Capítulo III

Números Reais

Tudo quanto vai ser dito nos capítulos seguintes se referirá a conjuntos de números reais: funções definidas e tomando valores nesses conjuntos, limites, continuidade, derivadas e integrais dessas funções. Por isso vamos estabelecer agora os fundamentos da teoria dos números reais.

Nossa atitude será a seguinte. Faremos uma lista contendo vários fatos elementares a respeito de números reais. Estes fatos serão admitidos como axiomas, isto é, não serão demonstrados. Deles deduziremos certas conseqüências, que demonstraremos como teoremas. Devemos esclarecer que, não somente o que usaremos neste livro, mas TODAS as propriedades dos números reais decorrem logicamente dos axiomas que enunciaremos neste capítulo. Esses axiomas apresentam o conjunto $\mathbb{R}$ dos números reais como um corpo ordenado completo.

Como as noções de corpo e de corpo ordenado possuem interesse algébrico próprio, apresentamos os axiomas dos números reais por etapas, deixando em último lugar a existência do sup, precisamente o axioma não-algébrico, aquele que desempenhará o papel mais importante nos capítulos seguintes.

Um espírito mais crítico indagaria sobre a *existência* dos números reais, ou seja, se realmente se conhece algum exemplo de corpo ordenado completo. Em outras palavras: partindo dos números naturais (digamos, apresentados através dos axiomas de Peano) seria possível, por meio de extensões sucessivas do conceito de número, chegar à construção dos números reais? A resposta é afirmativa. Isto pode ser feito de várias maneiras. A passagem crucial é dos racionais para os reais, a qual pode seguir o método dos cortes de Dedekind ou das seqüências de Cauchy (devido a Cantor), para citar apenas os dois mais populares.

Existem livros, como [Dedekind], [Landau], [Cohen e Ehrlich], que tratam apenas das extensões do conceito de número. Outros, como [Rudin] e [Jacy Monteiro] dedicam capítulos ao assunto. Estas são referências bibliográficas que recomendamos aos leitores interessados. Frisamos, porém, que nosso ponto de vista coincide com o exposto na p. 511 de [Spivak]:

"É inteiramente irrelevante que um número real seja, por acaso, uma coleção de números racionais; tal fato nunca deveria entrar na demonstração de qualquer teorema importante sobre números reais. Demonstrações aceitáveis deveriam usar apenas o fato de que os números reais formam um corpo ordenado completo..."

Assim, um processo qualquer de construção dos números reais a partir dos racionais é importante apenas porque prova que corpos ordenados completos existem. A partir daí, tudo o que interessa é que $\mathbb{R}$ é um corpo ordenado completo.

Uma pergunta relevante é, porém, a seguinte: ao definir o conjunto $\mathbb{R}$ dos números reais, não estamos sendo ambíguos? Em outras palavras, será que existem dois corpos ordenados completos com propriedades distintas? Esta é a questão da *unicidade* de $\mathbb{R}$.

Evidentemente, num sentido exageradamente estrito, não se pode dizer que existe apenas *um* corpo ordenado completo. Se construímos os números reais por meio de cortes de Dedekind, obtemos um corpo ordenado completo cujos elementos são coleções de números racionais. Se usamos o processo de Cantor, o corpo ordenado completo que obtemos é formado por classes de equivalência de seqüências de Cauchy. São, portanto, dois corpos ordenados completos diferentes um do outro. O ponto fundamental é que eles diferem apenas pela natureza dos seus elementos, mas não pela maneira como esses elementos se comportam. Ora, já concordamos, desde o capítulo anterior, em adotar o método axiomático, segundo o qual a natureza intrínseca dos objetos matemáticos é uma matéria irrelevante, sendo o importante as relações entre esses objetos. Assim sendo, a maneira adequada de formular a questão da unicidade dos números reais é a seguinte: existem dois corpos ordenados completos não-isomorfos? A resposta é negativa. Dados K, L, corpos ordenados completos, existe uma única bijeção $f\colon K \to L$ tal que $f(x+y) = f(x)+f(y)$ e $f(x\cdot y) = f(x)\cdot f(y)$. A função f chama-se um *isomorfismo* entre K e L. Ela cumpre, *ipso-facto*, a condição $x < y \Leftrightarrow f(x) < f(y)$. Os corpos K e L são, pois, *isomorfos*, ou seja, indistinguíveis no que diz respeito a propriedades de corpos ordenados completos.

Os Exercícios 55 e 56 no fim deste capítulo sugerem uma demonstração de que, a menos de um isomorfismo, existe apenas um corpo ordenado completo. Isto garante que os axiomas que apresentaremos a seguir descrevem os números reais sem ambigüidade alguma.

1 Corpos

Um *corpo* é um conjunto K, munido de duas operações, chamadas *adição* e *multiplicação*, que satisfazem a certas condições, chamadas os *axiomas de corpo*, abaixo especificadas.

A adição faz corresponder a cada par de elementos $x, y \in K$ sua *soma* $x + y \in K$, enquanto a multiplicação associa a esses elementos o seu produto $x \cdot y \in K$. Os axiomas de corpo são os seguintes:

A. *Axiomas da adição*

A1. *Associatividade* – quaisquer que sejam $x, y, z \in K$, tem-se $(x + y) + z = x + (y + z)$.

A2. *Comutatividade* – quaisquer que sejam $x, y \in K$, tem-se

$x + y = y + x$.

A3. *Elemento neutro* – existe $0 \in K$ tal que $x + 0 = x$, seja qual for $x \in K$. O elemento 0 chama-se *zero*.

A4. *Simétrico* – todo elemento $x \in K$ possui um simétrico $x \in K$ tal que $x + (-x) = 0$.

Da comutatividade, segue-se que $0 + x = x$ e $-x + x = 0$, seja qual for $x \in K$. A soma $x + (-y)$ será indicada com a notação $x - y$ e chamada a *diferença* entre x e y. A operação $(x, y) \mapsto x - y$ chama-se *subtração*.

Somando-se y a ambos os membros de uma igualdade do tipo $x - y = z$ obtém-se $x = y + z$. Analogamente, se $x = y + z$ então, somando $-y$ a ambos os membros, obtém-se $x - y = z$. Portanto, $x - y = z \Leftrightarrow x = y + z$. Daí decorre que o zero é único. Ou seja, se $x + \theta = x$ (para algum $x \in K$ e algum $\theta \in K$) então $\theta = x - x$, ou seja $\theta = 0$. Resulta também que todo $x \in K$ tem somente um simétrico: se $x + y = 0$, então, $y = 0 - x$, ou seja $y = -x$. Também temos $-(-x) = x$, já que $(-x) + x = 0$. Finalmente, vale a lei do corte: $x + z = y + z \Rightarrow x = y$. (Basta somar $-z$ a ambos os membros da primeira igualdade.) Concluímos assim que as regras usuais relativas à adição e subtração decorrem dos quatro axiomas acima e são, portanto, válidas em qualquer corpo. A propósito, um conjunto onde está definida apenas uma operação satisfazendo a estes axiomas é o que se chama um *grupo abeliano*.

B. *Axiomas da multiplicação*

M1. *Associatividade* – dados quaisquer x, y, z em K, tem-se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M2. *Comutatividade* – sejam quais forem $x, y \in K$, vale $x \cdot y = y \cdot x$.

M3. *Elemento neutro* – existe $1 \in K$ tal que $1 \neq 0$ e $x \cdot 1 = x$, qualquer que seja $x \in K$. O elemento 1 chama-se *um*.

M4. *Inverso multiplicativo* – todo $x \neq 0$ em K possui um inverso

x^{-1}, tal que $x \cdot x^{-1} = 1$.

Por comutatividade, segue-se que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in K$, e que $x \cdot x^{-1} = x^{-1} \cdot x = 1$ para todo $x \neq 0$ em K.

Os axiomas acima dizem, em particular, que os elementos diferentes de 0 num corpo K formam um grupo abeliano em relação à operação de multiplicação. (O elemento neutro é 1 e, em vez do simétrico $-x$, temos o inverso x^{-1}.) Conseqüentemente, valem propriedades análogas às que foram acima demonstradas para a adição, tendo-se o cuidado de lembrar que 0 *não possui inverso multiplicativo.*

Dados x e y em K, com $y \neq 0$, escreve-se também x/y em vez de $x \cdot y^{-1}$. A operação $(x, y) \mapsto x/y$, definida para x qualquer e $y \neq 0$ em K, chama-se *divisão* e o resultado x/y é o *quociente* de x por y. *Não se divide por zero:* $x/0$ *não tem sentido.*

Se $y \neq 0$, tem-se $x/y = z \Leftrightarrow x = y \cdot z$. Daí se deduz a utilíssima *lei do corte*: Se $x \cdot z = y \cdot z$ e $z \neq 0$, então $x = y$. (É importante ter em mente que $x \cdot z = y \cdot z$ só implica $x = y$ quando se sabe, *a priori* que $z \neq 0$.) Se $x \cdot y = x$ para todo $x \in K$ então, tomando $x = 1$ obtemos $y = 1$. Isto prova a unicidade do 1. Sabendo-se apenas que $x \cdot y = x$ para um certo x, há duas possibilidades: se $x \neq 0$ então $y = 1$, pela lei do corte. Se, porém, $x = 0$ então y pode ser qualquer pois, como veremos logo a seguir, $0 \cdot y = 0$ para todo $y \in K$. Finalmente, se $x \cdot y = 1$ então, como veremos abaixo, $x \neq 0$ e $y \neq 0$ e (multiplicando por x^{-1}) concluímos $y = x^{-1}$. Isto prova a unicidade do elemento inverso.

Por fim, as operações de adição e multiplicação num corpo K acham-se relacionadas por um axioma, com o qual fica completa a definição de corpo.

D1. *Axioma da distributividade.* Dados x, y, z quaisquer, em K, tem-se $x \cdot (y + z) = x \cdot y + x \cdot z$.

Por comutatividade, tem-se também $(x + y) \cdot z = x \cdot z + y \cdot z$.

Resulta desse axioma que $x \cdot 0 = 0$ para todo $x \in K$. Com efeito, $x \cdot 0 + x = x \cdot 0 + x \cdot 1 = x(0 + 1) = x \cdot 1 = x$, donde

$x \cdot 0 = 0$.

Por outro lado, dados $x, y \in K$ com $x \cdot y = 0$, segue-se que $x = 0$ ou $y = 0$. Com efeito, se for $x \cdot y = 0$ e $x \neq 0$, então obtemos $x \cdot y = x \cdot 0$ e, por corte, $y = 0$. Assim, num corpo K, tem-se $x \cdot y \neq 0$ sempre que os dois fatores x e y forem ambos diferentes de zero.

No axioma da distributividade está a explicação das "regras dos sinais" da Álgebra Elementar: $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ e $(-x) \cdot (-y) = x \cdot y$. De fato, em primeiro lugar temos $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = 0 \cdot y = 0$, donde $(-x) \cdot y = -(x \cdot y)$. Analogamente, $x \cdot (-y) = -(x \cdot y)$. Logo $(-x) \cdot (-y) = -[x \cdot (-y)] = -[-(x \cdot y)] = x \cdot y$. Em particular, $(-1) \cdot (-1) = 1$.

Exemplos de corpos.

Exemplo 1. O conjunto $\mathbb{Q}$ dos números racionais, com as operações $(p/q) + (p'/q') = (pq' + p'q)/qq'$ e $(p/q) \cdot (p'/q') = pp'/qq'$. (Lembremos a igualdade: $p/q = p'/q' \Leftrightarrow pq' = p'q$.) O simétrico de p/q é $-p/q$. O zero é $0/q$, seja qual for $q \neq 0$. O inverso do número racional $p/q \neq 0$ é q/p.

