# MAT01207 : Introdução aos Números Racionais

# Conteúdo

CAPíTULO 1

# Introdução

Os **números naturais**

$$1, 2, 3, 4, \cdots$$

surgiram para *contar* e *ordenar*:

- "há 5 laranjas na mesa"
- "o Rio de Janeiro é a segunda cidade mais populosa do país".

Foi também com números naturais que surgiu a *aritmética* — ou seja, o estudo das operações de adição e multiplicação:

- "se às 5 laranjas sobre a mesa eu acrescento 3, haverá 8 laranjas ao todo" $(8 = 5 + 3)$
- "se cada um dos 3 convidados trouxer 5 laranjas, teremos ao todo 15 laranjas" $(15 = 5 \cdot 3)$

Para estudar os números naturais, vamos agrupá-los em um *conjunto*

$$\mathbb{N} = \{1, 2, 3, \cdots\} = \text{todos os números naturais},$$

caracterizado abstratamente pelos *Axiomas de Peano*, e vamos interpretar adição e multiplicação como *funções*

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad \cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}.$$

Há também uma *ordem* $\leqslant$, em que $m \leqslant n$ indica que "$m$ não é maior que $n$", e que interpretamos como uma *relação* $\mathbb{O}_{\mathbb{N}}$ em $\mathbb{N}$.

Em números naturais, equações da forma

$$x + n = m$$

não têm solução $x \in \mathbb{N}$ se $m \leqslant n$, o que nos leva a discutir os **números inteiros** $\mathbb{Z}$, em que acrescentamos a $\mathbb{N}$ as soluções de equações dessa forma:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

As operações $+$ e $\cdot$ em $\mathbb{N}$ estendem a $\mathbb{Z}$ de maneira natural, e o tornam um *anel comutativo ordenado*. Em $\mathbb{Z}$, uma equação da forma

$$nx = m, \quad n \neq 0,$$

só tem solução inteira $x \in \mathbb{Z}$ se $m$ é divisível por $n$. Vamos então construir os **números racionais** $\mathbb{Q}$ acrescentando a $\mathbb{Z}$ as soluções

$$x = \frac{m}{n}$$

de *todas* equações dessa forma. Aqui, a notação $\frac{m}{n}$ deve ser lida "a solução (formal) $x$ de $nx = m$". Note que as equações

$$nx = m, \quad 2nx = 2m, \quad 3nx = 3m, \quad \cdots \quad (n \neq 0)$$

devem ter as mesmas soluções (formais):

$$\frac{m}{n} = \frac{2m}{2n} = \frac{3m}{3n} = \cdots$$

o que nos leva a construir $\mathbb{Q}$ como o conjunto de equações $nx = m$, onde duas equações seram identificadas ("vistas como a mesma") se suas soluções coincidem. Veremos então que isso torna $\mathbb{Q}$ um *corpo*, isto é, um anel comutativo em que todo elemento não-nulo tem inversa multiplicativa.

CAPíTULO 2

# Conjuntos

Um **conjunto** $X$ é uma coleção dos seus **elementos/membros**. A notação

$$x \in X \tag{1}$$

sinifica '$x$ é elemento do conjunto $X$', ou '$x$ pertence a $X$'.

EXEMPLO 1. *O* **conjunto vazio** $\varnothing$ *é o conjunto sem nenhum elemento.*

EXEMPLO 2. *O conjunto* $X = \{a, \spadesuit, \square\}$ *contém exatamente três elementos:* $a$, $\spadesuit$, *e* $\square$.

Dizemos que um conjunto $Y$ é **subconjunto** de $X$ se cada elemento $y$ que pertence a $Y$ pertence também a $X$. Nesse caso, escrevemos

$$Y \subset X \tag{2}$$

para denotar '$Y$ é subconjunto de $X$'.

EXEMPLO 3. *O conjunto vazio* $\varnothing$ *é subconjunto de qualquer conjunto* $X$.[1]

EXEMPLO 4. *O conjunto* $X = \{a, \spadesuit, \square\}$ *tem exatamente 8 subconjuntos distintos:*

$$X = \{a, \spadesuit, \square\}, \quad \{\spadesuit, \square\}, \quad \{a, \square\}, \quad \{a, \spadesuit\}, \quad \{\square\}, \quad \{\spadesuit\}, \quad \{a\}, \quad \varnothing = \{\}.$$

Uma maneira de descrever um conjunto $X$ é listar todos os seus elementos. Porém esse método é muito pouco eficiente (e só tem esperança no caso de conjuntos *finitos*)... Por exemplo, o conjunto $X$ de todas as pessoas vivas neste instante teria pelo menos 7 bilhões de entradas...

Podemos no entanto definir um conjunto $X$ pela propriedade[2] de que ele contém exatamente todas as pessoas vivas às 12.39 do dia 09/08/2018. Note que um mesmo conjunto pode ser descrito por propriedades diferentes; por exemplo, o conjunto de todas as pessoas que são seus próprios pais é o mesmo conjunto das pessoas que flutuam, e o mesmo conjunto dos hamsters que receberam o Prêmio Nobel da Paz: o conjunto vazio $\varnothing$.

Abstratamente, podemos pensar que *todo* conjunto $X$ é descrito por uma propriedade – por exemplo, a propriedade $\mathfrak{P}(X)$ de pertencer a $X$! Na linguagem de propriedades, dizemos que uma propriedade $\mathfrak{P}$ **implica** uma propriedade $\mathfrak{Q}$ exatamente quando o conjunto definido por $\mathfrak{P}$ é subconjunto do conjunto definido por $\mathfrak{Q}$, e nesse caso escrevemos

$$\mathfrak{P} \Longrightarrow \mathfrak{Q}. \tag{3}$$

---

[1] Demonstração: como não há nenhum $x \in \varnothing$, a frase 'todo $x \in \varnothing$ pertence tambem a $X$' é trivialmente válida para cada conjunto $X$.

[2] *Propriedade* tem aqui o seguinte sentido: se fixarmos um conjunto $U$ (um *universo*), uma propriedade $\mathfrak{P}$ é uma afirmação sobre os elementos $x \in U$, que é ou verdadeira ou falsa para cada elemento. Dizer que $\mathfrak{P}$ descreve $X \subset U$ significa que

$$X = \{x \in U \mid \mathfrak{P}(x) \text{ é verdade.}\}$$

EXEMPLO 5. *Seja $X$ o conjunto de dias em 2017 Diga que $\mathfrak{P}(x)$ é verdade se choveu no dia $x \in X$, e que $\mathfrak{Q}(x)$ é verdade se eu saí de guarda-chuva nesse dia. Então a frase 'em dias de chuva eu saí de guarda-chuvas' se traduz por $\mathfrak{P} \Rightarrow \mathfrak{Q}$.*

EXERCÍCIO 1. *Para uma propriedade $\mathfrak{P}$, definamos sua* **negação** *$\neg\mathfrak{P}$ por*

$$\neg\mathfrak{P}(x) \quad \textit{verdade se e só se} \quad \mathfrak{P}(x) \quad \textit{é falsa.}$$

*Mostre que, para propriedades $\mathfrak{P}, \mathfrak{Q}$, dizer que $\mathfrak{P} \Rightarrow \mathfrak{Q}$ é o mesmo que dizer que $\neg\mathfrak{Q} \Rightarrow \neg\mathfrak{P}$.*

EXERCÍCIO 2. *Diga que $\mathfrak{P} \Leftrightarrow \mathfrak{Q}$ (lê-se $\mathfrak{P}$* **se e só se** *$\mathfrak{Q}$', ou $\mathfrak{P}$ exatamente quando $\mathfrak{Q}$') se $\mathfrak{P} \Rightarrow \mathfrak{Q}$ e $\mathfrak{Q} \Rightarrow \mathfrak{P}$. Mostre que vale $\mathfrak{P} \Leftrightarrow \mathfrak{Q}$ exatamente quando vale $\neg\mathfrak{P} \Leftrightarrow \neg\mathfrak{Q}$.*

CAPíTULO 3

# Números Naturais

O conjunto dos **número naturais** é

$$\mathbb{N} = \{1, 2, 3, ...\}$$

Para o caracterizar abstratamente, temos os seguintes **axiomas de Peano**:

P1) 1 é um número natural;
P2) Todo número natural $n$ tem um *sucessor* $n + 1$;
P3) 1 não é o sucessor de nenhum número natural;
P4) Dois números naturais coincidem se seus sucessores coincidem;
P5) Se um subconjunto $X \subset \mathbb{N}$ contém 1, e contém também o sucessor $n + 1$ de todo número natural $n \in X$, então $X = \mathbb{N}$.

Esse conjunto de axiomas descreve precisamente o que sugerem as reticências em $\mathbb{N} = \{1, 2, 3, ...\}$: existe um primeiro elemento 1 em $\mathbb{N}$, todo elemento tem um sucessor único, e o único subconjunto que contém 1 e o sucessor de todo número nele é o próprio conjunto de todos os números naturais.

## 1. Divisibilidade

Definição 3. *Se $n, m \in \mathbb{N}$, dizemos que $n$* **divide** *$m$, ou que $m$ é* **múltiplo** *de $n$, se existe $q \in \mathbb{N}$ tal que $m = nq$.*

Exemplo 6. *Considere $n \in \mathbb{N}$. O subconjunto de $\mathbb{N}$ de múltiplos de $n$ é*

$$n\mathbb{N} = \{nm \mid m \in \mathbb{N}\} = \{n, 2n, 3n, \cdots\}$$

*Portanto:*

$$n \text{ divide } m \in \mathbb{N} \iff m \in n\mathbb{N} \iff m\mathbb{N} \subset n\mathbb{N}.$$

## 2. Ordem

Definição 4. *Dizemos que $n \leqslant m$, "n não ultrapassa m", se alguma das condições a seguir é satisfeita:*

- *$m = n$, ou*
- *a equação $x + n = m$ tem solução $x \in \mathbb{N}$.*

Exemplo 7. *$13 \leqslant 17$, pois $x + 13 = 17$ tem solução $x = 4 \in \mathbb{N}$.*

Note também que:

$$n|m \implies n \leqslant m.$$

## 3. Pares e ímpares

Definição 5. *Se 2 divide $m$, dizemos que $m$ é* **par***; caso contrário, dizemos que $m$ é* **ímpar***.*

Note que $n \in \mathbb{N}$ é ímpar se e só se seu sucessor é par; portanto

- $n$ é par se e só se existe $m \in \mathbb{N}$ tal que $n = 2m$;
- $n$ é ímpar se e só se existe $m \in \mathbb{N}$ tal que $n = 2m - 1$.

## 4. MMC e MDC

DEFINIÇÃO 6. *Se $n, m \in \mathbb{N}$, dizemos que $q \in \mathbb{N}$ é o* **MMC (menor múltiplo comum)** *$q = \text{mmc}(n, m)$ de $n$ e de $m$ se:*
*MMC1) $q$ é múltiplo de $n$ e de $m$;*
*MMC2) se $q' \in \mathbb{N}$ é múltiplo de $n$ e de $m$;, então $q'$ é múltiplo de $q$.*

EXEMPLO 8. *Considere $n = 6$ e $m = 9$. Então*

$$6\mathbb{N} = \{6, 12, 18, \cdots\}, \quad 9\mathbb{N} = \{9, 18, 27, \cdots\}.$$

*Portanto o subconjunto de números naturais que são simultaneamente múltiplos de 6 e de 9 é*

$$\{18, 36, 54, \cdots\},$$

*cujo elemento mínimo é $18 = \text{mmc}(6, 9)$.*

DEFINIÇÃO 7. *Se $n, m \in \mathbb{N}$, dizemos que $q \in \mathbb{N}$ é o* **MDC (maior divisor comum)** *$q = \text{mdc}(n, m)$ de $n$ e $m$ se:*
*MDC1) $q$ divide $n$ e $m$ (cotaç ao: $n|m$);*
*MDC2) se $q' \in \mathbb{N}$ divide $n$ e $m$, então $q'$ divide $q$.*

EXEMPLO 9. *Considere $n = 6$ e $m = 9$. Então o subconjunto dos números que dividem 6 é $\{1, 2, 3, 6\}$, e o subconjunto dos números que dividem 9 é $\{1, 3, 9\}$. Portanto o subconjunto de números naturais que simultaneamente dividem 6 e 9 é $\{1, 3\}$, cujo elemento máximo é $3 = \text{mdc}(6, 9)$.*

## 5. Primos

DEFINIÇÃO 8. *Um número natural $p \in \mathbb{N}$ é* **primo** *se:*
*Pr1) $p > 1$;*
*Pr2) $p$ só é divisível por 1 e por $p$.*

Observe que, como $n|p$ implica $n \leqslant p$, para verificar se $p$ é primo, é suficiente verificar que 1 é o único divisor de $p$ dentre $\{1, 2, ..., p - 1\}$.

EXEMPLO 10. *$p = 5$ é primo, pois*

$$5 \notin 2\mathbb{N} = \{2, 4, 6, \cdots\}, \quad 5 \notin 3\mathbb{N} = \{3, 6, 9, \cdots\}, \quad 5 \notin 4\mathbb{N} = \{4, 8, 12, \cdots\}.$$

## 6. Cardinalidade

DEFINIÇÃO 9. *Dizemos que um conjunto $X$ é* **finito** *se existe $n \in \mathbb{N}$ tal que $X$ tem tantos elementos quanto o conjunto $\{1, 2, 3, ..., n\}$. Nesse caso, dizemos que $X$ tem* **cardinalidade** *$n$, o que denotamos por $|X| = n$. Se $X$ não é finito, dizemos que $X$ é* **infinito**.

EXEMPLO 11. *Se $X = \{a, \spadesuit, \square\}$, então $|X| = 3$.*

## 7. Propriedades da soma e da multiplicação em $\mathbb{N}$

Recorde também que a soma e a multiplicação de números naturais têm as seguintes propriedades:

**Associatividade da soma:** Para todos $l, n, m \in \mathbb{N}$, temos que

$$(l + m) + n = l + (m + n);$$

**Comutatividade da soma:** Para todos $m, n \in \mathbb{N}$, temos que

$$m + n = n + m;$$

**Elemento neutro da multiplicação:** Para todo $n \in \mathbb{N}$, temos que

$$n = n \cdot 1;$$

**Associatividade da multiplicação:** Para todos $l, m, n \in \mathbb{N}$, temos que

$$(l \cdot m) \cdot n = l \cdot (m \cdot n);$$

**Comutatividade da multiplicação:** Para todos $m, n \in \mathbb{N}$, temos que

$$m \cdot n = n \cdot m;$$

**Distributividade:** Para todos $l, m, n \in \mathbb{N}$, temos que

$$(l + m) \cdot n = l \cdot n + m \cdot n.$$

CAPíTULO 4

# Métodos de provas

Uma *prova* é uma argumentação que convence as pessoas de que uma afirmação matemática é válida. Provas têm um vocabulário próprio — onde usamos palavras como 'e', 'ou', 'não', 'se... então', 'se e só se', 'existe', 'para todo' etc. — e uma gramática, em que, por exemplo, nega-se 'todo homem é mortal' com 'existe um homem que não é mortal'.

## 1. Direta

O método consiste em justapôr as hipóteses para derivar a tese através de silogismos. Por exemplo:

PROPOSIÇÃO 10. *Se $p, q, r \in \mathbb{N}$ são tais que $p + q = r$, então $r$ é divisível por $n$ se $p$ e $q$ são divisíveis por $n$.*

DEMONSTRAÇÃO. As hipóteses são:

H1) $n$, $p$, $q$ e $r$ são números naturais;
H2) $r$ é a soma de $p$ e $q$;
H3) $n$ divide $p$;
H4) $n$ divide $q$.

Nossa tese é:

T) $n$ divide $r$.

A hipótese H3 diz que existe $a \in \mathbb{N}$ tal que $p = an$. A hipótese H4, por outro lado, diz que existe $b \in \mathbb{N}$ tal que $q = bn$. Finalmente, H2 diz que $r = p + q$. Portanto

$$r \overset{H2}{=} p + q \overset{H3,H4}{=} an + bn = (a + b)n$$

mostra que $r$ é múltiplo de $n$, onde na última igualdade usamos a propriedade a Distributividade da soma sobre a multiplicação. □

Ainda outro exemplo:

PROPOSIÇÃO 11. *Se $n \in \mathbb{N}$ é ímpar, então $n^2$ é ímpar.*

DEMONSTRAÇÃO. As hipóteses são:

H1) $n$ é um número natural;
H2) $n = 2m - 1$ para algum $m \in \mathbb{N}$.

Nossa tese é:

T) $n^2 = 2M - 1$ para algum $m \in \mathbb{N}$.

Ora,

$$n^2 \overset{H2}{=} (2m - 1)^2 = 4m^2 - 4m + 1 = 2(2m^2 - 2m + 1) - 1.$$

Portanto basta mostrar que

$$M = 2m^2 - 2m + 1$$

é natural, e isso é verdade porque

$$M = 2m^2 - 2m + 1 = 2m(2m - 1) + 1 = 2mn + 1 \in \mathbb{N}.$$

□

## 2. Indução

A técnica de indução serve para demonstrar afirmações sobre os números naturais. Recorde que os axiomas de Peano dizem que se um subconjunto $X \subset \mathbb{N}$ satisfaz:

(1) $1 \in X$;
(2) Se $n \in X$, então seu sucessor $n+1$ também está em $X$,

então $X = \mathbb{N}$. Assim, para demonstrar que $X = \mathbb{N}$, basta mostrar que:

(1) $1 \in X$ ("passo inicial") e que
(2) $n+1$ está em $X$ se $n$ está em $X$ ("passo indutivo").

PROPOSIÇÃO 12. *Para todo $n \geqslant 0$, temos que $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.*

DEMONSTRAÇÃO. Seja $X \subset \mathbb{N}$ o subconjunto dos $n \in \mathbb{N}$ para os quais a fórmula acima é válida. Então:

(1) $1 \in X$, pois $0 + 1 = \frac{1(1+1)}{2}$;
(2) Se $n \in X$, isto é, se

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$

então

$$\begin{aligned} 0 + 1 + 2 + \cdots + n + (n+1) &= (0 + 1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= \frac{(n+1)(n+2)}{2}, \end{aligned}$$

e portanto $n + 1 \in X$.

