r_2[(\cos\theta_1\cos\theta_2 - \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2) + \\ &\quad + i(\cos\theta_1\,\mathrm{sen}\,\theta_2 + \mathrm{sen}\,\theta_1\cos\theta_2)] = \\ &= r_1 r_2[\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)]. \end{aligned}$$

□

Da Proposição 9.3.1, obtemos a seguinte regra:

O produto de dois números complexos tem por representação um vetor cujo módulo é o produto dos módulos destes números e cujo ângulo com o eixo $\mathbb{R} \times \{0\}$ é a soma dos ângulos (módulo 2π) que as representações destes números formam com o referido eixo.

Por exemplo, a multiplicação por i representa simplesmente uma rotação de um ângulo $\frac{\pi}{2}$ no sentido anti-horário. Mais geralmente, a multiplicação por $\cos\theta + i\,\mathrm{sen}\,\theta$ representa uma rotação de um ângulo θ no sentido anti-horário.

Proposição 9.3.2. *Sejam dados os números* $z_1 = r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1)$ *e* $z_2 = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2) \neq 0$. *Tem-se que*

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\,[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)]\,.$$

Demonstração Observe inicialmente que

$$\overline{z}_2 = r_1(\cos\theta_2 - i\,\mathrm{sen}\,\theta_2) = r_2\,[\cos(-\theta_2) + i\,\mathrm{sen}(-\theta_2)]\,.$$

Portanto, da Proposição 9.3.1, temos que

$$\begin{aligned}\frac{z_1}{z_2} &= \frac{z_1 \cdot \overline{z}_2}{z_2 \cdot \overline{z}_2} = \frac{1}{|z_2|^2}\, z_1 \cdot \overline{z}_2 \\ &= \frac{1}{r_2^2}\, r_1 r_2\,[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)] \\ &= \frac{r_1}{r_2}\,[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)]\,.\end{aligned}$$

□

Teorema 9.3.3 (Fórmula de De Moivre). *Para todo inteiro* n *e todo número complexo* $z = r(\cos\theta + i\,\mathrm{sen}\,\theta) \neq 0$, *temos que*

$$[r(\cos\theta + i\,\mathrm{sen}\,\theta)]^n = r^n(\cos n\theta + i\,\mathrm{sen}\,n\theta).$$

Demonstração Para $n = 0$, a igualdade é óbvia. Para $n > 0$, isto é facilmente demonstrado por indução usando a Proposição 9.3.1. Seja agora $n < 0$. Note que se $z = \cos\alpha + i\,\mathrm{sen}\,\alpha$, para algum $\alpha \in \mathbb{R}$, então $z^{-1} = \overline{z} = \cos\alpha - i\,\mathrm{sen}\,\alpha$, pois $z \cdot \overline{z} = |z|^2 = 1$. Temos então pelo caso $(-n) > 0$ que

$$[r(\cos\theta + i\,\mathrm{sen}\,\theta)]^n = [(r(\cos\theta + i\,\mathrm{sen}\,\theta))^{-n}]^{-1}$$

$$\begin{aligned}[r^{-n}(\cos(-n\theta) + i\,\mathrm{sen}(-n\theta)\,]^{-1} &= r^n(\cos n\theta - i\,\mathrm{sen}\,n\theta)^{-1} \\ &= r^n(\cos n\theta) + i\,\mathrm{sen}\,n\theta).\end{aligned}$$

□

Problemas

3.1 Escreva os seguintes números complexos sob forma trigonométrica.

a) -6 b) $1-i$ c) $-\frac{1}{2}-\frac{\sqrt{3}}{2}i$

d) $2+2\sqrt{3}i$ e) $16i$ f) $-\frac{1}{2}+\frac{\sqrt{2}}{2}i$

3.2 Mostre que se $\theta \neq 2m\pi$, para todo $m \in \mathbb{Z}$, então

a) $$1+\cos\theta+\cdots+\cos n\theta = \frac{\cos\dfrac{n\theta}{2}}{\operatorname{sen}\dfrac{\theta}{2}}\ \operatorname{sen}\ \frac{(n+1)\theta}{2}.$$

b) $$\operatorname{sen}\theta+\operatorname{sen}2\theta+\cdots+\operatorname{sen}n\theta = \frac{\operatorname{sen}\dfrac{n\theta}{2}}{\operatorname{sen}\dfrac{\theta}{2}}\ \operatorname{sen}\ \frac{(n+1)\theta}{2}.$$

Sugestão Substitua $z=\cos\theta+i\operatorname{sen}\theta$ na fórmula

$$1+z+z^2+\cdots+z^n=\frac{z^{n+1}-1}{z-1}.$$

3.3 Seja $n \in \mathbb{N}\setminus\{0\}$. Escreva

a) $\cos n\theta$ como polinômio de grau n em $\cos\theta$.

b) $\operatorname{sen} n\theta$ como produto de $\operatorname{sen}\theta$ por um polinômio de grau $n-1$ em $\cos\theta$.

Sugestão Escreva $(\cos\theta+i\operatorname{sen}\theta)^n$ pela fórmula de De Moivre, por um lado, e pelo binômio de Newton, por outro.

3.4 a) Escreva $\cos 3\theta$, $\cos 4\theta$ e $\cos 5\theta$ em função de $\cos\theta$.

b) Escreva $\operatorname{sen}3\theta$ e $\operatorname{sen}5\theta$ em função de $\operatorname{sen}\theta$.

c) Escreva $\frac{\operatorname{sen}4\theta}{\operatorname{sen}\theta}$ em função de $\cos\theta$.

d) Demonstre a identidade $\cos 5\theta+\cos 3\theta = 2\cos\theta\cos 4\theta$.

3.5 Mostre que $\cos\frac{\pi}{9}$ satisfaz a equação $8x^3-6x-1=0$.

Sugestão Use o Problema 3.4 (a).

3.6 Calcule $\cos 18^\circ$ e $\operatorname{sen}18^\circ$.

Sugestão Observe que $5\times 18 = 90$ e use as expressões de $\cos 5\theta$ e $\operatorname{sen}5\theta$ deduzidas no Problema 3.4.

3.7 Calcule o valor de $\left(\frac{\sqrt{3}+i}{2}\right)^n$ segundo os valores de $n \in \mathbb{Z}$.

4 Raízes

Sejam K um corpo e w um elemento de K. Se n é um número natural, uma *raiz* n*-ésima* de w é um elemento $z \in K$ tal que $z^n = w$. Dado um número complexo $w = a + bi$, queremos determinar as raízes n-ésimas de w. Se tentarmos seguir o mesmo procedimento que utilizamos no caso da extração de raízes quadradas, obtemos um sistema de equações cuja resolução é impraticável, indicando que este não é o caminho para resolver o problema. Veremos, no que se segue, como a fórmula de De Moivre nos permitirá resolver facilmente o problema.