Exemplo 2. O corpo $\mathbb{Z}_2 = \{0, 1\}$, formado apenas de dois elementos distintos 0 e 1, com as operações $0 + 1 = 1 + 0 = 1$, $0 + 0 = 1 + 1 = 0$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ e $1 \cdot 1 = 1$. Aqui, o simétrico de cada elemento é ele próprio (e o inverso também).

Exemplo 3. O corpo $\mathbb{Q}(i)$, cujos elementos são os pares ordenados $z = (x, y)$ de números racionais. (Ou seja, como conjunto, $\mathbb{Q}(i) = \mathbb{Q} \times \mathbb{Q}$.) As operações são definidas assim: $(x, y) + (x', y') = (x + x', y + y')$ e $(x, y) \cdot (x', y') = (xx' - yy', x'y + xy')$. O zero é o elemento $(0, 0)$ e a unidade é o elemento $(1, 0)$. Escrevendo x para representar o par $(x, 0)$ e usando a notação $i = (0, 1)$, observamos que cada elemento $z = (x, y) = (x, 0) + (0, y)$ pode escrever-se como $z = x + iy$ e que as operações acima foram definidas de modo que os "números complexos" da forma $z = x+iy$ se somem e multipliquem da maneira usual, com o cuidado de notar que $i^2 = -1$. $\mathbb{Q}(i)$ chama-se o *corpo dos números complexos racionais.* A verificação dos axiomas fica a cargo do leitor. Por exemplo, dado $z = (x, y) \neq 0$, tem-se $z^{-1} = \left(\dfrac{x}{x^2+y^2}, \dfrac{-y}{x^2+y^2}\right)$.

Exemplo 4. O conjunto $\mathbb{Q}(t)$, das funções racionais $r(t) = \dfrac{p(t)}{q(t)}$, onde p e q são polinômios com coeficientes racionais, sendo q não identicamente nulo. Se $u(t)$ é também não identicamente nulo, tem-se $\dfrac{p(t)}{q(t)} = \dfrac{p(t)\cdot u(t)}{q(t)\cdot u(t)}\cdot$ As operações em $\mathbb{Q}(t)$ são definidas da maneira óbvia.

Para encerrar estas considerações gerais sobre corpos, observemos um fato útil. Num corpo K, $x^2 = y^2 \Rightarrow x = \pm y$. Com efeito $x^2 = y^2 \Rightarrow x^2 - y^2 = 0 \Rightarrow (x+y)(x-y) = 0 \Rightarrow x+y = 0$ ou $x - y = 0$. No primeiro caso, $x = -y$ e, no segundo, $x = y$.

2 Corpos ordenados

Um *corpo ordenado* é um corpo K, no qual se destacou um subconjunto $P \subset K$, chamado o conjunto dos elementos *positivos* de K, tal que as seguintes condições são satisfeitas:

P1. A soma e o produto de elementos positivos são positivos. Ou seja, $x, y \in P \Rightarrow x + y \in P$ e $x \cdot y \in P$.

P2. Dado $x \in K$, exatamente uma das três alternativas seguintes ocorre: ou $x = 0$, ou $x \in P$ ou $-x \in P$.

Assim, se indicarmos com $-P$ o conjunto dos elementos $-x$, onde $x \in P$, temos $K = P \cup (-P) \cup \{0\}$, sendo os conjuntos P, $-P$ e $\{0\}$ dois a dois disjuntos. Os elementos de $-P$ chamam-se *negativos.*

Num corpo ordenado, se $a \neq 0$ então $a^2 \in P$. Com efeito, sendo $a \neq 0$, ou $a \in P$ ou $-a \in P$. No primeiro caso, $a^2 = a \cdot a \in P$. No segundo caso $a^2 = (-a)\cdot(-a) \in P$. Em particular, num corpo ordenado $1 = 1 \cdot 1$ é sempre positivo.

Segue-se que $-1 \in -P$. Em particular, num corpo ordenado, -1 não é quadrado de elemento algum.

Exemplo 5. $\mathbb{Q}$ é um corpo ordenado, no qual o conjunto P é formado pelos números racionais p/q tais que $p \cdot q \in \mathbb{N}$. (Intuitivamente, isto significa que os inteiros p e q têm "o mesmo sinal".)

Exemplo 6. O corpo $\mathbb{Q}(t)$ pode ser ordenado chamando-se uma fração $r(t) = \dfrac{p(t)}{q(t)}$ positiva quando, no polinômio pq, o coeficiente do termo de mais alto grau for positivo. O conjunto P das frações positivas segundo esta definição cumpre as condições P1 e P2. Com efeito, dadas as frações positivas $r = \dfrac{p}{q}$ e $r' = \dfrac{p'}{q'}$, os coeficientes dos termos de graus mais elevados em pq e em $p'q'$ são > 0. Em $r + r'$, o produto do numerador pelo denominador é o polinômio $pq(q')^2 + p'q' \cdot q^2$, cujo termo de mais alto grau deve ter coeficiente positivo. Logo, a soma de duas frações "positivas" é positiva. As demais afirmações se verificam sem dificuldade.

Exemplo 7. O corpo $\mathbb{Z}_2$ não pode ser ordenado pois $1 + 1 = 0$ enquanto num corpo ordenado 1 deve ser positivo e a soma $1+1$, de dois elementos positivos deveria ainda ser positiva. Também o corpo $\mathbb{Q}(i)$, dos números complexos racionais, não comporta uma ordenação compatível com suas operações pois o quadrado do elemento $i = (0, 1)$ é igual a -1. Num corpo ordenado, nenhum quadrado pode ser negativo e -1 sempre é negativo.

Num corpo ordenado K, escreveremos $x < y$, e diremos que x é *menor do que* y, para significar que $y - x \in P$, ou seja, que $y = x + z$, onde $z \in P$. Nas mesmas circunstâncias, escreve-se também $y > x$ e diz-se que y *é maior do que* x.

Em particular $x > 0$ significa que $x \in P$, isto é, que x é positivo, enquanto $x < 0$ quer dizer que x é negativo, isto é, que $-x \in P$. Se $x \in P$ e $y \in -P$ tem-se sempre $x > y$.

A relação de ordem $x < y$ num corpo ordenado K goza das propriedades seguintes:

O1. *Transitividade* – se $x < y$ e $y < z$ então $x < z$.
O2. *Tricotomia* – dados $x, y \in K$, ocorre exatamente uma das alternativas seguintes: ou $x = y$, ou $x < y$, ou $x > y$.
O3. *Monotonicidade da adição* – se $x < y$ então, para todo $z \in K$, tem-se $x + z < y + z$.
O4. *Monotonicidade da multiplicação* – se $x < y$ então, para todo $z > 0$, tem-se $xz < yz$. Se, porém, for $z < 0$, então $x < y$ implica $xz > yz$.

Demonstremos estas propriedades:

O1. Dizer $x < y$ e $y < z$ significa afirmar que $y - x \in P$ e $z - y \in P$. Por P1 concluímos que $(z - y) + (y - x) \in P$, ou seja, $z - x \in P$, o que significa $x < z$.
O2. Dados $x, y \in K$, ou $y - x \in P$, ou $y - x = 0$, ou $y - x \in -P$ (isto é, $x - y \in P$). No primeiro caso tem-se $x < y$, no segundo $x = y$ e no terceiro $x > y$. Estas possibilidades se excluem mutuamente, por P2.
O3. Se $x < y$ então $y - x \in P$, donde $(y + z) - (x + z) = y - x \in P$. Isso significa que $x + z < y + z$.
O4. Se $x < y$ e $z > 0$ então $y - x \in P$ e $z \in P$. Logo $(y - x) \cdot z \in P$, isto é, $y \cdot z - x \cdot z \in P$, o que significa $x \cdot z < y \cdot z$. Se, porém, $x < y$ e $z < 0$, então $y - x \in P$ e $-z \in P$, donde $(y - x) \cdot (-z) \in P$, isto é $x \cdot z - y \cdot z \in P$, o que significa $y \cdot z < x \cdot z$.

Em particular, num corpo ordenado K, $x < y$ é equivalente a $-y < -x$. Basta multiplicar ambos os membros de qualquer uma destas desigualdades por -1.

Segue-se de O1 e O3 que $x < y$ e $x' < y'$ implica $x + x' < y + y'$, ou seja, podem-se somar duas desigualdades, membro a membro. Com efeito, por O3, $x < y \Rightarrow x + x' < y + x'$ e $x' < y' \Rightarrow y + x' < y + y'$. Por O1, concluímos $x + x' < y + y'$.

Analogamente, de O1 e O4 segue-se que $0 < x < y$ e $0 < x' < y'$ implicam $xx' < yy'$, isto é, podem-se multiplicar membro a membro duas desigualdades formadas por elementos positivos.

Num corpo ordenado K, o produto de um elemento $x > 0$ por um elemento $y < 0$ dá um elemento $xy < 0$. (Basta observar que $x(-y) = -(x \cdot y)$ ou então multiplicar ambos os membros de $y < 0$ por x.) Como $1 > 0$, concluímos de $x \cdot x^{-1} = 1$ que se $x > 0$ deve ser $x^{-1} > 0$ também. Assim, o inverso de um elemento positivo é positivo. Segue-se que $x > 0$ e $y > 0$ implica $x/y > 0$.

Se $x < y$ e ambos são positivos, então $y^{-1} < x^{-1}$. Basta observar que $\frac{1}{y} - \frac{1}{x} = \frac{x-y}{xy} \cdot$

Num corpo ordenado K, escreve-se $x \leq y$ para significar que $x < y$ ou $x = y$. Lê-se: "x é menor do que ou igual a y". Nas mesmas circunstâncias, escreve-se $y \geq x$. Isto quer dizer, evidentemente, que $y - x \in P \cup \{0\}$. Os elementos do conjunto $P \cup \{0\}$ chamam-se *não-negativos* e são caracterizados pela relação $x \geq 0$.

Tem-se, evidentemente, $x \leq x$ para todo $x \in K$.

Dados $x, y \in K$, tem-se $x = y$ se, e somente se, $x \leq y$ e $y \leq x$. É muito freqüente, em Análise, provar-se que dois números x e y são iguais mostrando-se primeiro que $x \leq y$ e, depois, que $y \leq x$.

Com exceção de O2 (tricotomia), que é substituída pelas propriedades $x \leq x$ (reflexividade) e $x \leq y,\ \ y \leq x \Leftrightarrow x = y$ (anti-simetria), todas as propriedades acima demonstradas para a relação $x < y$ transferem-se para $x \leq y$.

Num corpo ordenado K, como $1 > 0$, temos $1 < 1 + 1 < 1 + 1 + 1 < \ldots$ e o subconjunto de K formado por estes elementos é, portanto, infinito. Mais precisamente, vamos mostrar como se pode considerar o conjunto $\mathbb{N}$, dos números naturais, naturalmente imerso em K.

Temporariamente, indiquemos com o símbolo $1'$ o elemento unidade do corpo ordenado K. Definamos uma função $f \colon \mathbb{N} \to K$ pondo $f(1) = 1'$, $f(2) = 1' + 1'$, etc. A maneira correta de definir f é por indução: $f(1) = 1'$ e $f(m + 1) = f(m) + 1'$. Por indução, verifica-se que $f(m + n) = f(m) + f(n)$ e que (como todos os valores $f(n)$ são positivos) $m < p \Rightarrow f(m) < f(p)$.