Logo $X = \mathbb{N}$ — ou seja, a fórmula da proposição é válida para todo $n \in \mathbb{N}$. □

De maneira análoga:

PROPOSIÇÃO 13. *Para todo $n \geqslant 0$, temos que $1 + 3 + 5 + \cdots + (2n-1) = n^2$.*

DEMONSTRAÇÃO. Seja $X \subset \mathbb{N}$ o subconjunto dos $n \in \mathbb{N}$ para os quais a fórmula acima é válida. Então:

(1) $1 \in X$, pois $1 = 1^2$;
(2) Se $n \in X$, isto é, se

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

então

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n-1) + (2(n+1)-1) &= (1 + 3 + 5 + \cdots + (2n-1)) + (2n+1) \\ &= n^2 + (2n+1) \\ &= (n+1)^2, \end{aligned}$$

e portanto $n + 1 \in X$.

Logo a fórmula da proposição é sempre válida. □

Um exemplo mais complicado:

PROPOSIÇÃO 14. *Todo $n \in \mathbb{N}$, $n > 1$, é produto de primos: $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, onde $k, r_1, ..., r_k \in \mathbb{N}$ e $p_1, p_2, ..., p_k$ são primos.*

DEMONSTRAÇÃO. Considere o conjunto:

$$X \subset \mathbb{N}, \quad X = \{m \mid \text{todo } n \text{ tal que } 1 < n \leqslant m+1 \text{ é produto de primos}\}$$

Então:

(1) $1 \in X$, pois $1 < n \leqslant 2$ sinifica $n = 2$, e 2 é produto de primos:
$$2 = 2^1 \qquad (k = 1, r_1 = 1, p_1 = 2);$$

(2) Se $m \in X$, isto é, se todo $1 < n \leqslant m+1$ é produto de primos, desejamos mostrar que todo número $n'$ tal que $1 < n' \leqslant m+2$ é produto de primos. Ora, o único caso novo a considerar é $n' = m+2$: é ele um produto de primos ? Ora, há dois casos apenas:
   a) $m+2$ é primo, em cujo caso ele é produto de primos:
   $$m+2 = (m+2)^1 \qquad (k = 1, r_1 = 1, p_1 = m+2);$$
   b) $m+2$ não é primo, em cujo caso ele é um produto
   $$m+2 = ab,$$
   onde $a, b \in \mathbb{N}$ são dois números tais que $1 < a \leqslant m+1$ e $1 < b \leqslant m+1$. Portanto $a$ e $b$ são produtos de primos pela hipótese indutiva $m \in X$:
   $$a = q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l}, \qquad b = (q'_1)^{s'_1} (q'_2)^{s'_2} \cdots (q'_{k'})^{s'_{k'}}$$
   e portanto também é $m = ab$:
   $$m = q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l} (q'_1)^{s'_1} (q'_2)^{s'_2} \cdots (q'_{k'})^{s'_{k'}}.$$
   Portanto $m+1 \in X$.

Logo $X = \mathbb{N}$ — isto é, todo natural $n > 1$ é produto de primos. □

## 3. Contradição (Reductio ad absurdum)

Numa demonstração por contradição, nós supomos ser falsa a tese a ser demonstrada, e através de silogismos, chegamos a uma contradição. Por exemplo:

PROPOSIÇÃO 15. *Se $n^2 \in \mathbb{N}$ é par, então $n$ é par.*

DEMONSTRAÇÃO. Suponhamos que a tese seja *falsa*. Então deveria existir $n$ ímpar, tal que $n^2$ é par. Mas como vimos no exemplo anterior, se $n$ for ímpar, então $n^2$ também é ímpar. □

Um exemplo mais razoável é o que segue:

PROPOSIÇÃO 16. *Existem infinitos números primos.*

DEMONSTRAÇÃO. Suponhamos que a tese seja *falsa*. Então o subconjunto

$$P \subset \mathbb{N}, \quad P = \{p \in \mathbb{N} \mid p \text{ é primo}\}$$

de todos os números primos deve ser finito:

$$P = \{p_1 = 2, p_2 = 3, \cdots, p_r\},$$

onde $r \in \mathbb{N}$. Defina $q \in \mathbb{N}$ por:

$$q := p_1 p_2 p_3 \cdots p_r + 1,$$

e note que, como $p_i < q$, segue que

$$(*) \qquad q \notin P.$$

Note também que nenhum primo $p_i$ divide $q$, pois $p_i$ divide $p_1 p_2 p_3 \cdots p_r$ mas não divide 1. Como $q$ é produto de primos pela Proposição 14, segue que $q$ ele mesmo deve ser primo:

$$(**) \qquad q \in P.$$

Ou seja: ao supôr que havia um número *finito* de primos, fomos levados a concluir que há $q \in \mathbb{N}$, $q > 1$, que ao mesmo tempo é e não é primo — um absurdo ! Portanto há infinitos primos. □

CAPíTULO 5

# Operações com conjuntos

## 1. União

Dados conjuntos $X$ e $Y$, defina a **união**

$$X \cup Y = \{x \mid x \in X \text{ ou } x \in Y\}. \tag{4}$$

Ou seja, um elemento é membro de $X \cup Y$ se for membro de $X$ ou de $Y$.

Exercício 17. *Mostre que, para quaisquer três conjuntos $X, Y, Z$, temos que*

$$(X \cup Y) \cup Z = X \cup (Y \cup Z).$$

Exercício 18. *Seja $\mathcal{X}$ um conjunto de conjuntos. Defina a união $\bigcup_{X \in \mathcal{X}} X$.*

## 2. Intersecção

Dados conjuntos $X$ e $Y$, defina a **intersecção**

$$X \cap Y = \{x \mid x \in X \text{ e } x \in Y\}. \tag{5}$$

Ou seja, um elemento é membro de $X \cap Y$ se for simultaneamente membro de $X$ e de $Y$.

Exercício 19. *Mostre que, para quaisquer três conjuntos $X, Y, Z$, temos que*

*a)* $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
*b)* $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
*c)* $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

Exercício 20. *Mostre que, para quaisquer conjuntos finitos $X, Y$, temos que*

$$|X \cup Y| + |X \cap Y| = |X| + |Y|$$

Exercício 21. *Seja $\mathcal{X}$ um conjunto de conjuntos. Defina a intersecção $\bigcap_{X \in \mathcal{X}} X$.*

## 3. Diferença

Dados conjuntos $X$ e $Y$, defina a **diferença**

$$X \setminus Y = \{x \mid x \in X \text{ e } x \notin Y\}. \tag{6}$$

Ou seja, um elemento é membro de $X \setminus Y$ se for membro de $X$ mas não de $Y$.

Exercício 22. *Mostre que, para quaisquer conjuntos $X, Y, Z$, temos que*

*a)* $(X \cup Y) \setminus Z = (X \setminus Z) \cup (Y \setminus Z)$
*b)* $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$
*c)* $(X \cap Y) \setminus Z = (X \setminus Z) \cap (Y \setminus Z)$
*d)* $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

Exercício 23. *Mostre que, para quaisquer conjuntos finitos $X, Y$, temos que*

$$|X \setminus Y| + |Y \setminus X| + |X \cap Y| = |X \cup Y|$$

## 4. Produto

Dados conjuntos $X$ e $Y$, defina seu **produto (Cartesiano)**

$$X \times Y = \{(x, y) \mid x \in X \text{ e } y \in Y\}. \tag{7}$$

Ou seja, elementos de $X \times Y$ são todos os pares de elementos de $X$ e de $Y$.

Exercício 24. *Mostre que, para quaisquer conjuntos $X, Y, Z$, temos que*

*a)* $(X \times Y) \times Z = X \times (Y \times Z)$
*b)* $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$
*c)* $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$
*d)* $(X \cap Y) \setminus Z = (X \setminus Z) \cap (Y \setminus Z)$
*e)* $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

Exercício 25. *Mostre que, para quaisquer conjuntos finitos $X, Y$, temos que*

$$|X \times Y| = |X||Y|$$

## 5. Partes

Dado um conjunto $X$, defina o conjunto de suas **partes**

$$\mathscr{P}(X) = \{Y \mid Y \subset X\}. \tag{8}$$

Ou seja, elementos de $\mathscr{P}(X)$ são todos os subconjuntos de $X$.

Exemplo 12. *Seja $X$ o conjunto $X = \{a, b, c\}$. Então*

$$\mathscr{P}(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Definição 26. *Uma* **partição** *$P$ de um conjunto $X$ é um subconjunto $P \subset \mathscr{P}(X)$, com a propriedade de que todo $x \in X$ pertence a um, e um único conjunto $Y \in P$.*

Portanto uma partição $P$ de um conjunto $X$ consiste de uma coleção $(X_\alpha)$ de subconjuntos $X_\alpha \subset X$, com as seguintes propriedades:
$P$ 1) $X = \bigcup_{X_\alpha \in P} X_\alpha = \{x \in X \mid x \text{ pertence a algum } X_\alpha\}$;
$P$ 2) $X_\alpha \cap X_\beta = \varnothing$ se $\alpha \neq \beta$.

Exemplo 13. *Seja $X$ o conjunto $X = \{a, b, c\}$. Então*

$$P \subset \mathscr{P}(X), \quad P = \{\{a\}, \{b\}, \{c\}\}$$

*define uma partição:*

$$X = \{a\} \cup \{b\} \cup \{c\}, \quad \varnothing = \{a\} \cap \{b\} = \{b\} \cap \{c\} = \{c\} \cap \{a\}$$

*Chamamos essa de partição* discreta.

Exemplo 14. *Seja $X$ o conjunto $X = \{a, b, c\}$. Então*

$$P \subset \mathscr{P}(X), \quad P = \{\{a, b, c\}\}$$

*define uma partição. Chamamos essa de partição* indiscreta.

Exemplo 15. *Seja $X$ o conjunto $X = \{a, b, c\}$. Então*

$$P \subset \mathscr{P}(X), \quad P = \{\{a, b\}, \{c\}\}$$

*define uma partição:*

$$X = \{a, b\} \cup \{c\}, \quad \varnothing = \{a, b\} \cap \{c\}.$$

Exercício 27. *Seja $X$ um conjunto finito, e defina*

$$\mathscr{P}_k(X) = \{Y \in \mathscr{P}(X) \mid |Y| = k\}.$$

*Então mostre que*

*a)* $\mathscr{P}(X) = \bigcup_k \mathscr{P}_k(X)$*;* *b)* $\mathscr{P}_k(X) \cap \mathscr{P}_l(X) = \begin{cases} \mathscr{P}_k(X) & \text{se } k = l; \\ \varnothing & \text{se } k \neq l. \end{cases}$

*c)* $|\mathscr{P}_k(X)| = \binom{|X|}{k} = \frac{|X|!}{k!(|X|-k)!}$ *d)* $|\mathscr{P}(X)| = \sum_k \binom{|X|}{k} = 2^{|X|}$.

*Conclua que*

$$P \subset \mathscr{P}(\mathscr{P}(X)), \quad P = \{\mathscr{P}_k(X) \mid k \in \mathbb{N}\}$$

*define uma partição do conjunto* $\mathscr{P}(X)$ *de partes de* $X$.

CAPíTULO 6

# Relações

Uma **relação** $R$ de $X$ em $Y$ é um subconjunto $R$ de $X \times Y$.

EXEMPLO 16. *Seja $X$ o conjunto de todas as pessoas vivas em 09/08/2018. Então temos relações $R \subset X \times X$:*

*a)* $R_{\text{pess}} = \{(x, y) \mid x \text{ conhece } y \text{ pessoalmente}\}$
*b)* $R_{\text{par}} = \{(x, y) \mid x \text{ é filho ou filha de } y\}$
*c)* $R_{\text{moth}} = \{(x, y) \mid x \text{ é mãe de } y\}$
*d)* $R_{\text{alt}} = \{(x, y) \mid x \text{ e } y \text{ têm a mesma altura}\}$

EXEMPLO 17. *Seja $\mathbb{N}$ o conjunto de números naturais. Então temos relações $R \subset \mathbb{N} \times \mathbb{N}$:*

*a)* $R_{\leqslant} = \{(x, y) \mid x \text{ é menor ou igual a } y\}$
*b)* $R_{<} = \{(x, y) \mid x \text{ é estritamente menor que } y\}$
*c)* $R_{\text{div}} = \{(x, y) \mid x \text{ divide } y\}$
*d)* $R_{\text{copr}} = \{(x, y) \mid x \text{ e } y \text{ não têm divisores comuns além de } 1\ \}$

### 1. Relações de um conjunto $X$ em si mesmo

Uma relação $R \subset X \times X$ é dita:

**reflexiva:** se $(x, x) \in R$ para cada $x \in X$;
**simétrica:** se $(x, y) \in R$ implica $(y, x) \in R$;
**antisimétrica:** se $(x, y) \in R$ e $(y, x) \in R$ implicam $x = y$;
**transitiva:** se $(x, y) \in R$ e $(y, z) \in R$ implicam $(x, z) \in R$.

EXERCÍCIO 28. *Decida quais das relações listadas acima são reflexivas, (anti)simétricas e transitivas.*

EXEMPLO 18. *O conjunto vazio $\varnothing$ pode ser visto como uma relação $\varnothing \subset X \times X$, para todo conjunto $X$, que chamamos de* **relação vazia** *(de $X$ em $X$). Note que ela:*

- *Se $X \neq \varnothing$, essa relação não é reflexiva, pois então existe $x \in X$ tal que $(x, x) \notin \varnothing$;*
- *Essa relação é sempre simétrica, pois nunca é verdade que $(x, y)$ pertença a $\varnothing$, e portanto*

$$(x, y) \in \varnothing \quad \Longrightarrow \quad (y, x) \in \varnothing$$

  *é trivialmente satisfeita;*
- *Essa relação é sempre transitiva, pois nunca é verdade que $(x, y)$ e $(y, z)$ pertençam a $\varnothing$, e portanto*

$$(x, y), (y, z) \in \varnothing \quad \Longrightarrow \quad (x, z) \in \varnothing$$

  *é trivialmente satisfeita.*

## 2. Saturação de relações de um conjunto $X$ em si mesmo

Cada uma das propriedades de uma relação $R \subset X \times X$:

i) reflexividade
ii) (anti-)simetria
iii) transitividade

é fechada sob intersecções: se $R$ e $R'$ têm alguma dessas propriedades, então também $R \cap R'$ tem essa propriedade.

Proposição 29. *Seja $X$ um conjunto, e seja $S \subset X \times X$ uma relação não-vazia qualquer. Então dentre todas as relações $R$ que contêm $S$, e possuem alguma combinação das seguintes propriedades:*

*a) reflexividade* *b) simetria* *c) transitividade*

*existe uma menor, no sentido de que qualquer relação $R'$ que contêm $S$, e possuem a mesma combinação dessas propriedades contém $R$.*

Demonstração. Seja $\mathfrak{P}$ uma propriedade de relações de $X$ em $X$, que satisfaz às seguintes propriedades:

a) $X \times X$ tem a propriedade $\mathfrak{P}$;
b) Se $(R_\alpha) \subset \mathscr{P}(X \times X)$ é uma coleção de relações de $X$ em $X$ que têm a propriedade $\mathfrak{P}$, então também $\cap_\alpha R_\alpha$ tem a propriedade $\mathfrak{P}$.

Fixe uma relação *qualquer* $S \subset X \times X$, e defina

$$\mathscr{S}_\mathfrak{P} = \{R \in \mathscr{P}(X \times X) \mid S \subset R, \quad R \text{ tem a propriedade } \mathfrak{P}.\}$$

Então $X \times X \in \mathscr{S}_\mathfrak{P}$ por a); em particular, $\mathscr{S}_\mathfrak{P} \neq \varnothing$. Além disso, por b), a intersecção $S_{\text{ref}}$ de todas as relações em $\mathscr{S}_\mathfrak{P}$,

$$S_\mathfrak{P} := \bigcap_{R \in \mathscr{S}_\mathfrak{P}} R,$$

pertence a $\mathscr{S}_\mathfrak{P}$, e é portanto a menor dentre todas as relações em $\mathscr{S}_\mathfrak{P}$ que contém $S$, no sentido que está contida em qualquer outra. Dizemos que $S_\mathfrak{P}$ é a **saturação** de $S$ com respeito à propridade $\mathfrak{P}$.

Note agora que as propriedades abaixo satisfazem às condições a) e b) acima que permitem saturar uma relação arbitrária:

— ser reflexiva;
— ser simétrica;
— ser transitiva;
— ser reflexiva e simétrica;
— ser reflexiva e transitiva;
— ser simétrica e transitiva;
— ser uma equivalência. □

Note que a propriedade de anti-simetria é diferente, pois se $S$ não é anti-simétrica, nenhuma relação que contenha $S$ pode ser anti-simétrica: se $x \neq y$ e tanto $(x, y)$ quanto $(y, x)$ estão em $S$, o mesmo se dá com todo conjunto que contenha $S$. Porém:

Proposição 30. *Seja $X$ um conjunto, e seja $S \subset X \times X$ uma relação não-vazia e anti-simétrica qualquer. Então dentre todas as relações anti-simétricas $R$ que contêm $S$, e possuem alguma combinação das seguintes propriedades:*

*a) reflexividade* *b) transitividade*

*existe uma menor, no sentido de que qualquer relação anti-simétrica $R'$ que contêm $S$ contém também $R$ se $R'$ possui a mesma combinação de propriedades.*

Exercício 31. *Demonstre essa última proposição.*

EXEMPLO 19. *Considere* $X = \{a, b, c, d\}$ *e* $S = \{(a, b), (b, c)\}$. *Então* $S_{\text{ref}} = \{(a, a), (a, b), (b, b), (b, c), (c, c), (d, d)\}$.