Teorema 9.4.1. *Sejam dados um número complexo não nulo* $w = r(\cos\theta + i\,\mathrm{sen}\,\theta)$*, um número natural* n *e um sistema completo* $\mathcal{R}$ *de resíduos módulo* n*. Então* w *admite* n *raízes* n*-ésimas dadas por*

$$z_\lambda = \sqrt[n]{r}\left(\cos\frac{\theta + 2\lambda\pi}{n} + i\,\mathrm{sen}\,\frac{\theta + 2\lambda\pi}{n}\right), \quad \lambda \in \mathcal{R}.$$

Demonstração Ponhamos $z = \rho(\cos\alpha + i\,\mathrm{sen}\,\alpha)$. Queremos resolver em ρ e α a equação

$$[\rho(\cos\alpha + i\,\mathrm{sen}\,\alpha)]^n = r(\cos\theta + i\,\mathrm{sen}\,\theta).$$

Pela fórmula de De Moivre, temos que

$$\rho^n(\cos n\alpha + i\,\mathrm{sen}\,n\alpha) = r(\cos\theta + i\,\mathrm{sen}\,\theta),$$

logo

$$\begin{cases} \rho^n = r \\ n\alpha = 0 + 2\lambda\pi, \quad \lambda \in \mathbb{Z} \end{cases}$$

Temos então que

$$\begin{cases} \rho = \sqrt[n]{r} \\ \alpha = \frac{\theta + 2\lambda\pi}{n}, \quad \lambda \in \mathbb{Z} \end{cases}$$

Portanto, as raízes n-ésimas de w são dadas por

$$z_\lambda = \sqrt[n]{r}\left(\cos\frac{\theta + 2\lambda\pi}{n} + i\,\mathrm{sen}\,\frac{\theta + 2\lambda\pi}{n}\right), \quad \lambda \in \mathbb{Z}.$$

Como λ é um inteiro arbitrário, aparentemente, as raízes n-ésimas de w são em número infinito. Isto não é o caso, pois $z_\lambda = z_\mu$ se, e

somente se, $\frac{1}{2\pi}\left[\frac{\theta+2\lambda\pi}{n}-\frac{\theta+2\lambda\pi}{n}\right]\in\mathbb{Z}$, isto é equivalente a $\frac{\lambda-\mu}{n}\in\mathbb{Z}$, o que é equivalente a $\lambda\equiv\mu \bmod n$. Isto completa a demonstração. □

Na prática, tomamos $\mathcal{R}=\{0,1,\ldots,n-1\}$.

Exemplos

1. Resolvamos a equação $z^4=-4$.

A forma trigonométrica de -4 é $4(\cos\pi+i\operatorname{sen}\pi)$ e, portanto, as soluções da equação são:

$$z_\lambda=\sqrt[4]{4}\left(\cos\frac{\pi+2\lambda\pi}{4}+i\operatorname{sen}\frac{\pi+2\lambda\pi}{4}\right),\quad \lambda=0,1,2,3.$$

Calculando estes valores, temos

$$\begin{aligned}
z_0&=\sqrt{2}\left(\cos\frac{\pi}{4}+i\operatorname{sen}\frac{\pi}{4}\right)=1+i,\\
z_1&=\sqrt{2}\left(\cos\frac{3\pi}{4}+i\operatorname{sen}\frac{3\pi}{4}\right)=-1+i,\\
z_2&=\sqrt{2}\left(\cos\frac{5\pi}{4}+i\operatorname{sen}\frac{5\pi}{4}\right)=-1-i,\\
z_3&=\sqrt{2}\left(\cos\frac{7\pi}{4}+i\operatorname{sen}\frac{7\pi}{4}\right)=1-i.
\end{aligned}$$

2. Resolvamos a equação $z^3=i$.

Como $i=\cos\frac{\pi}{2}+i\operatorname{sen}\frac{\pi}{2}$, temos que as soluções da equação acima são

$$z_\lambda=\cos\frac{\pi/2+2\lambda\pi}{3}+i\operatorname{sen}\frac{\pi/2+2\lambda\pi}{3},\quad \lambda=0,1,2.$$

Donde,

$$\begin{aligned}
z_0&=\cos\frac{\pi}{6}+i\operatorname{sen}\frac{\pi}{6}=\frac{\sqrt{3}}{2}+\frac{i}{2},\\
z_1&=\cos\frac{5\pi}{6}+i\operatorname{sen}\frac{5\pi}{6}=-\frac{\sqrt{3}}{2}+\frac{i}{2},\\
z_2&=\cos\frac{9\pi}{6}+i\operatorname{sen}\frac{9\pi}{6}=-i.
\end{aligned}$$

3. Resolvamos a equação $z^3 = 1$.

Como $1 = \cos 0 + i \operatorname{sen} 0$, as soluções da equação acima são

$$z_\lambda = \cos \frac{2\lambda\pi}{3} + i \operatorname{sen} \frac{2\lambda\pi}{3}, \quad \lambda = 0, 1, 2.$$

Portanto,

$$\begin{aligned} z_0 &= \cos 0 + i \operatorname{sen} 0 = 1 \\ z_1 &= \cos \frac{2\pi}{3} + i \operatorname{sen} \frac{2\pi}{3} = \frac{-1 + \sqrt{3}i}{2}, \\ z_2 &= \cos \frac{4\pi}{3} + i \operatorname{sen} \frac{4\pi}{3} = \frac{-1 - \sqrt{3}i}{2}. \end{aligned}$$

Problemas

4.1 Resolva as seguintes equações:

a) $z^3 = 1 + i$ b) $z^3 = 1 - i$ c) $z^4 = 16i$

d) $z^4 = 1 - i$ e) $z^4 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ f) $z^6 = -4$

4.2 Compare os seguintes conjuntos: as raízes n-ésimas de i^2 e os quadrados das raízes n-ésimas de i.

5 Raízes da unidade

Num corpo K, uma *raiz n-ésima da unidade*, para $n \in \mathbb{N} \setminus \{0\}$, é uma solução da equação $z^n = 1$.

Quando $K = \mathbb{C}$, as raízes n-ésimas da unidade são dadas por:

$$\xi_\lambda = \cos \frac{2\lambda\pi}{n} + i \operatorname{sen} \frac{2\lambda\pi}{n}, \quad \lambda = 0, 1, \ldots, n-1.$$

As raízes n-ésimas complexas da unidade têm por representação no plano os vértices de um polígono regular de n lados inscrito no círculo unitário com centro em $z = 0$ e tendo um vértice no ponto $z = 1$. As raízes da unidade desempenham um papel importante em vários ramos da matemática e particularmente na teoria das equações algébricas.

Continuaremos representando com ξ_λ o número $\cos \frac{2\lambda\pi}{n} + i \operatorname{sen} \frac{2\lambda\pi}{n}$, para $\lambda \in \mathbb{Z}$, sem a restrição $\lambda = 0, 1, \ldots, n-1$.

