A Construção dos Números Reais e suas Extensões

IVAN AGUILAR

&

MARINA SEQUEIROS DIAS

Universidade Federal Fluminense

4º Colóquio da Região Centro-Oeste

Novembro de 2015

Sumário

Capítulo 1

Introdução

1.1 Noções básicas sobre conjuntos

A atual Matemática, como é conhecida em pleno século XXI, tem praticamente todos os seus conceitos formalizados na linguagem dos *conjuntos*. A noção intuitiva de conjunto é tão antiga quanto a noção de número. Mesmo sendo uma noção antiga, foi apenas no século XIX que foi amplamente estudada e usada na formalização de diversos conceitos matemáticos por Cantor, Frege, Russell, etc. Existe a chamada *Teoria de Conjuntos* que trata seu estudo de modo rigoroso. Para os nossos propósitos será suficiente uma abordagem *ingênua* de conjuntos, no estilo de Halmos [13].

1.1.1 Conjuntos

O noção primitiva de *conjunto* é um conceito indefinido. Intuitivamente podemos dizer que um conjunto é uma *coleção* de objetos. Note que ao dizer que é uma coleção, precisaríamos definir o que é uma coleção, e assim sucessivamente iríamos utilizando apenas sinônimos, sem tê-la definido concretamente. Mesmo assim, intuitivamente, conseguimos conceber a ideia de um conjunto. Outro conceito primitivo, são os objetos que formam um conjunto, esses objetos são chamados *elementos* do conjunto.

Os conjuntos, costumam ser indicados por letras maiúsculas: A, B, C, etc. Os elementos, em geral, são indicados por letras minúsculas: a, b, c, etc.

O principal conceito primitivo entre um elemento x e um conjunto A é o de *pertinência*.

Se x *pertence a* A (ou x é um elemento de A, ou x está contido em A), denotamos

$$x \in A.$$

Caso contrário, dizemos que x *não pertence a* A, o que denotamos por $x \notin A$.

Um conjunto A é *bem definido* se sempre é possível determinar se um elemento qualquer x, pertence ou não pertence a A.

Existem varias formas de representar ou descrever um conjunto.

Por exemplo, para representar o conjunto formada pelas vogais a, e, i, o, u escrevemos

$$A = \{a, e, i, o, u\}.$$

O conjunto B dos ímpares positivos

$$B = \{1, 3, 5, 7, \ldots\}.$$

Nem sempre é possível descrever um conjunto A colocando um a um cada elemento. Se conhecermos alguma propriedade P comum aos elementos de A. Podemos definir A como o conjunto dos elementos x tal que goza (ou tem) a propriedade P. Denota-se

$$A = \{x \text{ tal que } x \text{ tem a propriedade } P\}$$

Usualmente a frase "*tal que*" é substituída pelos símbolos "|", "/", ":" ou ";". Se a frase "*x tem a propriedade P*" é substituída por $P(x)$ então, A pode ser escrito como

$$\{x \mid P(x)\} \quad \text{ou} \quad \{x \,/\, P(x)\} \quad \text{ou} \quad \{x : P(x)\} \quad \text{ou} \quad \{x;\, P(x)\}.$$

Quando a propriedade P refere-se a um conjunto U, então o conjunto A escreve-se

$$\{x \in U \mid P(x)\} \quad \text{ou} \quad \{x \in U \,/\, P(x)\} \quad \text{ou} \quad \{x \in U : P(x)\} \quad \text{ou} \quad \{x \in U;\, P(x)\}$$

e lê-se A é o conjunto dos x pertencentes a U tais que têm a propriedade P.

Exemplo 1.1 (Conjunto vazio e conjunto unitário)**.** O *conjunto vazio* é o conjunto sem elementos e é representado pelo símbolo $\emptyset$ ou $\{\ \}$. Um conjunto que possua apenas um único elemento x e denotado por $\{x\}$ é chamado *conjunto unitário*. Exemplos de conjuntos unitários são $\{\{\ \}\}$ ou $\{\emptyset\}$.

Sejam A e B conjuntos. Diz-se que A é *subconjunto* de B, se todo elemento de A, também é um elemento de B. Também costuma-se dizer: A está *incluído* em B; A está *contido* em B; A é *parte* de B; B *inclui* A ou B é *contém* A. Escrevemos tal situação como

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

Dizemos que A *não é subconjunto* de B, quando existe $x \in A$ tal que $x \notin B$. Tal situação denota-se $A \not\subset B$.

Proposição 1.1. *Para todo conjunto A, $\emptyset \subset A$.*

Demonstração. Se existisse A tal que $\emptyset \not\subset A$, deveria existir $x \in \emptyset$ tal que $x \notin A$. O que é absurdo. □

Um conjunto A é *igual* a B, se, e somente se, $A \subset B$ e $B \subset A$. Esse fato é denotado por $A = B$.

Se não é verdade que $A = B$, dizemos que A *não é igual* a B e denota-se: $A \neq B$. Isto é, quando $A \not\subset$ ou $B \not\subset A$. Um conjunto que não é igual a $\emptyset$ é chamado *não-vazio*.

Se $A \subset B$ e $A \neq B$ dizemos que A é *subconjunto próprio* de B. Às vezes, tal situação denota-se por $A \subsetneq B$.

Definição 1.1. Dado um conjunto A, o *conjunto potência* de A é o conjunto de todos os subconjuntos de A. Denota-se: $\mathcal{P}(A)$ ou 2^A. Em particular, sempre temos $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.

1.1.2 Conjuntos numéricos

Os exemplos mais importantes de conjuntos são aqueles formados por números. Historicamente, esses conjuntos surgiram por razões práticas ou de necessidade. Tais conjuntos podem ser definidos axiomaticamente. Isto é, como conjuntos gozando de certas propriedades (axiomas). Uma outra abordagem é construí-los a partir de algum outro com estrutura "mais simples". Os exemplos de conjuntos numéricos que seguem, são bem conhecidos e poderão ser utilizados em diversos exemplos ao longo do texto, mesmo, antes de tê-las construído formalmente.

Conjunto dos Números Naturais. $\mathbb{N} = \{1,\ 2,\ 3,\ 4,\ 5, \ldots\}$

Aparecem como uma abstração do processo de contagem (número cardinal) ou ordenamento (número ordinal). Diversos autores preferem incluir o zero entre os naturais. Isso dependerá do gosto do autor, praticidade ou circunstância. Em nosso estudo, o zero não será considerado natural. Aparecendo apenas ao construirmos $\mathbb{Z}$. Para uma opinião a respeito, recomendamos a leitura de [21].

Conjunto dos Números Inteiros. $\mathbb{Z} = \{\ldots -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5, \ldots\}$

Constituído pelos naturais; os simétricos dos naturais (negativos) e o zero. O símbolo $\mathbb{Z}$ vem do alemão *Zahlen*, que significa: número. Esse conjunto faz que tenham sentido equações do tipo $x + 2 = 1$, que não têm solução no conjunto dos naturais.

Conjunto dos Números Racionais. $\mathbb{Q} = \{a/b\ ;\quad a \in \mathbb{Z}, b \in \mathbb{Z},\ b \neq 0\}$

Constituído, além dos inteiros, por números que representam partes ou *frações*. O conjunto dos racionais faz que equações do tipo $2x = 1$ possuam solução. Tais equações no ão têm soluções em $\mathbb{Z}$. O símbolo $\mathbb{Q}$ provém da palavra *quociente*.

Conjunto dos Números Reais $\mathbb{R} = \{a\ ;\ a = \lim_{n\to\infty} x_n,\ \text{onde } x_n \in \mathbb{Q}\}$

$\mathbb{R}$ é formado pelos limites de todas as sequências convergentes de números racionais. O conjunto dos números reais faz que equações do tipo $x^2 = 2$ tenham solução. Tais equações não possuem solução em $\mathbb{Q}$. O conjunto dos reais serve para representar a ideia do contínuo (*continuum*), por exemplo podem representar comprimentos de segmentos de reta. Um números real que não é racional é chamado irracional. O conjunto dos irracionais é denotado por $\mathbb{R} - \mathbb{Q}$. Assim, $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$.

Conjunto dos Números Complexos $\mathbb{C} = \{a + ib\ ;\quad a, b \in \mathbb{R},\ i^2 = -1\}$

Os complexos fazem que equações do tipo $x^2 + 1 = 0$ tenham solução.

Temos as seguintes inclusões próprias: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

1.1.3 Operações entre conjuntos

Definição 1.2. A *reunião* ou *união* dos conjuntos A e B é o conjunto $A \cup B$ formado pelos elementos de A junto aos elementos de B. Desse modo, podemos escrever

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

Definição 1.3. A *interseção* dos conjuntos A e B é conjunto $A \cap B$ formado pelos elementos em comum de A e B. Desse modo, podemos escrever

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

Proposição 1.2 (Propriedades da reunião e interseção de conjuntos)**.** *Sejam A, B, C, D conjuntos*

$\cup 1)$ $A \cup \emptyset = A$,

$\cup 2)$ $A \cup A = A$,

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

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

$\cup 5)$ $A \cup B = A \Leftrightarrow B \subset A$,

$\cup 6)$ $A \subset B, C \subset D \Rightarrow A \cup C \subset B \cup D$

$\cup 7)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$\cap 1)$ $A \cap \emptyset = A$,

$\cap 2)$ $A \cap A = A$,

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

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

$\cap 5)$ $A \cap B = A \Leftrightarrow A \subset B$,

$\cap 6)$ $A \subset B, C \subset D \Rightarrow A \cap C \subset B \cap D$

$\cap 7)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Demonstração. Exercício. □

Definição 1.4 (Diferença de conjuntos)**.** A *diferença* entre os conjuntos A e B é o conjunto $A - B$ formado pelos elementos de A que não estão em B. Ou seja,

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

Outra notação para a diferença é $A \setminus B$. Dizemos que A e B são *disjuntos* quando $A \cap B = \emptyset$.

Se existe um conjunto U que contém todos os conjuntos $A \subset U$ com os quais trabalhamos, então a diferença $U - A$ é chamada o *complemento de A* ou *complementar de A* e escreve-se

$$A^c = U - A$$

Desse modo, para $x \in U$,

$$x \in A^c \Leftrightarrow x \notin A,$$

Também, é imediato verificar que para todo $A, B \subset U$,

$$A - B = A \cap B^c$$

Proposição 1.3 (Propriedades do complementar de um conjunto)**.** *Se $A, B \subset U$ então*

(C1) $(A^c)^c = A$,

(C2) $A \subset B \Leftrightarrow B^c \subset A^c$,

(C3) $A = \emptyset \Leftrightarrow A^c = U$,

(C4) $(A \cup B)^c \Leftrightarrow (A^c \cap B^c)$,

(C5) $(A \cap B)^c \Leftrightarrow A^c \cup B^c)$.

Demonstração. Exercício. □

As propriedades (C3) e (C4) são conhecidas como *identidades de De Morgan*.

1.1.4 Famílias ou coleções

Quando queremos trabalhar com conjuntos cujos elementos são conjuntos, frequentemente usamos as palavras *família* ou *coleção* como sinônimo de conjunto.

Definição 1.5. Seja $\mathcal{F}$ uma família de conjuntos. Definimos a *reunião de* $\mathcal{F}$, denotado por $\bigcup_{A \in \mathcal{F}} A$, como sendo o conjunto de elementos que pertencem pelo menos a algum conjunto de $\mathcal{F}$. A *interseção de* $\mathcal{F}$, denotado por $\bigcap_{A \in \mathcal{F}} A$ é conjunto de elementos que pertencem a cada um dos conjuntos de $\mathcal{F}$. A família ou coleção $\mathcal{F}$ é dita *disjunta* se a interseção de dois conjuntos quaisquer de $\mathcal{F}$ é vazia.

Quando $\mathcal{F}$ é de forma $\{A_1, A_2, \ldots A_n\}$ ou $\{A_1, A_2, A_3, \ldots\}$ a reunião e interseção de $\mathcal{F}$ escreve-se, respectivamente

$$\bigcup_{i=1}^{n} A_i \quad , \quad \bigcap_{i=1}^{n} A_i \qquad \text{ou} \qquad \bigcup_{i=1}^{\infty} A_i \quad , \quad \bigcap_{i=1}^{\infty} A_i.$$

Também são válidas a identidades de De Morgan. Se os elementos F de $\mathcal{F}$ são tal que $F \subset \mathcal{U}$ então

$$\left[\bigcup_{F \in \mathcal{F}} F\right]^c = \bigcap_{F \in \mathcal{F}} F^c \qquad \text{e} \qquad \left[\bigcap_{F \in \mathcal{F}} F\right]^c = \bigcup_{F \in \mathcal{F}} F^c.$$

1.1.5 Produto cartesiano

Sejam a e b dois elementos, introduzimos um novo objeto (como conceito não definido) que chamamos *par ordenado* e denotamos por

$$(a, b)$$

onde a é o *primeira coordenada* e b é a *segunda coordenada*.

Diremos que dois pares ordenados (a, b) e (c, d) são *iguais* se, e somente se, suas primeiras coordenadas são iguais e suas segundas coordenadas também o são. Isto é

$$(a, b) = (c, d) \;\Leftrightarrow\; a = c \quad \text{e} \quad b = d.$$

Definição 1.6. O *produto cartesiano* dos conjuntos A e B é conjunto $A \times B$ dos pares ordenados tal que a primeira coordenada está em A e a segunda em B. Assim,

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

Definimos, $A \times \emptyset = \emptyset$ e $\emptyset \times A = \emptyset$.

Para o caso $A \times A$ também podemos escrever A^2. O conjunto dos pares $(a, a) \in A^2$ é chamado *diagonal* de A^2.

1.2 Relações de equivalência

Dizemos que um subconjunto R de A^2 define uma relação de equivalência em A se

a) $(a, a) \in R$, para todo $a \in A$,

b) $(a, b) \in R \Rightarrow (b, a) \in R$,

c) $(a, b) \in R$ e $(b, c) \in R \Rightarrow (a, c) \in R$,

Em lugar de tratar as relações de equivalência como subconjuntos do produto cartesiano A^2 as redefinimos como sendo uma relações binárias em A (isto é, como uma relação entre dois elementos de A). Diremos que a está *relacionado* com b se $(a, b) \in R$. Desse modo as propriedades acima são reescritas como segue.

Definição 1.7. A relação binária $\sim$ sobre A, é uma *relação de equivalência* sobre A se

a) $a \sim a, \quad \forall a \in A,$ (reflexividade)

b) $a \sim b \Rightarrow b \sim a,$ (simetria)

c) $a \sim b$ e $b \sim c \Rightarrow a \sim c$ (transitividade)

As relações de equivalência são de extrema importância. Elas permitem classificar ou agrupar elementos de um conjunto A em subconjuntos contendo elementos equivalentes ou relacionados entre eles.

Definição 1.8. Se A é um conjunto e $\sim$ uma relação de equivalência em A, então a *classe de equivalência de* $a \in A$ é o conjunto

$$[a] = \{x \in A;\ x \sim a\}.$$

Outras notações para $[a]$ são: $\overline{a}$, C_a ou A_a.

Exemplo 1.2. No conjunto dos inteiros $\mathbb{Z}$ definimos a relação $\sim$ entre dois elementos $a, b \in \mathbb{Z}$ como

$$a \sim b \quad \Leftrightarrow \quad a - b \text{ é par.}$$

Como $a - a = 0$ é par, temos $a \sim a$. Se $a \sim b$ então $a - b$ é par. Como $-(a - b) = b - a$ é par, logo $b \sim a$. Finalmente, se $a \sim b$ e $b \sim c$, então $a - b$ e $b - c$ são pares. Como $a - c = (a - c) + (c - b)$ é par, obtemos $a \sim c$. Portanto, $\sim$ é uma relação de equivalência.

Note que

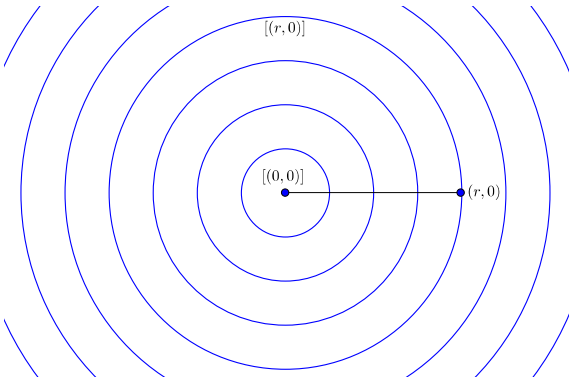
$$[0] = \{\ldots, -4, -2,\ 0,\ 2,\ 4, \ldots\} \qquad \text{e} \qquad [1] = \{\ldots, -5, -3, -1,\ 1,\ 3,\ 5, \ldots\}.$$

Desse modo, em $\mathbb{Z}$ a relação de equivalência $\sim$ determina exatamente duas classes de equivalência: o conjunto dos pares e dos ímpares.

Exemplo 1.3. Seja T o conjunto dos triângulos do plano e $\sim$ a relação de *semelhança* entre triângulos (isto é, triângulos com ângulos correspondentes iguais). Verifica-se que $\sim$ é uma relação de equivalência.

Exemplo 1.4. Seja $\mathbb{R}^2$ o conjunto formado pelos pontos da forma (x, y). Dois pontos são relacionados se eles são equidistantes da origem. É imediato concluir que tal relação é de equivalência. As classes de equivalência são, além da origem, circunferências com centro na origem.

$$[(0,0)] = \{(0,0)\} \qquad \text{e} \qquad [(r,0)] = \{(x,y);\ x^2 + y^2 = r^2\}, \quad (r > 0).$$



Nesses três exemplos, as classes de equivalência decompõem os conjuntos $\mathbb{Z}$, T e $\mathbb{R}^2$ em subconjuntos disjuntos. Essa propriedade é a principal caraterística das relações de equivalência.

Definição 1.9. Uma família $\mathcal{P}$ de subconjuntos de X é uma *partição* de X se

1. $\emptyset \notin \mathcal{P}$
2. $\bigcup_{A \in \mathcal{P}} A = X$
3. Se $A, B \in P$ e $A \neq B$ então $A \cap B = \emptyset$

Exemplo 1.5. Seja $X = \{a, b, c\}$ então

$$\{\{a\}, \{b\}, \{c\}\},\ \{\{a, b\}, \{c\}\} \text{ e } \{X\}$$

são exemplos de partições de X. Por outro lado,

$$\{\{a, b\}, \{b\}, \{c\}\},\ \{\{a\}, \{b\}\} \text{ e } \{X, \emptyset\}$$

não podem ser partições de X.

Exemplo 1.6. Todo conjunto não vazio A admite as partições triviais:

$$P_1 = \{\{a\};\ a \in A\} \ \text{ e } \ P_2 = \{A\}.$$

Proposição 1.4 (Partições e relações de equivalência)**.** *Para cada relação de equivalência $\sim$ em um conjunto X, o conjunto das classes de equivalência é uma partição de X. Reciprocamente, cada partição P de X induz a relação de equivalência $\sim$, tal que $a \sim b$ se, e somente se $a, b \in A$ para algum $A \in P$.*

Demonstração. Exercício. □

Definição 1.10. O conjunto das classes de equivalência de uma relação de equivalência $\sim$ em A é chamado *conjunto quociente* de A respeito a $\sim$ e é denotado por $A/_\sim$.

Exemplo 1.7. No exemplo 1.2, em $\mathbb{Z}$ é definida a relação de equivalência: $a \sim b \Leftrightarrow a - b$ é par. O conjunto quociente é

$$\mathbb{Z}/_\sim = \{[0], [1]\} = \{\{\ldots, -4, -2, 0, 2, 4, \ldots\}, \{\ldots, -3, -1, 1, 3, \ldots\}\}.$$

Exemplo 1.8. No exemplo 1.6, as partições triviais de A

$$P_1 = \{\{a\};\ a \in A\} \quad \text{e} \quad P_2 = \{A\},$$

induzem, respectivamente, as relações R_1 e R_2 dadas por

$$aR_1b \Leftrightarrow a = b \quad \text{e} \quad aR_2b \Leftrightarrow a, b \in A.$$

Portanto, os conjuntos quocientes respectivos, são

$$A/R_1 = \{\{a\};\ a \in A\} \quad \text{e} \quad A/R_2 = \{A\}.$$

1.3 Funções

Definição 1.11 (Função)**.** Dados dois conjuntos A e B, uma *função* $f : A \to B$ de A em B é uma relação que a cada elemento x de A lhe faz corresponder um único elemento $f(x)$ de B. Costuma-se escrever

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

O conjunto A é chamado *domínio* de f, B o *contradomínio* de f e $f(x)$ é o *valor* que f assume em cada $x \in A$. Desse modo, para definir uma função, são necessários: um domínio A, um contradomínio B e uma regra $x \mapsto f(x)$. Quando A e B estão subentendidos, é costume denotar essa função simplesmente por f.

Duas funções $f : A \to B$ e $g : M \to N$ são *iguais*, se e somente se, $A = M$, $B = N$ e $f(x) = g(x)$ para todo $x \in A$. Denotamos por $f = g$.

Definição 1.12 (Imagem e imagem inversa de um conjunto)**.** Seja $X \subset A$, o conjunto

$$f(X) = \{f(x);\ \ x \in A\}$$

é a *imagem de X por f*.

Se $Y \subset B$, o conjunto

$$f^{-1}(Y) = \{x \in A;\ f(x) \in Y\}$$

é a *imagem inversa de Y por f*.

Proposição 1.5 (Propriedades da imagem e imagem inversa)**.** *Seja $f : A \to B$ uma função. Se $X, Y \subset A$ e $V, W \subset B$ então,*

(a) $f(X \cup Y) = f(X) \cup f(Y)$,

(b) $f(X \cap Y) \subset f(X) \cap f(Y)$,

(c) $X \subset Y \Leftrightarrow f(X) \subset f(Y)$,

(d) $f(\emptyset) = \emptyset$,

(e) $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$,

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

(g) $f^{-1}(V^c) = [f^{-1}(V)]^c$,

(h) $f^{-1}(B) = A$,

(i) $f^{-1}(\emptyset) = \emptyset$.

Demonstração. Exercício. Veja o libro de Elon Lima [20]. □

Definição 1.13. Dizemos que uma função $f : A \to B$ é *injetiva* quando dados quaisquer $x, y \in A$, $f(x) = f(y) \Rightarrow x = y$; é *sobrejetiva* quando $f(A) = B$ e é *bijetiva* se for injetiva e sobrejetiva.

Exemplo 1.9. Seja $f : A \to B$, com B contendo mais de um elemento. Fixado um $c_0 \in B$, dado por $f(x) = c_0$. Assim definida, f não é sobrejetiva nem injetiva. Exemplos clássicos de funções injetivas são as *inclusões* $i : A \to B$, $i(x) = x$, para todo $x \in A$, onde $A \subset B$. As *projeções*, $\pi_1 : A \times B \to A$, $\pi_1(x, y) = x$ e $\pi_2 : A \times B \to A$, $\pi_2(x, y) = y$ são os exemplos canônicos de funções sobrejetivas. A função bijetiva mais simples é a função *identidade* $id_A : A \to A$, $id_A(x) = x$, para todo $x \in A$.

Definição 1.14 (Composição de funções)**.** Sejam $f : A \to B$ e $g : C \to D$ duas funções tal que $f(A) \subset C$ então, a *composição* $g \circ f : A \to D$ de f com g é definida por $[g \circ f](x) = g(f(x))$, para todo $x \in A$.

Definição 1.15 (Inversa de uma função)**.** Dizemos que uma função $f : A \to B$ *tem uma inversa* se existe $g : B \to A$ tal que

$$g \circ f = Id_A \quad \text{e} \quad f \circ g = Id_B.$$

Quando existe a inversa de f denotamos ela por $g = f^{-1}$. Nesse caso, temos

$$f^{-1} \circ f = Id_A \quad \text{e} \quad f \circ f^{-1} = Id_B.$$

Se $f : A \to B$ é bijetiva significa que para cada b de B existe um único a de A tal que $f(a) = b$. Ou seja, para cada $b \in B$ existe um único $a \in A$ que denotaremos por $g(b)$. Isso define uma função $g : B \to A$, $b \mapsto a = g(b)$, onde $a = g(b) \Leftrightarrow f(a) = b$. Ou seja, $g \circ f = Id_A$ e $f \circ g = Id_B$. Portanto, mostramos a seguinte proposição:

Proposição 1.6. *Uma função $f : A \to B$ possui inversa se, e somente se, é bijetiva.*

1.4 Corpos

Definição 1.16. Uma *operação binária* $*$ sobre um conjunto A é uma regra que a cada par $(a, b) \in A^2$ faz corresponder um único $a * b \in A$. Ou seja, é uma função $* : A^2 \to A$.

Definição 1.17. Um *corpo* $(K, +, \cdot)$ é um conjunto $K \neq \emptyset$ junto a duas operações binarias: $+$ e $\cdot$, chamadas respectivamente *adição* e *multiplicação*, satisfazendo nove axiomas,

Axiomas da adição

(A1) Para todo $x, y, z \in K$,
$(x + y) + z = x + (y + z)$,

(A2) Para todo $x, y \in K$,
$x + y = y + z$,

(A3) Existe $0 \in K$ tal que
$x + 0 = x, \forall x \in K$,

(A4) Para todo $x \in K$, existe $-x \in K$,
$x + (-x) = 0$.

Axiomas da multiplicação

(M1) Para todo $x, y, z \in K$,
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(M2) Para todo $x, y \in K$,
$x \cdot y = y \cdot z$,

(M3) Existe $1 \in K$, $1 \neq 0$ tal que
$x \cdot 1 = x, \forall x \in K$,

(M4) Para todo $x \neq 0$ em K, existe $x^{-1} \in K$,
$x \cdot x^{-1} = 1$.

Axioma da distributividade

(D1) Para todo $x, y, z \in K$ tem-se $x \cdot (y + z) = x \cdot y + x \cdot z$.

Observações.

- Os axiomas acima costumam ter nomes próprios: (A1) e (M1) *associatividade*; (A2) e (M2) *comutatividade*; em (A3) o *elemento neutro* 0 é chamado *zero*; em (M3) o elemento neutro 1 ou *identidade multiplicativa* é chamada *um*; (A4) e (M4) garantem, respectivamente, a existência do *inverso aditivo* (ou simétrico) e o *inverso multiplicativo*.

- Se $x, y \in K$, então $x + y$ e $x \cdot y$ são chamados, respectivamente, *soma* e *produto* de x e y. Muitas vezes, em lugar de $x \cdot y$, escrevemos simplesmente xy.
- Por (M3) todo corpo possui pelo menos dois elementos distintos, a saber 0 e 1.
- A *diferença* entre x e y é definida e denotada por $x - y := x + (-y)$. A operação $(x, y) \mapsto x - y$ é chamada *substração*.
- O *quociente* entre x e y, onde $y \neq 0$, definimos e denotamos por $x/y := xy^{-1}$. A operação $(x, y) \mapsto x/y$ é chamada *divisão*.
- O uso dos símbolos conhecidos $+$ e $\cdot$, para as duas operações binárias do corpo K, e o fato de chamarmos elas de: adição e multiplicação; é apenas por comodidade. Poderíamos ter usado quaisquer outros símbolos; por exemplo: $\oplus$ e $\odot$. A mesma observação vale para os símbolos conhecidos 0 e 1.

Exemplo 1.10. O conjunto $\mathbb{Z}_2 = \{0, 1\}$ com as operações $+$ e $\cdot$ dadas por

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

é um corpo.

Exemplo 1.11. O conjunto $\mathbb{Q}$ dos racionais com as operações de adição e multiplicação usuais é um corpo.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Exemplo 1.12. O conjunto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$ com as operações

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

é um corpo. Os elementos neutros para cada operação são

$$0 = 0 + 0\sqrt{2} \quad \text{e} \quad 1 = 1 + 0\sqrt{2}.$$

O simétrico de $z = a + b\sqrt{2}$ é $\quad -z = -a + (-b)\sqrt{2}$.
O inverso de $z = a + b\sqrt{2} \neq 0$ é:

$$z^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a - 2b^2}\sqrt{2}.$$

Exemplo 1.13 (Conjunto das funções racionais $\mathbb{Q}(t)$)**.** Seja $\mathbb{Q}[t]$ o conjunto das funções polinomiais com coeficientes racionais. Definimos o conjunto das funções racionais

$$\mathbb{Q}(t) = \left\{ f\,;\ f(t) = \frac{p(t)}{q(t)},\ p, q \in \mathbb{Q}[t],\ q \neq 0 \right\}$$

Com as operações

$$\frac{p(t)}{q(t)} + \frac{r(t)}{s(t)} = \frac{p(t)s(t) + q(t)r(t)}{q(t)s(t)},$$

$$\frac{p(t)}{q(t)} \cdot \frac{r(t)}{s(t)} = \frac{p(t)q(t)}{q(t)s(t)},$$

onde $0 \in \mathbb{Q}$ e $1 \in \mathbb{Q}$ são os elementos neutros; $-f$ é o simétrico de $f \in \mathbb{Q}(t)$, dado por $(-f)(t) = -f(t)$. O inverso multiplicativo f^{-1} de $f \neq 0$ é definido por $(f^{-1})(t) = 1/f(t)$. Desse modo, $\mathbb{Q}(t)$ é um corpo.

Seguem alguns resultados clássicos de corpos

Proposição 1.7. *Seja K um corpo e $x, y, z \in K$*

(a) *Os elementos neutros 0 e 1 são únicos.*

(b) *Os elementos: simétrico e inverso, são únicos. Isto é, para cada $x \in K$, $-x$ é único, e cada $x \neq 0$, x^{-1} é único.*

(c) $x \cdot 0 = 0$, *para todo $x \in K$.*

(d) $x + z = y + z \Rightarrow x = y$ *e*
para $z \neq 0$, $x \cdot z = y \cdot z \Rightarrow x = y$. *(leis de corte)*

(e) $x \cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0$.

(f) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ *e* $(-x) \cdot (-y) = x \cdot y$. *(regras dos sinais)*

Demonstração. Exercício. □

1.5 Corpos ordenados

Definição 1.18. Um *corpo ordenado* é um corpo K, com as operações $+$ e $\cdot$, del tal forma que existe um subconjunto $P \subset K$ com as propriedades seguintes:

P1) $\forall x, y \in P \Rightarrow x + y \in P$ e $x \cdot y \in P$.

P2) $\forall x \in K$ ocorre apenas uma das seguintes alternativas:

$$\text{ou} \quad x \in P \quad \text{ou} \quad x = 0 \quad \text{ou} \quad -x \in P.$$

O conjunto P é chamado o conjunto dos *elementos positivos* de K.

Se $-P = \{-x;\ x \in P\}$, decorre dos axiomas

$$K = -P \cup \{0\} \cup P \qquad \text{(dois a dois disjuntos).}$$

O conjunto $-P$ é chamado o conjunto dos *elementos negativos* de K.

Observações.

- Um corpo ordenado, isto é, um corpo $(K, +\cdot)$ e um conjunto de positivos $P \subset K$ é denotado por: $(K, +, \cdot, P)$. Quando não houver confusão, um corpo ordenado denotaremos simplesmente por K.
- Para todo elemento $a \neq 0$ de um corpo ordenado temos $a^2 \in P$.
- Como $1 = 1^2 \in P$, segue que num corpo ordenado o elemento 1 é sempre positivo. Em particular, como $-1 \in -P$, em corpos ordenados, $\forall a \in K,\ a^2 \neq -1$.

Exemplo 1.14. O corpo $\mathbb{Z}_2$ não é ordenado. Se fosse ordenado, existiria P tal que $1 \in P$ e assim $1 + 1 \in P$. Mas $1 + 1 = 0 \notin P$. Também o conjunto dos números complexos $\mathbb{C}$ não pode ser ordenado, pois existe $i \in \mathbb{C}$ tal que $i^2 = -1$.

Exemplo 1.15. O conjunto dos racionais $\mathbb{Q}$ é um corpo ordenado. O conjunto dos positivos é dado por $P = \{r \in \mathbb{Q};\ r > 0\}$.

Exemplo 1.16. O conjunto das funções racionais $\mathbb{Q}(t)$ é um corpo ordenado. O conjunto dos positivos P é formado pelos elementos $p(t)/q(t) \in \mathbb{Q}(t)$, distintos de 0, tal que os coeficientes dos termos de maior grau de p e q, têm o mesmo sinal. Verifica-se, sem dificuldade, as propriedades (P1) e (P2). Portanto, $\mathbb{Q}(t)$ é um corpo ordenado.

Definição 1.19. Em um corpo ordenado K, definimos as relações

$$\begin{aligned} a < b &\quad\Leftrightarrow\quad b - a \in P, \\ a > b &\quad\Leftrightarrow\quad b < a, \quad (\text{ou } a - b \in P) \\ a \leq b &\quad\Leftrightarrow\quad b < a, \text{ ou } a = b, \\ a \geq b &\quad\Leftrightarrow\quad b > a, \text{ ou } a = b. \end{aligned}$$

Essas relações são lidas,

$$\begin{aligned} a < b &\quad : \quad a \text{ é menor do que } b, \\ a > b &\quad : \quad a \text{ é maior do que } b, \\ a \leq b &\quad : \quad a \text{ é menor ou igual do que } b, \\ a \geq b &\quad : \quad a \text{ é maior ou igual do que } b. \end{aligned}$$

Proposição 1.8. *A relação de ordem $<$ tem as seguintes propriedades:*

(O1) *Transitividade.* $x < y$ e $y < z \ \Rightarrow\ x < z$.

(O2) *Tricotomia.* Se $x, y \in K$, apenas uma das seguinte alternativas ocorre

$$\text{ou} \quad x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y$$

(O3) *Monotonicidade da adição* $\forall z \in K,\ x < y \ \Rightarrow\ x + z < y + z$.

(O4) *Monotonicidade da multiplicação.*

$$\forall z > 0,\ x < y \ \Rightarrow\ xz < yz, \qquad \text{e} \qquad \forall z < 0,\ x < y \ \Rightarrow\ xz > yz.$$

Demonstração. Exercício. □

Fazendo as mudanças adequadas, resultados análogos podem ser enunciados para as outras três relações: $\leq$, $\geq$ e $>$.

1.5.1 Corpos ordenados são infinitos

Uma consequência muito importante da definição de corpo ordenado é que eles são necessariamente infinitos e contêm de modo natural (a menos de isomorfismo) o conjunto dos números naturais $\mathbb{N}$.

Seja K um corpo ordenado e P seu conjunto de números positivos. Sabemos que $1 \in P$. Como $1 - 0 = 1 \in P$, por definição, podemos escrever

$$1 > 0$$

Usando a monotonicidade da adição obtemos

$$0 \ < \ 1 \ < \ 1+1 \ < \ 1+1+1 \ < \ 1+1+1+1 \ < \cdots$$

Note que

$$\mathcal{N} = \{1,\ 1+1,\ 1+1+1,\ 1+1+1+1, \ldots\},$$

e um conjunto infinito (verifique isso!). Como $\mathcal{N} \subset K$, então o corpo ordenado K é necessariamente infinito. Não é difícil ver que a aplicação $\varphi : \mathbb{N} \to \mathcal{N}$ dada por $\varphi(n) = 1 + \cdots + 1$ (n vezes) é uma bijeção. Pode-se provar ainda que as operações de $\mathbb{N}$ são preservadas por φ. Isto é, $\varphi(n+m) = \varphi(n) + \varphi(m)$ e $\varphi(nm) = \varphi(n)\varphi(m)$ (nesse caso, dizemos que φ é um isomorfismo ou homomorfismo bijetivo). Isso mostra que todo corpo ordenado contém o subconjunto $\varphi(\mathbb{N}) = \mathcal{N}$, que é identificado com $\mathbb{N}$.

