Universidade do Minho
Escola de Ciências

Rosa das Dores da Rocha Marinho Almeida

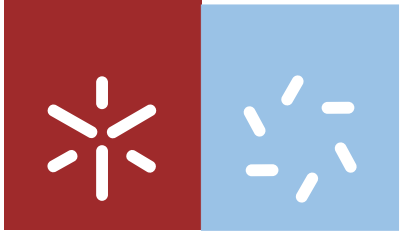
Construção e ordenação dos números - dos naturais aos reais

fevereiro de 2013

Rosa das Dores da Rocha Marinho Almeida Construção e ordenação dos números - dos naturais aos reais

Rosa das Dores da Rocha Marinho Almeida

UMinho | 2013



Universidade do Minho
Escola de Ciências

Rosa das Dores da Rocha Marinho Almeida

Construção e ordenação dos números - dos naturais aos reais

Dissertação de Mestrado
Mestrado em Ciências – Formação Contínua de Professores
Área de Especialização em Matemática

Trabalho realizado sob a orientação da
Doutora Maria Paula Marques Smith

fevereiro de 2013

Rosa das Dores da Rocha Marinho Almeida

Endereço eletrónico: rmarinho.almeida@gmail.com

Título da dissertação: Construção e ordenação dos números – dos naturais aos reais

Orientadora: Doutora Maria Paula Marques Smith

Ano de conclusão: 2013

Mestrado em Ciências - Formação Contínua de Professores, Área de especialização Matemática

Universidade do Minho, 21 de fevereiro de 2013

Assinatura:

AGRADECIMENTOS

Agradeço a todas as pessoas que tornaram possível a realização deste trabalho. Gostaria de expressar a minha gratidão de modo particular:

À Doutora Maria Paula Smith, orientadora deste trabalho, pelo apoio, total disponibilidade e qualidade das sugestões.

Aos colegas e amigos, António José Domingues e Helena Ferreira, pela ajuda, pelo apoio e incentivo constante.

À professora Rosalina Pinheiro, Diretora da minha escola, pelo exemplo e determinação com que encara os problemas e às amigas e colegas, Olívia Canedo e Eduarda Esperança, pela força que me deram nos momentos de maior desânimo.

A todos os meus colegas de trabalho, em particular aos colegas do grupo disciplinar de matemática, pela amizade e pela compreensão.

A toda a minha família, à minha querida mãe pelo carinho sorridente, à minha irmã pela sua calma e amizade e, em particular aos meus sogros, pelo incentivo e pela ajuda que me deram com o meu filho.

Ao meu querido pai, ... que sei estará sempre comigo e a quem procuro nunca desiludir.

Ao meu marido, Pedro, pela paciência durante os meus maus humores, pelos incentivos e por acreditar que tudo isto era possível.

Ao meu filho, André, pelos momentos divertidos e descontraídos.

RESUMO

Os números estão presentes em situações naturais do nosso dia-a-dia e o conceito de número é fundamental no nosso modo de vida. Crianças de tenra idade interiorizam muito naturalmente o conceito de número natural com a contagem de brinquedos e demais objetos que as rodeiam. O conceito de fração chega-lhes de modo também muito natural, basta pensarmos, por exemplo, na precisão que os pais *devem* ter no cortar de um bolo em fatias. Os números negativos aparecem-lhes mais tarde, mas rapidamente se apercebem da diferença entre perder e ganhar ou entre cedo e tarde ou, ainda, entre os andares da cave e os restantes andares do seu prédio. É em conceitos como estes que os números negativos encontram um lugar natural. Os números reais são, contudo, bastante mais sofisticados! Se, por um lado, é natural e útil associar números inteiros positivos a comprimentos, áreas e volumes, como fizeram os antigos gregos, por outro lado, percebeu-se, há muito, muito tempo atrás, que esta associação nos leva a uma dificuldade séria, já que nem todo o comprimento se pode exprimir como uma fração. É claro que um sistema de números, que, se pretende, se relacionem com a noção geométrica de comprimento, tem que ser suficientemente rico para conter todos os números que não são fracções!

O objetivo desta tese é proceder à construção e ordenação dos seguintes conjuntos de números: números naturais, números inteiros, números racionais e números reais. Neste sentido, procedemos à definição dos números naturais através de um conjunto de axiomas, os *axiomas de Peano*, que permitem obter as propriedades aritméticas conhecidas, e fazemos a construção algébrica dos números inteiros e dos números racionais, *aparecendo* estes números, em ambos os casos, como classes de equivalência de pares de números naturais, os primeiros, e de pares de números inteiros, os segundos. A construção dos números reais é feita com métodos da Análise, via sucessões de Cauchy.

ABSTRACT

Numbers are present in many natural situations of our day-to-day life and the concept of number is fundamental to our lifestyle. From early age children absorb very naturally the concept of number by counting their toys and other objects that surround them. The concept of fraction also arises naturally - one just has to think, for example, of the precision that parents must have when slicing a cake! They meet negative numbers later but they soon understand the difference between loosing and winning or between soon and late or between the basement and the upper floors of a building. It is in situations like these that negative numbers have a natural place. Real numbers are, however, more sophisticated! While, on one hand, it is natural and useful to associate positive integers to lengths, areas and volumes as the ancient greeks did, on the other hand it was understood long ago that this association leeds to serious difficulties since not every length can be expressed as a fraction. Clearly, a number system that is intended to be related to the geometric notion of length has to be sufficiently rich to contain all numbers that are not fractions.

The objective of this thesis is to construct and order the following systems of numbers: natural numbers, integer numbers, rational numbers and real numbers. In accordance with this objective, we define the natural numbers using a set of axioms, *Peano axioms*, that allow us to obtain the well known arithmetic properties, and we perform the algebraic construction of both integers and rationals, as equivalence classes of pairs of natural numbers and pairs of integer numbers, respectively. The construction of real numbers is done using methods of Analysis, via Cauchy sequences.

Índice

Capítulo 1

Introdução

Tudo é número
Pitagóricos

1.1 Introdução

Os números estão presentes em situações naturais do nosso dia-a-dia e o conceito de número é fundamental no nosso modo de vida. Os números têm sido usados pela humanidade desde sempre, para contar, para ordenar, para medir. O conceito de número foi, muito provavelmente, um dos primeiros conceitos matemáticos assimilados pela humanidade. Os primeiros números que surgiram foram os números naturais. Pitágoras, filósofo e matemático grego (570 a.C. - 495 a.C.) desenvolveu uma teoria tendo por base uma só ideia: a de que o mundo e tudo o que nos rodeia pode ser explicado pelos números naturais. Desse modo, todo o comprimento, área ou volume, diziam, era dado por números naturais ou pela razão entre dois números naturais - os chamados *números racionais*. No entanto, ao tentar encontrar o valor da diagonal de um quadrado de lado com medida igual a uma unidade, surgiram *medidas* que não podiam ser expressas como quociente entre dois números naturais. Pitágoras e os Pitagóricos descobriram, deste modo, estes novos números mas essa descoberta punha em causa todo o seu trabalho e a doutrina dos números que tinham criado pelo que a solução que encontraram foi ignorar tal descoberta!

A ideia de que todos os comprimentos podiam ser dados por números naturais ou pela razão entre dois números naturais estava, assim, errada, uma vez que existiam comprimentos

que não podiam ser dados dessa forma. Os valores desses comprimentos ficaram conhecidos como *números irracionais*. Era, então, necessário conceber um sistema de números suficientemente rico para conter os números naturais, os racionais e os números que não são fracções. Os números reais surgiram para responder a essa necessidade.

No Capítulo 2 procedemos à definição dos números naturais através de um conjunto de axiomas, os *axiomas de Peano*, que permitem definir duas operações binárias no conjunto $\mathbb{N}$ dos números naturais e obter as propriedades aritméticas conhecidas. Recorrendo a uma destas operações, definimos uma ordem total em $\mathbb{N}$ e analisamos como esta ordem se comporta em relação às operações binárias definidas. Mostramos ainda que, com esta ordem, o conjunto $\mathbb{N}$ é bem ordenado e provamos a equivalência do *Princípio da Boa Ordem de* $\mathbb{N}$ com o *Princípio de Indução Natural* e o *Princípio de Indução Completa*.

Tal como os conhecemos, os números naturais constituem um sistema de contagem perfeito. No entanto, com o progresso das sociedades, começou a ser evidente a necessidade de um sistema que permitisse fazer mais do que contar - por exemplo, com a implementação do comércio, surgiu o conceito de *dívida* e com ele a possibilidade de *tirar* mais do que aquilo que se tem. Ora nem sempre é possível usar os elementos de $\mathbb{N}$ para representar o estado de uma tal situação financeira. É, assim, preciso construir um conjunto de números que contenha, para além dos naturais, novos números que traduzam a situação de *dívida* referida. Mais precisamente, os números inteiros surgem para resolver um problema de existência de solução para certas equações: nem todas as equações $a+x=b$, de coeficientes naturais, têm solução em $\mathbb{N}$. Pretendendo ampliar o conjunto dos números naturais com *números* que resolvam a dificuldade apresentada, definimos, no Capítulo 3, os números inteiros como classes de equivalência de pares de números naturais. A algebrização do correspondente conjunto quociente dá-nos o anel comutativo, com identidiade, $\mathbb{Z}$, dos números inteiros. Neste capítulo, também definimos e estudamos uma ordem total que estende a ordem nos números naturais, obtendo, deste modo, o anel ordenado $(\mathbb{Z},+,\times,\leq)$.

O anel $(\mathbb{Z},+,\times)$ tem ainda sérias limitações. Tal como não se pode subtrair em $\mathbb{N}$, também não de se pode dividir em $\mathbb{Z}$: não há, em $\mathbb{Z}$, elementos suficientes para acomodar mecanismos de divisão. Mais formalmente, a equação $4x=3$, de coeficientes inteiros, por exemplo, não tem solução em $\mathbb{Z}$. Seguindo um procedimento semelhante ao tido na construção dos números inteiros, definimos, no capítulo 4, número racional e construimos um novo sistema de números,

que representamos por $\mathbb{Q}$ e designamos por conjunto dos números racionais, que estende $\mathbb{Z}$ de tal modo que a divisão seja possível em $\mathbb{Q}$. É claro que no novo sistema não vai ser possível dividir por 0 o que, do ponto de vista intuitivo, se compreende: dividir por menos *coisas* dá uma maior quantidade a cada um; se dividirmos por nada, o que obtemos será, necessariamente, algo infinitamente grande - um tal *elemento* não pertencerá a $\mathbb{Q}$! Ainda assim, este novo sistema de números constitui um melhoramento significativo relativamente a $\mathbb{Z}$: por um lado é um corpo (é nele possível dividir por qualquer número diferente de zero), o que não acontece com $\mathbb{Z}$, e, por outro lado, qualquer equação linear de coeficientes racionais tem solução em $\mathbb{Q}$.

Apesar das vantagens que $\mathbb{Q}$ apresenta em relação a $\mathbb{Z}$, $\mathbb{Q}$ não é, ainda, um sistema numérico adequado. Apontamos duas razões: (i) embora toda a sucessão de números racionais convergente seja uma sucessão de Cauchy, há sucessões de Cauchy de números racionais que não são convergentes em $\mathbb{Q}$; (ii) uma equação tão simples quanto a equação $x^2 = 2$ não é solúvel em $\mathbb{Q}$. Resolver estas falhas exige que se proceda a nova ampliação do sistema de números existente, de modo a incluir o limite de qualquer sucessão de Cauchy e *números* como, por exemplo, $\pm\sqrt{2}$. É deste modo que surgem os números reais. A construção dos números reais que apresentamos no Capítulo 5 é devida a Georg Cantor (1845-1918) e tem como objetivo a construção de um corpo ordenado que estenda $\mathbb{Q}$ e no qual toda a sucessão de Cauchy seja convergente. Definiremos número real como sendo uma classe de equivalência de certa sucessão de Cauchy, $(a_n)_n$, mais precisamente, o número real $[a_n]$ é o conjunto das sucessões de Cauchy de números racionais, $(b_n)_n$, tais que $a_n - b_n \to 0$.

1.2 Conceitos básicos

No decurso deste trabalho assumiremos como conhecidos conceitos e resultados de teoria de conjuntos e de Álgebra que se estudam nos primeiros anos de uma licenciatura em Matemática. Estes incluem os conceitos de relação de equivalência, relação de ordem, operação binária, grupo, anel, corpo, isomorfismo e resultados a eles associados. Relativamente ao conceito de relação de ordem, estabelecemos, desde já, a seguinte notação: num conjunto parcialmente ordenado $(X, \leq)$, dados $x, y \in X$ escreveremos, por vezes e por conveniência, $x \geq y$ para significar $y \leq x$.

Nesta secção destacamos resultados sobre anéis ordenados que serão especialmente úteis no Capítulo 5.

Definição 1.1. *Um grupo ordenado é um triplo $(G,+,\leq)$ formado por um conjunto G, uma operação binária $+$ definida em G e uma ordem total $\leq$ em G tais que:*

1. *$(G,+)$ é um grupo abeliano;*

2. *$\leq$ é compatível com a adição , isto é,*

$$x \leq y \Rightarrow x+z \leq y+z,$$

para quaisquer $x,y,z \in G$.

Como veremos no capítulo 3, o grupo aditivo dos números inteiros é um exemplo claro de um grupo ordenado.

Dados x e y elementos de um grupo ordenado $(G,+,\leq)$, escrevemos $x < y$ para significar que $x \leq y$ e $x \neq y$. Observamos que, para qualquer relação de ordem parcial $\leq$, se tem

$$x \leq y \Leftrightarrow x = y \vee x < y.$$

Proposição 1.1. (Proposição 4.1.3 [2]) *Num grupo ordenado G, as desigualdades $x < y$ e $x+z < y+z$ são equivalentes.*

Corolário 1.1. (Corolário da Proposição 4.1.3 [2]) *Num grupo ordenado G, as quatro relações seguintes são equivalentes:*

$$x < y; \quad x-y < 0; \quad 0 < y-x; \quad -y < -x.$$

Num grupo ordenado G, um elemento diz-se *positivo* (respetivamente *negativo*) se $x > 0$ (respetivamente, $x < 0$). O conjunto dos elementos positivos de G representa-se por G^+ e o conjunto dos elementos negativos de G representa-se por G^-.

Do Corolário 1.1 e do facto da relação $\leq$ ser tricotómica resulta que qualquer elemento x de G verifica uma e uma só das seguintes condições: x é positivo, x é negativo, $x = 0$. Ora isto equivale a afirmar que G^+, G^- e $\{0\}$ constituem uma partição de G.

Proposição 1.2. *Para qualquer grupo ordenado $(G,+,\leq)$, tem-se*

$$G = G^+ \dot{\cup} G^- \dot{\cup} \{0\}.$$

Reciprocamente, pode definir-se um grupo ordenado a partir de um grupo abeliano G e de um subconjunto de G que satisfaz as condições anteriores.

Proposição 1.3. (Proposição 4.2.2 [2]) *Seja P uma parte de um grupo abeliano G obedecendo às seguintes condições:*

$[P1]$ *P é fechada em G, isto é, $x \in P$ e $y \in P$ implica $x+y \in P$;*

$[P2]$ *a parte $-P$, formada pelos simétricos dos elementos de P, constitui com P uma partição de $G \setminus \{0\}$:*

$$P \cup (-P) = G \setminus \{0\} \ \wedge \ P \cap (-P) = \emptyset.$$

Então, a relação $x \leq y$ em G tal que

$$x < y \Leftrightarrow y - x \in P$$

é uma relação de ordem total em G compatível com a estrutura de grupo. No grupo ordenado assim obtido, P é o conjunto dos elementos positivos (e, portanto, $-P$ é o conjunto dos elementos negativos).

Definição 1.2. *Um anel ordenado é um quádruplo $(A,+,\times,\leq)$ formado por um conjunto A, duas operações binárias $+$ e $\times$ definidas em A e uma ordem total $\leq$ em A tais que:*

1. *$(A,+,\times)$ é um anel comutativo;*

2. *$\leq$ é compatível com a adição, isto é, para quaisquer $x,y,z \in A$,*

$$x \leq y \Rightarrow x+z \leq y+z;$$

3. *para quaisquer $x,y \in A$ tais que $x > 0$ e $y > 0$ tem-se $xy > 0$.*

Num anel ordenado $(A,+,\times,\leq)$, um elemento diz-se *positivo* (resp. *negativo*) se x é positivo (resp. *negativo*) no grupo ordenado $(A,+)$. O conjunto dos elementos positivos de $(A,+,\times,\leq)$ representa-se por A^+ e o conjunto dos elementos negativos de $(A,+,\times,\leq)$ representa-se por A^-.

O seguinte corolário é consequência imediata das definições de grupo ordenado e de anel ordenado.

Corolário 1.2. *Um quádruplo $(A,+,\times,\leq)$ é um anel ordenado se e só se $(A,+)$ é um grupo ordenado e se verifica, para qualquer $x,y \in A$,*

$$x > 0 \ \wedge \ y > 0 \Rightarrow xy > 0.$$

Um conjunto totalmente ordenado X diz-se *denso* se tiver mais do que um elemento e se, para quaisquer dois elementos $a,b \in X$ tais que $a < b$ existir um elemento $c \in X$ tal que $a < c < b$.

Um anel ordenado $(A,+,\times,\leq)$ diz-se *denso* se $(A,\leq)$ for um conjunto denso.

Proposição 1.4. *Todo o corpo ordenado é denso.*

Demonstração Seja K um corpo. Então K tem, pelo menos dois elementos, 0_K e 1_K, e $2.1_k \neq 0_k$, i.e., o elemento 2.1_k é invertível. Sejam, então, $a,b \in K$ tais que $a < b$. Procuramos $c \in K$ tal que $a < c < b$. Temos:

$$\begin{aligned} a < b &\Leftrightarrow a+a < a+b < b+b \\ &\Rightarrow a(1_K+1_K) < a+b < b(1_K+1_K) \\ &\Rightarrow (2\cdot 1_K)\,a < a+b < (2\cdot 1_K)\,b \\ &\Rightarrow a < (a+b)\,(2\cdot 1_K)^{-1} < b. \end{aligned}$$

Assim, $c = (a+b)\,(2\cdot 1_K)^{-1}$ satisfaz a condição pretendida.

■

Um anel ordenado $(A,+,\times,\leq)$ diz-se um *anel arquimediano* se verifica o chamado axioma de Arquimedes:

$$\forall a,b \in A^+ : a < b, \ \ \exists n \in \mathbb{Z} : \ b < na.$$

Capítulo 2

Definição axiomática e ordenação do conjunto dos números naturais

2.1 Definição axiomática dos números naturais

Os números estão presentes em situações naturais do nosso dia-a-dia e o conceito de número é fundamental no nosso modo de vida. Os números têm sido usados pela humanidade desde sempre, para contar, para ordenar, para medir. O conceito de número foi, muito provavelmente, um dos primeiros conceitos matemáticos assimilados pela humanidade. Os primeiros números que surgiram foram os números naturais. Neste capítulo procedemos à definição dos números naturais através de um conjunto de axiomas designados por *axiomas de Peano*, em homenagem ao matemático italiano G. Peano do séc XIX (1858-1932) que os desenvolveu.

Começamos por considerar um conjunto, que representamos por $\mathbb{N}$, e uma aplicação $s : \mathbb{N} \longrightarrow \mathbb{N}$ que satisfazem os seguintes axiomas:

A_1**:** $1 \in \mathbb{N}$;

A_2**:** $1 \notin s(\mathbb{N})$;

A_3**:** s é uma aplicação injetiva;

A_4**:** Se $\mathscr{P}$ é um subconjunto de $\mathbb{N}$ tal que $1 \in \mathscr{P}$ e $s(n) \in \mathscr{P} \ \ \forall n \in \mathscr{P}$, então $\mathscr{P} = \mathbb{N}$.

Os elementos de $\mathbb{N}$ designam-se por *números naturais*.

Observações:

1. Para cada $n \in \mathbb{N}$, $s(n)$ designa-se por sucessor de n.

2. O número 1 não é sucessor de qualquer número natural.

3. O axioma A_4 é conhecido por Princípio de Indução Natural.

A proposição seguinte mostra que o número 1 é o único número natural que não é sucessor de qualquer número natural.

Proposição 2.1.1 Todo o número natural diferente de 1 pertence ao contradomínio de s.

Demonstração. Seja $A = \{1\} \cup s(\mathbb{N})$. É claro que $1 \in A$ e que, para qualquer $n \in \mathbb{N}$, se tem $s(n) \in s(\mathbb{N}) \subseteq A$. Então, pelo Princípio de Indução Natural, obtemos $A = \mathbb{N}$ pelo que todos os números naturais diferentes de 1 pertencem a $s(\mathbb{N})$. ■

2.2 Operações em $\mathbb{N}$

Em $\mathbb{N}$ vamos definir duas **operações binárias**, a adição e a multiplicação e uma **operação unária**, a potenciação

2.2.1 Adição

Definição 2.1. *A operação de adição é uma aplicação de $\mathbb{N} \times \mathbb{N}$ em $\mathbb{N}$, que se representa por $+$ e se define de forma recursiva por:*

$$a_1 : \forall n \in \mathbb{N},\ n+1 = s(n);$$
$$a_2 : \forall n, m \in \mathbb{N},\ n + s(m) = s(n+m).$$

Observamos que o Princípio de Indução Natural garante que a_1 e a_2 definem uma operação binária em $\mathbb{N}$, i.e., que a cada par de números naturais a *operação de adição* faz corresponder um e um só número natural. De facto, seja $n \in \mathbb{N}$ e consideremos o conjunto

$$X = \{m \in \mathbb{N} : n+m \text{ está definido}\}.$$

Como $n+1 = s(n)$ está definido por a_1, temos que $1 \in X$. Além disso, supondo que $m \in X$, então$n+m$ está definido e, por a_2, também $n+s(m) = s(n+m)$ está definido para quaisquer naturais m e n.

Propriedades da adição

A operação que acabamos de definir verifica as seguintes propriedades:

2.2.1.1. Propriedade Associativa
$\forall n,m,p \in \mathbb{N},\ (n+m)+p = n+(m+p)$.

2.2.1.2. Propriedade Comutativa
$\forall n,m \in \mathbb{N},\ n+m = m+n$.

Demonstração. Seja $\mathscr{P} = \{n \in \mathbb{N} : \forall m \in \mathbb{N},\ m+n = n+m\}$. Então, $\mathscr{P} \subseteq \mathbb{N}$. Pretendemos mostrar que $\mathscr{P} = \mathbb{N}$. Comecemos por ver que $1 \in \mathscr{P}$. Seja $\mathscr{A} = \{m \in \mathbb{N} : m+1 = 1+m\}$. Como $1+1 = 1+1$, $1 \in \mathscr{A}$. Além disso, se $x \in \mathscr{A}$ então $s(x) \in \mathscr{A}$. De facto,

$$\begin{aligned} 1+s(x) &= s(1+x) && (a_2)\\ &= s(x+1) && (x \in \mathscr{A})\\ &= s(s(x)) && (a_1)\\ &= s(x)+1. && (a_1) \end{aligned}$$

Então $s(x) \in \mathscr{A}$ e, pelo axioma A_4, $\mathscr{A} = \mathbb{N}$. Logo $1 \in \mathscr{P}$.

Mostremos agora que, se $y \in \mathscr{P}$ então $s(y) \in \mathscr{P}$. Seja $a \in \mathbb{N}$. Temos, sucessivamente,

$$\begin{aligned} a+s(y) &= s(a+y) && (a_2)\\ &= (a+y)+1 && (a_1)\\ &= 1+(a+y) && (1 \in \mathscr{P})\\ &= 1+(y+a) && (y \in \mathscr{P})\\ &= (1+y)+a && \text{(a adição é associativa)}\\ &= (y+1)+a && (y \in \mathscr{P})\\ &= s(y)+a. && (a_1) \end{aligned}$$

Assim, $s(y) \in \mathscr{P}$ e, pelo axioma A_4, $\mathscr{P} = \mathbb{N}$. ■

2.2.1.3. Lei do corte

$\forall n,m,p \in \mathbb{N},\ n+p = m+p \Rightarrow n = m.$

Demonstração. Sejam $n,m,p \in \mathbb{N}$ tais que $n+p = m+p$. Se $p = 1$, então $n+1 = m+1$, isto é, $s(n) = s(m)$ e, como a aplicação s é injetiva (axioma A_3), segue-se que $n = m$. Se $p \neq 1$, então $p = s(q_1)$, para algum $q_1 \in \mathbb{N}$. De $n+p = m+p$ obtemos $n+s(q_1) = m+s(q_1)$ e, por a_2, $s(n+q_1) = s(m+q_1)$. A injetividade de s garante que $n+q_1 = m+q_1$. Tal como anteriormente, se $q_1 = 1$, obtemos $n = m$. Se $q_1 \neq 1$, então $q_1 = s(q_2)$, para algum $q_2 \in \mathbb{N}$. Aplicando este raciocínio um número finito de vezes (a cadeia $1 < 2 < \cdots q_2 < q_1 < p$ é finita), encontramos q_i tal que $q_i = s(1)$ e, de $n+q_i = m+q_i$ obtemos, sucessivamente, $n+s(1) = m+s(1)$ e $s(n+1) = s(m+1)$. A injetividade de s assegura que $n+1 = m+1$, i.e., que $s(n) = s(m)$ e, consequentemente, que $n = m$.

■

2.2.2 Multiplicação

Definição 2.2. *A operação de multiplicação é uma aplicação de $\mathbb{N} \times \mathbb{N}$ em $\mathbb{N}$, que se representa por $\times$ e se define de forma recursiva por:*

$$\begin{aligned} &m_1 : \forall n \in \mathbb{N},\ n \times 1 = n;\\ &m_2 : \forall n,m \in \mathbb{N},\ n \times s(m) = (n \times m)+n. \end{aligned}$$

Para simplificar a escrita, escreveremos nm para representar $n \times m$.

Um argumento semelhante ao apresentado para a adição mostra que o Princípio de Indução Natural garante que m_1 e m_2 definem, de facto, uma operação binária em $\mathbb{N}$.

A adição e a multiplicação ficam relacionadas pela chamada *propriedade distributiva*:

2.2.2.1. Propriedade Distributiva

Para quaisquer $m, n, p \in \mathbb{N}$,

$$(i)\ \ m\,(n+p) = mn + mp;$$
$$(ii)\ \ (m+n)\,p = mp + np.$$

Demonstração. Seja $\mathscr{P} = \{p \in \mathbb{N} : \forall m, n \in \mathbb{N},\ m\,(n+p) = mn + mp\}$. Então $\mathscr{P} \subseteq \mathbb{N}$. Vejamos que $1 \in \mathscr{P}$. Tem-se,

$$\begin{aligned} m\,(n+1) &= ms\,(n) && (a_1)\\ &= mn + m && (m_2)\\ &= mn + m1. && (m_1) \end{aligned}$$

Mostremos agora que, se $x \in \mathscr{P}$ então $s\,(x) \in \mathscr{P}$. Seja $x \in \mathscr{P}$. Tem-se,sucessivamente,

$$\begin{aligned} m\,(n + s\,(x)) &= m\,(s\,(n+x)) && (a_2)\\ &= m\,(n+x) + m && (m_2)\\ &= (mn + mx) + m && (x \in \mathscr{P})\\ &= mn + (mx + m) && \text{(a adição é associativa)}\\ &= mn + ms\,(x)\,. && (m_2) \end{aligned}$$

Logo $s\,(x) \in \mathscr{P}$ e, pelo axioma A_4, $\mathscr{P} = \mathbb{N}$.

■

Propriedades da Multiplicação

A operação multiplicação verifica as seguintes propriedades:

2.2.2.2. Propriedade Associativa

$\forall m,n,p \in \mathbb{N} \;\; m\,(n\,p) = (m\,n)\,p.$

Demonstração. Seja $\mathscr{P} = \{p \in \mathbb{N} : \forall m,n \in \mathbb{N},\ m\,(n\,p) = (m\,n)\,p\} \subseteq \mathbb{N}$. Temos que $1 \in \mathscr{P}$. De facto,

$$\begin{aligned} m\,(n1) &= m\,n && (m_1)\\ &= (m\,n)\,1. && (m_1) \end{aligned}$$

Vejamos agora que, se $x \in \mathscr{P}$ então $s(x) \in \mathscr{P}$. Seja $x \in \mathscr{P}$. Temos,sucessivamente,

$$\begin{aligned} m\,(n\,s(x)) &= m\,(n\,x+n) && (m_2)\\ &= m(\,n\,x) + m\,n && \text{(propriedade distributiva)}\\ &= (m\,n)\,x + m\,n && (x \in \mathscr{P})\\ &= (m\,n)\,s(x). && (m_2) \end{aligned}$$

Assim $s(x) \in \mathscr{P}$ e, pelo axioma A_4, $\mathscr{P} = \mathbb{N}$. ■

2.2.2.3. Propriedade Comutativa

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

2.2.2.4. Elemento neutro

$\forall m \in \mathbb{N},\;\; 1 \times m = m.$

2.2.3 Potenciação

Definição 2.3. *Sejam $n,k \in \mathbb{N}$. Chama-se potência k de n e representa-se por n^K ao número natural definido de forma recursiva por:*

$$\begin{aligned} p_1 &: \;\; n^1 = n;\\ p_2 &: \;\; \forall k \in \mathbb{N},\;\; n^{s(k)} = n^k\,n. \end{aligned}$$

Propriedades da potenciação

A operação que acabamos de definir verifica as seguintes propriedades:

2.2.3.1. $\forall m,n,p \in \mathbb{N},\ \ m^{n+p} = m^n m^p$.

2.2.3.2. $\forall m,n,p \in \mathbb{N},\ \ (m^n)^p = m^{np}$.

2.2.3.3. $\forall m,n,p \in \mathbb{N},\ \ (mn)^p = m^p n^p$.

Demonstração. Seja $\mathscr{P}$ o subconjunto de $\mathbb{N}$ definido por $\mathscr{P} = \{p \in \mathbb{N} :\ \forall m,n \in \mathbb{N},\ \ (mn)^p = m^p n^p\}$. $1 \in \mathscr{P}$ pois, $(mn)^1 = m^1 n^1$. De facto,

$$\begin{aligned} (mn)^1 &= mn && (p_1)\\ &= m^1 n^1. && (p_1) \end{aligned}$$

Vejamos agora que, se $x \in \mathscr{P}$ então $s(x) \in \mathscr{P}$. Seja $x \in \mathscr{P}$. Tem-se, sucessivamente,

$$\begin{aligned} (mn)^{s(x)} &= (mn)^x (mn) && (p_2)\\ &= m^x n^x (mn) && (x \in \mathscr{P})\\ &= m^x (mn) n^x && \text{(a multiplicação é comutativa)}\\ &= (m^x m)(nn^x) && \text{(a multiplicação é associativa)}\\ &= m^{s(x)} (n^x n) && (p_2 \text{ e propriedade 2.2.2.3})\\ &= m^{s(x)} n^{s(x)}. && (p_2) \end{aligned}$$

Assim, $s(x) \in \mathscr{P}$ e, pelo axioma A_4, $\mathscr{P} = \mathbb{N}$.

■

2.3 Uma relação de ordem em $\mathbb{N}$

Nesta secção estabelecemos uma relação de ordem no conjunto dos números naturais.

Definição 2.4. *Dados $m,n \in \mathbb{N}$, diz-se que m é menor ou igual a n e escreve-se $m \leq n$, se e só se $m = n$ ou $\exists k \in \mathbb{N} : n = m + k$.*

Notação: Para $m,n \in \mathbb{N}$, escrevemos $m < n$ para significar $m \leq n$ e $m \neq n$.

Proposição 2.1. *Para todo* $m,n \in \mathbb{N},\ \ m \neq m+n$.

Demonstração. Seja $\mathscr{A}$ o subconjunto de $\mathbb{N}$ definido por $\mathscr{A} = \{m \in \mathbb{N} :\ \forall n \in \mathbb{N},\ m \neq m+n\}$. Como 1 não é sucessor de qualquer número natural, $1 \neq n+1$, para qualquer natural n. Logo $1 \in \mathscr{A}$.

Seja $k \in \mathscr{A}$. Mostremos que $s(k) \in \mathscr{A}$. Temos, sucessivamente,

$$\begin{aligned}
k \in \mathscr{A} &\Rightarrow k \neq k+n \\
&\Rightarrow s(k) \neq s(k+n) && (s \text{ é injetiva}) \\
&\Rightarrow s(k) \neq n+s(k) && ((a_2)\text{e a adição é comutativa}) \\
&\Rightarrow s(k) \neq s(k)+n && (\text{a adição é comutativa}) \\
&\Rightarrow s(k) \in \mathscr{A}.
\end{aligned}$$

Pelo Princípio de Indução Natural podemos concluir que $\mathscr{A} = \mathbb{N}$. ■

Proposição 2.2. *A relação binária* $\leq$ *é uma relação de ordem parcial.*

Demonstração.

(i) $\leq$ é reflexiva. Para qualquer $n \in \mathbb{N}$ é claro que $n = n$ e, portanto, pela definição de $\leq$, $n \leq n$.

(ii) $\leq$ é anti-simétrica, i.e., para quaisquer $m,n \in \mathbb{N}$, se $m \leq n$ e $n \leq m$ então $m = n$.

Sejam $m,n \in \mathbb{N}$. Se $m = n$ e $n = m$ claramente $m = n$.

Se $m = n$ e $m = n+k$ para algum $k \in \mathbb{N}$, então $n = n+k$, o que o que contraria a Proposição 2.1.

Se $n = m+t$, $t \in \mathbb{N}$, e $n = m$ então $n = n+t$, o que contraria a Proposição 2.1.

Se $n = m+p$, $p \in \mathbb{N}$, e $m = n+q$, $q \in \mathbb{N}$, então $n = (n+q)+p$, ou seja, $n = n+(p+q)$, o que, de novo, contraria a Proposição 2.1.

Concluimos, assim, que, dados $m,n \in \mathbb{N},\ m \leq n$ e $n \leq m \Rightarrow m = n$.

(iii) $\leq$ é transitiva: para quaisquer $m,n,t \in \mathbb{N}$, se $m \leq n$ e $n \leq t$ então $m \leq t$.

Sejam $m,n,t \in \mathbb{N}$. Se $m = n$ e $n = t$, i.e., $m = t$ então $m \leq t$.

Se $m = n$ e $t = n+k$, $k \in \mathbb{N}$, então $t = m+k$ pelo que $m \leq t$.

Se $n = m+z$, $z \in \mathbb{N}$, e $t = n$ temos $t = m+z$ e, portanto, $m \leq t$.

Se $n = m+p$, $p \in \mathbb{N}$, e $t = n+q, q \in \mathbb{N}$, temos $t = (m+p)+q = m+(p+q)$, pelo que $m \leq t$.

■

A proposição anterior permite-nos dizer que $(\mathbb{N}, \leq)$ é um conjunto parcialmente ordenado. Escrevemos $(\mathbb{N}, \leq)$ é um c.p.o..

Teorema 2.1. *Dados $m,n \in \mathbb{N}$, ocorre um e um só dos seguintes casos $m < n$; $m = n$; $n < m$.*

Demonstração.

Seja $\mathscr{A} = \{m \in \mathbb{N} : \forall n \in \mathbb{N},\ m = n \text{ ou } m < n \text{ ou } n < m\}$. Então $\mathscr{A} \subseteq \mathbb{N}$. Mostremos que $\mathscr{A} = \mathbb{N}$. Seja $n \in \mathbb{N}$. Então, ou $n = 1$ ou $n \neq 1$. Se $n \neq 1$, então $n = s(t)$, para algum $t \in \mathbb{N}$, e, portanto, $1 < n$. Em qualquer dos casos $1 \in \mathscr{A}$.

Seja $k \in \mathscr{A}$. Mostremos que $s(k) \in \mathscr{A}$. Seja $n \in \mathbb{N}$. Como $k \in \mathscr{A}$, temos que ou $k = n$ ou $n < k$ ou $k < n$.

Se $k = n$ temos $s(k) = s(n) = n+1$ e, portanto, $n < s(k)$.

Se $k = n+p$ temos $s(k) = s(n+p) = (n+p)+1 = n+(p+1)$ e, logo $n < s(k)$.

Se $n = k+q$ então ou $q = 1$ ou $q \neq 1$.

- Se $q = 1$, $n = k+1 = s(k)$ e, portanto, $s(k) < n$.

- Se $q \neq 1$, q é sucessor de algum natural t, ou seja, $q = t+1$, para algum $t \in \mathbb{N}$. Assim, $n = k+(t+1) = (k+1)+t = s(k)+t$, isto é, $s(k) < n$.

Podemos então concluir que $s(k) \in \mathscr{A}$. Pelo Princípio de Indução Natural, $\mathscr{A} = \mathbb{N}$.

■

Por satisfazer a propriedade expressa no teorema anterior, a relação binária $\leq$ em $\mathbb{N}$ diz-se uma relação *tricotómica*. Uma relação de ordem parcial que é tricotómica designa-se por **relação de ordem total**.

O próximo resultado mostra, em particular, que a relação $\leq$ é compatível com as operações binárias definidas em $\mathbb{N}$. Recordemos, antes de mais, que, um elemento a de um c.p.o $(\mathscr{A}, \leq)$ se diz **elemento mínimo de** $\mathscr{A}$ se, para qualquer $b \in \mathscr{A}$, $a \leq b$. Claramente, 1 é o elemento mínimo de $\mathbb{N}$.

Teorema 2.2. *Para todo $m, n, p, q \in \mathbb{N}$ tem-se:*

(i) $m \leq n$ e $p \leq q \Rightarrow m + p \leq n + q$;

(ii) $m \leq n$ e $p \leq q \Rightarrow mp \leq nq$;

(iii) $mp = np \Rightarrow m = n$;

(iv) $mp = 1 \Rightarrow m = p = 1$.

Demonstração.

(i) Sejam $m, n, p, q \in \mathbb{N}$ tais que $m \leq n$ e $p \leq q$. Então $n = m + k$ e $q = p + t$, para certos $k, t \in \mathbb{N}$. Tendo em conta as propriedades associativa e comutativa da adição, temos:

$$n + q = (m + k) + (p + t) = (m + p) + (k + t) = (m + p) + r,$$

onde $r = k + t \in \mathbb{N}$. Logo, $m + p \leq n + q$.

(ii) Sejam $m, n, p, q \in \mathbb{N}$ tais que $m \leq n$ e $p \leq q$. Então $n = m + k$ e $q = p + t$, para certos $k, t \in \mathbb{N}$. Assim temos, sucessivamente,

$$nq = (m + k)(p + t) = mp + (kp + kt + mt) = mp + r,$$

onde $r = kp + kt + mt \in \mathbb{N}$. Logo $mp \leq nq$.

(iii) Suponhamos que $mp = np$. Se $m < n$, então $n = m + k$, para algum $k \in \mathbb{N}$. De $mp = np$ teríamos, então, $mp = np = mp + kp$, o que contraria a Proposição 2.1. Analogamente, $n < m$ leva-nos a uma contradição semelhante. Assim, e dada a tricotomia de $\leq$, temos que ter $m = n$.

(iv) Sejam $m, p \in \mathbb{N}$ tais que $mp = 1$. Se $1 < m$ e $1 < p$, então $m = 1+k$ e $p = 1+t$, para certos $k, t \in \mathbb{N}$. Assim,

$$1 = mp = (1+k)(1+t) = 1+t+k+kt,$$

i.e., $1 = 1+(t+k+kt)$, o que contraria a Proposição 2.1. Como $1 = \min \mathbb{N}$, concluimos que ou $1 = m$ ou $1 = p$. Como $mp = 1$, se $1 = m$ então $p = 1$ e se $1 = p$ então $m = 1$.

■

Para o que se segue precisamos de recordar o seguinte:

Definição 2.5. *Um c.p.o* $\mathscr{A}$ *diz-se bem ordenado se qualquer subconjunto, não vazio, de* $\mathscr{A}$ *tiver elemento mínimo.*

Teorema 2.3. *Todo o subconjunto não vazio de* $\mathbb{N}$ *tem elemento mínimo.*

Demonstração. Seja $\mathscr{A} \subseteq \mathbb{N}$ tal que $\mathscr{A} \neq \emptyset$. Suponhamos que $\mathscr{A}$ não tem elemento mínimo. Seja $\mathscr{B} = \mathbb{N} \setminus \mathscr{A}$ e seja $\mathscr{P}$ o subconjunto de $\mathbb{N}$ assim definido:

$$\mathscr{P} = \{n \in \mathbb{N} : \forall m \in \mathbb{N},\ m \leq n \Rightarrow m \in \mathscr{B}\}.$$

Temos que $1 \in \mathscr{B}$ pois se $1 \in \mathscr{A}$ ele seria o seu elemento mínimo, o que contraria a nossa suposição de que $\mathscr{A}$ não tem elemento mínimo. Logo $1 \in \mathscr{P}$.

Seja $k \in \mathscr{P}$. Então, para qualquer $m \in \mathbb{N}, m \leq k \Rightarrow m \in \mathscr{B}$. Portanto, $k+1 \notin \mathscr{A}$ pois, caso contrário, $k+1$ seria o elemento mínimo de $\mathscr{A}$, o que contraria a hipótese. Deste modo, $k+1 \in \mathscr{B}$, logo $k+1 \in \mathscr{P}$, i.e., $s(k) \in \mathscr{P}$.
Assim, o Princípio de Indução Natural permite concluir que $\mathscr{P} = \mathbb{N}$. Portanto

$$\forall n \in \mathbb{N}, a \leq n \Rightarrow a \notin \mathscr{A}.$$

Logo $\mathscr{A} = \emptyset$ o que contrataria a hipótese de se ter $\mathscr{A} \neq \emptyset$. A contradição veio de termos suposto que $\mathscr{A}$ não tem elemento mínimo. Assim sendo, $\mathscr{A}$ tem elemento mínimo.

■

Como consequência imediata do Teorema 2.3, temos:

Corolário 2.1. *(Princípio da Boa Ordenação de $\mathbb{N}$)*
$(\mathbb{N}, \leq)$ *é um conjunto bem ordenado.*

Teorema 2.4. *(Princípio de Indução Completa)*
Seja $\mathscr{A} \subseteq \mathbb{N}$ tal que

$$(\forall n \in \mathbb{N}),\ [m < n \Rightarrow m \in \mathscr{A}] \Rightarrow n \in \mathscr{A}.$$

Então $\mathscr{A} = \mathbb{N}$.

Demonstração. Seja $\mathscr{B} = \mathbb{N} \setminus \mathscr{A}$. Suponhamos que $\mathscr{B} \neq \emptyset$. Pelo Princípio da Boa Ordenação de $\mathbb{N}$, $\mathscr{B}$ tem elemento minimo. Seja x esse elemento. Mostremos que todo o elemento menor do que x está em $\mathscr{A}$. De facto, se $m \in \mathbb{N}$ é tal que $m < x$, como $x = \min \mathscr{B}$, segue-se que $m \notin \mathscr{B}$, i.e., $m \in \mathscr{A}$. Então, por hipótese, obtemos $x \in \mathscr{A}$. Dada a definição de $\mathscr{B}$, isto contraria o facto de x ser mínimo $\mathscr{B}$. Esta contradição resultou de termos suposto que $\mathscr{B} \neq \emptyset$. Logo $\mathscr{B} = \emptyset$ e, portanto, $\mathscr{A} = \mathbb{N}$. ■

Na demonstração do Teorema 2.4, usámos o Princípio da Boa Ordenação de $\mathbb{N}$. Terminamos este capítulo provando que os três princípios, *Princípio de Indução Natural*, *Princípio da Boa Ordenação de* $\mathbb{N}$ e *Princípio de Indução Completa*, são equivalentes.

Teorema 2.5. *O Princípio de Indução Natural, o Princípio da Boa Ordenação de $\mathbb{N}$ e o Princípio de Indução Completa, são equivalentes entre si.*

Demonstração. Princípio de Indução Natural $\Rightarrow$ Princípio da Boa Ordenação de $\mathbb{N}$

Demonstrado anteriormente, no Teorema 2.3.

Princípio da Boa Ordenação de $\mathbb{N} \Rightarrow$ Princípio de Indução Completa

Demonstrado anteriormente, no Teorema 2.4.

Princípio de Indução Completa $\Rightarrow$ Princípio de Indução Natural

Suponhamos válido o Princípio de Indução Completa. Comecemos por provar que todo o

número diferente de 1 é sucessor de algum número natural. Seja $\mathscr{A} = \{1\} \cup s(\mathbb{N})$. Mostremos que $\mathscr{A}$ satifaz

$$(\forall n \in \mathbb{N}),\ [m < n \Rightarrow m \in \mathscr{A}] \Rightarrow n \in \mathscr{A}.$$

Seja $n \in \mathbb{N}$ e $n \neq 1$. Suponhamos que, para qualquer $m \in \mathbb{N}$, $m < n \Rightarrow m \in \mathscr{A}$, i.e., que se $m < n$ então , $m = 1$ ou $m \in s(\mathbb{N})$. Se não existisse qualque número natural m menor do que n então teríamos $n = 1$, o que não acontece. Seja, portanto, $m \in \mathbb{N}$ tal que $m < n$. Então $n = m + k$, para algum $k \in \mathbb{N}$. Se $k = 1$, então $n = m + 1$, i.e., $n = s(m)$. Se $k \neq 1$, como, por hipótese, $m \in \mathscr{A}$, ou $m = 1$ e, portanto, de $n = m + k$ obtemos $n = 1 + k$, i.e., $n = s(k,)$ pelo que $n \in \mathscr{A}$, ou $m = s(t)$, para algum $t \in \mathbb{N}$, e temos $n = m + k = s(t) + k = s(t + k) \in \mathscr{A}$. Assim,

$$(\forall n \in \mathbb{N},\ n \neq 1)\ (\exists k \in \mathbb{N}) :\ n = s(k).$$

Seja agora $X \subseteq \mathbb{N}$ tal que $1 \in X$ e $s(n) \in X$, para qualquer $n \in \mathbb{N}$. Vejamos que se tem também $\mathbb{N} \subseteq X$ e, portanto, $X = \mathbb{N}$. De facto, dado $n \in \mathbb{N}$, ou $n = 1$ e, portanto, $n \in X$, ou $n \neq 1$ e, como acabámos de provar, $n = s(k)$ para algum $k \in \mathbb{N}$, pelo que, por hipótese, $n \in X$. ■

Capítulo 3

Construção e ordenação do conjunto dos números inteiros

Por que é que se criaram os números inteiros? Uma equação como, por exemplo, $x+7=3$ deveria ter solução "$3-7$" em $\mathbb{N}$ mas tal número natural não existe porque nem sempre se pode *subtrair* em $\mathbb{N}$. Pretendemos, assim, construir um sistema de números ampliado que contenha uma *resposta* para "$3-7$" e, mais geralmente, para todos os *problemas de subtracção* com quaisquer dois números naturais.

No princípio, os matemáticos limitaram-se a representar os números novos por $-1,-2,\cdots$ e a regulamentar o seu modo de funcionamento, e.g. $3-7=-4$; $-3-7=-10$; $\cdots$. Neste capítulo, o nosso objetivo é mostrar como definir estes números, usando *objectos* que já conhecemos: os números naturais.

3.1 Definição dos números inteiros

À partida, a ideia de considerar um inteiro como um par ordenado de números naturais parece apropriada. No entanto, após alguma reflexão, apercebemo-nos de que isso produziria *demasiados* inteiros e não acautelaria o que pretendemos: que pares como $(5,6),(7,8),(32,33),\cdots$ sejam inteiros que representam as *respostas* $5-6,7-8,32-33,\cdots$, ou seja, pretendemos que todos esses pares ordenados diferentes representem o mesmo inteiro e sejam, por isso, com ele identificados.

Mais geralmente, se $a-b=c-d$ pretendemos que $(a,b),(c,d)$ representem o mesmo inteiro,

i.e. pretendemos que (a,b) e (c,d) representem o mesmo inteiro se $a+d=b+c$. Ora isto consegue-se definindo uma relação de equivalência que *coloca* esses pares na mesma classe de equivalência. Temos, assim, a seguinte relação de equivalência para a definição formal dos números inteiros:

Definição 3.1. *Seja R uma relação binária definida em* $\mathbb{N}\times\mathbb{N}$ *da seguinte forma:*

$$\forall a,b,c,d\in\mathbb{N},\ (a,b)\,R\,(c,d)\Leftrightarrow a+d=b+c.$$

Proposição 3.1. *A relação R é uma relação de equivalência em* $\mathbb{N}\times\mathbb{N}$.

Demonstração. Sejam (a,b), (c,d), $(e,f)\in\mathbb{N}^2$. Como $a,\ b\in\mathbb{N}$ e a adição é comutativa em $\mathbb{N}$, $a+b=b+a$. Logo R é reflexiva. Dada a definição de R e a comutatividade da adição, temos:

$(a,b)\,R\,(c,d)\Rightarrow a+d=b+c\Rightarrow d+a=c+b\Rightarrow c+b=d+a\Rightarrow(c,d)\,R\,(a,b)$. Logo R é simétrica. Para concluir a demonstração provemos que R é transitiva. Tem-se, sucessivamente,

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

$$(c,d)\,R\,(e,f)\Leftrightarrow c+f=d+e$$

Logo,

$$(a+d)+f+b+(c+f)=(b+c)+f+b+(d+e)$$

isto é,

$$(a+f)+(b+d)+(c+f)=(b+e)+(c+f)+(b+d).$$

As propriedades comutativa e lei do corte da adição em $\mathbb{N}$ permitem concluir que $(a+f)=(b+e)$ e, portanto, $(a,b)\,R\,(e,f)$.

■

Dado $(a,b)\in\mathbb{N}^2$ representamos a classe de equivalência de (a,b), determinada por R, por $[a,b]$. Assim,

$$[a,b]=\left\{(c,d)\in\mathbb{N}^2:(a,b)\,R\,(c,d)\right\}.$$

O conjunto quociente determinado pela relação R, $\mathbb{N}^2/R$, é formado por todas as classes de equivalência determinadas por R.

Representamos o conjunto $\mathbb{N}^2/R$ por $\mathbb{Z}$. Assim, por definição

$$\mathbb{Z} = \left\{ [a,b] : (a,b) \in \mathbb{N}^2 \right\}.$$

Aos elementos de $\mathbb{Z}$ chamamos *números inteiros*.

3.2 Operações binárias em $\mathbb{Z}$

Nesta secção vamos ver como efetuar operações com os números inteiros.

Definição 3.2. *Sejam* $[a,b], [c,d] \in \mathbb{Z}$. *Define-se* $[a,b]+[c,d] = [a+c, b+d]$.

Mostremos que a adição, definida desta forma, não depende da escolha dos representantes das classes de equivalência envolvidas.

Proposição 3.2. *Para quaisquer* $a,b,c,d,e,f,g,h \in \mathbb{N}$ *tais que* $[a,b] = [c,d]$ e $[e,f] = [g,h]$, *então*

$$[a,b]+[e,f] = [c,d]+[g,h].$$

Demonstração. Como $[a,b] = [c,d]$, $(a,b)\,R\,(c,d)$ e, portanto, $a+d = b+c$. Analogamente, $e+h = f+g$.

Logo, dada a comutatividade e associatividade em $\mathbb{N}$, $(a+e)+(d+h) = (c+g)+(b+f)$ donde,

$$[a+e, b+f] = [c+g, d+h].$$

■

Proposição 3.3. *A adição definida em* $\mathbb{Z}$ *goza das seguintes propriedades:*

1. $\forall a,b,c,d \in \mathbb{N},\ [a,b]+[c,d] = [c,d]+[a,b]$;
2. $\forall a,b,c,d,e,f \in \mathbb{N},\ ([a,b]+[c,d])+[e,f] = [a,b]+([c,d]+[e,f])$;
3. $\forall a,b \in \mathbb{N},\ [a,b]+[1,1] = [a,b]$;
4. $\forall a,b \in \mathbb{N},\ [a,b]+[b,a] = [1,1]$.

Demonstração. Para demonstrar 1) e 2) basta aplicar a definição de adição e utilizar as propriedades análogas já demonstradas em $\mathbb{N}$.

3) O inteiro $[1,1]$ é o elemento neutro da adição. De facto, para quaisquer $a,\ b \in \mathbb{N}$, $[a,b]+[1,1]=[a+1,b+1]$ e, como $(a+1)+b=(b+1)+a$, temos que $(a+1,b+1)\,R\,(a,b)$, pelo que $[a+1,b+1]=[a,b]$.

4) Mostremos que, para quaisquer $a,\ b \in \mathbb{N}$, $[a,b]+[b,a]=[1,1]$. Temos:
$[a,b]+[b,a]=[a+b,b+a]=[a+b,a+b]=[1,1]$, uma vez que, $(1,1)\,R\,(a+b,a+b)$.

■

Observemos que, como $(a,b)\,R\,(1,1) \Leftrightarrow a+1=b+1 \Leftrightarrow a=b$, se tem $[1,1]=\{(a,a) : a \in \mathbb{N}\}$.

O elemento neutro de $(\mathbb{Z},+)$, i.e., $[1,1]$, é representado por 0.

Dado o inteiro $[a,b]$, a classe $[b,a]$ representa-se por $-[a,b]$ e designa-se por "o elemento simétrico de $[a,b]$".

Definição 3.3. *Sejam a, b, c, d* $\in \mathbb{N}$. *Define-se* $[a,b]\cdot[c,d]=[ac+bd,ad+bc]$.

Vejamos que a operação assim definida não depende da escolha dos representantes das classes de equivalência envolvidas.

Proposição 3.4. *Dados* $a,b,c,d,e,f,g,h \in \mathbb{N}$ *tais que* $[a,b]=[c,d]$ e $[e,f]=[g,h]$. *Então*

$$[a,b]\cdot[e,f]=[c,d]\cdot[g,h]\,.$$

Demonstração. Sejam $a,b,c,d,e,f,g,h \in \mathbb{N}$ e $[a,b]=[c,d]$ e $[e,f]=[g,h]$. Temos:

$$[a,b]\cdot[e,f]=[ae+bf,af+be] \quad \text{e} \quad [c,d]\cdot[g,h]=[cg+dh,ch+dg]\,.$$

Como $(a,b)\,R\,(c,d) \Leftrightarrow a+d=b+c$ e $(e,f)\,R\,(g,h) \Leftrightarrow e+h=f+g$, obtemos, sucessivamente,

$$e(a+d)=e(b+c);\ \ c(e+h)=c(f+g);\ \ f(b+c)=f(a+d);\ \ d(f+g)=d(e+h)\,.$$

Pela propriedade distributiva da multiplicação em relação à adição de números naturais, obtemos,

$$ea+ed=eb+ec;\ \ ce+ch=cf+cg;\ \ fb+fc=fa+fd;\ \ df+dg=de+dh.$$

Assim,

$$
\begin{aligned}
&ea+ed+ce+ch+fb+fc+df+dg = eb+ec+cf+cg+fa+fd+de+dh\\
&ea+fb+ch+dg = eb+cg+fa+dh\\
&(ae+bf)+(ch+dg) = (be+af)+(cg+dh)\\
&[ae+bf, af+be] = [cg+dh, ch+dg]\\
&[a,b]\cdot[e,f] = [c,d]\cdot[g,h]\,.
\end{aligned}
$$

■

Proposição 3.5. *A multiplicação definida em* $\mathbb{Z}$ *goza das seguintes propriedades:*

1. $\forall a,b,c,d \in \mathbb{N},\ [a,b]\cdot[c,d] = [c,d]\cdot[a,b]$;

2. $\forall a,b,c,d,e,f \in \mathbb{N},\ ([a,b]\cdot[c,d])\cdot[e,f] = [a,b]\cdot([c,d]\cdot[e,f])$;

3. $\forall a,b \in \mathbb{N},\ [2,1]\cdot[a,b] = [a,b]$;

4. $\forall a,b,c,d,e,f \in \mathbb{N},\ [a,b]\cdot([c,d]+[e,f]) = [a,b]\cdot[c,d]+[a,b]\cdot[e,f]\,.$

Demonstração. Para demonstrar 1), 2) e 4) basta aplicar a definição de multiplicação e utilizar as propriedades análogas já demonstradas em $\mathbb{N}$.

3) Para quaisquer naturais a,b, $[2,1]\cdot[a,b] = [a,b]$, pois, $[2,1]\cdot[a,b] = [2a+1b, 2b+1a]$ e, como $a+(2b+1a) = b+(2a+1b)$, $(a,b) \in [2a+1b, 2b+1a]$.

■

Tendo em conta as propriedades da adição e da multiplicação em $\mathbb{Z}$, expressas nas proposições 3.3 e 3.5, temos o seguinte resultado:

Proposição 3.6. *O triplo* $(\mathbb{Z}, +, \times)$ *é um anel comutativo com identidade.*

3.3 Relação entre $\mathbb{N}$ e $\mathbb{Z}$

Sendo os números inteiros classes de equivalência de pares de números naturais, é claro que $\mathbb{N} \not\subseteq \mathbb{Z}$. No entanto, como mostramos nesta secção, o grupo $(\mathbb{Z},+)$ contém um subsemigrupo $H = \{[n+1,1] : n \in \mathbb{N}\}$, isomorfo a $(\mathbb{N},+)$, sendo o monóide comutativo $(\mathbb{Z},\times)$ também isomorfo ao monóide $(H,\times)$. Identificando $\mathbb{N}$ com H, podemos considerar que $\mathbb{N}$ é um subconjunto de $\mathbb{Z}$.

Com esta identificação em mente, estabelecemos e provamos o seguinte teorema:

Teorema 3.1. *A aplicação $\theta : \mathbb{N} \to \mathbb{Z}$, definida por $\theta(n) = [n+1,1]$, para qualquer $n \in \mathbb{N}$, é injetiva e satisfaz*

$$\forall m,n \in \mathbb{N},\ \ \theta(m+n) = \theta(m) + \theta(n) \ \text{ e } \ \theta(mn) = \theta(m) \cdot \theta(n).$$

Demonstração. Verifiquemos que θ é injetiva. Sejam $m,n \in \mathbb{N}$ tais que $\theta(n) = \theta(m)$. Então $[n+1,1] = [m+1,1]$ e, portanto, $(n+1,1)\,R\,(m+1,1)$, pelo que $n = m$. Vejamos agora que, para quaisquer $m,n \in \mathbb{N}$ se tem,

$$\theta(m) + \theta(n) = [m+n+1,1] \quad \wedge \quad \theta(m) \cdot \theta(n) = [mn+1,1].$$

Como $\theta(m) = [m+1,1]$ e $\theta(n) = [n+1,1]$ tem-se,

$$\begin{aligned}
\theta(m) + \theta(n) &= [m+1,1] + [n+1,1] \\
&= [m+1+n+1, 1+1] \\
&= [m+n+1+1, 1+1] \\
&= [m+n+1,1] + [1,1] \\
&= [m+n+1,1] \\
&= \theta(m+n).
\end{aligned}$$

$$\begin{aligned}
\theta(m)\cdot\theta(n) &= [m+1,1]\cdot[n+1,1] \\
&= [(m+1)(n+1)+1,(m+1)1+1\cdot(n+1)] \\
&= [mn+m+n+1+1,m+n+1+1] \\
&= [(mn+1)+(m+n+1),1+(m+n+1)] \\
&= [mn+1,1]+[m+n+1,m+n+1] \\
&= [mn+1,1],\ \text{pois } [m+n+1,m+n+1]=[1,1] \\
&= \theta(mn).
\end{aligned}$$

■

Corolário 3.1. $(\mathbb{N},+)\simeq\theta((\mathbb{N},+))$ *e* $(\mathbb{N},\times)\simeq\theta((\mathbb{N},\times))$.

O Corolário 3.1 permite-nos identificar cada $n\in\mathbb{N}$ com o inteiro $[n+1,1]$. Para cada $n\in\mathbb{N}$, o inteiro $[1,n+1]$, por ser o elemento simétrico de $[n+1,1]$, representa-se por $-n$.

Teorema 3.2. *Qualquer inteiro é, exatamente, de uma das formas* 0, n *ou* $-n$, *para algum* $n\in\mathbb{N}$.

Demonstração. Seja $[m,n]\in\mathbb{Z}$.

Se $m<n$ então $\exists\, k\in\mathbb{N}: m+k=n$. Temos:

$$m+k=n\Leftrightarrow(m+k)+1=n+1\Leftrightarrow m+(k+1)=n+1\Leftrightarrow(m,n)\,R\,(1,k+1).$$

Portanto, $[m,n]=[1,k+1]\equiv -k$.

Se $m=n$ então $m+1=n+1$, i.e., $(m,n)\,R\,(1,1)$. Portanto, $[m,n]=[1,1]\equiv 0$.

Se $m>n$ então $\exists\, k\in\mathbb{N}: n+k=m$. Temos:

$$n+k=m\Leftrightarrow m=n+k\Leftrightarrow m+1=(n+k)+1\Leftrightarrow m+1=n+(k+1)\Leftrightarrow(m,n)\,R\,(k+1,1).$$

Portanto, $[m,n]=[k+1,1]\equiv k$.

■

Observação: Dados $x,y\in\mathbb{Z}$, não havendo ambiguidade, escreveremos xy para significar $x.y$.

3.4 Uma ordem parcial em $\mathbb{Z}$

Em $\mathbb{N}$ definimos uma relação binária que provámos ser uma ordem total. Sendo os inteiros classes de equivalência de pares de números naturais, faz sentido interrogarmo-nos em que medida se pode definir em $\mathbb{Z}$ uma ordem parcial que estenda a ordem dos números naturais. Em caso afirmativo, será essa ordem tricotómica?

Definição 3.4. *Dados os números inteiros* $[a,b]$ e $[c,d]$*, dizemos que* $[a,b]$ *é menor ou igual que* $[c,d]$*, e escrevemos* $[a,b] \leq_{\mathbb{Z}} [c,d]$ *se* $a+d \leq_{\mathbb{N}} b+c$*, onde* $\leq_{\mathbb{N}}$ *é a ordem parcial em* $\mathbb{N}$*.*

Antes de estabelecermos propriedades da relaçãp $\leq_{\mathbb{Z}}$, provamos o seguinte lema.

Lema 3.1 Sejam $a,b,c \in \mathbb{N}$. Então

$$a+b \leq_{\mathbb{N}} a+c \Rightarrow b \leq_{\mathbb{N}} c.$$

Demonstração. De $a+b \leq_{\mathbb{N}} a+c$ obtemos $a+c=(a+b)+k$, para algum $k \in \mathbb{N}$. Tendo em conta o Corolário 3.1, os números naturais a,b,c,k podem ser identificados com os inteiros $[a+1,1],[b+1,1],[c+1,1]$ e $[k+1,1]$, respetivamente. Deste modo, tomando o inteiro $[1,a+1]\,(=-a)$, obtemos, da igualdade $a+c=a+(b+k)$,

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

i.e., $c=b+k$. Logo, $b \leq c$. ■

Teorema 3.3. *(a) A relação* $\leq_{\mathbb{Z}}$ *é uma relação de ordem parcial em* $\mathbb{Z}$*.*

(b) Para quaisquer $x,y \in \mathbb{N}$ *tem-se,*

$$-x \leq_{\mathbb{Z}} y; \quad x \leq_{\mathbb{Z}} y \Leftrightarrow x \leq_{\mathbb{N}} y; \quad x \leq_{\mathbb{Z}} y \Rightarrow -y \leq_{\mathbb{Z}} -x; \quad -y \leq_{\mathbb{Z}} 0 \leq_{\mathbb{Z}} y.$$

Demonstração.

(a) Para qualquer $[x,y] \in \mathbb{Z}$ é claro que $[x,y]=[x,y]$ e, portanto, $[x,y] \leq_{\mathbb{Z}} [x,y]$, i.e., $\leq_{\mathbb{Z}}$ é reflexiva.

Sejam agora $[x,y]$ e $[a,b]$ dois números inteiros tais que $[x,y] \leq_{\mathbb{Z}} [a,b]$ e $[a,b] \leq_{\mathbb{Z}} [x,y]$. Então, $x+b \leq_{\mathbb{N}} y+a$ e $a+y \leq_{\mathbb{N}} b+x$, pelo que $x+b = y+a$, ou seja, $[a,b] = [x,y]$. Portanto, a relação $\leq_{\mathbb{Z}}$ é anti-simétrica.

Finalmente vejamos que a relação é transitiva, i.e., que, para quaisquer $a,b,c,d,x,y \in \mathbb{N}$, se $[a,b] \leq_{\mathbb{Z}} [c,d]$ e $[c,d] \leq_{\mathbb{Z}} [x,y]$ então $[a,b] \leq_{\mathbb{Z}} [x,y]$. Como

$$[a,b] \leq_{\mathbb{Z}} [c,d] \Leftrightarrow a+d \leq_{\mathbb{N}} b+c \text{ e } [c,d] \leq_{\mathbb{Z}} [x,y] \Leftrightarrow c+y \leq_{\mathbb{N}} d+x$$

temos, dadas as propriedades da adição em $\mathbb{N}$ e (ii) do Teorema 2.2,

$$a+d+y \leq b+c+y \text{ e } c+y+b \leq d+x+b$$

isto é,

$$a+y+d \leq b+c+y \leq b+x+d$$

Da transitividade de $\leq_{\mathbb{N}}$ e do Lema 3.1 segue-se agora que $a+y \leq b+x$, i.e., que $[a,b] \leq_{\mathbb{Z}} [x,y]$.

(b) Sejam $x,y \in \mathbb{N}$. É evidente que $-x \leq_{\mathbb{Z}} y$ pois,

$$\begin{aligned} & [1,x+1] \leq_{\mathbb{Z}} [y+1,1] \\ \Leftrightarrow\ & 1+1 \leq_{\mathbb{N}} (x+1)+(y+1) \\ \Leftrightarrow\ & 1+1 \leq_{\mathbb{N}} 1+1+(x+y) \\ \Leftrightarrow\ & 1 \leq_{\mathbb{N}} 1+(x+y). \end{aligned}$$

É também claro que, para quaisquer $x,y \in \mathbb{N}$ se tem $x \leq_{\mathbb{Z}} y \Leftrightarrow x \leq_{\mathbb{N}} y$. De facto,

$$\begin{aligned} x \leq_{\mathbb{Z}} y & \Leftrightarrow [x+1,1] \leq_{\mathbb{N}} [y+1,1] \\ & \Leftrightarrow (x+1)+1 \leq_{\mathbb{N}} 1+(y+1) \\ & \Leftrightarrow x+(1+1) \leq_{\mathbb{N}} y+(1+1) \\ & \Leftrightarrow x \leq_{\mathbb{N}} y. \end{aligned}$$

Mostremos agora que $x \leq_{\mathbb{Z}} y \Rightarrow -y \leq_{\mathbb{Z}} -x, \forall x,y \in \mathbb{N}$. De facto,

$$\begin{aligned} x \leq_{\mathbb{Z}} y &\Leftrightarrow [x+1,1] \leq_{\mathbb{Z}} [y+1,1] \\ &\Leftrightarrow (x+1)+1 \leq_{\mathbb{N}} 1+(y+1) \\ &\Leftrightarrow 1+(x+1) \leq_{\mathbb{N}} 1+(y+1) \\ &\Leftrightarrow [1,y+1] \leq_{\mathbb{Z}} [1,x+1] \\ &\Leftrightarrow -y \leq_{\mathbb{Z}} -x. \end{aligned}$$

Para completar a demonstração provemos que, para qualquer $x \in \mathbb{N}$, se tem $-x \leq_{\mathbb{Z}} 0 \leq_{\mathbb{Z}} x$. Comecemos por ver que $-x \leq_{\mathbb{Z}} 0$.

$$\begin{aligned} [1,x+1] \leq_{\mathbb{Z}} [x,x] &\Leftrightarrow 1+x \leq_{\mathbb{N}} (x+1)+x \\ &\Leftrightarrow 1 \leq_{\mathbb{N}} x+1. \end{aligned}$$

Vejamos agora que $0 \leq_{\mathbb{Z}} x, \forall x \in \mathbb{N}$. Temos:

$$\begin{aligned} 0 \leq_{\mathbb{Z}} x &\Leftrightarrow [x,x] \leq_{\mathbb{Z}} [x+1,1] \\ &\Leftrightarrow x+1 \leq_{\mathbb{N}} (x+1)+x \\ &\Leftrightarrow 1+x \leq_{\mathbb{N}} (x+1)+x \\ &\Leftrightarrow 1 \leq_{\mathbb{N}} x+1. \end{aligned}$$

No início desta demonstração mostrámos que, para quaisquer $x,y \in \mathbb{N}$, se tem $-x \leq_{\mathbb{Z}} y$, logo também se tem $-x \leq_{\mathbb{Z}} x$.

■

Observação: Não havendo ambiguidade, representaremos $\leq_{\mathbb{Z}}$ por $\leq$.

Como consequência do Teorema 2.1 e da definição 3.4 prova-se facilmente que a relação $\leq_{\mathbb{Z}}$ é uma ordem total em $\mathbb{Z}$. De facto, dados $[a,b], [c,d] \in \mathbb{Z}$, como $a+d \in \mathbb{N}$ e $b+c \in \mathbb{N}$, temos $a+d < b+c$ ou $a+d = b+c$ ou $b+c < a+d$, i.e., $[a,b] < [c,d]$ ou $[a,b] = [c,d]$ ou $[c,d] < [a,b]$.

Temos, assim, o seguinte resultado:

Proposição 3.7. $(\mathbb{Z}, \leq)$ *é um conjunto totalmente ordenado.*

Proposição 3.8. *Para quaisquer* $x, y, z \in \mathbb{Z}$*, tem-se*

1. $0\,x = 0$;
2. $-(x\,y) = (-x)\;y = x\;(-y)$;
3. $(x-y)\;z = x\,z - y\,z$;
4. $x\,z = y\,z \wedge z \neq 0 \Rightarrow x = y$;
5. $x\,y = 0 \Rightarrow x = 0 \vee y = 0$;
6. $x \leq y \Rightarrow x + z \leq y + z$;
7. $x \leq y \wedge 0 < z \Rightarrow x\,z \leq y\,z$;
8. $0 \leq x \;\wedge\; 0 \leq y \Rightarrow 0 \leq x + y \;\wedge\; 0 \leq x\,y$;
9. $0 \leq x \;\wedge\; y \leq 0 \Rightarrow x\,y \leq 0$;
10. $x \leq 0 \;\wedge\; y \leq 0 \Rightarrow 0 \leq x\,y$.

Demonstração.

1. Para qualquer $x = [a,b] \in \mathbb{Z}$ e $c \in \mathbb{N}$ tem-se, sucessivamente,

$$0\,x = [c,c]\;[a,b] = [ca + cb, cb + ca] = [ca + cb, ca + cb] = 0.$$

2. Sejam x,y tais que $x=[a,b]$ e $y=[c,d]$ com $a,b,c,d\in\mathbb{N}$. Tem-se:

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

e

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

Se $-(x\,y)=(-x)\ y$ e $(-x)\ y=x\ (-y)$ então $-(x\,y)=x\ (-y)$.

3. Sejam x,y,z tais que $x=[a,b]$, $y=[c,d]$ e $z=[e,f]$ com $a,b,c,d,e,f\in\mathbb{N}$. Tem-se, sucessivamente,

$$\begin{aligned}x\,z-y\,z&=[a,b]\ [e,f]-[c,d]\ [e,f]\\&=[ae+bf,af+be]-[ce+df,cf+de]\\&=[ae+bf,af+be]+[cf+de,ce+df]\\&=[ae+bf+cf+de,af+be+ce+df]\\&=[(a+d)\,e+(b+c)\,f,(a+d)\,f+(b+c)\,e]\\&=[a+d,b+c]\ [e,f]\\&=([a,b]+[d,c])\ [e,f]\\&=([a,b]-[c,d])\ [e,f]\\&=(x-y)\,z.\end{aligned}$$

4. Sejam $x,y,z \in \mathbb{Z}$ e $w \in \mathbb{N}$ tais que $x = [a,b]$,$y = [c,d]$ e $z = [w+1,1]$ ou $z = [1,w+1]$. Mostremos que $x\,z = y\,z \wedge 0 < z \Rightarrow x = y$. De facto,

$$\begin{aligned}
xz = y\,z &\Rightarrow [a,b]\ [w+1,1] = [c,d]\ [w+1,1] \\
&\Rightarrow [a(w+1)+b\,1, a\,1+b(w+1)] = [c\,(w+1)+d\,1, c\,1+d\,(w+1)] \\
&\Rightarrow (\,a\,(w+1)+b, a+b\,(w+1))\,R(c\,(w+1)+d, c+d\,(w+1) \\
&\Rightarrow a\,(w+1)+b+c+d\,(w+1) = a+b\,(w+1)+c\,(w+1)+d \\
&\Rightarrow aw+a+b+c+dw+d = a+bw+b+cw+c+d \\
&\Rightarrow aw+dw = cw+bw \\
&\Rightarrow w\,(a+d) = w\,(c+b) \\
&\Rightarrow a+d = c+b \\
&\Rightarrow (a,b)\,R\,(c,d) \\
&\Rightarrow [a,b] = [c,d] \\
&\Rightarrow x = y.
\end{aligned}$$

   Para $z < 0$ a demonstração é análoga.

5. Sejam $x,y \in \mathbb{Z}$. Provemos que $x\,y = 0 \Rightarrow x = 0 \vee y = 0$. Suponhamos que $x \neq 0$. Então, por (1), por (4) e propriedade comutativa:

$$x\,y = 0 \Rightarrow x\,y = x\,0 \Rightarrow y = 0.$$

6. Sejam $x = [a,b]$,$y = [c,d]$ e $z = [e,f]$. Sendo $a,b,c,d,e,f \in \mathbb{N}$ tem-se,

$$\begin{aligned}
[a,b] \leq [c,d] &\Rightarrow a+d \leq b+c \\
&\Rightarrow a+d+e+f \leq b+c+e+f \\
&\Rightarrow a+e+d+f \leq b+f+c+e \\
&\Rightarrow [a+e,b+f] \leq [c+e,d+f] \\
&\Rightarrow [a,b]+[e,f] \leq [c,d]+[e,f] \\
&\Rightarrow x+z \leq y+z.
\end{aligned}$$

7. Sejam $x = [a,b], y = [c,d]$ e $z = [e,f]$ números inteiros tais que $[a,b] \leq [c,d]$ e $[1,1] \leq [e,f]$. Então $a+d \leq_{\mathbb{N}} b+x$ e $1+f \leq_{\mathbb{N}} 1+e$. Por b) do Teorema 3.3 e por 6. obtemos:

$$1+f \leq_{\mathbb{N}} 1+e \Leftrightarrow 1+f \leq_{\mathbb{Z}} 1+e \Rightarrow 0 \leq e-f.$$

Assim, $e-f \in \mathbb{N}$ e, por ii) do Teorema 2.2 e pela reflexividade de $\leq_{\mathbb{N}}$, segue-se de $a+d \leq_{\mathbb{N}} b+x$ que

$$(a+d)(e-f) \leq_{\mathbb{N}} (b+x)(e-f),$$

i.e., que $xz \leq yz$.

8. Sejam $x,y \in \mathbb{Z}$ tais que $x = [a,b]$ e $y = [c,d]$, $a,b,c,d \in \mathbb{N}$.

Mostremos que: $0 \leq x \wedge 0 \leq y \Rightarrow 0 \leq x+y$. Tem-se, sucessivamente,

$0 \leq x \Rightarrow b \leq a$ e $0 \leq y \Rightarrow d \leq c$, donde, $b+d \leq a+c$, i.e., $0 \leq x+y$.

Vejamos agora que $0 \leq x \wedge 0 \leq y \Rightarrow 0 \leq xy$. De facto, se $0 \leq x \wedge 0 \leq y$, por 7., $0y \leq xy$, por 1., $0 \leq xy$.

9. Sejam $x,y \in \mathbb{Z}$ tais que $0 \leq x$ e $y \leq 0$. Então, por b) do Teorema 3.3, $0 \leq -y$, pelo que se segue, por 8., que $0 \leq x(-y)$. Por 2., obtemos então $0 \leq -(xy)$ e, de novo de b) do Teorema 3.3, resulta que $xy \leq 0$.

10. Sejam $x,y \in \mathbb{Z}$ tais que $0 \leq -x$ e $y \leq 0$. Então, por 9., $(-x)y \leq 0$, pelo que, por 2., $(-xy) \leq 0$. Por b) do Teorema 3.3 obtemos o pretendido: $0 \leq xy$.

■

Como consequência imediata de (6) e (8) da Proposição 3.8 obtemos:

Proposição 3.9. *O anel $(\mathbb{Z},+,\times,\leq)$ é um anel ordenado.*

Proposição 3.10. *Para quaisquer $x,y \in \mathbb{Z}$ tem-se $x \leq_{\mathbb{Z}} y \Leftrightarrow x-y \leq_{\mathbb{Z}} 0$.*

Demonstração. Sejam $x,y \in \mathbb{Z}$ tais que $x \leq_{\mathbb{Z}} y$. Como $x \leq_{\mathbb{Z}} y$ e $-y \leq_{\mathbb{Z}} -y$, temos $x-y \leq_{\mathbb{Z}} y-y$, isto é, $x-y \leq_{\mathbb{Z}} 0$.

Reciprocamente, suponhamos que $x-y \leq_{\mathbb{Z}} 0$. Como $y \leq_{\mathbb{Z}} y$, temos $x-y+y \leq_{\mathbb{Z}} 0+y$ i.e., $x \leq_{\mathbb{Z}} y$. ■

Proposição 3.11. *O anel* $(\mathbb{Z},+,\times,\leq)$ *é um anel arquimediano.*

Demonstração Sejam a e b dois inteiros positivos tais que $a<b$. Então,

$$\begin{aligned} a<b \quad &\Rightarrow b=a+k,\ k\in\mathbb{Z} \\ &\Rightarrow b\,(b+1)=a\,(b+1)+k\,(b+1) \\ &\Rightarrow a\,(b+1)=b+(b^2-bk-k). \end{aligned}$$

Portanto, para qualquer inteiro $n\geq b+1$, temos $na>b$. ■

Definição 3.5. *Para cada* $x\in\mathbb{Z}$*, chama-se módulo ou valor absoluto de* x*, e representa-se por* $|x|$*, ao elemento máximo do conjunto* $\{x,-x\}$*, isto é,*

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

Proposição 3.12. *Para quaisquer* $x,y\in\mathbb{Z}$*, tem-se*

1. $|x|\geq 0$;
2. $|x|=0\Leftrightarrow x=0$;
3. $|x\,y|=|x|\ |y|$;
4. $|x+y|\leq|x|+|y|$.

Demonstração. Sejam $x,y\in\mathbb{Z}$.

1. Se $0<x$ então $|x|=x$ logo $|x|>0$.

   Se $x<0$ então $|x|=-x$ logo $|x|>0$, pois $-x>0$.

   Se $x=0$ então $|x|=0$ pela definição 3.5 .

2. Consequência imediata da definição 3.5.

3. Se $0<x$ e $0<y$ então $0<xy$ pela proposição 3.8 (8) e, portanto, $|xy|=xy=|x|\,|y|$, por definição.

   Se $0<x$ e $y<0$ então $|x|=x$ e $|y|=-y$, isto é, $|x|\,|y|=x(-y)$, i.e., $|x|\,|y|=-(xy)$ pela proposição 3.8(2).

Mas $|xy| = -xy$, pois $xy < 0$ e, portanto, $|xy| = |x|\,|y|$.

Se $x < 0$ e $y < 0$, então $|x| = -x$ e $|y| = -y$, isto é, $|x|\,|y| = (-x)(-y)$, isto é,

$|x|\,|y| = xy$ pela proposição 3.8(10).

Como $0 < xy$ tem-se $|xy| = xy$ e, portanto, $|xy| = |x|\,|y|$.

Se $x = 0 \vee y = 0$ pela proposição 3.8 (1) e proposição 3.12 (2) tem-se $|x\,y| = |x|\ |y|$.
Como consequência de 2) e de 1) da proposição 3.8 é claro que se $x = 0$ ou $y = 0$ então $|xy| = |x|\,|y|$.

4. Se $0 < x$ e $0 < y$ então $|x| = x$ e $|y| = y$, pelo que, $|x| + |y| = x + y$.

   Por outro lado, $0 < x + y$, pelo que, $|x + y| = x + y$ e, portanto, $|x + y| \leq |x| + |y|$.

   Se $x < 0$ e $0 <$ y então $|x| = -x$ e $|y| = y$, pelo que, $|x| + |y| = -x + y$.

   Se $|x| < |y|$ então $0 < x + y$, pelo que, $|x + y| = x + y$ e, portanto, $|x + y| \leq |x| + |y|$.

   Se $|y| < |x|$ então $x + y < 0$ pelo que $|x + y| = -(x + y)$, e portanto, $|x + y| \leq |x| + |y|$.

   Se $0 < x$ e $y < 0$ então $|x| = x$ e $|y| = -y$, pelo que, $|x| + |y| = x - y$.

   Se $|x| < |y|$ então $x + y < 0$, pelo que, $|x + y| = -(x + y)$ e, portanto, $|x + y| \leq |x| + |y|$.

   Se $|y| < |x|$ então $0 < x + y$, pelo que, $|x + y| = x + y$ e, portanto, $|x + y| \leq |x| + |y|$.

   Se $x < 0$ e $y < 0$, então $|x| = -x$ e $|y| = -y$, pelo que, $|x| + |y| = -x - y$.

   Por outro lado, $x + y < 0$, pelo que, $|x + y| = -(x + y)$ e, portanto, $|x + y| \leq |x| + |y|$.

   Se $x = 0 \vee y = 0$ é óbvio que $|x + y| \leq |x| + |y|$.

■

Observemos que o conjunto $(\mathbb{Z}, \leq)$ não é um conjunto bem ordenado pois o subconjunto dos números inteiros menores que zero não tem elemento mínimo. No entanto o conjunto $\{n \in \mathbb{Z} : 0 < n\}$ é um subconjunto bem ordenado de $\mathbb{Z}$, cujo o elemento mínimo é 1 $(\equiv [2, 1])$.

Capítulo 4

Construção e ordenação do conjunto dos números racionais

O sistema de números que construímos no Capítulo 3, $\mathbb{Z}$, tem ainda sérias limitações. Tal como não se pode subtrair em $\mathbb{N}$, também não se pode dividir em $\mathbb{Z}$: não há, em $\mathbb{Z}$, elementos suficientes para acomodar mecanismos de divisão. Mais formalmente, a equação $4x = 3$, por exemplo, de coeficientes inteiros, não tem solução em $\mathbb{Z}$. Veremos, neste capítulo, como ultrapassar este tipo de dificuldade.

4.1 Definição dos números racionais

Definição 4.1. *Seja R a relação binária definida em* $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ *da seguinte forma:*

$$(\forall a, c \in Z \wedge b, d \in \mathbb{Z} \setminus \{0\})\,(a,b)\,R\,(c,d) \Leftrightarrow ad = bc.$$

Proposição 4.1. *A relação R é uma relação de equivalência em* $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$.

Demonstração. Sejam $a, c, e \in \mathbb{Z}$ e $b, d, f \in \mathbb{Z} \setminus \{0\}$. Como a multiplicação é comutativa em $\mathbb{Z}$, $ab = ba$. Logo R é reflexiva.

Suponhamos que $(a,b)\,R\,(c,d)$. Então $ad = bc$ e, como a mutiplicação em $\mathbb{Z}$ é comutativa, temos $da = cb$, ou seja, $cb = da$. Logo, $(c,d)\,R(a,b)$ e, portanto, R é simétrica.

Provemos agora que R é transitiva. Suponhamos que $(a,b)R(c,d)$ e $(c,d)R(e,f)$. Então $ad = bc$ e $cf = de$. Temos: $ad = bc \Rightarrow adf = bcf \Rightarrow adf = bde \Rightarrow af = be \Rightarrow (a,b)R(e,f)$.

■

Dado $(a,b) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$ representamos a classe de equivalência de (a,b), determinada por R, por $[a,b]$. Assim,

$$[a,b] = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\} : (a,b)R(c,d)\}.$$

Representamos o conjunto $(\mathbb{Z} \times \mathbb{Z}\setminus\{0\})/R$ por $\mathbb{Q}$. Assim, por definição,

$$\mathbb{Q} = \{[a,b] : (a,b) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}\}.$$

Aos elementos de $\mathbb{Q}$ chamamos *números racionais*.

4.2 Operações binárias em $\mathbb{Q}$

Em $\mathbb{Q}$ vamos definir a adição e a multiplicação de números racionais.

Definição 4.2. *Sejam* $[a,b],[c,d] \in \mathbb{Q}$. *Define-se* $[a,b]+[c,d] = [ad+cb,bd]$.

Na proposição seguinte mostramos que a adição, definida desta forma, não depende da escolha dos representantes das classes de equivalência envolvidas.

Proposição 4.2. *Para quaisquer* $[a,b],[c,d],[e,f],[g,h] \in \mathbb{Q}$, *tais que* $[a,b] = [c,d]$ *e* $[e,f] = [g,h]$, *tem-se* $[a,b]+[e,f] = [c,d]+[g,h]$.

Demonstração. Sejam $[a,b],[c,d],[e,f],[g,h] \in \mathbb{Q}$. Como $[a,b] = [c,d]$ e $[e,f] = [g,h]$ temos $(a,b)R(c,d)$ e $(e,f)R(g,h)$ e, portanto, $ad = cb$ e $eh = fg$.

Como $adfh = cbfh$ e $ehbd = fgbd$ temos, $adfh + ehbd = cbfh + fgbd$, i.e., $(af+eb)hd = fb(ch+gd)$ e, portanto, $[af+eb,fb] = [ch+gd,hd]$, i.e., $[a,b]+[e,f] = [c,d]+[g,h]$.

■

Proposição 4.3. *Se* $c \in \mathbb{Z}\setminus\{0\}$ *e* $[a,b] \in \mathbb{Q}$ *então* $[a,b] = [ac,bc] = [ca,cb]$.

Demonstração. $[a,b] = [ac,bc] \Leftrightarrow (a,b)\,R\,(ac,bc) \Leftrightarrow abc = bac \Leftrightarrow abc = abc$.

■

Proposição 4.4. *A adição definida em* $\mathbb{Q}$ *goza das seguintes propriedades:*

1. $\forall\,[a,b],[c,d] \in \mathbb{Q},\ \ [a,b]+[c,d] = [c,d]+[a,b]$;
2. $\forall\,[a,b],[c,d],[e,f] \in \mathbb{Q},\ \ [a,b]+([c,d]+[e,f]) = ([a,b]+[c,d])+[e,f]$;
3. $\forall n \in \mathbb{Z}\setminus\{0\}, \forall\,[a,b] \in \mathbb{Q},\ [0,n]+[a,b] = [a,b]+[0,n] = [a,b]$;
4. $\forall\,[a,b] \in \mathbb{Q}, [a,b]+[-a,b] = [0,n], n \in \mathbb{Z}\setminus\{0\}$.

Demonstração. Sejam $[a,b],[c,d]$ e $[e,f] \in \mathbb{Q}$

1) Temos:

$$\begin{aligned}[a,b]+[c,d] &= [ad+bc,bd] \text{ (por definição)}\\ &= [cb+da,db] \text{(pela propriedade comutativa da adição e multiplicação em } \mathbb{Z})\\ &= [c,d]+[a,b] \text{ (por definição).}\end{aligned}$$

2) Temos:

$$\begin{aligned}[a,b]+([c,d]+[e,f]) &= [a,b]+[cf+de,df]\\ &= [adf+(cf+de)b,bdf]\\ &= [adf+cfb+deb,bdf]\\ &= [ad+bc,bd]+[e,f]\\ &= ([a,b]+[c,d])+[e,f].\end{aligned}$$

3) O número racional $[0,n]$, $\forall n \in \mathbb{Z}\setminus\{0\}$, é o elemento neutro para a adição.

De facto, tem-se

$$\begin{aligned}[a,b]+[0,n] &= [an+b\cdot 0,bn]\\ &= [an,bn]\\ &= [a,b]. \text{ Proposição 4.3}\end{aligned}$$

4) Seja $n \in \mathbb{Z}\setminus\{0\}$. Temos:

$$\begin{aligned}[a,b]+[-a,b] &= [ab+b(-a),bb] \\ &= [ab-ab,bb] \\ &= [0,bb] \\ &= [0,n], \text{ sendo } n = bb.\end{aligned}$$

■

Em virtude da propriedade 3), o número racional $[0,n]$, para qualquer $n \in \mathbb{Z}\setminus\{0\}$, designa-se por elemento neutro da adição e representa-se por $0_{\mathbb{Q}}$. A propriedade 4) estabelece que qualquer número racional $[a,b]$ tem simétrico, a saber, o número racional $[-a,b]$. Este número representa-se por $-[a,b]$.

Definição 4.3. *Sejam* $[a,b],[c,d] \in \mathbb{Q}$. *Define-se* $[a,b]\cdot[c,d] = [ac,bd]$.

Tal como aconteceu com a adição, a operação definida desta forma não depende da escolha dos representantes das classes envolvidas, como podemos verificar pela proposição seguinte.

Proposição 4.5. *Para quaisquer* $[a,b],[c,d],[e,f],[g,h] \in \mathbb{Q}$, *tais que* $[a,b] = [c,d]$ *e* $[e,f] = [g,h]$, *tem-se* $[a,b]\cdot[e,f] = [c,d]\cdot[g,h]$.

Demonstração. Sejam $[a,b],[c,d],[e,f],[g,h] \in \mathbb{Q}$. Como $[a,b] = [c,d]$ e $[e,f] = [g,h]$ temos: $(a,b)R(c,d)$ e $(e,f)R(g,h)$, i.e., $ad = bc$ e $eh = fg$. Como $ehad = fgad \Leftrightarrow ehad = fgbc$, tem-se $aedh = cgbf$, i.e., $(ae,bf)R(cg,dh)$, i.e., $[ae,bf] = [cg,dh]$. i.e.,$[a,b]\cdot[e,f] = [c,d]\cdot[g,h]$.

■

Proposição 4.6. *A multiplicação definida em* $\mathbb{Q}$ *goza das seguintes propriedades:*

1. $\forall [a,b],[c,d] \in \mathbb{Q}, \quad [a,b]\cdot[c,d] = [c,d]\cdot[a,b]$;
2. $\forall [a,b],[c,d],[e,f] \in \mathbb{Q}, \quad [a,b]\cdot([c,d]\cdot[e,f]) = ([a,b]\cdot[c,d])\cdot[e,f]$;
3. $\forall n \in \mathbb{Z}\setminus\{0\}\ \forall [a,b] \in \mathbb{Q},\ [a,b]\cdot[n,n] = [n,n]\cdot[a,b] = [a,b]$;
4. *Para qualquer* $[a,b] \neq [0,n]$, $[a,b]\cdot[b,a] = [n,n]$, $\forall n \in \mathbb{Z}\setminus\{0\}$;
5. $\forall [a,b],[c,d],[e,f] \in \mathbb{Q}, \quad [a,b]\cdot([c,d]+[e,f]) = [a,b]\cdot[c,d]+[a,b]\cdot[e,f]$.

Demonstração. Para demonstrar 1) e 2) basta usar a definição da multiplicação e as propriedades análogas válidas em $\mathbb{Z}$.

3) Sejam $n \in \mathbb{Z}\setminus\{0\}$ e $[a,b] \in \mathbb{Q}$. Então $[a,b]\cdot[n,n] = [an,bn] = [a,b]$, pela proposição 4.3. Logo, o racional $[n,n]$ é o elemento neutro da multiplicação.

4) Seja $[a,b] \in \mathbb{Q}$ tal que $[a,b] \neq [0,n]$, $n \in \mathbb{Z}\setminus\{0\}$. Temos:

$$\begin{aligned}[a,b]\cdot[b,a] &= [ab,ba]\\ &= [ab,ab]\\ &= [n,n].\end{aligned}$$

5) Sejam $[a,b],[c,d],[e,f] \in \mathbb{Q}$. Temos:

$$\begin{aligned}[a,b]\cdot[c,d]+[a,b]\cdot[e,f] &= [ac,bd]+[ae,bf]\\ &= [acbf+bdae,bdbf]\\ &= [b(acf+dae),bdbf]\\ &= [bb]\cdot[acf+dae,dbf], \text{ pela proposição 4.6.3}\\ &= [acf+dae,dbf]\\ &= [a(cf+de),bdf]\\ &= [a,b]\cdot[cf+de,df]\\ &= [a,b]\cdot([c,d]+[e,f]).\end{aligned}$$

■

Observemos que, por 3), a multiplicação definida em $\mathbb{Q}$ admite elemento neutro. Representa-se este elemento neutro por $1_{\mathbb{Q}}$. Além disso, por 4), qualquer número racional não nulo r é invertível. O inverso de $r \in \mathbb{Q}\setminus\{0\}$ representa-se por r^{-1}.

Tendo em conta as propriedades da adição e da multiplicação em $\mathbb{Q}$, tem-se a seguinte proposição.

Proposição 4.7. *O terno* $(\mathbb{Q},+,\times)$ *é um corpo.*

4.3 Uma ordem parcial em $\mathbb{Q}$

Os números racionais são, como vimos, classes de equivalência de pares de números inteiros, pelo que definiremos uma relação de ordem parcial em $\mathbb{Q}$ a partir da ordem parcial definida em $\mathbb{Z}$.

Definição 4.4. *Dados os números racionais $[a,b]$ e $[c,d]$, dizemos que $[a,b]$ é menor ou igual que $[c,d]$, e escrevemos $[a,b] \leq_{\mathbb{Q}} [c,d]$ se $(ad-bc)(bd) \leq_{\mathbb{Z}} 0$, onde $\leq_{\mathbb{Z}}$ é a ordem total em $\mathbb{Z}$.*

Teorema 4.1. *A relação $\leq_{\mathbb{Q}}$ é uma relação de ordem total em $\mathbb{Q}$.*

Demonstração. Para qualquer $[a,b] \in \mathbb{Q}$ é claro que $[a,b] = [a,b]$ e, portanto, $[a,b] \leq [a,b]$, i.e., $\leq_{\mathbb{Q}}$ é reflexiva.

Sejam agora $[a,b]$ e $[c,d]$ dois números racionais. Mostremos que, se $[a,b] \leq_{\mathbb{Q}} [c,d]$ e $[c,d] \leq_{\mathbb{Q}} [a,b]$ então $[a,b] = [c,d]$. Como

$$[a,b] \leq_{\mathbb{Q}} [c,d] \Leftrightarrow (ad-bc)(bd) \leq_{\mathbb{Z}} 0 \Leftrightarrow adbd - bcbd \leq_{\mathbb{Z}} 0 \Leftrightarrow adbd \leq_{\mathbb{Z}} bcbd \quad (1)$$
$$[c,d] \leq_{\mathbb{Q}} [a,b] \Leftrightarrow (cb-da)(db) \leq_{\mathbb{Z}.} 0 \Leftrightarrow cbdb - dadb \leq_{\mathbb{Z}.} 0 \Leftrightarrow cbdb \leq_{\mathbb{Z}} dadb \quad (2).$$

podemos concluir que $addb = cbdb$, i.e., $ad = cb$, pelo que, $(a,b)\,R\,(c,d)$, i.e., $[a,b] = [c,d]$.

Mostremos agora que para qualquer $[a,b], [c,d], [e,f] \in \mathbb{Q}$, se $[a,b] \leq_{\mathbb{Q}} [c,d]$ e $[c,d] \leq_{\mathbb{Q}} [e,f]$, então $[a,b] \leq_{\mathbb{Q}} [e,f]$. Como,

$$[a,b] \leq_{\mathbb{Q}} [c,d] \wedge [c,d] \leq_{\mathbb{Q}} [e,f]$$

temos:

$$[af,bf] \leq_{\mathbb{Q}} [c,d] \wedge [c,d] \leq_{\mathbb{Q}} [be,bf],$$

i.e.,

$$(afd-bfc)(bfd) \leq_{\mathbb{Z}} 0 \wedge (cbf-dbe)(dbf) \leq_{\mathbb{Z}} 0.$$

Mas,

$$(afd-bfc)(bfd) + (cbf-dbe)(dbf) \leq_{\mathbb{Z}} 0,$$

i.e.,

$$(afd-cbf+cbf-dbe)(dbf) \leq_{\mathbb{Z}} 0,$$

i.e.,

$$(afd - dbe)(dbf) \leq_{\mathbb{Z}} 0.$$

Assim, $[a,b] \leq_{\mathbb{Q}} [e,f]$.

Finalmente, mostremos que $\leq_{\mathbb{Q}}$ é tricotómica. Sejam $[a,b],[c,d] \in \mathbb{Q}$ tais que $[a,b] \neq [c,d]$. Então $ad \neq bc$ pelo que $ad - bc \neq 0$. Como $\leq_{\mathbb{Z}}$ é tricotómica, temos então que ou $ad - bc < 0$ ou $0 < ad - bc$. Com $bd \neq 0$ $(b,d \in \mathbb{Z} \setminus \{0\})$, temos, também $bd < 0$ ou $0 < bd$. Assim, $(ad - bc)(bd) \leq 0$ ou $0 \leq (ad - bc)(bd)$, pelas propriedades (8), (9) e (10) da Proposição 3.8. Como $ad - bc \neq 0$ e $bd \neq 0$, segue-se, pela proposição 3.8(5), que $(ad - bc)(bd) < 0$ ou $0 < (ad - bc)(bd)$.

■

As propriedades enunciadas e demonstradas em $\mathbb{Z}$ (Proposição 3.8) verificam-se em $\mathbb{Q}$. De seguida destacamos três dessas propriedades e provamos duas delas.

Proposição 4.8. *Para quaisquer* $[a,b],[c,d],[e,f] \in \mathbb{Q}$ *tem-se,*

1. $[a,b] \leq [c,d] \Rightarrow [a,b] + [e,f] \leq [c,d] + [e,f]$;

2. $[a,b] \leq [c,d] \wedge [0,x] < [e,f], x \in \mathbb{Z}\setminus\{0\} \Rightarrow [a,b] \cdot [e,f] \leq [c,d] \cdot [e,f]$;

3. $[0,x] \leq [a,b], [0,x] \leq [c,d], x \in \mathbb{Z}\setminus\{0\} \Rightarrow [0,x] \leq [a,b] \cdot [c,d] \wedge [0,x] \leq [a,b] + [c,d]$.

Demonstração.

1) Sejam $[a,b],[c,d],[e,f] \in \mathbb{Q}$. Tem-se, sucessivamente,

$$\begin{aligned}
[a,b] \leq [c,d] &\Rightarrow (ad - bc)(bd) \leq 0 \\
&\Rightarrow (adf - cbf)(bdf) \leq 0 \\
&\Rightarrow (adf + bed - cfb - bed)(bfd) \leq 0 \\
&\Rightarrow [(af + be)d - (cf + ed)b](bfd) \leq 0 \\
&\Rightarrow [af + be, bf] \leq [cf + ed, df] \\
&\Rightarrow [a,b] + [e,f] \leq [c,d] + [e,f].
\end{aligned}$$

2) Sejam $[a,b],[c,d],[e,f] \in \mathbb{Q}$ tais que $[a,b] \leq [c,d] \wedge [0,x] < [e,f], x \in \mathbb{Z}\setminus\{0\}$. Temos:

$$\begin{aligned}
[a,b] \leq [c,d] &\Rightarrow (ad-bc)(bd) \leq 0 \\
&\Rightarrow e(ad-bc) f(bd) \leq 0 \\
&\Rightarrow (ade-bce)(fbd) \leq 0 \\
&\Rightarrow [ade, fbd] \leq [bce, fbd] \\
&\Rightarrow [ae, fb] \leq [ce, fd] \\
&\Rightarrow [a,b] \cdot [e,f] \leq [c,d] \cdot [e,f].
\end{aligned}$$

■

A proposição seguinte é consequência imediata da Proposição 4.7 e de (1) e (3) da Proposição 4.8.

Proposição 4.9. *O triplo $(\mathbb{Q},+,\leq)$ é um grupo ordenado e $(\mathbb{Q},+,\times,\leq)$ é um corpo ordenado.*

Proposição 4.10. *O corpo $(\mathbb{Q},+,\times,\leq)$ é arquimediano.*

Demonstração. Sejam $a,b \in \mathbb{Q}^+$ tais que $a < b$. Então $a = [p,q]$ e $b = [r,s]$, para certos inteiros positivos p,q,r,s. De $a = [p,q] < b = [r,s]$ obtemos, por (8), (9) e (10) da Proposição 3.8, uma das duas seguintes situações: (i) $ps - qr < 0$ e $qs > 0$; (ii) $ps - qr > 0$ e $qs < 0$. No caso de se dar (i), temos $ps < qr$ e, como $\mathbb{Z}$ é arquimediano, existe um inteiro n tal que $nps > qr$, i.e., $qr - nps < 0$. Deste modo, como $qs > 0$, segue-se, por (9) da Proposição 3.8, que $(qr - nps)(qs) < 0$, i.e., $[r,s] < n[p,q]$. Portanto, $b < na$. Analogamente, a situação (ii) leva-nos a $[r,s] < k[p,q]$ e, portanto, a $b < ka$, para algum inteiro k.

■

4.4 Relação entre $\mathbb{Q}$ e $\mathbb{Z}$

Nesta seção mostramos que o anel $(\mathbb{Z},+,\times)$ pode ser considerado um subanel de $(\mathbb{Q},+,\times)$.

Teorema 4.2. *A aplicação $\theta : \mathbb{Z} \to \mathbb{Q}$, definida por $\theta(z) = [z,1]$, para qualquer $z \in \mathbb{Z}$, é um monomorfismo de anel.*

Demonstração. Comecemos por verificar que θ é injetiva. Sejam $x,y \in \mathbb{Z}$ tais que $\theta(x) = \theta(y)$. Então $[x,1] = [y,1]$ pelo que $(x,1)\,R(y,1)$, i.e., $x\,1 = 1\,y$. Logo, $x = y$. Vejamos agora que, para quaisquer $x,y \in \mathbb{Z}$, se tem

$$\theta(x) + \theta(y) = [x+y,1] \;\wedge\; \theta(x) \cdot \theta(y) = [x\,y,1]\,.$$

Como, $\theta(x) = [x,1]$ e $\theta(y) = [y,1]$, tem-se,

$$\theta(x) + \theta(y) = [x,1] + [y,1] = [x\,1 + y\,1,1] = [x+y,1] = \theta(x+y)$$

$$\theta(x)\;\; \theta(y) = [x,1]\;\; [y,1] = [x\,y,1] = \theta(x\,y)\,.$$

■

Tendo em conta o teorema anterior, vemos que $\mathbb{Z} \simeq \theta(\mathbb{Z})$, onde $\theta(\mathbb{Z})$ é um subanel de $\mathbb{Q}$. Deste modo, cada elemento de $\mathbb{Z}$ pode ser identificado com o elemento $[z,1]$ de $\mathbb{Q}$. O racional $[1,z]$ é o elemento inverso de $[z,1]$ e representa-se por z^{-1}.

Observemos que, para quaisquer $a,b \in \mathbb{Q}$ e $a \neq 0$, como existe $a^{-1} \in \mathbb{Q}$, a equação $ax = b$ tem solução em $\mathbb{Q}$: $x = a^{-1}b$, ficando, deste modo, ultrapassada a dificuldade existente no anel $\mathbb{Z}$, relativamente à solubilidade de equações do 1º grau, apresentada no inicio deste capítulo.

Observemos, finalmente, que o conjunto $\mathbb{Q}^+ = \{[a,b] \in \mathbb{Q} : [0,1] < [a,b]\}$ não é bem ordenado. De facto, o subconjunto $A = \{[a,b] \in \mathbb{Q}^+ : [a,b] < [a,a]\}$ de $\mathbb{Q}^+$ não tem elemento mínimo, pois, para qualquer $b \in \mathbb{Z}/\{0\}$ e $0 < b$, $[1,b] \in A$ e, para qualquer $k \in \mathbb{Z}$ tal que $b < k$, $[1,k] \in A$ e $[1,k] <_{\mathbb{Q}} [1,b]$, uma vez que $(1 \cdot b - k \cdot 1)\,(kb) \leq 0$.

Capítulo 5

Construção e ordenação do conjunto dos números reais

Apesar das vantagens que $\mathbb{Q}$ apresenta em relação a $\mathbb{Z}$, $\mathbb{Q}$ não é, ainda, um sistema numérico adequado. Por exemplo, a equação $x^2 = 2$ não é solúvel em $\mathbb{Q}$.

Outra dificuldade com o corpo dos números racionais é que, embora toda a sucessão de números racionais convergente seja uma sucessão de Cauchy, há sucessões de Cauchy de números racionais que não são convergentes em $\mathbb{Q}$ (veremos um exemplo de uma tal sucessão mais à frente).

É assim necessário proceder a uma ampliação de $\mathbb{Q}$ que acomode a solução das *falhas* indicadas. Deste modo surgem os números reais. A construção dos números reais que apresentamos neste capítulo é devida a Georg Cantor (1845-1918) e tem como objetivo a construção de um corpo ordenado que estenda $\mathbb{Q}$ e no qual toda a sucessão de Cauchy seja convergente.

Começamos com uma breve apresentação de conceitos básicos.

5.1 Conceitos básicos

Seja G um grupo ordenado.

Definição 5.1. *Diz-se que uma sucessão* $(x_n)_n$, $n \in \mathbb{N}$, *de elementos de G, é convergente para* $x \in G$ *se* $\forall \varepsilon \in G^+,\ \exists p \in \mathbb{N} :\ \forall n \geq p\ |x_n - x| < \varepsilon$. *Escrevemos* $x_n \to x$ ou $limx_n = x$.

Definição 5.2. *Uma sucessão* $(x_n)_n$, $n \in \mathbb{N}$, *de elementos de G, diz-se limitada se*

$$\exists a,b \in G : a \leq x_n \leq b \ ,$$

para qualquer $n \in \mathbb{N}$.

Proposição 5.1. *Toda a sucessão convergente em G é limitada em G.*

Demonstração. Seja $(x_n)_n$, $n \in \mathbb{N}$, uma sucessão de elementos de G, convergente para $x \in G$. Assim,

$\forall \varepsilon \in G^+, \exists p \in \mathbb{N}, \forall n \geq p, |x_n - x| < \varepsilon$, i.e., $x - \varepsilon < x_n < x + \varepsilon$

e, portanto, $(x_n)_n$ é uma sucessão limitada em G.

■

No estudo do Exemplo 5.1, que apresentamos adiante, é importante o conceito de sucessão decimal de números racionais.

Definição 5.3. *Uma sucessão* $(x_n)_n$, $n \in \mathbb{N}$, *de números racionais, da forma*

$$x_0 = a_0; x_1 = a_0 + \frac{a_1}{10}; \ldots; x_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}; \ldots$$

onde a_0 *é um número inteiro e* $0 \leq a_n \leq 9$ *para qualquer* $n \geq 1$, *diz-se uma sucessão decimal.*

Definição 5.4. *Uma sucessão* $(x_n)_n$, $n \in \mathbb{N}$, *de elementos de G, diz-se uma sucessão de Cauchy em G se*

$$\forall \varepsilon \in G^+, \exists p \in \mathbb{N}, \forall n,m \geq p \ |x_n - x_m| < \varepsilon,$$

isto é, se

$$\forall \varepsilon \in G^+, \exists p \in \mathbb{N}, \forall n \geq p, \forall k > 0 \ |x_{n+k} - x_n| < \varepsilon.$$

Proposição 5.2. *Toda a sucessão decimal em* $\mathbb{Q}$ *é uma sucessão de Cauchy.*

Demonstração. Para mostrar que a sucessão

$$x_0 = a_0; x_1 = a_0 + \frac{a_1}{10}; \ldots; x_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}; \ldots$$

é uma sucessão de Cauchy determinemos, para cada $\varepsilon > 0$, uma ordem p que verifica a condição $|x_{n+k} - x_n| < \varepsilon$, para cada $n \geq p$ e para cada $k > 0$.

Como $|x_{n+k}-x_n| = \frac{a_{n+1}}{10^{n+1}} + \ldots + \frac{a_{n+k}}{10^{n+k}}$ temos, $|x_{n+k}-x_n| \leq \frac{9}{10^{n+1}}\left(1+\frac{1}{10}+\ldots+\frac{1}{10^{k-1}}\right)$, pois $0 \leq a_n \leq 9$, para qualquer $n \geq 1$. Mas $1+\frac{1}{10}+\ldots+\frac{1}{10^{k-1}} = \frac{1-\frac{1}{10^k}}{1-\frac{1}{10}} < \frac{10}{9}$ e, portanto, $|x_{n+k}-x_n| < \frac{9}{10^{n+1}} \cdot \frac{10}{9} = \frac{1}{10^n}$. Como $\frac{1}{10^n} \to 0$, a sucessão $(x_n)_n$ é uma sucessão de Cauchy.

■

Proposição 5.3. *Toda a sucessão de Cauchy de elementos de G é limitada.*

Demonstração. Consideremos $(x_n)_n$, $n \in \mathbb{N}$, uma sucessão de Cauchy de elementos de G. Tomemos um $\varepsilon \in G^+$. Então existe $p \in \mathbb{N}$ tal que $x_p - \varepsilon < x_n < x_p + \varepsilon$, $n \geq p$. Isto significa que a sucessão é limitada.

■

Proposição 5.4. *Toda a sucessão $(x_n)_n$, $n \in \mathbb{N}$, de elementos de G convergente é sucessão de Cauchy em G .*

Demonstração. Seja $(x_n)_n$, $n \in \mathbb{N}$ uma sucessão de elementos de G convergente para $x \in G$, i.e.,

$\forall \varepsilon \in G^+,\ \exists p \in \mathbb{N},\ \forall n \geq p\ |x_n - x| < \frac{\varepsilon}{2}$.

Tomando $m, n \in \mathbb{N}$ tais que $m, n \geq p$ tem-se

$$|x_m - x_n| = |x_m - x - x_n + x| \leq |x_m - x| + |x_n - x| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Logo $(x_n)_n$ é uma sucessão de Cauchy.

■

Observamos que existem grupos ordenados nos quais há sucessões de Cauchy que não são convergentes. O seguinte exemplo apresenta uma dessa situações.

Exemplo 5.1: Seja $x \in \mathbb{Q}$. A equação $x^2 = 2$ não tem solução em $\mathbb{Q}$. É, no entanto, possível definir sucessões de Cauchy de números racionais, $(a_n)_n$ e $(b_n)_n$, tais que $a_n^2 < 2 < b_n^2$ e $(b_n)_n - (a_n)_n \to 0$.

Comecemos por verificar que a equação $x^2 = 2$ não tem solução no conjunto dos números racionais. Para tal vamos supor que tal solução existe. Seja ela $x_0 = [a, b]$, onde $a, b \in \mathbb{Z}$ são primos entre si e $b \neq 1$. Então tem-se

$[a,b]\cdot[a,b]=[2,1]\Leftrightarrow[aa,bb]=[2,1]\Leftrightarrow aa=2bb$, isto é, $a^2=2b^2$

Logo a^2 é par e, portanto, a é também par, i.e., $a=2k$, para algum $k\in\mathbb{Z}$. Assim,

$$a^2=2b^2\Leftrightarrow 4k^2=2b^2\Leftrightarrow b^2=2k^2,$$

pelo que b^2 é par e, portanto, b é par. Deste modo, 2 é um divisor comum a a e b, o que contraria o facto destes dois números serem primos entre si.

Embora, como vimos, não seja possível encontrar em $\mathbb{Q}$ solução para a equação $x^2=2$, podemos definir duas sucessões de Cauchy de números racionais, $(a_n)_n$ e $(b_n)_n$, tais que $a_n^2<2<b_n^2$ e $(b_n)_n-(a_n)_n\to 0$. Estas sucessões não têm limite em $\mathbb{Q}$ pois, se $(a_n)_n\to a$, $a\in\mathbb{Q}$, também $(b_n)_n\to a$ porque $(b_n)_n-(a_n)_n\to 0$, logo ter-se-ia $a^2=2$, o que é absurdo como vimos anteriormente. Definamos, então, tais sucessões. Para cada $n\in\mathbb{N}_0$, seja p_n o maior inteiro tal que $p_n^2<2\cdot 10^{2n}$ e sejam $(a_n)_n=\frac{p_n}{10^n}$ e $(b_n)_n=(a_n)_n+\frac{1}{10^n}$. É claro que $\left(\frac{p_n}{10^n}\right)^2<2<\left(\frac{p_n+1}{10^n}\right)^2$ e que $(b_n)_n-(a_n)_n=\frac{1}{10^n}\to 0$. Mostremos agora que $(a_n)_n$ é uma sucessão de Cauchy. Pela Proposição 5.2, basta verificar que $(a_n)_n$ se pode escrever como uma sucessão decimal, isto é,

$$a_0=x_0,\ a_1=x_0+\frac{x_1}{10},\ a_2=x_0+\frac{x_1}{10}+\frac{x_2}{10^2},\ldots,\ a_n=x_0+\frac{x_1}{10}+\ldots+\frac{x_n}{10^n},$$

onde $x_0,\ x_1,\ \ldots,x_n$ são inteiros tais que $0\leq x_n\leq 9$, para $n\geq 1$. De facto, definindo

$$x_0=a_0$$

$$x_1=10\,(a_1-a_0)$$

$$\ldots$$

$$x_n=10^n(a_n-a_{n-1})$$

obtemos, para $n\geq 1$, $x_n=p_n-10p_{n-1}$ pelo que $0\leq p_n-10p_{n-1}\leq 9$, $n\geq 1$.

A construção dos números reais que aqui apresentamos será feita a partir de sucessões de Cauchy. O nosso objetivo é construir um corpo ordenado que seja uma extensão de $\mathbb{Q}$ e no qual toda a sucessão de Cauchy de números racionais seja convergente.

5.2 A construção de uma extensão de $\mathbb{Q}$

Como vimos no exemplo 5.1 existem sucessões de Cauchy de números racionais que não convergem em $\mathbb{Q}$. Vamos agora construir um corpo ordenado, que seja uma extensão de $\mathbb{Q}$, mas onde as sucessões de Cauchy sejam convergentes.

Seja C o conjunto das sucessões de Cauchy de números racionais, com as operações $(x_n)_n + (y_n)_n = (x_n + y_n)_n$ e $(x_n)_n \cdot (y_n)_n = (x_n \cdot y_n)_n$. O triplo $(C, +, \times)$ é um anel comutativo com identidade. O elemento nulo é a sucessão cujos termos são todos iguais a 0 e o elemento identidade é a sucessão constante com os termos todos iguais a 1. Seja I o subconjunto de C formado pelas sucessões que convergem para zero.

Proposição 5.5. *I é ideal de C.*

Demonstração. $(I, +)$ é um subgrupo do grupo $(C, +)$, pois, dadas $(a_n)_n, (b_n)_n \in I$ se $(a_n)_n \to 0$ e $(b_n)_n \to 0$ então $(a_n)_n - (b_n)_n \to 0$. Além disso, se $(a_n)_n \in I$ e $(b_n)_n \in C$ então $(a_n)_n \cdot (b_n)_n \to 0$, uma vez que, $(a_n)_n \to 0$ e $(b_n)_n$ é limitada, por ser sucessão de Cauchy.

■

Sendo I um ideal de C, I determina em C a seguinte relação de congruência:

$$\forall (a_n)_n, (b_n)_n \in C,\ (a_n)_n \equiv (b_n)_n \,(mod\, I) \Leftrightarrow (a_n)_n - (b_n)_n \in I,$$

i.e., $(a_n)_n \equiv (b_n)_n \,(mod\, I) \Leftrightarrow (a_n)_n - (b_n)_n \to 0$, para quaisquer $(a_n)_n, (b_n)_n \in C$. Em consequência, as igualdades

$$[(a_n)_n] + [(b_n)_n] = [(a_n + b_n)_n]$$

$$[(a_n)_n] \cdot [(b_n)_n] = [(a_n \cdot b_n)_n],$$

para quaisquer $[(a_n)_n], [(b_n)_n] \in C/I$, definem operações binárias em C/I, sendo que o triplo $(C/I, +, \cdot)$ é um anel comutativo com identidade. Neste anel, o zero é o conjunto das sucessões de Cauchy que convergem para 0 e a identidade é o conjunto das sucessões de Cauchy que convergem para zero 1.

Representamos o anel C/I por $\mathbb{R}$ e aos elementos de $\mathbb{R}$ chamamos *números reais*. Um número real é, assim, uma classe de equivalência de certa sucessão de Cauchy $(a_n)_n$, mais precisamente, o número real $[(a_n)_n]_I$, que representaremos por $[a_n]$, é o conjunto das sucessões de Cauchy $(b_n)_n$ tais que $(a_n)_n - (b_n)_n \to 0$.

Proposição 5.6. $(\mathbb{R}, +, \times)$ *é um corpo.*

Demonstração.
Como já observámos, $\mathbb{R}$ é um anel comutativo com identidade. Para mostrar que $\mathbb{R}$ é um corpo resta provar que todo o elemento não nulo de $\mathbb{R}$ é invertível. Seja $x \in \mathbb{R} \setminus \{0_{\mathbb{R}}\}$ e seja $(x_n)_n$ uma sucessão de Cauchy geradora de x. Então $(x_n)_n \nrightarrow 0$ e, portanto,

$$\exists \varepsilon_0 \in \mathbb{Q}^+ : \ \forall p \in \mathbb{N}, \ \exists n \geq p : \ |x_n| \geq \varepsilon.$$

Como a sucessão $(x_n)_n$ é de Cauchy, temos que, para o racional positivo ε_0,

$$\exists t \in \mathbb{N} : \ \forall n \geq t, \ \forall k > 0, \ |x_{n+k} - x_n| < \varepsilon_0.$$

Seja y_n a sucessão definida por $y_n = \begin{cases} \frac{1}{x_n} & \text{se } n > t \\ 0 & \text{se } n \leq t \end{cases}$. Mostremos que y_n é uma sucessão de Cauchy. De facto, para $n, m \geq t$ tem-se,

$$|y_n - y_m| = \left| \frac{1}{x_n} - \frac{1}{x_m} \right| = \left| \frac{x_m - x_n}{x_n \cdot x_m} \right| < \frac{1}{\alpha^2} |x_n - x_m| < \alpha \quad ,$$

i.e., y_n é uma sucessão de Cauchy. Além disso, $[x_n] \cdot [y_n] = \begin{cases} x_n \frac{1}{x_n} & \text{se } n > t \\ 0 & \text{se } n \leq t \end{cases} = \begin{cases} 1 & \text{se } n > t \\ 0 & \text{se } n \leq t \end{cases}$.

Assim, $(x_n y_n)_n$ converge para 1 e, portanto, $[x_n] \cdot [y_n] = 1_{\mathbb{R}}$. Logo, $[x_n]$ é invertível.

■

Teorema 5.1. *A aplicação $\varphi : \mathbb{Q} \to \mathbb{R}$, que associa a cada número racional r o número real $[r]$ gerado pela sucessão constante de termos todos iguais a r, é um monomorfismo.*

Demonstração. φ é injetiva pois dados $r, s \in \mathbb{Q}$ temos

$$\varphi(r) = \varphi(s) \Leftrightarrow [r_n] = [s_n] \Leftrightarrow r_n - s_n \to 0 \Leftrightarrow r - s = 0 \Leftrightarrow r = s.$$

Além disso, para quaisquer $r,s \in \mathbb{Q}$ tem-se,$\varphi(r+s) = \varphi(r) + \varphi(s)$ e $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$. De facto,

$$\varphi(r+s) = [r_n + s_n] = [r_n] + [s_n] = \varphi(r) + \varphi(s)$$

e

$$\varphi(r \cdot s) = [r_n \cdot s_n] = [r_n] \cdot [s_n] = \varphi(r) \cdot \varphi(s).$$

■

Como vimos no Teorema 5.1, a aplicação $\varphi : \mathbb{Q} \to \mathbb{R}$ é um monomorfismo. Assim, $\mathbb{Q}$ é isomorfo ao subanel $\varphi(\mathbb{Q})$ de $\mathbb{R}$. Como $\mathbb{Q}$ é corpo, segue-se que $\varphi(\mathbb{Q})$ também é corpo. Temos, portanto, o seguinte resultado:

Corolário 5.1. *O corpo* $(\mathbb{Q}, +, \times)$ *é isomorfo a um subcorpo de* $(\mathbb{R}, +, \times)$.

Observemos que, em virtude deste corolário, $\mathbb{Q}$ pode ser identificado com $\varphi(\mathbb{Q})$, i.e., cada elemento r de $\mathbb{Q}$ pode ser identificado com $\varphi(r)$, i.e., com o número real $[r] = r$.

Proposição 5.7. *Um número real é racional se e só se é gerado por uma sucessão* $(x_n)_n$ *convergente em* $\mathbb{Q}$.

Demonstração. Seja $(x_n)_n$ uma sucessão de números racionais convergente em $\mathbb{Q}$, i.e., $(x_n)_n \to r$, onde r é a sucessão constante de termos iguais a r. Reciprocamente, se $[x_n] = [r]$, então $(x_n)_n - r \to 0$ e, portanto, $(x_n)_n \to r$.

■

Definição 5.5. *Um número real diz-se um número irracional se não é racional.*

A proposição seguinte é consequência imediata da proposição 5.7.

Proposição 5.8. *Um número real é irracional se e só se é definido por uma sucessão de Cauchy de números racionais que não converge em* $\mathbb{Q}$.

Observação: Observemos que o exemplo 5.1 nos permite concluir que $\mathbb{R} \backslash \mathbb{Q} \neq \emptyset$.

5.3 Uma ordenação de $\mathbb{R}$

Como vimos no capítulo 4, o corpo dos racionais é um corpo ordenado. Nesta secção mostramos que é possível estender esta ordem total a $\mathbb{R}$ de modo que $(\mathbb{R},+,\times,\leq)$ seja também um corpo ordenado.

Proposição 5.9. *Seja $x \neq 0$ um número real. Verifica-se uma e uma só das seguintes condições:*

1. *existe uma sucessão geradora de x que tem, a partir de certa ordem, todos os termos positivos;*

2. *existe uma sucessão geradora de x que tem, a partir de certa ordem, todos os termos negativos.*

Demonstração. Sejam $x \in \mathbb{R}\{0\}$ e $(x_n)_n$ uma sucessão de Cauchy de números racionais que define x. Então existe ε racional positivo e, um inteiro p tais que $|x_n| > \varepsilon$ para qualquer ordem $n \geq p$. Supondo que $|x_m - x_n| < \varepsilon$ para $m,n \geq p$, todos os termos de $(x_n)_n$ a partir da ordem p são do mesmo sinal. De facto, se existissem $m,n \geq p$ tais que $x_m > 0$ e $x_n < 0$ teriamos $x_m > \varepsilon$ e $x_n < -\varepsilon$, i.e., $x_m - x_n > 2\varepsilon$ o que é, absurdo pois $|x_m - x_n| < \varepsilon$.

Se duas sucessões, $(x_n)_n$ e $(y_n)_n$, definem o mesmo número x, $(x_n)_n$ e $(y_n)_n$, têm que ser do mesmo sinal a partir de certa ordem, pois a sucessão $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$ define x.

■

Se o número real $x \neq 0$ satisfaz 1. [respetivamente 2.], então qualquer outra sucessão que define x tem os termos positivos [respetivamente, negativos], a partir de certa ordem.

Designamos por $\mathbb{R}^+$ o subconjunto de $\mathbb{R}$ formado pelos números reais diferentes de zero que verificam (1) e por $\mathbb{R}^-$ os números $x \in \mathbb{R}\setminus\{0\}$ que verificam (2). Chamamos aos primeiros *números reais positivos* e aos segundos *números reais negativos*.

Os conceitos de número real positivo e de número real negativo permitem definir em $\mathbb{R}$ uma relação de ordem total.

Definição 5.6. *Sejam $r,s \in \mathbb{R}$, diz-se que r é menor que s e escreve-se $r < s$ se e só se $s - r \in \mathbb{R}^+$, i.e., se e só se r e s são definidos por sucessões de números racionais, $(r_n)_n$ e $(s_n)_n$, respetivamente, tais que $(s_n - r_n)_n$ não tende para zero e, a partir de certa ordem, $r_n <_{\mathbb{Q}} s_n$.*

Definição 5.7. *Em* $\mathbb{R}$ *definimos a seguinte relação binária:*

$$\forall x,y \in \mathbb{R},\ x \leq y \Leftrightarrow x = y \text{ ou } x < y.$$

A próxima proposição estabelece que a relação $\leq$ é uma ordem total e que $(\mathbb{R},+,\times,\leq)$ é um corpo ordenado.

Proposição 5.10. $(\mathbb{R},+,\times,\leq)$ *é um corpo ordenado.*

Demonstração. Pela Proposição 5.6 $(\mathbb{R},+,\times)$ é um corpo. Tendo em conta a Proposição 1.3 e o Corolário 1.2, temos agora de provar que:

1) $\mathbb{R}^+$ é fechado para a adição e para a multiplicação;

2) $\mathbb{R} = \mathbb{R}^+ \dot{\cup} \{0\} \dot{\cup} \mathbb{R}^-$.

Vejamos que $\mathbb{R}^+$ é fechado para a adição e para a multiplicação. Sejam $x,y \in \mathbb{R}^+$ tais que $x = [x_n]$ e $y = [y_n]$. Como, a partir de certa ordem p, $x_n > 0$ e $y_n > 0$, também se tem, a partir da ordem p, $x_n + y_n > 0$ e, como $x_n + y_n$ não tende para zero ($x_n + y_n > x_n$, para $n \geq p$), segue-se que $x + y \in \mathbb{R}^+$. Analogamente, a partir da ordem p, também se tem $x_n\, y_n > 0$ e, como $x_n\, y_n$ não tende para zero, $x\, y \in \mathbb{R}^+$.

Falta mostrar que $\mathbb{R} = \mathbb{R}^+ \dot{\cup} \{0\} \dot{\cup} \mathbb{R}^-$. Seja $x = [x_n] \in \mathbb{R} \setminus \{0\}$. Pela Proposição 5.9, existe p tal que $x_n > 0$, para $n \geq p$, ou existe q tal que $x_n < 0$, para $n \geq q$. No primeiro caso, $x \in \mathbb{R}^+$ e, no segundo caso, $-x \in \mathbb{R}^+$. Para além disso, obtemos, também da Proposição 5.9, $\mathbb{R}^+ \cap \mathbb{R}^- = \emptyset$.

■

Proposição 5.11. *A ordem* $\leq$ *de* $\mathbb{R}$ *estende a ordem* $\leq$ *de* $\mathbb{Q}$ *, i.e.,* $(\leq_{\mathbb{R}})\,|_{\mathbb{Q}} = \leq_{\mathbb{Q}}$.

Demonstração. Observamos que, para cada $x \in \mathbb{Q}$, se tem $x > 0$ em $\mathbb{Q}$ se e só se $x > 0$ em $\mathbb{R}$, pois x é definido, como número real, por uma sucessão de termos constantes e iguais a x. Assim, dados $x,y \in \mathbb{Q}$, tem-se

$$x \leq_{\mathbb{R}} y \Leftrightarrow 0 \leq_{\mathbb{R}} y - x \Leftrightarrow 0 \leq_{\mathbb{Q}} y - x \Leftrightarrow x \leq_{\mathbb{Q}} y.$$

■

Proposição 5.12. *O corpo* $(\mathbb{R},+,\times,\leq)$ *é arquimediano.*

Demonstração. Sejam $a=[a_n]$, $b=[b_n]\in\mathbb{R}^+$ tais que $a<b$. Pretendemos mostrar que existe $p\in\mathbb{Z}$ tal que $b<pa$. Por um lado, como a_n não converge para 0, temos que, a partir de certa ordem, $h<a_n$, para certo $h\in\mathbb{Q}^+$ e, portanto, $h\leq a$. Por outro lado, como b_n é uma sucessão de Cauchy, b_n é majorada por um determinado racional k, pelo que, a partir de certa ordem, $b\leq k$ e, portanto, de $h<a<b$ obtemos $h<k$. Como $\mathbb{Q}$ é arquimediano (Proposição 4.10), existe $p\in\mathbb{Z}$ tal que $h<ph$. Assim, dado que $\mathbb{R}$ é um anel ordenado, obtemos

$$b\leq k<ph\leq pa$$

e, portanto, $pa>b$.

■

Proposição 5.13. $(\forall a,b\in\mathbb{R}:\ a<b)\ \exists\, c\in\mathbb{Q};\ a<c<b$.

Demonstração. Sejam $a,b\in\mathbb{R}$ tais que $a<b$. Então a sucessão $((b_n-a_n)/2)_n$, geradora do número real $(b-a)/2$, não tende para zero. Como vimos na demonstração da Proposição 5.12, existe um número racional positivo h tal que $h\leq(b-a)/2$. Logo, $h<b$ e, como $\mathbb{R}$ é arquimediano, existe $t\in\mathbb{Z}$ tal que $b<th$. De $a<b$, obtemos $th>a$, pelo que, de $a<b$ obtemos $a<th$. Consideremos agora a sucessão cujos termos são os múltiplo de h: $0,\ \pm h,\pm 2h,\cdots,\pm nh,\cdots$. Como vimos acima, $a<th$, para certo $t\in\mathbb{Z}$, logo existem termos desta sucessão que são maiores do que a. O facto de $\mathbb{N}$ ser bem ordenado, permite-nos fixar o mínimo do conjunto $\{k\in\mathbb{N}:a<kh\}$. Sejam p esse mínimo e $c=ph$.Temos, então,

$$c=(p-1)\,h+h\leq a+(1/2)(b-a)<a+(b-a)=b$$

e, portanto, $a<c<b$.

■

Observação: A Proposição 5.13 afirma que, para quaisquer números reais a,b tais que $a<b$, o intervalo $]a,b[$ de $\mathbb{R}$ contém uma infinidade de números racionais. Exprime-se esta propriedade

dizendo que $\mathbb{Q}$ *é denso em* $\mathbb{R}$. Prova-se, de modo análogo, que o conjunto $\mathbb{R} \setminus \mathbb{Q}$ é igualmente denso em $\mathbb{R}$, i.e., que, entre dois números reais quaisquer, existe sempre um número irracional.

5.4 Convergência das sucessões de Cauchy

Já vimos que $\mathbb{R}$ é um corpo ordenado que é uma extensão do corpo ordenado dos números racionais. Nesta secção mostramos que com o corpo dos números reais atingimos o objetivo apresentado no início do capítulo: o de construir um corpo, extensão de $\mathbb{Q}$, no qual toda a sucessão de Cauchy converge. Começamos com o seguinte resultado:

Proposição 5.14. *Uma sucessão de números racionais* $(x_n)_n$ *converge para* $a \in \mathbb{Q}$ *em* $\mathbb{Q}$ *se e só se* $(x_n)_n$ *converge para* a *em* $\mathbb{R}$.

Demonstração. Seja $(x_n)_n$ uma sucessão de números racionais, convergente em $\mathbb{Q}$ para $a \in \mathbb{Q}$. Mostremos que $(x_n)_n \to a$ em $\mathbb{R}$. Seja $\varepsilon > 0$ um número real. Pela Proposição 5.13, existe um número $r \in \mathbb{Q}^+$ tal que $r < \varepsilon$; como $(x_n)_n$ converge para $a \in \mathbb{Q}$ em $\mathbb{Q}$, temos que, a partir de certa ordem, $|x_n - a| < r$. Assim, $|x_n - a| < \varepsilon$ e, portanto, $(x_n)_n$ converge para a em $\mathbb{R}$.

Reciprocamente, suponhamos que $(x_n) \to a$ em $\mathbb{R}$ e seja $\delta \in \mathbb{Q}^+$. Então, $\delta \in \mathbb{R}^+$ e, como $(x_n)_n$ converge para a em $\mathbb{R}$, temos que, a partir de certa ordem, $|x_n - a| < \delta$. Portanto, $(x_n)_n \to a$ em $\mathbb{Q}$.

■

De novo com base na Proposição 5.13, prova-se, de modo análogo, a seguinte proposição:

Proposição 5.15. *Uma sucessão* $(x_n)_n$ *de números racionais é sucessão de Cauchy em* $\mathbb{Q}$ *se e só se* $(x_n)_n$ *é sucessão de Cauchy em* $\mathbb{R}$.

Proposição 5.16. *Toda a sucessão de Cauchy* $(x_n)_n$ *de números racionais converge em* $\mathbb{R}$ *para o número real que define, i.e.,* $x_n \to [x_n]$.

Demonstração. Seja $(x_n)_n$ uma sucessão de Cauchy e x o número real por ela definido. Queremos mostrar que

$$\forall \varepsilon \in \mathbb{R}^+,\ \exists p \in \mathbb{N} :\ \forall k \geq p,\ \ |x_k - x| < \varepsilon.$$

Seja $\varepsilon \in \mathbb{R}^+$ e seja $r \in \mathbb{Q}^+$ tal que $r < \varepsilon$ (a existência deste racional é garantida pela Proposição 5.13). Uma vez que $(x_n)_n$ é uma sucessão de Cauchy, existe $p \in \mathbb{N}$ tal que, para quaisquer, $n,k \geq p$, $|x_n - x_k| < r$, i.e., $x_n - r < x_k < x_n + r$. Então, para cada $k \geq p$, temos $[x_n - r]_n \leq [x_k]_n \leq [x_n + r]_n$, e, como r e x_k são números racionais, obtemos $x - r \leq x_k \leq x + r$, i.e., $| x_k - x | < \varepsilon$.

■

Proposição 5.17. *Toda a sucessão de Cauchy de números reais é convergente em* $\mathbb{R}$.

Demonstração.
Seja $(x_n)_n$ uma sucessão de Cauchy de números reais. Para cada $n \geq 1$, os números reais x_n e $x_n + 1/n$ são tais que $x_n < x_n + 1/n$. Então, existe $c \in \mathbb{Q}$ tal que $x_n < c < x_n + 1/n$ (Proposição 5.13). Para cada $n \geq 1$, seja então y_n um número racional tal que

$$x_n < y_n < x_n + 1/n.$$

Cálculos simples mostram que a sucessão $(y_n)_n$ é uma sucessão de Cauchy. Pela Proposição 5.16, $(y_n)_n$ converge em $\mathbb{R}$ para um número real x. Então, como $(x_n)_n = (y_n)_n + ((x_n)_n - (y_n)_n)$ e $(x_n)_n - (y_n)_n \to 0$, segue-se que $(x_n)_n = (y_n)_n$ e, portanto, $(x_n)_n \to x$.

■

Como consequência imediata das proposições 5.4, 5.10 e 5.17, temos o seguinte corolário:

Corolário 5.2. *É condição necessária e suficiente para que uma sucessão de números reais seja convergente, que ela seja uma sucessão de Cauchy.*

O corolário 5.2 é conhecido com o nome de *Princípio de Cauchy-Bolzano* e pode ser enunciado do seguinte modo:

Princípio de Cauchy-Bolzano. É condição necessária e suficiente para que uma sucessão, $(x_n)_n$, de números reais tenha limite finito que, para qualquer número real $\varepsilon > 0$, exista um inteiro p tal que $|x_{n+k} - x_n| < \varepsilon$, para qualquer $n \geq p$ e qualquer $k > 0$.

Bibliografia

[1] Monteiro, António J. & Matos, Isabel Teixeira, *Álgebra um primeiro curso,* Escolar Editora, 2001

[2] Guerreiro, SantosJ., *Curso de Matemáticas Gerais,* Volumes I e II, Escolar Editora, 1973