Proposição 9.5.1. *As raízes* n*-ésimas da unidade em* $\mathbb{C}$ *gozam das seguintes propriedades:*

i) $\xi_\lambda \cdot \xi_\mu = \xi_{\lambda+\mu}$.

ii) $\xi_\lambda^\ell = \xi_{\ell\lambda}$, *para todo* $\ell \in \mathbb{Z}$.

iii) $\xi_\lambda^{-1} = \overline{\xi}_\lambda = \xi_{n-\lambda}$.

Demonstração (i) Decorre da Proposição 9.3.1.
(ii) Decorre da Fórmula de De Moivre (Teorema 9.3.3).
(iii) Decorre do fato que $\xi_\lambda^{-1} = \xi_{-\lambda}$ (de (ii)) e do fato que $-\lambda \equiv n - \lambda \bmod n$.

□

Proposição 9.5.2. *Num corpo* K*, as raízes* n*-ésimas de um elemento podem ser obtidas multiplicando-se uma raiz* n*-ésima qualquer fixada deste elemento pelas raízes* n*-ésimas da unidade.*

Demonstração Seja $w \in K$. Se $w = 0$, é claro que a equação $z^n = w$ tem apenas a solução $z = 0$, e o resultado é banalmente verificado. Suponha que b_0 seja uma solução da equação $z^n = w$, com $w \neq 0$, logo $b_0 \neq 0$. Seja b uma solução qualquer da equação, logo $b^n = b_0^n = w$. Consequentemente, $(b/b_0)^n = 1$ e, portanto, b/b_0 é uma raiz n-ésima da unidade, logo $b = b_0\xi$, com ξ uma raiz n-ésima da unidade. Por outro lado, se ξ é uma raiz n-ésima da unidade, é imediato verificar que $b_0\xi$ é solução da equação $z^n = w$. □

Certas raízes n-ésimas da unidade se destacam sobre as demais. Vejamos um exemplo para introduzir um novo conceito.

Considere as raízes quartas complexas da unidade:

$$\xi_0 = 1, \qquad \xi_1 = i, \qquad \xi_2 = -1, \qquad \xi_3 = -i.$$

Verifica-se facilmente que

$$\begin{aligned}
\{\xi_0^n;\ n \in \mathbb{Z}\} &= \{\xi_0\},\\
\{\xi_1^n;\ n \in \mathbb{Z}\} &= \{\xi_0, \xi_1, \xi_2, \xi_3\},\\
\{\xi_2^n;\ n \in \mathbb{Z}\} &= \{\xi_0, \xi_2\},\\
\{\xi_3^n;\ n \in \mathbb{Z}\} &= \{\xi_0, \xi_1, \xi_2, \xi_3\}.
\end{aligned}$$

Vamos então que as raízes ξ_1 e ξ_3 têm a propriedade de gerar por potenciação todas as raízes quartas complexas da unidade. A seguinte

proposição caracterizará as raízes n-ésimas complexas da unidade que possuem tal propriedade.

Proposição 9.5.3. *Seja* $\xi_\lambda = \cos\frac{2\lambda\pi}{n} + i\,\mathrm{sen}\,\frac{2\lambda\pi}{n}$, *com* $\lambda, n \in \mathbb{Z}$ *e* $n > 1$, *uma raiz* n*-ésima da unidade em* $\mathbb{C}$. *São equivalentes as seguintes condições:*

i) $\xi_\lambda^0, \xi_\lambda^1, \ldots, \xi_\lambda^{n-1}$ *são todas as raízes* n*-ésimas da unidade*.

ii) $\xi_\lambda^m \neq 1$, *para todo* m *tal que* $0 < m < n$.

iii) $(n, \lambda) = 1$.

Demonstração (i) $\Rightarrow$ (ii) Suponha, por absurdo, que $\xi_\lambda^m = 1$ para algum m tal que $0 < m < n$. Como $\xi_\lambda^0 = 1$, os números $\xi_\lambda^0, \xi_\lambda^1, \ldots, \xi_\lambda^{n-1}$ não são todos distintos e, portanto, não podem representar todas as raízes n-ésimas da unidade.
(ii) $\Rightarrow$ (iii) Suponha, por absurdo, que $d = (n, \lambda) \neq 1$. Temos então que $\lambda = \ell d$, para algum $\ell \in \mathbb{Z}$, e $n = m \cdot d$, com $m \in \mathbb{Z}$ e $0 < m < n$. Segue-se então, da Proposição 9.5.1, que

$$\xi_\lambda^m = \xi_{\ell d}^m = \xi_{m\ell d} = \xi_{n\ell} = 1,$$

contradição.
(iii) $\Rightarrow$ (i) Se $(n, \lambda) = 1$, então $\{0, \lambda, 2\lambda, \ldots, (n-1)\lambda\}$ é um sistema completo de resíduos módulo n (veja Problema 2.1 (b), Capítulo 6). Logo,

$$\{\xi_\lambda^0, \xi_\lambda^1, \xi_\lambda^2, \ldots, \xi_\lambda^{n-1}\} = \{\xi_0, \xi_\lambda, \xi_{2\lambda}, \ldots, \xi_{(n-1)\lambda}\}$$

é o conjunto de todas as raízes n-ésimas da unidade. □

Uma raiz n-ésima da unidade ξ em um corpo K que goza da propriedade (ii), ou seja $\xi^m \neq 1$, para todo m tal que $0 < m < n$, é chamada *raiz* n*-ésima primitiva da unidade.*

Corolário 9.5.4. *O número de raízes* n*-ésimas primitivas da unidade em* $\mathbb{C}$ *é* $\Phi(n)$.

Demonstração Isto decorre da propriedade (iii) da proposição, recordando que $\Phi(n)$ representa o número de inteiros λ tais que $0 < \lambda < n$ e $(n, \lambda) = 1$. □

Proposição 9.5.5. *Seja* K *um corpo. Um elemento* $\xi \in K$ *é simultaneamente raiz* n*-ésima e raiz* m*-ésima da unidade se, e somente se,* ξ *é raiz* d*-ésima da unidade, onde* $d = (m, n)$.

Demonstração Suponha que $\xi^n = \xi^m = 1$. Se $d = (m, n)$, então existem $r, s \in \mathbb{Z}$ tais que $d = rm + sn$. Logo,

$$\xi^d = \xi^{rm+sn} = (\xi^m)^r(\xi^n)^s = 1.$$

Reciprocamente, suponha que $\xi^d = 1$. Como $n = td$ e $m = \ell d$ para t e ℓ em $\mathbb{Z}$, segue-se que

$$\xi^n = \xi^{td} = (\xi^d)^t = 1\,,$$

e que

$$\xi^m = \xi^{\ell d} = (\xi^d)^\ell = 1\,.$$

□

Corolário 9.5.6. *Se* $(m, n) = 1$*, então* 1 *é a única raiz simultaneamente* n*-ésima e* m*-ésima da unidade.*

Por exemplo, as raízes simultaneamente 28-ésimas e 32-ésimas da unidade em $\mathbb{C}$ são as raízes quartas da unidade, pois $(28, 32) = 4$. Portanto, essas são 1, i, -1 e $-i$.