1.5.2 Intervalos de um corpo K

Em corpo ordenado K, onde $a, b \in K$ e $a < b$, definem-se os seguintes conjuntos chamados *intervalos* (de extremos a e b)

$$\begin{aligned}
[a,b] &= \{x \in K;\ a \le x \le b\} && \text{(intervalo fechado)}\\
[a,b) &= \{x \in K;\ a \le x < b\} && \text{(intervalo fechado à esquerda)}\\
(a,b] &= \{x \in K;\ a < x \le b\} && \text{(intervalo fechado à direita)}\\
(a,b) &= \{x \in K;\ a < x < b\} && \text{(intervalo aberto)}
\end{aligned}$$

Os quatro intervalos, de extremos a e b, são limitados (veja a definição 1.21). Temos mais cinco possibilidades:

$$\begin{aligned}
(-\infty,b] &= \{x \in K;\ x \le b\} && \text{(interv. ilimitado fechado à direita)}\\
(-\infty,b) &= \{x \in K;\ x < b\} && \text{(interv. ilimitado aberto à direita)}\\
[a,+\infty) &= \{x \in K;\ a \le x\} && \text{(interv. ilimitado fechado à esquerda)}\\
(a,+\infty) &= \{x \in K;\ a < x\} && \text{(interv. ilimitado aberto à esquerda)}\\
(-\infty,+\infty) &= K
\end{aligned}$$

Se $a = b$, temos $[a,b) = (a,b] = (a,b) = \emptyset$ e $[a,b] = \{a\}$. Neste último caso, dizemos que $[a,a]$ é um *intervalo degenerado*.

Todo intervalo com extremos $a < b$ (ou ilimitado) é infinito (usando $x < \frac{x+y}{2} < y$).

1.5.3 Valor absoluto

Definição 1.20. Em um corpo ordenado K, definimos o *valor absoluto* de $x \in K$ como

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

Da definição, $|x| = x \geq 0$ ou $|x| = -x > 0$. Portanto, $|x| \geq 0$ para todo $x \in K$.
Note que, $|x| = x$ (se $x \geq 0$) ou $|x| = -x > x$ (se $x < 0$). Ou seja, $|x| = \max\{x, -x\}$.

Proposição 1.9. *Se K é um corpo ordenado e $x, a \in K$.*

$$-a \leq x \leq a \quad \Leftrightarrow \quad |x| \leq a.$$

Demonstração. Exercício. □

Resultado análogo vale para $<$.

Corolário 1.1. *Se $a, x, \varepsilon \in K$*

$$x \in (a-\varepsilon,\ a+\varepsilon) \quad \Leftrightarrow \quad a-\varepsilon < x < a+\varepsilon \quad \Leftrightarrow \quad |x-a| < \varepsilon.$$

Proposição 1.10 (Propriedades do valor absoluto)**.** *Seja K um corpo ordenado. Se $x, y, z \in K$ então*

(i) $|x+y| \leq |x| + |y|$; *(desigualdade triangular)*

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

(iii) $|x| - |y| \leq \big||x| - |y|\big| \leq |x-y|$;

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

Demonstração. Exercício. □

1.6 Supremo e ínfimo de um conjunto

1.6.1 Subconjuntos limitados de um corpo

Definição 1.21. Dizemos que um subconjunto X de um corpo ordenado K é *limitado superiormente* se existe $b \in K$ tal que $x \leq b$ para todo $x \in X$. O elemento $b \in K$ é *cota superior* de X. Analogamente, X é *limitado inferiormente* se existe $a \in K$ tal que $a \leq x$. O elemento a é dito, uma *cota inferior* de X. Diz-se que X é *limitado* se é limitado inferior e superiormente. Cotas superiores ou inferiores não são necessariamente únicas.

Exemplo 1.17. O conjunto dos naturais $\mathbb{N}$ como subconjunto do corpo ordenado $\mathbb{Q}$ é limitado inferiormente e não é limitado superiormente. Qualquer subconjunto finito de um corpo é limitado. Os intervalos com extremos $a, b \in K$ também são limitados.

Exemplo 1.18 ($\mathbb{N}$ como subconjunto $\mathbb{Q}(t)$ é limitado)**.** No exemplo anterior, o subconjunto dos naturais, como subconjunto do corpo dos racionais, não é limitado superiormente. Entretanto, o conjunto dos naturais $\mathbb{N}$ como subconjunto do corpo das funções racionais $\mathbb{Q}(t)$ é limitado. Uma cota inferior é 0 e uma cota superior é t (veja o exemplo 1.23).

1.6.2 Supremo e ínfimo

Definição 1.22 (Supremo)**.** Seja K um corpo ordenado e $X \subset K$ limitado superiormente. Dizemos que um elemento $\beta \in K$ é *supremo* de X (denotado por $\beta = \sup X$) se é a menor das cotas superiores.

Ou seja, β é supremo de X se:

(S1) $x \leq \beta, \forall x \in X$

(S2) Se $\exists c \in K$ tal que $x \leq c, \forall x \in X$, então $\beta \leq c$.

A condição (S2) pode ser reescrita como:
Se $c < \beta$ então c não é cota superior de X. Isto é, se $c < \beta$ então $\exists x \in K$ tal que $c < x$.

Analogamente, definimos

Definição 1.23 (Ínfimo)**.** Seja K um corpo ordenado e $X \subset K$ limitado inferiormente. Dizemos que um elemento $\alpha \in K$ é chamado *ínfimo* de X (denotado por $\alpha = \inf X$) se é a maior das cotas inferiores.

Assim, α é ínfimo de X se

(I1) $\alpha \leq x, \forall x \in X$

(I2) Se $\exists c \in K$ tal que $c \leq x, \forall x \in X$, então $c \leq \alpha$.

A condição (I2) pode ser reescrita como:
Se $\alpha < c$ então c não é cota inferior de X. Isto é, se $\alpha < c$ então $\exists x \in K$ tal que $x < c$.

Exemplo 1.19. Seja $F = \{x_1, x_2, \ldots, x_n\}$ subconjunto de um corpo ordenado K. Neste caso, o ínfimo e supremo de F é, respectivamente, o menor e maior elemento de F,

$$\inf F = \min F \quad \text{e} \quad \sup F = \max F.$$

Em particular, $\inf F \in F$ e $\sup F \in F$.

Exemplo 1.20. Seja $X = \{1/n;\ n \in \mathbb{N}\}$ subconjunto do corpo dos racionais $\mathbb{Q}$, então

$$\inf X = 0 \quad \text{e} \quad \sup F = 1.$$

O elemento 0 é cota inferior de X, pois $0 \leq 1/n$, $\forall n \in \mathbb{N}$. Resta verificar que 0 é a maior das cotas inferiores. Para isto, usamos o fato de $\mathbb{N}$ ser ilimitado superiormente em $\mathbb{Q}$ (veja o exemplo 1.22). Seja $c > 0$, então existe $n \in \mathbb{N}$ tal que $n > 1/c$. Logo, $0 < 1/n < c$. Isto é, existe $1/n \in X$ maior do que c. Assim, $\inf X = 0$. Observe que $\inf X \notin X$. O outro caso, $\sup X = 1$, é de verificação imediata.

Nos exemplos acima o ínfimo e supremo existem, no sentido de o ínfimo e o supremo serem elementos do corpo ordenado. Pode acontecer de eles não existirem.

Exemplo 1.21 (Não existência de supremo)**.** Seja $A = \{x \in \mathbb{Q};\ x > 0 \text{ e } x^2 < 2\}$

A é limitado superiormente. Afirmamos que, $\forall x \in A$, $x \leq 2$. De fato, se existisse algum $y \in A$ tal que $y > 2$ então $y^2 > 4$. Nesse caso, $y \notin A$, o que é absurdo.

Afirmamos que

não existe o supremo de A (em $\mathbb{Q}$).

De fato, suponha que existe $c = \sup A$ em $\mathbb{Q}$. Por tricotomia temos uma das seguintes possibilidades:

$$\text{ou} \quad c^2 < 2 \quad \text{ou} \quad c^2 > 2 \quad \text{ou} \quad c^2 = 2.$$

• Suponha que $c^2 < 2$. Seja $d \in \mathbb{Q}$ o positivo dado por $d = \frac{1}{2}\min\left\{\frac{2-c^2}{2c+1},\ 1\right\}$.
Em particular,

$$d \leq \frac{2-c^2}{2(2c+1)} \ \text{ e } \ d \leq \frac{1}{2}. \quad \text{De onde, } \ d(2c+1) \leq \frac{2-c^2}{2} < 2-c^2 \ \text{ e } \ d^2 \leq \frac{d}{2} < d.$$

Portanto, $d^2 < d$ e $d(2c+1) < 2-c^2$.
Seja $y = c + d$. Mostraremos que $y \in A$. De fato,

$$y^2 = c^2 + 2cd + d^2 < c^2 + 2cd + d = c^2 + d(2c+1) < c^2 + (2-c^2) = 2$$

Assim, existe $y \in A$ tal que $y = c + d > c = \sup A$. Tal contradição nos diz que não existe um supremo $c \in \mathbb{Q}$ de A tal que $c^2 < 2$.

• Suponha que $c^2 > 2$. Seja $d = \frac{c^2-2}{2c}$ um racional positivo. Logo $c^2 - 2cd = 2$
Se $\beta = c - d$, mostraremos que β é uma cota superior de A. De fato,

$$\beta^2 = c^2 - 2cd + d^2 > c^2 - 2cd = 2. \qquad \text{Ou seja, } \ \beta^2 > 2.$$

Afirmamos que $\beta \leq x$, $\forall x \in A$. Caso contrário, existiria $y \in A$ tal que $y > \beta$. Logo $y^2 > \beta^2 > 2$. Ou seja $y \notin A$. O que é absurdo.

Desse modo, β é uma cota superior A, menor do que o supremo de A. Pois, $\beta = c - d < c$. Tal contradição, implica que não pode existir supremo de A, $c \in \mathbb{Q}$, tal que $c^2 > 2$.

• O terceiro caso, $c^2 = 2$, também é impossível. Existe o seguinte resultado conhecido:

não existe $r \in \mathbb{Q}$ tal que $r^2 = 2$ (veja o Lema 5.1).

Concluímos, portanto, que não existe o supremo de A em $\mathbb{Q}$.

1.7 Corpos arquimedianos

Na seguinte definição, $\mathbb{N}$ denota o conjunto clássico dos naturais.

Definição 1.24. Um corpo ordenado K é *arquimediano* se, para todo cada $x \in K$ existe $n \in \mathbb{N}$ tal que

$$x < \overbrace{1+1+\cdots+1}^{n \text{ vezes}}$$

Observação. Como todo corpo ordenado contém um subconjunto isomorfo a $\mathbb{N}$, sem perda de generalidade, denotaremos tal subconjunto de K por $\mathbb{N}$. Assim, teríamos $n = 1+1+\cdots+1$ (n vezes). Com isso, podemos dizer que: *um corpo ordenado K é arquimediano, se, e somente se, o conjunto dos naturais $\mathbb{N} \subset K$ é ilimitado superiormente.*

Proposição 1.11 (Propriedade arquimediana)**.** *As seguintes propriedades num corpo ordenado arquimediano K 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) *para cada* $a > 0$ *de* K, *existe* $n \in \mathbb{N}$ *tal que* $0 < \frac{1}{n} < a$.

Demonstração.

(i)⇒(ii) Sendo $a > 0$, por (i), existe $n \in \mathbb{N}$ tal que $n > b/a$. Ou seja, $n \cdot a > b$.

(ii)⇒(iii) Em (ii) fazemos $b = 1$, obtemos $n \cdot a > 1$, isto é, $\frac{1}{n} < a$. Logo, $0 < \frac{1}{n} < a$.

(iii)⇒(i) Para todo $a \leq 0$ existe $1 \in \mathbb{N}$ tal que $a < 1$. Se $a > 0$ então $\frac{1}{a} > 0$. Por (iii) existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{a}$. Portanto, $n > a$. Isto é, $\mathbb{N}$ é ilimitado superiormente em K.

□

Exemplo 1.22. O conjunto dos números racionais $\mathbb{Q}$ é arquimediano, pois o conjunto dos naturais $\mathbb{N} \subset \mathbb{Q}$ é ilimitado superiormente.

Exemplo 1.23 (conjunto não arquimediano)**.** O corpo ordenado das funções racionais $\mathbb{Q}(t)$ não é arquimediano. Com efeito, o conjunto dos naturais em $\mathbb{Q}(t)$ é limitado superiormente. Para todo $n \in \mathbb{N}$, existe $f \in \mathbb{Q}(t)$ dado por $f(t) = t$ tal que $n < f$. Lembrando que $n < f$ se, e somente se, $f - n \in P$ (veja o exemplo 1.16). Note que o coeficiente de maior grau de $t - n$ é 1.

1.8 Corpo ordenado e completo

No Exemplo 1.21 vimos que o corpo ordenado $\mathbb{Q}$ contém um subconjunto A limitado superiormente, porém, não existe $\sup A$ no corpo $\mathbb{Q}$. Se pretendemos trabalhar com corpos ordenados, de tal forma que todos seus conjuntos limitados superiormente possuam supremo no corpo, precisamos definir um corpo ordenado especial com essa propriedade.

Definição 1.25. Um corpo ordenado K é chamado *corpo ordenado completo*, se todo subconjunto não-vazio de K limitado superiormente possui supremo em K.

Exemplo 1.24. Com essa definição e o Exemplo 1.21, concluímos que o corpo ordenado $\mathbb{Q}$ não é completo.

Proposição 1.12. *Todo corpo ordenado completo e arquimediano.*

Demonstração. Seja K um corpo ordenado completo. Suponha que K não é arquimediano, então o conjunto $\mathbb{N} \subset K$ é limitado superiormente. Afirmamos que $\mathbb{N}$ não possui supremo em K. De fato, suponha que existe $\beta = \sup \mathbb{N}$. Logo, $n+1 \leq \beta$ para todo $n \in \mathbb{N}$ (pois $n+1 \in \mathbb{N}$) o que implica que $n \leq \beta - 1$ para todo $n \in \mathbb{N}$. Isto é, $\beta - 1$ é cota superior de $\mathbb{N}$. Ou seja, existe uma cota superior de $\mathbb{N}$ menor do que o supremo de $\mathbb{N}$, o que é absurdo.

Assim, num corpo não-arquimediano K o conjunto $\mathbb{N} \subset K$, que é limitado superiormente, não possui supremo em K. Portanto, K não é completo. Essa contradição demonstra a proposição. □

Ainda não demos um exemplo concreto de um corpo ordenado e completo. Apenas estamos mostrando algumas consequências ou propriedades que esse tipo de conjunto deveria ter. Normalmente, a existência do conjunto dos números reais $\mathbb{R}$ é aceito como axioma. Em particular, aceita-se que $\mathbb{R}$ tem a propriedade do supremo. Também conhecido como *Axioma do supremo*. Desse modo, a rigor, não podemos afirmar que realmente exista um corpo ordenado completo. Os próximos capítulos, serão dedicados justamente a demonstrar que esse tipo de conjunto, de fato, existe. Será um longo caminho (pois antes devemos passar pelos, naturais, inteiros e racionais). Demonstraremos ainda que (a menos de isomorfismo) esse conjunto (o conjunto dos reais) é único.

1.9 Exercícios

1. Demonstre as propriedades de reunião e interseção da Proposição 1.2.
2. Demonstre as propriedades do complementar da Proposição 1.3.
3. Demonstre a Proposição 1.4 sobre partições e relações de equivalência.
4. Seja R uma relação em um conjunto M, tal que

   (i) Se aRb, então bRa.

   (ii) Se aRb e bRc, então aRc.

   (iii) Para todo $a \in M$, existe $b \in M$ tal que aRb.

   Prove que R é uma relação de equivalência.
5. Demonstre a Proposição 1.5, sobre a imagem e imagem inversa de uma função.
6. Demonstre a Proposição 1.7 sobre propriedades dos corpos.
7. Se $\dfrac{x_1}{y_1} = \dfrac{x_2}{y_2} = \ldots = \dfrac{x_n}{y_n}$ num corpo K, prove que, dados $a_1, \ldots, a_n \in K$ tais que $a_1 y_1 + \ldots a_n y_n \neq 0$, tem-se $\dfrac{a_1 x_1 + \ldots a_n x_n}{a_1 y_1 + \ldots a_n y_n} = \dfrac{x_1}{y_1}$.
8. Sejam K, L corpos. Uma função $f : K \to L$ chama-se um homomorfismo quando se tem $f(x+y) = f(x) + f(y)$ e $f(x.y) = f(x).f(y)$, quaisquer que sejam $x, y \in K$.

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

(b) Prove também que,

$$\text{ou } f(x) = 0 \text{ para todo } x \in K, \quad \text{ou} \quad \text{então } f(1) = 1 \text{ e } f \text{ é injetiva.}$$

9. Num corpo ordenado K, se $a \in K$ e $a \neq 0$, então $a^2 > 0$.

10. Seja K um corpo ordenado com identidade multiplicativa u. Mostre que o conjunto
$$\{u < u+u < u+u+u < u+u+u+u < \cdots\}$$
é infinito e , portanto, K é infinito.

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

12. Todo corpo ordenado contém um subconjunto isomorfo ao conjunto dos naturais.

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

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

15. Demonstre as propriedades de ordem da Proposição 1.8.

16. Demostre as propriedades do valor absoluto da Proposições 1.9 e 1.10.

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

18. Mostre que todo intervalo com extremos $a < b$ (ou ilimitado) é infinito.

Capítulo 2

Os Números Naturais

2.1 O conceito de número

Os algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 são, atualmente, de uso tão amplo e comum, que, conhecê-los e saber usá-los aparenta ser uma aptidão inata dos humanos. Entretanto, historicamente, sabemos que o conceito de *número* é uma abstração da mente humana. Tiveram que passar muitos milênios até os primeiros humanos perceberem que há "*algo comum*" num conjunto de: sete pessoas; de sete dias; de sete árvores; sete meses; etc. No caso, a ideia ou conceito abstrato desse "*algo comum*"é o que representamos pelo símbolo: 7. Nas palavras de Georges Ifrah no seu livro: *Os números* [15], cuja leitura recomendamos,

"...No entanto, o fato é certo: houve um tempo em que o ser humano não sabia contar..."

Houve um tempo em que o número era apenas *sentido*. Ainda existem tribos que só têm dois nomes próprios para números (*um, dois e ... muitos*). Outros para se referir ao três ou quatro, usam algo como: *dois-um* e *dois-dois*. Para um número maior a esses, usam termos como: *muitos*. Para eles, o número não é concebido como algo abstrato, para eles, é sentido e percebido, como se fosse um cheiro, uma cor ou um som. Nos humanos, existe uma aptidão natural que é a *percepção* ou *sensação numérica*, (por exemplo, algo ser menor ou maior) que não pode ser confundida com a *capacidade abstrata de contar*, a qual constitui uma faculdade bem recente da humanidade.

Embora o conjunto dos naturais, $\mathbb{N} = \{1, 2, 3, \ldots\}$, intuitivamente, pareça ser bem simples de concebê-lo, faz-se necessário formalizar sua definição, de tal forma que a partir dele seja possível construir praticamente quase toda a matemática que conhecemos.

Para tal formalização, diversos matemáticos se debruçaram. Destaca-se a realizada pelo italiano Giuseppe Peano em 1889 em *Arithmetices principia, nova methodo exposita* (uma tradução pode ser achada em [24]) e também o trabalho de Dedekind [8].

2.2 Definição axiomática dos Naturais

O conjunto dos números naturais $\mathbb{N}$ e todas suas propriedades podem ser deduzidos a partir de alguns postulados, conhecidos como *Axiomas de Peano*. Para esta seção podem ser consultados os livros de Halmos [13] e E. Lima [19], [20].

2.2.1 Axiomas de Peano

Assumimos o conjunto dos naturais, $\mathbb{N}$, como um objeto não definido, onde seus elementos são chamados *números naturais*, gozando dos seguintes axiomas:

(P1) 1 *é um número natural*

(P2) *Se* n *é um natural, então seu* **sucessor** $s(n)$ *também é um natural.*

(P3) *O natural* 1*, não é sucessor de nenhum outro natural.*

(P4) *Se dois naturais* m *e* n *têm o mesmo sucessor, isto é,* $s(m) = s(n)$*, então* $m = n$*.*

(P5) (Princípio de Indução) *Seja* $X \subset \mathbb{N}$*, tal que*

- $1 \in X$ *e*
- *se* $n \in X$ *então o sucessor* $s(n) \in X$*.*

Então $X = \mathbb{N}$*.*

No trabalho original de Peano de 1889 [24] foram considerados, além dos cinco axiomas, outros quatro sobre a relação de *igualdade*. Três, indicando que a igualdade "=" é uma relação de equivalência ($x = x$; $x = y \Rightarrow y = x$; $x = y$ e $y = z \Rightarrow x = z$). E uma quarta, afirmando que, se $x \in \mathbb{N}$ e $x = y$ então $y \in \mathbb{N}$. Deixar de colocá-los na lista acima não atrapalha em nada na definição de $\mathbb{N}$. Nos livros de Elon Lima [19] e [20] ao invés dos cinco axiomas acima, são apresentados três axiomas, a qual coincide com a proposta de Dedekind [8]. De qualquer forma esses axiomas, seja na forma de Peano ou a de Dedekind, são equivalentes.

Observações. Seguem algumas observações importantes sobre os Axiomas de Peano.

- No momento de definir o conjunto dos naturais pelos axiomas de Peano, fomos logo utilizando a notação $\mathbb{N}$. O que pode nos induzir a pensar que estamos trabalhando com o conjunto $\{1, 2, 3, \ldots\}$ (que costumamos denotar por $\mathbb{N}$) e que os axiomas apenas descrevem $\mathbb{N}$. Não é esse o caso. Neste momento deveríamos esquecer que se trata do conhecido $\{1, 2, 3, \ldots\}$. Devemos ter em conta que apenas estamos tomando *emprestado* o símbolo $\mathbb{N}$ por conveniência.

- O axioma (P1) diz que $\mathbb{N} \neq \emptyset$. Assim, a única certeza que temos sobre $\mathbb{N}$, é que ele deve conter pelo menos um elemento, que denotamos por 1. Poderíamos ter usado qualquer outro símbolo. O resto dos números, deve ser induzido a partir dos axiomas (ou regras do jogo).

- (P2) define uma função $s : \mathbb{N} \to \mathbb{N}$ tal que a cada $n \in \mathbb{N}$ lhe associa $s(n) \in \mathbb{N}$ chamado *sucessor de n*. Observe que nada foi dito sobre como opera a função s.
- O axioma (P4) afirma que s é injetiva. Assim, sabemos que cada elemento tem apenas um
- O axioma (P3) diz que s não é sobrejetiva (note que $s(\mathbb{N}) \neq \mathbb{N}$).
- Os quatro primeiros axiomas implicam que

$$X = \{1,\ s(1),\ s(s(1)),\ s(s(s(1))),\ \ldots\} \subset \mathbb{N}$$

- X é infinito e, portanto, $\mathbb{N}$ também é infinito. (prove isto!)
- Sabemos que X (acima definido) está contido em $\mathbb{N}$. A princípio, o conjunto de naturais $\mathbb{N}$ poderia conter elementos que não estão em X. Mas, o axioma (P5) nos garante que na verdade, $X = \mathbb{N}$. Como isso, agora sabemos, como são os elementos de $\mathbb{N}$. Além do 1, qualquer outro natural é sempre sucessor de algum natural. Veja o Teorema 2.1
- Será que existe algum outro conjunto distinto de $\mathbb{N}$ gozando dos axiomas de Peano? A resposta é: qualquer outro conjunto gozando dos Axiomas de Peano é isomorfo a $\mathbb{N}$. Não demonstraremos isso aqui. Provas disso podem ser achadas na literatura, veja [25]. Portanto, podemos assumir que $\mathbb{N}$ é único.

2.2.2 Princípio de Indução

O *Princípio de Indução* algumas vezes é enunciado como segue,

Suponha que $\mathcal{P}$ é alguma propriedade ou predicado sobre naturais, tal que

- *$\mathcal{P}(1)$ é verdadeiro*
- *se $\mathcal{P}(n)$ ser verdadeiro, implica que $\mathcal{P}(s(n))$ também é verdadeiro.*

Então, $\mathcal{P}(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Qualquer demonstração, usando esse princípio é chamada: *demonstração por indução*. Quando for definida a operação soma em $\mathbb{N}$ o $s(n)$ será trocado por $n + 1$.

Teorema 2.1. *Se $n \in \mathbb{N}$ então, $n = 1$ ou $\exists m \in \mathbb{N}$ tal que $n = s(m)$.*

Demonstração. Seja

$$A = \{n \in \mathbb{N};\quad n = 1 \text{ ou } \exists m \in \mathbb{N},\ n = s(m)\} = \{n \in \mathbb{N};\quad n = 1 \quad \text{ou} \quad n \text{ é um sucessor}\}.$$

Por definição de A, $1 \in A$. Suponha que n é um sucessor, isto é, $n = s(m)$ para algum $n \in \mathbb{N}$. Como $s(n) = s(s(m))$, segue que $s(n)$ é sucessor de $s(m)$. Ou seja, se $n \in A$ então $s(n) \in A$. Pelo princípio de indução, $A = \mathbb{N}$. □

Corolário 2.1. *Se $n \in \mathbb{N}$ e $n \neq 1$ então, existe um único $m \in \mathbb{N}$ tal que $n = s(m)$.*

Demonstração. Se $n \in \mathbb{N}$ e $n \neq 1$, o teorema 2.1 implica que existe $m \in \mathbb{N}$ tal que $n = s(m)$. Para a unicidade de m, suponha que existe $m' \in \mathbb{N}$ tal que $n = s(m')$. Pelo axioma (P4), s é injetiva, portanto, $m = m'$. □

O corolário acima, permite definir o *antecessor* ou *predecessor* de um natural $n \neq 1$ como sendo o único natural m tal que $n = s(m)$.

2.3 Operações de adição e multiplicação em $\mathbb{N}$

Antes de definirmos as operações para $\mathbb{N}$ explicamos o que entendemos por *iteração*.

Dada uma função $f : X \to X$ suponha que a cada $n \in \mathbb{N}$ lhe corresponde uma única função $f^n : X \to X$, tal que

$$f^1 = f \quad \text{e} \quad f^{s(n)} = f \circ f^n.$$

A função f^n é chamada *a n-ésima iterada de f*.

A n-ésima iterada da função $s : \mathbb{N} \to \mathbb{N}$ ficaria

$$s^1 = s \quad \text{e} \quad s^{s(n)} = s \circ s^n. \tag{1}$$

2.3.1 A Adição em $\mathbb{N}$

Definição 2.1 (Adição em $\mathbb{N}$)**.** Seja $s : \mathbb{N} \to \mathbb{N}$ a função dada pelo axiomas de Peano.

Dados $m, n \in \mathbb{N}$, sua *soma* $m + n \in \mathbb{N}$ é definida por

$$m + n := s^n(m)$$

A definição diz que somar m com n é tomar o natural m e iterá-la n vezes. Da definição de soma e (1) temos,

$$m + 1 = s^1(m) = s(m).$$

Essa igualdade nos indica que a notação do sucessor de m, $s(m)$, pode ser substituída pela notação $m + 1$. Ainda da definição 2.1 e (1) temos

$$m + s(n) = s^{s(n)}(m) = (s \circ s^n)(m) = s(s^n(m)) = s(m + n).$$

Desse modo, obtemos duas importantes igualdades que utilizaremos diversas vezes,

$$m + 1 = s(m), \tag{2}$$

$$m + s(n) = s(m + n). \tag{3}$$

O Teorema 2.1 diz que qualquer natural ou é 1 ou é o sucessor $s(n)$ de algum $n \in \mathbb{N}$. Desse modo, as equações (2) e (3), na verdade, são as *regras* de como devemos somar um número m com qualquer outro natural arbitrário. Muitos autores definem a soma de dois naturais pelas equações (2) e (3).

A igualdade (3), usando (2), é equivalente a escrever

$$m + (n + 1) = (m + n) + 1 \tag{4}$$

Essa equação não permitirá demonstrar que a adição é associativa.

Proposição 2.1 (Associatividade)**.** *Para todo* $m, n, p \in \mathbb{N}$,

$$m + (n + p) = (m + n) + p.$$

Demonstração. Seja, $X = \{\ p \in \mathbb{N};\ \forall m, n \in \mathbb{N},\ m + (n + p) = (m + n) + p\ \}$. Demonstramos por indução em p.

- Por (4), $1 \in X$.
- Suponha que $p \in X$, provaremos que $s(p) \in X$.
  Usando a hipótese $m + (n + p) = (m + n) + p$ e (3),

  $$m + (n + s(p)) = m + s(n + p) = s(m + (n + p)) = s((m + n) + p) = (m + n) + s(p).$$

  Assim, $s(p) \in X$. Segue, do princípio de indução, que $X = \mathbb{N}$. Ou seja, $m + (n + p) = (m + n) + p$, para todo $m, n, p \in \mathbb{N}$.

□

Para demonstrar que a adição goza da propriedade da comutatividade mostramos um lema.

Lema 2.1. *Para todo* $m \in \mathbb{N}$, $\quad m + 1 = 1 + m$.

Demonstração. Seja $Y = \{m \in \mathbb{N};\ m + 1 = 1 + m\}$. De $1 + 1 = 1 + 1$, temos $1 \in Y$. Suponha que $m \in Y$. Ou seja, $m + 1 = 1 + m$. Usando (3), $s(m) + 1 = s(m + 1) = s(1 + m) = 1 + s(m)$. Assim, $s(m) \in Y$. Pelo princípio de indução, $Y = \mathbb{N}$. □

Proposição 2.2 (Comutatividade)**.** *Para todo* $m, n \in \mathbb{N}$,

$$m + n = n + m.$$

Demonstração. Seja,

$$X = \{n \in \mathbb{N};\ \forall m \in \mathbb{N},\ m + n = n + m\}.$$

Demonstraremos por indução em n.

- Pelo Lema 2.1, $m + 1 = 1 + m$. Assim, $1 \in X$.
- Suponha que $n \in X$, provaremos que $s(n) \in X$.
  Usando (3), a hipótese de indução $m + n = n + m$, (2), o Lema 2.1 e a associatividade,

  $$\begin{aligned} m + s(n) &= s(m + n) = s(n + m) = n + s(m) \\ &= n + (m + 1) = n + (1 + m) = (n + 1) + m \\ &= s(n) + m. \end{aligned}$$

  Assim, $s(n) \in X$. Segue, do princípio de indução, que $X = \mathbb{N}$.
  Ou seja, $m + n = n + m$, para todo $m, n \in \mathbb{N}$.

□

Proposição 2.3 (Lei do corte da adição)**.** *Para $m, n \in \mathbb{N}$,*

$$m + n = m + p \quad \Longrightarrow \quad n = p.$$

Demonstração. Seja,

$$X = \{m \in \mathbb{N}; \quad m + n = m + p \Rightarrow \ n = p\}$$

para quaisquer $n, p \in \mathbb{N}$. Demonstraremos por indução em m.

- $1 \in X$. De fato, da injetividade de s e comutatividade,

$$1 + n = 1 + p \Rightarrow n + 1 = p + 1 \Rightarrow s(n) = s(p) \Rightarrow n = p.$$

- Suponha que $m \in X$, provaremos que $s(m) \in X$.
  Usando a comutatividade, (3), a injetividade de s e a hipótese de indução,

$$\begin{aligned} s(m) + n = s(m) + p &\Rightarrow n + s(m) = p + s(m) \\ &\Rightarrow s(n + m) = s(p + m) \\ &\Rightarrow n + m = p + m \\ &\Rightarrow m + n = m + p \\ &\Rightarrow n = p. \end{aligned}$$

  O que mostra que $s(m) \in X$.

Pelo princípio de indução, $X = \mathbb{N}$. A proposição está provada. □

Proposição 2.4 (Tricotomia)**.** *Para $m, n \in \mathbb{N}$, apenas uma e somente uma alternativa é valida:*

(i) *ou* $m = n$;

(ii) *ou existe* $p \in \mathbb{N}$ *tal que* $m = n + p$;

(iii) *ou existe* $q \in \mathbb{N}$ *tal que* $n = m + q$

Demonstração. Exercício. □

2.3.2 A multiplicação em $\mathbb{N}$

Intuitivamente, *o produto $m \cdot n$ é somar m vezes o mesmo número n.*

Definição 2.2 (Multiplicação em $\mathbb{N}$)**.** O produto de dois números é definido por

$$m \cdot 1 = m, \tag{5}$$
$$m \cdot s(n) = m \cdot n + m \tag{6}$$

Essas duas equações, são as regras para multiplicar um natural m com qualquer outro natural que, pelo Teorema 2.1, ou é 1 ou é um sucessor $s(n)$ de algum $n \in \mathbb{N}$.

Proposição 2.5 (Distributividade)**.** *Para todo* $m, n, p \in \mathbb{N}$, $\quad m \cdot (n + p) = m \cdot n + m \cdot p$.

Demonstração. Seja $X = \{\ p \in \mathbb{N};\ \forall m, n \in \mathbb{N}, \quad m \cdot (n + p) = m \cdot n + m \cdot p\ \}$.

- $1 \in X$. De fato, de (5) e (6) obtemos $\quad m \cdot (n + 1) = m \cdot n + m \cdot 1$.
- Suponha que $p \in X$. Provaremos que $s(p) \in X$.

  Usando a hipótese de indução $m \cdot (n + p) = m \cdot n + m \cdot p$, a associatividade e comutatividade da adição, e (6), temos

$$\begin{aligned}(m + n) \cdot s(p) &= (m + n) \cdot p + (m + n)\\ &= (m \cdot p + n \cdot p) + (m + n)\\ &= m \cdot p + (n \cdot p + m) + n\\ &= m \cdot p + (m + n \cdot p) + n\\ &= (m \cdot p + m) + (n \cdot p + n)\\ &= m \cdot s(p) + n \cdot s(p).\end{aligned}$$

  Assim, $s(p) \in X$.

Segue do princípio de indução que $X = \mathbb{N}$. O que prova a proposição. □

Proposição 2.6 (Associatividade)**.** *Para todo* $m, n, p \in \mathbb{N}$, $\quad m \cdot (n \cdot p) = (m \cdot n) \cdot p$.

Demonstração. Seja $X = \{\ p \in \mathbb{N};\ \forall m, n \in \mathbb{N}, \quad m \cdot (n \cdot p) = (m \cdot n) \cdot p\ \}$.

- $1 \in X$. De fato, usando (5) temos $\quad m \cdot (n \cdot 1) = m \cdot n = (m \cdot n) \cdot 1$.
- Suponha que $p \in X$. Provaremos que $s(p) \in X$.

  Usando (6), a hipótese de indução $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ e a distributividade,

$$\begin{aligned}m \cdot (n \cdot s(p)) &= m \cdot (n \cdot p + n)\\ &= m \cdot (n \cdot p) + m \cdot n\\ &= (m \cdot n) \cdot p + m \cdot n\\ &= (m \cdot n) \cdot s(p).\end{aligned}$$

  Assim, $s(p) \in X$.

Segue do princípio de indução que $X = \mathbb{N}$. O que prova a proposição. □

Proposição 2.7 (Lei de corte do produto)**.** *Para* $m, n, p \in \mathbb{N}$, $\quad m \cdot p = n \cdot p \Rightarrow m = n$.

Demonstração. Seja $X = \{\ p \in \mathbb{N};\ \forall m, n \in \mathbb{N}, \quad m \cdot p = n \cdot p \Rightarrow m = n\ \}$.

- $1 \in X$. De fato, por (5) temos $\quad m \cdot 1) = n \cdot 1 \Rightarrow m = n$.

- Suponha que $p \in X$. Provaremos que $s(p) \in X$.
  Usando (6), a hipótese de indução $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ e a lei de corte da adição,

$$\begin{aligned} m \cdot s(p) = n \cdot s(p) &\Rightarrow m \cdot p + m = n \cdot + n \\ &\Rightarrow m \cdot p + m = m \cdot p + n \\ &\Rightarrow m = n. \end{aligned}$$

  Assim, $s(p) \in X$.