EXEMPLO 20. *Considere* $X = \{a, b, c, d\}$ *e* $S = \{(a, b), (b, c), (c, d)\}$. *Então*

$S_{\text{ref}} = \{(a, a), (a, b), (b, b), (b, c), (c, c), (c, d), (d, d)\}$

$S_{\text{sim}} = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c)\}$

$S_{\text{trn}} = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$

$S_{\text{ref,sim}} = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b), (c, c), (c, d), (d, c), (d, d)\}$

$S_{\text{ref,trn}} = \{(a, a), (a, b), (a, c), (a, d), (b, b), (b, c), (b, d), (c, c), (c, d), (d, d)\}$

$S_{\text{sim,trn}} = \{(a, b), (a, c), (a, d), (b, a), (b, c), (b, d), (c, a), (c, b), (c, d), (d, a), (d, b), (d, c)\}$

$S_{\text{ref,sim,trn}} = \{(a, a), (a, b), (a, c), (a, d), (b, a), (b, b), (b, c), (b, d), (c, a), (c, b), (c, c),$
$(c, d), (d, a), (d, b), (d, c), (d, d)\}$

CAPíTULO 7

# Pré-ordem, ordem e boa-ordem

DEFINIÇÃO 32. *Uma* **ordem parcial** *em um conjunto $X$ é uma relação $R$ que é reflexiva, antisimétrica e transitiva.*

Escrevamos $x \leqslant y$ se $(x, y) \in R$. Então as condições na definição de uma ordem parcial se expressam por:

a) $x \leqslant x$;
b) $x \leqslant y$ e $y \leqslant x$ apenas se $x = y$;
c) $x \leqslant y$ e $y \leqslant z$ apenas se $x \leqslant z$.

EXEMPLO 21. *Seja $X$ um conjunto, e defina $R \subset \mathscr{P}(X) \times \mathscr{P}(X)$ como*

$$R = \{(Y, Z) \mid Y \subset Z\}.$$

*Portanto se $Y, Z$ são subconjuntos de $X$, escrevemos $Y \leqslant Z$ se e só se $Y$ está contido em $Z$. Verifique que essa é uma ordem parcial.*

EXERCÍCIO 33. *Seja $X$ um conjunto munido de uma ordem parcial $R \subset X \times X$, e seja $Y \subset X$ um subconjunto. Mostre que*

$$R_Y \subset Y \times Y, \quad R_Y = \{(x, y) \mid (x, y) \in R\}$$

*é uma ordem parcial em $Y$, dita* **induzida** *por aquela de $X$.*

Se $(X, \leqslant)$ é um conjunto munido de uma ordem parcial, e $A \subset X$ é um subconjunto, dizemos que $\omega \in X$ é um **limite superior** para $A$ se

$$x \in A \implies x \leqslant \omega.$$

Dizemos que $a \in A$ é um elemento **maximal** se

$$x \in A, \quad a \leqslant x \implies x = a.$$

Dizemos que $a \in A$ é um elemento **máximo** se ele for limite superior para $A$.

Analogamente, dizemos que $\alpha \in X$ é um **limite inferior** para $A$ se

$$x \in A \implies \alpha \leqslant x.$$

Dizemos que $a \in A$ é um elemento **minimal** se

$$x \in A, \quad x \leqslant a \implies x = a.$$

Dizemos que $a \in A$ é um elemento **mínimo** se ele for limite inferior para $A$.

EXEMPLO 22. *Seja $X = \{a, b, c, d\}$, e muna $\mathscr{P}(X)$ da ordem parcial do Exemplo 21. Considere o conjunto*

$$A \subset \mathscr{P}(X), \quad A = \{Y \subset X \mid a \in Y\}.$$

*Explicitamente,*

$$A = \{\{a\}, \{a, b\}, \{a, c\}, \{a, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{a, b, c, d\}\}.$$

*Então $\{a\} \in \mathscr{P}(X)$ é um limite inferior para $A$, que é também minimal e mínimo.*

*Seja agora*

$$A' = \{\{a, b\}, \{a, c\}, \{a, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{a, b, c, d\}\}.$$

*Então $\{a\} \in \mathscr{P}(X)$ é um limite inferior para $A'$. Há três elementos minimais em $A'$: $\{a,b\}$, $\{a,c\}$ e $\{a,d\}$. Porém, $A'$ não tem nenhum mínimo.*

EXEMPLO 23. *Seja $X = \{a,b,c,d\}$, e muna $\mathscr{P}(X)$ da ordem parcial do Exemplo 21. Considere o conjunto*

$$B \subset \mathscr{P}(X), \quad B = \{Y \subset X \mid d \notin Y\}.$$

*Explicitamente,*

$$B = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}.$$

*Então $\{a,b,c\} \in \mathscr{P}(X)$ é um limite superior para $B$, que é também maximal e máximo.*

*Seja agora*

$$B' = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}\}.$$

*Então $\{a,b,c\} \in \mathscr{P}(X)$ é um limite superior para $B'$. Há três elementos maximais em $B'$: $\{a,b\}$, $\{a,c\}$ e $\{b,c\}$. Porém, $B'$ não tem nenhum máximo.*

DEFINIÇÃO 34. *Uma ordem parcial é uma* **ordem** *se além disso, para todo $x, y \in X$, vale a alternativa*

*a)* $x \leqslant y$ *ou* *b)* $y \leqslant x$.

EXERCÍCIO 35. *Considere o conjunto dos números inteiros $\mathbb{Z}$, e defina $R \subset \mathbb{Z} \times \mathbb{Z}$ por*

$$R = \{(n,m) \mid n = m \quad ou \quad m - n \in \mathbb{N}\}$$

*É essa uma ordem?*

EXEMPLO 24. *A ordem parcial do Exemplo 21 não é uma ordem. Por exemplo, se $X = \{a,b\}$, $Y = \{a\}$ e $Z = \{b\}$, então $Y \not\subset Z$ e $Z \not\subset Y$.*

EXERCÍCIO 36. *Seja $(X, \leqslant)$ um conjunto munido de uma ordem. Mostre que a ordem parcial induzida em um subconjunto $Y \subset X$ é uma ordem.*

EXERCÍCIO 37. *Seja $X$ um conjunto, e defina em $\mathscr{P}(X)$ a relação $Y \leqslant Y'$ se e só se $Y \subset Y'$. É essa uma ordem parcial ? Uma ordem ?*

EXERCÍCIO 38. *Seja $X$ o conjunto de todas as pessoas, e diga que $x \leqslant y$ se $y$ é antepassado de $x$. É essa uma ordem parcial ? Uma ordem ?*

DEFINIÇÃO 39. *Uma ordem é uma* **boa-ordem** *se todo subconjunto $Y \subset X$ tem um elemento mínimo.*

EXERCÍCIO 40. *Seja $\mathbb{N}$ o conjunto de números naturais, pensado como subconjunto do conjunto dos números inteiros, e munido da ordem induzida (veja o Exercicio 36) a partir da ordem em $\mathbb{Z}$ descrita no Exercicio 35. É essa uma boa-ordem ?*

CAPíTULO 8

# Equivalências

*Equivalências* em Matemática são uma ferramenta para precisar a noção de "ser o mesmo sob um certo ponto de vista".

DEFINIÇÃO 41. *Uma* **equivalência** *em um conjunto $X$ é uma relação $R$ que é reflexiva, simétrica e transitiva.*

Escrevamos $x \sim y$ se $(x, y) \in R$. Então as condições na definição de uma equivalência se expressam por:

a) $x \sim x$;
b) $x \sim y$ se e só se $y \sim x$;
c) $x \sim y$ e $y \sim z$ apenas se $x \sim z$.

Se $R$ é uma equivalência em um conjunto $X$, então para cada $x \in X$, temos um subconjunto

$$[x] = \{y \in X \mid x \sim y\}$$

chamado de **classe de equivalência de** $x$. Note que $Rx = Ry$ exatamente quando $x \sim y$. Portanto

$$X/R \subset \mathscr{P}(X), \quad X/R = \{[x] \mid x \in X\}$$

define uma partição de $X$, dita **partição associada** à equivalência $R$;

EXERCÍCIO 42. *Mostre que:*

*a) Dada uma partição $P \subset \mathscr{P}(X)$ de $X$, a relação*

$$R(P) \subset X \times X, \quad R(P) := \{(x, y) \mid Rx = Ry\}$$

*define uma equivalência em $X$, dita* **equivalência associada** *à partição $P$;*

*b) $P = X/R(P)$ para toda partição $P$ — ou seja, a partição associada à equivalência associada à partição $P$ é a própria partição $P$;*

*c) $R = R(X/R)$ para toda equivalência $R$ — ou seja, a equivalência associada à partição associada à equivalência $R$ é a própria equivalência $R$.*

EXERCÍCIO 43. *Seja $X$ um conjunto finito, e $\mathscr{P}(X)$ o conjunto cujos elementos são todos os subconjuntos $Y$ de $X$. Diga que $Y \sim Y'$ se $Y$ e $Y'$ têm o mesmo número de elementos. É essa uma equivalência ?*

EXERCÍCIO 44. *Seja $X$ um conjunto finito, e $\mathscr{P}(X)$ o conjunto de suas partes. Diga que $Y \sim Y'$ se $Y$ e $Y'$ diferem por no máximo um número finito de elementos:*

$$Y \sim Y' \iff (Y \setminus Y') \cup (Y' \setminus Y) \text{ é um conjunto finito.}$$

*É essa uma equivalência ? De um exemplo de um conjunto $X$ e dois subconjuntos $Y, Y' \subset X$ que não sejam equivalentes.*

CAPíTULO 9

# Funções

Uma relação $R \subset X \times Y$ é chamada de **gráfico de uma função** de $X$ em $Y$ se, para cada $x \in X$, existe um, e um único $y \in R$ tal que $(x, y) \in R$. Nesse caso, escrevemos $y = f(x)$, e

$$f : X \longrightarrow Y, \quad x \mapsto f(x).$$

$X$ é dito o **domínio** da função $f$, e $Y$ é seu **codomínio**.

Exemplo 25. *Considere as relações $R, S \subset \mathbb{Z} \times \mathbb{Z}$ dadas por*

$$R = \{(x, x^2) \mid x \in \mathbb{Z}\}, \quad S = \{(n, m) \mid \exists\ k,\ n^2 + m^2 = k^2 \in \mathbb{Z}\}.$$

*Então $R$ é o gráfico da função*

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(x) = x^2.$$

*Porém, $S$ não é o gráfico de função alguma: Note que tanto $(3, 4)$ como $(3, -4)$ estão em $S$.*[1]

A **imagem** de uma função $f : X \to Y$ é o subconjunto $f(X) \subset Y$ dado por

$$f(X) = \{f(x) \mid x \in X\}$$

Exemplo 26. *Seja $X$ um conjunto qualquer. Então há uma função*

$$\mathrm{id}_X : X \longrightarrow X, \quad \mathrm{id}_X(x) = x,$$

*dita* **função identidade** *de $X$.*

Exemplo 27. *A imagem da função*

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(x) = x^2$$

*é o conjunto de números inteiros não-negativos:*

$$f(\mathbb{Z}) = \{f(n) \mid n \in \mathbb{Z}\} = \{n^2 \mid n \in \mathbb{Z}\} = \mathbb{N} \cup \{0\}.$$

Dado um subconjunto $Z \subset X$, dizemos que $f(Z) = \{f(z) \mid z \in Z\}$ é a **imagem de** $Z$ por $f$. Analogamente, dado um subconjunto $Z \subset Y$, dizemos que $f^{-1}(Z) = \{x \in X \mid f(x) \in Z\}$ é a **pré-imagem de** $Z$ por $f$.

Exemplo 28. *Seja $X$ um conjunto qualquer, e $Z \subset X$ um subconjunto. Então há uma função*

$$i_Z : Z \longrightarrow X, \quad i_Z(x) = x,$$

*dita* **inclusão** *de $Z$ em $X$.*

Exemplo 29. *Considere a função*

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(x) = \begin{cases} 0 & \text{se } x \text{ é par;} \\ 1 & \text{se } x \text{ é ímpar.} \end{cases}$$

*A imagem do subconjunto de números pares por $f$ é o conjunto $\{0\}$, enquanto a imagem do subconjunto de números ímpares por $f$ é o conjunto $\{1\}$. A pré-imagem de um conjunto $Z \subset \mathbb{Z}$ é:*

[1] E também $(3, 4)$ e $(-3, 4)$!

- *O conjunto vazio se $Z$ não contém $0$ e $1$;*
- *O conjunto de números pares se $Z$ contém $0$ mas não contém $1$;*
- *O conjunto de números ímpares se $Z$ contém $1$ mas não contém $0$;*
- *O conjunto de números inteiros se $Z$ contém $0$ e $1$.*

Dadas funções $f : X \to Y$ e $g : Y \to Z$, a **composição** $g \circ f : X \to Z$ é a função

$$x \mapsto g(f(x)).$$

EXEMPLO 30. *Considere as funções*

$$f, g : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(x) = x + 1, \quad g(x) = x^2.$$

*Então*

$$f \circ g : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (f \circ g)(x) = x^2 + 1,$$

*enquanto que*

$$g \circ f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (g \circ f)(x) = (x + 1)^2 = x^2 + 2x + 1.$$

DEFINIÇÃO 45. *Uma função $f : X \to Y$ é dita:*

**injetora:** *se cada $y \in Y$ pode ser imagem de no máximo um $x \in X$:*

$$y = f(x) = f(x') \quad \Longrightarrow \quad x = x';$$

**sobrejetora:** *se cada $y \in Y$ é imagem de algum $x \in X$:*

$$f(X) = Y;$$

**sobrejetora:** *se é injetora e sobrejetora.*

LEMA 46. *Seja $R \subset X \times Y$ o gráfico de uma função $f : X \to Y$. Então $f$ é bijetora exatamente quando $R$ é também o gráfico de uma função $g : Y \to X$, em cujo caso temos que*

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

DEMONSTRAÇÃO. Seja $y \in Y$. Como $f$ é sobrejetora, existe $x \in X$ com $(x, y) \in R$; como $f$ é injetora, tal $x$ é único. Defina então $g(y)$ como o único elemento de $X$ para o qual $(g(y), y) \in R$. Então $g : Y \to X$ é função, e $(g(y), y) = (x, f(x))$ implica que

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

e portanto que

$$g(f(x)) = x, \quad f(g(y)) = y.$$

□

Note que, dada função $f : X \to Y$, se existe uma função $g : Y \to X$ satisfazendo

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y,$$

então $g$ é a única tal função, dita **função inversa** a $f$, e denotada por $f^{-1}$.

EXERCÍCIO 47. *Seja $R$ uma relação de equivalência em um conjunto $X$. Mostre que existe uma função*

$$p : X \longrightarrow X/R, \quad p(x) := Rx.$$

*Mostre também que $p$ é sobrejetora.*

EXERCÍCIO 48. *Se $X$ e $Y$ são conjuntos, denotamos por*

$$\mathrm{Sets}(X,Y) = \{f \mid f \text{ é função de } X \text{ em } Y\}$$

*o conjunto das funções de $X$ em $Y$.*

*Mostre que para quaisquer três conjuntos $X, Y, Z$, a composição*

$$\circ : \mathrm{Sets}(Y,Z) \times \mathrm{Sets}(X,Y) \longrightarrow \mathrm{Sets}(X,Z)$$

*define uma função. Dê exemplos em que ela é injetora ou sobrejetora.*

EXERCÍCIO 49. *Seja $\mathbb{Z}_2 = \{0,1\}$, e seja $X$ um conjunto qualquer. Para um subconjunto $Y \subset X$, denote por $f_Y : X \to \mathbb{Z}_2$ a função de $X$ em $\mathbb{Z}_2$:*

$$f_Y(x) = \begin{cases} 1 & \text{se } x \in Y; \\ 0 & \text{se } x \notin Y. \end{cases}$$

*Mostre que a regra*

$$f : \mathscr{P}(X) \longrightarrow \mathrm{Sets}(X, \mathbb{Z}_2), \quad Y \mapsto f_Y$$

*é uma bijeção, e escreva a função inversa.*

EXERCÍCIO 50. *Sejam $X$ e $Y$ conjuntos, $f : X \to Y$ uma função, e $R \subset X \times X$ uma equivalência. Denote por $[x] \in X/R$ a classe de equivalencia de $x \in X$. Note que $[x]$ nao determina $x$, em geral; portanto quando escrevemos algo como*

*"Considere a função $F : X/R \longrightarrow Y, \quad F[x] := f(x)$ (...)"*

*está implícito que:*

- *para calcular o valor de $F$ em $[x]$, escolhemos algum representante $x' \in [x]$, e aplicamos $f$ a $x'$;*
- *se $x'' \in [x]$ é outro representante, então $[x'] = [x'']$, e portanto $f(x')$ e $f(x'')$ devem ser iguais.*

*Nesse caso, dizemos que $F$ está* **bem-definida**. *Verifique que $F$ está bem-definida se e só se, para todo $x \in X$, $f^{-1}(f(x)) \subset X$ é uniao de classes de equivalencia de $R$:*

$$\forall\ x \in X,\ \exists\ X_x \subset X \quad f^{-1}(f(x)) = \coprod_{x' \in X_x} [x'].$$

CAPíTULO 10

# Números Inteiros

Como vimos, uma equação da forma

$$(*) \qquad x + n = m$$

possui solução natural $x \in \mathbb{N}$ se e só se $n < m$. O conjunto de números inteiros $\mathbb{Z}$ resulta de acrescentar a $\mathbb{N}$ uma solução "formal" $x = m - n$ para *todas* as equações $(*)$, permitindo todos $n, m \in \mathbb{N}$. Note que $\mathbb{N}\times\mathbb{N}$ parametriza o conjunto de equações da forma $(*)$ — ou seja, para cada par $(n, m) \in \mathbb{N} \times \mathbb{N}$, temos uma e uma única equação $x + n = m$. Note que as soluções de

$$x + n = m, \qquad\qquad x + n + 1 = m + 1$$

deveriam ser as mesmas. Somos então levados a considerar a menor relação de equivalência

$$R \subset (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}),$$

na qual

$$((n, m), (n + 1, m + 1)) \in R$$

para todos $(n, m) \in \mathbb{N} \times \mathbb{N}$.