Proposição 9.5.7. *Suponha que* ξ *e* η *sejam respectivamente raízes* p*-ésima e* q*-ésima primitivas da unidade. Se* $(p, q) = 1$*, então* $\xi\eta$ *é raiz* pq*-ésima primitiva da unidade.*

Demonstração Inicialmente, observe que $\xi\eta$ é raiz pq-ésima da unidade, pois

$$(\xi\eta)^{pq} = (\xi^p)^q(\eta^q)^p = 1.$$

Suponha que $\xi\eta$ não seja raiz pq-ésima primitiva da unidade. Existe então $m \in \mathbb{N}$ tal que $0 < m < pq$ e $(\xi\eta)^m = 1$. Pela divisão euclidiana em $\mathbb{Z}$, existem $n_1, n_2, r_2, r_2 \in \mathbb{Z}$ tais que $m = pn_1 + r_1$ e $m = qn_2 + r_2$, com $0 \leq r_1 < p$ e $0 \leq r_2 < q$. Logo,

$$1 = (\xi\eta)^m = \xi^{pn_1+r_1}\,\eta^{qn_2+r_2} = (\xi^{p(n_1}(\eta^q)^{n_2}\,\xi^{r_1}\,\eta^{r_2} = \xi^{r_1}\,\eta^{r_2}.$$

Temos então que ξ^{r_1} é o inverso da raiz q-ésima da unidade η^{r_2} e, portanto, também raiz q-ésima da unidade. Segue-se então que ξ^{r_1} é simultaneamente raiz p-ésima e raiz q-ésima da unidade. Consequentemente, pelo Corolário 9.5.6, temos que $\xi^{r_1} = 1$. Como ξ é raiz p-ésima primitiva da unidade e $0 \leq r_1 < p$, segue-se que $r_1 = 0$. Um raciocínio totalmente análogo implica que $r_2 = 0$. Consequentemente, temos que

$p \mid m$ e $q \mid m$ e como $(p, q) = 1$, temos que $pq \mid m$. Isto contradiz o fato que $0 < m < pq$. □

Corolário 9.5.8. *Seja* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *um inteiro maior do que ou igual a* 2 *decomposto em fatores primos. Sejam* η_i, *com* $i = 1, \ldots, r$, *respectivamente, raízes* $p_i^{\alpha_i}$*-ésimas primitivas da unidade. Então* $\eta = \eta_1 \cdots \eta_r$ *é uma raiz* n*-ésima primitiva da unidade.*

Exemplo Considre a raiz quarta primitiva complexa da unidade

$$\xi = \cos \frac{2\pi}{4} + i \operatorname{sen} \frac{2\pi}{4},$$

e a raiz nona primitiva da unidade

$$\eta = \cos \frac{2\pi}{9} + i \operatorname{sen} \frac{2\pi}{9}.$$

Logo, é raiz trigésima sexta primitiva da unidade o número complexo:

$$\xi\eta = -\operatorname{sen} \frac{2\pi}{9} + i \cos \frac{2\pi}{9} \cdot$$

Problemas

5.1 Sejam ξ_λ com $\lambda = 0, 1, \ldots, n-1$ as raízes n-ésimas da unidade em $\mathbb{C}$ e seja m um inteiro qualquer. Calcule:

a) $\xi_0^m + \xi_1^m + \cdots + \xi_{n-1}^m$.

b) $\xi_0^m \cdot \xi_1^m \cdots \xi_{n-1}^m$.

5.2 Seja $\xi \neq 1$ uma raiz n-ésima da unidade. Mostre que ξ é raiz da equação

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0.$$

5.3 Seja $p > 1$ um número primo. Mostre que

a) Toda raiz p-ésima da unidade diferente de 1 é primitiva.

b) As raízes p^α-ésimas da unidade não primitivas são raízes $p^{\alpha-1}$-ésimas da unidade.

5.4 Seja ξ uma raiz n-ésima primitiva da unidade. Mostre que ξ^m é uma raiz n-ésima primitiva da unidade, para algum inteiro m, se, e somente se, $(m, n) = 1$.

5.5 Prove que as raízes n-ésimas primitivas complexas da unidade são duas a duas conjugadas.

5.6 Seja ξ uma raiz n-ésima da unidade. Considere o conjunto

$$P(\xi) = \{m \in \mathbb{Z};\ \xi^m = 1\}.$$

a) Mostre que $P(\xi)$ é um ideal não nulo de $\mathbb{Z}$. Se p é o gerador positivo de $P(\xi)$, então p é chamado de período de ξ.

b) Se ξ é uma raiz primitiva, qual é o seu período?

c) Mostre que $\xi^m = 1$ se, e somente se, $p \mid m$. Em particular, conclua que $p \mid n$.

d) Mostre que o período de uma raiz complexa da unidade ξ_λ é precisamente $\frac{n}{(\lambda,n)}$.

5.7 Com as definições do Problema 5.6, calcule o período da raiz complexa

a) décimo segunda da unidade ξ_8.

b) trigésima da unidade ξ_{12}.

c) n-ésima da unidade ξ_1.

5.8 Sejam $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$ e $\rho = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i$, respectivamente, raízes primitivas cúbica e oitava da unidade em $\mathbb{C}$. Ache valores para λ e μ, inteiros, de modo que

$$\cos 15^\circ + i \operatorname{sen} 15^\circ = w^\lambda \rho^\mu .$$

Use este resultado para calcular cos 15° e sen 15°.

5.9 Seja $z = \cos\theta + i \operatorname{sen}\theta$, com $\theta \in \mathbb{R}$. Mostre que as seguintes condições são equivalentes:

i) z é raiz da unidade.

ii) $\frac{\theta}{2\pi} \in \mathbb{Q}$.

iii) o conjunto $\{z^n;\ n \in \mathbb{Z}\}$ é finito.

Apêndice

Noções de lógica matemática

A lógica matemática lida com sentenças matemáticas, isto é, frases declarativas de conteúdo matemático e que devem possuir um valor lógico bem definido tomado dentre as duas possibilidades: verdade (**V**) ou falso (**F**).

O objetivo da lógica matemática é a construção de mecanismos para determinar quando uma dada instância de um raciocínio matemático é correta ou não. Portanto, trata-se de uma teoria formal, no sentido que não se preocupa com o significado nem com a interpretação das sentenças em si, mas preocupa-se apenas com o seu valor lógico e com o seu encadeamento, que deve basear-se em regras bem precisas de raciocínio que ela descreve.

Cabe observar que para a maioria dos matemáticos a lógica não é um fim por si só, constituindo-se apenas num meio; ou seja, uma de suas importantes ferramentas de trabalho.

Representaremos as sentenças com letras minúsculas do alfabeto latino, ususalmente as consoantes $\mathtt{p}, \mathtt{q}, \mathtt{r}, \mathtt{s}$ e $\mathtt{t}$. Duas sentenças $\mathtt{p}$ e $\mathtt{q}$ serão consideradas logicamente equivalentes quando elas tiverem o mesmo valor lógico; neste caso escrevemos $\mathtt{p} \equiv \mathtt{q}$.