Pelo princípio de indução, $X = \mathbb{N}$. A proposição está provada. □

2.4 Relação de ordem em $\mathbb{N}$

Definição 2.3. Sejam $m, n \in \mathbb{N}$, dizemos que *m é menor do que n*, o que denotamos por

$$m < n,$$

se, e somente se, existe $p \in \mathbb{N}$ tal que $n = m + p$.

Proposição 2.8 (Propriedades da relação de ordem)**.** *Sejam $m, n, p \in \mathbb{N}$. A relação $<$ tem as seguintes propriedades*

(1) *Transitividade.* $m < n$ *e* $n < p \Rightarrow m < p$.

(2) *Tricotomia. Dados $m, n \in \mathbb{N}$, uma e apenas uma das seguintes alternativas é valida*

$$ou \;\; m = n \;\; ou \;\; m < n \; ou \;\; n < m.$$

(3) *Monotonicidade da adição. $m < n \Rightarrow m + p < n + p$, para todo $p \in \mathbb{N}$.*

(4) *Monotonicidade da multiplicação. $m < n \Rightarrow m \cdot p < n \cdot p$, para todo $p \in \mathbb{N}$.*

Demonstração.

(1) Existem $r_1, r_2 \in \mathbb{N}$ tal que $m + r_1 = n$ e $n + r_2 = p$. Assim, existe $(r_1 + r_2) \in \mathbb{N}$ tal que $m + (r_1 + r_2) = (m + r_1) + r_2 = n + r_2 = p$. Portanto, $m < p$.

(2) Segue imediatamente da Proposição 2.4.

(3) Existe $q \in \mathbb{N}$ tal que $m + q = n$,

$$(m + p) + q = (m + q) + p = n + p. \qquad \text{Ou seja, } m + p < n + p.$$

(4) Existe $q \in \mathbb{N}$ tal que $m + q = n$,

$$m \cdot p + q \cdot p = (m + q) \cdot p = n \cdot p. \qquad \text{Portanto, } m \cdot p < n \cdot p.$$

□

2.5 Conjuntos finitos e infinitos

Definição 2.4. Para cada $n \in \mathbb{N}$ definimos o conjunto I_n como

$$I_n = \{1, 2, \ldots, n\}$$

Definição 2.5 (conjunto finito)**.** Dizemos que um conjunto X é *finito* quando for vazio ou, para algum $n \in \mathbb{N}$, existir uma bijeção

$$\varphi : I_n \to X,$$

Se $X = \emptyset$ dizemos que X tem zero elementos. Se existir uma bijeção com I_n dizemos que X tem n elementos.

Um conjunto X que não é finito é chamado *infinito*.

Enunciamos alguns resultados sobre conjuntos finitos (sem demonstração).

Proposição 2.9. *Se X é finito e $Y \subset X$ então Y é finito*

Proposição 2.10. *Se X e Y é finito, então $X \cup Y$ é finito.*

Proposição 2.11. *Se X e Y são finitos, então $X \times Y$ é finito.*

2.6 Conjuntos enumeráveis e não-enumeráveis

Definição 2.6. Dizemos que um conjunto X é *enumerável* se for finito ou então existir uma bijeção $\varphi : \mathbb{N} \to X$.

Quando o conjunto enumerável X não é finito, dizemos que é um conjunto *infinito enumerável*. Um conjunto X que não for enumerável é dito *não-enumerável*.

Exemplo 2.1. A bijeção $f : \mathbb{N} \to \mathbb{P}$, $f(n) = 2n$, mostra que o conjunto $\mathbb{P}$ dos números naturais pares é infinito enumerável. Analogamente, $g : \mathbb{N} \to \mathbb{I}$, $g(n) = 2n - 1$ define uma bijeção de $\mathbb{N}$ sobre o conjunto $\mathbb{I}$ dos números ímpares, o qual é, portanto, enumerável.

Exemplo 2.2. O conjunto $\mathbb{Z}$ dos números inteiros é enumerável, pois a função $h : \mathbb{Z} \to \mathbb{N}$ definida por $h(n) = 2n$, quando n é positivo e $h(n) = -2n + 1$ quando n é negativo ou zero, é um bijeção.

Proposição 2.12. *Todo subconjunto $X \subset \mathbb{N}$ é enumerável.*

Demonstração. Se X é finito nada há para demonstrar. Caso contrário, enumeramos os elementos de X pondo $x_1 =$ menor elemento de X, e supondo definidos $x_1 < x_2 < \ldots < x_n$, escrevemos $A_n = X - \{x_1, \ldots, x_n\}$. Observando que $A_n \neq \emptyset$, pois X é infinito, definimos $x_{n+1} =$ menor elemento de A_n. Então $X = \{x_1, x_2 \ldots, x_n, \ldots\}$. Com efeito, se existisse algum elemento $x \in X$ diferente de todos os x_n, teríamos $x \in A_n$ para todo $n \in \mathbb{N}$, logo x seria um número natural maior do que todos os elementos do conjunto infinito $\{x_1, x_2 \ldots, x_n, \ldots\}$, ou seja, o conjunto $\{x_1, x_2 \ldots, x_n, \ldots\}$, seria limitado e, portanto, finito. Contradição. □

Corolário 2.2. *Seja $f : X \to Y$ é injetiva. Se Y é enumerável então X é enumerável.*

Com efeito, basta considerar o caso em que existe uma bijeção $\varphi : Y \to \mathbb{N}$. Então $\varphi \circ f : X \to \mathbb{N}$ é uma bijeção de X sobre um subconjunto de $\mathbb{N}$, o qual é enumerável.

Corolário 2.3. *Seja $f : X \to Y$ sobrejetiva. Se X é enumerável então Y é enumerável.*

Com efeito, para cada $y \in Y$ podemos escolher um $x = g(y) \in X$ tal que $f(x) = y$. Isto define uma aplicação $g : Y \to X$ tal que $f(g(y)) = y$ para todo $y \in Y$. Segue-se daí que g é injetiva. Pelo corolário 2.2, Y é enumerável.

Corolário 2.4. *O produto cartesiano de dois conjuntos enumeráveis é um conjunto enumerável.*

Com efeito, se X e Y são enumeráveis então existem sobrejeções $f : \mathbb{N} \to X$ e $g : \mathbb{N} \to Y$, logo $\varphi : \mathbb{N} \times \mathbb{N} \to X \times Y$, dada por $\varphi(m, n) = (f(m), g(n))$ é sobrejetiva. Portanto, basta provar que $\mathbb{N} \times \mathbb{N}$ é enumerável. Para isto, consideremos a aplicação $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, dada por $\psi(m, n) = 2^m 3^n$. Pela unicidade da decomposição de um número em fatores primos, ψ é injetiva. Logo, $\mathbb{N} \times \mathbb{N}$ é enumerável.

Corolário 2.5. *A reunião de uma família enumerável de conjuntos enumeráveis é enumerável.*

Com efeito, dados $X_1, X_2, \ldots, X_n, \ldots$ enumeráveis, existem sobrejeções $f_1 : \mathbb{N} \to X_1, f_2 : \mathbb{N} \to X_2, \ldots, f_n : \mathbb{N} \to X_n, \ldots$ Tomando $X = \cup_{n=1}^{\infty} X_n$, definimos a sobrejeção $f : \mathbb{N} \times \mathbb{N} \to X$ pondo $f(m, n) = f_n(m)$.

Pelos resultados anteriores, podemos mostrar que $\mathbb{Q} = \{m/n; m, n \in \mathbb{Z}, n \neq 0\}$ é enumerável. Escrevendo $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, podemos definir uma função sobrejetiva $f : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$ pondo $f(m, n) = m/n$.

Proposição 2.13. *Todo conjunto infinito X contém um subconjunto infinito enumerável.*

Demonstração. Basta definir uma função injetiva $f : \mathbb{N} \to X$. Para isso, escolhemos para cada subconjunto não vazio $A \subset X$, um elemento $x_A \in A$. Em seguida, definimos f por indução. Pomos $f(1) = x_X$ e, supondo já definidos $f(1), f(2), \ldots, f(n)$, escrevemos $A_n = X - \{f(1), f(2), \ldots, f(n)\}$. Como X é infinito, A_n é não vazio. Definimos então $f(n+1) = x_{A_n}$. Isto completa a definição indutiva da função $f : \mathbb{N} \to X$. Afirmamos que f é injetiva. Com efeito, dados $m \neq n$ em $\mathbb{N}$ tem-se, digamos $m < n$. Então $f(m) \in \{f(1), \ldots, f(n-1)\}$ enquanto que $f(n) \in X - \{f(1), \ldots, f(n-1)\}$. Logo, $f(m) \neq f(n)$. A imagem $f(\mathbb{N})$ é, portanto, um subconjunto infinito enumerável de X. □

2.7 Exercícios

1. Demonstre que se um conjunto P goza das propriedades dadas pelos Axiomas de Peano, então, P é infinito enumerável.

2. O princípio da Boa Ordenação diz que *todo subconjunto não-vazio de $\mathbb{N}$ possui elemento mínimo.* Demonstre que $\mathbb{N}$, com a relação $\leq$, verifica o Princípio da Boa Ordenação.

3. Dados os números naturais a, b prove que existe um número natural m tal que $m \cdot a > b$.

4. Usando o princípio de indução, demonstre a propriedade de tricotomia enunciada na Proposição 2.4.

5. Use indução para demonstrar os seguintes fatos:

   (a) $(a-1)(1+a+\ldots+a^n) = a^{n+1} - 1$, seja quais forem $a, n \in \mathbb{N}$;

   (b) $n \geq 4 \Rightarrow n! > 2^n$

Capítulo 3

Os Números Inteiros

3.1 Definição axiomática dos inteiros

Antes de procedermos com a construção do conjunto dos inteiros, a definiremos axiomaticamente. Desse modo, saberemos quais as propriedades que devemos atingir ao construí-lo.

Definição 3.1. O *conjunto dos números inteiros*, denotado por $\mathbb{Z}$, é um conjunto onde são definidas duas operações binárias; a *adição* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto x + y$ e a *multiplicação* $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto x \cdot y$, as quais gozam dos seguintes axiomas.

Sejam $x, y, z \in \mathbb{Z}$,

(1) *Associatividade.* $(x + y) + z = x + (y + z)$ e $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(2) *Comutatividade.* $x + y = y + x$ e $x \cdot y = y \cdot x$.

(3) *Existência do elemento neutro.*

Existe $0 \in \mathbb{Z}$ tal que $x + 0 = x$ para todo $x \in \mathbb{Z}$.

Existe $1 \in \mathbb{Z}$ $(1 \neq 0)$ tal que $x \cdot 1 = x$ para todo $x \in \mathbb{Z}$.

(4) *Existência do simétrico.* Para cada $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$ tal que $x + (-x) = 0$.

(5) *Distributividade.* $x \cdot (y + z) = x \cdot y + x \cdot z$.

(6) $\mathbb{Z}$ *não tem divisores de zero.* $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$.

Um conjunto D junto a duas operações binárias gozando dos seis axiomas acima é chamado *domínio de Integridade.*

Todo corpo é um domínio de integridade.

O seguinte resultado afirma que todo domínio de integridade admite uma extensão chamada *corpo de frações*.

Proposição 3.1. *Se D é um domínio de integridade então, existe um corpo K, $D \subset K$, tal que os elementos de K podem ser escritos da forma a/b, onde $a, b \in D$.*

Ordem em $\mathbb{Z}$

Muitas propriedades em $\mathbb{Z}$ se originam do fato de escrevermos elas na ordem usual

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

Tal ordem pode ser expresso pela relação $a < b$, que se lê: *a é menor do que b*. Significando que, a está à esquerda de b. A relação $a < b$ é equivalente a dizer que $b - a$ é um inteiro positivo (ou natural). Toda propriedade da relação $a < b$ pode ser derivada da existência de um conjunto de inteiros positivos (neste caso $\mathbb{N}$) gozando das seguintes propriedades (ou axiomas)

(1) *(Fechadura)* se x, y são positivos então $x + y$ e $x \cdot y$ são positivos.

(2) *(Tricotomia)* para cada $a \in \mathbb{Z}$ vale uma e somente uma das seguintes alternativas:

$$\text{ou } a \text{ é positivo}, \quad \text{ou } a = 0, \quad \text{ou } -a \text{ é positivo.}$$

Desse modo, $a < b$ se e somente se $b - a \in \mathbb{N}$. Ou equivalentemente,

$$a < b \ \Leftrightarrow \ \text{existe } n \in \mathbb{N} \text{ tal que, } b + n = a.$$

Há outras três relações de ordem denotadas por: $>$; $\geq$ e $\leq$.
Dizemos que:

- a é *maior* do que b, denotado por $a > b$, se e somente se $b < a$;
- a é *maior ou igual* do que b, denotado por $a \geq b$, se e somente se $a > b$ ou $a = b$;
- a é *menor ou igual* do que b, denotado por $a \leq b$, se e somente se $a < b$ ou $a = b$.

Seguem algumas propriedades decorrentes da ordem em $\mathbb{Z}$. Ae demonstração é imediata e são baseadas na ordem definida em $\mathbb{N}$.

Proposição 3.2 (Propriedades da ordem em $\mathbb{Z}$)**.** *Sejam $a, b, c \in \mathbb{Z}$ então valem,*

(1) *Para todo $a \in \mathbb{Z} - \{0\}$, $a^2 > 0$ (portanto, $1 > 0$)*

(2) Transitividade. *Se $a < b$ e $b < c$ então $a < c$.*

(3) *se $a < b$ então $a + c < b + c$*

(4) *Se $a < b$ e $c > 0$ então $ac < bc$.*
Se $a < b$ e $c < 0$ então $ac > bc$.

(5) Tricotomia. *Para quaisquer $a, b \in \mathbb{Z}$ vale apenas uma e somente uma das relações*

$$ou \quad a < b \quad ou \quad a = b \quad ou \quad a > b.$$

Demonstração. Exercício. □

3.2 Construção dos Números Inteiros

Proposição 3.3. *A relação $\sim$ em $\mathbb{N} \times \mathbb{N}$ definida por*

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad a+d = b+c$$

é uma relação de equivalência.

Demonstração.

Reflexividade. Para todo $(a,b) \in \mathbb{N} \times \mathbb{N}$, $(a,b) \sim (a,b) \Leftrightarrow a+b = b+a$.

Simetria. Se $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$,

$$(a,b) \sim (c,d) \Leftrightarrow a+d = b+c \Leftrightarrow c+b = d+a \Leftrightarrow (c,d) \sim (a,b).$$

Transitividade. Se $(a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$ tal que $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$ Portanto,

$$a+d = b+c \text{ e } c+f = d+e \Rightarrow a+d+c+f = b+c+d+e.$$

Cancelando c e d, obtemos $a+f = b+e$. Isto é, $(a,b) \sim (e,f)$.

□

A relação de equivalência $\sim$ induz uma partição em $\mathbb{N} \times \mathbb{N}$. Assim, temos o conjunto quociente

$$(\mathbb{N} \times \mathbb{N})/\sim = \{[(a,b)];\ (a,b) \in \mathbb{N} \times \mathbb{N}\}$$

No conjunto $(\mathbb{N} \times \mathbb{N})/\sim$ definiremos uma adição e uma multiplicação.

3.3 Operações em $(\mathbb{N} \times \mathbb{N})/\sim$

3.3.1 Adição e multiplicação em $(\mathbb{N} \times \mathbb{N})/\sim$

Proposição 3.4 (Adição)**.** *Em $(\mathbb{N} \times \mathbb{N})/\sim$, a operação $+$ definida por*

$$[(a,b)] + [(c,d)] := [(a+c, b+d)]$$

é bem definida.

Demonstração. Sejam $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$. Precisamos mostrar que $[(a+c,b+d)] = [(a'+c',b'+d')]$. De fato, $(a,b) \sim (a',b')$ e $(c,d) \sim (c',d')$ implicam $a+b' = b+a'$ e $c+d' = d+c'$. Somando e associando adequadamente temos $(a+c)+(b'+d') = (b+d)+(a'+c')$. Ou seja, $(a+c,b+d) \sim (a'+c',b'+d')$. Portanto, $[(a+c,b+d)] = [(a'+c',b'+d')]$. □

Note que, sem perda de generalidade, estamos usando o mesmo símbolo $+$ para a adição em $(\mathbb{N} \times \mathbb{N}^*)/\sim$ e para adição em $\mathbb{N}$. Faremos o mesmo para a multiplicação.

Proposição 3.5 (Multiplicação). *Em* $(\mathbb{N}\times\mathbb{N})/\sim$, *a operação* $\cdot$ *definida por*

$$[(a,b)]\cdot[(c,d)] := [(ac+bd,\ ad+bc)]$$

é bem definida.

Demonstração. Sejam $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$. Assim, $(a,b)\sim(a',b')$ e $(c,d)\sim(c',d')$ implicam

$$a+b' = b+a' \quad \text{e} \quad c+d' = d+c'. \tag{1}$$

Precisamos mostrar que

$$[(ac+bd,\ ad+bc)] = [(a'c'+b'd',\ a'd'+b'c')],$$

que é equivalente a mostrar

$$ac+bd+a'd'+b'c' = a'c'+b'd'+ad+bc. \tag{2}$$

A verificação de (2), usando as identidades (1), segue de

$$\begin{aligned}
ac+bd+a'd'+b'c'+b'c &= (a+b')c+bd+a'd'+b'c' \\
&= (a'+b)c+bd+a'd'+b'c' \\
&= a'c+bc+bd+b'c'+a'd' \\
&= a'(c+d')+bc+bd+b'c' \\
&= a'(c'+d)+bc+bd+b'c' \\
&= a'c'+a'd+bc+bd+b'c' \\
&= a'c'+(a'+b)d+bc+b'c' \\
&= a'c'+(a+b')d+bc+b'c' \\
&= a'c'+ad+b'd+bc+b'c' \\
&= a'c'+ad+b'(d+c')+bc \\
&= a'c'+ad+b'(d'+c)+bc \\
&= a'c'+ad+b'd'+b'c+bc \\
&= a'c'+b'd'+ad+bc+b'c.
\end{aligned}$$

□

As duas proposições anteriores mostram que $+$ e $\cdot$ são operações binárias.

Observação. Como pretendemos construir o conjunto dos inteiros, justificaremos, *grosso modo*, como cada classe de equivalência (i.e., cada elemento de $(\mathbb{N}\times\mathbb{N})/\sim$) se identifica com um elemento de $\mathbb{Z}$, onde $\mathbb{Z}$ é o conjunto definido axiomaticamente na Definição 3.1.

Sejam $a,b,c,d \in \mathbb{N}$ e seja $\mathbb{Z}$ o conjunto da Definição 3.1. Como $\mathbb{N}\subset\mathbb{Z}$ então $a,b,c,d\in\mathbb{Z}$. Sejam $[(a,b)],[(c,d)]\in(\mathbb{N}\times\mathbb{N})/\sim$ tal que $[(a,b)] = [(c,d)]$. Considerando $a,b,c,d\in\mathbb{Z}$ então

$$[(a,b)] = [(c,d)] \Leftrightarrow a+d = b+c \Leftrightarrow a-b = a-d.$$

Assim, cada classe $[(a,b)]\in(\mathbb{N}\times\mathbb{N})/\sim$ pode ser identificada com a *diferença* $a-b\in\mathbb{Z}$. Aproveitamos essa identificação para definir o conjunto dos números inteiros como sendo o conjunto $(\mathbb{N}\times\mathbb{N})/\sim$.

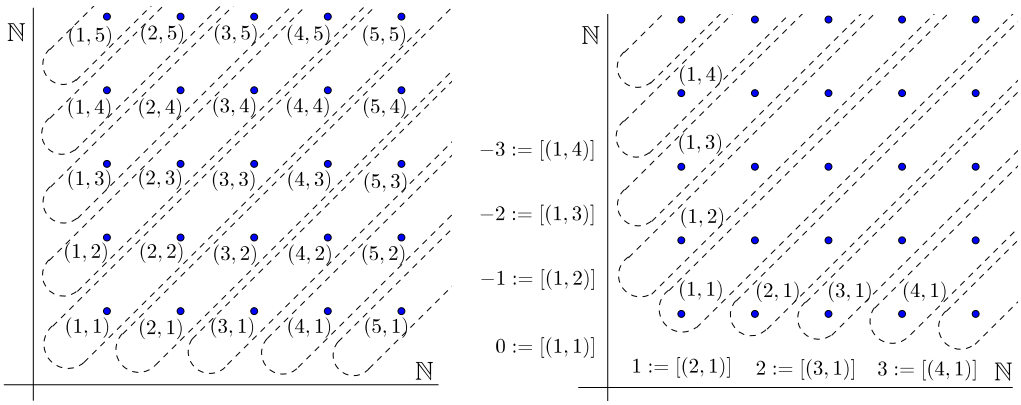


Figura 3.1: Obtenção de $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$

Definição 3.2. O *conjunto dos números inteiros*, denotado por $\mathbb{Z}$, é definido como sendo o conjunto das classes de equivalência $[(a,b)]$ dos elementos (a,b) de $\mathbb{N}\times\mathbb{N}$ respeito à relação de equivalência $\sim$. Ou seja,

$$\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim .$$

A *adição* $+$ e *multiplicação* $\cdot$ em $\mathbb{Z}$ é são definidas, respectivamente, por

$$[(a,b)] + [(c,d)] = [(a+c, b+d)] \quad \text{e} \quad [(a,b)]\cdot[(c,d)] = [(ac+bd,\ ad+bc)].$$

Teorema 3.1 (Propriedades da adição $+$)**.** *A adição $+$ em $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$ tem as seguintes propriedades:*

(1) *é associativa;*

(2) *comutativa;*

(3) $0 := [(1,1)]$ *é o elemento neutro e*

(4) *existe simétrico. Para cada $x = [(a,b)] \in \mathbb{Z}$ existe $-x := [(b,a)]$ tal que $x + (-x) = 0$.*

Demonstração.

(1) Sejam $x = [(a,b)]$, $y = [(c,d)]$ e $z = [(e,f)]$

$$\begin{aligned}
(x+y)+z &= \Big([(a,b)] + [(c,d)]\Big) + [(e,f)] \\
&= [(a+c, b+d)] + [(e,f)] \\
&= \big[\big((a+c)+e,\ (b+d)+f\big)\big] \\
&= \big[\big(a+(c+e),\ b+(d+f)\big)\big] \\
&= [(a,b)] + [(c+e,\ d+f)] \\
&= [(a,b)] + \Big([(c+e,\ d+f)]\Big) \\
&= [(a,b)] + \Big([(c,d)] + [(e,f)]\Big) \\
&= x + (y+z).
\end{aligned}$$

(2) Sejam $x = [(a,b)]$ e $y = [(c,d)]$

$$\begin{aligned} x + y &= [(a,b)] + [(c,d)] \\ &= [(a+c,\ b+d)] \\ &= [(c+a,\ d+b)] \\ &= [(c,d)] + [(a,b)] \\ &= y + x. \end{aligned}$$

(3) Se $x = [(a,b)] \in \mathbb{Z}$, existe $0 = [(1,1)]$ tal que $x + 0 = x$. Como $(a+1, b+1) \sim (a,b)$,

$$\begin{aligned} x + 0 &= [(a,b)] + [(1,1)] \\ &= [(a+1,\ b+1)] \\ &= [(a,b)] \\ &= x. \end{aligned}$$

(4) Dado $x = [(a,b)] \in \mathbb{Z}$ seja $-x = [(b,a)]$.
Observando que para todo $n \in \mathbb{N}$, $(n,n) \sim (1,1)$, temos

$$\begin{aligned} x + (-x) &= [(a,b)] + [(b,a)] \\ &= [(a+b,\ b+a)] \\ &= [(a+b,\ a+b)] \\ &= [(1,1)] \\ &= 0. \end{aligned}$$

Teorema 3.2 (Propriedades da multiplicação)**.** *A multiplicação* $\cdot$ *em* $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ *tem as seguintes propriedades:* □

(1) *é associativa;*

(2) *comutativa;*

(3) $1 := [(2,1)]$ *é elemento neutro e*

(4) *é distributiva sobre a adição.*

Demonstração.

(1) Sejam $x = [(a,b)],\ y = [(c,d)]$ e $z = [(e,f)]$.

$$\begin{aligned} (x \cdot y) \cdot z &= \Big([(a,b)] \cdot [(c,d)]\Big) \cdot [(e,f)] \\ &= [(ac+bd, ad+bc)] \cdot [(e,f)] \\ &= \big[\big((ac+bd)e + (ad+bc)f,\ (ac+bd)f + (ad+bc)e\big)\big] \\ &= [(ace+bde+adf+bcf,\ acf+bdf+ade+bce)] \\ &= [(ace+adf+bcf+bde,\ acf+ade+bce+bdf)] \\ &= \big[\big(a(ce+df) + b(cf+de),\ a(cf+de) + b(ce+df)\big)\big] \\ &= [(a,b)] \cdot [(ce+df,\ cf+de\ )] \\ &= [(a,b)] \cdot \Big([(c,d)] \cdot [(e,f)]\Big) \\ &= x \cdot (y \cdot z). \end{aligned}$$

(2) Sejam $x=[(a,b)]$ e $y=[(c,d)]$

$$\begin{aligned} x\cdot y &= [(a,b)]\cdot[(c,d)] \\ &= [(ac+bd,\ ad+bc)] \\ &= [(ac+bd,\ bc+ad)] \\ &= [(ca+db, cb+da\ )] \\ &= [(c,d)]\cdot[(a,b)] \\ &= y\cdot x. \end{aligned}$$

(3) Se $x=[(a,b)]\in\mathbb{Z}$ e $1=[(2,1)]$. Usando $\big(a+(a+b), b+(a+b)\big)\sim(a,b)$,

$$\begin{aligned} x\cdot 1 &= [(a,b)]\cdot[(2,1)] \\ &= [(a\cdot 2+b\cdot 1,\ a\cdot 1+b\cdot 2)] \\ &= [(2a+b,\ a+2b)] \\ &= \big[\big(a+(a+b),\ b+(a+b)\ \big)\big] \\ &= [(a,b)] \\ &= x. \end{aligned}$$

(4) $x=[(a,b)], y=[(c,d)]$ e $z=[(e,f)]$

$$\begin{aligned} x\cdot(y+z) &= [(a,b)]\cdot\Big([(c,d)]+[(e,f)]\Big) \\ &= [(a,b)]\cdot[(c+e,\ d+f)] \\ &= \big[\big(a(c+e)+b(d+f),\ a(d+f)+b(c+e)\big)\big] \\ &= [(ac+ae+bd+bf,\ ad+af+bc+be)] \\ &= \big[\big((ac+bd)+(ae+bf),\ (ad+bc)+(af+be)\big)\big] \\ &= [(ac+bd,\ ad+bc)]+[(ae+bf,\ af+be)] \\ &= [(a,b)]\cdot[(c,d)]+[(a,b)]\cdot[(e,f)] \\ &= x\cdot y+x\cdot z. \end{aligned}$$

□

Teorema 3.3 ($\mathbb{Z}$ não possui divisores de zero)**.** *Para* $x=[(a,b)]$ *e* $y=[(c,d)]$

$$[(a,b)]\cdot[(c,d)]=0\Longrightarrow[(a,b)]=0\quad ou\quad [(c,d)]=0.$$

Demonstração. Suponha que $[(a,b)]\cdot[(c,d)]=0$ e $[(c,d)]\neq 0$.
Ou equivalentemente,

$$[(a,b)]\cdot[(c,d)]=[(1,1)]\quad \text{e}\quad [(c,d)]\neq[(1,1)].$$

Por um lado,

$$\begin{aligned} [(a,b)]\cdot[(c,d)]=[(1,1)] &\Leftrightarrow [(ac+bd,\ ad+bc)]=[(1,1)] \\ &\Leftrightarrow ac+bd+1=ad+bc+1 \\ &\Leftrightarrow ac+bd=ad+bc. \end{aligned} \tag{3}$$

Por outro lado, $[(c,d)] \neq 0$ implica que $c \neq d$.

Por tricotomia em $\mathbb{N}$ temos duas possibilidades

$$c >_{\mathbb{N}} d \quad \text{ou} \quad c <_{\mathbb{N}} d,$$

onde $<_{\mathbb{N}}$ denota a ordem definida em $\mathbb{N}$.

Suponha $c >_{\mathbb{N}} d$.

Existe $p \in \mathbb{N}$ tal que $c = d + p$. Usando o valor de c em (3)

$$\begin{aligned} ac + bd = ad + bc &\Rightarrow a(d+p) + bd = ad + b(d+p) \\ &\Rightarrow ad + ap + bd = ad + bd + bp \\ &\Rightarrow ap = bp \\ &\Rightarrow a = b. \end{aligned}$$

Portanto, $[(a,b)] = 0$.

Para o caso, $c <_{\mathbb{N}} d$ de modo análogo, existe $p \in \mathbb{N}$ tal que $d = p + c$ e substituindo o valor de d em (3) obtemos $b = a$, ou seja $[(a,b)] = 0$. . □

Os resultados dos Teoremas 3.1, 3.2 e 3.3 mostram as propriedades que caracterizam o conjunto dos inteiros $\mathbb{Z}$. Ou seja, $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ é um *domínio de integridade*.

3.3.2 A substração em $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$

Definição 3.3. Sejam $x = [(a,b)]$ e $y = [(c,d)]$ elementos de $\mathbb{Z}$. A operação *substração*, $-$, é definida por

$$x - y := x + (-y).$$

Desse modo

$$[(a,b)] - [(c,d)] = [(a,b)] + ([(d,c)]) = [(a+d, b+c)].$$

Em $\mathbb{N}$, a substração não é bem definida (ou seja, não é operação binária). Em $\mathbb{Z}$ a substração é uma operação binária.

3.4 Relação de ordem em $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$

Definição 3.4. Dizemos que $x = [(a,b)]$ *é menor do que* $y = [(c,d)]$, o que denotamos por $x < y$ se, e somente se, $a + d <_{\mathbb{N}} b + c$. Ou seja,

$$x < y \quad \Leftrightarrow \quad a + d <_{\mathbb{N}} b + c,$$

onde $<_{\mathbb{N}}$ é a relação de ordem definida em $\mathbb{N}$.

A relação $<$ está bem definida. Isto é, não depende da escolha dos representantes das classes de equivalência.

De fato, $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$ é equivalente a

$$a + b' = b + a' \quad \text{e} \quad c + d' = d + c' \tag{4}$$

Usando (4)

$$\begin{aligned}
[(a,b)] < [(c,d)] &\Leftrightarrow a+d <_{\mathbb{N}} b+c \\
&\Leftrightarrow \exists p \in \mathbb{N} \text{ tal que } (a+d)+p = b+c \\
&\Leftrightarrow (a'+b'+c'+d')+a+d+p = (a'+b'+c'+d')+b+c \\
&\Leftrightarrow (a'+d')+p+[a+b']+\{c+d'\} = (b'+c')+[a'+b]+\{c+d'\} \\
&\Leftrightarrow (a'+d')+p = b'+c' \\
&\Leftrightarrow a'+d' <_{\mathbb{N}} b'+c' \\
&\Leftrightarrow [(a',b')] < [(c',d')].
\end{aligned}$$

As propriedades da Proposição 3.2, sobre a ordem $<$ dos inteiros inicialmente definidos axiomaticamente, também são válidas para o conjunto $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$. A demonstração decorre da boa definição da relação de ordem $<$ definida em $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$. Note que a forma como foi definida a relação de ordem em $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/\sim$ é exatamente a mesma da da relação de ordem da Proposição 3.2, pois dependem exclusivamente da relação $<_{\mathbb{N}}$ definida em $\mathbb{N}$.

3.5 Exercícios

1. Um conjunto que goze das propriedades da definição 3.1 é chamado *domínio de integridade*. Quais dos seguintes conjuntos são domínios de integridade?
   (a) Os inteiros pares;
   (b) Os inteiros ímpares;
   (c) Os números da forma $a+b\sqrt{2}$, onde $a,b\in\mathbb{Z}$.
   (d) Os inteiros positivos.
2. Demonstre as propriedades de ordem em $\mathbb{Z}$ enunciadas na Proposição 3.2.
3. Seja $a\in\mathbb{Z}$, prove que, se $b\in\mathbb{Z}$ é tal que $a\leq b\leq a+1$ então $b=a$ ou $b=a+1$.
4. Prove que não existe inteiro entre 0 e 1.
5. Um elemento $a\in\mathbb{Z}$ diz-se inversível se existe um outro elemento $a'\in\mathbb{Z}$ tal que $aa'=1$. Mostrar que os únicos elementos inversíveis de $\mathbb{Z}$ são 1 e -1.
6. Provar que todo conjunto não-vazio de inteiros limitado superiormente contém um elemento máximo.
7. Provar que, se um conjunto de inteiros tem elemento mínimo, então este é único. Fazer o mesmo, em relação ao máximo.
8. Se $a\in\mathbb{Z}$, a *potência* de a^n é definida por: $a^1=a$, $a^{n+1}=a^n a$. Prove por indução que as leis seguintes para expoentes positivos valem em $\mathbb{Z}$.

   $$\text{(i) } (a^m)^n = a^{mn}, \qquad \text{(ii) } (ab)^n = a^n b^n, \qquad \text{(iii) } 1^n = 1.$$

9. Prove que $\mathbb{Z}$ é enumerável.

Capítulo 4

Os Números Racionais

Antes de procedermos com a construção formal do conjunto dos números racionais $\mathbb{Q}$ a partir do conjunto dos inteiros $\mathbb{Z}$. O apresentaremos como é usual, ou seja, como um conjunto junto a duas operações binárias gozando axiomas que fazem dele um corpo.

4.1 Os Números Racionais

Um *número racional* é um número que pode ser expresso como o quociente ou fração a/b de dois números inteiros a e b, com $b \neq 0$. O conjunto de todos os racionais é denotado por

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0 \right\}.$$

Notação devida a Guiseppe Peano em 1895, do italiano *quoziente*. O termo *racional* provém do fato de a/b representar a *razão* ou proporção entre dois inteiros a e b.

4.1.1 $\mathbb{Q}$ como estrutura algébrica

Em $\mathbb{Q}$ são definidas duas operações binárias

Adição

Sejam $\frac{a}{b}$, $\frac{c}{d} \in \mathbb{Q}$ então a *adição*, $+$, lhes associa o elemento

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in \mathbb{Q}.$$

Multiplicação

Sejam $\frac{a}{b}$, $\frac{c}{d} \in \mathbb{Q}$ então a *multiplicação*, $\cdot$, lhes associa o elemento

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}.$$

Diremos que $\frac{a}{b} = \frac{c}{d} \ \Leftrightarrow\ ad = bc$.

$(\mathbb{Q}, +\cdot)$ é um corpo

Proposição 4.1. *O conjunto dos racionais $\mathbb{Q}$ com as duas operações de adição e multiplicação, acima definidas, é um corpo.*

Demonstração. Exercício. Use a definição 1.17 da seção 1.5. □

A Proposição 4.1 nos diz que as duas operações em $\mathbb{Q}$ gozam das seguintes propriedades.

1. *Associatividade.* Para todo $x, y, z \in \mathbb{Q}$ valem

$$(x + y) + z = x + (y + z) \quad \text{e} \quad (xy)z = x(yz)$$

2. *Comutatividade.* Para todo $x, y \in \mathbb{Q}$

$$x + y = y + x \quad \text{e} \quad xy = yx$$

3. *Existência de elementos neutros.* Existem $0 = \frac{0}{1} \in \mathbb{Q}$ e $1 = \frac{1}{1} \in \mathbb{Q}$ tais que

$$x + 0 = x \quad \text{e} \quad x \cdot 1 = x, \quad \forall x = \frac{a}{b} \in \mathbb{Q}.$$

4. *Existência dos inversos.*

   Para todo $x = \frac{a}{b} \in \mathbb{Q}$, existe $-x = \frac{-a}{b} \in \mathbb{Q}$ tal que $x + (-x) = 0$.