Assim, a função $f\colon \mathbb{N} \to K$ define uma bijeção do conjunto $\mathbb{N}$ dos números naturais sobre um subconjunto $\mathbb{N}' = f(\mathbb{N})$, formado pelos elementos $1'$, $1' + 1'$, $1' + 1' + 1'$, etc. Costuma-se identificar $\mathbb{N}'$ com $\mathbb{N}$ e considerar os números naturais contidos em K. Isto é o que faremos. Temos $\mathbb{N} \subset K$ e voltamos a escrever 1, em vez de $1'$.

Em particular, todo corpo ordenado é infinito e tem "característica zero", isto é $1 + 1 + \cdots + 1 \neq 0$ sempre.

Dado o corpo ordenado K e considerando $\mathbb{N} \subset K$, como estamos fazendo, os simétricos $-n$ dos elementos $n \in \mathbb{N}$ e mais o zero ($0 \in K$) constituem um grupo abeliano, que se identifica com o grupo $\mathbb{Z}$ dos inteiros. Assim, temos $\mathbb{N} \subset \mathbb{Z} \subset K$.

Mais ainda, dados $m, n \in \mathbb{Z}$, com $n \neq 0$, existe o inverso $n^{-1} \in K$. Podemos, portanto, nos referir ao conjunto formado por todos os elementos $m \cdot n^{-1} = \dfrac{m}{n} \in K$, onde $m, n \in \mathbb{Z}$ e $n \neq 0$. Este conjunto é um subcorpo de K (isto é, as operações de K, quando aplicadas a elementos deste conjunto dão resultados ainda no conjunto). Trata-se do menor subcorpo de K. Com efeito, todo subcorpo deve conter pelo menos 0 e 1; por adições sucessivas de 1, todo subcorpo de K deve conter $\mathbb{N}$; por tomadas de simétricos, deve conter $\mathbb{Z}$ e, por divisões em $\mathbb{Z}$, deve conter o conjunto das frações $\dfrac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$. Evidentemente, este menor subcorpo de K identifica-se ao corpo $\mathbb{Q}$ dos números racionais.

Concluímos assim que, dado um corpo ordenado K, podemos considerar, de modo natural, as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset K$. Por exemplo, o corpo $\mathbb{Q}(t)$ contém as frações do tipo p/q, onde p e q são polinômios constantes, inteiros, com $q \neq 0$. Estas frações formam o corpo $\mathbb{Q}$ e tem-se $\mathbb{Q} \subset \mathbb{Q}(t)$.

Exemplo 8. *Desigualdade de Bernoulli.* Em todo corpo ordenado K, se $n \in \mathbb{N}$ e $x \geq -1$, vale $(1 + x)^n \geq 1 + nx$. Isto se demonstra por indução em n. Para $n = 1$ é óbvio. De $(1+x)^n \geq 1+n\cdot x$ deduz-se $(1+x)^{n+1} = (1+x)^n\cdot(1+x) \geq (1+nx)(1+x) = 1 + nx + x + nx^2 = 1 + (n + 1)x + n \cdot x^2 \geq 1 + (n + 1)x$.

(Multiplicaram-se ambos os membros da desigualdade $(1+x)^n \geq 1+n\cdot x$ por $1+x$. Por isso foi preciso supor $x \geq -1$.) Quando $n > 1 (n \in \mathbb{N})$ e $x > -1$, tem-se, pelo mesmo argumento, a desigualdade estrita $(1+x)^n > 1+n\cdot x$, desde que seja $x \neq 0$.

Observação sobre boa ordenação

O Princípio da Boa Ordenação não se aplica imediatamente ao conjunto $\mathbb{Z}$ dos inteiros. Existem conjuntos não-vazios de números inteiros que não possuem um menor elemento. O próprio $\mathbb{Z}$ é um deles: qualquer que seja $n \in \mathbb{Z}$, o inteiro $n-1$ é menor do que n, logo não existe um inteiro n_0 menor do que todos os outros. Também o conjunto $A = \{\ldots, -4, -2, 0, 2, \ldots\}$ dos inteiros pares, ou seja $A = \{2n; n \in \mathbb{Z}\}$, não possui um menor elemento. Em geral, se $X \subset \mathbb{N}$ for um conjunto infinito de números naturais, então o conjunto $-X = \{-n; n \in X\}$ é um conjunto não-vazio de números inteiros que não possui elemento mínimo.

Entretanto, podemos constatar o seguinte: *se um conjunto não-vazio $X \subset \mathbb{Z}$ for limitado inferiormente, isto é, se existir algum $a \in \mathbb{Z}$ tal que $a < x$ para todo $x \in X$, então X possui um elemento mínimo.*

Este fato se reduz ao Princípio da Boa Ordenação do seguinte modo. Sendo $a < x$ para todo $x \in X$, concluímos que os elementos do conjunto não-vazio $A = \{x - a; x \in X\}$ são todos números inteiros positivos, isto é, $A \subset \mathbb{N}$. Logo existe $n_0 \in A$, $n_0 =$ menor elemento de A. Temos $n_0 = x_0 - a$, com $x_0 \in X$ e, como se verifica facilmente, x_0 é o menor elemento do conjunto X.

Intervalos

Num corpo ordenado K, existe a importante noção de *intervalo*. Dados $a, b \in K$, com $a < b$, usaremos as notações abaixo:

$[a, b]$	$= \{x \in K; a \leq x \leq b\}$	$(-\infty, b]$	$= \{x \in K; x \leq b\}$
$[a, b)$	$= \{x \in K; a \leq x < b\}$	$(-\infty, b)$	$= \{x \in K; x < b\}$
$(a, b]$	$= \{x \in K; a < x \leq b\}$	$[a, +\infty)$	$= \{x \in K; a \leq x\}$
(a, b)	$= \{x \in K; a < x < b\}$	$(a, +\infty)$	$= \{x \in K; a < x\}$
		$(-\infty, +\infty)$	$= K$

Os quatro intervalos da esquerda têm *extremos* a e b. $[a, b]$ é um *intervalo fechado*, $[a, b)$ é *fechado à esquerda*, $(a, b]$ *é fechado à direita* e (a, b) é um *intervalo aberto*. Estes são intervalos *limitados*. Os cinco intervalos da direita são *ilimitados*: $(-\infty, b]$ é a *semi-reta* esquerda fechada, de origem b; $(-\infty, b)$ é a semi-reta esquerda aberta, de origem b; $[a, +\infty)$ é a semi-reta direita fechada, de origem a e $(a, +\infty)$ é a semi-reta direita aberta, de origem a. Finalmente, o intervalo total $(-\infty, +\infty) = K$ pode ser considerado aberto ou fechado.

Quando considerarmos um intervalo de extremos a e b, suporemos sempre $a < b$, com uma exceção que destacaremos agora. Ao tomarmos o intervalo fechado $[a, b]$, é conveniente admitir o caso em que $a = b$. O intervalo $[a, a]$ consiste em um único ponto a e chama-se *intervalo degenerado*. Todo intervalo não-degenerado é um conjunto infinito. Basta observar o seguinte: num corpo ordenado K, se $x < y$, então, $x < \dfrac{x+y}{2} < y$. Assim, se I for um intervalo contendo os elementos a, b, com $a < b$, podemos obter uma infinidade de elementos $x_1, x_2, \ldots, x_n, \ldots$ em I, tomando $x_1 = \dfrac{a+b}{2}$, $x_2 = \dfrac{a+x_1}{2}, \ldots, x_{n+1} = \dfrac{a+x_n}{2}, \ldots$ Teremos $a < \cdots < x_3 < x_2 < x_1 < b$.

Num corpo ordenado K, definiremos o *valor absoluto* de um elemento x, como sendo x, se $x \geq 0$ e $-x$ se $x < 0$. Usaremos o símbolo $|x|$ para indicar o valor absoluto. Assim,

$$\text{dado } x \in K, \text{ tem-se} \begin{cases} |x| = x & \text{se} \quad x > 0 \\ |0| = 0 \\ |x| = -x & \text{se} \quad x < 0 \end{cases}$$

A noção de valor absoluto é da maior importância em Análise. Estudaremos agora suas propriedades.

Dado x num corpo ordenado K, ou x e $-x$ são ambos zero, ou um é positivo e o outro é negativo. Aquele, entre x e $-x$, que não for negativo, será chamado $|x|$. Portanto, $|x|$ é o maior dos elementos x e $-x$. Este fato poderia ter sido usado como definição:

$$|x| = \max\{x, -x\}.$$

Temos, portanto, $|x| \geq x$ e $|x| \geq -x$. Esta última desigualdade pode ser escrita $-|x| \leq x$. Assim, temos

$$-|x| \leq x \leq |x|, \text{ para todo } x \in K.$$

Mais geralmente, vale o

Teorema 1. *Sejam* x, a *elementos de um corpo ordenado* K. *As seguintes afirmações são equivalentes;*

(i) $-a \leq x \leq a$*;*

(ii) $x \leq a$ *e* $-x \leq a$*;*

(iii) $|x| \leq a$.

Demonstração. $-a \leq x \leq a \Leftrightarrow [-a \leq x$ e $x \leq a]$ $\Leftrightarrow [a \geq x$ e $a \geq -x] \Leftrightarrow a \geq |x|$. A última equivalência se deve ao fato de ser $|x|$ o maior dos dois elementos x e $-x$.

Corolário. *Dados* a, x, $b \in K$, *tem-se* $|x-a| \leq b$ *se, e somente se,* $a - b \leq x \leq a + b$.

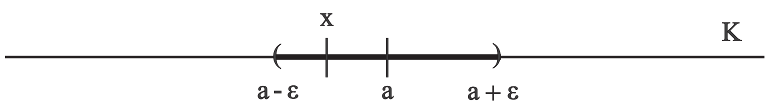
Com efeito, pelo teorema, $|x - a| \leq b$ é equivalente a $-b \leq x - a \leq b$, ou seja, $a - b \leq x \leq a + b$ (somando a).

Observação: Todas as afirmações do teorema e do seu corolário são ainda verdadeiras com $<$ em lugar de $\leq$, como se verifica facilmente.

Em particular, temos as seguintes equivalências, que serão utilizadas amplamente no estudo dos limites e das funções contínuas:

$$\boxed{x \in (a - \varepsilon, a + \varepsilon) \Leftrightarrow a - \varepsilon < x < a + \varepsilon \Leftrightarrow |x - a| < \varepsilon}$$

Se representarmos geometricamente os elementos de um corpo ordenado como pontos de uma reta, o valor absoluto $|x-a|$ significa a distância do ponto x ao ponto a. A relação $x < y$ significa que x está à esquerda de y. As equivalências acima exprimem o fato de que o intervalo aberto $(a-\varepsilon, a+\varepsilon)$, de centro a e raio ε, é formado pelos pontos x cuja distância a a é menor do que ε.



Tais interpretações geométricas não devem intervir nas demonstrações mas constituem um auxílio valiosíssimo para o entendimento dos conceitos e teoremas de Análise.

Teorema 2. *Para elementos arbitrários de um corpo ordenado* K*, valem as relações:*

(i) $|x+y| \le |x| + |y|$*;*

(ii) $|x \cdot y| = |x| \cdot |y|$*;*

(iii) $|x| - |y| \le \big|\,|x| - |y|\,\big| \le |x-y|$*;*

(iv) $|x-z| \le |x-y| + |y-z|$*.*

Demonstração. (i) se demonstra observando que $-|x| \le x \le |x|$ e $-|y| \le y \le |y|$, donde, por adição, $-(|x|+|y|) \le x+y \le |x|+|y|$. Pelo Teorema 1 isto significa que $|x+y| \le |x| + |y|$.

Para provar (ii), começamos notando que, seja qual for $x \in K$, temos $x^2 = |x|^2$, pois $|x|$ é um dos elementos x ou $-x$ e vale $x^2 = (-x)^2$. Logo $|x \cdot y|^2 = (x \cdot y)^2 = x^2 \cdot y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2$. Segue-se daí que $|x \cdot y| = \pm |x| \cdot |y|$. Como $|x \cdot y|$ e $|x| \cdot |y|$ são ambos não-negativos, concluímos que $|x \cdot y| = |x| \cdot |y|$.

Agora provemos (iii). Em virtude de (i), temos $|x| = |(x-y)+y| \le |x-y| + |y|$, o que dá $|x| - |y| \le |x-y|$. Pelo mesmo motivo, temos $|y| - |x| \le |y-x|$. Ora, é evidente que

$|y-x| = |x-y|$. Concluímos que $|y|-|x| \leq |x-y|$. Assim, valem, simultaneamente, $|x-y| \geq |x|-|y|$ e $|x-y| \geq -(|x|-|y|)$. Pelo Teorema 1, resulta que $||x|-|y|| \leq |x-y|$. A outra desigualdade em (iii) é óbvia.

A última afirmação do teorema, a desigualdade (iv), resulta de (i) aplicada à soma $x-z = (x-y)+(y-z)$.

Um subconjunto X de um corpo ordenado K chama-se *limitado superiormente* quando existe $b \in K$ tal que $b \geq x$ para todo $x \in X$. Em outras palavras, tem-se $X \subset (-\infty, b]$. Cada $b \in K$ com esta propriedade chama-se uma *cota superior* de X.

Analogamente, $X \subset K$ diz-se *limitado inferiormente* quando existe $a \in K$ tal que $x \in X \Rightarrow a \leq x$. Um elemento $a \in K$ com esta propriedade chama-se uma *cota inferior* de X. Tem-se então $X \subset [a, +\infty)$.

Um subconjunto X de um corpo ordenado K chama-se *limitado* quando é limitado superior e inferiormente, isto é, quando existem a, $b \in K$ tais que $X \subset [a, b]$.

Exemplo 9. No corpo $\mathbb{Q}$ dos números racionais, o conjunto $\mathbb{N}$ dos números naturais é limitado inferiormente, pois $\mathbb{N} \subset [0, \infty)$, mas não é limitado superiormente. Com efeito, dado qualquer $p/q \in \mathbb{Q}$, tem-se $|p|+1 \in \mathbb{N}$ e $|p|+1 > p/q$. O conjunto $\mathbb{Z} \subset \mathbb{Q}$ não é limitado superiormente nem inferiormente. Constitui talvez uma surpresa o fato de que existem corpos ordenados nos quais o conjunto $\mathbb{N}$ é limitado superiormente. Um deles é o corpo $\mathbb{Q}(t)$ das funções racionais, com a ordem introduzida no Exemplo 6. O polinômio $p(t) = t$ é uma fração com denominador 1, e, portanto, pertence a $\mathbb{Q}(t)$. Para todo $n \in \mathbb{N}$ o coeficiente do termo de mais alto grau de $t-n$ é positivo $(=1)$, logo $t-n \in P$. Logo, temos $n < t$ qualquer que seja $n \in \mathbb{N}$, isto é, $p(t) = t$ é uma cota superior para $\mathbb{N}$ em $\mathbb{Q}(t)$. Neste corpo, portanto, o conjunto $\mathbb{N}$ é limitado.

A propósito desta situação, temos a proposição abaixo.

Teorema 3. *Num corpo ordenado* K*, as seguintes afirmações são equivalentes:*

(i) $\mathbb{N} \subset K$ *é ilimitado superiormente;*

(ii) *dados* $a, b \in K$*, com* $a > 0$*, existe* $n \in \mathbb{N}$ *tal que* $n \cdot a > b$*;*

(iii) *dado qualquer* $a{>}0$ *em* K*, existe* $n{\in}\mathbb{N}$ *tal que* $0 < \frac{1}{n} < a$*.*

Demonstração. (i) $\Rightarrow$ (ii). Como $\mathbb{N}$ é ilimitado, dados $a > 0$ e b em K, existe $n \in \mathbb{N}$ tal que $\frac{b}{a} < n$ e, portanto, $b < a \cdot n$. Para provar que (ii) $\Rightarrow$ (iii), dado $a > 0$, existe, em virtude de (ii), um $n \in \mathbb{N}$ tal que $n \cdot a > 1$. Então $0 < \frac{1}{n} < a$. Finalmente, mostremos que (iii) $\Rightarrow$ (i). Dado qualquer $b > 0$ existe, por (iii) um $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{b}$, ou seja $n > b$. Assim, nenhum elemento > 0 em K pode ser cota superior de $\mathbb{N}$. Evidentemente, um elemento ≤ 0 também não pode. Logo $\mathbb{N}$ é ilimitado superiormente.

Um corpo ordenado K chama-se *arquimediano* quando nele é válida qualquer das três condições equivalentes citadas no Teorema 3.

Assim, o corpo $\mathbb{Q}$ dos números racionais é arquimediano, enquanto o corpo $\mathbb{Q}(t)$ das funções racionais, com a ordem introduzida no Exemplo 6, é não-arquimediano.

3 Números reais

Sejam K um corpo ordenado e $X \subset K$ um subconjunto limitado superiormente. Um elemento $b \in K$ chama-se *supremo* do subconjunto X quando b é a menor das cotas superiores de X em K. (Às vezes se diz "extremo superior" em vez de "supremo".)

Assim, para que $b \in K$ seja supremo de um conjunto $X \subset K$, é necessário e suficiente que sejam satisfeitas as duas condições abaixo:

S1. Para todo $x \in X$, tem-se $x \leq b$;
S2. Se $c \in K$ é tal que $x \leq c$ para todo $x \in X$, então $b \leq c$.

A condição S1 diz que b é cota superior de X, enquanto S2 afirma que qualquer outra cota superior de X deve ser maior do que ou igual a b.

A condição S2 pode ser reformulada assim:

S2'. Dado $c < b$ em K, existe $x \in X$ tal que $c < x$.

Com efeito, a condição S2' diz que nenhum elemento de K, que seja inferior a b, pode ser cota superior de X.

É imediato que se dois elementos b e b' em K cumprem as condições S1 e S2 acima, deve-se ter $b \leq b'$ e $b' \leq b$, ou seja $b = b'$. Portanto, o supremo de um conjunto, quando existe, é único. Escreveremos $\sup X$ para indicá-lo.

As condições que caracterizam o supremo podem, portanto, ser escritas assim:

S1. $x \in X \Rightarrow x \leq \sup X$;
S2. $c \geq x$ para todo $x \in X \Rightarrow c \geq \sup X$;
S2'. Se $c < \sup X$ então existe $x \in X$ tal que $c < x$.

Observação: Se $X = \emptyset$ então todo $b \in K$ é cota superior de X. Como não existe menor elemento num corpo ordenado K, segue-se que o conjunto vazio $\emptyset$ não possui supremo em K. O mesmo se aplica para o ínfimo, que estudaremos agora.

Analogamente, um elemento $a \in K$ chama-se *ínfimo* de um conjunto $Y \subset K$, limitado inferiormente, quando a é a maior das cotas inferiores de K.

Para que $a \in K$ seja o ínfimo de $Y \subset K$ é necessário e suficiente que as condições abaixo sejam satisfeitas:

I1. Para todo $y \in Y$ tem-se $a \leq y$;
I2. Se $c \in K$ é tal que $c \leq y$ para todo $y \in Y$, então $c \leq a$.

O ínfimo de Y, quando existe, é único e escreve-se $a = \inf Y$.

A condição I2 acima pode ser reformulada nos seguintes termos:

I2'. Dado $c \in K$ com $a < c$, existe $y \in Y$ tal que $y < c$.

Isso significa que um elemento c de K, que seja maior do que a, não pode ser cota inferior de Y.

Exemplo 10. Se $X \subset K$ possuir um elemento máximo, este será o seu supremo, se X possuir um elemento mínimo, ele será seu ínfimo. Reciprocamente, se $\sup X$ pertence a X então é o maior elemento de X; se $\inf X$ pertencer a X, será o seu menor elemento. Em particular, todo subconjunto finito $X \subset K$ possui inf e sup. Outro exemplo: se $X = (-\infty, b]$ e $Y = [a, +\infty)$, temos $\inf Y = a$ e $\sup X = b$.

Exemplo 11. Dados $a < b$ em K, seja $X = (a, b)$ o intervalo aberto com esses extremos. Tem-se $\inf X = a$ e $\sup X = b$. Com efeito, a é, evidentemente, uma cota inferior de X. Provemos agora que nenhum $c \in K$ com $a < c$ é cota inferior de X. Isto é claro se $c \geq b$. Por outro lado, se for $a < c < b$ então $x = \dfrac{a+c}{2}$ é um elemento de X, com $a < x < c$, o que prova que c não é cota inferior de X. Assim $a = \inf X$. De modo análogo se mostra que $b = \sup X$. Neste caso, tem-se $\sup X \notin X$ e $\inf X \notin X$.

Exemplo 12. Seja $Y \subset \mathbb{Q}$ o conjunto das frações do tipo $\dfrac{1}{2^n}$, com $n \in \mathbb{N}$.

Afirmamos que $\inf Y = 0$ e $\sup Y = \dfrac{1}{2}$. Com efeito, em primeiro lugar, temos $\dfrac{1}{2} \in Y$ e $\dfrac{1}{2^n} < \dfrac{1}{2}$ para todo $n > 1$. Logo $\dfrac{1}{2}$ é o maior elemento de Y e, por conseguinte, $\dfrac{1}{2} = \sup Y$. Por outro lado, como $0 < \dfrac{1}{2^n}$ para todo $n \in \mathbb{N}$, vemos que 0 é cota inferior de Y. Resta apenas provar que nenhum número racional $c > 0$ é cota inferior de Y. Com efeito, sendo $\mathbb{Q}$ arquimediano, dado

$c > 0$, podemos obter $n \in \mathbb{N}$ tal que $n > \frac{1}{c} - 1$. Isto significa $1 + n > \frac{1}{c} \cdot$ Ora, pela desigualdade de Bernoulli (Exemplo 8), temos $2^n = (1+1)^n \geq 1 + n > \frac{1}{c}$, ou seja, $\frac{1}{2^n} < c$. Logo nenhum $c > 0$ é cota inferior de Y e, portanto, $\inf Y = 0$.

A insuficiência mais grave dos números racionais, para efeitos da Análise Matemática, é o fato de que alguns conjuntos limitados de números racionais não possuem supremo (ou ínfimo). Este fato está ligado à inexistência de raízes quadradas racionais de certos números inteiros, mas é uma dificuldade que vai muito além dessa falta.

Pitágoras e seus discípulos descobriram o seguinte

Lema. *Não existe um número racional cujo quadrado seja igual a* 2.

Demonstração. Suponhamos, por absurdo, que se tenha $\left(\frac{p}{q}\right)^2 = 2$, ou seja $p^2 = 2q^2$, com p e q inteiros. O fator 2 aparece um número par de vezes na decomposição de p^2 e de q^2 em fatores primos. Logo p^2 contém um número par de fatores iguais a 2 enquanto $2q^2$ contém um número ímpar desses fatores. Assim sendo, não se pode ter $p^2 = 2q^2$.

Exemplo 13. Sejam $X = \{x \in \mathbb{Q}; x \geq 0 \text{ e } x^2 < 2\}$ e $Y = \{y \in \mathbb{Q}; y > 0 \text{ e } y^2 > 2\}$. Como $x > 2 \Rightarrow x^2 > 4 \Rightarrow x \notin X$, concluímos que $X \subset [0, 2]$, logo X é um conjunto limitado de números racionais. Por outro lado, $Y \subset (0, +\infty)$, de modo que Y é limitado inferiormente. Mostraremos agora que não existem $\sup X$ nem $\inf Y$ em $\mathbb{Q}$. (É claro que existe $\inf X = 0$, pois 0 é o menor elemento de X.) Para isto, estabeleceremos os seguintes fatos:

A) *O conjunto* X *não possui elemento máximo.* Com efeito, dado $x \in X$ (isto é, dado um número racional não-negativo cujo quadrado é inferior a 2), tomamos um número racional $r < 1$ tal que $0 < r < (2-x^2)/(2x+1)$. Afirmamos que $x+r$ ainda pertence a X. Com efeito, de $r < 1$ segue-se $r^2 < r$. Da outra desigualdade que r satisfaz segue-se $r(2x+1) < 2 - x^2$. Por conseguinte, $(x+r)^2 = x^2 + 2rx + r^2 < x^2 + 2rx + r = x^2 + r(2x+1) < x^2 + 2 - x^2 = 2$. Assim, dado qualquer $x \in X$, existe um número maior, $x + r \in X$.

B) *O conjunto* Y *não possui elemento mínimo.* De fato, dado qualquer $y \in Y$, temos $y > 0$ e $y^2 > 2$. Logo podemos obter um número racional r tal que $0 < r < \dfrac{y^2-2}{2y}\cdot$ Então $2ry < y^2 - 2$ e daí $(y-r)^2 = y^2 - 2ry + r^2 > y^2 - 2ry > 2$. Note-se também que $r < \dfrac{y}{2} - \dfrac{1}{y}$, donde $r < y$, isto é, $y - r$ é positivo. Assim, dado $y \in Y$ arbitrário, podemos obter $y - r \in Y$, $\;y - r < y$.

C) *Se* $x \in X$ *e* $y \in Y$*, então* $x < y$. Com efeito, tem-se $x^2 < 2 < y^2$ e, portanto, $x^2 < y^2$. Como x e y são ambos positivos, conclui-se que $x < y$. (A rigor, poderia ser $x = 0$, mas, neste caso, a conclusão $x < y$ é óbvia.)

Usando os fatos **A**, **B** e **C** mostremos que, entre os números racionais, não existem $\sup X$ nem $\inf Y$.

Suponhamos, primeiro, que existisse $a = \sup X$. Seria forçosamente $a > 0$. Não poderia ser $a^2 < 2$ porque isto obrigaria $a \in X$ e, então, a seria o elemento máximo de X, que não existe, por **A**. Tampouco poderia ser $a^2 > 2$, porque isto faria $a \in Y$. Como, em virtude de **B**, Y não possui elemento mínimo, existiria $b \in Y$, com $b < a$. Usando **C**, concluiríamos que $x < b < a$ para todo $x \in X$, o que contradiz ser $a = \sup X$.

Assim, se existir $a = \sup X$, deverá ser $a^2 = 2$. Mas, pelo Lema de Pitágoras, nenhum número racional existe com esta propriedade. Concluímos que em $\mathbb{Q}$ o conjunto X não possui supremo.

Um raciocínio inteiramente análogo, baseado nos fatos **A**, **B** e **C**, mostraria que o número $b = \inf Y$, se existir, deve satisfazer $b^2 = 2$, e, portanto, Y não possui ínfimo em $\mathbb{Q}$.

Ao mesmo tempo, estes argumentos mostram que, se existir um corpo ordenado no qual todo conjunto não-vazio, limitado superiormente, possua supremo, existirá, nesse dito corpo, um elemento $a > 0$ cujo quadrado é 2. Com efeito, tal corpo, sendo ordenado contém $\mathbb{Q}$, logo contém o conjunto X e nele existirá $a = \sup X$, cujo quadrado, não podendo ser menor nem maior do que 2, deverá ser igual a 2. Escreve-se $a = \sqrt{2}$.

Exemplo 14. Vejamos agora outro exemplo de um conjunto limitado superiormente num corpo ordenado K, o qual não possui supremo em K. Para isso, tomemos um corpo não-arquimediano K. O conjunto $\mathbb{N} \subset K$ é limitado superiormente. Se $b \in K$ é uma cota superior de $\mathbb{N}$ então $n + 1 \leq b$ para todo $n \in \mathbb{N}$. Segue-se que $n \leq b - 1$ qualquer que seja $n \in \mathbb{N}$. Em outras palavras, se $b \in K$ for uma cota superior de $\mathbb{N}$, $b - 1$ também o será. Como $b - 1 < b$, segue-se que, num corpo não-arquimediano K, o conjunto $\mathbb{N}$ dos números naturais é limitado superiormente mas não existe $\sup \mathbb{N}$ em K.

Um corpo ordenado K chama-se *completo* quando todo subconjunto não-vazio, limitado superiormente, $X \subset K$, possui supremo em K.

Resulta da definição que, num corpo ordenado completo, todo conjunto não-vazio, limitado inferiormente, $Y \subset K$, possui um ínfimo. Com efeito, dado Y, seja $X = -Y$, isto é, $X = \{-y; y \in Y\}$. Então X é não-vazio e limitado superiormente; logo existe $a = \sup X$. Como se vê facilmente, tem-se $-a = \inf Y$.

Segue-se do Exemplo 14 acima que *todo corpo ordenado completo é arquimediano.*

Adotaremos, a partir de agora, o axioma fundamental da Análise Matemática.

Axioma. *Existe um corpo ordenado completo, $\mathbb{R}$, chamado o corpo dos números reais.*

Passaremos a examinar agora algumas propriedades dos números reais que resultam imediatamente da definição de $\mathbb{R}$ como um corpo ordenado completo.

Voltamos a enfatizar que, em todo o restante deste livro, as únicas propriedades dos números reais que usaremos são aquelas que decorrem de ser $\mathbb{R}$ um corpo ordenado completo. Isto inclui, evidentemente, as proposições demonstradas no início deste capítulo sobre corpos e corpos ordenados em geral.

Como foi observado no fim do Exemplo 13, existe em $\mathbb{R}$ um número positivo a tal que $a^2 = 2$. Este número é representado pelo símbolo $\sqrt{2}$. É claro que só existe um número positivo cujo quadrado é 2, pois $a^2 = b^2 = 2 \Rightarrow 0 = a^2 - b^2 = (a-b)(a+b) \Rightarrow a + b = 0$ ou $a - b = 0$. No primeiro caso, $a = -b$ (logo não podem ser a e b ambos positivos) e no segundo $a = b$. Pelo Lema de Pitágoras, $\sqrt{2}$ não é um número racional.

Aos elementos do conjunto $\mathbb{R} - \mathbb{Q}$, isto é, aos números reais que não são racionais, chamaremos *números irracionais*. Assim, $\sqrt{2}$ é um número irracional. Veremos outros logo mais.

Provaremos agora que, dados $a > 0$ em $\mathbb{R}$ e $n \in \mathbb{N}$ quaisquer, existe um único número real $b > 0$ tal que $b^n = a$. O número b chama-se a *raiz* n-*ésima* de a e é representado pelo símbolo $b = \sqrt[n]{a}$. A demonstração imita o argumento usado no Exemplo 13. Vejamo-la.

Consideramos o conjunto $X = \{x \in \mathbb{R}; x \geq 0, x^n < a\}$. O conjunto X é não-vazio (pois $0 \in X$) e é limitado superiormente. (Se $a < 1$, então, 1 é uma cota superior de X. Se $a > 1$, então $a^n > a$ e daí a é uma cota superior de X.)

Seja $b = \sup X$. Afirmamos que $b^n = a$. Isto se baseia nos seguintes fatos:

A) *O conjunto* X *não possui elemento máximo.* Dado $x \in X$ qualquer, provaremos que é possível tomar $d > 0$ tão pequeno que ainda se tenha $(x + d)^n < a$, isto é $x + d \in X$. Para isto, usaremos um fato auxiliar, que demonstraremos por indução. Trata-se do seguinte: dado $x > 0$ existe, para cada n, um número real positivo A_n (dependendo de x) tal que $(x+d)^n \leq x^n + A_n \cdot d$, seja qual for d com $0 < d < 1$. Isto é claro para $n = 1$. Supondo verdadeiro para n, temos $(x+d)^{n+1} = (x+d)^n(x+d) \leq (x^n + A_n \cdot d)(x + d) = x^{n+1} + A_n \cdot d \cdot x + d \cdot x^n + A_n \cdot d^2 = x^{n+1} + (A_n \cdot x + x^n + A_n \cdot d) \cdot d < x^{n+1} + (A_n \cdot x + x^n + A_n) \cdot d$

(já que $0 < d < 1$). Tomando $A_{n+1} = A_n \cdot x + x^n + A_n$, obtemos $(x+d)^{n+1} < x^{n+1} + A_{n+1} \cdot d$.

Agora, se $x \in X$, isto é, $x \geq 0$ e $x^n < a$, tomamos d tal que $d < 1$ e $0 < d < \dfrac{a - x^n}{A_n} \cdot$ Teremos $x^n + A_n \cdot d < a$ e, por conseguinte, $(x+d)^n < a$, o que prova que X não possui elemento máximo.

B) *O conjunto* $Y = \{y \in \mathbb{R}; y > 0, y^n > a\}$ *não possui elemento mínimo.* Seja $y \in Y$. Escolheremos d, com $0 < d < y$, tal que $(y-d)^n > a$, isto é, $y - d \in Y$. Para tal observemos que, sendo $0 < d < y$, temos $(y-d)^n = y^n\big(1 - \dfrac{d}{y}\big)^n > y^n\big(1 - n \cdot \dfrac{d}{y}\big) = y^n - ny^{n-1} \cdot d$, como resulta da desigualdade de Bernoulli (Exemplo 8), com $x = -\dfrac{d}{y} \cdot$ Se tomarmos $0 < d < \dfrac{y^n - a}{n \cdot y^{n-1}}$ obteremos então $y^n - ny^{n-1}\, d > a$ e, portanto, $(y-d)^n > a$. Isto mostra que Y não possui elemento mínimo.

C) *Se* $x \in X$ *e* $y \in Y$ *então* $x < y$. De fato, nestas condições $x^n < a < y^n$ e, como x e y são positivos, vem $x < y$. (O caso $x = 0$ dá $x < y$ obviamente.)

Deduz-se de **A**, **B** e **C** que o número $b = \sup X$ satisfaz à condição $b^n = a$. Com efeito, se fosse $b^n < a$ então b pertenceria ao conjunto X do qual é supremo, logo b seria o elemento máximo de X, o que contradiz **A**. Também não pode ser $b^n > a$ porque então $b \in Y$ e como, por **B**, Y não possui elemento mínimo, haveria um $c \in Y$ com $c < b$. Por **C**, viria $x < c < b$ para todo $x \in X$: c seria uma cota superior de X menor do que $b = \sup X$, outra contradição. Logo, deve ser $b^n = a$.

De agora em diante, todos os intervalos que considerarmos se referirão ao conjunto $\mathbb{R}$ dos números reais.

Pelo que acabamos de ver, dado $n \in \mathbb{N}$, a função $f\colon [0, +\infty) \to [0, +\infty)$, definida por $f(x) = x^n$, é sobrejetiva. É claro que $0 < x < y$ implica $0 < x^n < y^n$ (pela monotonicidade da multiplicação). Logo f é injetiva e portanto é uma bijeção de $[0, +\infty)$ sobre si mesmo. Sua função inversa é dada por $y \mapsto \sqrt[n]{y}$, a raiz n-ésima (positiva única) de $y > 0$.

O Lema de Pitágoras mostra que o número real $\sqrt{2}$ não é racional. Generalizando este fato, provaremos agora que, dado um $n \in \mathbb{N}$, se um número natural m não possui uma raiz n-ésima natural também não possuirá uma raiz n-ésima racional. Com efeito, seja $\left(\frac{p}{q}\right)^n = m$. Podemos supor p e q primos entre si. Então p^n e q^n também serão primos entre si. Mas temos $p^n = q^n \cdot m$, o que implica ser q^n um divisor de p^n. Absurdo, a menos que fosse $q = 1$. Em suma, dados $m, n \in \mathbb{N}$, se $\sqrt[n]{m} \notin \mathbb{N}$ então $\sqrt[n]{m} \in \mathbb{R} - \mathbb{Q}$.

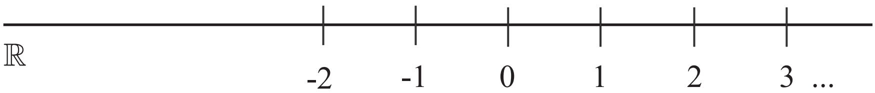
Os números reais que não são racionais, isto é, os elementos do conjunto $\mathbb{R} - \mathbb{Q}$, são chamados *números irracionais*. Acabamos de ver que eles existem: $\sqrt{2}$, $\sqrt{5}$, $\sqrt[3]{6}$, etc. são números irracionais. Mas há muitos outros, obtidos de modos bem mais complicados do que simplesmente extrair raízes não-inteiras de números inteiros ou mesmo resolver equações algébricas com coeficientes inteiros. (Vide Exercícios 44, 45 e 46.)

Mostraremos agora que os números irracionais se acham espalhados por toda parte entre os números reais. Em seguida, provaremos que há mais números irracionais do que racionais. Para explicar precisamente o que significa "espalhados por toda parte", começaremos com uma definição.

Um conjunto $X \subset \mathbb{R}$ chama-se *denso em* $\mathbb{R}$ quando todo intervalo aberto (a, b) contém algum ponto de X.

Em outras palavras, diremos que o conjunto X de números reais é denso em $\mathbb{R}$ quando, dados arbitrariamente $a < b$ em $\mathbb{R}$, for possível encontrar $x \in X$ tal que $a < x < b$.

Por exemplo, seja $X = \complement\mathbb{Z}$ o conjunto dos números reais que não são inteiros. X é denso em $\mathbb{R}$. Com efeito, todo intervalo (a, b) é um conjunto infinito, enquanto existe no máximo um número finito de inteiros n tais que $a < n < b$. Logo qualquer intervalo (a, b) contém elementos de X (isto é, números reais não-inteiros).



É recomendável pensar nos números reais como pontos de uma reta, sendo a distância de x a y dada por $|x-y|$ e significando a relação $x < y$ que x está à esquerda de y. Neste caso, os números inteiros acham-se a uma distância inteira ≥ 1 uns dos outros. A imagem geométrica deixa evidente que $\complement\mathbb{Z}$ é denso em $\mathbb{R}$, embora não deva intervir na demonstração deste fato.

Teorema 4. *O conjunto $\mathbb{Q}$ dos números racionais e o conjunto $\mathbb{R}-\mathbb{Q}$ dos números irracionais são ambos densos em $\mathbb{R}$.*

Demonstração. Seja (a, b) um intervalo aberto qualquer em $\mathbb{R}$. Devemos mostrar que existem um número racional e um número irracional em (a, b). Como $b-a > 0$, existe um número natural p tal que $0 < \frac{1}{p} < b-a$. Os números da forma $\frac{m}{p}$, $m \in \mathbb{Z}$, decompõem a reta $\mathbb{R}$ em intervalos de comprimento $\frac{1}{p}\cdot$ Como $\frac{1}{p}$ é menor do que o comprimento $b-a$ do intervalo (a, b), algum dos números $\frac{m}{p}$ deve cair dentro de (a, b). Esta é a idéia intuitiva da demonstração. Raciocinemos agora logicamente. Seja $A = \left\{m \in \mathbb{Z}; \frac{m}{p} \geq b\right\}$. Como $\mathbb{R}$ é arquimediano, A é um conjunto não-vazio de números inteiros, limitado inferiormente por $b \cdot p$. Seja $m_0 \in A$ o menor elemento de A. Então $b \leq \frac{m_0}{p}$ mas, como $m_0 - 1 < m_0$, tem-se $\frac{m_0-1}{p} < b$. Afirmamos que $a < \frac{m_0-1}{p} < b$. Com efeito, se não fosse assim, teríamos $\frac{m_0-1}{p} \leq a < b \leq \frac{m_0}{p}$. Isto acarretaria $b-a \leq \frac{m_0}{p} - \frac{m_0-1}{p} = \frac{1}{p}$, uma contradição. Logo, o número racional $\frac{m_0-1}{p}$ pertence ao intervalo (a, b). Para obter um número irracional no intervalo (a, b), tomamos $p \in \mathbb{N}$ tal que $\frac{1}{p} < \frac{b-a}{\sqrt{2}}$, ou seja $\frac{\sqrt{2}}{p} < b - a$. Os números da forma $\frac{m\sqrt{2}}{p}$, onde $m \in \mathbb{Z}$, são (salvo $m = 0$) irracionais e dividem a reta $\mathbb{R}$ em intervalos de comprimento $\frac{\sqrt{2}}{p}\cdot$ Como $\frac{\sqrt{2}}{p}$ é menor do que o comprimento $b - a$ do intervalo (a, b), conclui-se que algum $\frac{m\sqrt{2}}{p}$ deve pertencer a (a, b). A demonstração formal se faz como no caso anterior: se m_0 for o menor inteiro tal que $b \le \frac{m_0\sqrt{2}}{p}$ então o número irracional $\frac{(m_0-1)\sqrt{2}}{p}$ pertence ao intervalo (a, b).

O teorema abaixo, às vezes chamado "Princípio dos Intervalos Encaixados", é usado por alguns autores na definição dos números reais.

Teorema 5. *Seja* $I_1 \supset I_2 \supset \cdots \supset I_n \supset \ldots$ *uma seqüência decrescente de intervalos limitados e fechados* $I_n = [a_n, b_n]$. *A interseção* $\bigcap_{n=1}^{\infty} I_n$ *não é vazia. Isto é, existe pelo menos um número real* x *tal que* $x \in I_n$ *para todo* $n \in \mathbb{N}$. *Mais precisamente, temos* $\cap I_n = [a, b]$, *onde* $a = \sup a_n$ *e* $b = \inf b_n$.

Demonstração. Para $n \in \mathbb{N}$, temos $I_{n+1} \subset I_n$, o que significa $a_n \le a_{n+1} \le b_{n+1} \le b_n$. Podemos então escrever:

$$a_1 \le a_2 \le \cdots \le a_n \le \cdots \le b_n \le \cdots \le b_2 \le b_1 .$$

Chamemos de A o conjunto dos a_n e B o conjunto dos b_n. A é limitado: a_1 é uma cota inferior e cada b_n é uma cota superior de A. Por motivo semelhante, B é também limitado. Sejam $a = \sup A$ e $b = \inf B$. Como cada b_n é cota superior de A, temos $a \le b_n$ para cada n. Assim, a é cota inferior de B e, portanto, $a \leq b$. Podemos então escrever:

$$a_1 \leq a_2 \leq \cdots \leq a_n \leq \cdots \leq a \leq b \leq \cdots \leq b_n \leq \cdots \leq b_2 \leq b_1\,.$$

Concluímos que a e b (podendo ser $a = b$!) pertencem a todos os I_n, donde $[a, b] \subset I_n$ para cada n. Logo $[a, b] \subset \bigcap_{n=1}^{\infty} I_n$. Mais ainda, nenhum $x < a$ pode pertencer a todos os intervalos I_n. Com efeito, sendo $x < a = \sup A$, existe algum $a_n \in A$ tal que $x < a_n$, ou seja, $x \notin I_n$. Do mesmo modo, $y > b \Rightarrow y > b_m$ para algum m, donde $y \notin I_m$. Concluímos então que $\cap I_n = [a, b]$.

Usaremos o Teorema 5 para provar que o conjunto dos números reais não é enumerável.

Teorema 6. *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração. Dados um intervalo limitado, fechado $I = [a, b]$, com $a < b$, e um número real x_0, existe um intervalo fechado, limitado, $J = [c, d]$, com $c < d$, tal que $x_0 \notin J$ e $J \subset I$. Isto pode ser verificado facilmente. Usaremos este fato repetidamente para mostrar que, dado qualquer subconjunto enumerável $X = \{x_1, x_2, \ldots, x_n, \ldots\} \subset \mathbb{R}$, podemos encontrar um número real $x \notin X$. Com efeito, sejam I_1 um intervalo limitado fechado e não-degenerado, tal que $x_1 \notin I_1$, I_2 um intervalo do mesmo tipo com $x_2 \notin I_2$ e $I_2 \subset I_1$ e assim indutivamente: supondo obtidos $I_1 \supset I_2 \supset \cdots \supset I_n$ limitados fechados e não-degenerados, com $x_i \notin I_i$ $(1 \leq i \leq n)$, podemos obter $I_{n+1} \subset I_n$ com $x_{n+1} \notin I_{n+1}$. Isto nos fornece uma seqüência decrescente $I_1 \supset \cdots \supset I_n \supset \ldots$ de intervalos limitados e fechados. Pelo Teorema 5, existe um número real x que pertence a todos os I_n. Como $x_n \notin I_n$, segue-se que x não é nenhum dos x_n, e portanto nenhum conjunto enumerável X pode conter todos os números reais.

Corolário 1. *Todo intervalo não-degenerado de números reais é não-enumerável.*

Com efeito, como $f\colon (0,1) \to (a,b)$, definida por $f(x) = (b-a)x + a$, é uma bijeção do intervalo aberto $(0,1)$ no intervalo aberto arbitrário (a,b), se provarmos que $(0,1)$ não é enumerável, resultará que nenhum intervalo não-degenerado pode ser enumerável. Ora, se $(0,1)$ fosse enumerável, $(0,1]$ também seria e, conseqüentemente, para cada $n \in \mathbb{Z}$, o intervalo $(n, n+1]$ seria enumerável (pois $x \mapsto x+n$ é uma bijeção de $(0,1]$ sobre $(n,n+1]$). Mas $\mathbb{R} = \bigcup\limits_{n\in\mathbb{Z}} (n, n+1]$ seria enumerável, por ser uma reunião enumerável dos conjuntos $(n, n+1]$.

Corolário 2. *O conjunto dos números irracionais não é enumerável.*

Com efeito, temos $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$. Sabemos que $\mathbb{Q}$ é enumerável. Se $\mathbb{R} - \mathbb{Q}$ também o fosse, $\mathbb{R}$ seria enumerável, como reunião de dois conjuntos enumeráveis.

Exercícios

1. Dados a, b, c, d num corpo K, sendo b e d diferentes de zero, prove:

   1º) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad+bc}{bd}$;

   2º) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$.

2. Dado $a \neq 0$ num corpo K, põe-se, por definição, $a^0 = 1$ e, se $n \in \mathbb{N}$, $a^{-n} = \dfrac{1}{a^n}$ ou seja, $a^{-n} = (a^n)^{-1}$. Prove:

   1º) $a^m \cdot a^n = a^{m+n}$;

   2º) $(a^m)^n = a^{mn}$ sejam quais forem $m, n \in \mathbb{Z}$.

3. Se $\dfrac{x_1}{y_1} = \dfrac{x_2}{y_2} = \cdots = \dfrac{x_n}{y_n}$ num corpo K, prove que, dados $a_1, \ldots, a_n \in K$ tais que $a_1y_1 + \cdots + a_ny_n \neq 0$, tem-se $\dfrac{a_1x_1 + \cdots + a_nx_n}{a_1y_1 + \cdots + a_ny_n} = \dfrac{x_1}{y_1}$.

4. Sejam K, L corpos. Uma função $f\colon K \to L$ chama-se um *homomorfismo* quando se tem $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$, quaisquer que sejam $x, y \in K$.

   i) Dado um homomorfismo $f\colon K \to L$, prove que $f(0) = 0$.

   ii) Prove também que, ou $f(x) = 0$ para todo $x \in K$, ou então $f(1) = 1$ e f é injetivo.

5. Seja $f\colon \mathbb{Q} \to \mathbb{Q}$ um homomorfismo. Prove que, ou $f(x) = 0$ para todo $x \in \mathbb{Q}$ ou então $f(x) = x$ para todo $x \in \mathbb{Q}$.

6. Verifique as associatividades da adição e da multiplicação em $\mathbb{Z}_2$. (*Nota.* Há dois modos de se proceder. Um requer a verificação de 16 igualdades. Outro consiste em observar que, definindo-se $f\colon \mathbb{Z} \to \mathbb{Z}_2$ por $f(n) = 0$ se n é par, e $f(n) = 1$ se n é ímpar, f é sobrejetiva e, para $m, n \in \mathbb{Z}$ quaisquer, valem $f(m+n) = f(m) + f(n)$, $f(m \cdot n) = f(m) \cdot f(n)$. As associatividades em $\mathbb{Z}$ implicam nas de $\mathbb{Z}_2$.)

7. Seja p um número natural primo. Para cada inteiro m, indiquemos com $\overline{m}$ o resto da divisão de m por p. No conjunto $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ definamos duas operações: uma adição $\oplus$ e uma multiplicação $\odot$, pondo $m \oplus n = \overline{m+n}$ e $m \odot n = \overline{m \cdot n}$. Prove que a função $f\colon \mathbb{Z} \to \mathbb{Z}_p$, definida por $f(n) = \overline{n}$, cumpre $f(m+n) = f(m) \oplus f(n)$ e $f(m \cdot n) = f(m) \odot f(n)$. Conclua que $\oplus$ e $\odot$ são comutativas, associativas, vale a distributividade, existem 0 e 1. Observe que dados $m, n \in \mathbb{Z}_p$, $m \odot n = 0 \Rightarrow m = 0$ ou $n = 0$. Conclua que $\mathbb{Z}_p$ é um corpo.

8. Seja K um conjunto onde são válidos todos os axiomas de corpo, salvo a existência de inverso multiplicativo.

   i) Dado $a \neq 0$ em K, prove que a função $f\colon K \to K$, definida por $f(x) = ax$, é uma bijeção se, e somente se, a possui inverso.

ii) Mostre que f é injetiva se, e somente se, vale a lei do corte para a.

iii) Conclua que, se K é finito, a lei do corte é equivalente à existência de inverso para cada elemento não-nulo de K.

9. Explique por que as operações usuais não tornam corpos o conjunto $\mathbb{Z}$ dos inteiros nem o conjunto $\mathbb{Q}[t]$ dos polinômios de coeficientes racionais.

10. Num corpo ordenado K, prove que $a^2+b^2=0 \Leftrightarrow a=b=0$.

11. Seja P o conjunto dos elementos positivos de um corpo ordenado K.

    i) Dado um número natural n, prove que a função $f\colon P \to P$, definida por $f(x) = x^n$, é monótona crescente (isto é, $x < y \Rightarrow f(x) < f(y)$).

    ii) Dê um exemplo em que f não é sobrejetiva.

    iii) Prove que $f(P)$ não é um subconjunto limitado superiormente de K.

12. Sejam X um conjunto qualquer e K um corpo. Indiquemos com $\mathcal{F}(X;K)$ o conjunto de todas as funções $f\colon X \to K$. Definamos em $\mathcal{F}(X;K)$ as operações de adição e de multiplicação de modo natural: dadas $f, g\colon X \to K$, as funções $f+g\colon X \to K$ e $f \cdot g\colon X \to K$ são dadas por $(f+g)(x) = f(x)+g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$. Verifique quais dos axiomas de corpo são válidos e quais não são válidos no conjunto $\mathcal{F}(X;K)$, relativamente a estas operações.

13. Sejam x, y elementos positivos de um corpo ordenado K. Tem-se $x < y \Leftrightarrow x^{-1} > y^{-1}$. Prove também que $x > 0 \Leftrightarrow x^{-1} > 0$.

14. Seja a um elemento positivo de um corpo ordenado K. Definamos $f\colon \mathbb{Z} \to K$ pondo $f(n) = a^n$. (Veja o Exercício 2.) Prove que f é crescente se $a > 1$, decrescente se $a < 1$ e constante se $a = 1$.

15. Dados $x \neq 0$ num corpo ordenado K e $n \in \mathbb{N}$ qualquer, prove que $(1 + x)^{2n} > 1 + 2n \cdot x$.

16. Se $n \in \mathbb{N}$ e $x < 1$ num corpo ordenado K, prove que $(1 - x)^n \geq 1 - nx$.

17. Num corpo ordenado, se a e $a + x$ são positivos, prove que $(a + x)^n \geq a^n + n \cdot a^{n-1} \cdot x$. Enuncie e demonstre desigualdades análogas às dos Exercícios 15 e 16, com a em vez de 1.

18. Sejam a, b, c, d elementos de um corpo ordenado K, onde b e d são positivos. Prove que $\dfrac{a + c}{b + d}$ está compreendido entre o menor e o maior dos elementos $\dfrac{a}{b}$ e $\dfrac{c}{d}\cdot$ Generalize: mostre que $\dfrac{a_1 + \cdots + a_n}{b_1 + \cdots + b_n}$ está compreendido entre o menor e o maior dos elementos $\dfrac{a_1}{b_1}, \cdots, \dfrac{a_n}{b_n}$, desde que $b_1, \ldots, b_n$ sejam todos positivos.

19. Dados x, y num corpo ordenado K, com $y \neq 0$, prove que $|x \cdot y^{-1}| = |x| \cdot |y|^{-1}$, ou seja $|\dfrac{x}{y}| = \dfrac{|x|}{|y|}\cdot$

20. Prove por indução que, dados $x_1, \ldots, x_n$ num corpo ordenado K, tem-se $|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|$ e $|x_1 \cdot x_2 \cdots x_n| = |x_1| \cdot |x_2| \ldots |x_n|$.

21. Seja K um corpo ordenado. Exprima cada um dos conjuntos abaixo como reunião de intervalos:

    a) o conjunto dos $x \in K$ tais que $|x - 3| + |x + 3| < 8$;

    b) idem $|x^2 - 2| \leq 1$;

c) $|2x+1| \leq 1$;

d) $|x-5| < |x+1|$;

e) $(2x+3)^6(x-2) \geq 0$.

22. Prove que, para todo x num corpo ordenado K, tem-se

$$|x-1| + |x-2| \geq 1.$$
$$|x-1| + |x-2| + |x-3| \geq 2.$$

23. Dados a, b, ε num corpo ordenado K, prove que

$$|a-b| < \varepsilon \Rightarrow |b| - \varepsilon < |a| < |b| + \varepsilon.$$

Conclua que $|a-b| < \varepsilon \Rightarrow a < |b| + \varepsilon$.

24. Prove que, num corpo ordenado K, as seguintes afirmações são equivalentes:

(i) K é arquimediano;

(ii) $\mathbb{Z}$ é ilimitado superior e inferiormente;

(iii) $\mathbb{Q}$ é ilimitado superior e inferiormente.

25. Prove que um corpo ordenado K é arquimediano se, e somente se, para todo $\varepsilon > 0$ em K, existe $n \in \mathbb{N}$ tal que $\dfrac{1}{2^n} < \varepsilon$.

26. Seja $a > 1$ num corpo arquimediano K. Considere a função $f\colon \mathbb{Z} \to K$, definida por $f(n) = a^n$. Prove as seguintes afirmações:

(i) $f(\mathbb{Z})$ não é limitado superiormente;

(ii) $\inf f(\mathbb{Z}) = 0$.

27. Sejam a racional diferente de zero, e x irracional. Prove que ax e $a+x$ são irracionais. Dê exemplo de dois números irracionais x, y tais que $x+y$ e $x \cdot y$ são racionais.

28. Sejam a, b, c e d números racionais. Prove que $a + b\sqrt{2} = c + d\sqrt{2} \Leftrightarrow a = c$ e $b = d$.

29. Prove que o conjunto K dos números reais da forma $a+b\sqrt{2}$, com a e b racionais, é um corpo relativamente às operações de adição e multiplicação de números reais. Examine se o mesmo ocorre com os números da forma $a+b\sqrt[3]{2}$, com $a, b \in \mathbb{Q}$.

30. Sejam a, b números racionais positivos. Prove que $\sqrt{a} + \sqrt{b}$ é racional se, e somente se, $\sqrt{a}$ e $\sqrt{b}$ forem ambos racionais. (*Sugestão*: multiplique por $\sqrt{a} - \sqrt{b}$.)

31. Sejam $X \subset \mathbb{R}$ não-vazio, limitado superiormente, e c um número real. Tem-se $c \leq \sup X$ se, e somente se, para cada $\varepsilon > 0$ real dado pode-se achar $x \in X$ tal que $c - \varepsilon < x$. Enuncie e demonstre um resultado análogo com inf em vez de sup.

32. Seja $X = \left\{\dfrac{1}{n}; n \in \mathbb{N}\right\}$. Prove que $\inf X = 0$.

33. Sejam $A \subset B$ conjuntos não-vazios limitados de números reais. Prove que $\inf B \leq \inf A \leq \sup A \leq \sup B$.

34. Sejam A, B conjuntos não-vazios de números reais, tais que $x \in A, \quad y \in B \Rightarrow x \leq y$. Prove que $\sup A \leq \inf B$. Prove que $\sup A = \inf B$ se, e somente se, para todo $\varepsilon > 0$ dado, podem-se obter $x \in A$ e $y \in B$ tais que $y - x < \varepsilon$.

35. Dado $A \subset \mathbb{R}$ não-vazio, limitado inferiormente, seja $-A = \{-x; x \in A\}$. Prove que $-A$ é limitado superiormente e que $\sup(-A) = -\inf A$.

36. Seja $A \subset \mathbb{R}$ não-vazio, limitado. Dado $c > 0$, seja $c \cdot A = \{c \cdot x; x \in A\}$. Prove que $c \cdot A$ é limitado e que $\sup(c \cdot A) = c \cdot \sup A, \quad \inf(c \cdot A) = c \cdot \inf A$. Enuncie e demonstre o que ocorre quando $c < 0$.

37. Dados $A, B \subset \mathbb{R}$ não-vazios e limitados, seja $A + B = \{x + y; x \in A, y \in B\}$. Prove:

i) $A + B$ é limitado;

ii) $\sup(A + B) = \sup A + \sup B$;

iii) $\inf(A + B) = \inf A + \inf B$;

iv) Enuncie e demonstre resultados análogos supondo apenas A e B limitados superiormente (ou A e B limitados inferiormente).

38. Seja $X \subset \mathbb{R}$. Uma função $f\colon X \to \mathbb{R}$ chama-se *limitada* quando sua imagem $f(X) \subset \mathbb{R}$ é um conjunto limitado. Neste caso define-se o $\sup f$ como o supremo do conjunto $f(X)$. (Às vezes se escreve $\sup\limits_{x \in X} f(x)$ ou $\sup\limits_{X} f$)

i) Prove que a soma de duas funções limitadas $f, g\colon X \to \mathbb{R}$ é uma função limitada $f + g\colon X \to \mathbb{R}$.

ii) Mostre que $(f + g)(X) \subset f(X) + g(X)$, na notação do Exercício 37.

iii) Conclua que $\sup(f+g) \leq \sup f + \sup g$ e que $\inf(f+g) \geq \inf f + \inf g$.

iv) Considerando as funções $f, g\colon [-1, +1] \to \mathbb{R}$, definidas por $f(x) = x$ e $g(x) = -x$, mostre que se pode ter $\sup(f + g) < \sup f + \sup g$ e $\inf(f + g) > \inf f + \inf g$.

39. Sejam A, B conjuntos de números reais positivos. Definamos $A \cdot B = \{x \cdot y; x \in A \text{ e } y \in B\}$. Prove que se A e B forem limitados então $A \cdot B$ é limitado, sendo $\sup(A \cdot B) = \sup A \cdot \sup B$ e $\inf(A \cdot B) = \inf A \cdot \inf B$.

40. i) Prove que o produto de duas funções limitadas $f, g\colon X \to \mathbb{R}$ é uma função limitada $f \cdot g\colon X \to \mathbb{R}$.

ii) Mostre que $(f \cdot g)(X) \subset f(X) \cdot g(X)$.

iii) Conclua que, se f e g forem ambas positivas, tem-se $\sup(f \cdot g) \leq \sup f \cdot \sup g$ e $\inf(f \cdot g) \geq \inf f \cdot \inf g$.

iv) Dê exemplo em que valham as desigualdades estritas.

v) Mostre porém que para toda f positiva tem-se $\sup(f^2) = [\sup f]^2$.

41. Analise os Exercícios 39 e 40 sem as hipóteses de positividade neles feitas.

42. Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio com coeficientes inteiros.

    i) Se um número racional $\dfrac{p}{q}$ (com p e q primos entre si) é tal que $f\left(\dfrac{p}{q}\right) = 0$, prove que p divide a_0 e q divide a_n.

    ii) Conclua que, quando $a_n = 1$, as raízes reais de f são inteiras ou irracionais. Em particular, examinando $x^n - a = 0$, conclua que, se um número inteiro $a > 0$ não possui n-ésima raiz inteira, então $\sqrt[n]{a}$ é irracional.

    iii) Use o resultado geral para provar que $\sqrt{2} + \sqrt[3]{2}$ é irracional.

43. Dado um número natural $p > 1$, prove que os números racionais da forma $\dfrac{m}{p^n}$, onde $m \in \mathbb{Z}$ e $n \in \mathbb{N}$ constituem um subconjunto denso em $\mathbb{R}$.

44. Um número real r chama-se *algébrico* quando existe um polinômio $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, não identicamente nulo, com coeficientes inteiros, tal que $f(r) = 0$.

    i) Prove que o conjunto dos polinômios de coeficientes inteiros é enumerável.

    ii) Dada uma enumeração $\{f_1, f_2, \ldots, f_n, \ldots\}$ desses polinômios não identicamente nulos, seja, para cada $n \in \mathbb{N}$, A_n o conjunto das raízes reais de f_n. Cada A_n é um conjunto finito (podendo ser vazio). O conjunto A dos números algébricos reais escreve-se $A = \bigcup_{n \in \mathbb{N}} A_n$. Conclua que A é enumerável. Mostre que A é denso em $\mathbb{R}$.

45. Seja X o complementar de um conjunto enumerável de números reais. Mostre que, para cada intervalo aberto (a, b), a interseção $(a, b) \cap X$ é não-enumerável. Em particular, X é denso.

46. Um número real chama-se *transcendente* quando não é algébrico. Prove que o conjunto dos números transcendentes é não-enumerável e denso em $\mathbb{R}$.

47. Prove que o conjunto dos números algébricos é um corpo. (Este exercício requer conhecimentos de Álgebra muito acima do que estamos admitindo até aqui.)

48. Dê exemplo de uma seqüência decrescente de intervalos fechados (ilimitados) cuja interseção seja vazia e de uma seqüência decrescente de intervalos (abertos) limitados cuja interseção seja vazia.

49. Sejam $B \subset A$ conjuntos não-vazios de números reais. Suponha que A seja limitado superiormente e que, para cada $x \in A$, exista um $y \in B$ tal que $x \leq y$. Prove que, nestas condições, tem-se $\sup B = \sup A$. Enuncie e demonstre um resultado análogo para inf.

50. Um *corte de Dedekind* é um par ordenado (A, B) onde A e B são subconjuntos não-vazios de números racionais, tais que A não possui elemento máximo, $A \cup B = \mathbb{Q}$ e, dados $x \in A$ e $y \in B$ quaisquer, tem-se $x < y$.

    a) Prove que, num corte de Dedekind (A, B), vale $\sup A = \inf B$.

    b) Seja $\mathcal{D}$ o conjunto dos cortes de Dedekind. Prove que existe uma bijeção $f\colon \mathcal{D} \to \mathbb{R}$.

51. Sejam X, Y conjuntos não-vazios e $f\colon X \times Y \to \mathbb{R}$ uma função limitada. Para cada $x_0 \in X$ e cada $y_0 \in Y$, ponhamos $s_1(x_0) = \sup\{f(x_0, y); y \in Y\}$ e $s_2(y_0) = \sup\{f(x, y_0);$

$x \in X\}$. Isto define funções $s_1 \colon X \to \mathbb{R}$ e $s_2 \colon Y \to \mathbb{R}$. Prove que se tem $\sup\limits_{x \in X} s_1(x) = \sup\limits_{y \in Y} s_2(y)$. Em outras palavras

$$\sup_x [\sup_y f(x, y)] = \sup_y [\sup_x f(x, y)].$$

52. Enuncie e demonstre um resultado análogo ao anterior com inf em vez de sup. Considere, em seguida, o caso "misto" e prove que

$$\sup_y [\inf_x f(x, y)] \leq \inf_x [\sup_y f(x, y)].$$

Dê um exemplo onde se tem $<$ na desigualdade acima.

53. Sejam x, y números reais positivos. Prove que se tem

$$\sqrt{xy} \leq \frac{x + y}{2} \cdot$$

54. A desigualdade entre a média aritmética e a média geométrica, vista no exercício anterior, vale para n números reais positivos $x_1, \ldots, x_n$. Sejam $G = \sqrt[n]{x_1 x_2 \ldots x_n}$ e $A = \dfrac{x_1 + \cdots + x_n}{n} \cdot$ Tem-se $G \leq A$. Isto é evidente quando $x_1 = \cdots = x_n$. Para provar a desigualdade no caso geral, considere a operação que consiste em substituir o menor dos números dados, digamos x_i e o maior deles, digamos x_j respectivamente por $x_i' = \dfrac{x_i \cdot x_j}{G}$ e $x_j' = G$. Isto não altera a média geométrica e, quanto à aritmética, ela não aumenta, pois, como é fácil de se ver, $x_i' + x_j' \leq x_i + x_j$. Prove que, repetida esta operação no máximo n vezes, obtemos n números todos iguais a G e, portanto, sua média aritmética é G. Como em cada operação a média aritmética não aumentou, conclua que $G \leq A$, ou seja $\sqrt[n]{x_1 x_2 \ldots x_n} \leq \dfrac{x_1 + \cdots + x_n}{n} \cdot$

55. Seja K um corpo ordenado completo. Indique com $0'$ e $1'$ o zero e a unidade de K. Para cada $n \in \mathbb{N}$, sejam $n' = n \cdot 1' + \cdots + 1'$ (n vezes) e $(-n)' = -n'$. Definamos uma função $f\colon \mathbb{R} \to K$ pondo $f\left(\dfrac{p}{q}\right) = \dfrac{p'}{q'}$ para todo $\dfrac{p}{q} \in \mathbb{Q}$ e, para x irracional, seja $f(x) = \sup\left\{\dfrac{p'}{q'} \in K; \dfrac{p}{q} < x\right\}$. Prove que f é um homomorfismo sobrejetivo e conclua que f é uma bijeção, ou seja um isomorfismo de $\mathbb{R}$ sobre K.

56. Seja $f\colon \mathbb{R} \to \mathbb{R}$ um isomorfismo de $\mathbb{R}$ em si mesmo. Prove que $f =$ identidade. Conclua que se K e L são corpos ordenados completos, existe um único isomorfismo de K sobre L.

57. Verifique que $f\colon \mathbb{R} \to (-1, 1)$, definida por $f(x) = \dfrac{x}{\sqrt{1+x^2}}$, é uma bijeção de $\mathbb{R}$ sobre o intervalo $(-1, 1)$.

58. Um conjunto G de números reais chama-se um *grupo aditivo* quando $0 \in G$ e $x, y \in G \Rightarrow x - y \in G$. Então, $x \in G \Rightarrow -x \in G$ e $x, y \in G \Rightarrow x + y \in G$. Seja então $G \subset \mathbb{R}$ um grupo aditivo de números reais. Indiquemos com G^+ o conjunto dos números reais positivos pertencentes a G. Excetuando o caso trivial $G = \{0\}$, G^+ é não-vazio. Suponhamos pois $G \neq \{0\}$. Prove que:

i) Se $\inf G^+ = 0$, então G é denso em $\mathbb{R}$;

ii) Se $\inf G^+ = a > 0$, então $a \in G^+$ e $G = \{0, \pm a, \pm 2a, \ldots\}$.

[*Sugestão*: para provar (ii) note primeiro que se fosse $a \notin G^+$ existiriam $g, h \in G^+$ com $a < h < g < a + \dfrac{a}{2}$, donde $\dfrac{a}{2} > g - h \in G^+$, uma contradição. Em seguida, observe que todo $g \in G$ se escreve sob a forma $g = a \cdot q + r$, com $q \in \mathbb{Z}$, sendo $0 \leq r < a$. Veja que $r = g - a \cdot q \in G$, pois q é inteiro.]

iii) Conclua que, se $\alpha \in \mathbb{R}$ é irracional, os números reais da forma $m+n\alpha$, com $m, n \in \mathbb{Z}$, constituem um subconjunto *denso* em $\mathbb{R}$.

59. Sejam $f, g\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ e $\varphi, \psi\colon \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as funções definidas por $f(x, y)=3x-y$, $g(x, y)=(x-1)^2+(y+1)^2-9$, $\varphi(x, y, z) = 3z$, $\psi(x, y, z) = x^2 + y^2 - z$. Interpretando (x, y) como as coordenadas cartesianas de um ponto do plano $\mathbb{R}^2$ e (x, y, z) como coordenadas de um ponto do espaço $\mathbb{R}^3$, descreva geometricamente os conjuntos $f^{-1}(0)$, $g^{-1}(0)$, $\varphi^{-1}(0)$ e $\psi^{-1}(0)$.

60. Seja a um número real positivo. Dado um número racional p/q (onde $p \in \mathbb{Z}$ e $q \in \mathbb{N}$), defina a potência de base a e expoente racional p/q como $a^{p/q} = \sqrt[q]{a^p}$. Prove:

    1º) Para quaisquer $r, s \in \mathbb{Q}$ tem-se $a^r \cdot a^s = a^{r+s}$ e $(a^r)^s = a^{r \cdot s}$;

    2º) Para todo $r \in \mathbb{Q}^+$, a função $f\colon (0, +\infty) \to (0, +\infty)$, dada por $f(x) = x^r$, é uma bijeção crescente;

    3º) A função $g\colon \mathbb{Q} \to \mathbb{R}$ definida por $g(r) = a^r$, (onde a é um número real positivo fixado) é crescente se $a > 1$, e decrescente se $0 < a < 1$.