1 Conectivos lógicos

As sentenças matemáticas são os componentes do raciocínio matemático, que se juntam através dos conectivos para formar novas sentenças.

Há basicamente cinco conectivos lógicos que descreveremos abaixo.

1.1. Negação Dada uma sentença p, a sua negação (não p) forma uma nova sentença denotada por $\sim p$, cujo valor lógico é o oposto do valor lógico de p.

Isto é representado por meio de uma tabela, chamada tabela verdade, como se segue:

p	$\sim p$
V	F
F	V

Note que a dupla negação de uma sentença p nos conduz a uma sentença cujo valor lógico é idêntico ao de p. Em símbolos:

$$\sim (\sim p) \equiv p.$$

Exemplo 1 Sejam $p : 2 < 3$ e $q : 1 = 2$. Temos que o valor lógico de p é V e o de q é F e que $\sim p : 2 \geq 3$ e $\sim q : 1 \neq 2$, cujos valores lógicos são, respectivamente, F e V.

1.2. Conjunção Duas sentenças podem ser combinadas numa única sentença mediante o uso do conectivo de *conjunção* **e**. Dados p e q, forma-se a sentença (p **e** q), simbolizada por $p \wedge q$, que é classificada como verdade ou falso segundo a seguinte tabela verdade:

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

Note que $p \wedge q$ só é verdade se ambos p e q são verdade.

Exemplo 2

$2 < 3 \wedge 1 \neq 2$ é verdade,
$2 < 3 \wedge 1 = 2$ é falso,
$1 = 2 \wedge 1 \neq 1$ é falso.

Note também que o valor lógico de $p \wedge q$ não depende da ordem em que p e q são tomados. Em símbolos, isto se expressa como

$$p \wedge q \equiv q \wedge p,$$

quaisquer que sejam os valores lógicos de p e q. Isto significa que a conjunção é uma operação comutativa.

Exemplo 3 Usando a conjunção, podemos descrever a interseção de dois conjuntos A e B do seguinte modo:

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

1.3. Disjunção Duas sentenças também podem ser combinadas numa única sentença mediante o uso do conectivo de *disjunção* **ou**. Dados p e q, forma-se a sentença (p **ou** q), simbolizada por $p \vee q$, que é classificada como verdade ou falso segundo a seguinte tabela verdade:

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

Note que $p \vee q$ só é falso se ambos p e q são falsos. Note também que o nosso conectivo de disjunção tem caráter inclusivo, isto é, $p \vee q$ não exclui o fato de p e q serem simultaneamente verdade, em contraste com o uso do ou significando uma coisa ou outra.

Exemplo 4

$2 < 3 \vee 1 \neq 2$ é verdade,
$2 < 3 \vee 1 = 2$ é verdade,
$1 = 2 \vee 1 \neq 1$ é falso.

O valor lógico de $p \vee q$ também não depende da ordem em que p e q são tomados. Em símbolos, isto se expressa como

$$p \vee q \equiv q \vee p,$$

e significa que a disjunção é uma operação comutativa.

Exemplo 5 Usando a disjunção, podemos descrever a união de dois conjuntos A e B como se segue:

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

1.4. Condicional Duas sentenças podem ser juntadas numa única sentença mediante o uso do conectivo *condicional*. Dados p e q, forma-se a sentença (**se** p, **então** q), simbolizada por $p \to q$, que é classificada como verdade ou falso segundo a seguinte tabela verdade:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Este é o mais delicado e ao mesmo tempo mais importante dentre todos os conectivos, pois ele é o principal instrumento para realizar deduções em Matemática. De fato, é ele que permite expressar que uma dada sentença é consequência de outra.

Note que $p \to q$ só é falso se p é verdade e q é falso; ou seja, $p \to q$ é verdade toda vez que p é falso. O que precisa ser bem compreendido é que de uma asserção falsa p segue-se qualquer asserção, por mais absurdo que isso possa parecer.

Conta-se a esse respeito uma anedota envolvendo o famoso matemático inglês G.H. Hardy. Estava Hardy numa festa conversando numa roda sobre amenidades, quando lhe escapou que de uma asserção falsa poder-se ia concluir qualquer coisa. Rápido como uma águia, um dos seus interlocutores lançou-lhe o seguite desafio:
- Dou-lhe a sentença $2 + 2 = 6$, prove-me que você é o Papa.

Hardy pensou um pouco e disse:
- Suponha então que $2 + 2 = 6$. Logo $4 = 6$. Dividindo ambos os lados da igualdade por 2, tem-se que $2 = 3$. Somando -1 a ambos os lados dessa nova igualdade, obtemos $1 = 2$. Invertendo, temos $2 = 1$. Agora, é bem sabido que eu e o Papa somos dois homens. Mas como dois é igual a um, o Papa e eu somos um.

Exemplo 6

$$2 < 3 \to 1 \neq 2 \text{ é verdade}, \quad 2 < 3 \to 1 = 2 \text{ é falso},$$
$$1 = 2 \to 1 \neq 1 \text{ é verdade}, \quad 1 = 2 \to 2 = 2 \text{ é verdade}.$$

Note que o valor lógico de $p \to q$ depende da ordem em que p e q são tomados. Por exemplo, se p é verdade e q é falso, temos que $p \to q$ é falso, enquanto $q \to p$ é verdade.

Numa sentença condicional $p \to q$, a sentença p é chamada de *antecedente*, enquanto q é chamada de *consequente*.

Quando a sentença condicional $p \to q$ for verdade escrevemos $p \Rightarrow q$ e dizemos que p *implica* q.

Assim, de acordo com o Exemplo 6 temos que

$$2 < 3 \Rightarrow 1 \neq 2, \quad 1 = 2 \Rightarrow 1 \neq 1, \quad 1 = 2 \Rightarrow 2 = 2.$$

1.5. Bicondicional Dados p e q, forma-se a sentença (p **se e somente se** q), simbolizada por $p \leftrightarrow q$, que é classificada como verdade ou falso segundo a seguinte tabela verdade:

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

Portanto, $p \leftrightarrow q$ é verdade quando, e somente quando, p e q têm mesmo valor lógico. Em outras palavras, é sempre verdade a sentença

$$(p \leftrightarrow q) \leftrightarrow (p \equiv q).$$

Exemplo 7

$$2 < 3 \leftrightarrow 1 \neq 2 \text{ é verdade},$$
$$2 < 3 \leftrightarrow 1 = 2 \text{ é falso},$$
$$1 = 2 \leftrightarrow 1 = 1 \text{ é falso},$$
$$1 = 2 \leftrightarrow 2 \neq 2 \text{ é verdade}.$$

Note que o valor lógico de $p \leftrightarrow q$ não depende da ordem em que p e q são tomados. Em símbolos,

$$p \leftrightarrow q \equiv q \leftrightarrow p.$$

No caso em que $p \leftrightarrow q$ for verdade, escrevemos $p \Longleftrightarrow q$ e dizemos que p é uma *condição necessária e suficiente* para q. Assim, temos que

$$(p \leftrightarrow q) \Longleftrightarrow (p \equiv q).$$

O bicondicional pode ser expresso através do condicional e do conectivo *e*. De fato, temos que

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p).$$

Para verificar isto, note que, por definição, o lado esquerdo da equivalência só é verdade se p e q têm mesmo valor lógico. Vejamos agora o que ocorre com o lado direito. Este só será verdade se ambos $p \rightarrow q$ e $q \rightarrow p$ são verdade, o que só não ocorre quando p é verdade e q é falso ou quando q é verdade e p é falso, ou seja, quando p e q têm valores lógicos distintos.