   Para todo $x = \frac{a}{b} \in \mathbb{Q}$, $x \neq 0$, existe $x^{-1} = \frac{b}{a} \in \mathbb{Q}$ tal que $x \cdot x^{-1} = 1$.

5. *Distributividade.* Para todo $x, y, z \in \mathbb{Q}$

$$x(y + z) = xy + xz$$

4.1.2 $\mathbb{Z}$ como subconjunto de $\mathbb{Q}$

Cada inteiro n pode ser identificado com o racional $\frac{n}{1}$. De fato, pelo algoritmo da divisão $n = \frac{n}{1} \Leftrightarrow n = n \cdot 1$. Portanto, de modo natural, os elementos de $\mathbb{Z}$ fazem parte de $\mathbb{Q}$.

4.1.3 $\mathbb{Q}$ é corpo ordenado

Para a definição de corpo ordenado, veja a seção 1.5. Definimos um conjunto de positivos $P \subset \mathbb{Q}$ como

$$P = \left\{ \frac{a}{b} \in \mathbb{Q};\ ab >_{\mathbb{Z}} 0 \right\}$$

Observação. A relação $>_{\mathbb{Z}}$ é a relação de ordem "*maior do que*" definida no conjunto dos inteiros $\mathbb{Z}$.

Proposição 4.2. *O conjunto $\mathbb{Q}$ junto ao conjunto $P = \left\{\frac{a}{b} \in \mathbb{Q};\ ab >_{\mathbb{Z}} 0\right\}$ é um corpo ordenado.*

Demonstração. Se $\frac{a}{b}, \frac{c}{d} \in P$ então $ab >_{\mathbb{Z}} 0$ e $cd >_{\mathbb{Z}} 0$. Com isso, a adição e multiplicação é fechada em P. De fato,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in P \Leftrightarrow (ad+bc)bd = abd^2 + cdb^2 >_{\mathbb{Z}} 0 \quad \text{e}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in P \Leftrightarrow acbd >_{\mathbb{Z}} 0.$$

Se $\frac{a}{b} \in \mathbb{Q}$ então $ab \in \mathbb{Z}$, segue da tricotomia em $\mathbb{Z}$ que

$$\text{ou } ab >_{\mathbb{Z}} 0 \quad \text{ou} \quad ab = 0 \quad \text{ou} \quad ab <_{\mathbb{Z}} 0.$$

Portanto,

$$\text{ou } \frac{a}{b} \in P \quad \text{ou} \quad \frac{a}{b} = 0 \quad \text{ou} \quad -\frac{a}{b} \in P.$$

Desse modo, $\mathbb{Q}$ é um corpo ordenado. □

4.2 Construção dos Números Racionais

A construção dos números racionais é realizada a partir do domínio de integridade dos inteiros $(\mathbb{Z}, +, \cdot)$. O conjunto dos inteiros diferentes de zero, denotamos por $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Proposição 4.3. *A relação $\sim$ em $\mathbb{Z} \times \mathbb{Z}^*$ definida por*

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad = bc$$

é uma relação de equivalência.

Demonstração. Para todo $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ $(a,b) \sim (a,b) \Leftrightarrow ab = ba$ de onde segue que $\sim$ é reflexiva. Para a simetria, se $(a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$ temos

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c,d) \Leftrightarrow (a,b).$$

Finalmente, sejam $(a,b), (c,d), (e,f) \in \mathbb{Z} \times \mathbb{Z}^*$ tal que $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$. Assim, $ad = bc$ e $cf = de$. Com isso

$$ad = bc \Rightarrow adf = bcf \Rightarrow (af)d = b(cf) \Rightarrow (af)d = b(de) \Rightarrow (af)d = (be)d.$$

Como $d \neq 0$ e a lei do corte sendo válida em $\mathbb{Z}$ então, $(af)d = (be)d$ implica $af = be$. Ou seja, $(a,b) \sim (e,f)$. O que mostra a transitividade. □

A relação de equivalência $\sim$ induz uma partição em $\mathbb{Z} \times \mathbb{Z}^*$. Assim, obtemos o conjunto quociente

$$(\mathbb{Z} \times \mathbb{Z}^*)/\sim = \{[(a,b)];\ (a,b) \in \mathbb{Z} \times \mathbb{Z}^*\}$$

4.3 Operações em $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$

4.3.1 Adição e multiplicação $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$

Proposição 4.4 (Adição). *Em $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$, a operação dada por*

$$[(a,b)] + [(c,d)] := [(ad + bc, bd)]$$

é bem definida.

Demonstração. Sejam $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$. Mostraremos que

$$[(a,b)] + [(c,d)] = [(a',b')] + [(c',d')].$$

De fato, $(a,b) \sim (a',b')$ e $(c,d) \sim (c',d')$ implicam

$$ab' = ba' \quad \text{e} \quad cd' = dc'. \tag{1}$$

Multiplicando os termos dd' e bb' em (1)

$$(ab')(dd') = (ba')(dd') \quad \text{e} \quad (cd')(bb') = (dc')(bb'). \tag{2}$$

Usando (2) temos

$$\begin{aligned}(ad + bc)(b'd') &= adb'd' + bcb'd' \\ &= (ab')(dd') + (cd')(bb') \\ &= (ba')(dd') + (dc')(bb') \\ &= bda'd' + bdb'c' \\ &= (bd)(a'd' + b'c').\end{aligned}$$

Como $(ad + bc)(b'd') = (bd)(a'd' + b'c') \Leftrightarrow (ad + bc, bd) \sim (a'd' + b'c', b'd')$. Logo, $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$. Ou seja, $[(a,b)] + [(c,d)] = [(a',b')] + [(c',d')]$. □

Proposição 4.5. *Em $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$, a operação dada por*

$$[(a,b)] \cdot [(c,d)] := [(ac, bd)]$$

é bem definida.

Demonstração. Se $[(a,b)] = [(a',b')]$ e $[(c,d)] = [(c',d')]$, então $(a,b) \sim (a',b')$ e $(c,d) \sim (c',d')$ o que implica

$$ab' = ba' \quad \text{e} \quad cd' = dc'. \tag{3}$$

Usando (3) obtemos $(ab')(cd') = (ba')(dc')$.

Desse modo,

$$\begin{aligned}[(a,\ b)] \cdot [(c,\ d)] = [(a',\ b')] \cdot [(c',\ d')] &\Leftrightarrow [(ac, bd)] = [(a'c', b'd')] \\ &\Leftrightarrow (ac)(b'd') = (bd)(a'c') \\ &\Leftrightarrow (ab')(cd') = (ba')(dc').\end{aligned}$$

Portanto, o produto independe dos representantes das classes de equivalência. □

Observação. Como estamos construindo o conjunto dos racionais, *grosso modo*, justificaremos como cada elemento de $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ se identifica com um elemento de $\mathbb{Q}$ (onde $\mathbb{Q}$ é o conjunto definido na Seção 4.1.1).

Sejam $m, a \in \mathbb{Z}$; $n, b \in \mathbb{Z}^*$ e seja $\mathbb{Q}$ o conjunto definido na Seção 4.1.1. Como $\mathbb{Z} \subset \mathbb{Q}$ (veja a subseção 4.1.2) então $m, n, a, b \in \mathbb{Q}$. Sejam $[(m,n)], [(a,b)] \in (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ tal que $[(m,n)] = [(a,b)]$.
Considerando $m, n, a, b \in \mathbb{Q}$ então

$$[(m,n)] = [(a,b)] \Leftrightarrow mb = na \Leftrightarrow \frac{m}{n} = \frac{a}{b}.$$

Cada elemento $[(m,n)]$ de $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ pode ser identificado com o *quociente* $m/n \in \mathbb{Q}$. Note que a classe $[(m,n)]$ é o conjunto solução da equação

$$\frac{x}{y} = \frac{m}{n} \quad \text{onde } (x,y) \in \mathbb{Z} \times \mathbb{Z}^*.$$

Assim, as classes de equivalência $[(m,n)]$ são retas de $\mathbb{Z} \times \mathbb{Z}^*$. Cada classe $[(m,n)]$ representa o racional m/n. Aproveitamos tal identificação para definir o conjunto dos números racionais como sendo o conjunto $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$.

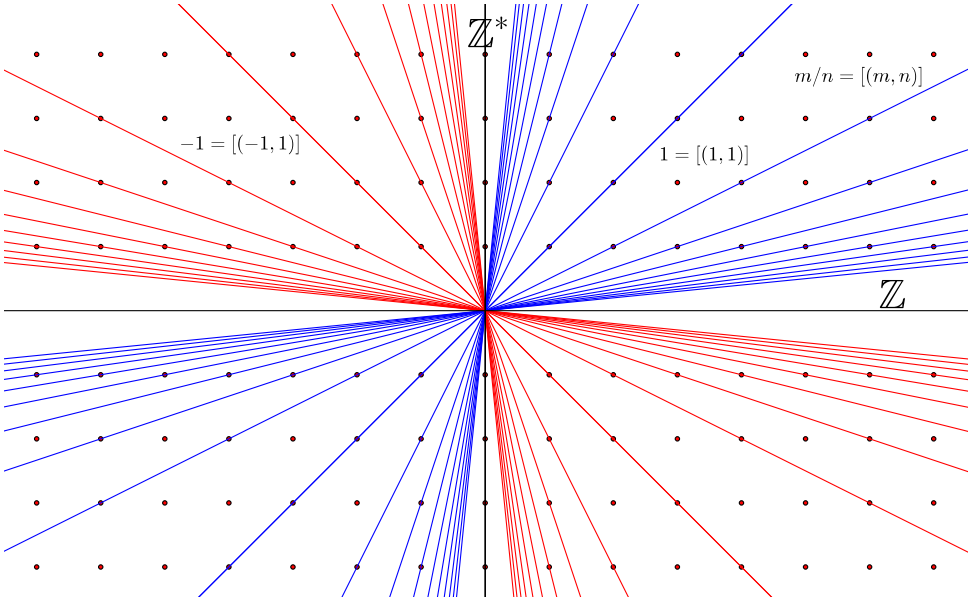


Figura 4.1: Obtenção de $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$

Definição 4.1. O *conjunto dos números racionais*, denotado por $\mathbb{Q}$, é definido como sendo o conjunto das classes de equivalência $[(a,b)]$ dos elementos (a,b) de $\mathbb{Z} \times \mathbb{Z}^*$ respeito à relação de equivalência. Ou seja,

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim .$$

A *adição* $+$ e *multiplicação* $\cdot$ em $\mathbb{Q}$ é definido, respectivamente, por

$$[(a,b)] + [(c,d)] = [(ad + bc,\ bd)] \quad \text{e} \quad [(a,b)] \cdot (c,d)] = [(ac, bd)].$$

Teorema 4.1 (Propriedades da adição em $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$)**.** *A adição $+$ em $\mathbb{Z}$ tem as seguintes propriedades:*

(1) *Associativa.*

(2) *Comutativa.*

(3) *Existência do elemento neutro da adição* $0 := [(0,1)]$.

(4) *Existência do inverso aditivo. Para cada $x = [(a,b)] \in \mathbb{Z}$ existe $-x := [(b,a)]$ tal que $x + (-x) = 0$. O elemento $-x$ é o inverso aditivo de x.*

Demonstração.

(1) Sejam $x = [(a,b)]$, $y = [(c,d)]$ e $z = [(e,f)]$.

$$\begin{aligned}(x+y)+z &= \Big([(a,b)] + [(c,d)]\Big) + [(e,f)] \\ &= [(ad+bc, bd)] + [(e,f)] \\ &= \big[\big((ad+bc)f + (bd)e\ ,\ (bd)f\big)\big] \\ &= \big[\big(adf + bcf + bde\ ,\ bdf\big)\big] \\ &= \big[\big(a(df) + b(cf+de)\ ,\ b(df)\big)\big] \\ &= [(a,b)] + [(cf+de, df)] \\ &= [(a,b)] + \Big([(c,d)] + [(e,f)]\Big) \\ &= x + (y+z).\end{aligned}$$

(2) Sejam $x = [(a,b)]$ e $y = [(c,d)]$

$$\begin{aligned}x + y &= [(a,b)] + [(c,d)] \\ &= [(ad+bc, bd)] \\ &= [(cb+da, db)] \\ &= [(c,d)] + [(a,b)] \\ &= y + x.\end{aligned}$$

(3) Existe $0 := [(0,1)]$ tal que $x + 0 = x$, para todo $x = [(a,b)] \in \mathbb{Q}$. De fato,

$$x + 0 = [(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)] = x.$$

(4) Dado $x = [(a,b)] \in \mathbb{Q}$ seja $-x := [(-a,b)]$.
Considerando que $[(0,n)] = 0$, para todo $n \in \mathbb{Z}^*$

$$x + (-x) = [(a,b)] + [(-a,b)] = [(ab + b(-a), bb)] = [(0,bb)] = 0.$$

□

Teorema 4.2 (Propriedades da multiplicação em $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$)**.** *A multiplicação* $\cdot$ *em* $\mathbb{Q}$ *tem as seguintes propriedades:*

(1) *é associativa;*

(2) *comutativa;*

(3) $1 := [(1,1)]$ *é elemento neutro da multiplicação;*

(4) *existe o inverso multiplicativo. Isto é,*
para cada $x = [(a,b)] \in \mathbb{Q} \setminus \{0\}$*, existe* $x^{-1} = [(b,a)] \in \mathbb{Q}$ *tal que* $x \cdot x^{-1} = 1$*, é*

(5) *é distributiva sobre a adição.*

Demonstração.

(1) Sejam $x = [(a,b)]$, $y = [(c,d)]$ e $z = [(e,f)]$.

$$\begin{aligned}(x \cdot y) \cdot z &= \Big([(a,b)] \cdot [(c,d)]\Big) \cdot [(e,f)] \\ &= [(ac, bd)] \cdot [(e,f)] \\ &= \big[\big((ac)e,\ (bd)f\big)\big] \\ &= \big[\big(a(ce),\ b(df)\big)\big] \\ &= [(a,b)] \cdot [(ce,\ df\ )] \\ &= [(a,b)] \cdot \Big([(c,d)] \cdot [(e,f)]\Big) \\ &= x \cdot (y \cdot z).\end{aligned}$$

(2) Sejam $x = [(a,b)]$ e $y = [(c,d)]$

$$\begin{aligned}x \cdot y &= [(a,b)] \cdot [(c,d)] \\ &= [(ac,\ bd)] \\ &= [(ca,\ db)] \\ &= [(c,d)] \cdot [(a,b)] \\ &= y \cdot x.\end{aligned}$$

(3) Se $x = [(a,b)] \in \mathbb{Q}$ e $1 = [(1,1)]$.

$$\begin{aligned}x \cdot 1 &= [(a,b)] \cdot [(1,1)] \\ &= [(a \cdot 1, b \cdot 1)] \\ &= [(a,b)] \\ &= x.\end{aligned}$$

(4) Se $x = [(a,b)] \in \mathbb{Q} \setminus \{0\}$, se $x^{-1} = [(b,a)]$ $\qquad$ ($x^{-1} \in \mathbb{Q}$, pois $a \neq 0$)

$$x \cdot x^{-1} = [(a,b)] \cdot [(b,a)] = [(ab,ba)] = [(ab,ab)] = [(1,1)] = 1.$$

Note que $ab \neq 0$ e $(ab,ab) \sim (1,1)$.

(5) Sejam $x = [(a,b)]$, $y = [(c,d)]$ e $z = [(e,f)]$. Como $b \neq 0$, $1 = [(b,b)]$, segue

$$\begin{aligned}
x \cdot (y+z) &= [(a,b)] \cdot \Big([(c,d)] + [(e,f)] \Big) \\
&= [(a,b)] \cdot [(cf+de,\ df)] \\
&= \big[\big(a(cf+de),\ b(df)\big) \big] \\
&= [(acf+ade+bdf,\ bdf)] \\
&= [(acf+ade+bdf,\ bdf)] \cdot 1 \\
&= [(acf+ade+bdf,\ bdf)] \cdot [(b,b)] \\
&= \big[\big((acf+ade+bdf)b,\ (bdf)b\big) \big] \\
&= \big[\big(acfb+adeb+bdfb,\ bdfb\big) \big] \\
&= \big[\big((ac)(bf)+(bd)(ae),\ (bd)(bf)\big) \big] \\
&= [(ac,\ bd)] + [(ae,\ bf)] \\
&= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] \\
&= x \cdot y + x \cdot z.
\end{aligned}$$

□

Proposição 4.6. *O conjunto $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ junto às duas operações, $+$ e $\cdot$ é um corpo.*

Demonstração. A prova segue dos teoremas 4.1 e 4.2 □

Definição 4.2. A estrutura algébrica $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ junto às operações de adição e multiplicação definidas é chamada *corpo dos números racionais.*

4.3.2 A substração e divisão em $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$

Definição 4.3. Sejam $x = [(a,b)]$ e $y = [(c,d)]$ elementos de $\mathbb{Q}$. A operação *substração*, $-$, é definida por

$$x - y := x + (-y).$$

O elemento $x - y \in \mathbb{Q}$ é chamado a $diferena$ e de x e y. Desse modo

$$[(a,b)] - [(c,d)] = [(a,b)] + ([(d,c)]) = [(a+d, b+c)].$$

Definição 4.4. Sejam $x = [(a,b)]$ e $y = [(c,d)] \neq 0$ elementos de $\mathbb{Q}$. A *divisão*, de x e y é definida por

$$x/y := x \cdot y^{-1}.$$

Desse modo

$$[(a,b)]/[(c,d)] = [(a,b)] \cdot ([(d,c)]) = [(ad,bc)].$$

O elemento $x/y \in \mathbb{Q}$ é chamado o *quociente* de x e y.

Em $\mathbb{Q}$ a substração é divisão são operações binárias. Em $\mathbb{Z}$, a divisão não é binária.

4.4 $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ como corpo ordenado

Precisamos definir, em $\mathbb{Q}$, um conjunto de positivos P de tal forma que os axiomas de ordem sejam satisfeitos. Isto é, a adição e multiplicação seja fechada em P e seja válida a tricotomia. Veja a seção 1.5, definição 1.18. O símbolo $>_{\mathbb{Z}}$ é a relação de ordem: *maior do que*, no conjunto dos inteiros $\mathbb{Z}$.

Proposição 4.7 ($\mathbb{Q}$ é ordenado)**.** *Seja $P = \{[(a,b)] \in \mathbb{Q};\ ab >_{\mathbb{Z}} 0\}$. O conjunto P faz de $\mathbb{Q}$ um corpo ordenado.*

Demonstração. Sejam $x = [(a,b)]$ e $y = [(c,d)]$ elementos de P. Assim,

$$ab >_{\mathbb{Z}} 0 \quad e \quad cd >_{\mathbb{Z}} 0 \tag{4}$$

Usando (4), $d \neq 0$ (e assim $d^2 >_{\mathbb{Z}} 0$) e as propriedades da ordem em $\mathbb{Z}$ verifica-se

$$x + y = [(ad + bc, bd)] \in P \iff (ad + bc)bd = (ab + cd)d^2 >_{\mathbb{Z}} 0,$$

$$x \cdot y = [(ac, bd)] \in P \iff (ac)(bd) = (ab)(cd) >_{\mathbb{Z}} 0$$

Portanto, a adição e multiplicação são fechadas em P. Resta mostrar a tricotomia.

Seja $[(a,b)] \in \mathbb{Q}$. Então $ab \in \mathbb{Z}$. Da tricotomia em $\mathbb{Z}$

$$\text{ou } ab >_{\mathbb{Z}} 0 \text{ ou } ab = 0 \text{ ou } ab <_{\mathbb{Z}} 0.$$

Como $b \neq 0$ então

$$\text{ou } ab >_{\mathbb{Z}} 0 \text{ ou } a = 0 \text{ ou } (-a)b = -ab >_{\mathbb{Z}} 0.$$

Assim,

$$\text{ou } [(a,b)] \in P \text{ ou } [(a,b)] = [(0,b)] = 0 \text{ ou } [(-a,b)] \in P.$$

Ou seja

$$\text{ou } [(a,b)] \in P \text{ ou } [(a,b)] = 0 \text{ ou } -[(a,b)] \in P.$$

□

Portanto, $\mathbb{Q}$ é corpo ordenado. Isso permite definir em $\mathbb{Q}$ a relação de ordem $>$ como segue

Definição 4.5. Dados $x, y \in \mathbb{Q}$, dizemos que x é *maior do que* y se, e somente, $x - y \in P$, e denotamos por $x > y$.

Como $x > 0$ se, e somente se $x - 0 = x \in P$. Nesse caso, sendo que P é chamado o conjunto de positivos, diremos que x é *positivo*, quando $x > 0$.

Dizemos que

i) x é *menor do que* y, denotado por $x < y$ se, e somente se, $y > x$

ii) x é *maior ou igual do que* y, denotado por $x \geq y$ se, e somente se, $x > y$ ou $x = y$, e

iii) x é *menor ou igual do que* y, denotado por $x \leq y$ se, e somente se, $x < y$ ou $x = y$.

4.4.1 Propriedades da relação de ordem

Como $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ é um corpo ordenado. Então automaticamente são válidas todas as propriedades de ordem da Proposição 1.8. Essas propriedades dependem apenas da existência de conjunto de positivos P de positivos no corpo.

Por exemplo, a relação de ordem $<$ em $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ tem as seguintes propriedades:

(a) *Transitividade.* $x < y \text{ e } y < z \Rightarrow x < z$.

(b) *Tricotomia.* Se $x, y \in \mathbb{Q}$, apenas uma das seguinte alternativas ocorre

$$\text{ou} \quad x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y$$

(c) *Monotonicidade da adição* $x < y \Rightarrow x + z < y + z, \forall z \in \mathbb{Q}$.

(d) *Monotonicidade da multiplicação.*

$$x < y \text{ e } z > 0 \Rightarrow xz < yz.$$

$$x < y \text{ e } z < 0 \Rightarrow xz > yz.$$

4.5 Exercícios

1. Demonstre que o conjunto $\mathbb{Q}$ da Proposição 4.1 é um corpo.
2. Seja $\alpha \in \mathbb{Q}$. Prove que existe um único $n \in \mathbb{Z}$ tal que $n \leq \alpha \leq n + 1$.
3. Mostrar com um exemplo que nem todo conjunto não-vazio de números racionais limitado superiormente tem máximo.
4. 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.
5. Sejam a, b 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 $\sqrt{a} - \sqrt{b}$.)
6. Prove que não existe número racional cujo quadrado seja 12.
7. Mostre que em $\mathbb{Q}$ valem

   (i) $0 < 1/a \Leftrightarrow a > 0$,

   (ii) $a/b < c/d \Leftrightarrow abd^2 < b^2cd0$,

   (iii) $0 < a < b \Rightarrow 0 < 1/b < 1/a$,

   (iv) $a < b < 0 \Rightarrow 0 > 1/a > 1/b$,

   (v) $a_1^2 + a_2^2 + \cdots + a_n^2 \geq 0$.
8. Mostre que $\mathbb{Q}$ é um conjunto enumerável.

Capítulo 5

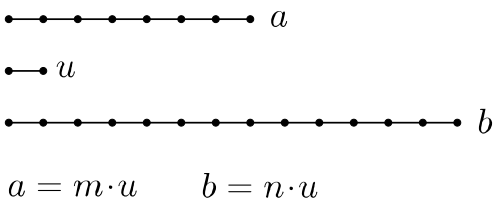
Os Números Irracionais

5.1 Números comensuráveis e incomensuráveis

Os antigos gregos, intuitivamente, acreditavam que dados dois objetos quaisquer, de comprimentos a e b, sempre existia alguma unidade u, suficientemente pequena, de tal forma que ambos objetos pudessem ser medidos de modo "*exato*"com essa unidade u. Ou seja,

$$\forall\ a \text{ e } b, \exists\ u \text{ tal que } \ a = m \cdot u \ \text{ e } \ b = n \cdot u, \text{ onde } m, n \in \mathbb{N}.$$

Desse modo, usando a medida u, um objeto mediria m vezes u e o outro n vezes u. Os objetos (números) a e b são ditos *comensuráveis*. Para os antigos gregos, dois comprimentos quaisquer eram sempre comensuráveis. Em outras palavras, tudo se podia comparar ou medir utilizando números inteiros.



Dizer que dois números a e b são sempre comensuráveis implica que o quociente de dois números a e b quaisquer é sempre racional.

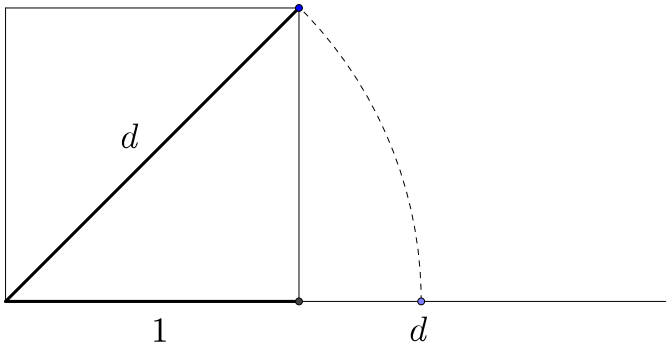
$$\frac{a}{b} = \frac{m \cdot u}{n \cdot u} = \frac{m}{n},$$

sendo $m, n \in \mathbb{N}$, então $\dfrac{a}{b} \in \mathbb{Q}$.

Seria grande a surpresa desses gregos ao descobrirem que pudessem existir números não comensuráveis ou *incomensuráveis*. Acredita-se que foi Hípaso de Metaponto, membro da escola pitagórica, quem demonstrara (provavelmente por métodos geométricos) que a *hipotenusa de um triângulo retângulo isósceles e um dos seus catetos não eram comensuráveis.* Ou, equivalentemente, que a diagonal d de um quadrado e um dos seus lados l são incomensuráveis.

Sem perda de generalidade, suponha $l = 1$. Pelo teorema de Pitágoras

$$d^2 = 1^2 + 1^2 = 2.$$



Se d e $l = 1$ fossem comensuráveis então teríamos que $\frac{d}{l} = d$ é racional.
Portanto, deveríamos admitir que,

$$\exists\, d \in \mathbb{Q} \text{ tal que } d^2 = 2$$

Mostraremos que tal conclusão é absurda.

Lema 5.1. *Não existe racional d tal que $d^2 = 2$.*

Demonstração. Suponha que existe $d \in \mathbb{Q}$ tal que $d^2 = 2$. Ou seja, $d = \frac{m}{n}$, onde m e n são primos relativos (isto é, m e n não têm fatores em comum). Logo,

$$\left(\frac{m}{n}\right)^2 = 2 \quad \Leftrightarrow \quad m^2 = 2n^2.$$

Significa que m^2 é par. Logo, necessariamente m *é par* (se m fosse ímpar, o produto $m \cdot m = m^2$ seria ímpar). Sendo m par, existe $k \in \mathbb{Z}$ tal que $m = 2k$.

Assim, $m^2 = 4k^2$ e, portanto, $n^2 = 2k^2$. O que implica que n^2 é par. Desse modo, necessariamente, n é par. Isto é, existe $r \in \mathbb{Z}$ tal que $n = 2r$. Isso mostra que m e n não podem ser primos relativos, pois têm como fator comum o 2. Tal contradição prova o lema. □

Portanto, deve-se concluir que *existem números incomensuráveis*. Note que a diagonal d pode ser "levada"até a reta onde encontra o cateto do quadrado (rotando $\pi/4$ no sentido horário). Ou seja, o comprimento d corresponde a um ponto da reta, portanto, existe. Mas, quem era esse número d? Antes dessa descoberta, achavam que todo ponto da reta poderia ser representado por um racional.

Conta a lenda que essa descoberta teria levado a uma crise da matemática pitagórica. Na época, a escola pitagórica tratava os números como entidades místicas (números: amigáveis; primos; perfeitos; deficientes; abundantes; etc).

5.2 Existência de números não racionais

O Lema 5.1 mostra que deve existir número d não racional cujo quadrado é 2. Mostra também que o conjunto dos racionais é um conjunto *incompleto*, no sentido de que existe número (pelo menos o d) que não é racional.

O número d, tal que $d^2 = 2$, é chamado *raiz quadrada de 2* e é denotado por $\sqrt{2}$.

Definição 5.1. Um número que não é racional é chamado *irracional*.

No próximo capítulo será construído o conjunto dos números reais, denotado por $\mathbb{R}$.

Definição 5.2. O *conjunto dos números irracionais* é o conjunto formado pelos números reais que não são racionais. Denotamos

$$\mathbb{R} \setminus \mathbb{Q} = \{a \in \mathbb{R};\ a \notin \mathbb{Q}\}$$

Pode parecer estranho termos definido os irracionais como sendo elementos do conjunto dos reais $\mathbb{R}$, conjunto que ainda não foi construído nem definido. Não há problema com isso; se fossemos definir um irracional como sendo *um número que não é racional*, não estaríamos sendo muito claros. Por exemplo, a unidade imaginária i é irracional? Sabemos que i não pertence aos reais, e que todo racional é real, então é lógico concluir que o número i não é racional. Então isso significa que i é irracional? Para resolver esse dilema, devemos lembrar que, os gregos, mesmo que ainda não soubessem quem eram os reais, quando se referiam aos irracionais estavam se referindo a pontos de reta.

Infinitude dos irracionais

Note que para cada $n \in \mathbb{N}$, o número $n\sqrt{2}$ é irracional. De fato, se $r = n\sqrt{2}$ fosse racional, teríamos que concluir que $\sqrt{2} = r \cdot \dfrac{1}{n} \in \mathbb{Q}$. O que é absurdo. Portanto, necessariamente: $n\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, $\forall n \in \mathbb{N}$. Se $S = \{n\sqrt{2}, n \in \mathbb{N}\}$ temos $S \subset \mathbb{R} \setminus \mathbb{Q}$. A aplicação $\varphi : \mathbb{N} \to S$, dada por $\varphi(n) = n\sqrt{2}$ é uma bijeção. Portanto, S é infinito.

Os mesmos argumentos da demonstração do Lema 5.1 servem para mostrar mostrar que

Proposição 5.1. *Para todo primo p, não existe $d \in \mathbb{Q}$ tal que $d^2 = p$.*

Isto mostra que números da forma $\sqrt{p}$, onde p é primo, são irracionais (este seria um outro modo de verificar a existência de infinitos irracionais).

Os exemplos de números irracionais, mostrados até agora, fazem parte de um tipo especial de irracionais chamados números algébricos.

5.3 Números algébricos e números transcendentes

Definição 5.3. Um número α é chamado *algébrico* se for raiz de algum polinômio com coeficientes inteiros. Ou seja, raiz de um polinômio da forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

onde $a_i \in \mathbb{Z}$, $i \in \{0, 1, \ldots, n\}$ e $a_n \neq 0$.

Exemplo 5.1. Todo número racional $\alpha = p/q$ é algébrico, pois é raiz de $qx - p$.

Exemplo 5.2. Os números irracionais $\alpha = \sqrt{p}$, onde p é primo, são algébricos. De fato, são raízes de $x^2 - p$.

Definição 5.4. Um número que não é algébrico é chamado *transcendente*.

Os números transcendentes mais conhecidos e famosos são:

- $\pi = C/D$, onde C é o perímetro de uma circunferência de diâmetro D,

$$\pi = 3,1415926535897932\ldots$$

- $e = \dfrac{1}{0!} + \dfrac{1}{1!} + \dfrac{1}{2!} + \dfrac{1}{3!} \cdots$

$$e = 2.71828182846\ldots$$

Recomendamos a leitura do livro de Eli Maor: ***e*** *: a história de um número* [22], dedicado integramente a esse importante número e o livro de Beckman: *A History of* π [6] dedicado a outro número famoso: π.

Pelo Exemplo 5.1, todo racional é algébrico, é equivalente a dizer que se um número não for algébrico então ele não é racional. Ou seja,

todo número real transcendental é irracional.

Para um estudo mais detalhado sobre números transcendentes recomendamos o livro de Marques [23].

Um texto excelente que se dedica de forma exclusiva aos irracionais é o livro de Havil: *The Irrationals* [14].

5.4 Exercícios

1. Mostre que qualquer intervalo de $\mathbb{R}$ contém algum irracional.
2. Mostre que um número real da forma $0,101001000100001000010\ldots$ é irracional.
3. Se p é primo, mostre que $\sqrt{p}$ é irracional. (Proposição 5.1).
4. Se $m, a \in \mathbb{N}$, prove que $\sqrt[n]{a}$ é irracional ou então é inteiro.
5. Mostre que $\log_{10} 2$ e $\log_{10} 3$ são irracionais.
6. Sejam a racional diferente de zero, e x irracional. Prove que $a + x$ e ax são irracionais. Dê um exemplo de dois números irracionais x, y tais que $x + y$ e $x \cdot y$ são racionais.

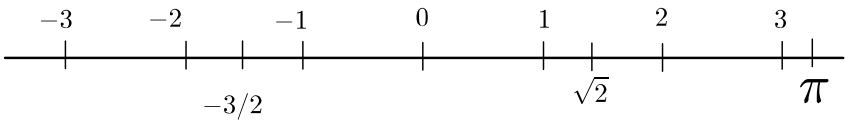
Capítulo 6

Os Números Reais e sua Construção

Vários matemáticos do século XIX apresentaram construções dos números reais, entre eles: Karl Weierstrass, Charles Méray, Richard Dedekind e Georg Cantor. Neste capítulo, estudamos os métodos de Cantor, de Dedekind e as expansões decimais.

6.1 Definição axiomática do conjunto dos números reais

O conjunto dos números reais e suas propriedades são apresentados ao aluno desde muito cedo em diversas disciplinas de matemática. Ele é associado, geometricamente, à reta. Com o advento da geometria analítica e o uso de coordenadas, os números reais podem ser vistos como pontos da reta.



Existem vários caminhos para abordar o estudo dos *Números Reais*. Temos os sintéticos e os rigorosos (árduos). Ambas abordagens têm vantagens e desvantagens. Os caminhos curtos tem a vantagem da praticidade, pois é suficiente defini-los como um conjunto que satisfaz certos axiomas de tal forma que seja um *corpo ordenado e completo* e pronto. Ou então, simplesmente afirmar algo como: o conjunto dos números reais é o conjunto formado pelos números decimais, se a parte decimal do número for periódica, então é um racional; se a parte decimal não for periódica, então é um irracional. Em geral, é desse último modo que os estudantes têm seu primeiro contato com os números reais. Já num nível universitário, por exemplo, quando o aluno começa o estudo do Cálculo Diferencial e Integral, os reais costumam ser definidos axiomaticamente. Desse modo, não precisamos nos preocupar em demonstrar sua existência. Aliás, é esse o caminho recomendado para qualquer estudante.

Entretanto, é válido sim se questionar sobre a existência desse tal conjunto definido apenas axiomaticamente. Como demonstrar que esse conjunto existe? E se ele existe,

é único? Existem outros corpos ordenados e completos? Nas próximas seções deste capítulo serão respondidas essas questões.

Para iniciar o estudo dos números reais, primeiramente adotaremos a forma sintética. Isto é, apresentaremos os números reais como um conjunto gozando de certas propriedades ou axiomas. Feito isso, teremos claro quais são as propriedades que devemos procurar, quando de fato estivermos construindo o conjunto dos números reais.

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

Os elementos de $\mathbb{R}$ são chamados *números reais*.
O Axioma Fundamental nos diz que em $\mathbb{R}$ existem duas operações binárias $+ : \mathbb{R}\times\mathbb{R}\to\mathbb{R}$; $\cdot : \mathbb{R}\times\mathbb{R}\to\mathbb{R}$ e um conjunto de positivos P, com os seguintes treze axiomas

A. Axiomas de Corpo. *Para $x, y, z \in \mathbb{R}$ temos*

(A.1) $x + y = y + x$.

(A.2) $(x + y) + z = x + (y + z)$.

(A.3) $\exists\, 0 \in \mathbb{R}$ *tal que* $x + 0 = x, \forall x \in \mathbb{R}$.

(A.4) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ *tal que* $x + y = 0$.

(A.5) $xy = yx$.

(A.6) $(xy)z = x(yz)$.

(A.7) $\exists\, 1 \in \mathbb{R}$ *tal que* $1 \neq 0$ *e* $x \cdot 1 = x, \forall x \in \mathbb{R}$.

(A.8) $\forall x \in \mathbb{R} - \{0\}, \exists y \in \mathbb{R}$ *tal que* $xy = 1$.

(A.9) $x(y + z) = xy + xz$.

B. Axiomas de Ordem. *Existe um conjunto $P \subset \mathbb{R}$ tal que*

(B.1) $x, y \in P \Rightarrow x + y \in P$.

(B.2) $x, y \in P \Rightarrow xy \in P$.

(B.3) $\forall x \in \mathbb{R} \Rightarrow$ *ou* $-x \in P$ *ou* $x = 0$ *ou* $x \in P$.

C. Axioma de Completitude. *Todo subconjunto não vazio de $\mathbb{R}$, limitado superiormente, possui supremo.*

A partir desses axiomas é possível derivar todas as propriedades conhecidas de $\mathbb{R}$. Veja a seção 1.4 do capítulo 1.

6.2 A construção de Cantor (sequências de Cauchy)

Suponha que os números racionais e suas propriedades são conhecidos. No método de Cantor, cada número real é definido como uma classe de equivalência de sequências de Cauchy de números racionais. Assim, primeiramente definiremos sequência de números racionais, sequência de Cauchy e seguiremos a construção dos números reais por sequências de Cauchy, conforme feita em Kemp(2014) [17].

Definição 6.1. Uma *sequência de números racionais* (ou uma *sequência racional*) é uma função $x : \mathbb{N} \to \mathbb{Q}$. Para cada $n \in \mathbb{N}$ o valor $x(n) \in \mathbb{R}$ representamos por x_n e chamamos *termo de ordem n* da sequência x.

A sequência x também representamos por $(x_1, x_2, \ldots, x_n, \ldots)$ ou $(x_n)_{n\in\mathbb{N}}$ ou (x_n).

Definição 6.2. Seja (x_n) uma sequência de números racionais. Ela se chama uma *sequência de Cauchy* se, dado arbitrariamente um número racional $\omega > 0$, pode-se obter $n_0 \in \mathbb{N}$ tal que $m, n > n_0$ implicam $|x_m - x_n| < \omega$.

Definição 6.3. Uma sequência (x_n) de números racionais é dita ser *convergente em* $\mathbb{Q}$ se existe $L \in \mathbb{Q}$ tal que, para todo $\omega > 0$, existe $n_0 \in \mathbb{N}$ com a propriedade, $|x_n - L| < \omega, \forall n > n_0$.

O número L definido acima, se existir, será chamado de *limite da sequência* (x_n). Neste caso, diremos que a sequência (x_n) *converge* para L e indicaremos por $x_n \to L$.

Exemplo 6.1. A sequência de números racionais (x_n) definida por $x_n = 1/n$ converge para zero. De fato, dado $\omega > 0$ em $\mathbb{Q}$, tome n_0 inteiro com $n_0 > \frac{1}{\omega}$, (isto é possível pela propriedade arquimediana de $\mathbb{Q}$). Então, para $n > n_0$, temos que:

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} < \frac{1}{n_0} < \omega.$$

Definição 6.4. Seja (x_n) uma sequência de números racionais. Dizemos que (x_n) *tende a 0* se, dado arbitrariamente $\omega > 0$, existe $n_0 \in \mathbb{N}$ tal que $n > n_0$ implica $|x_n| < \omega$. Simbolicamente, denotamos $x_n \to 0$.

Para que (x_n) seja uma sequência de Cauchy, é preciso que seus termos x_m, x_n, para valores suficientemente grandes dos índices m, n se aproximem arbitrariamente uns dos outros. Ou seja, se impõe uma condição sobre os termos da própria sequência. Uma sequência de Cauchy também é chamada *sequência fundamental*.

Note que existem tantas sequências de Cauchy quantos são os números racionais, pois, qualquer que seja o número racional r, a sequência constante $(r_n) = (r, r, r, \ldots)$ é de Cauchy. Dentre as sequências de Cauchy, algumas são convergentes: como as sequências constantes; uma como $(1/2, 2/3, 3/4, \ldots)$ e uma infinidade de outras mais. Mas há também uma infinidade de sequências de Cauchy que não convergem, como a sequência das aproximações decimais de π,

$$(r_n) = (3,\ 3.1,\ 3.14,\ 3.141,\ 3.1415,\ 3.14159, \ldots), \tag{1}$$

ou a sequência $x_n = (1+1/n)^n$, que converge a $e = 2.718281\ldots$, ou ainda, a sequência $(y_n) = (1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ldots)$, que aproxima $\sqrt{2}$ por falta.

Essas sequências não convergem em $\mathbb{Q}$ pois π, e ou $\sqrt{2}$ não são racionais. Na construção dos números reais, a ideia de Cantor é definir os reais como o conjunto de todas as sequências de aproximações racionais e definir operações algébricas e ordenação linear para essas sequências.

Vejamos alguns resultados envolvendo sequências de Cauchy de números racionais.

Teorema 6.1. *Se (x_n) é uma sequência convergente de números racionais (i.e., $x_n \to r$, para algum número racional r) então (x_n) é uma sequência de Cauchy.*

Demonstração. Temos que $x_n \to r$. Dado $\omega > 0$, existe $n_0 \in N$ tal que $n > n_0 \Rightarrow |x_n - r| < \omega/2$. Então, se $m, n > n_0$, temos

$$|x_n - x_m| = |(x_n - r) + (x_m - r)| \leq |x_n - r| + |x_m - r| < \frac{\omega}{2} + \frac{\omega}{2} = \omega.$$

Portanto, (x_n) é uma sequência de Cauchy. □

Intuitivamente: se para valores grandes de n, os termos (x_n) se aproximam de r, então eles devem necessariamente aproximar-se uns dos outros. É natural pensar que se os termos estão mais próximos uns dos outros então eles devem estar próximos de algum número. Esta intuição motivou Cauchy a usar sequências para definir os números reais. Embora a sequência 3, 3.1, 3.14, 3.141, 3.1415, 3.14159,... seja de Cauchy ela não converge para um número racional; portanto, deve haver algum número irracional para o qual ela convirja. Desse modo, completaremos os racionais adicionando esse número.

O teorema seguinte nos mostra que mesmo que uma sequência de Cauchy não convirja, ela não pode se tornar arbitrariamente grande.

Teorema 6.2. *Se (x_n) é uma sequência de Cauchy, então ela é limitada; isto é, existe algum $M > 0$ tal que $|x_n| \leq M$ para todo n.*

Demonstração. Seja (x_n) uma sequência de Cauchy. Tomando $\omega = 1$, obtemos $n_0 \in \mathbb{N}$ tal que $m, n \geq n_0 \Rightarrow |x_m - x_n| < 1$. Em particular, $n \geq n_0 \Rightarrow |x_{n_0} - x_n| < 1$, ou seja, $n \geq n_0 \Rightarrow x_n \in (x_{n_0} - 1, x_{n_0} + 1)$. Sejam α o menor e β o maior elemento do conjunto $X = \{x_1, x_2, \ldots, x_{n_0} - 1, x_{n_0} + 1\}$. Então $x_n \in [\alpha, \beta]$ para cada $n \in \mathbb{N}$, logo (x_n) é limitada. □

Deve-se observar que diferentes sequências definem o mesmo número irracional. Por exemplo, a sequência racional

$$(q_n) = \left(3, \frac{22}{7}, \frac{333}{106}, \frac{355}{1}, \frac{103993}{33102}, \ldots\right),$$

também aproxima π. A sequência das aproximações decimais por excesso de $\sqrt{2}$, define $\sqrt{2}$. Para lidar com esse problema, uma relação de equivalência é imposta no conjunto das sequências. Ou seja, todas as sequências que têm o mesmo limite devem

pertencer a mesma classe. Em seguida, uma estrutura de corpo é construída.

Definiremos uma relação de equivalência no conjunto das sequências de Cauchy. Para a definição e propriedades das relações de equivalência veja a seção 1.2

Definição 6.5. Sejam as sequências de Cauchy de números racionais $x = (x_n)$ e $y = (y_n)$. No conjunto das sequências de Cauchy racionais, definimos a relação $\sim$ como

$$x \sim y \Leftrightarrow (x_n - y_n) \to 0.$$

Teorema 6.3. *A relação $\sim$ definida no conjunto das de sequências de Cauchy de números racionais é uma relação de equivalência.*

Demonstração. Vamos provar que esta relação é reflexiva, simétrica e transitiva.

(a) Reflexiva: $x_n - x_n = 0$, e a sequência cujos termos são 0 claramente converge para 0. Logo, $x \sim x$.

(b) Simétrica: Suponha $x \sim y$, então $x_n - y_n \to 0$. Mas $y_n - x_n = -(x_n - y_n)$, e, $|y_n - x_n| = |x_n - y_n|$, logo, $y_n - x_n \to 0$, isto é, $y \sim x$.

(c) Transitiva: Suponha que $x \sim y$ e $y \sim z$. Isto significa que $x_n - y_n \to 0$ e $y_n - z_n \to 0$. Dado $\omega > 0$, existe $n_1 \in \mathbb{N}$ tal que $|x_n - y_n| < \omega/2$ para todo $n > n_1$. Também existe $n_2 \in \mathbb{N}$ tal que $|y_n - z_n| < \omega/2$ para todo $n > n_2$. Seja $n_0 = \max\{n_1, n_2\}$, então para todo $n > n_0$, temos

$$|x_n - z_n| = |(x_n - y_n) + (y_n - z_n)| \leq |x_n - y_n| + |y_n - z_n| < \frac{\omega}{2} + \frac{\omega}{2} = \omega.$$

Portanto, $x_n - z_n \to 0$, isto é, $x \sim z$.

□

Definição 6.6. *O conjunto dos números reais* $\mathbb{R}$ é o conjunto das classes de equivalência $[(x_n)]$ das sequências de Cauchy de números racionais. Isto é, cada classe de equivalência é um número real.

Note que o conjunto dos números racionais $\mathbb{Q}$ estão contidos em $\mathbb{R}$ como sequências constantes. Isto é, um número racional qualquer r, está representado em $\mathbb{R}$ como a classe de equivalência $[r]$ da sequência constante $(r, r, r, \ldots)$.

Considere a classe à qual pertencem as sequências que aproximam π. É fácil perceber que nenhuma sequência $r_n = r$, com r racional, pode pertencer a essa classe, senão $r - r_n$ teria de tender a zero, o que é impossível. Essas classes que não contém sequências do tipo $r_n = r$ são precisamente aquelas que corresponderão aos números irracionais a serem criados.

É preciso determinar a estrutura algébrica de $\mathbb{R}$. Para isso, definiremos na classe de equivalências as operações de adição e multiplicação, e suas inversas, a subtração e a divisão; quem é o elemento neutro 0 e o 1 e, determinar quando uma classe de equivalência é menor do que outra. Ou seja, definir uma relação de ordem.

Definição 6.7 (adição e multiplicação)**.** Sejam $s, t \in \mathbb{R}$. Então existem sequências de Cauchy $(x_n), (y_n)$ de números racionais com $s = [(x_n)]$ e $t = [(y_n)]$.

(a) $s + t$ é a classe de equivalência da sequência $(x_n + y_n)$.

(b) $s \cdot t$ é a classe de equivalência da sequência $(x_n \cdot y_n)$.

Precisamos verificar que as operações de adição e multiplicação no conjunto de classes de equivalência está bem definida. Isto é feito no teorema a seguir, o qual mostra que sequências equivalentes adicionadas a sequências equivalentes são equivalentes e sequências equivalentes multiplicadas por sequências equivalentes são equivalentes.

Teorema 6.4. *Se (x_n) e (x'_n) são sequências de Cauchy equivalentes, da mesma forma que (y_n) e (y'_n), então $(x_n) + (y_n)$ e $(x'_n) + (y'_n)$ são equivalentes, do mesmo modo que, $(x_n) \cdot (y_n)$ e $(x'_n) \cdot (y'_n)$ são equivalentes.*

Demonstração. Temos $[(x_n)] = [(x'_n)]$ e $[(y_n)] = [(y'_n)]$. Assim, $x_n - x'_n \to 0$ e $y_n - y'_n \to 0$. Então $(x_n + y_n) - (x'_n + y'_n) = (x_n - x'_n) + (y_n - y'_n)$. É fácil perceber que $(x_n - y_n) + (x'_n - y'_n) \to 0$ e, portanto, $[(x_n + y_n)] = [(x'_n + y'_n)]$.

Queremos mostrar que $[(x_n)(y_n)] = [(x'_n)(y'_n)]$, isto é, $x_n y_n - x'_n y'_n \to 0$.
Assim,

$$\begin{aligned} x_n \cdot y_n - x'_n \cdot y'_n &= x_n \cdot y_n + (y_n \cdot x'_n - y_n \cdot x'_n) - x'_n \cdot y'_n \\ &= (x_n \cdot y_n - y_n \cdot x'_n) + (y_n \cdot x'_n - x'_n \cdot y'_n) \\ &= y_n \cdot (x_n - x'_n) + x'_n \cdot (y_n - y'_n). \end{aligned}$$

Portanto, $|x_n \cdot y_n - x'_n \cdot y'_n| \leq |y_n| \cdot |x_n - x'_n| + |x'_n| \cdot |y_n - y'_n|$. Pelo teorema 6.2, existem M, L tais que $|y_n| \leq M$ e $|x'_n| \leq L$, para todo n. Tomando R (por exemplo, $R = M + L$) maior do que M e L, temos:

$$|x_n \cdot y_n - x'_n \cdot y'_n| \leq |y_n| \cdot |x_n - x'_n| + |x'_n| \cdot |y_n - y'_n| \leq R \cdot (|x_n - x'_n| + |y_n - y'_n|).$$

Como $x_n - x'_n \to 0$ e $y_n - y'_n \to 0$, então $x_n \cdot y_n - x'_n \cdot y'_n \to 0$. □

Portanto, as duas operações, $+$ e $\cdot$, estão bem definidas. É preciso mostrar que $\mathbb{R}$, equipado com essas operações, é um corpo.

Lema 6.1. *Se (x_n) é uma sequência de Cauchy que não tende a 0, então existe um $n_0 \in \mathbb{N}$ tal que para $n > n_0$, $x_n \neq 0$.*

Teorema 6.5. *Dado qualquer número real $s \neq 0$, existe um número real t tal que $s \cdot t = 1$.*

Demonstração. Temos $s \neq 0$, isto significa que s não está na classe de equivalência de $(0, 0, 0, \ldots)$. Em outras palavras, $s = [(x_n)]$ onde $x_n - 0$ não converge para 0. Devemos mostrar que existe um número real $t = [(y_n)]$ tal que $s \cdot t = [(x_n \cdot y_n)]$ é a mesma classe de equivalência de $[(1, 1, 1, \ldots)]$. Isto decorre do fato de que números racionais não nulos possuem inversos multiplicativos. Como $x_n - 0$ não converge para 0, pelo lema anterior, existe n_0 tal que $x_n \neq 0$, para $n > n_0$. Defina uma

sequência (y_n) de números racionais onde $y_n = 0$, para $n \leq n_0$ e $y_n = 1/x_n$, para $n > n_0; (y_n) = (0, 0, \ldots, 0, 1/x_{n_0+1}, 1/x_{n_0+2}, \ldots)$. Então $x_n \cdot y_n$ é igual a $x_n \cdot 0 = 0$ para $n \leq n_0$ e igual a $x_n \cdot y_n = x_n \cdot 1/x_n = 1$ para $n > n_0$. Observando a sequência $(1, 1, 1, \ldots)$, temos que $(1, 1, 1, \ldots) - (x_n \cdot y_n)$ é a sequência a qual é $1 - 0 = 1$ para $n \leq n_0$ e igual a $1 - 1 = 0$, para $n > n_0$. Desde que esta sequência é a partir de n_{0+1} igual a 0, ela converge para 0 e então $[(x_n \cdot y_n)] = [(1, 1, 1, \ldots)] = 1 \in \mathbb{R}$. Isto mostra que $t = [(y_n)]$ é o inverso multiplicativo de $s = [(x_n)]$. □

Teorema 6.6. $\mathbb{R}$ *é um corpo.*

A demonstração fica como exercício. Basta mostrar a definição e propriedades de um corpo para o conjunto das classes de equivalência das sequências de Cauchy de números racionais. Após mostrar que $(\mathbb{R}, +, .)$ é um corpo, o próximo passo consiste em mostrar que $\mathbb{R}$ é um corpo ordenado, isto é, que existe uma relação de ordem $<$ em $\mathbb{R}$ que respeita as operações de corpo. Definiremos o conceito de uma sequência positiva e de classes de equivalência de sequências positivas.

Definição 6.8. Uma sequência de Cauchy de números racionais (x_n) é chamada *positiva* se existem inteiros positivos M e n_0 tais que, se $n > n_0$ então $x_n > 1/M$. Se $s \in \mathbb{R}$, dizemos que s é *positivo* se uma das sequências em s é positiva. Dados dois números reais s, t, dizemos que $s > t$ se $s - t$ é positiva.

A boa definição dessas relações de ordem definidas é garantida pelo próximo teorema.

Teorema 6.7. *Se uma sequência de Cauchy na classe de equivalência de s no final tem apenas termos positivos, então qualquer outra sequência de Cauchy na mesma classe de equivalência no final tem apenas termos positivos.*

Fica a cargo o leitor, verificar que todos os axiomas de ordem valem para $\mathbb{R}$. Mostraremos apenas uma propriedade e as demonstrações das demais são similares.

Teorema 6.8. $\mathbb{R}$ *é um corpo ordenado.*

Teorema 6.9. *Considere s, t números reais tais que $s > t$, e seja $r \in \mathbb{R}$. Então $s + r > t + r$.*

Demonstração. Seja $s = [(x_n)], t = [(y_n)]$, e $r = [(z_n)]$. Como $s > t$, isto é, $s - t > 0$, então existe um n_0 tal que, para $n > n_0$, $x_n - y_n > 0$. Assim, $x_n > y_n$ para $n > n_0$. Adicionando z_n a ambos os lados desta desigualdade (pois isto pode ser feito para números racionais), obtemos $x_n + z_n > y_n + z_n$ para $n > n_0$, ou $(x_n + z_n) - (y_n + z_n) > 0$ para $n > n_0$. Note também que $(x_n + z_n) - (y_n + z_n) = x_n - y_n$ não converge para zero, pois, por hipótese, $s - t > 0$. Portanto, pela definição de número real positivo, $s + r = [(x_n + z_n)] > [(y_n + z_n)] = t + r$. □

Vamos provar que $\mathbb{R}$ é um corpo arquimediano. Em seguida, mostraremos que $\mathbb{R}$ possui a propriedade da menor cota superior, característica que o distingue de $\mathbb{Q}$.

Teorema 6.10. $\mathbb{R}$ *tem a propriedade arquimediana. Isto é, existe $m, n_0 \in \mathbb{N}$ tal que $mx_n > y_n$ para todo $n > n_0$.*

Demonstração. Sejam s, t números reais. Vamos obter um número natural m tal que $m.s > t$. Neste contexto, $m = [(m, m, m, \ldots)]$. Considere ainda $s = [(x_n)]$ e $t = [(y_n)]$. Vamos provar que existe m tal que

$$[(m, m, m, \ldots)].[(x_1, x_2, x_3, x_4, \ldots)] = [(mx_1, mx_2, mx_3, mx_4, \ldots)] > [(y_1, y_2, y_3, y_4, \ldots)].$$

Para mostrar que $[(mx_n)] > [(y_n)]$, ou $[(mx_n - y_n)]$ é positiva, basta mostrar que existe um n_0 tal que $mx_n - y_n > 0$ para todo $n > n_0$, e que $mx_n - y_n \nrightarrow 0$.

Suponha, por absurdo, que para todo m e n_0, existe um $n > n_0$ tal que $mx_n \leq y_n$. Como (y_n) é uma sequência de Cauchy, é limitada, isto é, existe um número racional M tal que $y_n \leq M$ para todo n. Pela propriedade arquimediana para números racionais, dado qualquer número racional pequeno $\omega > 0$ existe um m tal que $M/m < \omega/2$. Fixemos tal m. Então, se $mx_n \leq y_n$, temos $x_n \leq y_n/m \leq M/m < \omega/2$.

Como (x_n) é uma sequência de Cauchy, existe n_0 tal que para $n, k > n_0$, $|x_n - x_k| < \omega/2$. Por hipótese, assumimos que para $n > n_0$ temos $mx_n \leq y_n$, o que significa que $x_n < \omega/2$. Mas, para todo $k > n_0$, temos $x_k - x_n < \omega/2$, assim, $x_k < x_n + \omega/2 < \omega/2 + \omega/2 = \omega$. Portanto, $x_k < \omega$ para todo $k > n_0$. Isto prova que $x_k \to 0$, o que contradiz o fato de que $[(x_n)] = s > 0$.

Portanto, existe de fato algum $m \in \mathbb{N}$ tal que $mx_n - y_n > 0$ para todo n suficientemente grande. Para concluir, devemos mostrar que $mx_n - y_n \nrightarrow 0$. Na verdade, é possível que $mx_n - y_n \to 0$ (por exemplo, se $(x_n) = (1, 1, 1, \ldots)$ e $(y_n) = (m, m, m, \ldots)$). Neste caso, basta simplesmente tomar um valor grande para m. Isto é, seja m um número natural qualquer obtido como descrito anteriormente, de modo que $mx_n - y_n > 0$ para todo n suficientemente grande. Se é verdade que $mx_n - y_n \nrightarrow 0$, então a demonstração está completa. Por outro lado, se $mx_n - y_n \to 0$, então toma-se o inteiro $m + 1$. Desde que $s = [(x_n)] > 0$, temos $x_n > 0$ para n grande, então $(m+1)x_n - y_n = mx_n - y_n + x_n > x_n > 0$ para todo n grande, então $m + 1$ funciona tão bem quanto m; e, desde que $mx_n - y_n \to 0$, temos $(m+1)x_n - y_n = (mx_n - y_n) + x_n \nrightarrow 0$ desde que $s = [(x_n)] > 0$ (então $x_n \nrightarrow 0$).

□

A seguir, mostramos que $\mathbb{Q}$ é denso em $\mathbb{R}$.

Teorema 6.11. *Dado qualquer número real r, e qualquer número racional (pequeno) $\omega > 0$, existe um número racional q tal que $|r - q| < \omega$.*

Demonstração. O número real r é representado por uma sequência de Cauchy $(x_1, x_2, x_3, \ldots)$. Como esta sequência é de Cauchy, dado ω, existe n_0 tal que, para todo $m, n > n_0$, $|x_m - x_n| < \omega$. Tome algum $l > n_0$ fixo, podemos tomar o número racional q dado por $q = [(x_l, x_l, x_l, \ldots)]$. Então temos $r - q = [(x_n - x_l)_{n=1}^{\infty}]$, e $q - r = [(x_l - x_n)_{n=1}^{\infty}]$. Desde que $l > n_0$, para $n > n_0$, temos $x_n - x_l < \omega$ e $x_l - x_n < \omega$, o que significa que $r - q < \omega$ e $q - r < \omega$; portanto, $|r - q| < \omega$.

□

Antes de mostrar que $\mathbb{R}$ é completo, precisamos mostrar alguns resultados que nos auxiliarão nessa demonstração.

Sejam $S \subset \mathbb{R}$ um subconjunto não vazio e M uma cota superior para S. Vamos construir duas sequências de números reais (u_n) e (l_n). Como S é não vazio, existe algum elemento $s_0 \in S$. Usaremos indução para obter os elementos das sequências (u_n) e (l_n).

- Seja $u_0 = M$ e $l_0 = s_0$;
- Suponha que já definimos u_n e l_n. Considere o número $m_n = (u_n + l_n)/2$, a média entre u_n e l_n.
- Se m_n é uma cota superior para S, defina $u_{n+1} = m_n$ e $l_{n+1} = l_n$;
- Se m_n não é uma cota superior para S, defina $u_{n+1} = u_n$ e $l_{n+1} = m_n$;

Como $s_0 < M$, é fácil provar por indução que (u_n) é uma sequência não-crescente $(u_{n+1} \leq u_n)$e (l_n) é uma sequência não-decrescente $(l_{n+1} \geq l_n)$.

Lema 6.2. *(u_n) e (l_n) como definidos anteriormente são sequências de Cauchy de números reais.*

Demonstração. Note que $l_n \leq M$ para todo n. Como (l_n) é não-decrescente, temos que (l_n) é de Cauchy. Para (u_n), temos $u_n \geq s_0$, para todo n, e então $-u_n \leq -s_0$. Como (u_n) é não-crescente, $(-u_n)$ é não-decrescente, e, como já vimos, $(-u_n)$ é de Cauchy. Logo, é fácil verificar que (u_n) é de Cauchy. □

Lema 6.3. *Existe um número real u tal que $u_n \to u$.*

Demonstração. Fixe um termo u_n na sequência (u_n). Pelo teorema 6.11, existe um número racional q_n tal que $|u_n - q_n| < 1/n$. Considere a sequência $(q_1, q_2, q_3, \ldots)$ de números racionais. Mostraremos que esta sequência é de Cauchy. Fixe $\omega > 0$. Pela propriedade arquimediana, escolha N tal que $1/N < \omega/3$. Como (u_n) é de Cauchy, existe $n, m > M; |u_n - u_m| < \omega/3$. Então, contanto que $n, m > \max\{N, M\}$, temos:

$|q_n - q_m| = |(q_n - u_n) + (u_n - u_m) + (u_m - q_m)| \leq |q_n - u_n| + |u_n - u_m| + |u_m - q_m| < \frac{\omega}{3} + \frac{\omega}{3} + \frac{\omega}{3} = \omega$.

Portanto, (q_n) é uma sequência de Cauchy de números racionais, logo, representa um número real $u = [(q_n)]$. Devemos mostrar que $u_n - u \to 0$, mas isto é praticamente construído na definição de u. Para ser preciso, considere $\widetilde{q_n}$ um número real $[(q_n, q_n, q_n, \ldots)]$, vemos que $\widetilde{q_n} - u \to 0$. Mas, $u_n - \widetilde{q_n} < 1/n$ por construção. Logo, se $\widetilde{q_n} \to u$ e $u_n - \widetilde{q_n} \to 0$, então $u_n \to u$. □

Temos que (u_n) é uma sequência não-crescente de cotas superiores para S, tende a um número real u, o qual é a menor cota superior para o conjunto S, conforme demonstrado no lema seguinte.

Lema 6.4. $l_n \to u$.

Demonstração. Note que no primeiro caso acima, temos

$$u_{n+1} - l_{n+1} = m_n - l_n = \frac{u_n + l_n}{2} - l_n = \frac{u_n - l_n}{2}.$$

No segundo caso, temos:

$$u_{n+1} - l_{n+1} = u_n - m_n = u_n - \frac{u_n + l_n}{2} = \frac{u_n - l_n}{2}.$$

Isto significa que $u_1 - l_1 = \frac{1}{2}(M - s)$, e então $u_2 - l_2 = \frac{1}{2}(u_1 - l_1) = \left(\frac{1}{2}\right)^2 (M - s)$, e, pode-se provar por indução que, $u_n - l_n = 2^{-n}(M - s)$. Desde que $M > s$ temos $M - s > 0$, e desde que $2^{-n} < 1/n$, pela propriedade arquimediana para $\mathbb{R}$, temos que para qualquer $\omega > 0, 2^{-n}(M - s) < \omega$ para todo n suficientemente grande. Portanto, $u_n - l_n < 2^{-n}(M - s) < \omega$ e, então $u_n - l_n \to 0$. Logo, desde que $u_n \to u$, temos também $l_n \to u$.

□

Teorema 6.12. $\mathbb{R}$ *tem a propriedade da menor cota superior.*

Demonstração. Primeiramente, devemos mostrar que u é uma cota superior. Suponha, por absurdo, que u não é cota superior. Assim, $u < s$, para algum $s \in S$. Então $\omega \equiv s - u$ é > 0 e, desde que $u_n \to u$ e é não-crescente, deve haver um n tal que $u_n - u < \omega$, o que significa que $u_n < u + \omega = u + (s - u) = s$. Mas, u_n é uma cota superior para S. Contradição. Portanto, u é cota superior para S.

Sabemos também que, para cada n, l_n não é uma cota superior, significando que para cada n, existe um $s_n \in S$ tal que $l_n \leq s_n$. Pelo lema 6.4, temos que $l_n \to u$, e, como a sequência (l_n) é não-decrescente, isto significa que para cada $\omega > 0$, existe um n_0 tal que, para $n > n_0, l_n > u - \omega$. Portanto, para $n > n_0, s_n \geq l_n > u - \omega$. Em particular, para cada $\omega > 0$, existe um $s \in S$ tal que $s > u - \omega$. Isto significa que nenhum número menor do que u pode ser uma cota superior para S. Portanto, u é a menor cota superior para S, isto é, sup s existe. □

Portanto, o conjunto $\mathbb{R}$, cujos elementos são classes de equivalência de sequências racionais de Cauchy é um corpo ordenado e completo.

6.3 O método de Dedekind (cortes de Dedekind)

Richard Dedekind (1831-1916) na metade do século XIX, ao preparar suas aulas de Cálculo Diferencial e tentar demonstrar que toda sequência monótona limitada é convergente, percebeu a necessidade de uma fundamentação adequada de número real. Ele foi buscar inspiração para sua construção dos números reais na teoria de proporções de Eudoxo. Para entender essa construção, vamos considerar conhecidos os números racionais e seguir os passos dados no livro de Rudin (1971) [28]. Neste método, os elementos de $\mathbb{R}$ são certos subconjuntos de $\mathbb{Q}$, chamados cortes.

Cortes de Dedekind

Definição 6.9. Diz-se que um conjunto α de números racionais é um corte se:

(i) $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$;

(ii) Seja $q \in \mathbb{Q}$. Se $p \in \alpha$ e $q < p$ então $q \in \alpha$.

(iii) Se $p \in \alpha$ então $p < r$, para algum $r \in \alpha$.

A primeira afirmação implica que α contém pelo menos um racional, mas não todos. A segunda afirma que todo número racional do conjunto é menor do que todo número racional que não pertence ao conjunto. A última implica que, em α, não existe racional máximo.

Notação: As letras $p, q, r, \ldots$ denotam números racionais e $\alpha, \beta, \gamma, \ldots$ denotam cortes.

Exemplo 6.2. Qualquer número racional r determina um corte em que α é o conjunto de todos os números racionais menores do que r.

É claro que α satisfaz os itens (i) e (ii) da definição 6.9. Para provar o item (iii), basta observar que qualquer que seja $p \in \alpha$, tem-se

$$p < \frac{p+r}{2} < r,$$

e, portanto, $(p+r)/2 \in \alpha$.

Note que $r \notin \alpha$. Este corte dado pelo exemplo 6.2 é chamado corte racional. Para indicar que um corte α é o corte racional relacionado a r escreveremos $\alpha = r^*$.

Teorema 6.13. *Se $p \in \alpha$ e $q \notin \alpha$, então $p < q$.*

Demonstração. Suponha que $p \in \alpha$ e $q \leq p$, conclui-se de (ii) que $q \in \alpha$. Contradição. Logo, $p < q$. □

Os elementos de α são, às vezes, chamados números inferiores de α e os números racionais que não estão em α são chamados números superiores de α. No exemplo 6.2, r é o número superior mínimo de α.

Uma vez entendido o conceito de corte, é preciso definir ordem, isto é, o que significa um corte ser menor do que outro; definir adição e multiplicação de cortes e demonstrar as propriedades para essas operações com base nas propriedades já estabelecidas para os racionais.

Definição 6.10. Sejam α, β cortes. Escrevemos $\alpha = \beta$ se de $p \in \alpha$ resulta $p \in \beta$ e de $q \in \beta$ resulta $q \in \alpha$, isto é, se os dois conjuntos são idênticos. Caso contrário, escrevemos $\alpha \neq \beta$.

Observação. A igualdade nem sempre é identidade. Por exemplo, dados dois racionais $p = a/b$ e $q = c/d$, onde $a, b, c, d \in \mathbb{Z}, p = q$ significa $ad = bc$ e não necessariamente $a = c$ e $b = d$.

Definição 6.11. Sejam α, β cortes. Escrevemos $\alpha < \beta$(ou $\beta > \alpha$) para significar que α é subconjunto próprio de β, isto é, existe um racional p tal que $p \in \beta$ e $p \notin \alpha$.

Observação.

1. $\alpha \leq \beta$ significa $\alpha = \beta$ ou $\alpha < \beta$.
2. $\alpha \geq \beta$ significa $\beta \leq \alpha$.
3. Se $\alpha > 0^*$, dizemos que α é positivo; se $\alpha \geq 0^*$, dizemos que α não é negativo. Analogamente, se $\alpha < 0^*$, α é negativo, e se $\alpha \leq 0^*$, α não é positivo.

Teorema 6.14. *Sejam α, β cortes. Então $\alpha = \beta$ ou $\alpha < \beta$ ou $\beta < \alpha$.*

Demonstração. Pelas definições 6.10, 6.11, se $\alpha = \beta$ então nenhuma das outras duas relações é válida. Vamos mostrar que $\alpha < \beta$ e $\beta < \alpha$ se excluem mutuamente. Para isso, suponha que ambas as relações sejam válidas. Como $\alpha < \beta$, existe um racional p tal que $p \in \beta$ e $p \notin \alpha$. Como $\beta < \alpha$, existe um racional q tal que $q \in \alpha$ e $q \notin \beta$. Pelo teorema 6.13,de $p \in \beta$ e $q \notin \beta$ resulta $p < q$, enquanto que, $q \in \alpha$ e $p \notin \alpha$ resulta $q < p$. Contradição, pois não pode ser $p < q$ e $q < p$. Assim, provamos que, no máximo, uma das três relações é válida. Suponhamos que $\alpha \neq \beta$. Então, ou existe um número racional p em α mas não em β e, neste caso, $\beta < \alpha$ ou existe um racional q em β, mas não em α, e, neste caso, $\alpha < \beta$. □

Teorema 6.15. *Sejam α, β, γ cortes. Se $\alpha < \beta$ e $\beta < \gamma$, então $\alpha < \gamma$.*

Demonstração. Como $\alpha < \beta$, existe um racional p tal que $p \in \beta$ e $p \notin \alpha$. Como $\beta < \gamma$, existe um racional q tal que $q \in \gamma$ e $q \notin \beta$. Mas, se $p \in \beta$ e $q \notin \beta$ então $p < q$. Como $p \notin \alpha$, então $q \notin \alpha$. Logo, $q \in \gamma$ e $q \notin \alpha$, o que significa que $\alpha < \gamma$. □

Portanto, o conjunto de cortes é um conjunto ordenado. Vamos definir a adição nesse conjunto.

Teorema 6.16. *Sejam α, β cortes. Seja γ o conjunto de todos os racionais r tais que $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Então γ é um corte.*

Demonstração. Precisamos provar que γ cumpre as três condições da definição 6.9.

(i) É claro que γ é não vazio. Consideremos $s \notin \alpha, t \notin \beta$, onde $s, t \in \mathbb{Q}$. Temos que $s > p$, para todo $p \in \alpha$ e $t > q$, para todo $q \in \beta$. Assim, $s + t > p + q$ e $s + t \notin \gamma$. Logo, γ não contém todos os racionais.

(ii) Suponhamos $r \in \gamma, s < r$, sendo s racional. Logo, $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Como $s < r$, temos que $s - q < p$, assim, $s - q \in \alpha$ e $s = (s - q) + q \in \alpha + \beta$.

(iii) Suponhamos $r \in \gamma$. Logo, $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Existe um racional $s > p$ tal que $s \in \alpha$. Portanto, $s + q > r$ e r não é o maior racional em γ.

□

Definição 6.12. Se α, β são cortes, então

$$\gamma = \alpha + \beta = \{r + s; r \in \alpha \text{ e } s \in \beta\}$$

é um corte e chama-se soma de α e β.

Vejamos algumas propriedades da operação de adição no conjunto dos cortes.

Teorema 6.17. *Sejam α, β, γ cortes. Então,*

(i) $\alpha + \beta = \beta + \alpha$;

(ii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

(iii) $\alpha + 0^* = \alpha$;

Demonstração.

(i) $\alpha + \beta$ é o conjunto de todos os racionais da forma $p + q$, onde $p \in \alpha$ e $q \in \beta$. Na definição de $\beta + \alpha$, consideramos $q + p$, em vez de $p + q$. Pela comutatividade da adição de racionais, $p + q = q + p$. Portanto, $\alpha + \beta = \beta + \alpha$.

(ii) resultado da propriedade associativa da adição de números racionais.

(iii) Seja $r \in \alpha + 0^*$. Logo, $r = p + q$ com $p \in \alpha$ e $q \in 0^*$(isto é, $q < 0$). Assim, $p + q < p$, de modo que, $p + q \in \alpha$ e $r \in \alpha$. Portanto, $\alpha + 0^* \subset \alpha$.

A seguir, suponhamos $r \in \alpha$ e tomemos $s \in \alpha$ com $s > r$. Então, $r - s \in 0^*$, e $r = s + (r - s) \in \alpha + 0^*$. Portanto, $\alpha \subset \alpha + 0^*$. Assim, $\alpha + 0^* = \alpha$.

□

Teorema 6.18. *Seja α um corte e $r > 0$ um racional dado. Existem racionais p, q tais que $p \in \alpha, q \notin \alpha, q$ não é o número superior mínimo de α e $q - p = r$.*

Demonstração. Consideremos um racional $s \in \alpha$. Para $n = 0, 1, 2, \ldots$ seja $s_n = s + nr$. Então existe um único inteiro m tal que $s_m \in \alpha$ e $s_{m+1} \notin \alpha$. Se s_{m+1} não for o número superior mínimo de α, consideremos $p = s_m, q = s_{m+1}$.

Se s_{m+1} for o número superior mínimo de α, consideremos
$p = s_m + \frac{r}{2},\ q = s_{m+1} + \frac{r}{2}$. □

Teorema 6.19. *Seja α um corte. Existe um único corte β tal que $\alpha + \beta = 0^*$.*

Demonstração. Primeiramente, provaremos a unicidade. Se $\alpha + \beta_1 = \alpha + \beta_2 = 0^*$, temos das propriedades da adição de cortes que, $\beta_2 = 0^* + \beta_2 = (\alpha + \beta_1) + \beta_2 = (\alpha + \beta_2) + \beta_1 = 0^* + \beta_1 = \beta_1$.

Para provar a existência do corte, seja β o conjunto de todos os racionais p tais que $-p$ é um número superior de α, mas não o número superior mínimo. Temos que verificar que este conjunto β satisfaz as três condições da definição 6.9. A primeira condição é óbvia. Vamos provar a segunda condição. Se $p \in \beta$ e $q < p$ (q racional), então $-p \notin \alpha$ e $-q > -p$, de modo que $-q$ é um número superior de α, mas não o mínimo. Portanto, $q \in \beta$. Por fim, se $p \in \beta, -p$ é um número superior de α, mas não o mínimo, de modo que existe um racional q tal que $-q < -p$ e $-q \notin \alpha$. Seja $r = \frac{p+q}{2}$. Logo, $-q < -r < -p$, de modo que $-r$ é um número superior de α, mas não o mínimo. Portanto, encontramos um racional $r > p$ tal que $r \in \beta$, o que prova a terceira condição. Assim, mostramos que β é um corte, precisamos verificar se $\alpha + \beta = 0^*$.

Suponhamos $p \in \alpha + \beta$. Logo, $p = q + r$, com $q \in \alpha$ e $r \in \beta$. Portanto, $-r \notin \alpha, -r > q, q + r < 0$ e $p \in 0^*$.

Suponhamos $p \in 0^*$. Portanto, $p < 0$. Podemos determinar racionais $q \in \alpha, r \notin \alpha$ (e tal que r não seja o número superior mínimo de α), de modo que $r - q = -p$. Como $-r \in \beta$, temos $p = q - r = q + (-r) \in \alpha + \beta$, o que completa a demonstração.

□

Observação. Designamos por $-\alpha$ o corte β do teorema 6.19.

Teorema 6.20. *Sejam α, β, γ cortes.*

(i) *Se $\alpha + \beta = \alpha + \gamma$ então $\beta = \gamma$.*

(ii) *Se $\beta < \gamma$ então $\alpha + \beta < \alpha + \gamma$. Em particular, (para $\beta = 0^*$) temos $\alpha + \gamma > 0^*$, se $\alpha > 0^*$ e $\gamma > 0^*$.*

Demonstração.

(i) Pelo teorema 6.17, $\beta = 0^* + \beta = (-\alpha) + (\alpha + \beta) = (-\alpha) + (\alpha + \gamma) = 0^* + \gamma = \gamma$

(ii) É óbvio que $\alpha + \beta \leq \alpha + \gamma$; se $\alpha + \beta = \alpha + \gamma$, pelo item anterior, $\beta = \gamma$.

□

Teorema 6.21. *Sejam α, β cortes. Existe um único corte γ tal que $\alpha + \gamma = \beta$.*

Demonstração. Se $\gamma_1 \neq \gamma_2$ então $\alpha + \gamma_1 \neq \alpha + \gamma_2$. Assim, existe no máximo um γ nas condições enunciadas.

Seja $\gamma = \beta + (-\alpha)$, então $\alpha + \gamma = \alpha + [\beta + (-\alpha)] = \alpha + [(-\alpha) + \beta] = [\alpha + (-\alpha)] + \beta = 0^* + \beta = \beta$. □

Observação.

1. Em vez de $\beta + (-\alpha)$ escrevemos $\beta - \alpha$;
2. Pode-se verificar pelos resultados apresentados que o conjunto dos cortes é um grupo comutativo em relação à adição.

Vamos definir a multiplicação no conjunto dos cortes e mostrar que se obtém um corpo. Nessa operação temos que considerar os diferentes casos correspondentes aos sinais dos fatores em questão.

Teorema 6.22. *Sejam α, β cortes tais que $\alpha \geq 0^*, \beta \geq 0^*$. Seja γ o conjunto de todos os racionais r tais que $r = pq$, em que $p \in \alpha, q \in \beta, p \geq 0, q \geq 0$. Então γ é um corte.*

Definição 6.13. Chamamos o corte γ do teorema 6.22 de produto de α e β e representamos por $\alpha\beta$.

Definição 6.14. Sejam α, β cortes. Definimos

$$\alpha\beta = \begin{cases} -[(-\alpha)\beta] & \text{se } \alpha < 0^*, \beta \geq 0^*, \\ -[\alpha(-\beta)] & \text{se } \alpha \geq 0^*, \beta < 0^*, \\ (-\alpha)(-\beta) & \text{se } \alpha < 0^*, \beta < 0^*. \end{cases}$$

Teorema 6.23. *Quaisquer que sejam os cortes α, β, γ temos:*

(i) $\alpha\beta = \beta\alpha$;

(ii) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$;

(iii) $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$;

(iv) $\alpha 0^* = 0^*$;

(v) $\alpha\beta = 0^*$ *somente se* $\alpha = 0^*$ *ou* $\beta = 0^*$;

(vi) $\alpha 1^* = \alpha$;

(vii) *Se* $0^* < \alpha < \beta$ *e* $\gamma > 0^*$, *então* $\alpha\gamma < \beta\gamma$.

Demonstração. São análogas as demonstradas para a adição, exceto quando se faz necessário considerar vários casos, correspondentes aos sinais dos fatores em questão. Como exemplo, vamos provar o item (iii). Para isso, é preciso considerar diferentes casos. Suponha $\alpha > 0^*, \beta < 0^*, \beta+\gamma > 0^*$. Então $\gamma = (\beta+\gamma)+(-\beta)$. Como a lei distributiva vale para os racionais, temos que $\alpha\gamma = \alpha(\beta+\gamma)+\alpha(-\beta)$. Mas, $\alpha(-\beta) = -(\alpha\beta)$. Portanto, $\alpha\beta+\alpha\gamma = \alpha(\beta+\gamma)$. Os outros casos são análogos.

□

Definição 6.15. A cada corte α associamos um corte $|\alpha|$, que chamamos o valor absoluto de α, definido por:

$$|\alpha| = \begin{cases} \alpha, & \text{se } \alpha \geq 0^*, \\ -\alpha, & \text{se } \alpha < 0^*. \end{cases}$$

É claro que $|\alpha| \geq 0^*$ para todo α e $|\alpha| = 0^*$ somente se $\alpha = 0^*$.

Teorema 6.24. *Se* $\alpha \neq 0^*$, *para cada corte* β *existe um único corte* γ *(que designamos por* β/α*) tal que* $\alpha\gamma = \beta$.

Teorema 6.25. *Quaisquer que sejam os racionais* p *e* q, *temos:*

(i) $p^* + q^* = (p+q)^*$

(ii) $p^* q^* = (pq)^*$

(iii) $p^* < q^*$ *se, e somente se,* $p < q$.

Demonstração.

(i) Se $r \in p^* + q^*$, temos $r = s+t$, com $s < p, t < q$, de modo que $r < p+q$. Portanto, $r \in (p+q)^*$. Se $r \in (p+q)^*$, então $r < p+q$. Sejam $h = p+q-r, s = p - \frac{h}{2}, t = q - \frac{h}{2}$. Logo, $s \in p^*, t \in q^*$ e $r = p+q-h = (p-\frac{h}{2}) + (q-\frac{h}{2}) = s+t$, de modo que $r \in p^* + q^*$, o que prova (i).

(ii) análoga ao item (i).

(iii) Se $p < q$, então $p \in q^*$, mas $p \notin p^*$, de modo que $p^* < q^*$. Se $p^* < q^*$, existe um racional r tal que $r \in q^*, r \notin p^*$. Portanto, $p \leq r < q$, de modo que $p < q$.

□

Teorema 6.26. *Se* α, β *são cortes e* $\alpha < \beta$, *existe um corte racional* r^* *tal que* $\alpha < r^* < \beta$.

Demonstração. Se $\alpha < \beta$, existe um número racional p tal que $p \in \beta$ e $p \notin \alpha$. Escolhemos $r > p$ de modo que $r \in \beta$. Como $r \in \beta$ e $r \notin r^*$, temos $r^* < \beta$. Como $p \in r^*$ e $p \notin \alpha$, temos $\alpha < r^*$. □

Teorema 6.27. *Qualquer que seja o corte α, $p \in \alpha$ se, e somente se, $p^* < \alpha$.*

Demonstração. Qualquer que seja o racional p, $p \notin p^*$. Portanto, $p^* < \alpha$, pois $p \in \alpha$. Reciprocamente, se $p^* < \alpha$, existe um racional q tal que $q \in \alpha$ e $q \notin p^*$. Assim, $q \geq p$, donde concluímos que $p \in \alpha$, pois $q \in \alpha$. □

Os números reais como cortes de Dedekind

Consideramos certos conjuntos racionais, chamados cortes, definimos uma relação de ordem, duas operações - adição e multiplicação, definimos as propriedades dessas operações e demonstramos que a aritmética dos cortes satisfaz as mesmas leis da aritmética dos racionais. Assim, mostramos que o conjunto dos cortes é um corpo ordenado.

Mostramos ainda que a substituição dos números racionais r pelos cortes racionais r^* correspondentes preserva somas, produtos e ordens. Desse modo, podemos dizer que o corpo ordenado de todos os números racionais é isomorfo ao corpo ordenado de todos os cortes racionais, o que permite identificar o corte racional r^* com o número racional r. Isto é, do ponto de vista das operações de adição, multiplicação e da relação de ordem, não há por que distinguir $\mathbb{Q}$ do conjunto de cortes determinados por racionais, bem como, não há razão para distinguir o número 5 e o corte que ele determina, já que os dois têm o mesmo comportamento do ponto de vista das operações e da relação de ordem. Essa identificação foi feita por Dedekind e usada na construção dos números reais.

Definição 6.16. Os cortes serão chamados *números reais*. Cortes racionais serão identificados com *números racionais* e chamados de números racionais. Todos os demais cortes serão chamados números irracionais.

Consideramos, assim, os racionais como subconjunto do conjunto dos números reais. O teorema 6.26 mostra que entre dois reais quaisquer existe um número racional e o teorema 6.13 mostra que cada número real α é o conjunto de todos os racionais p tais que $p < \alpha$.

Teorema 6.28 (Dedekind)**.** *Sejam A e B conjuntos de números reais tais que:*

(a) todo número real está em A ou em B;

(b) nenhum número real está simultaneamente em A e em B;

(c) nem A nem B é vazio;

(d) se $\alpha \in A$ e $\beta \in B$, temos $\alpha < \beta$.

Então, existe um e somente um, número real γ, tal que $\alpha \leq \gamma$ para todo $\alpha \in A$, e $\gamma \leq \beta$, para todo $\beta \in B$.

Demonstração. *(Unicidade)* Suponhamos que existam dois números γ_1 e γ_2, para os quais a conclusão é válida e que $\gamma_1 < \gamma_2$. Pelo teorema 6.26, existe γ_3 tal que $\gamma_1 < \gamma_3 < \gamma_2$. De $\gamma_3 < \gamma_2$ resulta $\gamma_3 \in A$, enquanto que $\gamma_1 < \gamma_3$ resulta $\gamma_3 \in B$, o que contradiz (b). Não pode, pois, existir mais de um número γ com as propriedades desejadas.

(Existência) Seja γ o conjunto de todos os racionais p tais que $p \in \alpha$ para algum $\alpha \in A$. Temos que verificar se γ satisfaz as condições da definição 6.9.

(i) Como $A \neq \emptyset, \gamma \neq \emptyset$. Se $\beta \in B$ e $q \notin \beta$ então $q \notin \alpha$ qualquer que seja $\alpha \in A$ (pois $\alpha < \beta$); portanto $q \notin \gamma$.

(ii) Se $p \in \gamma$ e $q < p$, então $p \in \alpha$, para algum $\alpha \in A$ e, por conseguinte, $q \in \alpha$; logo $q \in \gamma$.

(iii) Se $p \in \gamma$, então $p \in \alpha$, para algum $\alpha \in A$; logo, existe $q > p$ tal que $q \in \alpha$; logo $q \in \gamma$.

Assim, γ é um número real.

É claro que $\alpha \leq \gamma$ qualquer que seja $\alpha \in A$. Se existisse algum $\beta \in B$ tal que $\beta < \gamma$, haveria um racional p que satisfaria as condições $p \in \gamma$ e $p \notin \beta$; mas, se $p \in \gamma$, então $p \in \alpha$ para algum $\alpha \in A$, do que resulta ser $\beta < \alpha$, em contradição com (d). Assim, $\gamma \leq \beta$ qualquer que seja $\beta \in B$, o que completa a demonstração. □

Corolário 6.1. *Nas condições do teorema 6.28, ou existe, em A, um número máximo, ou, em B, um número mínimo.*

Com efeito, se $\gamma \in A$ então γ é o maior número de A. Se $\gamma \in B$ então γ é o menor número de B. Pelo item (i) do teorema 6.28, um desses dois casos deve ocorrer, enquanto, pelo item (ii), eles não podem ocorrer simultaneamente.

É a existência de γ a parte importante do teorema, que mostra que as lacunas encontradas no conjunto $\mathbb{Q}$ estão agora preenchidas.

Definição 6.17. Seja E um conjunto de números reais. Se existe um número y tal que $x \leq y$ para todo $x \in E$, dizemos que E é limitado superiormente e y é uma cota superior de E.

Analogamente, definem-se cotas inferiores. Se E é limitado superior e inferiormente, dizemos que E é limitado.

Definição 6.18. Seja E limitado superiormente. Suponhamos que y tenha as seguintes propriedades:

(a) y é uma cota superior de E;

(b) se $x < y$, então x não é uma cota superior de E.

Nestas condições, y é chamado o supremo de E e escreveremos $y = \sup E$.

Analogamente, define-se o ínfimo de qualquer conjunto E limitado inferiormente.

Tanto o conjunto $\mathbb{Q}$ quanto $\mathbb{R}$ são corpos ordenados, mas apenas $\mathbb{R}$ satisfaz o teorema a seguir, o que permite caracterizar $\mathbb{R}$ como corpo ordenado completo.

Teorema 6.29. *Seja E um conjunto não vazio de números reais, limitado superiormente. Existe, então, o* sup E.

Demonstração. Seja A o seguinte conjunto de números reais: $\alpha \in A$ se, e somente se, existe $x \in E$ tal que $\alpha < x$. Seja B o conjunto de todos os números reais que não estão em A. É claro que nenhum elemento de A é cota superior de E, e todo elemento de B é cota superior de E. Para provar a existência do sup, basta, portanto, provar que B possui um mínimo.

Vamos verificar que A e B satisfazem as hipóteses do teorema 6.28. Evidentemente, (a) e (b) são válidas. Como E é não vazio, existe y tal que $x \leq y$ qualquer que seja $x \in E$; portanto, $y \in B$ e a condição (c) é válida. Se $\alpha \in A$, existe $x \in E$ tal que $\alpha < x$. Se $\beta \in B, x \leq \beta$. Assim, $\alpha < \beta$ para todo $\alpha \in A, \beta \in B$ e a condição (d) é válida.

Portanto, pelo corolário do teorema 6.28, ou A possui máximo, ou B possui mínimo. Vamos provar que a primeira alternativa não pode ocorrer.

Se $\alpha \in A$, existe $x \in E$ tal que $\alpha < x$. Consideremos α' tal que $\alpha < \alpha' < x$. Sendo $\alpha' < x, \alpha' \in A$, de modo que α não é o maior número em A. □

O resultado do teorema 6.29 é a criação dos números irracionais.

Os cortes de Dedekind são definidos como um par de classes A e B de racionais, tais que: A e B são conjuntos não vazios cuja união é o conjunto $\mathbb{Q}$ dos números racionais; todo número menor que algum elemento de A pertence a A, e todo número maior que algum número de B pertence a B. Dedekind postulou, de um modo geral, que todo corte possui um elemento de separação (supremo da classe A e ínfimo da classe B). Isto equivale a dizer que A tem supremo ou B tem ínfimo. E o efeito desse postulado é a criação dos números irracionais. É importante observar que não é necessário trabalhar com as duas classes de cada corte, podemos trabalhar somente com as classes da esquerda ou somente com as classes da direita, pois umas ou outras bastam para caracterizar os números que elas definem. Se usamos as classes da esquerda, postulamos a existência de supremo em cada classe; se usamos as da direita, postulamos que cada classe possui ínfimo. A construção dos números reais fica completa com a identificação de $\mathbb{Q}$ com o conjunto dos cortes determinados por números racionais juntamente com a afirmação de que todo corte possui um elemento de separação.

Em resumo, o que Dedekind essencialmente fez foi definir um número real como um corte no conjunto de números racionais. Este procedimento nos permite "construir" o conjunto dos números reais $\mathbb{R}$ a partir do conjunto dos números racionais $\mathbb{Q}$.

Pode-se pensar em considerar o conjunto de todos os cortes de números reais e repetir a postulação de que todo corte deve ter um elemento separador, para tentar ampliar o conjunto dos números reais. Entretanto, isso não é possível pois todos esses cortes possuem elemento separador, diferente do que acontecia com os cortes de números racionais. Por esse motivo, diz-se que o conjunto dos números reais é um corpo completo, justamente porque todo corte tem elemento separador, ou seja, todo conjunto não vazio e limitado superiormente possui supremo. Mostraremos ainda

que quaisquer dois corpos ordenados com a propriedade da menor cota superior são isomorfos, ou seja, na seção 6.6 provaremos um teorema que afirma que qualquer corpo ordenado completo é necessariamente isomorfo ao corpo dos números reais. Como o conjunto dos números reais é único, muitos autores admitem a existência de um corpo ordenado completo, que é chamado o corpo dos números reais.

6.4 O método das expansões decimais

Stevin, em 1585, foi responsável pela fundamentação da notação decimal. Apesar de não ter produzido uma construção rigorosa dos números reais, ele afirmou que não existe na natureza nada significativamente diferente entre números racionais e irracionais. Essa construção é interessante devido a ênfase dada às expansões decimais no ensino de Matemática. Nesta seção, será definida formalmente a expansão decimal, segundo trabalho de Aragona (2010) [2].

Vamos mostrar que os números reais podem ser aproximados, com erro arbitrariamente pequeno, por números racionais do tipo $p.10^{-m}$, com $p \in \mathbb{Z}$ e $m \in \mathbb{N}$. Para isso, primeiramente, definiremos os reais usando um conceito intuitivo, isto é, um número real (racional ou irracional, que por simplicidade suporemos não negativo) será dado por uma expressão decimal.

Considere $x > 0$ real. Seja n_0 o maior inteiro tal que $n_0 \leq x$ e $0 \leq n_i \leq 9, \forall i \in \mathbb{N}$. Então

$$x = n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \frac{n_3}{10^3} + \ldots + \frac{n_k}{10^k} + \ldots$$

Como a construção de $\mathbb{Q}$ é bastante simples, o caso $x \in \mathbb{Q}$ não será considerado por enquanto, de modo que consideraremos o caso em que x não é racional (como $\sqrt{2}$). Neste caso, $x \notin \mathbb{Q}$, assim, sempre teremos

$$x \neq n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \frac{n_3}{10^3} \ldots + \frac{n_m}{10^m}$$

mas cada expressão finita

$$x_m := n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \frac{n_3}{10^3} \ldots + \frac{n_m}{10^m}$$

será uma aproximação de x e esta aproximação será melhor quanto maior for o número m de somandos. Logo, podemos considerar sequências de números racionais que aproximam um dado número real. Por exemplo, considere a sequência de números racionais:

$$\begin{cases} x_1 = 1,4 = 1 + \frac{4}{10} \\ x_2 = 1,41 = 1 + \frac{4}{10} + \frac{1}{10^2} \\ x_3 = 1,414 = 1 + \frac{4}{10} + \frac{1}{10^2} + \frac{4}{10^3} \\ x_4 = 1,414 = 1 + \frac{4}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} \\ \vdots \end{cases}$$

A sequência de números racionais anterior aproxima-se de $\sqrt{2}$.

Já vimos que se pode aproximar números reais por sequências de racionais e, estas sequências são as sequências de Cauchy. Uma sequência de Cauchy de números racionais arbitrária pode aproximar um número irracional, como por exemplo $\sqrt{2}$, ou um número racional, como $1/3$ (que é aproximado pela sequência de Cauchy $0,3;0,33;0,333;\ldots$). Como já sabemos definir os números racionais, não é necessário usar sequências de Cauchy em $\mathbb{Q}$ para isso, pois todo $r \in \mathbb{Q}$ é aproximado pela sequência de Cauchy em $\mathbb{Q}$ constante: $x_0 := r, x_1 := r, x_2 := r, \ldots, x_m := r, \ldots$, ou seja, recairíamos no caso trivial. O interesse está, portanto, em definir os irracionais. Já estudamos a construção dos reais por sequências de Cauchy, veremos que ela nos leva de forma rápida e natural à representação decimal dos números reais, que foi a forma em que estes números foram conhecidos durante muito tempo antes de ter sua teoria devidamente estruturada pelos trabalhos de Dedekind, Cantor e outros. Além disso, a representação decimal é a forma tradicional de apresentar os números reais no ensino médio.

O objetivo é a aproximação dos números reais por decimais e a representação resultante de números reais por desenvolvimentos decimais ilimitados. O resultado a seguir nos mostra uma aproximação dos reais por números racionais.

Proposição 6.1. *Quaisquer que sejam $\alpha \in \mathbb{R}$ e $m \in \mathbb{N}$, existe um único $p_m \in \mathbb{Z}$ tal que*

$$p_m.10^{-m} \leq \alpha < (p_m + 1).10^{-m}.$$

Demonstração. Pela propriedade arquimediana de $\mathbb{R}$, existe $m \in \mathbb{N}$ tal que $m.10^{-m} > |\alpha|$, ou seja, $-m.10^{-m} < \alpha < m.10^{-m}$, donde resulta que o conjunto $X := \{q \in \mathbb{Z}; q.10^{-m} \leq \alpha\}$ é não vazio pois $-m \in X$ e, além disto, X é majorado por m. Em consequência, X admite um máximo p_m que evidentemente satisfaz a desigualdade que queremos demonstrar, o que prova a afirmação relativa à existência. Se existisse um outro $p'_m \in \mathbb{Z}$ tal que $p'_m.10^{-m} \leq \alpha < (p'_m + 1).10^{-m}$ teríamos as desigualdades estritas $p'_m.10^{-m} < (p_m + 1).10^{-m}$ e $p_m.10^{-m} < (p'_m + 1).10^{-m}$ que implicam $p'_m < p_m + 1$ e $p_m < p'_m + 1$, ou seja, $p'_m \leq p_m$ e $p_m \leq p'_m$, donde $p_m = p'_m$, o que prova a unicidade. □

Definição 6.19. Seja $\alpha \in \mathbb{Z}$ arbitrário. Para cada $m \in \mathbb{N}$, o número $\zeta_m := p_m 10^{-m}$ determinado pela proposição 6.1 é chamado valor decimal aproximado por falta de ordem m de α.

Exemplo 6.3. Se $\alpha = 0,333\ldots$, então as sequências (p_m) e (ζ_m) são $(p_m)_{m\in\mathbb{N}} = (0,3,33,333,\ldots)$ e $(\zeta_m) = (0;0,3;0,33;\ldots)$

A proposição 6.1 associa a cada $\alpha \in \mathbb{R}$ duas sequências, (p_m) e (ζ_m) em $\mathbb{Z}$ e $\mathbb{Q}$ respectivamente. O resultado seguinte mostra a estrutura da sequência (p_m).

Proposição 6.2. *Sejam $\alpha \in \mathbb{R}$ arbitrário e $(p_m)_{m\in\mathbb{N}}$ a sequência em $\mathbb{Z}$ determinada por α na proposição 6.1. Então p_m é o número de dezenas de p_{m+1}, para cada $m \in \mathbb{N}$ (em outros termos, (p_m) é o quociente da divisão inteira de (p_{m+1}) por 10).*

Demonstração. Substituindo m por $m + 1$ na desigualdade da proposição 6.1 obtemos:

$$p_{m+1}.10^{-m-1} \leq \alpha < (p_{m+1}+1)10^{-m-1}$$

o que junto com a desigualdade da proposição 6.1 implica as desigualdades estritas

$$p_m.10^{-m} < (p_{m+1}+1)10^{-m-1} \text{ e } p_{m+1}.10^{-m-1} < (p_m+1)10^{-m}$$

donde resultam as desigualdades seguintes:

$$10p_m \leq p_{m+1} < 10(p_m+1)$$

ou seja,

$$p_m \leq \frac{p_{m+1}}{10} < p_m + 1.$$

□

Fixado $\alpha \in \mathbb{R}$ arbitrário, sejam $(p_m)_{m\in\mathbb{N}}$ e $(\zeta_m)_{m\in\mathbb{N}}$ as sequências determinadas por α a partir da proposição 6.1 e da definição 6.19. Para cada $m \in \mathbb{N}$, vamos indicar com α_{m+1} o resto da divisão inteira de p_{m+1} por 10. Como p_m é o quociente da divisão inteira de p_{m+1} por 10, é claro que a definição acima de α_{m+1} equivale a seguinte definição:

$$\alpha_{m+1} := p_{m+1} - 10p_m \ \forall m \in \mathbb{N} \text{ e portanto } 0 \leq \alpha_{m+1} \leq 9). \tag{2}$$

Multiplicando (2) por 10^{-m-1} obtemos

$$\zeta_{m+1} = \zeta_m + \alpha_{m+1}10^{-m-1} \ (m \in \mathbb{N}).$$

A expressão (2) define uma sequência de números inteiros $(\alpha_{m+1})_{m\in\mathbb{N}} = (\alpha_1, \alpha_2, \alpha_3, \ldots)$ tal que $0 \leqslant \alpha_j \leq 9$ para cada $j \in \mathbb{N}^*$ (pois α_j é o resto de uma divisão inteira por 10). A seguir, definimos, com as notações da proposição 6.1: $\alpha_0 := p_0$, isto é, $p_0 \leq \alpha \leq p_0 + 1$. O inteiro α_0 junto com a sequência $(\alpha_{m+1})_{m\in\mathbb{N}}$ acima determinam uma nova sequência $(\alpha_m)_{m\in\mathbb{N}} = (\alpha_0, \alpha_1, \alpha_2, \ldots)$.

As considerações precedentes mostram que a cada $\alpha \in \mathbb{R}$ podemos associar o símbolo:

$$\alpha_0, \alpha_1\alpha_2\alpha_3 \ldots \alpha_m \ldots \tag{3}$$

onde $\alpha_m \in \mathbb{Z}$ para cada $m \in \mathbb{N}$ e $0 \leq \alpha_m \leq 9$ para cada $m \in \mathbb{N}^*$. O símbolo (3) é chamado desenvolvimento decimal ilimitado de α. O resultado seguinte mostra a relação existente entre as sequências (ζ_m) e (α_m) :

Proposição 6.3. *Sejam $\alpha \in \mathbb{R}$, $(p_m)_{m\in\mathbb{N}}$ a sequência definida pelas desigualdades $p_m.10^{-m} \leq \alpha < (p_m+1).10^{-m}$, $(\zeta_m)_{m\in\mathbb{N}}$ a sequência dos valores decimais aproximados por falta de α (isto é, $\zeta_m = p_m.10^{-m} \ \forall m \in \mathbb{N}$)) e $(\alpha_m)_{m\in\mathbb{N}}$ a sequência definida por $\alpha_{m+1} := p_{m+1} - 10p_m \ \forall m \in \mathbb{N}$ e $\alpha_0 := p_0$. Então, para cada $m \in \mathbb{N}$ vale a igualdade*

$$\zeta_m = \sum_{k=0}^{m} 10^{-k}.\alpha_k \tag{4}$$

Demonstração. Exercício. Basta usar indução em m. □

A proposição 6.3 mostra que ζ_m fica determinado pela sequência $(\alpha_0, \alpha_1, \ldots, \alpha_m)$, o que sugere usar o símbolo $\alpha_0, \alpha_1\alpha_2 \ldots \alpha_m$ para denotar ζ_m.

Definição 6.20. Dados $m \in \mathbb{N}$ e uma sequência $(\alpha_i)_{0\leq i\leq m}$ em $\mathbb{Z}$ tal que $0 \leq \alpha_i \leq 9$ para cada $i = 1, 2, \ldots, m$, definimos

$$\alpha_0, \alpha_1\alpha_2 \ldots \alpha_m := \sum_{k=0}^{m} 10^{-k}.\alpha_k \tag{5}$$

Observação. Considere a notação anterior.

1. A desigualdade em 6.1 pode ser definida como:

$$\alpha_0, \alpha_1\alpha_2 \ldots \alpha_m \leq \alpha < \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m + 10^{-m}.$$

2. $\forall m \in \mathbb{N}$, o número decimal $\zeta_{m+1} = p_{m+1}.10^{-m-1}$ se deduz do número decimal $\zeta_m = p_m.10^{-m}$, somando a este $\alpha_{m+1}.10^{-m-1}$.

3. Fixados $\alpha \in \mathbb{R}$ e $r \in \mathbb{N}$ arbitrários, se $\zeta_r = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_r$ denota o valor decimal aproximado por falta de ordem r de ordem α, então é fácil ver que o desenvolvimento decimal ilimitado de ζ_r é: $\alpha_0, \alpha_1\alpha_2 \ldots \alpha_r 000 \ldots 0 \ldots$

4. Considere o número decimal $\zeta = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m$, onde vamos supor $m \in \mathbb{N}$ (no caso $m = 0$, a sequência $(\alpha_i)_{1\leq i\leq 0}$ é vazia e definimos $\alpha_0, \alpha_1\alpha_2 \ldots \alpha_m := \alpha_0$). Comecemos examinando $\alpha_0 \in \mathbb{N}^*$. É fácil ver que podemos expressar α_0 de modo único, como soma de múltiplos naturais de potências não negativas de 10 com coeficientes β_j tais que $0 \leq \beta_j \leq 9$ para cada índice j; em outros termos, existe uma única sequência $(\beta_j)_{0\leq j\leq n}$ em $\mathbb{N}$ tal que $0 \leq \beta_j \leq 9$ para cada $j = 0, 1, \ldots, n$ e

$$\alpha_0 = \sum_{k=0}^{n} 10^k \beta_{n-k}.$$

   Assim, podemos denotar $\beta_0\beta_1 \ldots \beta_n := \alpha_0$ e usar o símbolo

$$\beta_0\beta_1 \ldots \beta_n, \alpha_1\alpha_2 \ldots \alpha_m \tag{6}$$

   para denotar o decimal $\zeta = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m$, que também pode ser representado do seguinte modo:

$$\sum_{k=0}^{n} 10^k \beta_{n-k} + \sum_{l=1}^{m} 10^{-l} \alpha_l.$$

   Em particular, se $m \geq 1$ e $\alpha_1 = \ldots = \alpha_m = 0$, obtemos

$$\beta_0\beta_1 \ldots \beta_n, 00 \ldots 0 = \beta_0\beta_1 \ldots \beta_n = \alpha_0.$$

   Se $\alpha_0 = 0$, escrevemos $0, \alpha_1\alpha_2 \ldots \alpha_m$ e podemos convencionar que neste caso a sequência $(\beta_j)_{0\leq j\leq n}$ tem apenas um elemento $\beta_0 = 0$. Desta forma, podemos usar a notação (6) sempre que $\alpha_0 \in \mathbb{N}$. Precisamos considerar o caso $\alpha_0 \in \mathbb{Z}^*_-(\alpha_0 \leq -1)$ então, como $0 < 0, \alpha_1\alpha_2 \ldots \alpha_m < 1$, é claro que $\zeta := \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m = \alpha_0 + 0, \alpha_1\alpha_2 \ldots \alpha_m < 0$ que implica $0 < -\zeta = -\alpha_0 - 0, \alpha_1\alpha_2 \ldots \alpha_m = |\alpha_0| - 0, \alpha_1\alpha_2 \ldots \alpha_m = \alpha'_0, \alpha'_1\alpha'_2 \ldots \alpha'_m$, onde $|\alpha'_0| = |\alpha_0| - 1 \geq 0$ e $0 \leq \alpha'_j \leq 9$ para

cada $j = 1, 2, \ldots, m$ (a existência dessa sequência $(\alpha'_j)_{0 \leq tj \leq m}$ fica como exercício). Como $\alpha'_0 \in \mathbb{N}$, pelo que precede existe uma única sequência $(\beta'_j)_{0 \leq j \leq n}$ em $\mathbb{Z}$ tal que $0 \leq \beta'_j \leq 9$ para cada $j = 1, 2, \ldots, n$ de modo que:

$$-\zeta = \alpha'_0, \alpha'_1 \alpha'_2 \ldots \alpha'_m = \beta'_0 \beta'_1 \ldots \beta'_n, \alpha'_1 \alpha'_2 \ldots \alpha'_m$$

donde

$$\zeta = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m = -\beta'_0 \beta'_1 \ldots \beta'_n, \alpha'_1 \alpha'_2 \ldots \alpha'_m$$

Resumindo, todo decimal do tipo $\zeta = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m$ admite uma representação única por um símbolo do tipo (6) se $\alpha_0 \in \mathbb{N}$ e por um símbolo do tipo $-\beta'_0 \beta'_1 \ldots \beta'_n, \alpha'_1 \alpha'_2 \ldots \alpha'_m$ se $\alpha_0 \in \mathbb{Z}^*_-$, onde (α_i) e (β_j) são sequências de inteiros entre 0 e 9.

Definição 6.21. Chama-se desenvolvimento decimal ilimitado a qualquer símbolo do tipo

$$\beta_0, \beta_1 \ldots \beta_m \ldots \tag{7}$$

determinado por uma sequência $(\beta_m)_{m \in \mathbb{N}}$ em $\mathbb{Z}$ tal que $0 \leq \beta_m \leq 9$ para cada $m \in \mathbb{N}^*$ e, neste caso, para cada $m \in \mathbb{N}^*$, β_m é chamado $m-$ésima casa decimal de (7).

O desenvolvimento decimal de (7) é dito próprio se contém uma infinidade de casas decimais β_m diferentes de 9. Indicamos com o símbolo $\mathbb{D}$ o conjunto de todos os desenvolvimentos decimais ilimitados próprios.

A expressão "número decimal" é frequentemente utilizada para indicar um desenvolvimento decimal ilimitado (próprio ou não). Já vimos que é possível associar a cada $\alpha \in \mathbb{R}$ o seu desenvolvimento decimal ilimitado, o qual é único e dado por:

$$J(\alpha) = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m \ldots$$

Assim, fica definida uma aplicação

$$J : \alpha \in \mathbb{R} \to J(\alpha) = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m \ldots \in \mathbb{D}^0,$$

onde $\mathbb{D}^0$ denota o conjunto de todos os desenvolvimentos decimais ilimitados.

Teorema 6.30. *A aplicação*

$$J : \alpha \in \mathbb{R} \to J(\alpha) = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m \ldots \in \mathbb{D}$$

é bijetora e, para cada $\alpha \in \mathbb{R}$, a sequência $(J_m(\alpha))_{m \in \mathbb{N}}$ definida por $J_0(\alpha) := \alpha_0$ e $(J_m(\alpha)) := \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m$ para cada $m \in \mathbb{N}^*$, é uma sequência de Cauchy em $\mathbb{Q}$ que representa α.

Demonstração. A demonstração será omitida e pode ser encontrada em Aragona (2010) [2]. □

A bijeção $J := \mathbb{R} \to \mathbb{D}$ sugere naturalmente não fazer distinção entre α e o seu desenvolvimento decimal ilimitado $J(\alpha) = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m \ldots \in \mathbb{D}$, isto é,

$$\alpha = J(\alpha) = \alpha_0, \alpha_1 \alpha_2 \ldots \alpha_m \ldots \in \mathbb{D} \; \forall \alpha \in \mathbb{R}$$

o que implica na identificação $\mathbb{R} = \mathbb{D}$.

A identificação $\mathbb{R} = \mathbb{D}$ mostra que é possível definir diretamente os números reais usando os desenvolvimentos decimais ilimitados próprios sem passar pelas sequências de Cauchy. A teoria assim construída é tão rigorosa quanto as outras e permite definir muito facilmente a relação de ordem em $\mathbb{R}$ que é a ordem lexicográfica, pois é fácil ver que

$$x_0, x_1x_2 \dots x_m \dots < y_0, y_1y_2 \dots y_m \dots$$

se para o menor $m \in \mathbb{N}$ tal que $x_m \neq y_m$ se verifica $x_m < y_m$. Entretanto, esta forma de construir a teoria dos números reais apresenta algumas dificuldades técnicas no estudo da estrutura algébrica de $\mathbb{R}$.

Vamos explicar o significado de igualdades do tipo seguinte: $1 = 0,99\dots9\dots$ ou $2,13 = 2,1299\dots9\dots$. Suponhamos que $\overline{\beta} = \beta_0, \beta_1 \dots \beta_m \dots \in \mathbb{D}^0 \cap \complement\mathbb{D}$ o que significa que existe $v \in \mathbb{N}$ tal que $\beta_m = 9$ para $m > v$, onde podemos evidentemente supor que v é o menor número natural que tem esta propriedade, isto é,

$$v = 0 \text{ ou } \beta_v < 9 \text{ se } v \geq 1.$$

Definimos o símbolo

$$\beta^* := \beta_0, \beta_1 \dots \beta_{v-1}\beta'_v 00\dots0\dots$$

por $\beta'_v := \beta_v + 1$ (observe que se $v = 0$ então $\beta^* = \beta'_0, 00\dots0\dots$). É claro que $\beta^* \in \mathbb{D}$ e portanto, o teorema 6.30 assegura que existe um único $\beta \in \mathbb{R}$ tal que $J(\beta) = \beta^*$. Queremos mostrar que $\overline{\beta}$ é um desenvolvimento ilimitado legítimo de β.

De fato, $m > v$, consideremos os números decimais:

$$\overline{\beta_m} := \beta_0, \beta_1 \dots \beta_v \overbrace{99\dots9}^{m-v} = \sum_{j=0}^{v} \beta_j 10^{-j} + 9 \sum_{l=v+1}^{m} 10^{-l}$$

$$\beta^*_m := \beta_0, \beta_1 \dots \beta_{v-1}\beta'_v \overbrace{00\dots0}^{m-v} = \sum_{j=0}^{v-1} \beta_j 10^{-j} + \beta'_v.10^{-v}.$$

Então como $\beta'_v - \beta_v = 1$, pode-se mostrar (exercício) que $\beta^*_v - \overline{\beta_m} = 10^{-m}$
o que implica

$$|\beta - \overline{\beta_m}| \leq |\beta - \beta^*_m| + |\beta^*_m - \overline{\beta_m}| = |\beta - \beta^*_m| + 10^{-m} \ \forall m > v.$$

Pode-se mostrar que $\lim_{n\to\infty} \beta^*_m = \beta$ e então, a desigualdade anterior acarretará que $\lim_{m\to\infty} \overline{\beta_m} = \beta$ (e, portanto, $(\overline{\beta_m})_{m\in\mathbb{N}}$ é uma sequência de Cauchy).

Convencionamos identificar $\overline{\beta}$ com β^* (exemplos: $1 = 0,99\dots9\dots; 2,13 = 2,1299\dots9\dots; 0,3126 = 0,312600\dots0\dots = 3,12599\dots9\dots$).

Define-se número decimal como qualquer elemento de $\mathbb{D}^0$ (lembrar que $\mathbb{D}^0 \supsetneq \mathbb{D}$).

Podemos usar a bijeção $J : \mathbb{R} \to \mathbb{D}$ para obter a estrutura de corpo totalmente ordenado de $\mathbb{D}$ a partir de $\mathbb{R}$ por meio das seguintes definições de adição, multiplicação e ordem em $\mathbb{D}$.

$$\begin{cases} J(\alpha) + J(\beta) & := J(\alpha + \beta) & \forall \alpha, \beta \in \mathbb{R} \\ J(\alpha).J(\beta) & := J(\alpha\beta) & \forall \alpha, \beta \in \mathbb{R} \\ J(\alpha) < J(\beta) & \text{ se e só se } \alpha < \beta, & \forall \alpha, \beta \in \mathbb{R} \end{cases}$$

que evidentemente definem uma estrutura de corpo totalmente ordenado sobre $\mathbb{D}$ tal que J é isomorfismo estritamente crescente de $\mathbb{R}$ sobre $\mathbb{D}$. O número decimal $J(\alpha) \in \mathbb{D}$ é chamado a representação decimal de $\alpha \in \mathbb{R}$.

Existem dois tipos de desenvolvimentos decimais ilimitados próprios, um deles caracterizando os racionais e o outro os irracionais. Na escola, aprendemos a distinguir os racionais dos irracionais a partir de suas representações decimais. Os racionais são aqueles números decimais que, a partir de uma certa casa decimal, são periódicos como $2,32541\underbrace{258}\underbrace{258}\underbrace{258}$ ou, em particular, os estacionários como $1,1500\ldots0\ldots$. Estes números decimais são chamados dízimas periódicas. Já os irracionais são apresentados como aqueles números decimais sem nenhum tipo de periodicidade. Antes de demonstrar esses fatos precisamos definir os conceitos de divisão aproximada.

Definição 6.22. Dados $a, b \in \mathbb{N}^*$ com $a < b$, chamamos de divisão aproximada de a por b de ordem $v \in \mathbb{N}$ quando obtemos dois números inteiros q e r que satisfazem

$$a.10^v = bq + r \text{ e } 0 \leq r < b. \tag{8}$$

Se dividirmos a igualdade (8) por $b.10^v$:

$$\frac{a}{b} = q.10^{-v} + \left(\frac{r}{b}\right) 10^{-v} \text{ (e } 0 \leq \frac{r}{b} < 1). \tag{9}$$

O número decimal $q.10^{-v}$ será chamado de resultado de ordem v da divisão aproximada de a por b.

De (9), resulta $0 \leq \frac{r}{b} < 1$ e $\left|\frac{a}{b} - q.10^{-v}\right| = \frac{a}{b} - q.10^{-v} = \left(\frac{r}{b}\right) 10^{-v} < 10^{-v}$, que mostra que, mesmo no caso $r > 0$ pode-se tornar $q.10^{-v}$ tão próximo quanto se queira do racional a/b desde que se tome $v \in \mathbb{N}$ suficientemente grande.

Proposição 6.4. *Se $v = 0$, a hipótese $0 < a < b$ e (8) mostram que $q = 0$ e $r = a$ e portanto o desenvolvimento decimal ilimitado de q é $J(q) = 0,00\ldots0\ldots$ Se $v \geq 1$ então o desenvolvimento decimal ilimitado de $q.10^{-v}$ é da forma:*

$J(q.10^{-v}) = 0,\alpha_1\alpha_2\ldots\alpha_v00\ldots0\ldots, (*)$ onde $0 \leq \alpha_j \leq 9$ para cada $j = 1, 2, \ldots, v$.

Demonstração. Fixado $v \in \mathbb{N}$ arbitrário, temos: $a.10^{-v} < b$ ou $a.10^{-v} \geq b$. No primeiro caso, por (8), resulta $q = 0$ e $r = a.10^{-v} < b$, o que prova $(*)$ com $\alpha_1 = \alpha_2 = \ldots = \alpha_v = 0$. Se $a.10^{-v} \geq b$ então é claro que $0 < q < 10^v$. Em consequência, q admite um desenvolvimento em potências de 10 do tipo seguinte:

$q_v = a_1.10^{v-1} + a_2.10^{v-2} + \ldots + \alpha_v = \sum_{j=1}^{v} 10^{v-j}.\alpha_j$, com $0 \leq \alpha_j \leq 9$ e portanto:

$q_v.10^{-v} = \frac{\alpha_1}{10} + \frac{\alpha_2}{10^2} + \ldots + \frac{\alpha_v}{10^v} = 0,\alpha_1\alpha_2\ldots\alpha_v = 0,\alpha_1\alpha_2\ldots\alpha_v00\ldots0\ldots$ □

Consideremos $a, b \in \mathbb{N}^*$ com $a \geq b$. Ao fazermos a divisão inteira de a por b obteremos um quociente Q e um resto R, caracterizados pelas duas condições: $a = b.Q + R$ e $0 < R < b$, onde o caso $R = 0$ foi excluído, pois neste caso a divisão aproximada é simplesmente a divisão exata. Em consequência,

$$\frac{a}{b} = Q + \frac{R}{b} \text{ e } 0 < \frac{R}{b} < 1. \tag{10}$$

Fazendo a divisão aproximada de R por b de ordem $v \in \mathbb{N}$, obtemos a igualdade:

$$\frac{R}{b} = q.10^{-v} + \left(\frac{r}{b}\right) 10^{-v} \; (0 \leq \frac{r}{b} < 1)$$

Substituindo em (10) temos

$$\frac{a}{b} = (Q + q.10^{-v}) + \left(\frac{r}{b}\right) 10^{-v} \text{ e } 0 < \frac{r}{b} < 1. \tag{11}$$

Assim, quando $a, b \in \mathbb{N}^*$ com $a \geq b$, chamaremos de divisão aproximada de a por b de ordem v o processo descrito anterior e definimos o resultado de ordem v da divisão aproximada de a por b como sendo o número racional $Q + q.10^{-v}$ cujo desenvolvimento decimal ilimitado é do tipo

$$Q, \alpha_1\alpha_2 \ldots \alpha_v 00 \ldots 0 \ldots$$

Por fim, se $a \in \mathbb{Z}^*_-$ (ainda suporemos $b \in \mathbb{N}^*$) então $a' := -a \in \mathbb{N}$ e definimos divisão aproximada de a por b de ordem $v \in \mathbb{N}$ como o processo que consiste em fazer a divisão aproximada de a' por b de ordem v obtendo uma igualdade do tipo (9) ou (11) (dependendo de que $0 \leq a' < b$ ou $a' \geq b$.

Chamaremos resultado de ordem v da divisão aproximada de a por b, o número decimal $-(Q + q.10^{-v})$, isto é, o oposto do resultado de ordem v da divisão aproximada de $a' = -a$ por b.

Por fim, dados $a \in \mathbb{Z}$ e $b \in \mathbb{N}^*$, chamaremos resultado da divisão prolongada de a por b ao símbolo $\alpha_0, \alpha_1\alpha_2 \ldots \alpha_m \ldots \in \mathbb{D}^0$ onde $(\alpha_m)_{m\in\mathbb{N}}$ é a sequência definida assim: para cada $v \in \mathbb{N}$, o número decimal $\alpha_0, \alpha_1\alpha_2 \ldots \alpha_v = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_v 00 \ldots 0 \ldots$ é o resultado de ordem v da divisão aproximada de a por b.

O lema seguinte formaliza alguns resultado já conhecidos desde o ensino primário e, como a demonstração é longa, será omitida.

Lema 6.5.

(a) *Se* $t \in \mathbb{Z}$ *então* $J(t) = t, 00 \ldots 0 \ldots$

(b) $J(10^{-m}) = 0, \underbrace{00 \ldots 01}_{m} 00 \ldots 0 \ldots$

(c) *Se* $\alpha \in \mathbb{R}$ *e* $J(\alpha) = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m \ldots$, *então*

$$\alpha = \alpha_0 + J^{-1}(0, \alpha_1\alpha_2 \ldots \alpha_m \ldots) \; e$$
$$J(\alpha) = \alpha_0, 00 \ldots 0 \ldots + 0, \alpha_1\alpha_2 \ldots \alpha_m \ldots$$

Demonstração. Exercício. Para detalhes, consulte Aragona(2010)[2]. □

Vejamos a notação adotada e em seguida definiremos dízima periódica.

Sejam $\alpha_0 \in \mathbb{N}, \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m \ldots \in \mathbb{D}$ e $(\beta_j)_{0\leq j\leq n}$ a sequência determinada por α_0 de modo que

$$\alpha_0 = \beta_0\beta_1 \ldots \beta_n := \sum_{k=0}^{n} 10^k \beta_{n-k}$$

onde $\beta_j \in \mathbb{Z}$ e $0 \leq \beta_j \leq 9$ para cada $j = 0, 1, \ldots, n$. Definimos

$$\beta_0\beta_1 \ldots \beta_n, \alpha_1\alpha_2 \ldots \alpha_m \ldots := \alpha_0, \alpha_1\alpha_2 \ldots \alpha_m \ldots$$

donde resulta em particular $\beta_0\beta_1 \ldots \beta_n, 00 \ldots 0 \ldots = \alpha_0, 00 \ldots 0 \ldots$

Logo, podemos escrever

$$\beta_0\beta_1 \ldots \beta_n, \alpha_1\alpha_2 \ldots \alpha_m \ldots := \beta_0\beta_1 \ldots \beta_n, 00 \ldots 0 \ldots + 0, \alpha_1\alpha_2 \ldots \alpha_m.$$

Definição 6.23. Sejam $\alpha \in \mathbb{R}$ e $J(\alpha) \in \mathbb{D}$ seu desenvolvimento decimal ilimitado. Diz-se que $J(\alpha) = \alpha_0, \alpha_1\alpha_2 \ldots$ é uma dízima periódica se existem $v' \in \mathbb{N}$ e $t' \in \mathbb{N}^*$ tais que $\alpha_m = \alpha_{m+t'}\ \forall m > v'$

São chamados índice divisório e tamanho da dízima $J(\alpha)$, respectivamente, os seguintes números:

$$v := \min\{v' \in \mathbb{N}; \exists t' \in \mathbb{N}^* \text{ tal que vale } \alpha_m = \alpha_{m+t'}\ \forall m > v'\}$$
$$t := \min\{t' \in \mathbb{N}^*; \alpha_m = \alpha_{m+t'}\ \forall m > v\}$$

Pelas definições de t e v temos: $\alpha_m = \alpha_{m+t}\ \forall m > v$.

Chama-se período da dízima $J(\alpha)$ ao número inteiro

$$\theta := \sum_{\sigma=1}^{t} 10^{t-\sigma} \cdot \alpha_{v+\sigma}.$$

Vamos verificar que $\theta = p_{v+t} - 10^t p_v$.

Temos

$$p_{v+t} = 10^{v+t}\zeta_{v+t} = 10^{v+t}\sum_{k=0}^{v+t} 10^{-k}\alpha_k = \sum_{k=0}^{v+t} 10^{v+t-k}\alpha_k$$

e

$$10^t p_v = 10^t(10^t\zeta_v) = 10^{t+v}\sum_{k=0}^{v} 10^{-k}\alpha_k = \sum_{k=0}^{v} 10^{v+t-k}\alpha_k,$$

donde

$$\begin{aligned} p_{v+t} - 10^t p_v &= \sum_{k=0}^{v+t} 10^{v+t-k}\alpha_k - \sum_{k=0}^{v} 10^{v+t-k}\alpha_k \\ &= \sum_{k=v+1}^{v+t} 10^{v+t-k}\alpha_k = \sum_{\sigma=1}^{t} 10^{t-\sigma}\alpha_{v+\sigma} = \theta. \end{aligned}$$

Esquematicamente,

$$\alpha_0, \alpha_1\alpha_2 \ldots \alpha_v \underbrace{\alpha_{v+1} \ldots \alpha_{v+t}}\ \underbrace{\alpha_{v+t+1} \ldots \alpha_{v+2t}}\ \underbrace{\alpha_{v+2t+1} \ldots}\quad \text{e} \quad \theta = \sum_{\sigma=1}^{t} 10^{t-\sigma}\alpha_{v+\sigma}$$

é representado por

$$\theta = \alpha_{v+1} \ldots \alpha_{v+t}.$$

Proposição 6.5. *Se $a \in \mathbb{N}$ e $b \in \mathbb{N}^*$ então o resultado de ordem $v \in \mathbb{N}$ da divisão aproximada de a por b coincide com a aproximação decimal por falta de ordem v do racional a/b. Em consequência, o desenvolvimento decimal ilimitado próprio de a/b coincide com o resultado da divisão prolongada de a por b.*

Demonstração. As definições de divisão aproximada e de resultado de uma divisão aproximada mostram que podemos nos limitar a considerar o caso $0 < a < b$ (pois o caso $a > b$ se reduz a este e o caso $a = b$ é óbvio). A igualdade em (9) implica

$$q \cdot 10^{-v} \leq \frac{a}{b}$$

pois $\frac{r}{b} \geq 0$ e, portanto, $\left(\frac{r}{b}\right) 10^{-v} \geq 0$; e

$$\frac{a}{b} < (q+1)10^{-v}$$

pois $\frac{r}{b} < 1$ e portanto $\left(\frac{r}{b}\right).10^{-v} < 10^{-v}$. Donde resulta que $q \in \mathbb{Z}$ satisfaz as desigualdades $q \cdot 10^{-v} \leq \frac{a}{b} < (q+1)10^{-v}$. □

Proposição 6.6. *Dados $\xi \in \mathbb{R}$ são equivalentes as condições:*

(a) $\xi \in \mathbb{Q}$.

(b) O desenvolvimento decimal ilimitado próprio de ξ é periódico a partir de alguma casa decimal (em outras palavras, $J(\xi)$ é uma dízima periódica).

Demonstração. $(a) \Rightarrow (b)$ Vamos supor que $\xi = a/b$ com $b \in \mathbb{N}^*$; assim como em (a), basta considerar o caso $0 < a < b$. Temos que $a10^v = b.q_v + r_v$ e $0 \leq r_v < b (v \in \mathbb{N})$.

Para os valores $v = 0, 1, 2, \ldots, b$ teremos $b+1$ restos $r_0, r_1, r_2, \ldots, r_b$ que são os $b+1$ inteiros que pertencem ao conjunto $\{0, 1, 2, \ldots, b-1\}$ logo é claro que aparece pelo menos um resto "repetido", isto é, existem $v, v' \in \mathbb{N}$ com $0 \leq v, v' \leq b$ e $v \neq v'$ com $r_v = r_{v'}$ e, neste momento aparece a periodicidade da divisão prolongada de a por b que, pela proposição anterior, coincide com o desenvolvimento decimal ilimitado próprio de a/b.

$(b) \Rightarrow (a)$ O desenvolvimento decimal ilimitado $J(\xi)$ de ξ é dado por

$$\alpha_0, \alpha_1\alpha_2 \ldots \alpha_v \overbrace{\alpha_{v+1} \ldots \alpha_{v+t}} \overbrace{\alpha_{v+t+1} \ldots \alpha_{v+2t}} \ldots \overbrace{\alpha_{v+1+lt} \ldots \alpha_{v+(l+1)t}} \ldots$$

Esse desenvolvimento é, por hipótese, periódico de período $\theta = \sigma_{v+1} \ldots \sigma_{v+t} = \cdots = \sigma_{v+1+lt} \ldots \sigma_{v+(l+1)t} = \cdots$. Para simplificar, vamos usar a identificação $\mathbb{R} = \mathbb{D}$, o que permite escrever $\xi = J(\xi)$, isto é,

$$\xi = \alpha_0, \alpha_1\alpha_2 \ldots \alpha_v\alpha_{v+1} \ldots \alpha_{v+t} \ldots \alpha_{v+1+lt} \ldots \alpha_{v+(l+1)t} \ldots$$

Vamos supor $\alpha_0 \geq 0$ (e portanto, $\xi = 0$ se eliminarmos o caso trivial $\alpha_0 = \alpha_1 = \cdots = \alpha_v = \alpha_{v+1} = \cdots = \alpha_{v+t} = 0$). Vimos que existe uma única sequência $(\beta_j)_{0 \leq j \leq n}$ em $\mathbb{Z}$ verificando $0 \leq \beta_j \leq 9$ sempre que $0 \leq j \leq n$ tal que $\alpha_0 = \beta_0\beta_1 \ldots \beta_n$ e então, ξ pode ser escrito assim:

$$\xi = \beta_0\beta_1 \dots \beta_n, \alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t} \dots \alpha_{v+1+lt} \dots \alpha_{v+(l+1)t} \dots$$

Assim,

$$10^v\xi = \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v, \alpha_{v+1} \dots \alpha_{v+t} \dots$$

e

$$10^{v+t}\xi = \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t}, \alpha_{v+t+1} \dots \alpha_{v+2t} \dots$$

As potências 10^v e 10^{v+t} foram escolhidas de modo que, após a vírgula, em cada uma das igualdades anteriores aparecesse o período completo θ repetido indefinidamente. Como já mostrado, podemos escrever:

$$10^v\xi = \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v, 00 \dots 0 \dots + 0, \alpha_{v+1} \dots \alpha_{v+t} \dots$$

e

$$10^{v+t}\xi = \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t}, 00 \dots 0 \dots + 0, \alpha_{v+t+1} \dots \alpha_{v+2t} \dots$$

o que implica

$$\begin{aligned}(10^{v+t} - 10^v)\xi = {} & \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t}, 00 \dots 0 \dots \\ & - \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v, 00 \dots 0 \dots\end{aligned}$$

e então $(10^{v+t} - 10^v)\xi = r - s$ onde

$$\begin{aligned}r &:= \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t} \\ &= \sum_{k=0}^{n} 10^{n+v+t-k} \cdot \beta_k + \sum_{l=1}^{v} 10^{v+t-l} \cdot \alpha_l + \sum_{j=1}^{t} 10^{t-j} \cdot \alpha_{v+j}\end{aligned}$$

e

$$s := \beta_0\beta_1 \dots \beta_n\alpha_1\alpha_2 \dots \alpha_v = \sum_{k=0}^{n} 10^{n+v-k} \cdot \beta_k + \sum_{i=1}^{v} 10^{v-i} \cdot \alpha_i.$$

Portanto, $r - s \in \mathbb{Q}$, donde $\xi = \dfrac{r-s}{10^v(10^t - 1)} \in \mathbb{Q}$.
O caso $\alpha_0 \in \mathbb{Z}_-^*$ é deixado como exercício.

□

Observação. A expressão $\dfrac{r-s}{10^v(10^t - 1)}$ obtida na prova acima, é chamada a fração geratriz da dízima periódica $\alpha_0, \alpha_1\alpha_2 \dots \alpha_v\alpha_{v+1} \dots \alpha_{v+t}\alpha_{v+t+1} \dots$

6.5 $\mathbb{R}$ é um corpo ordenado e completo

Assim como o conjunto dos racionais $\mathbb{Q}$, o conjunto dos números reais $\mathbb{R}$ é um corpo ordenado. Entretanto, $\mathbb{R}$ tem a propriedade da completude, que o difere do conjunto $\mathbb{Q}$.

Como $\mathbb{R}$ é completo, podemos demonstrar a existência de raízes n-ésimas de números reais positivos.

Teorema 6.31. *Para cada $x > 0$, real, e cada $n > 0$, inteiro, existe um único número real $y > 0$ tal que $y^n = x$. Este número y é designado por $\sqrt[n]{x}$ ou por $x^{1/n}$.*

Demonstração. É claro que não pode existir mais de um y nas condições acima, pois de $0 < y_1 < y_2$ resulta $y_1^n < y_2^n$.

Seja E o conjunto de todos os reais positivos t tais que $t^n < x$.

Se $t = x/(1+x)$, então $0 < t < 1$; portanto, $t^n \leq t < x$, de modo que E não é vazio.

Seja $t_0 = 1 + x$. Se $t > t_0$, então $t^n \geq t > x$, de modo que $t \notin E$ e t_0 é uma cota superior de E.

Seja $y = \sup E$. Suponhamos $y^n < x$. Consideremos h tal que $0 < h < 1$ e $h < \dfrac{x - y^n}{(1+y)^n - y^n}$. Seja $\binom{n}{m}$ o coeficiente de z^m no desenvolvimento do binômio $(1+z)^n$, temos:

$$\begin{aligned}(y+h)^n &= y^n + \binom{n}{1}y^{n-1}h + \binom{n}{2}y^{n-2}h^2 + \ldots + \binom{n}{n}h^n \\ &\leq y^n + h\left[\binom{n}{1}y^{n-1} + \binom{n}{2}y^{n-2} + \ldots + \binom{n}{n}\right] \\ &= y^n + h[(1+y)^n - y^n] \\ &< y^n + (x - y^n) = x.\end{aligned}$$

Logo, $y + h \in E$, contradizendo o fato de y ser cota superior de E.

Suponhamos $y^n > x$. Consideremos k tal que $0 < k < 1, k < y$, e, ainda, $k < \dfrac{y^n - x}{(1+y)^n - y^n}$.

Então, para $t \geq y - k$, temos:

$$\begin{aligned}t^n \geq (y-k)^n &= y^n - \binom{n}{1}y^{n-1}k + \binom{n}{2}y^{n-2}k^2 - \ldots + (-1)^n\binom{n}{n}k^n \\ &= y^n - k\left[\binom{n}{1}y^{n-1} - \binom{n}{2}y^{n-2}k + \ldots - (-1)^n\binom{n}{n}k^{n-1}\right] \\ &\geq y^n - k\left[\binom{n}{1}y^{n-1} + \binom{n}{2}y^{n-2} + \ldots + \binom{n}{n}\right] \\ &= y^n - k\,[(1+y)^n - y^n] > y^n - (y^n - x) = x.\end{aligned}$$

Assim, $y - k$ é uma cota superior de E, contradizendo o fato de $y = \sup E$.

Portanto, $y^n = x$.

□

6.6 A unicidade de $\mathbb{R}$

Nesta seção mostraremos que não existem outros corpos ordenados completos além de $\mathbb{R}$. Ou seja, mostraremos que quaisquer dois corpos ordenados completos são isomorfos. Para isso, definiremos isomorfismo e seguiremos o roteiro feito por Spivak em [34].

Definição 6.24. Se F_1 e F_2 são dois corpos, um *isomorfismo* de F_1 em F_2 é uma função f de F_1 em F_2 com as seguintes propriedades:

(a) Se $x \neq y$, então $f(x) \neq f(y)$.

(b) Se $z \in F_2$, então $z = f(x)$ para algum $x \in F_1$.

(c) Se $x, y \in F_1$, então
$$f(x \oplus y) = f(x) \mathbf{+} f(y),$$
$$f(x \odot y) = f(x) \mathbf{.} f(y);$$

Se F_1 e F_2 são corpos ordenados, com relações de ordem $\prec$ e $\mathbf{<}$ respectivamente, também é preciso satisfazer:

(d) Se $x \prec y$, então $f(x) \mathbf{<} f(y)$.

Os corpos F_1 e F_2 são chamados isomorfos se existe um isomorfismo entre eles. Corpos isomorfos podem ser considerados como essencialmente o mesmo, isto é, qualquer propriedade de um, vale automaticamente para o outro.

Dado um corpo ordenado F, vamos verificar se F é isomorfo a $\mathbb{R}$. Seja F um corpo, com as operações $\mathbf{+}$ e $\mathbf{.}$, e "elementos positivos" $\mathbf{P}$; escrevemos $a \mathbf{<} b$ para significar que $b \mathbf{-} a \in \mathbf{P}$.

Teorema 6.32. *Se F é um corpo ordenado completo, então F é isomorfo a $\mathbb{R}$.*

Demonstração. Vamos construir uma função f de $\mathbb{R}$ em F e mostrar que existe um isomorfismo entre $\mathbb{R}$ e F.

Inicialmente, definimos f nos inteiros como segue:

$$\begin{aligned} f(0) &= \mathbf{0} \\ f(n) &= \underbrace{\mathbf{1+\cdots+1}}_{n \text{ vezes}} && \text{para } n > 0, \\ f(n) &= \underbrace{-(\mathbf{1+\cdots+1})}_{|n| \text{ vezes}} && \text{para } n < 0, \end{aligned}$$

É fácil verificar que:

$$f(m+n) = f(m) \mathbf{+} f(n); \quad f(m \cdot n) = f(m) \mathbf{.} f(n),$$

para todos os inteiros m, n e é conveniente denotar $f(n)$ por $\mathbf{n}$. Definimos f nos números racionais por:

$$f(m/n) = \mathbf{m/n} = \mathbf{m} \mathbf{.} \mathbf{n}^{-\mathbf{1}}$$

Note que, como f é um corpo ordenado, $\mathbf{1+}\cdots\mathbf{+1} \neq 0$ se $n > 0$. Esta definição faz sentido porque se $m/n = k/l$, então $ml = nk$, daí $\mathbf{m.l} = \mathbf{k.n}$, ou seja, $\mathbf{m.n^{-1}} = \mathbf{k.l^{-1}}$. É fácil verificar que:

$$f(r_1 + r_2) = f(r_1)\mathbf{+}f(r_2)$$
$$f(r_1 \cdot r_2) = f(r_1)\,\mathbf{.}\,f(r_2)$$

para todos os racionais r_1 e r_2, e que $f(r_1) < f(r_2)$ se $r_1 < r_2$.

A definição de $f(x)$ para x arbitrário é baseada na ideia familiar de que qualquer número real é determinado pelos números racionais menores do que ele. Para qualquer $x \in \mathbb{R}$, seja A_x o subconjunto de F consistindo de todos $f(r)$, para todos os números racionais $r < x$. O conjunto A_x é certamente não vazio, e é limitado superiormente, pois se r_0 é um número racional com $r_0 > x$, então $f(r_0) > f(r)$, para todo $f(r)$ em A_x. Como F é um corpo ordenado completo, o conjunto A_x tem uma menor cota superior; definimos $f(x)$ como $\sup A_x$.

Temos assim $f(x)$ definida de dois modos diferentes, primeiro para x racional e depois para x arbitrário. É necessário mostrar que estas duas definições coincidem para x racional. Em outras palavras, se x é um número racional, queremos mostrar que $\sup A_x = f(x)$, onde $f(x)$ denota $\mathbf{m/n}$, para $x = m/n$. Isto não é automático, mas depende da completude de F.

Como F é completo, os elementos $\underbrace{\mathbf{1+}\cdots\mathbf{+1}}_{n \text{ vezes}}$, para números naturais n formam um conjunto não limitado superiormente. As consequências deste fato para $\mathbb{R}$ têm equivalência em F : em particular, se a e b são elementos de F com $a<b$, então existe um número racional r tal que $a<f(r)<b$.

Tendo feito esta observação, voltemos a demonstração de que as duas definições de $f(x)$ coincidem para x racional. Se y é um número racional com $y < x$, então já vimos que $f(y)<f(x)$. Portanto, todo elemento de A_x é $<f(x)$. Consequentemente, $\sup A_x \leq f(x)$.

Por outro lado, suponha que temos $\sup A_x < f(x)$. Então existiria um número racional r tal que $\sup A_x < f(r) < f(x)$. Mas a condição $f(r) < f(x)$ significa que $r < x$, o que implica que $f(r)$ está no conjunto A_x; isto contradiz a condição $\sup A_x < f(r)$. Logo, $\sup A_x = f(x)$.

Temos portanto uma função bem definida f de $\mathbb{R}$ em F. A fim de mostrar que f é um isomorfismo, devemos verificar as condições $(a) - (d)$ da definição. Começaremos com a condição (d).

Se x e y são números reais com $x < y$, então claramente A_x está contido em A_y. Portanto,

$f(x) = \sup A_x \leq \sup A_y = f(y)$

Para rejeitar a possibilidade de igualdade, note que existem números racionais r e s com $x < r < s < y$. Nós sabemos que $f(r) < f(s)$. Daí, segue que

$$f(x) \leq f(r) < f(s) \leq f(y).$$

o que prova (d).

A condição (a) segue imediatamente da (d) : Se $x \neq y$, então tanto $x < y$ ou $y < x$; no primeiro caso $f(x) < f(y)$, e no segundo caso $f(y) < f(x)$; em qualquer dos casos $f(x) \neq f(y)$.

Para provar (b), seja a um elemento de F, e seja B o conjunto de todos os números racionais r com $f(r) < a$. O conjunto B não é vazio, e é limitado superiormente, porque existe um número racional s com $f(s) > a$, de modo que $f(s) > f(r)$ para r em B, o que implica que $s > r$. Seja x a menor cota superior de B; afirmamos que $f(x) = a$. Para provar isto, é suficiente eliminar as alternativas $f(x) < a$ e $a < f(x)$. No primeiro caso, existiria um número racional r com $f(x) < f(r) < a$. Mas, isto significaria que $x < r$ e que r estaria em B, o que contradiz o fato de que $x = \sup B$. No segundo caso, existiria um número racional r com $a < f(r) < f(x)$. Isto implicaria que $r < x$. Como $x = \sup B$, teríamos $r < s$ para algum s em B. Portanto, $f(r) < f(s) < a$, contradição. Portanto, $f(x) = a$, provando (b).

Para mostrar (c), sejam x e y números reais e suponha que $f(x+y) \neq f(x)+f(y)$. Então, $f(x+y) < f(x)+f(y)$ ou $f(x)+f(y) < f(x+y)$. No primeiro caso, existiria um número racional r tal que $f(x+y) < f(r) < f(x)+f(y)$. Isto significaria que $x+y < r$. Portanto, r poderia ser escrito como a soma de dois números racionais $r = r_1 + r_2$, onde $x < r_1$ e $y < r_2$. Então, usando os fatos verificados sobre f para números racionais, seguiria que $f(r) = f(r_1 + r_2) = f(r_1)+f(r_2) > f(x)+f(y)$. Contradição. O outro caso é análogo a este.

Finalmente, se x e y são números reais positivos, o mesmo raciocínio mostra que $f(x.y) = f(x).f(y)$; o caso geral é uma simples consequência.

□

6.7 $\mathbb{R}$ é não-enumerável

Segundo Georg Cantor, dois conjuntos são equivalentes, ou têm a mesma cardinalidade, quando é possível estabelecer uma correspondência que leve elementos distintos de um conjunto em elementos distintos do outro, todos os elementos de um e do outro conjunto sendo objeto dessa correspondência. Em outras palavras, dois conjuntos são equivalentes, ou têm a mesma cardinalidade, quando existe uma bijeção entre eles.

Com relação a conjuntos finitos, a equivalência entre dois conjuntos implica em possuírem o mesmo número de elementos, ou seja, a mesma cardinalidade. E quando se consideram conjuntos infinitos? Pode-se afirmar que todos têm a mesma cardinalidade? Georg Cantor respondeu a esta questão e mostrou que o conjunto dos números reais tem cardinalidade diferente dos números naturais.

Cantor passou a chamar de enumerável a todo conjunto que tem a mesma cardinalidade dos números naturais. Mostraremos que o conjunto dos números reais é não-enumerável. Para isso, definiremos inicialmente o conceito de enumerabilidade e provaremos alguns resultados importantes, como por exemplo, que todo conjunto infinito contém um subconjunto infinito enumerável. Este resultado significa que o enumerável é o "menor" dos infinitos.

O conjunto dos números racionais é enumerável, entretanto o conjunto dos números reais não é enumerável. Para provar isso, utilizaremos o método desenvolvido por Cantor, chamado método da diagonal.

Estudaremos o intervalo $(0,1)$, que tem a mesma cardinalidade que a reta toda, pois existe uma bijeção $y = tg(\pi x - \pi/2)$ do intervalo $(0,1)$ na reta toda $(-\infty, \infty)$.

Usaremos a representação decimal e mostraremos que nenhuma função $f : \mathbb{N} \to (0,1)$ é sobrejetiva. Na seção 6.4 mostramos que dado $x > 0$ real e, n_0 o maior inteiro tal que $n_0 \leq x$, a representação decimal de x é $n_0, n_1 n_2 n_3 \ldots$, onde cada dígito n_i é igual a $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Logo, todo número real decimal x com $0 < x < 1$ tem uma representação decimal na forma $x = 0, n_1 n_2 n_3 \ldots$. Deve-se notar que certos números reais têm duas representações nesta forma, por exemplo, o número racional $1/10$ tem as representações: $0,1000\cdots$ e $0,0999\cdots$. Assim, poderia-se decidir em favor de uma dessas representações, mas isso não será necessário.

Suponha que exista uma enumeração $x_1, x_2, x_3, \ldots$ de todos os números reais satisfazendo $0 < x < 1$ dada por:

$$\begin{aligned} x_1 &= 0, y_{11} y_{12} y_{13} \ldots \\ x_2 &= 0, y_{21} y_{22} y_{23} \ldots \\ x_3 &= 0, y_{31} y_{32} y_{33} \ldots \\ &\vdots \end{aligned}$$

onde os y_{ij} são algarismos de 0 a 9. Escrevemos $f(1) = x_1, f(2) = x_2, f(3) = x_3, \ldots$. Considere o número $y = 0, y_1 y_2 y_3 \ldots$ com y_1 diferente de $0, y_{11}$ e 9; y_2 diferente de $0, y_{22}$ e 9; y_3 diferente de $0, y_{33}$ e 9, etc. É fácil verificar que $0 < y < 1$. Desse modo, o número y não é nenhum dos números com duas representações decimais, desde que $y_n \neq 0, 9$. Ao mesmo tempo, $y \neq x_n$ para todo n (desde que o $n-$ésimo dígito da representação decimal de y e x_n é diferente). Portanto, qualquer coleção enumerável de números reais no intervalo $(0,1)$ omitirá pelo menos um número real pertencente a este intervalo. Desse modo, f não é sobrejetiva e este intervalo não é enumerável. Como $(0,1) \subset \mathbb{R}$ temos que $\mathbb{R}$ é não-enumerável.

Daremos uma outra demonstração de que o conjunto dos números reais não é enumerável. Para isso, precisamos provar o teorema dos intervalos encaixados, dado a seguir. Esta demonstração é a mais próxima da demonstração original da não enumerabilidade de $\mathbb{R}$ feita por Cantor.

Teorema 6.33. *Dada uma sequência decrescente $I_1 \supset I_2 \supset \ldots \supset I_n \supset \ldots$ de intervalos limitados e fechados $I_n = [a, b]$, então existe pelo menos um número real c tal que $c \in I_n$ para todo $n \in \mathbb{N}$.*

Demonstração. As inclusões $I_n \supset I_{n+1}$ significam que

$$a_1 \leq a_2 \leq \ldots \leq a_n \leq \ldots \leq b_n \leq \ldots \leq b_2 \leq b_1.$$

Seja A o conjunto dos a_n, isto é, $A = \{a_1, a_2, \ldots, a_n, \ldots\}$, e B o conjunto dos b_n, isto é, $B = \{b_1, b_2, \ldots, b_n, \ldots\}$. O conjunto A é limitado superiormente (cada b_n é uma cota superior de A) e o conjunto B é limitado inferiormente (cada a_n é uma cota inferior de B). Sejam $a = \sup A$ e $b = \inf B$. Temos que $a \leq b_n$, para cada n. Assim, a é cota inferior de B e, portanto, $a \leq b$. Podemos então escrever:

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

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, $[a, b] \subset \cap_{n=1}^{\infty} I_n$. 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 $y_m \notin I_m$. Concluímos então que $\cap I_n = [a, b]$.

□

Observação.

1. A condição de que os intervalos I_n sejam fechados é essencial no teorema 6.33. Por exemplo, os intervalos $I_n = (0, 1/n)$ são encaixados e limitados, mas não são fechados. É fácil verificar que sua interseção é vazia.

2. A condição de que os intervalos I_n sejam limitados também é essencial no teorema 6.33. Por exemplo, $I_n = [0, +\infty)$ é uma família de intervalos fechados e encaixados, porém não limitados e sua interseção é vazia.

Proposição 6.7. *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração. Mostraremos que nenhuma função $f : \mathbb{N} \to \mathbb{R}$ pode ser sobrejetiva. Para isto, supondo f dada, construiremos uma sequência decrescente $I_1 \supset I_2 \supset \ldots \supset I_n \supset \ldots$ de intervalos limitados e fechados tais que $f(n) \notin I_n$. Então se c é um número real pertencente a todos os I_n, nenhum dos valores $f(n)$ pode ser igual a c, logo f não é sobrejetiva. Para obter os intervalos, começamos tomando $I_1 = [a_1, b_1]$ tal que $f(1) < a_1$ e, supondo obtidos $I_1 \supset I_2 \supset \ldots \supset I_n$ tais que $f(j) \notin I_j$, olhamos para $I_n = [a_n, b_n]$. Se $f(n+1) \notin I_n$, podemos simplesmente tomar $I_{n+1} = I_n$. Se, porém, $f(n+1) \in I_n$, pelo menos um dos extremos, digamos a_n, é diferente de $f(n+1)$, isto é, $a_n < f(n+1)$. Neste caso, tomamos $I_{n+1} = [a_{n+1}, b_{n+1}]$, com $a_{n+1} = a_n$ e $b_{n+1} = (a_n + f(n+1))/2$. □

Corolário 6.2. *Todo intervalo não-degenerado de números reais é não-enumerável.*

Com efeito, $f : (0,1) \to (a,b)$ definida por $f(x) = (b-a)x + a$ é uma bijeção do intervalo aberto $(0,1)$ no intervalo aberto arbitrário (a,b), assim, 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, consequentemente, para cada $n \in \mathbb{Z}$, o intervalo $(n, n+1]$ seria enumerável (pois $x \to x + n$ é uma bijeção de $(0,1]$ sobre $(n, n+1]$). Mas $\mathbb{R} = \cup_{n\in\mathbb{Z}}(n, n+1]$ seria enumerável, por ser uma reunião enumerável dos conjuntos $(n, n+1]$.

Corolário 6.3. *O conjunto dos números irracionais não é enumerável.*

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

Os irracionais $\mathbb{R} - \mathbb{Q}$ constituem um conjunto não-enumerável, logo, formam a maioria dos reais.

6.8 A densidade dos racionais e irracionais em $\mathbb{R}$

Definição 6.25. Um conjunto $X \subset \mathbb{R}$ chama-se denso em $\mathbb{R}$ quando todo intervalo aberto (a, b) contém algum ponto de X.

Exemplo 6.4. $X = \mathbb{R} - \mathbb{Z}$ 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.

Teorema 6.34. *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 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 $\frac{1}{p}$. 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 ideia intuitiva da demonstração. 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 $\frac{m_0 - 1}{p} \leq a < b \leq \frac{m_0}{p}$. Isso 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 $\frac{\sqrt{2}}{p}$. 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 $b \leq \frac{m_0\sqrt{2}}{p}$ então o número irracional $\frac{(m_0 - 1)\sqrt{2}}{p}$ pertence ao intervalo (a, b). □

A proposição anterior pode ser reformulada assim: todo intervalo não-degenerado I contém números racionais e irracionais.

6.9 Exercícios

1. Seja (x_n) uma sequência convergindo para um limite racional b; $[(x)]$ a classe de equivalência contendo (x_n); (y_n) outra sequência na classe de equivalência $[(x)]$. Prove que (y_n) converge para b.

2. Considere o conjunto dos números reais como sendo o conjunto das classes de equivalência das sequências de Cauchy de números racionais.

   (a) Prove que $\mathbb{R}$ é um corpo, isto é, verifique todos os axiomas de corpo.

(b) Prove que os reais satisfazem a lei da tricotomia.

3. Prove que o conjunto $\{r/r > 0, r^2 > 2\}$ é um corte.

4. Prove que a união de um número finito de cortes é um corte.

5. Considere a condição (iii) da definição 6.9, de cortes de Dedekind. Quais seriam as dificuldades encontradas no desenvolvimento da teoria dos números reais se esta condição fosse omitida?

6. Considere os reais de Dedekind.

   (a) Prove que a adição em $\mathbb{R}$ satisfaz as leis da comutatividade, associatividade, identidade da adição e inversa aditiva.

   (b) Prove que os reais de Dedekind satisfazem a lei da tricotomia.

   (c) Prove que a multiplicação em $\mathbb{R}$ satisfaz as leis da comutatividade, associatividade, identidade, inversa e lei da distributividade (apenas para cortes não-negativos).

7. A propriedade do supremo (teorema 6.29) foi deduzida do teorema de Dedekind (teorema 6.28). Mas, estes dois teoremas são equivalentes. Para demonstrar esta afirmação, admita a propriedade do supremo como postulado, além das propriedades usuais dos números reais, e demonstre o teorema de Dedekind sem considerar cortes no conjunto dos números racionais.

8. Observe que a propriedade do supremo tem como consequência a propriedade dos intervalos encaixados, que diz: se $I_n = [a_n, b_n]$ é uma família de intervalos fechados tais que $I_1 \supset I_2 \supset \ldots I_n \supset \ldots$ e o comprimento $|I_n| = b_n - a_n$ tende a zero, então existe um e um só número c pertencendo a todos os intervalos I_n. Prove que essa última propriedade implica a propriedade do supremo, ficando assim provado que a propriedade do supremo equivale à propriedade dos intervalos encaixados.

9. Prove que se postularmos que "toda sequência não decrescente e limitada é convergente" conseguiremos provar a propriedade dos intervalos encaixados, portanto, também a propriedade do supremo, estabelecendo assim que essa propriedade é equivalente a afirmar que "toda sequência não decrescente e limitada converge".

10. Observe que a propriedade do supremo tem como consequência que toda sequência de Cauchy converge. Prove a recíproca dessa proposição, isto é, prove que se toda sequência de Cauchy converge, então vale a propriedade do supremo, ficando assim provado que essa propriedade é equivalente a toda sequência de Cauchy ser convergente.

Capítulo 7

Extensões dos Números Reais

7.1 Extensões multidimensionais

7.1.1 Os Números Complexos

Os *números complexos* são a extensão mais antiga e conhecida dos números reais. Inicialmente surgiram como uma necessidade para dar sentido a equações do tipo

$$x^2 + 1 = 0.$$

Tal equação não tem solução no mundo dos reais. Se existisse uma solução real, nos levaria a ter que aceitar a existência de um real cujo quadrado é negativo ($\exists x \in \mathbb{R}$; $x^2 = -1 < 0$). O que é absurdo, pois, em todo corpo ordenado (como $\mathbb{R}$) o quadrado de um número nunca é negativo. De qualquer, se "*imaginarmos*"que existisse um tal i tal que $i^2 = -1$, teríamos

$$x^2 + 1 = x^2 - i^2 = (x - i)(x + i),$$

de onde, $x = i$ e $x = -i$ seriam justamente soluções (não reais, imaginárias?) de $x^2 + 1 = 0$.

Se os números reais representam um modelo algébrico de uma linha reta (unidimensional), onde estariam localizados o i e $-i$?

Fica evidente que os números reais precisam ser estendidos a um conjunto de tal forma que contenham os números i e $-i$.

Tal extensão existe e é chamada de conjunto dos números complexos, e denotado por $\mathbb{C}$. Eles formam uma estrutura algébrica (corpo). Atualmente, possuem uma teoria bem elaborada e com muitas aplicações importantes em diversas áreas. Os complexos foram vistos com desconfiança pelos matemáticos por muitos anos, sendo usados somente com relutância, pois aparentavam não ter qualquer base na realidade. Interpretando os complexos como pontos do plano ($\mathbb{C} = \mathbb{R}^2$) podemos dizer que se trata de uma extensão bidimensional dos reais.

Um *número complexo* z é um número da forma

$$z = a + bi$$

onde $a, b \in \mathbb{R}$ e i chamado de unidade imaginária tal que $i^2 = -1$. O real a é chamado parte real de z e b a parte imaginária de z. O conjunto formado por números complexos

é denotado por $\mathbb{C}$. Portanto,

$$\mathbb{C} = \{a + bi;\ a, b \in \mathbb{R},\ i^2 = -1\}$$

A soma e produto de dois complexos é definido por

$$(a + bi) + (c + di) = (a + c) + (b + d)i. \tag{1}$$
$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i. \tag{2}$$

onde $i^2 = -1$. Essas operações fazem de $\mathbb{C}$ um corpo. Os elementos neutros dessas operações são $0 = 0 + 0\,i$ e $1 = 0 + 1\,i$. O inverso aditivo de $z = a + bi$ é $-z = -a - bi$ e o inverso multiplicativo de $z = a + bi \neq 0$ é $z^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}i$.

Com esta abordagem, fica evidente que $\mathbb{R} \subset \mathbb{C}$, pois todo real a pode ser escrito da forma $a + 0\,i$.

Uma das características importantes dos complexos é que cada $z = a + bi$ pode ser vista como um ponto (a, b) do plano $\mathbb{R}^2$.

Números complexos vistos como o pontos de plano $\mathbb{R}^2$

Definimos o conjunto dos números complexos, $\mathbb{C}$ como sendo o plano $\mathbb{R}^2$ munido de duas operações definidas como

$$(a, b) + (c, d) = (a + c,\ b + d) \tag{3}$$
$$(a, b) \cdot (c, d) = (ac - bd,\ bc + ad). \tag{4}$$

Fica como exercício verificar os nove axiomas (de corpo), que nos permitem afirmar que $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$, é de fato, um corpo.

Quando nos referimos ao conjunto dos reais como sendo unidimensional e o dos complexos bidimensional, estamos nos referindo à *dimensão* deles visto como espaços vetoriais[1] sobre o corpo $\mathbb{R}$.

Foi visto que $\mathbb{C}$ é um corpo que não pode ser ordenado, pois existe $i \in \mathbb{C}$ tal que $i^2 < 0$. Entretanto, diferente de $\mathbb{R}$, é um conjunto algebricamente fechado. Em $\mathbb{C}$, todo polinômio tem raiz (Teorema Fundamental da Álgebra).

Complexos como matrizes

Uma outra forma de representar um número complexo $a + bi$ é como matrizes quadradas de ordem dois.

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

A soma e produto é dado pelas operações usuais de matrizes.

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ -(b + d) & a + c \end{bmatrix}$$

[1] assumiremos que o leitor conhece os axiomas que caracterizam um espaço vetorial V sobre um corpo K de dimensão finita, onde a dimensão de V é definida como o número de elementos de uma base de V

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -(bc + ad) & -bd + ac \end{bmatrix}$$

A unidade imaginária i é identificada com $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

Note que

$$z = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Se usássemos a notação $a = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ e $i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, escreveríamos simplesmente $z = a + bi$.

7.1.2 Quaternions

Tanto $\mathbb{R}$ como $\mathbb{C}$ são espaços vetoriais sobre o corpo $\mathbb{R}$.

A base canônica de $\mathbb{R}$ é $\{1\}$, todo real é combinação linear de 1 ($a = a \cdot 1$). Assim, $\dim \mathbb{R} = 1$. O tabela do produto dos elementos da base de $\mathbb{R}$ se reduz a

$\cdot$	1
1	1

A base canônica de $\mathbb{C}$ é $\{1, i\}$ todo complexo z é combinação linear de 1 e i ($z = a + bi$). Portanto, $\dim \mathbb{C} = 2$. A tabela do produto dos elementos da base é

$\cdot$	1	i
1	1	i
i	i	-1

A tabela mostra a regra básica que é utilizada para lidar com a quantidade imaginária i ($i^2 = -1$).

De modo análogo, existe um espaço vetorial $\mathbb{H}$ cujo corpo é $\mathbb{R}$ com a base canônica dada pelo conjunto $\{1, i, j, k\}$ e a regra para multiplicar os elementos da base é

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Do mesmo modo que em $\mathbb{C}$ foi suficiente colocar a regra $i^2 = -1$. Em $\mathbb{H}$ a tabela poderia ser resumida como

$$i^2 = j^2 = k^2 = ijk = -1$$

Assim pode-se escrever

$$\mathbb{H} = \{\, a + bi + cj + dk\,; \quad a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = ijk = -1 \,\}$$

$\mathbb{H}$ é chamado conjunto dos *quatérnios*. Foram descobertos por Hamilton em 1835. Eles são uma extensão natural dos complexos. Os pontos de $\mathbb{H}$ da forma $a + bi + 0\,j + 0\,k = a + bi$ são identificados com os complexos. Assim $\mathbb{C} \subset \mathbb{H}$. Esse tipo de extensões pode realizadas teoricamente *ad infinitum*, seguindo um processo chamado *construcción de Cayley-Dickson*. Sempre duplicando a dimensão. O próximo é conhecido por Octônios.

7.2 Extensões unidimensionais

7.2.1 Os Números Hiper-reais

Antes de falarmos dos hiper-reais é preciso lembrar uma consequência importante de um corpo ordenado e completo. Na Proposição 1.12 foi mostrado que:

Todo corpo ordenado e completo é necessariamente arquimediano.

Portanto, $\mathbb{R}$ é arquimediano. Ou seja, em $\mathbb{R}$ o subconjunto dos naturais $\mathbb{N}$ é um conjunto ilimitado superiormente. Ser arquimediano tem a seguinte consequência importante.

$$\textit{Seja } a \in \mathbb{R},\ a \geq 0 \ \textit{ tal que } \ \forall\, \epsilon > 0, a < \epsilon \ \textit{ então } \ a = 0.$$

A prova disso, é bem simples. Como $a \geq 0$. Suponha que $a \neq 0$, logo $a > 0$. Sendo $\mathbb{R}$ arquimediano, existe $n \in \mathbb{N}$ tal que $0 < \dfrac{1}{n} < a$. O que contraria a hipótese, pois existe $\epsilon = 1/n$ tal que $0 < \epsilon < a$. Desse modo, só resta concluir que $a = 0$.

Esse resultado, permitiu escrever

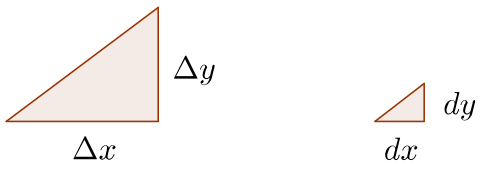
> *Se uma quantidade não-negativa fosse tão pequena que ele é menor do que qualquer outra dada, então ele certamente não poderia ser outra coisa senão zero. Para aqueles que perguntam o que é uma quantidade infinitamente pequena em matemática, nós respondemos que ele é realmente zero. Portanto, não há tantos mistérios escondidos nesse conceito como geralmente eles acreditam. Esses supostos mistérios tornaram o cálculo do infinitamente pequeno bastante duvidoso para muitas pessoas. Essas dúvidas que possam permanecer as eliminaremos completamente, nas páginas seguintes, onde vamos explicar este cálculo.*
>
> *Leonhard Euler*

Infinitesimais

Um *infinitésimo* ou *infinitesimal* é definido como uma *quantidade infinitamente pequena*. Nesse sentido no mundo dos reais e nas palavras de Euler, só pode ser o zero. Entretanto, os infinitesimais desempenharam um papel essencial no surgimento e desenvolvimento do cálculo diferencial e integral. As marcas disso ainda nos acompanham na notação usada por Leibniz no cálculo de derivadas e integrais.

Por exemplo, a notação para a derivada.

$$\frac{dy}{dx} = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x}$$

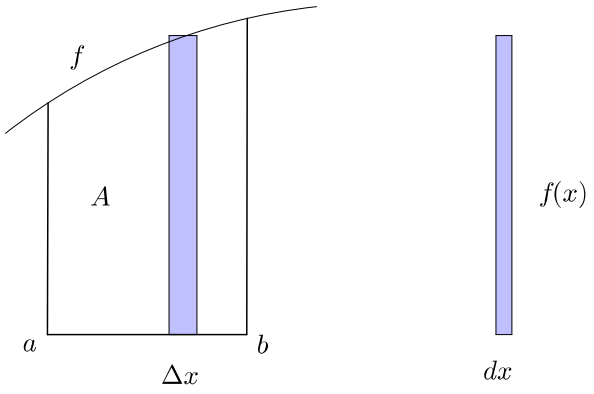


As quantidades dy e dx chamadas *diferenciais* são exemplos de infinitesimais. O que é exatamente dy e dx? Será que $\Delta y \to dy$ e $\Delta x \to dx$? Bom, sabemos que se dy e dx fossem reais, certamente $dy = 0$ e $dx = 0$.

Também na notação de cálculo de integrais. Por exemplo no cálculo de áreas.

$$A = \int_a^b f(x)dx = \lim_{|P|\to 0} \sum_{i=1}^{n} f(x_i^*)\Delta x,$$

onde $P = \{x_0 < x_i < \cdots < x_n\}$ é uma partição de $[a,b]$, $|P| = \max_{1\le i\le n} |x_i - x_{i-1}|$ e $x_i^* \in (x_{i-1}, x_i)$. Se $|P| \to 0$ então $n \to \infty$ e $\Delta x \to 0$.



Sabemos que o símbolo $\int$ nada mais do que um "S"esticado, representando uma soma ou somatório, cujo função é juntar ou "*integrar*"*áreas infinitesimais* de retângulos, digamos de altura $f(x)$ e base dx cujas áreas infinitesimais seriam justamente $f(x)dx$. No mundo real $dx = 0$ logo $f(x)dx = 0$. Assim $A = \int_a^b f(x)dx = 0$? Bom um jeito de lidar com isso, era afirmar que esses infinitesimais eram menores do que qualquer positivo, mas que não eram nulos. Seriam uma espécie de *indivisíveis* mesmo que não soubessem explicar o que seria de fato. Algo bem similar ao uso de números imaginários que não se sabiam o que eram, porém que funcionavam na hora dos cálculos.

Por exemplo se o objetivo era calcular a derivada de $f(x) = x^2$, então Leibniz explicava assim seu método: tomamos um infinitésimo dx, calculamos o incremento (ou diferencial) $df = f(x+dx) - f(x)$, dividimos entre a quantidade (não nula) dx. Resultando

$$\frac{df}{dx} = \frac{(x+dx)^2 - x^2}{dx} = \frac{2xdx + (dx)^2}{dx} = 2x + dx.$$

Agora, como dx é infinitesimal e, portanto, insignificante, a podemos eliminar. Assim,

$$\frac{df}{dx} = 2x + dx = 2x.$$

Note que há algo estranho, inicialmente supõe-se que $dx \neq 0$ e após fazermos as contas como se fosse números reais a eliminamos como se $dx = 0$. Entretanto, mesmo assim, o resultado é correto. Era isso o que se chamava de *Cálculo Infinitesimal*.

Esse tipo de raciocínio foi duramente criticado na época. Levando a diversas discussões filosóficas.

Posteriormente, pelo uso da teoria de limites, esses infinitesimais foram trocados pelo uso de quantidades *arbitrariamente pequenas*, não nulas, porém não infinitamente

pequenas. Euler, Cauchy e outros, reformularam a teoria de derivadas e integrais. Com isso nos livrávamos de ter que usar os estranhos infinitesimais. Mas, agora teríamos que lidar com épsilons e deltas: ϵ, δ, que estudantes que têm um primeiro contato com Cálculo Diferencial e Integral adoram.

Graças aos limites, os infinitesimais haviam sido banidos da matemática. Mas, eles voltaram. Graças ao trabalhos de Abraham Robinson [27]. Se o uso deles funcionava mesmo que não fossem reais, então devia existir um conjunto que fosse uma extensão do reais. Foi esse o trabalho de Robinson com sua Análise Não-Standard. Conseguiu mostrar que é possível estender, de forma rigorosa, o conjunto dos reais num conjunto que contivesse, além dos reais, os infinitesimais e também as quantidades "*infinitamente grandes*"que chamaremos *números infinitos*. Um número infinito é um número ω tal que $\omega > n$, $\forall n \in \mathbb{N}$). A inversa $1/\omega$ é um infinitesimal. Essa extensão dos números reais chamamos *conjunto dos Números Hiper-reais* e denota-se por ${}^*\mathbb{R}$. Recomendamos a leitura do artigo *A revanche dos infinitesimais* de Michèle Artigue [4].

Por exemplo, como os Hiper-reais contém números ω tal que $\omega > n$, $\forall n \in \mathbb{N}$. Então, isso mostra que em ${}^*\mathbb{R}$ o conjunto dos naturais $\mathbb{N}$ é limitado. Assim, ${}^*\mathbb{R}$ não é arquimediano, consequentemente, pela Proposição 1.12 não pode ser completo. Embora possua o subconjunto completo $\mathbb{R}$.

Para aplicar os números hiper-reais, faz-se uso do *princípio de transferência*[2] a qual quando aplicado a problemas de Análise é chamada de Análise Não-Standard.

Uma aplicação imediata da Análise Não-Standard é no cálculo de derivadas e integrais sem ter que usar quantificadores, ou seja, nada de limites ou ϵ's e δ's. Assim, para calcular a derivada de f em x,

$$f'(x) = \text{st}\left(\frac{f(x+dx) - f(x)}{dx}\right)$$

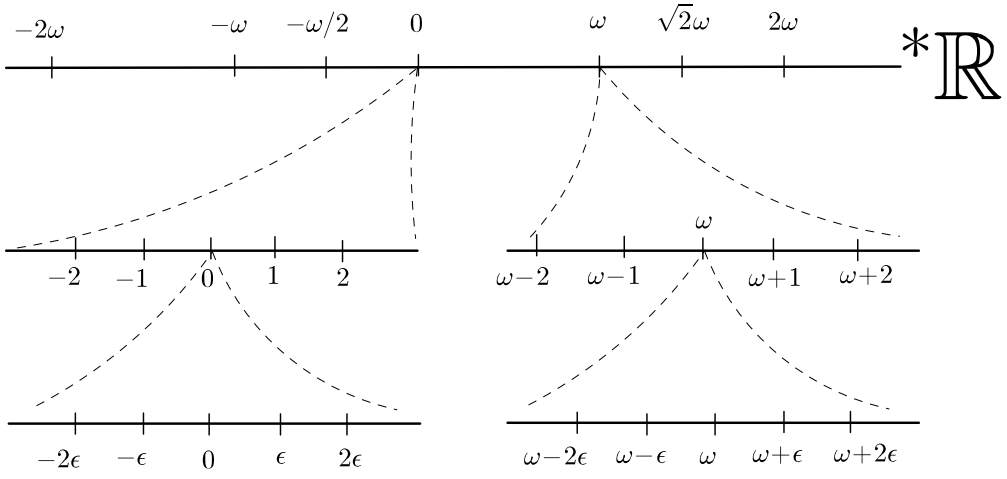
onde dx é um infinitesimal, $\text{st}(\cdot)$ denota a função "*parte standard*". No caso, a parte standard de um *elemento finito a* de ${}^*\mathbb{R}$ é o único real que se encontra infinitamente próximo de a. A função $\text{st}(\cdot)$ age como se fosse uma função que "arredonda"um elemento finito de ${}^*\mathbb{R}$ o transformando num real. Em outras palavras é exatamente o que Leibniz fazia. Para calcular a derivada de $f(x) = x^2$,

$$f'(x) = \text{st}\left(\frac{f(x+dx) - f(x)}{dx}\right) = \text{st}\left(\frac{(x+dx)^2 - x^2}{dx}\right) = \text{st}(2x + dx) = 2x.$$

O hiper-real $2x + dx$ está infinitamente próximo de $2x$.

[2]O princípio de transferência afirma que qualquer sentença exprimível em uma determinada linguagem formal que é verdadeira nos números reais também é verdadeira nos números hiper-reais.

Representação dos hiper-reais



A reta dos hiper-reais sendo mostrados em 3 níveis de escala. Na primeira linha optamos por marcar apenas os *números infinitos*. Por exemplo os naturais devem estar à esquerda de ω. Na segunda linha, após aumentar numa *escala infinita*. Conseguimos visualizar, por exemplo, os reais que se encontram infinitamente próximos de zero. Mas nessa segunda linha ainda não é possível visualizar os infinitesimais. Novamente, aumentando numa *escala infinita*, finalmente podemos vê-los.

Existem várias abordagens para construir os hiper-reais. Os mais simples e intuitivos são aqueles que após definirmos o que se entende por número infinitesimal e número infinito, formamos um novo conjunto, simplesmente acrescentando os reais e definindo uma aritmética nessa extensão dos reais. Bastante intuitivo e prático, mas perde rigorosidade matemática. No lado oposto, se encontram construções via lógica matemática, rigorosas mas requerem ferramentas abstratas da Lógica, tornando-as nada intuitivas. De qualquer forma, mais uma vez, como acontecera com a construção da estrutura algébrica, o corpo dos complexos $\mathbb{C}$, que deu sentido aos imaginários e complexos, que até antes de aparecer $\mathbb{C}$ muitos relutavam em aceitar. Agora temos o conjunto dos hiper-reais,$^*\mathbb{R}$, como a casa natural onde podem morar à vontade, os outrora "sem teto"infinitesimais e infinitos. E nessa casa, mesmo não sendo completa, ainda foram acolhidos os reais.

Referências Bibliográficas

[1] A'CAMPO, N. A natural construction for the real numbers. *Arxiv preprint 2003.* Disponível em http://arxiv.org/abs/math/0301015

[2] ARAGONA, J. *Números Reais*. 1. ed. Livraria da Física, Instituto de Matemática e Estatística- USP, São Paulo, 2010.

[3] ARTHAN, R. D. The Eudoxus Real Numbers. *Arxiv preprint 2004.* Disponível em http://arxiv.org/abs/math/0405454

[4] ARTIGUE, M. *A revanche dos infinitesimais*.
Disponivel em http://blog.kleinproject.org/?p=2669&lang=pt-br

[5] ÁVILA, G. *Introdução à Análise Matemática*. 2ed. Blucher,São Paulo, 2011.

[6] BECKMAN, P. *A History of π*. St. Martin's Press. 1971

[7] BRIDGES, D. S. A constructive look at the real number line. in *Real Numbers, Generalizations of the Reals, and Theories of Continua.* Synthese Library, v 242, p. 29-92 1994.

[8] DEDEKIND, R. Stetigkeit und irrationale zahlen, braunschweig: Vieweg, 1872. *R. Dedekind, Gesarnrnelte mathematische Werke, eds. R. Fricke, E. Noether and O. Ore, Braunschweig: Vieweg*, 1932:1?2, 1930.

[9] EHRLICH, P. (editor) *Real Numbers, Generalizations of the Reals, and theories of continua.* Synthese Library Volume 242, 1994.

[10] EVES, H. *Introdução à História da Matemática.* Editora Unicamp, Unicamp - SP, 2004.

[11] FIGUEIREDO, D. G. *Números Irracionais e Transcendentes*. SBM, Rio de Janeiro, 2011.

[12] FLANNERY, D. *The Square Root of 2: A dialogue concerning a number and a sequence.* Springer, 2006.

[13] HALMOS, P. R. *Naive Set Theory.* Undergraduate Texts in Mathematics, Springer, 1974.

[14] HAVIL, J. *The Irrationals*. Princeton University Press., New Jersey, 2012.

[15] IFRAH, G. *Os Números: a história de uma grande invenção.* Editora Globo, São Paulo, 1985.

[16] KATZ, K. U.; KATZ, M. G. Stevin Numbers and Reality. *Foundations of Science* Volume 17, Issue 2, p. 109–123, 2012.

[17] KEMP, T. *Cauchy's Construction of* $\mathbb{R}$. Lecture Notes. Department of Mathematics. University of California, San Diego, 2014.
Disponível em www.math.ucsd.edu/~tkemp/140A/Construction.of.R.pdf

[18] KLAZAR, M. Real numbers as infinite decimals and irrationality of $\sqrt{2}$. *Arxiv preprint 2009.* Disponível em http://arxiv.org/abs/0910.58704

LANDAU, E. *Foundations of Analysis: The Arithmetic of whole, rational, irrational, and complex numbers.* A.M.S Chelsea Publishing, 3rd ed, 1966.

[19] LIMA, E. L. *Curso de Análise Vol. 1* Projeto Euclides, IMPA, Rio de Janeiro, 2012.

[20] LIMA, E. L. *Análise Real, volume 1*. Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2012.

[21] LIMA, E. L. *Meu Professor de Matemática e outras histórias*. Coleção Professor de Matemática, Rio de Janeiro, SBM, 2011.

[22] MAOR, E. e *: a história de um número.* Editora Record, Rio de Janeiro, 2003.

[23] MARQUES, D. *Teoria dos Números Transcendentes*. Textos Universitários, SBM, Rio de Janeiro, 2013.

[24] PEANO, G. Arithmetices principia, nova methodo exposita. 1889. Tradução em: Jean van Heijenoort, ed.. *From Frege to Godel: A Source Book in Mathematical Logic, 1879–1931.* 3rd ed. Cambridge, Harvard University Press, 1967.

[25] PARSONS, C. *The Uniqueness of the Natural Numbers*. The Jerusalem Philosophical Quarterly 39, pp. 13-44,1990.

[26] PUGH, C. *Real Mathematical Analysis*. Undergraduate Texts in Mathematics, Springer, 2002.

[27] ROBINSON, A. *Introduction to model theory and to the metamathematics of algebra*, Amsterdam, North-Holland, 1963.

[28] RUDIN, W. *Princípios de Análise Matemática* . Ao Livro Técnico S.A. e Editora Universidade de Brasília, Rio de Janeiro, 1971.

[29] RUDIN, W. *Principles of Mathematical Analysis*. 3. ed. McGraw-Hill Book Co., New York, 1976.

[30] STILLWELL, J. *The Real Numbers, An Introduction to Set theory and Analysis.* Undergraduate Texts in Mathematics, Springer, 2013.

[31] STREET, R. An efficient construction of the real numbers. *Gazette of the Australian Math. Soc.* v.12, p. 57-58, 1985.

[32] STREET, R. Updated on the efficient reals. Preprint 2003.
Disponível em www.maths.mq.edu.au/~street/reals.pdf

[33] STRICHARTZ, R. S. *The Way of Analysis*. Jones & Bartlett Learning, 2000.

[34] SPIVAK, M. *Calculus* . Publish or Perish, Inc., Houston, 1994.

[35] WEISS, I. The Real Numbers - A survey of constructions. *Arxiv preprint 2015.* Disponível em http://arxiv.org/abs/1506.03467