Lema 51. *A menor relação de equivalencia $R$ em $\mathbb{N} \times \mathbb{N}$, em que $(n, m) \sim (n + 1, m + 1)$ para todo par $(n, m) \in \mathbb{N} \times \mathbb{N}$ é aquela composta de todos os pares $((n, m), (n'm'))$, onde*

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

Demonstração. Mostremos primeiro que $R$ é uma equivalencia:

**reflexiva:** Para todo $(n, m) \in \mathbb{N} \times \mathbb{N}$, temos que

$$n + m = m + n,$$

e portanto $((n, m), (n, m)) \in R$;

**simétrica:** Se $((n, m), (n', m')) \in R$, isto é, se $n + m' = m + n'$, então $n' + m = m' + n$, e portanto $((n', m'), (n, m)) \in R$;

**transitiva:** Se $((n, m), (n', m')) \in R$ e $((n', m'), (n'', m'')) \in R$, isto é, se

$$n + m' = m + n', \qquad\qquad n' + m'' = m' + n'',$$

então

$$\begin{aligned} n + m'' + (n' + m') &= (n + m') + (n' + m'') \\ &= (m + n') + (m' + n'') \\ &= m + n'' + (n' + m'), \end{aligned}$$

e portanto $((n, m), (n'', m'')) \in R$.

Seja $S \subset (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ a relação

$$S = \{((n, m), (n + 1, m + 1)) \mid n, m \in \mathbb{N}\}$$

Ela é visivelmente uma subrelação de $R$, e portanto a menor equivalencia $\widetilde{S}$ que contém $S$ está contida em $R$. Seja $((n, m), (n', m')) \in R$ um elemento qualquer de $R$. Então há três casos a considerar:

i) $n > n'$, em cujo caso $n' = n+k$ para algum $k \in \mathbb{N}$, e portanto $n+m' = m+n'$ implica que $m' = m+k$, e portanto

$$\begin{cases} ((n,m),(n+1,m+1)) \ \in S \\ ((n+1,m+1),(n+2,m+2)) \ \in S \\ \vdots \\ ((n+k-1,m+k-1),(n',m')) \ \in S \end{cases}$$

implica que $((n,m),(n',m')) \in \widetilde{S}$ por transitividade;

ii) $n = n'$, em cujo caso $((n,m),(n',m')) \in \widetilde{S}$ por reflexividade;

iii) $n < n'$, em cujo caso $((n',m'),(n,m)) \in \widetilde{S}$ pelo primeiro caso, e portanto $((n,m),(n',m')) \in \widetilde{S}$ por simetria.

□

Denotemos por $[n,m]$ a classe de equivalência de $(n,m)$ sob a relação $R$:

$$[n,m] = \{\cdots, ((n+1,m+1),(n,m)), ((n,m),(n,m)), ((n,m),(n+1,m+1)), \cdots\},$$

e por

$$\mathbb{Z} = \{[n,m] \mid (n,m) \in \mathbb{N} \times \mathbb{N}\}$$

o conjunto de todas as classes de equivalência.

Lema 52. *Todo $x \in \mathbb{Z}$ é de uma das três formas:*

*i)* $x = [1,1]$*;*
*ii)* $x = [1,n+1]$ *para um único* $n \in \mathbb{N}$*;*
*iii)* $x = [n+1,1]$ *para um único* $n \in \mathbb{N}$*.*

Dessa forma, identificamos $\mathbb{N}$ como subconjunto de $\mathbb{Z}$ através do mapa injetor

$$i : \mathbb{N} \longrightarrow \mathbb{Z}, \quad i(n) = [1,n+1],$$

O único elemento da forma i) é chamado de **zero** $0 \in \mathbb{Z}$:

$$0 = [1,1] = [2,2] = \cdots = [n,n] = \cdots$$

O único elemento da forma ii), $x = [1,n+1]$, costumeiramente se escreve $x = n$, já que $n$ é solução da equação $x+1 = n+1$. O único elemento da forma iii), $x = [n+1,1]$, costuma ser escrito como $x = -n$.

Lema 53 (Tricotomia de $\mathbb{Z}$). *Vale a seguinte tricotomia: para todo $x \in \mathbb{Z}$:*

*i) ou* $x = 0$*;*
*ii) ou* $x \in \mathbb{N}$*;*
*iii) ou* $-x \in \mathbb{N}$*.*

Demonstração. Pois dado inteiro $x \in \mathbb{Z}$, temos □

Assim podemos escrever $\mathbb{Z}$ da maneira usual:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

Proposição 54. *As operações de* soma

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad [n,m] + [n',m'] := [n+n', m+m']$$

*e* multiplicação

$$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad [n,m] \cdot [n',m'] := [nm' + n'm, mm' + nn']$$

*a) estão bem-definidas;*
*b) recuperam a soma e a multiplicação de números naturais:*
*c) satisfazem às propriedades listadas na Seção 7;*
*d) satisfazem também:*

**Elemento neutro da soma:** *Para todo $x \in \mathbb{Z}$, temos que $x = x + 0$;*
**Inversa aditiva:** *Para todo $x \in \mathbb{Z}$, existe $y \in \mathbb{Z}$, tal que $x + y = 0$.*

Demonstração. a) Dizer que $[n, m] + [n', m'] = [n + n', m + m']$ está bem-definida sinifica que a classe $[n+n', m+m']$ independente da escolha de representantes $(n, m)$ de $[n, m]$ e $(n', m')$ de $[n', m']$. Ou seja: afirmamos que se $(N, M) \sim (n, m)$ e $(N', M') \sim (n', m')$, então $(N + N', M + M') \sim (n + n', m + m')$. De fato,

$$\begin{aligned}(N, M) \sim (n, m) &\iff N + m = n + M,\\ (N', M') \sim (n', m') &\iff N' + m' = n' + M'\end{aligned}$$

e portanto

$$N+N'+m+m' = (N+m)+(N'+m') = (n+M)+(n'+M') = n+n'+M+M'.$$

donde se conclui que $(N + N', M + M') \sim (n + n', m + m')$. Portanto a soma está bem-definida. Analogamente,

$$\begin{aligned}NM' + N'M + Nn' + Mm' &= N(M' + n') + (N' + m')M\\ &= N(N' + m') + (M' + n')M\\ &= NN' + MM' + Nm' + Mn'\\ \implies &\quad (NM' + MN', NN' + MM') \sim (Nm' + Mn', Nn' + Mm')\\ Nm' + Mn' + nn' + mm' &= (N + m)m' + (M + n)n\\ &= (M + n)m' + (N + m)n\\ &= Nn' + Mm' + nm + mn'\\ \implies &\quad (Nm' + Mn', Nn' + Mm') \sim (nm' + mn', nn' + mm').\end{aligned}$$

Portanto $(N, M) \sim (n, m)$ e $(N', M') \sim (n', m')$ implicam que

$$(NM' + MN', NN' + MM') \sim (nm' + mn', nn' + mm')$$

e logo a multiplicação está bem-definida.

b) Se $i : \mathbb{N} \to \mathbb{Z}$ denota a inclusão $i(n) = [1, n + 1]$, então

$$\begin{aligned}i(n) + i(m) &= [1, n + 1] + [1, m + 1] = [2, n + m + 2] = [1, n + m + 1]\\ &= i(n + m),\\ i(n) \cdot i(m) &= [1, n + 1] \cdot [1, m + 1] = [m + n + 2, nm + n + m + 2] = [1, nm + 1]\\ &= i(nm)\end{aligned}$$

mostra que soma e multiplicação em $\mathbb{Z}$ restringem àquelas de $\mathbb{N}$.

c) Verificamos as propriedades:

**Associatividade da soma:**

$$\begin{aligned}([n, m] + [n', m']) + [n'', m''] &= [n + n', m + m'] + [n'', m'']\\ &= [n + n' + n'', m + m' + m'']\\ &= [n, m] + [n' + n'', m' + m'']\\ &= [n, m] + ([n', m'] + [n'', m'']);\end{aligned}$$

**Comutatividade da soma:** Para todos $m, n \in \mathbb{N}$, temos que

$$\begin{aligned}[n, m] + [n', m'] &= [n + n', m + m']\\ &= [n' + n, m' + m]\\ &= [n', m'] + [n, m];;\end{aligned}$$

**Elemento neutro da multiplicação:** Para todo $n \in \mathbb{N}$, temos que

$$\begin{aligned}[n,m] \cdot [1,2] &= [2n+m, n+2m] \\ &= [n,m];\end{aligned}$$

**Associatividade da multiplicação:** Para todos $l, m, n \in \mathbb{N}$, temos que

$$\begin{aligned}([n,m] \cdot [n',m']) \cdot [n'',m''] &= [nm'+mn', nn'+mm'] \cdot [n'',m''] \\ &= [(nm'+mn')m'' + (nn'+mm')n'', (nm'+mn')n'' + (nn'+mm')m''] \\ &= [n(n'n''+m'm'') + m(n'm''+m'n''), n(n'm''+m'n'') + m(nn'+mm')] \\ &= [n,m] \cdot ([n',m'] \cdot [n'',m''])\end{aligned}$$

**Comutatividade da multiplicação:** Para todos $m, n \in \mathbb{N}$, temos que

$$\begin{aligned}[n,m] \cdot [n',m'] &= [nm'+mn', nn'+mm'] \\ &= [n'm+m'n, n'n+m'm] \\ &= [n',m'] \cdot [n,m];\end{aligned}$$

**Distributividade:**

$$\begin{aligned}([n,m] + [n',m']) \cdot [n'',m''] &= [n+n', m+m'] \cdot [n'',m''] \\ &= [(n+n')m'' + (m+m')n'', (n+n')n'' + (m+m')m''] \\ &= [nm''+mn'', nn''+mm''] + [n'm''+m'n'', n'n''+m'm''] \\ &= [n,m] \cdot [n'',m''] + [n',m'] \cdot [n'',m'']\end{aligned}$$

d) Verificamos:

**Elemento neutro da soma:**

$$\begin{aligned}[n,m] + [1,1] &= [n+1, m+1] \\ &= [n,m];\end{aligned}$$

**Inversa aditiva:**

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

□

Para elementos $a, b \in \mathbb{Z}$, dizemos que:

- $b$ divide $a$, ou $a$ é múltiplo de $b$, se existe $c \in \mathbb{Z}$ tal que $a = bc$;
- o mdc de $a$ e $b$ é o maior $c \in \mathbb{N}$ que divide simultaneamente $a$ e $b$;
- o mmc de $a$ e $b$ é o menor $c \in \mathbb{N}$ que é simultaneamente múltiplo de $a$ e $b$.

Proposição 55. *O mdc de $a, b \in \mathbb{Z}$ é o elemento mínimo do conjunto*

$$S = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}.$$

Demonstração. Seja $c$ o elemento mínimo de $S$. Precisamos mostrar que $c$ divide $a$, que $c$ divide $b$, e que qualquer outro inteiro $d$ que divide simultaneamente $a$ e $b$ divide também $c$.

Ora, como $c \in S$, devem existir inteiros $x, y \in \mathbb{Z}$ tais que $c = ax + by$. Pelo algoritmo da divisão, podemos escrever

$$a = pc + r,$$

onde $p \in \mathbb{Z}$ e $r \in \{0, 1, ..., c-1\}$. Portanto

$$r = a - pc = a - p(ax + by) = a(1 - px) + b(-py),$$

o que mostra que $r = 0$ ou $r \in S$. Se $r \in S$, então como $r$ é estritamente menor que $c$, contradizemos a escolha de $c$ mínimo — portanto $r = 0$, o que significa que $a = pc$ para algum $p \in Z$.

De maneira análoga se demonstra que $b = qc$ para algum $q \in \mathbb{Z}$. Portanto $c$ divide $a$ e $b$.

Suponha agora que $c' \in \mathbb{N}$ também divida $a$ e $b$; digamos, $a = p'c'$ e $b = q'c'$. Então

$$c = ax + by = c'(p'x + q'y)$$

e portanto $c'$ divide $c$. □

Exemplo 31. *Considere $a = 21$ e $b = 15$. Então seu maior múltiplo comum é $3 = 3a - 4b$.*

Proposição 56 (Divisão com resto). *Sejam $m \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então existem únicos $q \in \mathbb{Z}$ e $r \in \{0, 1, ..., n-1\}$, tais que $m = qn + r$.*

Demonstração. Se $n = 1$, $q = m$ e $r = 0$. Por outro lado, se $n > 1$, há duas situações possíveis:

i) ou $m \in n\mathbb{Z}$, em cujo caso $m = nq$ para um único $q$;
ii) ou $m \notin n\mathbb{Z}$, em cujo caso $X \subset \mathbb{N}$, $X := \{i \mid m + i \in n\mathbb{Z}\}$ não é vazio, e tem portanto um elemento mínimo $k = \min X \leqslant n$, e então $m + k = q'n$ para um único $q'$, e então

$$m = qn + r,$$

onde

$$q := q' - 1, \quad r = n - k.$$

□

Proposição 57. *A relação $\mathscr{O} \subset \mathbb{Z} \times \mathbb{Z}$*

$$\mathscr{O} = \{(x, y) \mid y = x \ \ ou \ \ y - x \in \mathbb{N}\}$$

*a) define uma ordem em $\mathbb{Z}$;*
*b) Para todos $x, y \in \mathbb{Z}$, temos que:*
  *i) $x \leqslant y$ se e só se $x + z \leqslant y + z$ para todo $z \in \mathbb{Z}$;*
  *ii) $x \leqslant y$ se e só se $ax \leqslant ay$ para todo $a \in \mathbb{N}$.*

CAPíTULO 11

# Anéis comutativos e Corpos

O conjunto de números inteiros $\mathbb{Z}$ possui duas operações, **soma** $+$ e **multiplicação** $\cdot$, que satisfazem a uma série de condições. Se abstrairmos essas condições, chegamos à noção de *anel comutativo*:

DEFINIÇÃO 58. *Um* **anel comutativo** $(A, +, \cdot)$ *é um conjunto* $A$*, munido de funções*

$$+ : A \times A \longrightarrow A, \quad \cdot : A \times A \longrightarrow A,$$

*satisfazendo as seguintes propriedades:*

**Elemento neutro da soma:** *Existe* $0 \in A$*, tal que para todo* $x \in A$*, temos que*

$$x = x + 0;$$

**Associatividade da soma:** *Para todos* $x, y, z \in A$*, temos que*

$$(x + y) + z = x + (y + z);$$

**Comutatividade da soma:** *Para todos* $x, y \in A$*, temos que*

$$x + y = y + x;$$

**Inversa aditiva:** *Para todo* $x \in A$*, existe* $-x \in A$*, tal que*

$$x + (-x) = 0;$$

**Elemento neutro da multiplicação:** *Existe* $1 \in A$*, tal que para todo* $x \in A$*, temos que*

$$x = x \cdot 1;$$

**Associatividade da multiplicação:** *Para todos* $x, y, z \in A$*, temos que*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z);$$

**Comutatividade da multiplicação:** *Para todos* $x, y \in A$*, temos que*

$$x \cdot y = y \cdot x;$$

**Distributividade:** *Para todos* $x, y, z \in A$*, temos que*

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

O exemplo principal é:

EXEMPLO 32. $(\mathbb{Z}, +, \cdot)$ *é um anel comutativo.*

Outros exemplos importantes são discutidos a seguir.

## 1. Anéis de polinômios

EXEMPLO 33. *Um* **polinômio** *$p$ na variável $t$, e com coeficientes em $\mathbb{Z}$, é uma expressão da forma*

$$p = \sum_{i=0}^{\infty} a_i t^i,$$

*onde os $a_i$'s são números inteiros, e só um número finito deles não é zero*[1] *Seja $\mathbb{Z}[t]$ o conjunto de tais polinômios $p$ na variável $t$, e com coeficientes em $\mathbb{Z}$. Se $q = \sum_{i=0}^{\infty} b_i t^i \in \mathbb{Z}[t]$, defina*

$$p + q := \sum_i (a_i + b_i) t^i, \qquad p \cdot q := \sum_{i,j=0}^{\infty} a_i b_j t^{i+j} = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} a_i b_j \right) t^k$$

*Então $(\mathbb{Z}[t], +, \cdot)$ é um anel comutativo.*

EXERCÍCIO 59. *O* **grau** $\deg(p)$ *de um tal polinômio $p = \sum_{i=0}^{\infty} a_i t^i$ é o maior $i \in \mathbb{N}$ para o qual $a_i \neq 0$. Verifique que*

$$\deg(p+q) \leqslant \max\{\deg(p), \deg(q)\}, \qquad \deg(p \cdot q) = \deg(p) + \deg(q).$$

EXERCÍCIO 60. *Se $A$ é um anel comutativo qualquer, um* **polinômio** *$p$ na variável $t$, e com coeficientes em $A$, é uma expressão da forma*

$$p = \sum_{i=0}^{\infty} a_i t^i,$$

*onde os $a_i$'s são elementos de $A$, e só um número finito deles não é zero. Verifique que o conjunto $A[t]$ de tais polinômios, munido das operações análogas às de $\mathbb{Z}[t]$, tornam $A[t]$ um anel comutativo.*

DEFINIÇÃO 61. *Um anel comutativo $(A, +, \cdot)$ é um* **corpo** *se satisfaz*

**Inversa multiplicativa:** *Para todo $x \in A \setminus \{0\}$, existe $x^{-1} \in A$, tal que*

$$x \cdot x^{-1} = 1.$$

Note que $\mathbb{Z}$ não é um corpo: os únicos elemento que têm inversa multiplicativa são 1 e $-1$:

$$1 \cdot 1 = 1, \quad (-1)(-1) = 1.$$

## 2. O anel dos inteiros mod $n$

Seja $n > 1$ um número natural, e considere a relação $R_n \subset \mathbb{Z} \times \mathbb{Z}$,

$$R_n = \{(m, m') \mid m - m' \in n\mathbb{Z}\}.$$

Ou seja: $(m, m') \in R_n$ se e só se $m' = m + kn$ para algum $k \in \mathbb{Z}$.

LEMA 62. *$R_n$ é uma equivalência.*

DEMONSTRAÇÃO. Verificamos as três propridades que caracterizam uma equivalência:

**reflexiva:** pois $m = m + 0n$ implica que $(m, m) \in R_n$ para todo $m \in \mathbb{Z}$;

**simétrica:** pois $m' = m + kn$ onde $k \in \mathbb{Z}$ implica que $m = m' + ln$, onde $l = -k \in \mathbb{Z}$;

**transitiva:** pois se $m' = m + kn$ e $m'' = m' + ln$, onde $k, l \in \mathbb{Z}$, então

$$m'' = m' + ln = (m + kn) + ln = m + (k + l)n.$$

□

[1] E portanto a soma que expressa $p$ é *finita*.

Denote por

$$[m] = \{\cdots m - 2n, m - n, m, m + n, m + 2n, \cdots\}$$

a classe de equivalência de $m \in \mathbb{Z}$ sob a relação $R_n$, e por

$$\mathbb{Z}_n = \{[m] \mid m \in \mathbb{Z}\}$$

o conjunto de todas as classes de equivalencia. Observe que, se

$$m = qn + r, \quad q \in \mathbb{Z}, \quad 0 \leqslant r < n,$$

então $[m] = [r]$. Portanto todo elemento $x \in \mathbb{Z}_n$ pode ser representado por $r \in \{0, 1, ..., n - 1\}$:

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n - 1]\}.$$

Portanto $\mathbb{Z}_n$ tem $n$ elementos.

PROPOSIÇÃO 63. *As operações $+, \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ dadas por*

$$[m] + [m'] := [m + m'], \qquad [m] \cdot [m'] := [mm']$$

*estão bem-definidas e munem $\mathbb{Z}_n$ de uma estrutura de anel comutativo. Além disso, $[m] \in \mathbb{Z}_n$ tem inversa multiplicativa se e só se $m$ e $n$ são coprimos.*

DEMONSTRAÇÃO. Verificamos que soma e multiplicação estão bem-definidas: se

$$M \sim m \iff M = m + kn, \qquad M' \sim m' \iff M' = m' + ln,$$

então

$$M + M' = (m + kn) + (m' + ln) = m + m' + (k + l)n,$$
$$MM' = (m + kn)(m' + ln) = mm' + (ml + km' + kln)n$$

mostram que $M + M' \sim m + m'$ e $MM' \sim mm'$. Portanto soma e multiplicação estão bem-definidas.

Verificamos que é anel comutativo:

**Elemento neutro da soma:**

$$\begin{aligned}[m] + [0] &= [m + 0] \\ &= [m];\end{aligned}$$

**Associatividade da soma:**

$$\begin{aligned}([m] + [m']) + [m''] &= [m + m'] + [m''] \\ &= [m + m' + m''] \\ &= [m] + [m' + m''] \\ &= [m] + ([m'] + [m''']);\end{aligned}$$

**Comutatividade da soma:**

$$\begin{aligned}[m] + [m'] &= [m + m'] \\ &= [m' + m] \\ &= [m'] + [m];\end{aligned}$$

**Inversa aditiva:**

$$\begin{aligned}[m] + [-m] &= [m - m] \\ &= [0];\end{aligned}$$

**Elemento neutro da multiplicação:**

$$[m] = [m \cdot 1] = [m] \cdot [1];$$

**Associatividade da multiplicação:**

$$([m]\cdot[m'])\cdot[m''] = [mm']\cdot[m''] = [mm'm''] = [m]\cdot[m'm''] \\ = [m]\cdot([m']\cdot[m''])\text{;}$$

**Comutatividade da multiplicação:**

$$[m]\cdot[m'] = [mm'] = [m'm] = [m']\cdot[m]\text{;}$$

**Distributividade:**

$$([m]+[m'])\cdot[m''] = [m+m']\cdot[m''] = [mm''+m'm''] = [mm'']+[m'm''] \\ = [m]\cdot[m'']+[m']\cdot[m'']$$

Recorde agora que $n, m$ são coprimos se e só se existem inteiros $x, y \in \mathbb{Z}$, tais que

$$1 = nx + my\text{;}$$

portanto se $\mathrm{mdc}(n, m) = 1$, segue que

$$[1] = [nx + my] = [my] = [m]\cdot[y],$$

e portanto $[y] \in \mathbb{Z}_n$ é inversa multiplicativa de $[m]$. Por outro lado, se $[m]$ tem inversa multiplicativa $[y]$, então $[my] = [1]$ significa que $my - 1$ é divisível por $n$, e portanto

$$my - 1 = nx$$

para algum $x$. Logo $1 = nx + my$, e portanto $m$ e $n$ são coprimos. □

Exemplo 34. *Um exemplo para ilustrar: considere $n = 4$. Então*

$$\mathbb{Z}_4 = \{[0],\ [1],\ [2],\ [3]\}$$

*As tabelas de soma e multiplicação são dadas abaixo:*

| $+$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
|---|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[0]$ |
| $[2]$ | $[2]$ | $[3]$ | $[0]$ | $[1]$ |
| $[3]$ | $[3]$ | $[0]$ | $[1]$ | $[2]$ |

| $\cdot$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
|---|---|---|---|---|
| $[0]$ | $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[2]$ | $[0]$ | $[2]$ | $[0]$ | $[2]$ |
| $[3]$ | $[0]$ | $[3]$ | $[2]$ | $[1]$ |

Corolário 64. *Se $p$ é primo, então $(\mathbb{Z}_p, +, \cdot)$ é corpo.*

Demonstração. Se $p$ é primo, então $p$ é coprimo a todo elemento $m$ que não é múltiplo de $p$ — ou seja, se $[m] \neq 0$, então $m$ e $p$ são coprimos — e portanto $[m]$ tem inversa multiplicativa pela Proposição 63. □

CAPíTULO 12

# Números Racionais

Construímos os números inteiros $\mathbb{Z}$ ao acrescentar a $\mathbb{N}$ todas as soluções de equações da forma

$$(*) \qquad q + x = p,$$

onde $p, q \in \mathbb{N}$. A soma e a multiplicação de números inteiros estende a uma soma e multiplicação em $\mathbb{Z}$ — isto é, $\mathbb{Z}$, munidos dessas operações, se torna um anel comutativo. Um "defeito", porém, dos números inteiros, é que equações da forma

$$(**) \qquad q \cdot x = p,$$

onde $p \in \mathbb{Z}$ e $q \in \mathbb{Z}\setminus\{0\}$, não podem ser resolvidas para $x \in \mathbb{Z}$ — exceto quando $q \in \{-1, 1\}$, i.e., exceto se $q$ tiver inversa multiplicativa em $\mathbb{Z}$, pois então

$$x = q^{-1}p \in \mathbb{Z}$$

é solução de $(**)$.

Desejamos expandir $\mathbb{Z}$ a um anel comutativo maior, no qual acrescentamos todas as soluções $x = \frac{p}{q}$ dessas equações $(**)$. Como na construção de $\mathbb{Z}$, podemos parametrizar equações da forma $(**)$ por $(p, q) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$, e como as equações

$$q \cdot x = p, \qquad\qquad q \cdot r \cdot x = p \cdot r$$

deveriam ter a mesma solução para todo $r \in \mathbb{Z}\setminus\{0\}$, somos levados a considerar a menor relação de equivalência

$$R \subset (\mathbb{Z} \times \mathbb{Z}\setminus\{0\}) \times (\mathbb{Z} \times \mathbb{Z}\setminus\{0\})$$

em que

$$((p, q), (pr, qr)) \in R$$

para todos $p \in \mathbb{Z}$ e $q, r \in \mathbb{Z}\setminus\{0\}$.

Lema 65. *A menor tal relação de equivalencia é*

$$R \subset X \times X, \quad R = \{((p, q), (p', q')) \mid pq' = p'q\}.$$

Demonstração. Mostremos primeiro que $R$ é equivalencia:

**reflexiva:** Para todo $(p, q) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$, temos que $pq = pq$, e portanto $((p, q), (p, q)) \in R$;

**simétrica:** Se $((p, q), (p', q')) \in R$, isto é, se $pq' = p'q$, então $p'q = pq'$, e portanto $((p', q'), (p, q)) \in R$;

**transitiva:** Se $((p, q), (p', q')) \in R$ e $((p', q'), (p'', q'')) \in R$, isto é, se

$$pq' = p'q, \qquad\qquad p'q'' = p''q',$$

então

$$(pq'')q' = (pq')q'' = (p'q)q'' = q(p'q'') = q(p''q') = (p''q)q'.$$

Como $q' > 0$, a igualdade $(pq'')q' = (p''q)q'$ implica $pq'' = p''q$, o que significa que $((p, q), (p'', q'')) \in R$.

Considere agora a relação

$$S = \{((p,q),(pr,qr)) \mid p,q,r \in \mathbb{Z},\ q \neq 0,\ r \neq 0\}$$

e observe que $S \subset R$. Portanto a menor equivalencia $\widetilde{S}$ que contém $S$ está contida em $R$. Suponha que $((p,q),(p',q')) \in R$ é um elemento qualquer. Então $k = pq' = p'q$,

$$\begin{cases} ((p,q),(pq',qq')) = ((p,q),(k,qq')) \in S \\ ((p,'q'),(p'q,qq')) = ((p,'q'),(k,qq')) \in S \end{cases}$$

implica que

$$\begin{cases} ((p,q),(k,qq')) \in \widetilde{S} \\ ((k,qq'),(p,'q')) \in \widetilde{S}, \end{cases}$$

por simetria, e portanto $((p,q),(p',q')) \in \widetilde{S}$ por transitividade. Portanto $R = \widetilde{S}$. □

Definição 66. *O conjunto dos* **números racionais** $\mathbb{Q}$ *é o conjunto de classes de equivalência da relação $R$ em $X$. A classe de equivalência de um par $(p,q) \in X$ é denotada por $\frac{p}{q}$, e chamada de uma* **fração**.

Lema 67 (Fração irredutível). *Para todo número racional $r \in \mathbb{Q}$, existe um e um único par $(p,q) \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$, tal que:*

*a) $r = \frac{p}{q}$;* *b) $p,q$ são coprimos;* *c) $q \in \mathbb{N}$.*

*Além disso, dado qualquer par $(p',q') \in \mathbb{Z} \times \mathbb{Z}\setminus\{0\}$ com $r = \frac{p'}{q'}$, existe $a \in \mathbb{Z}$ tal que $p' = pa$ e $q' = qa$.*

Demonstração. Seja $(p',q') \in r \in \mathbb{Q}$, e seja $c' = \mathrm{mdc}(p',q')$. Podemos supor sem perda de generalidade que $q' \in \mathbb{N}$ (pois do contrário trocamos $(p,q)$ por $(-p,-q)$). Então existem $p \in \mathbb{Z}$ e $q \in \mathbb{N}$ tais que

$$p' = c'p, \qquad q' = c'q$$

e além disso, $p$ e $q$ são coprimos. Portanto $(p,q)$ satisfaz às condições a)-c) acima. Seja agora $(p'',q'') \in r$. Então como $p,q$ são coprimos,

$$pq'' = p''q \implies p|qp'' \implies p'' = ap$$

para algum $a \in \mathbb{Z}\setminus\{0\}$; portanto

$$pq'' = p''q = apq \implies q'' = aq.$$

Portanto $(p'',q'') = (ap,aq)$. □

Proposição 68. *As operações*

$$\frac{p}{q} + \frac{p'}{q'} := \frac{pq' + p'q}{qq'}, \qquad \frac{p}{q} \cdot \frac{p'}{q'} := \frac{pp'}{qq'}$$

*estão bem-definidas, e tornam $\mathbb{Q}$ um corpo.*

Demonstração. Mostremos que a soma está bem-definida: se $(P,Q) \sim (p,q)$ e $(P',Q') \sim p',q')$, então

$$Pq = pQ, \qquad P'q' = p'Q',$$

e portanto

$$(PQ' + QP')qq' = (Pq)Q'q' + Qq(P'q') = (pQ)Q'q' + Qq(p'Q') = (pq' + p'q)QQ',$$

o que significa que

$$(PQ' + QP', QQ') \sim (pq' + qp', qq')$$

Portanto a soma está bem-definida. Por outro lado,

$$PP'qq' = (Pq)(P'q') = (pQ)(p'Q') = pp'QQ',$$

isto é,

$$(PP', QQ') \sim (pp', qq').$$

Portanto a multiplicação está bem-definida.

**Elemento neutro da soma:**

$$(p, q) + (0, 1) = (p + 0, q \cdot 1) = (p, q);$$

**Associatividade da soma:**

$$\begin{aligned}((p, q) + (p', q')) + (p'', q'') &= (pq' + qp', qq') + (p'', q'') \\ &= (pq'q'' + qp'q'' + qq'p'', qq'q'') \\ &= (p, q) + (p'q'' + q'p'', q'q'') \\ &= (p, q) + ((p', q') + (p'', q''));\end{aligned}$$

**Comutatividade da soma:**

$$\begin{aligned}(p, q) + (p', q') &= (pq' + qp', qq') \\ &= (p'q + q'p, q'q) \\ &= (p', q') + (p, q);\end{aligned}$$

**Inversa aditiva:**

$$\begin{aligned}(p, q) + (-p, q) &= (pq - qp, q^2) \\ &= (0, q^2) \\ &\sim (0, 1);\end{aligned}$$

**Elemento neutro da multiplicação:**

$$(p, q) = (p \cdot 1, q \cdot 1) = (p, q) \cdot (1, 1);$$

**Associatividade da multiplicação:**

$$\begin{aligned}((p, q) \cdot (p', q')) \cdot (p'', q'') &= (pp', qq') \cdot (p'', q'') \\ &= (pp'p'', qq'q'') \\ &= (p, q) \cdot (p'p'', q'q'') \\ &= (p, q) \cdot ((p', q') \cdot (p'', q''));\end{aligned}$$

**Comutatividade da multiplicação:**

$$\begin{aligned}(p, q) \cdot (p', q') &= (pp', qq') \\ &= (p'p, q'q) = (p', q') \cdot (p, q);\end{aligned}$$

**Distributividade:**

$$\begin{aligned}((p, q) + (p', q')) \cdot (p'', q'') &= (pq' + qp', qq') \cdot (p'', q'') \\ &= (pq'p'' + qp'p'', qq'q'') \\ &= (pq'' + qp'', qq'') + (p'q'' + q'p'', q'q'') \\ &= (p, q) \cdot (p'', q'') + (p', q') \cdot (p'', q'')\end{aligned}$$

**Inversa multiplicativa:** Se $(p, q) \notin [0, 1]$, então $p \neq 0$, e portanto $(q, p) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, e

$$\begin{aligned}(p, q) \cdot (q, p) &= (pq, qp) \\ &\sim (1, 1).\end{aligned}$$

□

LEMA 69. *O conjunto* $\mathbb{Q}_+ = \{\frac{p}{q} \in \mathbb{Q} \mid pq \in \mathbb{N}\}$ *está bem-definido, e tanto* $x+y$ *quanto* $xy$ *estão em* $\mathbb{Q}_+$ *se* $x, y$ *estiverem em* $\mathbb{Q}_+$.

DEMONSTRAÇÃO. Primeiro observamos que $\mathbb{Q}_+$ está bem-definido, pois se $(P,Q) \sim (p,q)$, então $Pq = pQ$ implica

$$PQpq = p^2Q^2.$$

O lado direito dessa igualdade é não-negativo como produto de quadrados, e só se anula se $p = 0 = P$. Portanto $PQ$ e $pq$ são simultaneamente negativos, nulos ou positivos. Portanto $\mathbb{Q}_+$ está bem-definido.

Note que, se $x = \frac{p}{q}$ e $y = \frac{p'}{q'}$ estão em $\mathbb{Q}_+$, isto é, se $pq, p'q' \in \mathbb{N}$, então

$$(pq)(p'q') = (pp')(qq') \in \mathbb{N}$$

e portanto $\frac{pp'}{qq'} = xy$ está em $\mathbb{Q}_+$. Da mesma forma,

$$(pq' + p'q)(qq') = pq(q')^2 + p'q'q^2 \in \mathbb{N}$$

é soma de produtos de naturais, e portanto $x + y \in \mathbb{Q}_+$. □

LEMA 70 (Tricotomia de $\mathbb{Q}$). *Vale a seguinte tricotomia: para todo* $x \in \mathbb{Q}$*:*

*i) ou* $x = 0$*;*
*ii) ou* $x \in \mathbb{Q}_+$*;*
*iii) ou* $-x \in \mathbb{Q}_+$.

DEMONSTRAÇÃO. Pois dado racional $x = \frac{p}{q}$, temos por tricotomia em $\mathbb{Z}$ que $pq$ ou é zero (em cujo caso vale i), ou é positivo (em cujo caso vale ii) ou negativo (em cujo caso vale iii). □

PROPOSIÇÃO 71. *A relação* $\mathscr{O} \subset \mathbb{Q} \times \mathbb{Q}$

$$\mathscr{O} = \{(x,x') \;\Big|\; x' = x \quad ou \quad x' - x \in \mathbb{Q}_+\}$$

*a) define uma ordem em* $\mathbb{Q}$*;*
*b) Para todos* $x, y \in \mathbb{Q}$*, temos que:*
  *i)* $x \leqslant y$ *se e só se* $x + z \leqslant y + z$ *para todo* $z \in \mathbb{Q}$*;*
  *ii)* $x \leqslant y$ *se e só se* $ax \leqslant ay$ *para todo* $a \in \mathbb{Q}_+$.

DEMONSTRAÇÃO. Verificamos primeiro que $\mathscr{O}$ define uma pré-ordem:

**reflexiva:** por definição, $(x,x) \in \mathscr{O}$ para todo $x \in \mathbb{Q}$;

**anti-simétrica:** se $x = \frac{p}{q}$ e $y = \frac{p'}{q'}$, e tanto $(x,y)$ como $(y,x)$ pertencem a $\mathscr{O}$, então $y - x$ e $x - y$ são ambos nulos ou ambos positivos. Porém eles não podem ser ambos positivos, pois isso implicaria que tanto $p'q - pq'$ e seu oposto são naturais. Portanto $x = y$;

**transitiva:** Sejam $(x,y)$ e $(y,z)$ estão em $\mathscr{O}$. Se dois dentre $x, y, z$ são iguais, então $(x,z) \in \mathscr{O}$ por hipótese. Caso contrário, temos que $z - y$ e $y - x$ estão em $\mathbb{Q}_+$, em cujo caso $(z-y)+(y-x) = z-x$ está em $\mathbb{Q}_+$, e portanto $(x,z) \in \mathscr{O}$.

Para verificar que $\mathscr{O}$ é uma ordem, sejam $x, y \in \mathbb{Q}$, e considere $y - x \in \mathbb{Q}$. Então:

i) ou $y - x = 0$;
ii) ou $y - x \in \mathbb{Q}_+$;
iii) ou $-(y-x) = x - y \in \mathbb{Q}_+$.

Nos casos i) e ii), temos que $(x,y) \in \mathscr{O}$, e nos casos i) e iii), temos que $(y,x) \in \mathscr{O}$. Portanto a pré-ordem $\mathscr{O}$ é uma ordem.

Por fim, suponha que $(x,y) \in \mathscr{O}$, e que $z \in \mathbb{Q}$. Então

$$(y + z) - (x + z) = y - x \in \mathbb{Q}_+$$

mostra que $(x+z, y+z) \in \mathscr{O}$. Por outro lado, se $a \in \mathbb{Q}_+$, então

$$ay - ax = a(y-x) \in \mathbb{Q}_+$$

mostra que $(ax, ay) \in \mathscr{O}$. □

CAPíTULO 13

# Irracionais ?

Uma outra maneira de descrever $\mathbb{Q}$ seria a seguinte: todo polinômio

$$qt - p \quad \in \quad \mathbb{Z}[t]$$

de grau 1 tem raízes em $\mathbb{Q}$. Porém, os racionais são insuficientes para resolver polinômios com coeficientes inteiros arbitrários, como mostra a

PROPOSIÇÃO 72. *Seja $f \in \mathbb{Z}[t]$ um polinômio com coeficientes inteiros:*

$$f(x) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0.$$

*Se $p, q$ são coprimos, e $\frac{p}{q}$ é raiz de $f$, então $p$ divide $a_0$ e $q$ divide $a_n$.*

DEMONSTRAÇÃO. Suponha que $p$ e $q$ sejam coprimos, e observe que

$$0 = q^n f\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n.$$

Como

$$q | (a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n) \quad \Longrightarrow \quad q | a_n p^n \quad \Longrightarrow \quad q | a_n.$$

Analogamente,

$$p | (a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1}) \quad \Longrightarrow \quad p | a_0 q^n \quad \Longrightarrow \quad p | a_0.$$

□

EXEMPLO 35. *$a = \sqrt{2}$ é irracional. De fato, $f(x) = x^2 - 2$ tem a por raiz. Se $\frac{p}{q}$ fosse raiz, então $p|2$ e $q|1$. Como $\frac{0}{1}, \frac{1}{1}$ e $\frac{2}{1}$ não são raízes, a não pode ser racional.*

EXEMPLO 36. *$a = \sqrt{3} - \sqrt{2}$ é irracional. De fato,*

$$1 - a^2 = 2\sqrt{2}a \quad \Longrightarrow \quad a^4 - 10a^2 + 1 = 0.$$

*Portanto $f(x) = x^4 - 10x^2 + 1$ tem a por raiz. Se a fosse racional, $a = \frac{p}{q}$, então tanto $p$ como $q$ dividiriam 1, o que implicaria que $a = 1$, e esse não é o caso, já que $f(1) = -8 \neq 0$. Portanto a é irracional.*

CAPíTULO 14

# Seqüências

DEFINIÇÃO 73. *Uma* **seqüência** *em um conjunto $X$ é um mapa $\underline{x} : \mathbb{N} \to X$.*

Uma seqüência consiste portanto de uma escolha *ordenada* de pontos (não necessariamente distintos)

$$x_1, x_2, \cdots, x_n, \cdots \in X.$$

EXEMPLO 37. *Seja $P \subset \mathbb{N}$ o conjunto de primos. Então definimos $\underline{x} : \mathbb{N} \longrightarrow \mathbb{N}$ indutivamente por:*

$$x_1 = \min P, \quad x_n := \min\left(P \diagdown \{x_1, ..., x_{n-1}\}\right).$$

*Essa é a seqüência dos números primos.*

EXEMPLO 38. *Considere $X = \mathbb{Z}_5$. Então temos a seqüência*

$$\underline{x} : \mathbb{N} \longrightarrow \mathbb{Z}_5, \quad x_n = [2]^n$$

*Portanto:*

$$x_1 = [2], \quad x_2 = [4], \quad x_3 = [3], \quad x_4 = [1], \quad x_5 = [2], \quad x_6 = [4], \quad \cdots$$

DEFINIÇÃO 74. *Se $\underline{x} : \mathbb{N} \to X$ e $\underline{y} : \mathbb{N} \to X$ são seqüências, definimos seu* **embaralhamento**

$$(\underline{x} \star \underline{y})_n = \begin{cases} x_{\frac{n+1}{2}} & \text{se } n \text{ é ímpar;} \\ y_{\frac{n}{2}} & \text{se } n \text{ é par.} \end{cases}$$

DEFINIÇÃO 75. *Uma seqüência $\underline{x} : \mathbb{N} \longrightarrow X$ é* **alfim periódica** *se existem $N, r \in \mathbb{N}$, tais que*

$$n \geqslant N \quad \Longrightarrow \quad a_{n+r} = a_n.$$

## 1. Seqüências de números racionais

DEFINIÇÃO 76. *Uma seqüência $\underline{x} : \mathbb{N} \longrightarrow \mathbb{Q}$ é* **limitada** *se existe $M \in \mathbb{N}$ tal que $|x_n| \leqslant M$ para todo $n \in \mathbb{N}$.*

DEFINIÇÃO 77. *Uma seqüência $\underline{x} : \mathbb{N} \longrightarrow \mathbb{Q}$* **converge** *a $\gamma \in \mathbb{Q}$ se, para todo $\epsilon \in \mathbb{Q}_+$, existe $N_{\underline{x}}(\epsilon) \in \mathbb{N}$ tal que*

$$n \geqslant N_{\underline{x}}(\epsilon) \quad \Longrightarrow \quad |x_n - \gamma| < \epsilon.$$

*Nesse caso, dizemos também que $\gamma$ é o* **limite** *da sequencia $\underline{x}$, o que denotamos por*

$$\gamma = \lim_{n \to \infty} x_n.$$

OBSERVAÇÃO 78. *Se $\underline{x} : \mathbb{N} \longrightarrow \mathbb{Q}$ converge a $\gamma \in \mathbb{Q}$, a escolha de um $N_{\underline{x}}(\epsilon) \in \mathbb{N}$ para cada $\epsilon \in \mathbb{Q}_+$ define uma função $N_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$. Portanto uma maneira equivalente de dizer que $\underline{x} : \mathbb{N} \longrightarrow \mathbb{Q}$ converge a $\gamma \in \mathbb{Q}$ é: "existe função $N_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$, tal que $|x_n - \gamma| < \epsilon$ sempre que $n \geqslant N_{\underline{x}}(\epsilon)$".*

EXEMPLO 39. *A seqüência* constante $x_n = \gamma$ *converge a* $\gamma$. *De fato, para qualquer função* $N : \mathbb{Q}_+ \to \mathbb{N}$, *temos que*

$$0 = |x_n - \gamma| < \epsilon$$

*sempre que* $n \geqslant N(\epsilon)$.

EXEMPLO 40. *A seqüência* $x_n = \frac{1}{n}$ *converge a* 0. *De fato, se* $N : \mathbb{Q}_+ \to \mathbb{N}$ *é tal que* $N(\epsilon)\epsilon > 1$, *então*

$$n \geqslant N(\epsilon) \quad \Longrightarrow \quad n\epsilon > 1 \quad \Longrightarrow \quad |x_n| = \left|\frac{1}{n}\right| < \epsilon.$$

EXEMPLO 41. *A seqüência* $x_n = \frac{1}{2^n}$ *converge a* 0. *De fato, se* $N : \mathbb{Q}_+ \to \mathbb{N}$ *é tal que* $2^{N(\epsilon)}\epsilon > 1$, *então*

$$n \geqslant N(\epsilon) \quad \Longrightarrow \quad 2^n\epsilon > 1 \quad \Longrightarrow \quad |x_n| = \left|\frac{1}{2^n}\right| < \epsilon.$$

EXEMPLO 42. *Seja* $0 \leqslant \beta < 1$, *e defina a sequencia*

$$\underline{x} : \mathbb{N} \longrightarrow \mathbb{Q}, \quad x_n := \sum_{i=1}^{n} \beta^i.$$

*Note que*

$$(1-\beta)x_n = (1-\beta)\sum_{i=1}^{n}\beta^i = \beta - \beta^{n+1} = \beta(1-\beta^n)$$

*Tome por exemplo* $\beta = \frac{1}{2}$. *Então afirmamos que* $\underline{x}$ *converge a* $\gamma = \frac{\beta}{1-\beta} = 1$. *De fato,*

$$(1-\beta)\left(\frac{\beta}{1-\beta} - x_n\right) = \beta - (1-\beta)x_n = \beta - \beta(1-\beta^n) = \beta^{n+1}.$$

*Portanto*

$$|1 - x_n| = \left|\frac{\beta}{1-\beta} - x_n\right| = \frac{\beta^{n+1}}{1-\beta} = \frac{1}{2^n};$$

*logo se* $2^{N(\epsilon)}\epsilon > 1$, *então*

$$n \geqslant N(\epsilon) \quad \Longrightarrow \quad 2^n\epsilon > 1 \quad \Longrightarrow \quad |1 - x_n| = \left|\frac{1}{2^n}\right| < \epsilon.$$

Nem toda sequencia tem limite — um exemplo simples é o que segue:

EXEMPLO 43. *Considere a seqüência* $x_n = (-1)^n$. *Suponha que* $(x_n)$ *convirja a* $\gamma \in \mathbb{Q}$. *Há três casos:*

- $\gamma \neq \pm 1$**:** *Então* $\beta := \min(|\gamma - 1|, |\gamma + 1|) > 0$. *Portanto para todo* $0 < \epsilon < \beta$, *temos que*
  $$|x_n - \gamma| \geqslant \epsilon,$$
  *o que contradiz* $\gamma = \lim_{n\to\infty} x_n$;
- $\gamma = 1$ **ou** $\gamma = -1$**:** *Então para todo* $0 < \epsilon < 2$ *e* $n \in \mathbb{N}$, *temos que*
  $$|x_{2n-1} - \gamma| \geqslant \epsilon, \quad se \quad \gamma = 1$$
  $$|x_{2n} - \gamma| \geqslant \epsilon, \quad se \quad \gamma = -1.$$
  *Ambos os casos contradizem* $\gamma = \lim_{n\to\infty} x_n$.

*Portanto a seqüência* $x_n = (-1)^n$ *não converge.*

Porém:

LEMA 79. *O limite de uma seqüência* $(x_n)$, *se existir, é único.*

DEMONSTRAÇÃO. Suponha que $x = (x_n)$ convirja a $\alpha \in \mathbb{Q}$ e a $\beta \in \mathbb{Q}$. Desejamos mostrar que $\alpha = \beta$. Suponhamos por contradição que $\alpha \neq \beta$. Então $\epsilon = \frac{|\alpha-\beta|}{2} > 0$, e temos que $B_\epsilon(\alpha) \cap B_\epsilon(\beta) = \varnothing$.

Como $\alpha = \lim_{n\to\infty} x_n$, existe $N_\alpha(\epsilon) \in \mathbb{N}$ tal que $n \geqslant N_\alpha(\epsilon)$ implica $|x_n - \alpha| < \epsilon$. Por outro lado, como $\beta = \lim_{n\to\infty} x_n$, existe $N_\beta(\epsilon) \in \mathbb{N}$ tal que $n \geqslant N_\beta(\epsilon)$ implica $|x_n - \beta| < \epsilon$. Portanto se

$$n \geqslant \max\{N_\alpha(\epsilon), N_\beta(\epsilon)\} \quad \Longrightarrow \quad x_n \in B_\epsilon(\alpha) \cap B_\epsilon(\beta),$$

o que é impossível pois o último conjunto é vazio. A contradição mostra que $\alpha = \beta$. □

LEMA 80. *Se uma seqüência $(x_n)$ tem limite, ela é* limitada *— i.e., existe $M \in \mathbb{N}$ tal que $|x_n| \leqslant M$ para todo $n \in \mathbb{N}$.*

DEMONSTRAÇÃO. Seja $\alpha = \lim_{n\to\infty} x_n$, e seja $N_x : \mathbb{Q}_+ \to \mathbb{N}$ tal que $n \geqslant N_x(\epsilon)$ implica $|x_n - \alpha| < \epsilon$. Então se

$$M' = \max\{|x_1|, |x_2|, ..., |x_{N_x(1)}|, |\alpha| + 1\}$$

temos $|x_n| \leqslant M'$ para todo $n$. Portanto um múltiplo inteiro $M = qM'$ é natural, e satisfaz $|x_n| \leqslant M$ para todo $n$. □

LEMA 81. *Sejam $(x_n)$ e $(y_n)$ são seqüência tais que*

$$\alpha = \lim_{n\to\infty} x_n, \quad \beta = \lim_{n\to\infty} y_n.$$

*Então*

*a)* $\alpha + \beta = \lim_{n\to\infty}(x_n + y_n)$, *b)* $\alpha\beta = \lim_{n\to\infty}(x_n y_n)$.

DEMONSTRAÇÃO. Como $x$ converge a $\alpha$, existe $N_x : \mathbb{Q}_+ \to \mathbb{N}$ tal que $n \geqslant N_x(\epsilon)$ implica $|x_n - \alpha| < \epsilon$. Do mesmo modo, como $y$ converge a $\beta$, existe $N_y : \mathbb{Q}_+ \to \mathbb{N}$ tal que $n \geqslant N_y(\epsilon)$ implica $|y_n - \beta| < \epsilon$. Defina então $N_{x+y}\mathbb{Q}_+ \to \mathbb{N}$ por

$$N_{x+y}(\epsilon) := \max\{N_x(\frac{\epsilon}{2}), N_y(\frac{\epsilon}{2})\}.$$

Então

$$n \geqslant N_{x+y}(\epsilon) \quad \Longrightarrow \quad |(\alpha + \beta) - (x_n + y_n)| \leqslant |\alpha - x_n| + \beta - y_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Portanto $\alpha + \beta = \lim_{n\to\infty}(x_n + y_n)$. Por outro lado, como $x$ e $y$ têm limite, elas são limitadas, e sejam $M_x, M_y \in \mathbb{N}$ tais que

$$|x_n| \leqslant M_x, \quad |y_n| \leqslant M_y$$

para todo $n$. Defina $N_{xy}\mathbb{Q}_+ \to \mathbb{N}$ por

$$N_{xy}(\epsilon) := \max\{N_x(\frac{\epsilon}{2M_y}), N_y(\frac{\epsilon}{2M_x})\}.$$

Então se $n \geqslant N_{xy}(\epsilon)$, temos que

$$|\alpha\beta - x_n y_n| = |\alpha\beta - \alpha y_n + \alpha y_n - x_n y_n| \leqslant |\alpha||\beta - y_n| + |\alpha - x_n||y_n| < |\alpha|\frac{\epsilon}{2M_x} + \frac{\epsilon}{2M_y}|y_n|$$
$$\leqslant \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Portanto $\alpha\beta = \lim_{n\to\infty} x_n y_n$. □

## Seqüências de Cauchy

DEFINIÇÃO 82. *Uma seqüência $(x_n)$ é dita* **Cauchy** *se existe função $\widetilde{N}_x : \mathbb{Q}_+ \to \mathbb{N}$, tal que*

$$n, m \geqslant N(\epsilon) \quad \Longrightarrow \quad |x_n - x_m| < \epsilon.$$

PROPOSIÇÃO 83. *Sejam $\underline{x}, \underline{y} : \mathbb{N} \to \mathbb{Q}$ duas seqüências de números racionais.*

*a) $\underline{x}$ é Cauchy se converge.*
*b) $\underline{x}$ é limitada se é Cauchy.*
*c) Se $\underline{x}, \underline{y}$ são Cauchy, então também são Cauchy as seqüências*

$$\underline{x} + \underline{y} := (x_n + y_n), \quad \underline{x} \cdot \underline{y} := (x_n y_n).$$

DEMONSTRAÇÃO. a) Suponha que $\underline{x}$ convirja a $\alpha \in \mathbb{Q}$ Então existe $N_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$, tal que

$$n \geqslant N_{\underline{x}}(\epsilon) \quad \Longrightarrow \quad |x_n - \alpha| < \epsilon.$$

Então se $\widetilde{N}_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$ é a função

$$\widetilde{N}_{\underline{x}}(\epsilon) := N_x\left(\frac{\epsilon}{2}\right),$$

então se $n, m \geqslant \widetilde{N}_{\underline{x}}(\epsilon)$, temos que

$$|x_n - x_m| = |(x_n - \alpha) - (x_m - \alpha)| \leqslant |x_n - \alpha| + |x_m - \alpha| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Portanto $x$ é Cauchy.

b) Seja $\widetilde{N}_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$ tal que $n, m \geqslant \widetilde{N}_x(\epsilon)$ implica $|x_n - x_m| < \epsilon$. Defina

$$M' := \max(|x_1|, |x_2|, ..., |x_{\widetilde{N}_x(1)}|) + 1;$$

então $|x_n| \leqslant M'$ para todo $n$, e um múltiplo inteiro $M = qM'$ é natural.

c) Sejam $\widetilde{N}_{\underline{x}}, \widetilde{N}_{\underline{x}} : \mathbb{Q}_+ \to \mathbb{N}$ tais que

$$n, m \geqslant \widetilde{N}_{\underline{x}}(\epsilon) \ \Rightarrow \ |x_n - x_m| < \epsilon, \quad n, m \geqslant \widetilde{N}_{\underline{y}}(\epsilon) \ \Rightarrow \ |y_n - y_m| < \epsilon.$$

Note que, se

$$\widetilde{N}_{\underline{x}+\underline{y}} : \mathbb{Q}_+ \longrightarrow \mathbb{N}, \quad \widetilde{N}_{\underline{x}+\underline{y}}(\epsilon) := \max\left(\widetilde{N}_{\underline{x}}(\frac{\epsilon}{2}), \widetilde{N}_{\underline{y}}(\frac{\epsilon}{2})\right),$$

então

$$\begin{aligned}|(x_n + y_n) - (x_m + y_m)| = |(x_n - x_m) - (y_n - y_m)| &\leqslant |x_n - x_m| + |y_n - y_m| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.\end{aligned}$$

Portanto $\underline{x} + \underline{y}$ é Cauchy.

Por outro lado, como $\underline{x}$ e $\underline{y}$ são limitadas, podemos escolher $M_{\underline{x}}, M_{\underline{y}} \in \mathbb{N}$ tais que $|x_n| \leqslant M_{\underline{x}}$ e $|y_n| \leqslant M_{\underline{y}}$ para todo $n$. Portanto se

$$\widetilde{N}_{\underline{x}\cdot\underline{y}} : \mathbb{Q}_+ \longrightarrow \mathbb{N}, \quad \widetilde{N}_{\underline{x}\cdot\underline{y}}(\epsilon) := \max\left(\widetilde{N}_{\underline{x}}(\frac{\epsilon}{2M_y}), \widetilde{N}_y(\frac{\epsilon}{2M_{\underline{x}}})\right),$$

então

$$\begin{aligned}|x_n y_n - x_m y_m| = |x_n y_n - x_n y_m + x_n y_m - x_m y_m| &\leqslant |x_n||y_n - y_m| + |x_n - x_m||y_m| \\ &< |x_n|\frac{\epsilon}{2M_{\underline{x}}} + \frac{\epsilon}{2M_{\underline{y}}}|y_m| \leqslant \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.\end{aligned}$$

Portanto $\underline{x} \cdot \underline{y}$ é Cauchy.

□

PROPOSIÇÃO 84. *Para seqüências Cauchy $\underline{x}, \underline{y} : \mathbb{N} \to \mathbb{Q}$, as seguintes afirmações são equivalentes:*

*i)* $\lim_{n\to\infty}(x_n - y_n) = 0$
*ii) Seu embaralhamento* $\underline{x} \star \underline{y}$ *é Cauchy.*

Demonstração. Sejam $\underline{x} = (x_n)$ e $\underline{y} = (y_n)$ duas seqüências Cauchy, e fixe funções $\widetilde{N}_{\underline{x}}, \widetilde{N}_{\underline{y}} : \mathbb{Q}_+ \to \mathbb{N}$ tais que

$$n, m \geqslant \widetilde{N}_{\underline{x}}(\epsilon) \quad \Longrightarrow \quad |x_n - x_m| < \epsilon,$$
$$n, m \geqslant \widetilde{N}_{\underline{y}}(\epsilon) \quad \Longrightarrow \quad |y_n - y_m| < \epsilon.$$

**i) ⇒ ii)** Suponha que i) vale. Então existe $N_{\underline{x}-\underline{y}} : \mathbb{Q}_+ \to \mathbb{N}$ tal que

$$n \geqslant N_{\underline{x}-\underline{y}}(\epsilon) \quad \Longrightarrow \quad |x_n - y_n - 0| = |x_n - y_n| < \epsilon.$$

Denote por $\underline{z} = (z_n)$ o embaralhamento $\underline{x} \star \underline{y}$, e note que

$$z_n - z_m = \begin{cases} y_{\frac{n}{2}} - y_{\frac{m}{2}} & \text{se } n, m \text{ são pares;} \\ y_{\frac{n}{2}} - x_{\frac{m+1}{2}} & \text{se } n \text{ é par e } m \text{ é ímpar;} \\ x_{\frac{n+1}{2}} - y_{\frac{m}{2}} & \text{se } m \text{ é par e } n \text{ é ímpar;} \\ x_{\frac{n+1}{2}} - x_{\frac{m+1}{2}} & \text{se } n, m \text{ são ímpares.} \end{cases}$$

Defina a função

$$\widetilde{N}_{\underline{z}} : \mathbb{Q}_+ \longrightarrow \mathbb{N}, \quad \widetilde{N}_{\underline{z}}(\epsilon) = \max\left(2\widetilde{N}_{\underline{x}}(\frac{\epsilon}{2}), 2\widetilde{N}_{\underline{y}}(\frac{\epsilon}{2}), 2N_{\underline{x}-\underline{y}}(\frac{\epsilon}{2})\right)$$

e note que se $n, m \geqslant \widetilde{N}_{\underline{z}}(\epsilon)$ e:

- $n, m$ são pares, então
$$n, m \geqslant 2\widetilde{N}_{\underline{y}}(\frac{\epsilon}{2}) \quad \Longrightarrow \quad |z_n - z_m| = |y_{\frac{n}{2}} - y_{\frac{m}{2}}| < \frac{\epsilon}{2};$$
- $n$ é par e $m$ é ímpar, então como $n, m \geqslant 2\widetilde{N}_{\underline{y}}(\frac{\epsilon}{2})$ e $m \geqslant 2N_{\underline{x}-\underline{y}}(\frac{\epsilon}{2})$, temos que
$$|z_n - z_m| = |y_{\frac{n}{2}} - x_{\frac{m+1}{2}}| \leqslant |y_{\frac{n}{2}} - y_{\frac{m+1}{2}}| + |y_{\frac{m+1}{2}} - x_{\frac{m+1}{2}}| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon;$$
- $n$ é ímpar e $m$ é par, então como $n, m \geqslant 2\widetilde{N}_{\underline{x}}(\frac{\epsilon}{2})$ e $m \geqslant 2N_{\underline{x}-\underline{y}}(\frac{\epsilon}{2})$, temos que
$$|z_n - z_m| = |x_{\frac{n+1}{2}} - y_{\frac{m}{2}}| \leqslant |x_{\frac{n+1}{2}} - x_{\frac{m}{2}}| + |x_{\frac{m}{2}} - y_{\frac{m}{2}}| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon;$$
- $n, m$ são ímpares, então
$$n, m \geqslant 2\widetilde{N}_{\underline{x}}(\frac{\epsilon}{2}) \quad \Longrightarrow \quad |z_n - z_m| = |x_{\frac{n+1}{2}} - x_{\frac{m+1}{2}}| < \frac{\epsilon}{2}.$$

Portanto $\underline{z}$ é Cauchy.

**ii) ⇒ i)** Suponha que ii) vale. Então existe $\widetilde{N}_{\underline{z}} : \mathbb{Q}_+ \to \mathbb{N}$ tal que

$$n, m \geqslant \widetilde{N}_{\underline{z}}(\epsilon) \quad \Longrightarrow \quad |z_n - z_m| < \epsilon.$$

Defina

$$N_{\underline{x}-\underline{y}} : \mathbb{Q}_+ \to \mathbb{N}, \quad N_{x,y}(\epsilon) := \begin{cases} \frac{\widetilde{N}_{\underline{z}}(\epsilon)}{2} + 1 & \text{se } \widetilde{N}_{\underline{z}}(\epsilon) \text{ é par;} \\ \frac{\widetilde{N}_{\underline{z}}(\epsilon)+1}{2} & \text{se } \widetilde{N}_{\underline{z}}(\epsilon) \text{ é ímpar.} \end{cases}$$

e observe que

$$n \geqslant N_{\underline{x}-\underline{y}}(\epsilon) \quad \Longrightarrow \quad |x_n - y_n - 0| = |x_n - y_n| < \epsilon.$$

Portanto $\underline{x} - \underline{y}$ converge a zero. □

CAPíTULO 15

# Números reais

Seja então $\mathfrak{X} \subset \mathrm{Sets}(\mathbb{N}, \mathbb{Q})$ o subconjunto de todas as seqüências Cauchy:

$$\mathfrak{X} = \{\underline{x} : \mathbb{N} \to \mathbb{Q} \mid \exists\ \widetilde{N} : \mathbb{Q}_+ \to \mathbb{N},\ n, m \geqslant \widetilde{N}(\epsilon)\ \Rightarrow\ |x_n - x_m| < \epsilon\}.$$

LEMA 85. *A relação*

$$\mathscr{R} \subset \mathfrak{X} \times \mathfrak{X}, \quad \mathscr{R} = \{(x, y) \mid x \star y \in \mathfrak{X}\}$$

*é uma relação de equivalência.*

DEMONSTRAÇÃO. Pela Proposição 84, se $\underline{x}, \underline{y} \in \mathfrak{X}$, então $\underline{x} \star \underline{y} \in \mathfrak{X}$ se e só se $\underline{x} - \underline{y}$ converge a zero. Portanto:

$\mathscr{R}$ **é reflexiva:** pois $0 = \lim_{n\to 0} 0 = \lim_{n\to 0}(x_n - x_n)$;
$\mathscr{R}$ **é simétrica:** pois $0 = \lim_{n\to 0}(x_n - y_n)$ se e só se $0 = \lim_{n\to 0}(y_n - x_n)$;
$\mathscr{R}$ **é transitiva:** pois se $0 = \lim_{n\to 0}(x_n - y_n)$ e $0 = \lim_{n\to 0}(y_n - z_n)$, então $0 = \lim_{n\to 0}(x_n - z_n) = \lim_{n\to 0}(x_n - y_n) + \lim_{n\to 0}(y_n - z_n)$ pelo Lema 81.

□

Escrevamos $[\underline{x}]$ para a classe de equivalência de $x \in \mathfrak{X}$:

$$[\underline{x}] = \{\underline{y} \in \mathfrak{X} \mid (\underline{x}, \underline{y}) \in \mathscr{R}\}.$$

Chamamos de **número real** uma tal classe de equivalência $[\underline{x}]$, e denotamos o conjunto de classes de equivalência por

$$\mathbb{R} = \{[\underline{x}] \mid \underline{x} \in \mathfrak{X}\},$$

chamado de **conjunto dos números reais**.

EXERCÍCIO 86. *Mostre que $\mathbb{R}$ é um anel comutativo sob as operações*

$$[\underline{x}] + [\underline{y}] = [\underline{x} + \underline{y}], \quad [\underline{x}] \cdot [\underline{y}] = [\underline{x} \cdot \underline{y}],$$

*e onde*

$$0 = [0, 0, 0, \cdots], \quad 1 = [1, 1, 1, \cdots].$$

Dizemos que uma função $f : \mathbb{N} \longrightarrow \mathbb{N}$ é **estritamente crescente** se $f(n+1) > f(n)$ para todo $n \in \mathbb{N}$.

LEMA 87. *Para toda seqüência Cauchy $\underline{x} = (x_n)$, e função estritamente crescente $f : \mathbb{N} \to \mathbb{N}$, $\underline{y} = (x_{f(n)})$ é Cauchy e $[\underline{x}] = [\underline{y}]$.*

DEMONSTRAÇÃO. Da hipótese de $f$ ser estritamente crescente, segue que $f(n) \geqslant n$ para todo $n$. Portanto se

$$n, m \geqslant \widetilde{N}_x(\epsilon) \quad \Longrightarrow \quad |x_n - x_m| < \epsilon,$$

então

$$n, m \geqslant \widetilde{N}_x(\epsilon) \quad \Longrightarrow \quad |y_n - y_m| = |x_{f(n)} - x_{f(m)}| < \epsilon,$$

Logo $y = (x_{f(n)})$ é Cauchy. Além disso,

$$n \geqslant \widetilde{N}_x(\epsilon) \quad \Longrightarrow \quad |y_n - x_n| = |x_{f(n)} - x_n| < \epsilon$$

mostra que $x$ e $y$ são equivalentes sob a relação de equivalência $\mathscr{R}$. □

PROPOSIÇÃO 88. $\mathbb{R}$ *é um corpo.*

DEMONSTRAÇÃO. Basta mostrar que se $x \in \mathfrak{X}$ é tal que $[x] \neq 0$, então existe $y \in \mathfrak{X}$ tal que $[xy] = [x][y] = 1$. Note que $[x] \neq 0$ significa que zero não é limite de $x = (x_n)$. Portanto, para todo $\delta \in \mathbb{Q}_+$ e $n \in \mathbb{N}$, existe $m \geqslant n$ com $|x_m| \geqslant \delta$. Defina $f : \mathbb{N} \to \mathbb{N}$ indutivamente por

$$f(1) := \min\{n \mid |x_n| \geqslant \delta\}, \quad f(n) = \min\{n \mid |x_n| \geqslant \delta,\ n \neq f(1), ..., f(n-1)\}.$$

Então $f$ é estritamente crescente. Portanto $y = (x_{f(n)})$ nunca se anula, e pelo Lema 87, $y$ é Cauchy e equivalente a $x$. Portanto $z = (\frac{1}{y_n})$ está definida. $z$ é Cauchy, pois se

$$\widetilde{N}_z : \mathbb{Q}_+ \longrightarrow \mathbb{N}, \quad \widetilde{N}_z(\epsilon) := \widetilde{N}_y(\epsilon\delta^2),$$

então

$$|z_n - z_m| = \left|\frac{1}{y_n} - \frac{1}{y_m}\right| = \left|\frac{y_m - y_n}{y_n y_m}\right| = \frac{|y_m - y_n|}{|y_n y_m|} \leqslant \frac{|y_m - y_n|}{\delta^2} < \epsilon.$$

Além disso,

$$[x][z] = [y][z] = [x_{f(n)} \frac{1}{x_{f(n)}}] = 1.$$

Portanto $[z] \in \mathbb{R}$ é a inversa multiplicativa de $[x]$. □

Dizemos que uma seqüência Cauchy $\underline{x} \in \mathfrak{X}$ é **alfim positiva** se $[\underline{x}] \neq 0$, e existe $N \in \mathbb{N}$ tal que

$$n \geqslant N \quad \Longrightarrow \quad x_n > 0.$$

LEMA 89. *Seja* $\mathbb{R}_+ \subset \mathbb{R}$ *o subconjunto*

$$\mathbb{R}_+ = \{[\underline{x}] \mid \underline{x} \ \text{ é alfim positiva}\}.$$

*Então* $[\underline{x}], [\underline{y}] \in \mathbb{R}_+$ *implica que* $[\underline{x} + \underline{y}]$ *e* $[\underline{x} \cdot \underline{y}]$ *estão em* $\mathbb{R}_+$*. Além disso, a relação*

$$\mathscr{O} \subset \mathbb{R} \times \mathbb{R}, \quad \mathscr{O} = \{([\underline{x}], [\underline{y}]) \mid [\underline{x}] = [\underline{y}] \text{ ou } [\underline{y} - \underline{x}] \in \mathbb{R}_+\}$$

*define uma ordem em* $\mathbb{R}$*.*

DEMONSTRAÇÃO. Se $x_n > 0$ para $n \geqslant N$ e $y_n > 0$ para $n \geqslant N'$, então $x_n + y_n > 0$ e $x_n y_n > 0$ para $n \geqslant \max(N, N')$. Portanto $[\underline{x} + \underline{y}], [\underline{x} \cdot \underline{y}] \in \mathbb{R}_+$. Verificamos que $\mathscr{O}$ é uma pre-ordem:

**reflexiva:** pois $([\underline{x}], [\underline{x}]) \in \mathscr{O}$ para todo $[\underline{x}] \in \mathbb{R}$ por definição;
**anti-simétrica:** pois se $([\underline{x}], [\underline{y}]) \in \mathscr{O}$ e $([\underline{y}], [\underline{x}]) \in \mathscr{O}$, então se $[\underline{y}] \neq [\underline{x}]$, teríamos que tanto $\underline{x} - \underline{y}$ quanto $\underline{y} - \underline{x}$ são alfim positivas, o que é impossível.
**transitiva:** pois se $([\underline{x}], [\underline{y}]) \in \mathscr{O}$ e $([\underline{y}], [\underline{z}]) \in \mathscr{O}$, então $([\underline{x}], [\underline{z}]) \in \mathscr{O}$ pois $\mathbb{R}_+$ é fechado sob adição.

Para verificar que a pre-ordem $\mathscr{O}$ é uma ordem, note que se $[\underline{x}] \neq 0$, então podemos supor sem perda de generalidade que nenhum $x_n$ é zero — e portanto sao todos positivos (em cujo caso $[\underline{x}] \in \mathbb{R}_+$) ou são todos negativos (em cujo caso $-[\underline{x}] \in \mathbb{R}_+$). Portanto dados $[\underline{x}], [\underline{y}] \in \mathbb{R}$ distintos, temos que ou $[\underline{y}] - [\underline{x}] \in \mathbb{R}_+$ (em cujo caso $[\underline{x}] < [\underline{y}]$), ou $[\underline{x}] - [\underline{y}] \in \mathbb{R}_+$ (em cujo caso $[\underline{y}] < [\underline{x}]$). □

DEFINIÇÃO 90. *O* **valor absoluto** $|x|$ *de* $x \in \mathbb{R}$ *é* $x$ *se* $x \geqslant 0$*, e* $-x$ *se* $x \leqslant 0$*.*

EXERCÍCIO 91. *Mostre que, para quaisquer* $x, y \in \mathbb{R}$*, temos que*

*a)* $|x + y| \leqslant |x| + |y|$*;*
*b)* $|xy| = |x||y|$*.*

PROPOSIÇÃO 92. *Existe uma função injetora (canônica)*

$$i : \mathbb{Q} \longrightarrow \mathbb{R}, \quad i(a) = [a, a, a, \cdots],$$

*tal que*

$$i(a + b) = i(a) + i(b), \quad i(a \cdot b) = i(a) \cdot i(b).$$

*Além disso, sua imagem é* **densa**, *no sentido que, dados* $x \in \mathbb{R}$ *e* $\epsilon \in \mathbb{Q}_+$, *existe* $a \in \mathbb{Q}$, *tal que* $|x - a| < \epsilon$.

DEMONSTRAÇÃO. $i$ é claramente injetora, pois $i(a) = 0$ se e só se $a = 0$. Que $i(a+b) = i(a)+i(b)$ e $i(a\cdot b) = i(a)\cdot i(b)$ segue das definicoes. Seja agora $x = [\underline{x}] \in \mathbb{R}$ e $\epsilon \in \mathbb{Q}_+$. Então existe $N(\epsilon) \in \mathbb{N}$ tal que $|x_n - x_m| < 2\epsilon$ se $n, m \geqslant N(\epsilon)$; portanto $|x - x_n| < \epsilon$ se $n \geqslant N(\epsilon)$. □

Portanto $\mathbb{Q}$ está incluído em $\mathbb{R}$, e suas operações de anel comutativo são aquelas de $\mathbb{R}$.

Os conceitos de seqüências Cauchy e limites se estendem imediatamente aos números reais:

— Uma seqüência $\underline{x} : \mathbb{N} \to \mathbb{R}$ **converge** a $\alpha \in \mathbb{R}$ se existe $N : \mathbb{R}_+ \to \mathbb{N}$, tal que $|\alpha - x_n| < \epsilon$ sempre que $n \geqslant N(\epsilon)$, em cujo caso $\alpha$ é o **limite** de $\underline{x}$, e escrevemos

$$\alpha = \lim_{n\to\infty} x_n;$$

— Uma seqüência $\underline{x} : \mathbb{N} \to \mathbb{R}$ é **Cauchy** se existe $N : \mathbb{R}_+ \to \mathbb{N}$, tal que $|x_n - x_m| < \epsilon$ sempre que $n, m \geqslant N(\epsilon)$.

LEMA 93. *Se* $\underline{x} : \mathbb{N} \to \mathbb{Q}$ *é Cauchy, então* $i \circ \underline{x} : \mathbb{N} \to \mathbb{Q}$ *converge a* $[\underline{x}] \in \mathbb{R}$*:*

$$\lim_{n\to\infty} x_n = [\underline{x}].$$

DEMONSTRAÇÃO. Seja $\widetilde{N} : \mathbb{Q}_+ \to \mathbb{N}$ tal que $|x_n - x_m| < \epsilon$ se $n, m \geqslant \widetilde{N}(\epsilon)$. Então

$$n \geqslant \widetilde{N}(\frac{\epsilon}{2}) \quad \Longrightarrow \quad |[\underline{x}] - x_n| < \epsilon.$$

Portanto $\lim_{n\to\infty} x_n = [\underline{x}]$. □

PROPOSIÇÃO 94. *Em* $\mathbb{R}$, *toda seqüência Cauchy converge.*

DEMONSTRAÇÃO. Seja $\underline{x} : \mathbb{N} \to \mathbb{R}$ uma seqüência Cauchy, e seja $N : \mathbb{R}_+ \to \mathbb{N}$ tal que

$$n, m \geqslant N(\epsilon) \quad \Longrightarrow \quad |x_n - x_m| < \epsilon.$$

Cada $x_n$ é um número real, e podemos escolher uma sequencia Cauchy $\underline{x_n} : \mathbb{N} \to \mathbb{Q}$, tal que $x_n = [\underline{x_n}]$. Sem perda de generalidade, podemos supôr que

$$|x_{n,p} - x_n| < 10^{-p}.$$

Defina então a seqüência

$$\underline{z} : \mathbb{N} \longrightarrow \mathbb{Q}, \quad z_n = x_{n,n},$$

e seja $N_{\underline{z}} : \mathbb{Q}_+ \longrightarrow \mathbb{N}$ uma função tal que

$$10^{N_{\underline{z}}(\epsilon)}\epsilon > 3N(\epsilon).$$

Então se $n, m \geqslant N_{\underline{z}}$, temos que

$$\begin{aligned} |z_n - z_m| &= |x_{n,n} - x_{m,m}| \\ &= |(x_{n,n} - x_n) + (x_n - x_m) + (x_m - x_{m,m})| \\ &\leqslant |x_{n,n} - x_n| + |x_n - x_m| + |x_m - x_{m,m}| \\ &< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon. \end{aligned}$$

Portanto $\underline{z}$ é Cauchy, $\alpha := [\underline{z}] \in \mathbb{R}$, e

$$\lim_{n\to\infty} z_n = \alpha.$$

Porém

$$|z_n - x_n| < 10^{-n} \quad \Longrightarrow \quad \lim_{n\to\infty} z_n = \lim_{n\to\infty} x_n = \alpha.$$

Logo $\underline{x}$ converge a $\alpha \in \mathbb{R}$. □

CAPíTULO 16

# Expansões decimais

Um **dígito** é um elemento de

$$\mathscr{D} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

PROPOSIÇÃO 95. *Sejam $p \in \mathbb{Z}$ e $q \in \mathbb{N}$.*

*a) Existe um único inteiro $k \in \mathbb{Z}$ e uma única seqüência de dígitos $\underline{a} : \mathbb{N} \to \mathscr{D}$, tal que*

$$0 \leqslant p - \left( k + \sum_{i=1}^{n} 10^{-i} a_i \right) q < 10^{-n} q.$$

*para todo inteiro não-negativo $n$;*

*b) A sequencia de dígitos $\underline{a}$ é alfim periódica.*

DEMONSTRAÇÃO. a) Por divisão com resto temos únicos $k \in \mathbb{Z}$ e $\varrho \in \mathbb{N}$, tais que

$$p = kq + \varrho, \quad 0 \leqslant \varrho < q.$$

Analogamente, para cada $n \in \mathbb{N}$, por divisão com resto temos únicos $K_n \in \mathbb{Z}$ e $r_n \in \mathbb{N}$, tais que

$$10^n p = K_n q + r_n, \quad 0 \leqslant r_n < q.$$

Interpretamos esses dados como definindo seqüências

$$\underline{K} : \mathbb{N} \longrightarrow \mathbb{Z}, \quad \underline{r} : \mathbb{N} \longrightarrow \mathscr{D}.$$

Observe que

$$K_n q + r_n = 10^n p = 10(10^{n-1} p) = 10(K_{n-1} q + r_{n-1})$$

implica que

$$(K_n - 10K_{n-1})q = 10r_{n-1} - r_n.$$

o que por sua vez implica que

$$10r_{n-1} = a_n q + r_n$$

para algum $a_n \in \mathbb{Z}$. Como $q, r_{n-1}, r_n$ são não-negativos, segue que $a_n \geqslant 0$. Afirmamos que $a_n < 10$. De fato, é suficiente notar que se $a_n = 10 + j$, então

$$10(r_{n-1} - q) - jq = r_n;$$

como $r_n \geqslant 0$ e $r_{n-1} - q < 0$, segue que $j < 0$. Portanto $a_n \in \mathscr{D}$, e

$$K_n = 10K_{n-1} + a_n.$$

Portanto

$$K_n = 10^n k + 10^{n-1} a_1 + 10^{n-2} a_2 + \cdots + a_n = 10^n k + \sum_{i=1}^{n} 10^{n-i} a_i$$

e logo

$$p = \left( k + \sum_{i=1}^{n} 10^{-i} a_i \right) q + r_n 10^{-n}, \quad 0 \leqslant r_n < q.$$

b) Observe também que $a_n, r_n$ podem ser definidos indutivamente por

$$10r_n = a_{n+1}q + r_{n+1};$$

essa última expressão implica que, se existe $s \in \mathbb{N}$ tal que $r_{N+s} = r_N$ para algum $N \in \mathbb{N}$, então $r_{n+s} = r_n$ para todo $n \geqslant N$. Portanto $a_{n+s} = a_n$ para todo $n \geqslant N$ — isto é, $\underline{a}$ é alfim periódica.

□

Uma **expansão decimal** é um elemento de

$$\mathscr{E} := \mathbb{Z} \times \mathrm{Sets}(\mathbb{N}, \mathscr{D});$$

ou seja, é um par $e = (k, \underline{a})$, onde $k \in \mathbb{Z}$ é um inteiro, e $\underline{a} : \mathbb{N} \to \mathscr{D}$ é uma seqüência de dígitos. Pensamos em uma expansão decimal $e$ como uma expressão de uma das seguintes formas:

$$e = k + \sum_{i=1}^{\infty} a_i 10^{-i} = k.a_1a_2a_3\cdots a_n\cdots .$$

Note que a Proposição 95 diz que existe uma função (canônica)

$$G : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathscr{E}, \quad G(p,q) = (k, \underline{a}) = k + \sum_{i=1}^{\infty} a_i 10^{-i},$$

unicamente determinada pela condição:

$$0 \leqslant p - \left(k + \sum_{i=1}^{n} 10^{-i} a_i\right) q < 10^{-n} q, \quad n \in \mathbb{N},$$

e além disso, $\underline{a}$ é alfim periódica.

Exemplo 44. *Considere $p = 17$ e $q = 13$. Então:*

$$\begin{aligned}
17 &= 13 \cdot 1 + 4 \\
40 &= 13 \cdot 3 + 1 \\
10 &= 13 \cdot 0 + 10 \\
100 &= 13 \cdot 7 + 9 \\
90 &= 13 \cdot 6 + 12 \\
120 &= 13 \cdot 9 + 3 \\
30 &= 13 \cdot 2 + 4 \\
40 &= 13 \cdot 3 + 1 \\
10 &= 13 \cdot 0 + 10 \\
100 &= 13 \cdot 7 + 9 \\
90 &= 13 \cdot 6 + 12 \\
120 &= 13 \cdot 9 + 3 \\
30 &= 13 \cdot 2 + 4 \\
&\vdots
\end{aligned}$$

*mostra que se*

$$\alpha = 3 \cdot 10^5 + 0 \cdot 10^4 + 7 \cdot 10^3 + 6 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0,$$

*então*

$$0 \leqslant 17 - (1 + \alpha + \alpha^2 + \cdots + \alpha^n) < 10^{-5n} \cdot 13$$

*Note que a seqüência de dígitos correspondente $\underline{a}$ é* periódica*:*

$$a_1 = 3, \quad a_2 = 0, \quad a_3 = 7, \quad a_4 = 6, \quad a_5 = 9, \quad a_6 = 2, \quad a_{n+6} = a_n.$$

Observação 96. *Note que nem toda seqüência $\underline{a}$ alfim periódica está na imagem de $G$. Por exemplo, se*

$$e = \sum_{i=1}^{\infty} 9 \cdot 10^{-i}$$

*nao há $(p, q) \in \mathbb{Z} \times \mathbb{N}$ tal que $G(p, q) = e$. De fato, se houvesse tal $(p, q)$, teríamos*

$$p = q0 + r_0, \quad 10r_{n-1} = 9q + r_n, \quad n \in \mathbb{N}$$

*o que implica que*

$$10^n(r_0 - r_1) = r_n - r_{n+1}.$$

*Como $0 \leqslant r_n < q$, isso implica que $r_0 = r_n =: r$ para todo $n$ logo*

$$10r = 9q + r \quad \Longrightarrow \quad r = q,$$

*o que contradiz a escolha de $r < q$.*

Lema 97. *Existe uma função injetora (canônica)*

$$F : \mathscr{E} \longrightarrow \mathfrak{X}$$

*de expansões decimais em seqüências Cauchy de números racionais.*

Demonstração. Dada expansão decimal $e = m + \sum_{i=1}^{\infty} a_i 10^{-i}$, defina a seqüência $F(e) : \mathbb{N} \to \mathbb{Q}$ por

$$F(e)_n := k + \sum_{i=1}^{n} a_i 10^{-i} \in \mathbb{Q}.$$

Para ver que ela é injetora, note que se $e = (k, \underline{a})$ e $e' = (k', \underline{a'})$ são duas expansões decimais, e $F(e) = F(e')$, então

$$\lfloor F(e)_1 \rfloor = \lfloor F(e')_1 \rfloor \quad \Longrightarrow \quad k = k', \quad a_1 = F(e)_1 - k = F(e')_1 - k' = a'_1,$$

e além disso,

$$a_n = F(e)_n - F(e)_{n-1} = F(e')_n - F(e')_{n-1} = a'_n, \quad n > 1.$$

Portanto $\underline{a} = \underline{a'}$, e logo $e = e'$.

Para ver que $F(e)$ é Cauchy para todo $e \in \mathscr{E}$, note que

$$|F(e)_n - F(e)_m| = \left| \sum_{i=\min(n,m)+1}^{\max(n,m)} a_i 10^{-i} \right| < 10^{-\min(n,m)}$$

Portanto se $N : \mathbb{Q}_+ \to \mathbb{N}$ é tal que $10^{N(\epsilon)}\epsilon > 1$, então

$$n, m \geqslant N(\epsilon) \quad \Longrightarrow \quad |F(e)_n - F(e)_m| < 10^{-N(\epsilon)} < \epsilon.$$

Logo $F(e)$ é Cauchy. □

Dizemos que um número real $\alpha \in \mathbb{R}$ **tem uma expansão decimal** $e \in \mathscr{E}$ se $\alpha$ é representado por $F(e)$: $\alpha = [F(e)]$.

Lema 98. *Todo número real $\alpha \in \mathbb{R}$ tem uma expansão decimal.*

Demonstração. Seja $\alpha \in \mathbb{R}$ o número real representado por uma seqüência Cauchy $(x_n)$. Então para cada $s \in \mathbb{N}$, temos $N(10^{-s}) \in \mathbb{N}$, tal que

$$n, m \geqslant N(10^{-s}) \quad \Longrightarrow \quad |x_n - x_m| < 10^{-s}.$$

Então a seqüência

$$y_n := x_{N(10^{-n})}$$

é Cauchy, e pelo Lema 87, $[\underline{y}] = [\underline{x}]$. Observe que

$$|y_n - y_m| < 10^{-\min(n,m)}$$

por construção, e portanto

$$|y_n - \alpha| < 10^{-n}.$$

Defina $k \in \mathbb{Z}$, $0 \leqslant \varrho_0 < 1$ de modo que $\alpha = k + \varrho_0$. Defina também seqüências $a_n \in \mathscr{D}$, $0 \leqslant \varrho_n < 1$ de forma que

$$10\varrho_n = a_{n+1} + \varrho_{n+1}$$

Então

$$e = k + \sum_{i=1}^{\infty} a_i 10^{-i} \ \in \ \mathscr{E}$$

é uma expansão decimal. Afirmamos que $F(e)$ converge a $\alpha$. De fato, observe que, para todo $n \in \mathbb{N}$, temos que

$$10^n \alpha = (10^n k + 10^{n-1} a_1 + \cdots + a_n) + \varrho_n,$$

e portanto

$$\left| \alpha - (k + \sum_{i=1}^{n} 10^{-i}) \right| = 10^{-n} \varrho_n < 10^{-n}$$

implica que

$$\left| y_n - (k + \sum_{i=1}^{n} 10^{-i}) \right| < 2 \cdot 10^{-n}$$

Portanto a seqüência $y - F(e)$ converge a zero: basta tomar $N : \mathbb{Q}_+ \to \mathbb{N}$ tal que $10^{N(\epsilon)}\epsilon > 2$ para que

$$n \geqslant N(\epsilon) \quad \Longrightarrow \quad |y_n - F(e)_n| < \epsilon.$$

Assim concluímos que $\alpha = [F(e)]$. □

Proposição 99. *Um número real $\alpha \in \mathbb{R}$ tem duas expansões decimais distintas se e só se $10^l \alpha \in \mathbb{Z}$ para algum $l \in \mathbb{N}$, em cujo caso $\alpha$ é representado por exatamente duas expansões decimais*

$$e = k + \sum_{i=1}^{\infty} a_i 10^{-i}, \quad e' = k' + \sum_{i=1}^{\infty} a'_i 10^{-i},$$

*que coincidem nos primeiros $s-1$ termos, e*

- $a_s = a'_s + 1$*;*
- $a_{s+n} = 0$ *para todo* $n \in \mathbb{N}$*;*
- $a'_{s+n} = 9$ *para todo* $n \in \mathbb{N}$*.*

Demonstração. Sejam

$$e = k + \sum_{i=1}^{\infty} a_i 10^{-i}, \quad e' = k' + \sum_{i=1}^{\infty} a'_i 10^{-i},$$

duas expansões decimais distintas que representam o mesmo número real $\alpha \in \mathbb{R}$. Sem perda de generalidade, podemos supor que (A) ou $k > k'$, ou (B) que $k = k'$ e, para algum $s \in \mathbb{N}$, $a_i = a_i$ para todo $i < s$ e $a_s > a_{s-1}$.

Passo 1: Redução ao caso (A) com $k' = 0$ e $k = 1$. Se vale o caso (B), então defina

$$\beta = k + \sum_{i=1}^{s-1} a_i 10^{s-i},$$

e note que $\widetilde{\alpha} := 10^s \alpha - \beta - a'_s \in \mathbb{R}$ é representado por

$$(a_s - a'_s) + \sum_{i=1}^{\infty} a_{i+s} 10^{-i}, \quad 0 + \sum_{i=1}^{\infty} a'_{i+s} 10^{-i}.$$

Note que, se $k > 1$, então

$$\left|\sum_{i=1}^{n}(a'_i - a_i)\right| > 1,$$

o que contradiria a hipótese de que ambos representam o mesmo $\widetilde{\alpha} \in \mathbb{R}$. Portanto $k = 1$.

Passo 2 Duas expansões decimais da forma

$$1 + \sum_{i=1}^{\infty} a_i 10^{-i}, \quad 0 + \sum_{i=1}^{\infty} a'_i 10^{-i}.$$

representam o mesmo $\alpha \in \mathbb{R}$ se e só se

$$0 = \lim_{n\to\infty}(1 + \sum_{i=1}^{n}(a_i - a'_i))10^{-i},$$

o que implica que

$$\lim_{n\to\infty}\sum_{i=1}^{n} b_i 10^{-i} = 1, \quad b_i := a'_i - a_i$$

Note que cada $b_n$ é não-negativo, pois se $a'_N < a_N$ para algum $N \in \mathbb{N}$, então os números reais representados por essas expansões difeririam por pelo menos $10^{-N}$. Portanto somos levados a determinar todas as seqüências de dígitos $\underline{b} : \mathbb{N} \to \mathscr{D}$, tais que

$$0 + \sum_{i=1}^{\infty} b_i 10^{-i}$$

representada o número 1. Ora, a seqüência $b_n = 9$ cumpre essa propriedade:

$$\lim_{n\to\infty}\sum_{i=1}^{\infty} 9 \cdot 10^{-i} = 1,$$

e se uma seqüência $b'_n$ é tal que $b'_N \neq 9$ para algum $N \in \mathbb{N}$, então o número real por ela representado é $\leqslant 1 - 10^{-N}$. Portanto $b_n = 9$ á a única tal seqüência de dígitos; como $a'_n, a_n$ são dígitos, segue que $a'_n = 9$ e $a_n = 0$ para cada $n \in \mathbb{N}$. Daqui concluímos que $\widetilde{\alpha} = 1$, e portanto

$$10^s\alpha = (1 + a'_s) + \beta \in \mathbb{Z}.$$

Portanto se $\alpha$ tem duas expansões decimais distintas, $10^s\alpha \in \mathbb{Z}$ e há exatamente duas expansões.

Reciprocamente, $\frac{m}{10^l}$ é representado simultaneamente por

$$m \cdot 10^{-l} + \sum_{i=1}^{\infty} 0 \cdot 10^{-i-l}, \quad (m-1) \cdot 10^{-l} + \sum_{i=1}^{\infty} 9 \cdot 10^{-i-l}$$

□