Esta verificação poderia ser feita de modo mais mecânico, porém certamente mais entediante, usando tabelas verdade.

Problemas

1.1 Mostre que

a) $p \wedge p \equiv p$ b) $p \wedge F \equiv F$ c) $p \wedge V \equiv p$

d) $p \wedge \sim p \equiv F$ e) $p \wedge q \equiv q \wedge p$

1.2 Mostre que

a) $p \vee p \equiv p$ b) $p \vee F \equiv p$ c) $p \vee V \equiv V$

d) $p \vee q \equiv q \vee p$ e) $p \vee \sim p \equiv V$

1.3 Mostre que não vale a equivalência:

$$(p \rightarrow q) \rightarrow r \equiv p \rightarrow (q \rightarrow r).$$

1.4 Mostre as equivalências:

a) $p \rightarrow q \equiv \sim p \vee q$.

b) $p \leftrightarrow q \equiv (\sim p \vee q) \wedge (\sim q \vee p)$.

1.5 Com o uso dos conectivos citados no texto, crie o conectivo disjuntivo *ou*, denotado por $\sqcup$, tal que $p \sqcup q$ é verdade se e somente se apenas uma das duas sentenças p ou q é verdade.

2 Cálculo sentencial

Os conectivos lógicos funcionam como operações aritméticas sobre sentenças onde a equivalência entre sentenças desempenha o papel da igualdade na aritmética comum. Desse modo, podemos olhar a equivalência entre composições de sentenças, via conectivos lógicos, como identidades que independem do valor lógico de cada sentença envolvida, expressando assim propriedades aritméticas dos conectivos. A isso chamamos de *cálculo sentencial*.

A seguir daremos uma lista de propriedades dos conectivos.

2.1. Propriedades da Conjunção

Vimos no Problema 1.1 que valem as equivalências:

$$\begin{aligned} p \wedge p &\equiv p \\ p \wedge q &\equiv q \wedge p \end{aligned}$$

chamadas, respectivamente, de idempotência e comutatividade da conjunção.

Estas propriedades decorrem imediatamente da definição. Menos imediata é a propriedade a seguir.

Associatividade da Conjunção Dadas sentenças p, q e r, tem-se que

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r).$$

De fato, pode-se verificar esta propriedade mediante a construção de uma tabela verdade como se segue:

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

Alternativamente, podemos fazer a verificação de modo mais inteligente como se segue:

$(\mathtt{p} \wedge \mathtt{q}) \wedge \mathtt{r}$ só é verdade se $(\mathtt{p} \wedge \mathtt{q})$ é verdade e $\mathtt{r}$ é verdade, o que por sua vez só é verdade se $\mathtt{p}$ é verdade, $\mathtt{q}$ é verdade e $\mathtt{r}$ é verdade.

Por outro lado,
$\mathtt{p} \wedge (\mathtt{q} \wedge \mathtt{r})$ só é verdade se $\mathtt{p}$ é verdade e $(\mathtt{q} \wedge \mathtt{r})$ é verdade, o que por sua vez só é verdade se $\mathtt{p}$ é verdade, $\mathtt{q}$ é verdade e $\mathtt{r}$ é verdade.

Isto mostra a equivalência anunciada.

2.2. Propriedades da Disjunção

No Problema 1.2 tivemos a oportunidade de mencionar as seguintes propriedades:

$$\begin{aligned} \mathtt{p} \vee \mathtt{p} &\equiv \mathtt{p} \\ \mathtt{p} \vee \mathtt{q} &\equiv \mathtt{q} \vee \mathtt{p} \end{aligned}$$

chamadas, respectivamente, de idempotência e comutatividade da disjunção.

Estas propriedades decorrem imediatamente da definição. Temos também a propriedade a seguir.

Associatividade da Disjunção Dadas sentenças $\mathtt{p}$, $\mathtt{q}$ e $\mathtt{r}$, tem-se

$$(\mathtt{p} \vee \mathtt{q}) \vee \mathtt{r} \equiv \mathtt{p} \vee (\mathtt{q} \vee \mathtt{r}).$$

A verificação desta equivalência decorre das seguintes afirmações:

Temos que $(\mathtt{p} \vee \mathtt{q}) \vee \mathtt{r}$ só é falso se $(\mathtt{p} \vee \mathtt{q})$ é falso e $\mathtt{r}$ é falso, o que por sua vez só é falso se $\mathtt{p}$ é falso, $\mathtt{q}$ é falso e $\mathtt{r}$ é falso.

Por outro lado, $\mathtt{p} \vee (\mathtt{q} \vee \mathtt{r})$ só é falso se $\mathtt{p}$ é falso e $(\mathtt{q} \vee \mathtt{r})$ é falso, o que por sua vez só é falso se $\mathtt{p}$ é falso, $\mathtt{q}$ é falso $\mathtt{r}$ é falso.

A seguir listamos algumas das várias relações existentes entre os conectivos lógicos.

2.3. Distributividade Valem as seguintes equivalências:

$$\mathtt{p} \wedge (\mathtt{q} \vee \mathtt{r}) \equiv (\mathtt{p} \wedge \mathtt{q}) \vee (\mathtt{p} \wedge \mathtt{r})$$

$$\mathtt{p} \vee (\mathtt{q} \wedge \mathtt{r}) \equiv (\mathtt{p} \vee \mathtt{q}) \wedge (\mathtt{p} \vee \mathtt{r})$$

Verificaremos apenas a primeira das identidades acima, deixando a segunda à cargo do leitor.

Temos que $p \wedge (q \vee r)$ só é verdade se p é verdade e $q \vee r$ é verdade, ou seja, só é verdade se p é verdade e q ou r é verdade.

Por outro lado, $(p \wedge q) \vee (p \wedge r)$ só é verdade se $p \wedge q$ é verdade ou $p \wedge r$ é verdade, ou seja, só é verdade se p é verdade e q ou r é verdade.

Isto mostra a equivalência.

2.4. Leis de De Morgan Valem as seguintes equivalências:

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

Novamente, verificaremos apenas a primeira equivalência, deixando a segunda como exercício para o leitor.

A primeira equivalência decorre das seguintes afirmações:

Temos que $\sim (p \wedge q)$ só é verdade se $p \wedge q$ é falso, o que só ocorre quando p é falso ou q é falso, o que por sua vez só ocorre quando $\sim p$ é verdade ou $\sim q$ é verdade.

A primeira das leis de De Morgan nos mostra que

$$p \wedge q \equiv \sim (\sim p \vee \sim q),$$

o que por sua vez mostra que a conjunção pode ser obtida a partir apenas da negação e da disjunção.

2.5. Propriedades do Condicional

Valem as seguintes equivalências:

i) $p \to q \equiv (\sim p) \vee q$.

ii) $\sim (p \to q) \equiv p \wedge \sim q$.

iii) $p \to q \equiv \sim q \to \sim p$.

Para verificar (i), note que $p \to q$ só é falso quando p é verdade e q é falso, o mesmo ocorrendo claramente para $(\sim p) \vee q$.

Para verificar (ii), usa-se a seguinte cadeia de equivalências, que decorrem de (i) e das leis de De Morgan:

$$\sim (p \to q) \equiv \sim [(\sim p) \vee q] \equiv p \wedge \sim q.$$

Para verificar (iii), temos de (i) que

$$\sim q \rightarrow \sim p \ \equiv \sim(\sim q) \vee \sim p \ \equiv \sim p \vee q \ \equiv \ p \rightarrow q.$$

A propriedade (i) acima mostra que também o conectivo implicação pode se expressar em termos apenas da negação e da disjunção.

A sentença $\sim q \ \rightarrow \sim p$ é chamada de sentença *contrapositiva* de $p \rightarrow q$, à qual é equivalente.

Damos abaixo um exemplo típico de aplicação na aritmética comum da sentença contrapositiva.

Suponha que a e b representem dois inteiros. Dizer que

$$a \neq 0 \text{ e } b \neq 0 \implies a \cdot b \neq 0$$

é equivalente a dizer que

$$a \cdot b = 0 \implies a = 0 \text{ ou } b = 0.$$

2.6. Silogismos

Um *silogismo* ou uma *tautologia* é uma sentença composta por várias sentenças ligadas por conectivos e que sempre tem o valor lógico verdade, qualquer que sejam os valores lógicos das sentenças que a compõem.

Há algumas tautologias que são óbvias, como por exemplo:

1) $V \vee p$
2) $p \vee \sim p$,
3) $p \rightarrow p$,
4) $p \leftrightarrow p$,

Menos óbvio, é o seguinte silogismo, um dos mais importantes da lógica matemática.

Modus Ponens: $[\,(p \rightarrow q) \wedge p\,] \rightarrow q$.

Para mostrar que a sentença acima é uma tautologia, note que ela só seria falsa se $(p \rightarrow q) \wedge p$ fosse verdade e q falso, o que só aconteceria se $p \rightarrow q$ fosse verdade, p fosse verdade e q falso, mas isto só ocorreria se q fosse verdade e ao mesmo tempo falso, impossível.

Note que a tautologia Modus Ponens pode ser escrita como

$$(p \to q) \wedge p \Rightarrow q.$$

É possível construir inúmeras tautologias; entretanto, vamos nos contentar em listar algumas a seguir que serão úteis.

5) $p \to p \vee q$.
6) $p \wedge q \to p$.
7) $[(p \to q) \wedge (q \to r)] \to (p \to r)$.
8) $\sim q \wedge (p \to q) \to \sim p$.

Verificação:
(5) Usando a propriedade (i) do condicional, temos que

$$p \to p \vee q \equiv \sim p \vee (p \vee q) \equiv (\sim p \vee p) \vee q \equiv V \vee q \equiv V.$$

(6) Usando a propriedade (i) do condicional, a lei de De Morgan e a distributividade da disjunção, temos

$$p \wedge q \to p \equiv \sim (p \wedge q) \vee p \equiv (\sim p \vee \sim q) \vee p$$

$$\equiv (\sim p \vee p) \vee \sim q \equiv V \vee \sim q,$$

donde se segue o resultado por ser $V \vee \sim q$ uma tautologia.
(7) Isto decorre facilmente da tabela verdade.
(8) Temos que

$$\sim q \wedge (p \to q) \to \sim p \equiv \sim [\sim q \wedge (\sim p \vee q)] \vee \sim p \equiv q \vee (p \wedge \sim q) \vee \sim p$$

$$\equiv (q \vee \sim p) \vee (p \wedge \sim q) \equiv (q \vee \sim p) \vee [\sim (q \vee \sim p)] \equiv V.$$

Problemas

2.1 Decida quais das sentenças abaixo são tautologias
(a) $(p \wedge q \to r) \to (p \to (q \to r))$
(b) $(p \to (q \to r)) \to (p \wedge q \to r)$
(c) $((p \to q) \wedge \sim q) \to \sim p$
(d) $(p \to q) \to (p \vee r \to q \vee r)$
(e) $(p \to q) \to (p \wedge r \to q \wedge r)$

2.2 Mostre que a sentença abaixo é uma tautologia

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

2.3 É a sentença abaixo uma tautologia?

$$(p \wedge q) \rightarrow r \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow r).$$

2.4 Mostre que a sentença abaixo á uma tautologia

$$(p \rightarrow q) \wedge (p' \rightarrow q') \rightarrow (p \vee p' \rightarrow q \vee q')$$

3 Quantificadores

É comum em matemática trabalhar com as chamadas sentenças abertas, cuja definição damos a seguir.

Uma *sentença aberta* em uma indeterminada x sobre um conjunto S é uma frase de conteúdo matemático onde figura a letra x como palavra e que se torna uma sentença quando x é substituido pelo nome de um objeto bem determinado do conjunto S. Uma sentença aberta em x será representada por um símbolo como $p(x)$ (que se lê-se p de x).

Exemplo 1 Sejam dadas as seguintes sentenças abertas:

$p(x)$: x é um número positivo,

$q(x)$: x é um número primo,

$r(x)$: $2x + 1 > 3$.

Temos que $p(1), p(2)$; $q(2), q(3), q(5), q(7)$; $r(2)$ e $r(3)$ são verdade, enquanto $p(-1)$; $q(4), q(6), q(8), q(9)$; $r(0), r(1)$ e $r(-1)$ são falsos.

É comum quantificar uma sentença aberta $p(x)$, transformando-a numa sentença de verdade. Abaixo descrevemos os dois quantificadores usados em matemática.

O *quantificador existencial*, representado pelo símbolo $\exists$ e usado como se segue :

$$\exists\, x \in S,\ p(x),$$

significando que existe pelo menos um x em S tal que $p(x)$ é verdade.

O *quantificador universal*, representado pelo símbolo $\forall$ e usado como se segue:

$$\forall\, x \in S,\ p(x),$$

significando que para todo x em S, a sentença $p(x)$ é verdade.

O quantificador universal pode ser utilizado para representar a relação de inclusão entre conjuntos, como se segue:

$$A \subset B \ \equiv\ \forall x \in S,\ x \in A \rightarrow x \in B,$$

onde S é o universo onde A e B vivem.

Daí conclui-se que $A = B$ é equivalente a

$$\forall x \in S,\ x \in A \leftrightarrow x \in B.$$

A negação de uma sentença $\exists\, x,\ p(x)$ é obtida mostrando que para todo x tem-se que $p(x)$ é falso; ou seja, $\sim p(x)$ é verdade. Portanto,

$$\sim (\exists\, x,\ p(x)) \equiv \forall\, x,\ \sim (p(x)).$$

Por outro lado, a negação de uma sentença $\forall\, x,\ p(x)$ é obtida mostrando que existe pelo menos um x tal que $p(x)$ é falso; ou seja, $\sim p(x)$ é verdade. Portanto,

$$\sim (\forall\, x,\ p(x)) \equiv \exists\, x,\ \sim (p(x)).$$

Problemas

3.1 Negue a sentença:

$$\forall \varepsilon,\ \ \exists \delta,\ \ p(\delta) \rightarrow q(\varepsilon).$$

3.2 Mostre que $A \not\subset B$ pode se expressar como:

$$\exists x\ \ x \in A \wedge\ x \notin B.$$

3.3 Mostre que $A \neq B$ pode se expressar como:

$$\exists x,\ \ (x \in A\ \wedge\ x \notin B)\ \vee\ (x \in B\ \wedge\ x \notin A).$$

3.4 Mostre que

$$\exists x,\ (P(x) \wedge Q(x)) \implies \exists x,\ P(x) \wedge \exists x,\ Q(x).$$

Dê um exemplo mostrando que não vale a implicação inversa.

3.5 Mostre que

$$\exists x,\ (P(x) \vee Q(x)) \iff \exists x,\ P(x) \vee \exists x,\ Q(x).$$

4 O que são os Teoremas?

Desde o tempo de Euclides, 300 AC, a matemática tem tido um modo bem peculiar de ser apresentada. Em linhas gerais, a apresentação de uma teoria matemática segue um roteiro onde se inicia com os *conceitos primitivos* que são os conceitos que não se definem, como por exemplo os conceitos de ponto, reta e plano na Geometria Euclidiana, o conceito de elemento e de conjunto na Teoria dos Conjuntos, etc. Os conceitos primitivos possuem propriedades que são aceitas sem prova e que são enunciados nos axiomas.

As sentenças matemáticas que enunciam as demais propriedades dos objetos em estudo são os chamados *teoremas*. Normalmente, cada um desses consiste de um enunciado formado por uma sentença declarativa, na maioria das vezes sob forma de um condicional $p \to q$, cujo valor lógico se afirma ser verdade, ou seja, é da forma $p \Rightarrow q$. As sentenças que compõem o antecedente p da implicação são chamadas de hipóteses, enquanto que o consequente q é a tese.

Tais asserções, por não serem em geral óbvias, requerem uma demonstração. Em matemática, há vários tipos de demonstrações, a seguir descreveremos muito brevemente três desses tipos mais comuns.

Demonstração Direta Esse tipo de demonstração, o mais comum de todos, consiste no uso seguido do Modus Ponens. Trata-se de determinar uma sequência de sentenças $p_1 = p, p_2, \ldots, p_n = q$, onde p é a hipótese e q é a tese, de modo que se prove ser verdade a sentença $p_1 \to p_2$. Sendo p_1 verdade, por Modus Ponens temos que p_2 é verdade. Em seguida supomos que se prove que $p_2 \to p_3$ é verdade, logo do mesmo

modo conclui-se que p_3 é verdade; e, assim sucessivamente, concluindo desse modo que a tese $p_n = q$ é verdade.

Demonstração por Absurdo Esse tipo de demonstração, usa o seguinte silogismo:

$$(p \Rightarrow q) \Longleftrightarrow (p \wedge \sim q \rightarrow F).$$

Para provar $p \Rightarrow q$, admitem-se as hipóteses p, nega-se a tese q e tenta-se chegar a uma contradição (ie. uma sentença falsa). Esse tipo de prova é utilizado em vários lugares no livro.

Demonstração por Indução Esse tipo de demonstração é estudado em detalhes no Capítulo 3.

Os teoremas se dividem em *lemas*, *proposições*, *teoremas*, propriamente ditos, e *corolários*, segundo uma certa hierarquia que explicamos a seguir.

Via de regra, um lema é um resultado técnico que, isoladamente, não tem um enunciado impactante, mas que é parte essencial na prova de uma proposição ou de um teorema. Às vezes são necessários vários lemas para se provar um teorema. As proposições são resultados cujo significado pode ser compreendido de modo mais universal. Reserva-se o nome teorema às proposições mais importantes de uma teoria.

O termo corolário é reservado aos resultados que se seguem de modo bastante direto das proposições e dos teoremas.

Para finalizar este apêndice mostraremos como as noções de lógica que apresentamos nesse apêndice podem ser utilizadas para demonstrar os resultados sobre conjuntos que provamos no Capítulo 1.

Por exemplo, a Proposição 1 do Capítulo 1 é uma consequência direta da tautologia do Problema 2.4. As Proposições 2 e 3 decorrem imediatamente das propriedades de distributividade da disjunção com relação à conjunção e de distributividade da conjunção com relação à disjunção. As Proposições 5 e 6 são consequências das leis de De Morgan.

Bibliografia

[1] A. Hefez, *Elementos de Aritmética*, Textos Universitários, SBM 2006.

[2] S.C. Coutinho, *Números Inteiros e Criptografia RSA*, Série de Computação Matemática, IMPA-SBM 2000.

[3] W.J. Leveque, *Topics in Number Theory*, Volume 1, Addison-Wesley 1956.

[4] L.H.J. Monteiro, *Elementos de Álgebra*, Coleção Elementos de Matemática, Ao Livro Técnico 1969.

[5] I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley 1955.

[6] A. Weil, *Number Theory for Beginners*, com a colaboração de M. Rosenlicht, Springer-Verlag 1979.

Índice Remissivo

Índice Remissivo

O autor:

Abramo Hefez graduou-se em Matemática na Pontifícia Universidade Católica do Rio de Janeiro. Posteriormente, estudou e pesquisou na Universidade de Pisa, Itália. Obteve o grau de PhD em Matemática no Massachusetts Institute of Technology e o título de Livre Docente na Unicamp. É Professor Titular na Universidade Federal Fluminense. Suas áreas de pesquisa são a Geometria Algébrica e a Teoria Algébrica de Singularidades, nas quais publicou dezenas de artigos. É também autor e coautor de vários livros.

A coleção

A coleção Matemática Universitária é uma série de livros escritos por matemáticos competentes e com grande experiência didática, a fim de servirem de textos para cursos em nível de graduação nas universidades brasileiras.

Os livros da coleção contêm exposições objetivas e bem organizadas, acompanhadas de exercícios selecionados.

O livro

Este é um livro texto para o primeiro curso de Álgebra destinado aos alunos de graduação em Matemática e cursos afins. O livro trata da Álgebra dos conjuntos numéricos (inteiros, racionais, reais e complexos) e contém muitos exercícios. A apresentação é elementar e cada conceito introduzido é ilustrado com vários exemplos.

impa

INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA