

UNIVERSIDADE FEDERAL DO AMAZONAS  
INSTITUTO DE CIÊNCIAS EXATAS  
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA  
MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

*Enumerabilidade e Não-Enumerabilidade de Conjuntos: Uma Abordagem  
para O Ensino Básico*

Rogério Jacinto de Moraes Júnior

MANAUS

2015

UNIVERSIDADE FEDERAL DO AMAZONAS  
INSTITUTO DE CIÊNCIAS EXATAS  
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA  
PROGRAMA DE MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

Rogério Jacinto de Moraes Júnior

*ENUMERABILIDADE E NÃO ENUMERABILIDADE DE CONJUNTOS,  
UMA ABORDAGEM PARA O ENSINO BÁSICO*

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

MANAUS  
2015

ROGÉRIO JACINTO DE MORAES JÚNIOR

ENUMERABILIDADE E NÃO ENUMERABILIDADE DE CONJUNTOS,  
UMA ABORDAGEM NO ENSINO BÁSICO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em 15 de Maio de 2015.

BANCA EXAMINADORA

Prof. Dr. Nilomar Vieira de Oliveira  
Presidente

Prof. Dr. Roberto Antônio Cordeiro Prata  
Membro

Prof. Dr. Alcides de Castro Amorim Neto  
Membro

# AGRADECIMENTOS

A Deus, pelo dom da vida e bênçãos a mim concedidas por sempre guiar meus passos para realizar com sucesso os meus objetivos.

A meus pais Rogério e Maria das Graças pelos momentos de plenitude e apoio familiar incondicionais. A vocês, minha eterna gratidão.

A meu filho Davi Teles de Moraes a quem devo servir de exemplo como pai e como profissional.

Ao meu orientador, Prof. Dr. Nilomar Vieira de Oliveira, por ter confiado no nosso trabalho, por ter dedicado horas do seu precioso tempo para as orientações, correções e o aperfeiçoamento do TCC. Obrigado pelas horas e apoio disponibilizados.

A Universidade Federal do Amazonas, seu corpo docente, direção e administração que oportunizaram o PROFMAT que foi de um crescimento significativo na minha vida pessoal, profissional e intelectual.

Enfim, agradeço aos amigos pelo companheirismo nas árduas vitórias conquistadas e todas as pessoas que, direta ou indiretamente, contribuíram para a execução dessa Dissertação de Mestrado.

## RESUMO

Neste trabalho abordaremos alguns assuntos tratados brevemente durante o curso de graduação tais como enumerabilidade e não enumerabilidade de conjuntos, cardinalidade e outros assuntos correlatos. Apresentaremos um pequeno aparato histórico que deram origem a esses problemas, assim como as pessoas que lançaram conhecimento sobre tais temas. O objetivo é apresentar sucintamente aos professores do ensino básico suporte para as aulas, dando a oportunidade do professor ter mais segurança quando trabalhar com conjuntos numéricos. Também servirá como elemento motivacional tanto para professores como para os alunos interessados, pois trata de assuntos curiosos e atípicos para quem gosta de estudar matemática, como comparar a cardinalidade de conjuntos infinitos, a infinidade de números transcendentos e sua dificuldade de determiná-los e outros assuntos que são de grande riqueza de pesquisa na matemática moderna. Dessa forma pensamos estar contribuindo para o aperfeiçoamento de professores e alunos do ensino básico.

Palavras-chave: Ensino -Aprendizagem, Enumerabilidade e Não-enumerabilidade, Cardinalidade, Hipótese do Contínuo.

# ABSTRACT

In this dissertation we discuss briefly some issues quickly treated during the undergraduate course such as countable and uncountable sets, cardinality and other related subjects. We will present a brief historical review of the facts that gave rise to these problems, as well as people who have developed knowledge on these issues. The purpose of this report is succinctly present a direction to the Basic Education teachers for their classes, giving the opportunity to teachers to have more confidence when working with numerical sets and functions on these sets. It will also be used as a motivational element to the theoretical approach, or this associated with the problems that gave rise to such issues, both for teachers, and for students and scholars interested, because these are curious and intriguing subjects for those which enjoy studying mathematics of such subjects that are, of some kind, advanced or abstract. Among others, we can assign the comparison of cardinality of infinite sets, demonstrating that sets of rational numbers and the algebraic numbers are countable, and the real numbers and the transcendental numbers are uncountable, and besides, we show the cardinality of other interesting sets that are of great value to research in modern mathematics. Thus we think we are contributing to the improvement of teachers and students of Basic Education.

Keywords: Teaching-Learning, Countable and Non-countable Cardinality,  
The Continuum Hypothesis.

# Sumário

<b>1</b>	<b>Fundamentação Teórica</b>	<b>1</b>
1.1	Conjuntos . . . . .	1
1.2	Conjuntos Numéricos . . . . .	2
1.2.1	Conjunto dos naturais, inteiros e racionais . . . . .	2
1.2.2	Conjunto dos números reais . . . . .	5
1.3	Produto Cartesiano . . . . .	8
1.4	Relações e funções . . . . .	9
1.5	Classificação da Funções . . . . .	11
1.5.1	Funções Injetivas e Sobrejetivas . . . . .	11
1.5.2	Funções Compostas . . . . .	15
<b>2</b>	<b>Cardinalidade dos Conjuntos</b>	<b>19</b>
2.1	Uma breve reflexão sobre conjuntos e paradoxos . . . . .	19
2.2	O Conjunto dos Números Naturais . . . . .	23
2.2.1	Destaque para o axioma da Indução . . . . .	24
2.2.2	Ordem entre os números naturais . . . . .	31
2.2.3	Conjunto finitos e conjuntos infinitos . . . . .	32
2.2.4	Um pouco mais sobre conjuntos infinitos . . . . .	34
2.2.5	Notas históricas sobre teoria dos conjuntos . . . . .	36
<b>3</b>	<b>Conjuntos enumeráveis</b>	<b>44</b>
3.1	Uma forma de construir enumerabilidade . . . . .	44
3.2	Exemplos de conjuntos enumeráveis . . . . .	49
3.2.1	Enumerabilidade de $\mathbb{N}$ , $\mathbb{Z}$ e seus subconjuntos . . . . .	49
3.2.2	Enumerabilidade das $n$ -uplas e do conjunto $\mathbb{Q}$ pela tabela de Cantor . . . . .	50
3.2.3	Enumerabilidade do produto cartesiano de qualquer conjunto enumerável . . . . .	55
3.2.4	Enumerabilidade do conjunto dos polinômios com coeficiente em $\mathbb{Z}$ . . . . .	57
3.2.5	Enumerabilidade das sequências finitas de inteiros positivos . . . . .	58
3.2.6	Enumerabilidade dos subconjuntos de conjuntos enumeráveis . . . . .	60
3.3	Números algébricos e transcendentos . . . . .	62
3.3.1	Números algébricos . . . . .	62

3.3.2	Enumerabilidade do conjunto dos números algébricos . . . . .	62
3.3.3	Os números transcendentos . . . . .	63
<b>4</b>	<b>Conjuntos não enumeráveis</b>	<b>64</b>
4.1	A irracionalidade do número $e$ e $\pi$ . . . . .	64
4.1.1	O número $e$ é irracional . . . . .	64
4.1.2	O número $\pi$ é irracional . . . . .	65
4.2	A Não-Enumeráveis de alguns conjuntos . . . . .	68
4.2.1	O conjunto das partes de $\mathbb{N}$ não é enumerável . . . . .	68
4.2.2	O conjunto dos números reais não é enumerável . . . . .	68
4.2.3	Um pouco mais sobre os números transcendentos . . . . .	72
4.2.4	Conjunto de Cantor não é enumerável . . . . .	73
4.3	A Hipótese do Contínuo e sua impossibilidade de demonstração . . . . .	76
4.3.1	A Hipótese do Continuo . . . . .	79
<b>5</b>	<b>Considerações Finais</b>	<b>81</b>
	<b>Referências Bibliográficas</b>	<b>82</b>



# LISTA DE SÍMBOLOS

$\in$	Pertence.
$\notin$	Não pertence.
$=$	Igualdade.
$\neq$	Diferente.
$<$	Menor.
$>$	Maior.
$\leq$	Menor ou igual.
$\geq$	Maior ou igual.
$\subset$	Contido.
$\supset$	Contém.
$A \times B$	O produto cartesiano de $A$ e $B$ .
$A \sim B$	$A$ é equipotente (ou mesma cardinalidade) de $B$ .
$\#A$	Cardinalidade do conjunto $A$ .
$\mathcal{P}(M)$	Conjunto das partes de $M$ .
$\aleph_0$	Cardinalidade dos Inteiros.
$\aleph_1$	Cardinalidade dos Reais.

# Capítulo 1

## Fundamentação Teórica

### 1.1 Conjuntos

O conceito de conjunto aparece em todos os ramos da Matemática. Intuitivamente, um conjunto é qualquer coleção bem definida de objetos ou seres e será aqui designado por letras maiúsculas  $A, B, C, \dots, Z$ . Os objetos ou seres que constituem um conjunto serão designados por letras minúsculas,  $a, b, c, \dots, z$ . A afirmação “ $p$  é elemento de  $A$ ” ou, equivalentemente, “ $p$  pertence a  $A$ ”, escreve-se

$$p \in A.$$

A negação de  $p \in A$  escreve-se  $p \notin A$ .

Há, essencialmente, duas maneiras de especificar um dado conjunto. Uma delas consiste em enumerar (quando possível) seus elementos. Por exemplo,

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

representa o conjunto  $A$ , cujos os elementos são as letras  $a, e, i, o, u$ . Observa-se que os elementos vêm separados por vírgulas e incluídos entre chaves  $\{\}$ . A outra maneira de caracterizar um conjunto consiste em dar as propriedades que caracterizam seus elementos. Por exemplo

$$B = \{x; \text{inteiro}, x > 0\}$$

(lê-se: “ $B$  é o conjunto dos elementos  $x$  tais que  $x$  é inteiro e  $x$  é maior do que zero”) representa o conjunto dos inteiros positivos. Emprega-se uma letra minúscula, geralmente  $x$ , para representar um elemento arbitrário do conjunto; ponto e vírgula equivalem a “tal que”, e a vírgula corresponde à conjunção “e”.

**Exemplo 1.1.** O conjunto  $B$  acima pode também escrever-se  $B = \{1, 2, 3, \dots\}$ . Note que  $-6 \notin B, 3 \in B$  e  $\pi \notin B$ .

**Exemplo 1.2.** Aparecem com frequência, em Matemática, os intervalos na reta, a seguir definidos.  $a$  e  $b$  são números reais,  $a < b$ .

Intervalos abertos de extremos  $a$  e  $b$ :  $(a, b) = \{x; a < x < b\}$

Intervalos fechado de extremos  $a$  e  $b$ :  $[a, b] = \{x; a \leq x \leq b\}$

Intervalos semi abertos a esquerda, de extremos  $a$  e  $b$ :  $(a, b] = \{x; a < x \leq b\}$

Intervalos semi abertos a direita, de extremos  $a$  e  $b$ :  $[a, b) = \{x; a \leq x < b\}$

Dois conjuntos  $A$  e  $B$  são iguais, o que se representa por  $A = B$ , quando constituídos dos mesmos elementos, ou seja, quando cada membro de  $A$  pertence a  $B$  e cada membro de  $B$  pertence a  $A$ . A negação de  $A = B$  escreve-se  $A \neq B$ .

**Exemplo 1.3.** Seja  $E = \{x : x^2 - 3x + 2 = 0\}$ ,  $F = \{2, 1\}$  e  $G = \{1, 2, 2, 1\}$ . Então,  $E = F = G$ . Nota-se que um conjunto não depende da maneira como seus elementos nele comparecem. Um conjunto permanece o mesmo se seus elementos se repetem ou se dispõem de maneira diferente.

**Definição 1.1.** Os conjuntos podem ser *finitos* ou *infinitos*. Um conjunto é finito se consiste em  $n$  elementos diferentes, sendo  $n$  inteiros positivos; caso contrário, é infinito. Em particular, um conjunto constituído exatamente de *um* elemento é chamado *conjunto unitário*. (Veja mais exemplos em [1] )

## 1.2 Conjuntos Numéricos

### 1.2.1 Conjunto dos naturais, inteiros e racionais

Usando as seguintes notações:

$\mathbb{N}$  - conjunto dos números naturais  $\{1, 2, 3, \dots\}$

$\mathbb{Z}$  - conjunto dos números inteiros  $\{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q}$  - conjunto dos números racionais, isto é, dos números da forma  $\frac{p}{q}$ , onde  $p$  e  $q$  são inteiros e  $q \neq 0$ .

Não é o intuito fazer um estudo sistemático desses três conjuntos nesse momento, os conjuntos dos naturais e inteiros serão trabalhados posteriormente. Assim, faremos apenas alguns comentários rápidos.

O conjunto dos números racionais nada mais são que as frações da aritmética do curso de primeiro grau. Quando aprendemos a operar com frações, a rigor, o que estava fazendo era definir as operações de adição e multiplicação. As propriedades (1) e (6) dessas operações enunciadas a seguir, apesar de usadas frequentemente, não recebem maior atenção. Isto parece explicável, porque os números inteiros gozam de quase todas essas propriedades. E, na verdade, se construirmos os racionais a partir dos inteiros, tais propriedades podem ser deduzidas facilmente de propriedades análogas para  $\mathbb{Z}$ . Também foram ensinadas relações do tipo  $\frac{8}{6} = \frac{4}{3}$ ,  $\frac{3}{1} = 3$  e  $0,99999\dots = \frac{1}{1}$ . No fundo, as duas primeiras relações são escritas por definição e, portanto, não se demonstram. a primeira define a relação de igualdade entre as frações, isto é,  $\frac{p}{q} = \frac{r}{s}$  se  $ps = qr$ . A segunda igualdade faz uma identificação do conjunto  $\mathbb{Z}$  com um conjunto de  $\mathbb{Q}$ , isto é, com o subconjunto

$$\left\{ \frac{p}{q} \in \mathbb{Q}; q = 1 \right\}$$

Portanto, com um certo abuso de linguagem, dizemos que  $\mathbb{Z}$  é um subconjunto de  $\mathbb{Q}$ .

**Definição 1.2.** Um *corpo*  $F$  é um conjunto de elementos  $x, y, z, \dots$ , onde se acham definidas as operações de adição (a cada par de elementos  $x$  e  $y$  em  $F$  corresponde um elemento de  $F$  que se designa  $x + y$ ) e de multiplicação (a cada elemento  $x$  e  $y$  em  $F$  corresponde um elemento de  $F$  que se designa por  $xy$ ) satisfazendo as propriedades que seguem.

- (1) Leis comutativas:  $x + y = y + x$ ,  $xy = yx$ .
- (2) Leis associativas:  $(x + y) + z = x + (y + z)$ ,  $(xy)z = x(yz)$ .
- (3) Existência de um zero: existe um elemento  $0 \in F$  tal que  $x + 0 = x$  para todo  $x \in F$ .
- (4) Existência de uma unidade: existe um elemento  $1 \in F$  tal que  $x1 = x$ .
- (5) Existência de inverso: dado  $x \in F$ , existe  $-x \in F$  tal que  $x + (-x) = 0$ , e dado  $x \in F$ ,  $x \neq 0$ , existe  $x^{-1} \in F$  tal que  $xx^{-1} = 1$ .
- (6) Lei distributiva:  $(x + y)z = xz + yz$ .

É imediato verificar que o conjunto  $\mathbb{Q}$  dos racionais é um corpo. Observe também que  $\mathbb{Z}$  não é um corpo.

Vamos interpretar geometricamente os números Racionais através de uma reta  $R$ , onde se escolhe dois pontos, o 0 e o 1.

Os inteiros são marcados facilmente, se usarmos o segmento de extremidade 0 e 1 como unidade. Os racionais são obtidos por subdivisões adequadas do segmento da unidade. Se

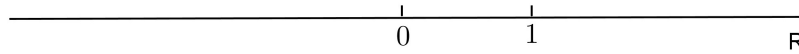


Figura 1.1: reta R

imaginarmos os números racionais marcados sobre a reta, veremos que eles formam um subconjunto da reta que é *denso* no sentido que esclareceremos a seguir.

Dado um ponto qualquer da reta, podemos obter racionais tão perto dele quanto se queira; basta tomar subdivisões cada vez mais finas da unidade. Pode parecer, pois, que os racionais cobrem a reta  $R$ , isto é, a cada ponto de  $R$  corresponde a um racional. Que isso não é verdade já era conhecido pelos matemáticos da Escola Pitagórica. Sabiam eles que a hipotenusa de um triângulo retângulo isósceles não é comensurável com os catetos, isto é, se os catetos têm comprimento igual a 1, então a hipotenusa não é racional. Portanto, o ponto  $P$  da reta  $R$ , obtido traçando-se a circunferência centrada em 0 e raio igual a hipotenusa, não corresponde a um racional

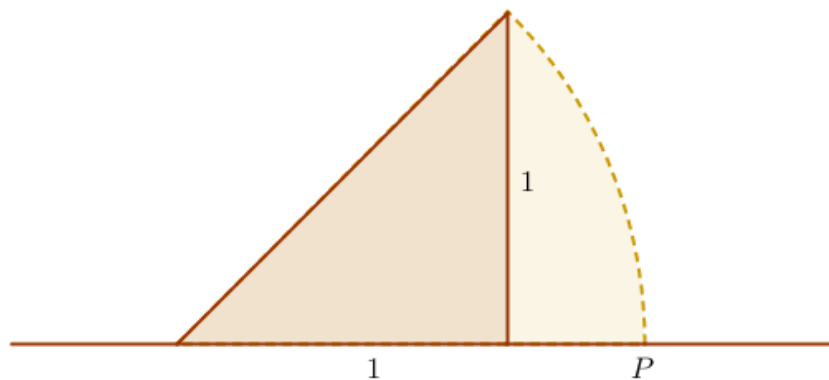


Figura 1.2: Triângulo retângulo isósceles

Podemos demonstrar facilmente que a hipotenusa não é racional.

Suponhamos, por contradição, que a hipotenusa seja racional  $\frac{p}{q}$ . podemos supor que  $p$  e  $q$  são primos entre si. Pelo teorema de Pitágoras,  $(\frac{p}{q})^2 = 1 + 1$ , ou seja,  $p^2 = 2q^2$ . Logo,  $p^2$  é um inteiro par, o que implica que  $p$  é par, isto é,  $p = 2r$ . Portanto,  $4r^2 = 2q^2$ . Portanto,  $4r^2 = 2q^2$ , ou seja,  $q^2 = 2r^2$ , de onde se segue que  $q$  é par. Ora,  $p$  e  $q$ , sendo números pares, não podem ser primos entre si. Essa é a contradição.

O fato demonstrado diz que existem pontos em  $R$  que não correspondem a elementos de  $\mathbb{Q}$ , é só dividirmos a reta  $R$  em duas partes. A primeira formada por números negativos ou cujo o quadrado é menor que dois, e a segunda formada por números positivos cujo o quadrado é maior que dois. Como a raiz quadrada de dois não é número racional, vemos que esta divisão de  $R$  foi feita de forma que todos os números da primeira metade são todos menores que os da segunda metade, mas ficou nenhum número dividindo as duas partes. Este fato indica uma deficiência dos racionais. (Veja mais exemplos em [5] )

Procedemos agora no sentido de se obter um conjunto numérico mais amplo que o dos racionais e cujos os elementos estejam em correspondência biunívoca com os pontos de  $R$ . (Dois conjuntos  $A$  e  $B$  estão em correspondência biunívoca, se a cada elemento de  $A$  corresponde um, e somente um, elemento de  $B$  e vice-versa.) O conjunto que vai resolver essa questão é o corpo dos números reais.

## 1.2.2 Conjunto dos números reais

Embora a necessidade de introdução dos números irracionais fosse já clara para os matemáticos da Grécia antiga nos seus estudos de Geometria, métodos satisfatórios de construção dos números irracionais, a partir dos números racionais, só foram introduzidas muito mais tarde, no século XIX. Nessa época foram delineadas três teorias respectivamente por Karl Weierstrass (1815-1897), Georg Cantor (1845-1918) e Richard Dedekind (1831-1916). Em 1889 o Matemático Italiano Giuseppe Peano (1858-1932) apresentou cinco axiomas para os inteiros positivos que podem ser utilizados como ponto de partida para a construção total. Esses axiomas serão estudados mais profundamente no capítulo seguinte.

**Definição 1.3.** Um corpo  $F$  é *ordenado* se contiver um subconjunto  $P$  com as seguintes propriedades:

$$(P1) \ x \in P, y \in P \text{ implica } x + y \in P \text{ e } xy \in P,$$

(P2) dado  $x \in F$ , então uma, e somente uma das três possibilidades ocorre:  $x \in P$ ,  $-x \in P$ ,  $x = 0$ .

É imediatamente que  $\mathbb{Q}$  é um corpo ordenado, onde  $P$  é o conjunto  $\mathbb{Q}^+$  dos racionais positivos. Isso motiva o nome de *elementos positivos* para os elementos do subconjunto  $P$  de um corpo ordenado qualquer  $F$ . Em um corpo ordenado  $F$ , podemos introduzir uma ordem estrita entre seus elementos, do seguinte modo:

$$x > y \text{ se } x - y \in P.$$

No caso dos racionais, essa é precisamente a ordem usual, pois  $x \in \mathbb{Q}^+$  se  $x > 0$ . Então vale o seguinte:

$$x \geq y, \text{ se } x > y \text{ ou } x = y$$

$$x < y, \text{ se } y > x$$

$$x \leq y, \text{ se } y \geq x.$$

Temos também que o “ $\leq$ ” é uma *relação de ordem* em  $F$ , isto é:

(i)  $x \leq x$ , para todo  $x \in F$  (reflexiva);

(ii)  $x \leq y$  e  $y \leq x \implies x = y$  (anti-simétrica);

(iii)  $x \leq y, y \leq z \implies x \leq z$  (transitividade).

Além disso,  $\leq$  é o que se chama de *ordem total*, isto é, além de (i), (ii) e (iii) temos

(iv) dados  $x, y \in \mathbb{R} \implies$  ou  $x \leq y$  ou  $y \leq x$ . (tricotomia)

(As demonstrações destas propriedades estão em [2] [3] )

**Cota superior.** Seja  $F$  um corpo ordenado e  $A$  um subconjunto de  $F$ . Um elemento  $x \in F$  é uma *cota superior* de  $A$  se  $x \geq y$ , para todo  $y \in A$ . Existem conjuntos que não tem cota superior. Por exemplo, considere o corpo ordenado  $\mathbb{Q}$  dos números racionais; é fácil ver que o subconjunto  $\mathbb{N}$  dos números naturais não tem cota superior. Esse fato motiva a seguinte definição: um subconjunto  $A$  de  $F$  se diz *limitado superiormente* se ele possui cota superior.

**Cota inferior.** De modo análogo, introduzimos os conceitos de cota inferior e conjunto limitado inferiormente. Um elemento  $x \in F$  é uma *cota inferior* se  $x \leq y$ , para todo  $y \in A$ . Existem conjuntos que não possuem cota inferior. O conjunto  $\mathbb{Z}$  dos números inteiros não tem cota inferior no corpo  $\mathbb{Q}$  dos números racionais. Um subconjunto  $A$  de um corpo ordenado  $F$  se diz *limitado inferiormente* se ele possui cota inferior.

**Supremo de um conjunto limitado superiormente.** Seja  $F$  um corpo ordenado e  $A \subset F$  um conjunto limitado superiormente. O *supremo* do conjunto  $A$ , que designamos  $\sup A$ , é definido como a menor das cotas superiores de  $A$  (quando existe). Em outras palavras,  $x \in F$  é supremo de  $A$  se:

(i)  $x$  for cota superior de  $A$ , e

(ii) se  $z$  for uma cota superior de  $A$ , então,  $x \leq z$ .

**Exemplo 1.4.** Considere o corpo ordenado  $\mathbb{Q}$  e o subconjunto  $A$  dos racionais maiores que 0 e menores que 1.

$$A = \{y \in \mathbb{Q}; 0 < y < 1\}$$

Qualquer racional maior ou igual a 1 é cota superior, e  $\sup A = 1$ . É fácil verificar que  $\sup B = 1$ , onde  $B = \{y \in \mathbb{Q}; 0 \leq y \leq 1\}$ . Por esse exemplo, vemos que o  $\sup$  (quando

existe) pode pertencer ou não ao conjunto.

**Ínfimo de um conjunto limitado inferiormente.** Seja  $F$  um corpo ordenado, e  $A \subset F$ , um conjunto limitado inferiormente.

O *ínfimo* de um conjunto  $A$ , que designamos por  $\inf A$ , é definido como a maior das cotas inferiores (quando existe). Em outras palavras,  $x \in F$  é o ínfimo de  $A$  se:

- (i)  $x$  for cota inferior de  $A$ , e
- (ii) se  $z$  for uma cota inferior de  $A$ , então  $x \geq z$ .

**Exemplo 1.5.** Considere, no corpo ordenado dos racionais, os conjuntos  $A$  e  $B$  definidos no exemplo 1.4. Vê-se que  $\inf A = 0$  e  $\inf B = 0$ . como no caso do sup, o inf (quando existe) pode pertencer ou não ao conjunto.

A partir dos conceitos de *cotas, supremo e ínfimo*. Vemos que o conjunto dos números racionais tem uma deficiência, ou seja, ele não completa toda a reta. (essas demonstrações encontramos nas referências [6] [2])

Isso nos motiva a seguinte definição.

**Definição 1.4.** Um corpo ordenado  $K$  chama-se *completo* quando todo subconjunto não vazio, limitado superiormente,  $X \subset K$ , possui supremo em  $K$ .

A partir do que vimos podemos adotar o axioma fundamental da Análise Matemática  
**Axioma.** *Existe um corpo ordenado completo,  $\mathbb{R}$  chamado o corpo dos números reais.*

Há várias maneiras de introduzir o sistema de números reais. O que fizemos aqui não é o modo construtivo, o processo que adotamos foi bastante avançado, consideramos os números reais como conceitos primitivos, isto é, supomos a existência de um conjunto  $\mathbb{R}$ , chamado de números reais, que nele verificam as três definições que são conhecidas como: *axioma do corpo, axioma de ordem e axioma do extremo* (também chamado de continuidade ou axioma da completeza). Esse último que difere os números reais dos números racionais.

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

Podemos definir os números reais a partir do teorema conhecido como *Princípio dos intervalos encaixados*, que será mostrado a seguir.



**Teorema 1.2.1. (Intervalos encaixados.)** *Dada uma sequência decrescente  $I_1 \supset I_2 \cdots \supset I_n \cdots$  de intervalos limitados e fechados  $I_n = [a_n, b_n]$ , existe pelo menos um número real  $c$  tal que  $c \in I_n$  para todo  $n \in \mathbb{N}$ .*

**Demonstração** A inclusão  $I_n \supset I_{n+1}$  significa que

$$a_1 \leq a_2 \leq \cdots \leq a_n \leq \cdots \leq b_n \leq \cdots \leq b_2 \leq b_1$$

Consideremos os conjuntos  $A = \{a_1, a_2, \dots, a_n\}$  e  $B = \{b_1, b_2, \dots, b_n\}$ . Observa-se que ambos são limitados, pois no caso de  $A$  o  $a_1$  é cota inferior e cada um dos  $b_n$  é uma cota superior, já no caso do conjunto  $B$  o  $b_1$  é uma cota superior e cada um dos  $a_n$  é uma cota inferior. Sejam  $a, b$ , respectivamente, os supremos de  $A$  e o ínfimo de  $B$ . Como cada um dos  $b_n$  é cota superior de  $A$ , então  $a \leq b_n$  para cada valor de  $n$ , assim como cada  $a_n$  é cota inferior de  $B$  então  $a_n \leq b$  para cada  $n$ , portanto  $a \leq b$ , logo.

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

Conclui-se que  $a$  e  $b$  pertencem a todos os intervalos  $I_n$ , ou seja,  $[a, b] \subset I_n$  para cada  $n$ , o que significa que pelo menos um ponto pertence a todos os intervalos  $I_n$  (caso  $a = b$ ) ou um intervalo está contido em todos intervalos  $I_n$  (caso  $a \neq b$ ). Se considerar um  $x < a = \sup A$ , existe algum  $a_n \in A$  tal que  $x < a_n$ , ou seja,  $x \notin I_n$ . Assim, nenhum  $x < a$  pertenceria a todos os intervalos  $I_n$ , com  $n \in \mathbb{N}$ . De modo análogo, conclui-se que nenhum  $y > b$  pertenceria a todos intervalos  $I_n$ , com  $n \in \mathbb{N}$ . Portanto, apenas os elementos do intervalo  $[a, b]$  pertencem a todos intervalos  $I_n$ , com  $n \in \mathbb{N}$ .

Nos capítulos seguintes usaremos esse importante teorema para demonstrar outros fatos.

### 1.3 Produto Cartesiano

Sejam dois conjuntos  $A$  e  $B$ . O produto cartesiano de  $A$  e  $B$ , denotado por  $A \times B$ , constitui-se de todos os pares ordenados  $(a, b)$  tais que  $a \in A$  e  $b \in B$ , isto é:

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

O produto de um conjunto por si próprio, isto é,  $A \times A$ , representa-se por  $A^2$ .

**Exemplo 1.6.** O plano cartesiano  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  (figura abaixo) cada ponto  $P$  representa um par ordenado  $(a, b)$  de números reais e vice-versa.

**Exemplo 1.7.** Seja  $A = \{1, 2, 3\}$  e  $B = \{a, b\}$ . Então

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

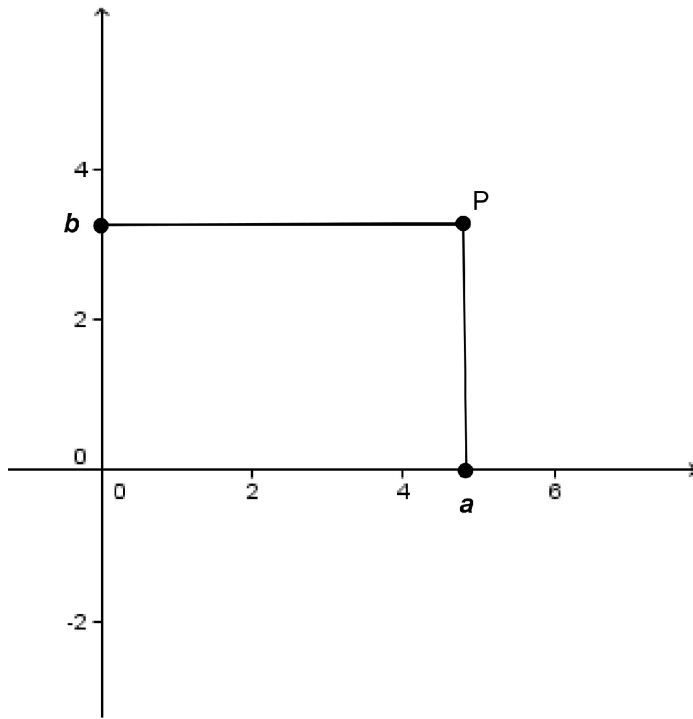


Figura 1.3: Representação de um ponto no plano cartesiano

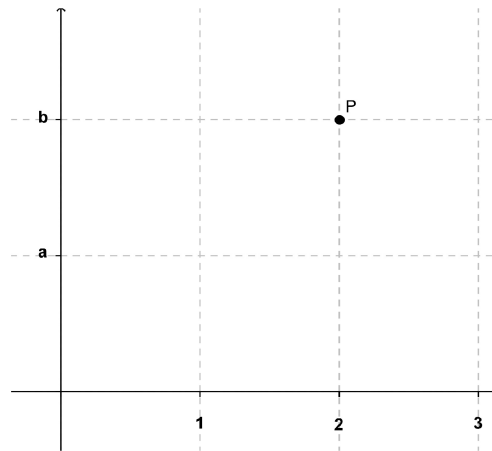


Figura 1.4: Representação vários pontos no plano cartesiano

## 1.4 Relações e funções

**Definição 1.5.** Uma relação  $R$  de  $A$  para  $B$  é um subconjunto de  $A \times B$ .

O domínio de uma relação  $R$  de  $A$  para  $B$  é o conjunto das primeiras coordenadas dos pares de  $R$ , e seu *contradomínio* é o conjunto das segundas coordenadas, isto é:

$$\begin{aligned}\text{domínio de } R &= \{a; (a, b) \in R\} \\ \text{contradomínio de } R &= \{b; (a, b) \in R\}\end{aligned}$$

**Definição 1.6.** Uma função é uma relação  $f : A \longrightarrow B$  que, a cada elemento  $x \in A$ ; associa um, e somente um, elemento  $y \in B$ : Além disso,

1. Os conjuntos  $A$  e  $B$  são chamados **domínio** e **contradomínio** de  $f$ , respectivamente.
2. O conjunto  $f(A) = \{y \in B; \text{existe } x \in A \text{ tal que } f(x) = y\} \subset B$  é chamado **imagem** de  $f$ .
3. Dado  $x \in A$ , o (único) elemento  $y = f(x) \in B$  correspondente é chamado imagem de  $x$ .

Uma função  $f : A \longrightarrow B$  consta de três partes: Um conjunto  $A$ , chamado o domínio da função (ou conjunto onde a função é definida), um conjunto  $B$ , chamado o contradomínio da função, ou o conjunto onde a função toma valores, e uma regra que permite associar, de um modo bem determinado, a cada elemento  $x \in A$ , um único elemento  $f(x) \in B$ , chamado o valor que função assume em  $x$  (ou no ponto  $x$ ).

Muitas vezes se diz a "função  $f$ " em vez de "a função  $f : A \longrightarrow B$ ". Neste caso, ficam subentendidos o conjunto  $A$ , domínio de  $f$ , e o conjunto  $B$ , contradomínio de  $f$ .

Não deve confundir  $f$  com  $f(x)$ :  $f$  é uma função, enquanto que  $f(x)$  é o valor que a função assume num ponto  $x$  do seu domínio.

A natureza da regra que ensina como obter o valor  $f(x) \in B$  quando é dado  $x \in A$  é inteiramente arbitrária, sendo sujeita apenas a duas condições:

1ª) Não deve haver exceções: afirm de que  $f$  tenha o conjunto  $A$  como domínio, a regra deve fornecer  $f(x)$  para todo  $x \in A$ .

2ª) Não deve haver ambiguidade: a cada  $x \in A$ , a regra deve fazer corresponder um único  $f(x)$  em  $B$ .

Veremos que não existem funções "plurívocas". Pela segunda condição, acima, se  $x = y$  em  $A$ , então,  $f(x) = f(y)$  em  $B$ .

Segue das condições acima que duas funções  $f : A \longrightarrow B$  e  $g : A' \longrightarrow B'$  são iguais se, somente se,  $A = A'$ ,  $B = B'$  e  $f(x) = g(x)$  para todo  $x \in A$ . Ou seja duas funções são iguais quando tem o mesmo domínio, o mesmo contradomínio e a mesma regra de correspondência.

**Exemplo 1.8.** Sejam  $P$  conjunto dos polígonos no plano,  $\mathbb{R}$  o conjunto dos números reais e  $f : P \longrightarrow \mathbb{R}$  a função que associa a cada polígono  $x$  sua área  $f(x)$ .

**Exemplo 1.9.** Sejam  $A = B = \mathbb{Q}$ . Tentamos definir uma função de  $f : \mathbb{Q} \rightarrow \mathbb{Q}$ , considere a seguinte regra: a cada número  $x \in \mathbb{Q}$ , façamos corresponder o número  $f(x) \in \mathbb{Q}$  tal que  $x \cdot f(x) = 1$ . Esta regra não define uma função de  $\mathbb{Q}$  em  $\mathbb{Q}$ , pois, dado  $0 \in \mathbb{Q}$ , não existe número racional algum  $y = f(0)$  tal que  $0 \cdot y = 1$ . Entretanto, se escolhermos o conjunto  $A = \mathbb{Q} - \{0\}$  para o domínio, a mesma regra define a função  $f : A \rightarrow \mathbb{Q}$ ,  $f(x) = 1/x$ .

## 1.5 Classificação da Funções

### 1.5.1 Funções Injetivas e Sobrejetivas

Assim como é útil descrever as diferentes propriedades que as relações têm, é útil nomear certas propriedades das funções.

**Definição 1.7.** Uma função  $f : X \rightarrow Y$  é *injetiva* se, para todo  $a$  e  $b$  em  $X$ ,  $f(a) = f(b)$  implica que  $a = b$ . Nesse caso, nós dizemos que  $f$  é uma *função injetiva* de  $X$  para  $Y$ .

**Definição 1.8.** Uma função  $f : X \rightarrow Y$  é *sobrejetiva* se para todo  $y \in Y$  existe um  $x \in X$  tal que  $f(x) = y$ .

Nesse caso dizemos que  $f$  envia  $X$  sobre  $Y$ .

Uma função injetiva sempre ira associar elementos diferentes do domínio a diferentes elementos do contradomínio. Em outras palavras, no máximo *um* elemento do domínio é enviado a *um* elemento qualquer do contradomínio.

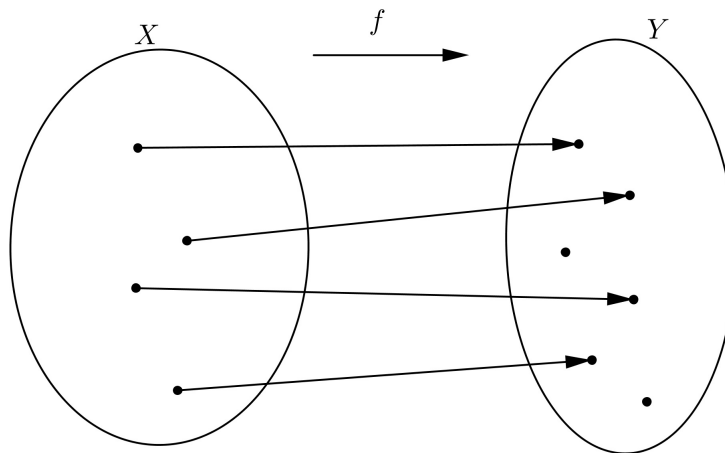


Figura 1.5: Uma função injetiva associa a cada elemento de  $X$  um elemento diferente de  $Y$

Usando o termo *imagem* para descrever o conjunto de todos os valores que uma função pode ter. Uma função sobrejetiva tem cada elemento do contradomínio em sua imagem. A figura 1.4

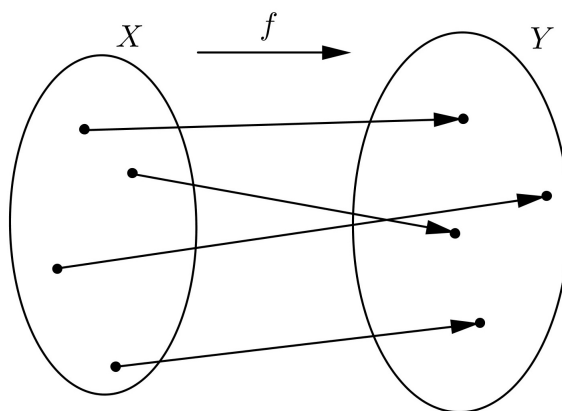


Figura 1.6: Se uma função é sobrejetiva, então cada elemento de  $Y$  é associado a pelo menos um elemento de  $X$

ilustra uma função sobrejetiva. Note que o domínio é enviado sobre todo contradomínio.

Lembre como as definições são usadas em matemática: afim de provar que uma função é injetiva ou sobrejetiva, quase sempre temos que usar a definição.

**Exemplo 1.10.** Prove que a função  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  definida por  $f(x) = 2x + 1$  é injetiva.

**Demonstração** Sejam  $a, b \in \mathbb{Z}$  e suponha que  $f(a) = f(b)$ .

Então

$$2a + 1 = 2b + 1$$

$$2a = 2b$$

$$a = b$$

Mostramos que  $f(a) = f(b)$  implica que  $a = b$ , ou seja, que  $f$  é injetiva.

Denotemos por  $\lfloor x \rfloor$  o maior inteiro menos ou igual a  $x$ . Então, por exemplo,  $\lfloor 4,3 \rfloor = 4$ ,  $\lfloor -2,1 \rfloor = -3$  e  $\lfloor 17 \rfloor = 17$ . A função que envia  $x$  a  $\lfloor x \rfloor$  é chamada de função *piso*.

**Exemplo 1.11.** Seja  $f : \mathbb{R} \rightarrow \mathbb{Z}$  definida por  $f(x) = \lfloor x \rfloor$ . Prove que  $f$  leva  $\mathbb{R}$  sobre  $\mathbb{Z}$ .

**Demonstração** Seja  $n \in \mathbb{Z}$ . Uma vez que  $\mathbb{Z} \subseteq \mathbb{R}$ , então  $n \in \mathbb{R}$  também. Mas, uma vez que  $n$  é um número inteiro,  $\lfloor n \rfloor = n$ . Portanto,  $f(n) = n$ .

As demonstrações nos dois últimos exemplos são padrões. Para provar que uma função é injetiva, suponha  $f(a) = f(b)$  e mostre que  $a = b$ . Para mostrar que uma função  $f$  é sobrejetiva, considere  $y$  um elemento do contradomínio e encontre algum  $x$  do domínio tal que  $f(x) = y$ .

Para provar que uma função não é injetiva ou sobrejetiva, procure um contraexemplo. A função do exemplo 1.8 não é sobrejetiva porque, por exemplo,  $38 \in \mathbb{Z}$ , mas não existe um número inteiro  $x$  tal que  $2x + 1 = 38$ . Da mesma forma, a função no exemplo 1.9 não é injetiva porque  $[9, 3] = [9, 8]$ , mas  $9, 3 \neq 9, 8$ . Note que esses dois exemplos mostram que ser injetiva não é o mesmo que ser sobrejetiva.

É claro que é possível para uma função ser tanto injetiva quanto sobrejetiva como no exemplo:

**Exemplo 1.12.** Seja  $X$  um conjunto. então a função *identidade*

$$f : X \longrightarrow X$$

é definida por  $f(x) = x$

Tal função é chamada de *bijetiva*, ou uma *bijeção*.

**Exemplo 1.13.** Prove que a função  $f : \mathbb{R} \longrightarrow \mathbb{R}$  definida por  $f(x) = 2x + 1$  é uma bijeção.

**Demonstração** Precisamos mostrar que  $f$  é tanto injetiva quanto sobrejetiva. A demonstração de que essa função é injetiva é exatamente a mesma que a do exemplo 1.10. Para demonstrar que  $f$  é sobrejetiva seja  $y \in \mathbb{R}$  qualquer número real. Tome  $x = \frac{y-1}{2}$ .

Então  $x \in \mathbb{R}$  e

$$\begin{aligned} f(x) &= f\left(\frac{y-1}{2}\right) \\ f(x) &= 2\left(\frac{y-1}{2}\right) + 1 \\ f(x) &= y - 1 + 1 \\ f(x) &= y \end{aligned}$$

Assim,  $f$  é também uma função sobrejetiva.

**Exemplo 1.14.** Seja  $E = \{n \in \mathbb{Z}; n \text{ é par}\}$ , e seja  $O = \{n \in \mathbb{Z}; n \text{ é ímpar}\}$ . Defina a função.

$$f : E \times O \longrightarrow \mathbb{Z}$$

por  $f(x, y) = x + y$ . Responda se  $f$  é injetiva e/ou sobrejetiva. Prove ou dê um contraexemplo.

**Demonstração** Primeiramente mostramos que  $f$  não é sobrejetiva. Suponha, ao contrário que  $f$  é sobrejetiva. Uma vez que  $2 \in \mathbb{Z}$  é um elemento do contradomínio, existe algum par ordenado  $(x, y) \in E \times O$  tal que

$$f(x, y) = x + y = 2$$

Mas, uma vez que  $x$  é par e  $y$  é ímpar,  $x + y$  é ímpar. Uma vez que a soma de um número par com um número ímpar é sempre um número ímpar. Isso contradiz que 2 é par.

A seguir mostraremos que  $f$  não é injetiva. Note que

$$f(4, -3) = 1 = f(6, -5)$$

mas  $f(4, -3) \neq f(6, -5)$ . Este contraexemplo mostra que  $f$  não é injetiva.

**Exemplo 1.15.** Seja  $P$  um conjunto de  $n$  pontos em uma circunferência. Desenhe segmentos de reta conectando cada ponto com todos os outros pontos. Suponha que os pontos estão dispostos de forma que nenhum ponto interior da circunferência pertence simultaneamente a três segmentos. (A figura 1.5 mostra uma possível configuração.) Seja  $X$  o conjunto de todos os pontos de interseção dos segmentos no interior da circunferência (note que os pontos em  $P$  não estão incluídos em  $X$ ). Seja  $Y$  o conjunto de todos os conjuntos com quatro dos pontos de  $P$ , ou seja,

$$Y = \{\{A, B, C, D\} \subseteq P; A, B, C, D \text{ são todos diferentes}\}$$

. Descreva uma correspondência injetiva  $f : X \rightarrow Y$ . Mostre que a função é tanto injetiva quanto sobrejetiva.

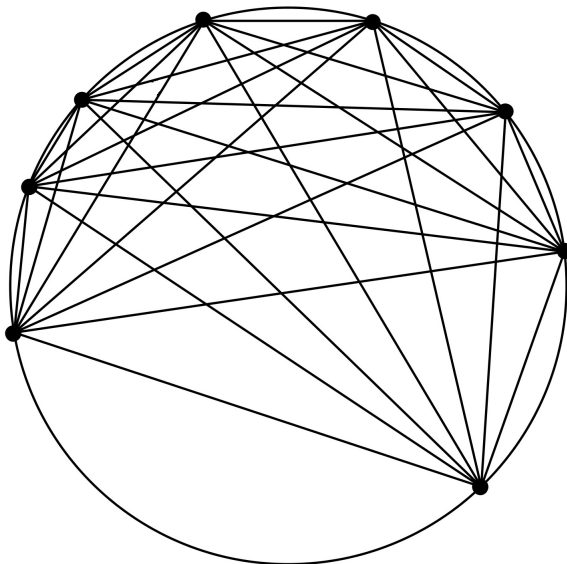


Figura 1.7: Uma possível configuração de pontos para o exemplo 1.13 com  $n = 8$

**Demonstração** Seja  $H \in X$  um ponto de interseção. Então  $H$  pertence a dois segmentos, de

maneira que podemos definir  $f(H)$  como o conjunto que contém as quatro extremidades desses dois seguimentos.

Provamos que  $f$  é injetiva por contraposição. Suponha que  $H$  e  $K$  são dois pontos distintos de  $Y$ , isto é,  $H \neq K$ . Se  $l_1$  e  $l_2$  são os dois seguimentos que cortam em  $H$ , então pelo menos um dos seguimentos que passam por  $K$  deve ser diferente de  $l_1$  e  $l_2$ , já que dois seguimentos só podem se cortar em no máximo um ponto. Chamemos esse terceiro seguimento de  $l_3$ . Então  $f(K)$  contém ambas das extremidades de  $l_3$ , mas  $f(H)$  não. Por isso  $f(K) \neq f(H)$ .

Para mostrar que  $f$  é sobrejetiva, seja  $\{A, B, C, D\} \subseteq P$ . Sem perda de generalidade, podemos rotular novamente esses pontos (se necessário) de modo que  $A, B, C, D$  aparecem ordenados em sentido horário à medida que percorrem a circunferência. Seja  $l_1$  o segmento entre  $A$  e  $C$ , e seja  $l_2$  o segmento entre  $B$  e  $D$ . Uma vez que  $B$  está no arco de circunferência que vai no sentido horário de  $A$  até  $C$  e  $D$  está no arco de circunferência que vai no sentido anti-horário de  $A$  até  $C$ , o segmento  $l_1$  separa  $B$  e  $D$ , de maneira que os seguimentos  $l_1$  e  $l_2$  se cortam. Chamemos esse ponto de interseção de  $H$ . Então  $f(H) = \{A, B, C, D\}$ , como exigido.

Pense em uma bijeção  $f : X \rightarrow Y$  como uma maneira de atribuir a cada elemento de  $X$  um único elemento de  $Y$ , e vice-versa. Pode escrever

$$X \longleftrightarrow Y$$

para enfatizar a simetria da relação que uma bijeção define. Cada elemento de um conjunto tem um parceiro no outro conjunto.

## 1.5.2 Funções Compostas

Existem algumas maneiras comuns para formar novas funções a partir de antigas. Uma tal construção é a *composição* de duas funções. Se  $f : X \rightarrow Y$  e  $g : Y \rightarrow Z$ , então  $g \circ f$  é uma função de  $X$  a  $Z$  definida por  $(g \circ f)(x) = g(f(x))$ .

A rigor podemos levar em consideração as seguintes definições:

**Definição 1.9.** Sejam  $f : X \rightarrow Y$  e  $g : Y \rightarrow V$  duas funções, com  $Y \subset U$ . A função composta de  $g$  com  $f$  é uma função denotada por  $g \circ f$ , com domínio em  $X$  e contradomínio em  $V$ , que a cada elemento  $x \in X$  faz corresponder o elemento  $y = g \circ f(x) = g(f(x)) \in V$ , isto é:

$$\begin{aligned} g \circ f : X &\rightarrow Y \subset U \rightarrow V \\ x &\mapsto f(x) \mapsto g(f(x)) \end{aligned}$$

**Definição 1.10.** Uma função  $f : X \rightarrow Y$  é invertível se existe uma função  $g : Y \rightarrow X$  tal que:

(i)  $f \circ g = I_y$ ;



$$(ii) g \circ f = I_x;$$

Observemos que  $I_A$  denota a função identidade do conjunto  $A$ , ou seja,  $I_A : x \in A \mapsto x \in A$ . Neste caso, a função  $g$  é dita função inversa de  $f$  e denotada  $g = f^{-1}$ .

**Exemplo 1.16.** Seja  $f : \mathbb{R} \rightarrow \mathbb{R}$  definida por  $f(x) = \lfloor x \rfloor$  e seja  $g : \mathbb{R} \rightarrow \mathbb{R}$  definida por  $g(x) = 3x$ . Então

$$(g \circ f)(2, 4) = g(f(2, 4))$$

$$(g \circ f)(2, 4) = g(2)$$

$$(g \circ f)(2, 4) = 6$$

e

$$(f \circ g)(2, 4) = f(g(2, 4))$$

$$(f \circ g)(2, 4) = f(7, 2)$$

$$(f \circ g)(2, 4) = 7$$

Esse exemplo mostra que  $f \circ g$  pode ser diferente de  $g \circ f$ . Perceba uma coisa potencialmente confusa sobre a notação: na composição  $g \circ f$ , fazemos  $f$  primeiro, e depois aplicamos  $g$  ao resultado. A ordem importa em geral.

Algumas vezes gostaríamos de ser capazes de "desfazer" uma função, de forma que ela envie cada ponto de volta para onde veio. Se  $f : X \rightarrow Y$  é uma função, então a função inversa de  $f$  é a função

$$f^{-1} : X \rightarrow Y$$

que tem a propriedade que  $f^{-1} \circ f = 1_X$  e  $f \circ f^{-1} = 1_Y$ .

Nem toda função têm inversa. Se  $f : X \rightarrow Y$  tem uma inversa, então, para qualquer  $y \in Y$ ,  $f(f^{-1}(y)) = y$ , de maneira que  $f$  deve enviar  $X$  sobre  $Y$ . Além disso, se  $f(a) = f(b)$ , então podemos aplicar  $f^{-1}$  em ambos os lados dessa equação para ter  $a = b$ , de modo que  $f$  também deve ser injetiva. Assim vemos que, se uma função possui uma inversa, ela deve ser uma bijeção.

De forma recíproca, podemos construir a inversa de qualquer bijeção  $f : X \rightarrow Y$  ao pegar  $f^{-1}(y)$  como o único elemento de  $X$  que é enviado em  $y$ . Sabemos que tal elemento existe, porque  $f$  é sobrejetiva, e sabemos que esse elemento é único, uma vez que  $f$  é injetiva. Essa é a única escolha que temos para  $f^{-1}$ .

**Exemplo 1.17.** Se  $f : \mathbb{R} \rightarrow \{y \in \mathbb{R}; y > 0\}$  é uma função  $f(x) = 2^x$ , então a inversa de  $f$  é dada por  $f^{-1}(x) = \log_2 x$ .

Neste último exemplo, poderíamos definir  $f(x) = 2^x$  como uma função de  $\mathbb{R}$  para  $\mathbb{R}$ , mas ela não seria invertível porque não seria sobrejetiva.

Uma última maneira de construir funções é por *restrição*. Se  $f : X \rightarrow Y$  é alguma função, e  $H \subseteq X$ , então a restrição de  $f$  para  $H$  é a função

$$f|_H : H \rightarrow Y$$

definida por  $f|_H(x) = f(x)$ . Em outras palavras, apenas restringimos o domínio a um conjunto menor, e usamos a mesma regra que atribui um elemento do contradomínio a cada elemento desse domínio menor. Para que isso? Algumas vezes a nova função restrita é mais simples de descrever, ou tem outras propriedades desejadas.

**Exemplo 1.18.** Seja  $D$  o disco unitário em  $\mathbb{R}^2$ , isto é,

$$D = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 \leq 1\}$$

e seja  $D^* = D - \{(0, 0)\}$ . Seja  $S^1 = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = 1\}$  o círculo unitário. Defina uma função  $p : D^* \rightarrow S^1$  projetando cada ponto para fora ao longo de um raio até alcançar a fronteira do disco. Veja a figura a seguir.

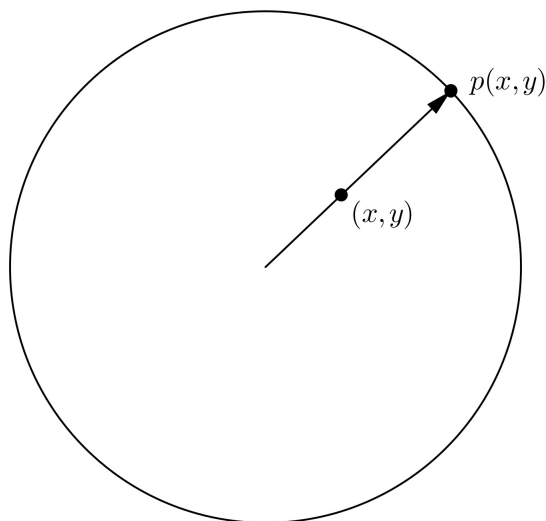


Figura 1.8: projeção de um ponto até a fronteira do disco

**Demonstração** Obter uma fórmula para  $p$  pode ser um pouco confuso, mas as coisas podem ficar claras se considerarmos uma restrição. Seja  $H$  o círculo de raio  $\frac{1}{2}$ :

$$H = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = \frac{1}{4}\}$$

Como  $H \subset D$ , temos que  $p|_H : H \rightarrow S^1$  definida por  $p|_H(x, y) = (2x, 2y)$ . Como a função está restrita a  $H = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = \frac{1}{4}\}$ , temos:

$$(2x)^2 + (2y)^2 = \frac{1}{4}$$

$$4x^2 + 4y^2 = \frac{1}{4}$$

$$x^2 + y^2 = 1$$

portanto, qualquer ponto do novo domínio é projetado até encontrar a fronteira do disco.

# Capítulo 2

## Cardinalidade dos Conjuntos

### 2.1 Uma breve reflexão sobre conjuntos e paradoxos

Consideremos, para fixar ideias, os conjuntos  $A = \{a, b, c\}$  e  $B = \{m, n, p\}$ , onde supomos que os elementos  $a, b$  e  $c$  são distintos entre si, bem como  $m, n$  e  $p$ . Entre esses conjuntos podemos estabelecer uma correspondência que a cada elemento de  $A$  associa um e apenas um elemento de  $B$ , e reciprocamente. Isto poderia ser feito assim: associamos  $a$  a  $m$ ,  $b$  a  $n$ , e  $c$  a  $p$ . Quando entre dois conjuntos é possível estabelecer uma correspondência desse tipo, diz-se que eles são equipotentes. Há equipotência, também, entre conjuntos infinitos; assim, os conjuntos  $\{2, 4, 6, \dots\}$  e  $\{1, 3, 5, \dots\}$  são equipotentes. Mas é claro que o conjunto  $\{1, 2, 3\}$  não é equipotente ao conjunto  $\{1, 3, 4, \dots\}$ ; outro exemplo de dois conjuntos que não são equipotentes é constituído pelo conjunto de todos os números naturais e pelo conjunto de todos os pontos de uma reta da geometria comum, como seria possível provar. Evidentemente, se os conjuntos  $A$  e  $B$  forem finitos, eles têm o mesmo número de elementos se, e somente se, forem equipotentes.

Isso nos conduz a definir a relação “ $A$  tem o mesmo número de elementos de  $B$ ” ( $A$  e  $B$  sendo conjuntos quaisquer) se, e só se,  $A$  for equipotente a  $B$ . Em seguida, definiremos o número de elementos (ou o número cardinal) de um conjunto  $M$  qualquer como sendo a classe de todos os conjuntos equipotentes a  $M$ .

A definição precedente pode parecer estranha, mas caracteriza, perfeitamente, tanto o número cardinais finitos, como os infinitos. Em síntese, sobre ela é possível estabelecer uma teoria logicamente precisa dos números cardinais, que inclui o caso dos cardinais finitos, em particular. Mediante a um processo de análise lógica, devido a Frege e Russell, pode-se definir o conceito de número cardinal em termos puramente lógicos. Naturalmente, a definição foi delineada sem os recursos da lógica simbólica, de modo que o processo parece algo impreciso e aparentemente encerra um círculo vicioso. Pois, na definição de equipotência, dissemos que a cada elemento do conjunto  $A$  deve corresponder *um* e apenas *um* de  $B$ ; aqui aparece o número *um* explicitamente, o que não é correto, posto que é desejável definir a noção de número cardinal, em geral, incluso o próprio número *um*. No entanto, isto se deu pelo fato de utilizar a linguagem comum,

que se presta muito pouco para análises lógicas precisas. A dificuldade facilmente se evita por meio do simbolismo da lógica moderna.

Não se pode definir nem demonstrar tudo. Assim para definir um conceito  $A$ , necessitamos de outro, por exemplo, de  $A_1$  e  $A_2$ ; para definir  $A_1$ , precisamos de outros, e assim sucessivamente. Logo, numa disciplina dedutiva, se pretende evitar círculos viciosos, há conceitos que se deve aceitar sem definição e que se denominam conceitos primitivos da disciplina em questão. Da mesma maneira, qualquer disciplina matemática sempre encerra certas proposições aceitas sem demonstração, chamadas proposições primitivas (ou axiomas ou, ainda, postulados). Porém, escolhidas as noções e as proposições primitivas, todos os outros conceitos da disciplina, para serem empregados, devem ser definidos em termos das noções primitivas, e todas as suas outras proposições (verdadeiras) só devem ser aceita mediante demonstração. Uma disciplina elaborada estritamente de acordo com o que acabamos de dizer, constitui uma teoria axiomática ou, simplesmente, uma axiomática.

Já nos referimos ao fato que a análise matemática clássica (aritmética, álgebra, cálculo diferencial e integral, teoria das funções, etc...) fundamentam-se no conceito de número natural (além dos conceitos e princípios lógicos, é claro). Após a descoberta dessas circunstâncias, Peano foi adiante, mostrando que a teoria ordinária dos números naturais pode ser construída a partir, tão somente, de três conceitos primitivos e quatro postulados.

Os conceitos primitivos de Peano são:

- 1) *número natural*
- 2) *um* (1)
- 3) a relação “*sucessor de*”

Intuitivamente, o número natural  $x$  é o sucessor do número natural  $y$ . Se  $x$  segue  $y$  na ordem do comum dos números naturais, que é a seguinte: 1, 2, 3, 4, 5, .... Assim, 2 é sucessor de 1, 3 é sucessor de 2, etc.

Os quatro postulados de Peano são:

1. Um não é sucessor de nenhum número natural.
2. O sucessor de um número natural é um número natural.
3. Dois números naturais que tiverem o mesmo sucessor são iguais.
4. Se um possui uma propriedade  $P$ , e se do fato de um número natural qualquer  $n$  possui  $P$ , isto acarreta que  $n + 1$  também a possui, então todo número natural possui a propriedade  $P$ .(Princípio da *indução matemática*, da *indução completa* ou da *recorrência*)

Dos axiomas de Peano podemos deduzir todas as proposições usuais da aritmética elementar. Analogamente, todas as ideias comuns da aritmética são definíveis em função dos conceitos primitivos de Peano.

Como já foi observado que a análise matemática inteira fundamenta-se apenas no conceito de números naturais (e na lógica), resulta que grande parte da matemática decorre, por meio de definições e demonstrações, dos conceitos primitivos e dos postulados de Peano. Pois bem:

Bertrand Russell, como o auxílio de sua conceituação de número cardinal, mostrou como se pode definir os primitivos de Peano em termos puramente lógicos. Além disso, demonstrou os postulados de Peano por intermédios de princípios lógicos. Portanto, verificamos, assim, de que forma uma extensa porção da matemática reduz-se a lógica. E o mesmo sucede, de conformidade com o logismo, com a matemática toda.

No decurso da elaboração das concepções logicistas, surgiram, em matemática, por volta de 1900, numerosos paradoxos (uma proposição que apesar de parecer coerente, demonstra falta de nexos ou lógica), especialmente em teoria dos conjuntos.

Há conjuntos que podem pertencer a si mesmo: por exemplo, o conjunto de todos os conjuntos, que, por ser um conjunto, pertence a si mesmo. Mas existem conjuntos que não pertencem a si mesmo; é o caso do *conjunto de todos os homens, que, por não ser um homem, não pertence a si mesmo*. Vamos considerar um conjunto  $A$  formado por todos os conjuntos que não pertencem a si mesmo. Pelo princípio do terceiro excluído,  $A$  pertence ou não pertence a  $A$ . Suponhamos que  $A$  pertença a  $A$ ; então, como  $A$  é o conjunto de todos os conjuntos que não pertencem a si mesmos,  $A$  não pertence a  $A$ . Admitamos, então, que  $A$  não pertence a  $A$ ; logo, de acordo com a definição de  $A$ , este conjunto deve pertencer a si mesmo. Há, por conseguinte, contradição. Este paradoxo é conhecido por paradoxo de Russell, embora tenha sido descoberto independentemente por Zermelo.

Outro paradoxo interessante é o paradoxo de Cantor ou do máximo cardinal, que diz:

“Se todo elemento de um conjunto  $A$  (suposto diferente de  $\emptyset$  ou, o que significa o mesmo não vazio) pertencer ao conjunto  $B$ . Diz-se que  $A$  é parte ou subconjunto de  $B$ ; por extensão, o conjunto vazio,  $\emptyset$ , é subconjunto de qualquer conjunto. Imediatamente, conclui-se que qualquer conjunto é subconjunto de si mesmo.”

Cantor provou que o número cardinal do conjunto de todas as partes de um conjunto  $A$  é sempre maior que o número cardinal de  $A$ . Consideremos o conjunto de todas as coisas, ou seja, a classe universal  $I$ . O número cardinal de  $I$  deve ser tal que não existe nenhum outro cardinal que lhe seja maior, como parece óbvio. Mas, segundo demonstrou Cantor, o número cardinal de conjunto das partes de  $I$  é maior do que o número cardinal de  $I$ . Chega-se, assim, a uma contradição.

Tudo que vimos até o momento nos levam as seguintes definições:

**Definição 2.1.** Sejam  $A$  e  $B$  dois conjuntos quaisquer. Se existe uma função bijetora  $f : A \rightarrow B$ , dizemos que o conjunto  $A$  é equipotente ao conjunto  $B$ . Dizemos também que eles tem igual potência ou mesmo número de elementos (ou mesma cardinalidade). Usaremos a simbologia  $A \sim B$  para representar a equivalência entre esses conjuntos.

Por esta razão, podemos pensar no conceito de cardinalidade como a generalização do conceito de números de elementos.

A relação de equipotência é uma relação de equivalência. Este último fato pode ser mostrado

da seguinte maneira.

(1) Como para todo conjunto  $A$ , a aplicação  $id_A : A \rightarrow A$  dada por  $id_A(x) = x$  para todo  $x \in A$ , é bijetora então todo conjunto é equipotente a si mesmo. Logo vale a propriedade reflexiva para essa relação entre conjuntos.

$$A \sim A, \text{ (reflexiva)}$$

(2) Se  $A$  é equipotente a  $B$ , isto é, se existe  $f : A \rightarrow B$  bijetora, então, como  $f^{-1} : B \rightarrow A$  é também bijetora,  $B$  também é equipotente a  $A$ . Portanto vale a propriedade simétrica.

$$\text{Se } A \sim B, \text{ então } B \sim A \text{ (simétrica)}$$

(3) Se  $A$  é equipotente a  $B$  e se  $B$  é equipotente a  $C$ , então existe  $f : A \rightarrow B$  e  $g : B \rightarrow C$  bijetoras. Daí  $g \circ f : A \rightarrow C$  também é bijetora e portanto  $A$  é equipotente a  $C$ . Portanto vale a propriedade transitiva.

$$\text{Se } A \sim B \text{ e } B \sim C, \text{ então } A \sim C \text{ (transitiva)}$$

A cada conjunto  $A$  está associado um objeto  $|A|$  chamado número cardinal de  $A$ , ou cardinalidade de  $A$ , tal que  $|A| = |B|$  se, e somente se,  $A$  é equipotente a  $B$ .

Outras notações para cardinalidade de  $A$ :

$$\text{card}(A)$$

$$c(A)$$

$$\#A$$

**Definição 2.2.** Dado dois conjuntos  $A$  e  $B$ , dizemos que  $\#A \leq \#B$  se existe uma aplicação  $f : A \rightarrow B$  injetora ( $A$  é equipotente a um subconjunto de  $B$ ). Se  $\#A \leq \#B$  e  $\#A \neq \#B$  dizemos que  $\#A < \#B$ .

Definiremos os cardinais finitos ( número cardinal de conjuntos finitos) da seguinte maneira:

$$\#\emptyset = 0$$

$$\#\{0\} = 1$$

$$\#\{0, 1\} = 2$$

$$\#\{0, 2, \dots, 2n\} = n$$

Ou seja, O número cardinal de um conjunto finito é o número de elementos que ele tem. Temos que, dado um conjunto  $A$  com  $n$  elementos a  $\#A = n$ .

Chamaremos  $\mathcal{P}(A)$  o conjunto das partes ou potências de  $A$ . E será provado no capítulo seguinte, quando explorarmos mais o conceito de indução, que  $\#\mathcal{P}(A) = 2^n$ .

Quantos elementos tem um conjunto infinito?

Cantor chegou à noção de infinito - infinito real, e não a infinidade potencial de limites por séculos utilizada pelos matemáticos - sem considerar diretamente os números, mas sim os conjuntos.

Cantor começou procurando atribuir “tamanhos”, que ele chamou de potências, aos diversos tipos de conjuntos de infinitos elementos. A esses tamanhos deu o nome de “ números transfinitos ”. A princípio denotou o menor dos números transfinitos, que é a cardinalidade do conjunto dos números naturais.

Todo conjunto infinito possui um subconjunto equipotente a  $\mathbb{N}$ . Logo a cardinalidade de qualquer conjunto infinito é maior ou igual à cardinalidade dos naturais. ( ver mais em [6], [9] e [8]).

## 2.2 O Conjunto dos Números Naturais

*“Deus criou os números naturais. O resto é obra dos homens”*

Leopold Kronecker

Lentamente, à medida em que se civilizava, a humanidade apoderou-se desse modelo abstrato de contagem ( um, dois, três, quatro,...) que são os números naturais. Foi uma evolução demorada. As tribos mais rudimentares contam apenas *um, dois, muitos*. A língua inglesa ainda guarda um resquício desse estágio na palavra *thrice*, que tanto pode significar “três vezes” como “muito” ou “tremendamente”.

As necessidades provocadas por um sistema social cada vez mais complexo e as longas reflexões, possíveis graças à disponibilidade de tempo trazida pelo progresso econômico, conduziram através dos séculos, ao aperfeiçoamento do extraordinário instrumento de avaliação que é o conjunto dos números naturais.

Decorrido muitos milênios, podemos hoje descrever concisa e precisamente O conjunto  $\mathbb{N}$  dos números naturais, valendo-nos da notável síntese feita pelo matemático italiano Giuseppe Peano no limiar do século 20.

$\mathbb{N}$  é um conjunto, cujos elementos são chamados *números naturais*. A essência da caracterização de  $\mathbb{N}$  reside na palavra “sucessor”. Intuitivamente, quando  $n, n' \in \mathbb{N}$ , dizer que  $n'$  é o sucessor de  $n$  significa que  $n'$  vem logo depois de  $n$ , não havendo outros números naturais entre  $n$  e  $n'$ . Evidentemente, esta explicação apenas substitui “sucessor” por “logo depois”, portanto não



é uma definição. O termo primitivo “sucessor” não é definido explicitamente. Seu uso e suas propriedades são regidos por algumas regras, abaixo enumeradas:

a) Todo número natural tem um único sucessor;

b) Números naturais diferentes têm sucessores diferentes;

c) Existe um único número natural, chamado *um* e representado pelo símbolo 1, que não é sucessor de nenhum outro.

d) Seja  $X$  um conjunto de números naturais (isto é,  $X \subset \mathbb{N}$ ). Se  $1 \in X$  e se, além disso, o sucessor de todo elemento de  $X$  ainda pertence a  $X$ , então  $X = \mathbb{N}$ .

As afirmações a), b), c) e d) acima são conhecidas como os *axiomas de Peano*. Tudo o que se sabe sobre os números naturais pode ser demonstrado como consequência desses axiomas.

Um engenhoso processo, que por muitos anos foi uma das maiores descobertas da humanidade, chamado de *sistema de numeração decimal*, permite representar todos os números naturais com o auxílio do símbolo 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Além disso, os primeiros números naturais têm nomes: O sucessor do número *um* chama-se *dois*, o sucessor de dois chama-se *três*, etc. A partir de um certo ponto, esses nomes tornam-se muito complicados, sendo preferível abrir mão deles e designar os grandes números por sua representação decimal. (Na realidade, os números muito grandes não possuem nomes. Por exemplo, como se chamaria o número  $10^{1000}$ ?).

Deve ficar claro que o conjunto  $\mathbb{N} = \{1, 2, 3, \dots\}$  dos números naturais é uma sequência de objetos abstratos que, em princípio, são vazios de significado. Cada um desses objetos (um número natural) possui apenas um lugar determinado nesta sequência. Nenhuma outra propriedade lhe serve de definição. Todo número tem um sucessor (único) e, com exceção de 1, tem também um único antecessor (número do qual é sucessor).

Visto desta maneira podemos dizer que os números naturais são *números ordinários*: 1 é o primeiro, 2 é o segundo, etc.

### 2.2.1 Destaque para o axioma da Indução

O último dos axiomas de Peano é conhecido como o *axioma da indução*. Ele é a base de um eficiente método de demonstração de proposições referentes a números naturais (demonstração por indução, ou recorrência). Enunciado sob propriedades em vez de conjuntos, ele se formula assim:

Seja  $P(n)$  uma propriedade relativa ao número natural  $n$ . Suponha que

i)  $P(1)$  é válida;

ii) Para todo  $n \in \mathbb{N}$ , a validade de  $P(n)$  implica a validade de  $P(n+1)$ , onde  $n+1$  é o sucessor de  $n$ .

Então  $P(n)$  é válida qualquer que seja o número natural  $n$ .

Com efeito, se chamarmos de  $X$  o conjunto dos números naturais  $n$  para os quais  $P(n)$  é válida, vemos que  $1 \in X$  em virtude de i) e que  $n \in X \implies n+1 \in X$  em virtude de ii). Logo pelo axioma de indução, concluímos que  $X = \mathbb{N}$ .

O axioma da indução é uma forma sagaz e operacional de dizer que qualquer número natural  $n$  pode ser alcançado se partimos de 1 e repetirmos suficientemente a operação de tomar o sucessor de um número. Ele está presente (pelo menos de forma implícita) sempre que, ao afirmarmos a veracidade de uma proposição referente aos números naturais, verificamos que ela é verdadeira para  $n = 1, n = 2, n = 3$  e dizemos e assim por diante...". (Ver mais nas referências [2], [3] e [10])

**Exemplo 2.1.** Seja  $s(n)$  uma função  $s : \mathbb{N} \rightarrow \mathbb{N}$ . Sendo  $s(n)$  uma função injetiva, onde para cada  $n \in \mathbb{N}$ , o número  $s(n)$  é o valor que a função assume no ponto  $n$ , é chamado sucessor de  $n$ . Mostre que para todo  $n \in \mathbb{N}$ , tem-se  $s(n) \neq n$ . (exemplo encontrado nas referências [2] e [3] )

**Demonstração** Consideremos  $X = \{n \in \mathbb{N}; s(n) \neq n\}$ . Tem-se  $1 \in X$ , pois 1 não é sucessor de número algum, em particular  $1 \neq s(1)$ . Além disso  $n \in X \implies n \neq s(n)$  (pela injetividade de  $s$ )  $s(n) \neq s[s(n)] \implies s(n) \in X$ . Assim,  $n \in X \implies s(n) \in X$ . Como  $1 \in X$ , segue-se do axioma de indução que  $X = \mathbb{N}$ , ou seja,  $n \neq s(n)$  para todo  $n \in \mathbb{N}$ .

**Exemplo 2.2.** Seja  $\mathcal{P}(X)$  o conjunto cujos os elementos são os subconjuntos de  $X$ . Prove por indução que se  $X$  é finito então  $\text{card } \mathcal{P}(X) = 2^{\text{card}(X)}$ . ( Estão como exercício nas referências [2] e [3])

**Demonstração** Para  $X = \{a\}$ ,  $\text{card } \mathcal{P}(X)$  é verdadeira, pois  $X = \{a\}$ ,  $\mathcal{P}(X) = \{\emptyset, \{a\}\}$ .  $\text{card } \mathcal{P}(X) = 2^1 = 2$ .

Suponhamos  $\text{card } \mathcal{P}(X) = 2^{\text{card}(X)}$ , para um conjunto  $X$  finito. Seja  $Y = X \cup \{a\}$  onde  $a \notin X$  então  $\mathcal{P}(Y)$  é formado pelas partes de  $Y$  que não contém  $a$  mais as que contém  $a$ . As primeiras constituem  $\mathcal{P}(X)$  e as outras são em mesmo número que as primeiras, logo  $\text{card } \mathcal{P}(Y) = 2 \text{card } \mathcal{P}(X) = 2^{\text{card}(X)+1}$ . O que prova para todo conjunto  $X$  finito.

**Exemplo 2.3.** Prove que  $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$ , para todo  $n \in \mathbb{N} \cup \{0\}$ .

**Demonstração** Para  $n = 0$ , temos

$$2^0 = 2^1 - 1,$$

logo a afirmação vale para  $n = 0$ .

Suponhamos que a sentença seja válida para um número natural  $k > 0$  e vamos mostrar que ela é válida para  $k + 1$ .

De fato,

$$\begin{aligned}(2^0 + 2^1 + \dots + 2^k) + 2^{k+1} &= (2^{k+1} - 1) + 2^k \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{k+2} - 1.\end{aligned}$$

Portanto,  $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$ , para todo  $n \in \mathbb{N} \cup \{0\}$ .

**Exemplo 2.4.** Prove que  $3 \mid (n^3 - n)$ , para todo  $n \in \mathbb{N} \cup \{0\}$ .

**Demonstração** Para  $n = 0$ ,

$$3 \mid (0^3 - 0) = 0,$$

logo a asserção é válida para  $n = 0$ .

Suponhamos que a afirmação acima seja válida para um número natural  $k > 0$ , isto é,  $k^3 - k = 3m$ , para algum  $m \in \mathbb{N}$  e vamos mostrar que ela é verdadeira para  $k + 1$ .

Temos

$$\begin{aligned}(k + 1)^3 - (k + 1) &= (k^3 + 3k^2 + 3k + 1) - (k + 1) \\ &= (k^3 - k) + 3(k^2 + k) \\ &= 3m + 3(k^2 + k),\end{aligned}$$

pois  $k^3 - k$  é múltiplo de 3, pela hipótese da indução.

Portanto,  $3 \mid (n^3 - n)$ , para todo  $n \in \mathbb{N} \cup \{0\}$ .

**Exemplo 2.5.** Demonstre que  $2^n > n^2$ , para todo número natural  $n \geq 5$ .

**Demonstração** Para  $n = 5$ , temos

$$2^5 = 32 > 5^2 = 25,$$

logo a afirmação é válida para  $n = 5$ .

Suponhamos que ela seja válida para  $k > 5$  e vamos mostrar que ela é válida para  $k + 1$ .

Realmente, pois

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &> 2 \cdot k^2 && \text{(pela hipótese indutiva)} \\ &= k^2 + k^2 \\ &\geq k^2 + 5k, && \text{(pois } k \geq 5\text{)} \\ &= k^2 + 2k + 3k \\ &> k^2 + 2k + 1 \\ &= (k + 1)^2. \end{aligned}$$

Portanto,  $2^n > n^2$ , para todo número natural  $n \geq 5$ .

**Exemplo 2.6.** Demonstre que  $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ , para todo  $n \in \mathbb{N}$ .

**Demonstração** Para  $n = 1$ , temos

$$1 = 1(1 + 1)/2 = 1,$$

assim a afirmação é válida para  $n = 1$ .

Suponhamos que a sentença seja válida para  $k > 1$ , e vamos mostrar que ela é verdadeira para  $k + 1$ .

Com efeito,

$$\begin{aligned}
1 + 2 + 3 + \cdots + k + (k + 1) &= \frac{k(k + 1)}{2} + (k + 1) \\
&= \frac{k(k + 1)}{2} + 2 \frac{(k + 1)}{2} \\
&= \frac{(k + 1)(k + 2)}{2}
\end{aligned}$$

Portanto,  $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ , para todo  $n \in \mathbb{N}$ .

**Exemplo 2.7.** Demonstre que  $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$ , para todo  $n \in \mathbb{N}$ .

**Demonstração** Para  $n = 1$ , temos

$$1^2 = 1(1 + 1)(2 \cdot 1 + 1)/6 = 6/6,$$

assim a afirmação é válida para  $n = 1$ .

Suponhamos que a sentença seja válida para  $k > 1$ , e vamos mostrar que ela é verdadeira para  $k + 1$ .

Com efeito,

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + k^2 + (k + 1)^2 &= \frac{k(k + 1)(2k + 1)}{6} + (k + 1)^2 \\
&= \frac{k(k + 1)(2k + 1)}{6} + 6 \frac{(k + 1)^2}{6} \\
&= \frac{(k + 1)(2k^2 + 7k + 6)}{6} \\
&= \frac{(k + 1)(k + 2)(2k + 3)}{6}.
\end{aligned}$$

Portanto,  $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$ , para todo  $n \in \mathbb{N}$ .

**Exemplo 2.8.** Demonstre que  $1^3 + 2^3 + 3^3 + \cdots + n^3 = [n(n + 1)/2]^2$ , para todo  $n \in \mathbb{N}$ .

**Demonstração** Para  $n = 1$ , a afirmação é válida, pois

$$1^3 = \left[ \frac{1(1 + 1)}{2} \right]^2.$$

Suponhamos que a sentença acima em questão seja válida para  $k > 1$ , vamos mostrar que ela é válida para  $k + 1$ .

De fato,

$$\begin{aligned}
 1^3 + 2^3 + 3^3 + \dots + k^3 + (k + 1)^3 &= \left[ \frac{k(k + 1)}{2} \right]^2 + (k + 1)^3 \\
 &= \frac{k^2(k + 1)^2}{4} + (k + 1)^3 \\
 &= \frac{k^2(k + 1)^2}{4} + 4 \frac{(k + 1)^2(k + 1)}{4} \\
 &= \frac{(k + 1)^2(k^2 + 4k + 4)}{4} \\
 &= \frac{(k + 1)^2(k + 2)^2}{4} \\
 &= \left[ \frac{(k + 1)(k + 2)}{2} \right]^2.
 \end{aligned}$$

Portanto,  $1^3 + 2^3 + 3^3 + \dots + n^3 = [n(n + 1)/2]^2$ , para todo  $n \in \mathbb{N}$ .

As propriedades da soma e da multiplicação podem ser provadas por esse engenhoso processo de demonstração. Para isso vamos definir essas operações.

A *adição*, que associa a cada par de números  $m$  e  $n$  sua *soma*  $m + n$ , e a *multiplicação*, faz corresponder ao par  $m$  e  $n$  seu produto  $m \cdot n$ . Essas operações são caracterizadas pelas seguintes igualdades, que lhes servem de definição:

$$m + 1 = s(m), \text{ onde } s(m) \text{ é o sucessor de } m;$$

$$m + s(n) = s(m + n), \text{ isto é, } m + (n + 1) = (m + n) + 1;$$

$$m \cdot 1 = m;$$

$$m \cdot s(n) = m \cdot (n + 1) = m \cdot n + m.$$

Em outros termos, somar 1 a  $m$  significa tomar o sucessor de  $m$ . E se já conhecemos a soma  $m + n$  também conheceremos  $m + (n + 1)$ , que é o sucessor de  $m + n$ . Quanto a multiplicação, multiplicar por 1 não altera o número. E se conhecermos o produto  $m \cdot n$ , conheceremos  $m \cdot (n + 1) = m \cdot n + m$ .

A partir do que foi definido como adição e multiplicação de números naturais pode-se enun-

ciar suas propriedades.

Para todo  $m, n, p \in \mathbb{N}$ , tem-se:

1. associatividade :  $(m + n) + p = m + (n + p)$ ,  $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ ;
2. distributividade :  $p \cdot (m + n) = p \cdot m + p \cdot n$ ;
3. comutatividade :  $m + n = n + m$ ,  $m \cdot n = n \cdot m$ ;
4. lei do corte:  $n + m = p + m \implies n = p$ ,  $n \cdot m = p \cdot m \implies n = p$

## Demonstração

**1. Adição,** fixaremos  $m$  e  $n$  e utilizaremos indução sobre  $p$ .

(i) Se  $p = 1$ , então  $m + (n + 1) = m + s(n) = s(m + n) = (m + n) + 1$ , como foi visto na definição da adição.

(ii) Supondo  $(m + n) + p = m + (n + p)$  e utilizando a definição da adição, temos  $(m + n) + s(p) = s([(m + n) + p])$ , que por hipótese é igual a  $s([m + (n + p)]) = m + s(n + p)$ , que por sua vez é igual a  $m + (n + s(p))$ . Portanto, pelo Princípio da Indução Matemática,  $(m + n) + p = m + (n + p)$ .

**1. Multiplicação,** usando a indução sobre  $p$ .

(i) Se  $p = 1$ , então  $m \cdot (n \cdot 1) = m \cdot n = (m \cdot n) \cdot 1$ , como foi visto na definição de multiplicação.

(ii) Supondo  $m \cdot (n \cdot p) = (m \cdot n) \cdot p$  e utilizando a definição de multiplicação, temos  $m \cdot (n \cdot s(p)) = m \cdot (n \cdot p + n)$ . Pela propriedade distributiva, isto é igual a  $m \cdot (n \cdot p) + (m \cdot n)$ , que por hipótese é igual a  $(m \cdot n) \cdot p + (m \cdot n)$ , que pela definição de multiplicação é igual a  $(m \cdot n) \cdot s(p)$ . Portanto, pelo Princípio da Indução Matemática,  $m \cdot (n \cdot p) = (m \cdot n) \cdot p$ .

(2) *Distributividade*, novamente indução sobre  $p$ .

(i) Se  $p = 1$ , temos  $1 \cdot (m + n) = m + n = 1 \cdot m + 1 \cdot n$ , como foi visto na definição.

(ii) Supondo  $p \cdot (m + n) = p \cdot m + p \cdot n$ , e utilizando a definição de multiplicação temos que,  $s(p) \cdot (m + n) = p \cdot (m + n) + (m + n)$ , que por hipótese  $p \cdot m + p \cdot n + m + n$ . Por sua vez, isto é igual a  $(p \cdot m + m) + (p \cdot n + n) = s(p) \cdot m + s(p) \cdot n$ . Portanto, pelo Princípio da Indução Matemática,  $p \cdot (m + n) = p \cdot m + p \cdot n$

(3) *Adição*, indução sobre  $m$ .

(i) Se  $m = 1$ , então  $1 + n = s(n) = n + 1$ . Pela definição de sucessor.

(ii) Supondo  $m + n = n + m$ , e usando a definição de soma, temos  $s(m) + n = s(m + n)$ , que por hipótese é igual a  $s(n + m) = n + m + 1 = n + s(m)$ . Portanto pelo Princípio da

Indução Matemática,  $m + n = n + m$ .

(3) *Multiplicação*, novamente indução sobre  $m$ .

(i) Se  $m = 1$ , então  $1 \cdot n = n = n \cdot 1$ , Pela definição de multiplicação.

(ii) Supondo  $m \cdot n = n \cdot m$ , temos que  $s(m) \cdot n = (m + 1) \cdot n$ , e pela distributividade,  $m \cdot n + n$ , onde por hipótese  $n \cdot m + n$ , que pela definição de multiplicação é igual a  $n \cdot s(m)$ . Portanto pelo Princípio da Indução Matemática,  $m \cdot n = n \cdot m$

(4) *Adição*, usando indução sobre  $m$ .

(i) Se  $m = 1$ , então  $n + 1 = p + 1$ , significa que  $s(n) = s(p)$ , logo  $n = p$  pela injetividade de  $s$ .

(ii) Supondo  $n + m = p + m \implies n = p$ , então  $n + m + 1 = p + m + 1$ . Novamente pela injetividade de  $s$ , tem-se  $n + m = p + m$ , que por hipótese de indução  $n = p$ .

(4) *Multiplicação*, usando indução sobre  $m$ .

(i) Se  $m = 1$ , então  $n \cdot 1 = p \cdot 1$ , que pela definição de multiplicação é igual a  $n = p$ .

(ii) Supondo  $n \cdot m = p \cdot m \implies n = p$ , temos que  $n \cdot (m + 1) = p \cdot (m + 1)$ , pela distributividade  $n \cdot m + n = p \cdot m + p$ , onde por hipótese  $n \cdot m = p \cdot m$  e pela lei do corte da adição temos que  $n = p$ .

( Foram construídas a partir das referências [2], [3] e [10] )

## 2.2.2 Ordem entre os números naturais

Nossa breve descrição do conjunto  $\mathbb{N}$  dos números naturais termina com a relação de ordem  $m < n$ .

Dados  $m, n \in \mathbb{N}$ , diz-se que  $m$  é menor do que  $n$ , e escreve-se  $m < n$ , para significar que existe algum  $p \in \mathbb{N}$  tal que  $n = m + p$ . ( isto quer dizer  $n$  é o sucessor do sucessor...do sucessor de  $m$ , o ato de tomar o sucessor sendo  $p$  vezes)

A relação  $m < n$  tem as seguintes propriedades:

*Transitividade:* Se  $m < n$  e  $n < p$  então  $m < p$ .

*Tricotomia:* Dados  $m, n \in \mathbb{N}$ , vale uma, e somente uma, das alternativas:  $m = n$ ,  $m < n$  ou  $m > n$ .

*Monotonicidade:* Se  $m < n$  então, para qualquer  $p \in \mathbb{N}$ , tem-se  $m + p < n + p$  e  $mp < np$ .

**Teorema 2.2.1. (Princípio da Boa Ordenação).** *Todo subconjunto não vazio  $A \subseteq \mathbb{N}$  possui um elemento mínimo.*

**Demonstração.** O enunciado do teorema é equivalente a dizer que *Todo subconjunto não vazio  $A \subset \mathbb{N}$  possui um menor elemento, isto é, um elemento  $n_0 \leq n$  para todo  $n \in A$ .*

Afim de provar esta afirmação, para cada  $n \in \mathbb{N}$ , chamemos de  $I_n$  o conjunto dos números naturais  $\leq n$ , ou seja,  $I_n = \{1, 2, \dots, n\}$ . Se  $1 \in A$  então 1 será o menor elemento de  $A$ . Se, porem  $1 \notin A$ , então consideremos o conjunto  $X$  dos números naturais  $n$  tais que  $I_n \subset \mathbb{N} - A$  (assim, dizer que  $n \in X$  significa afirmar que  $n \notin A$  e que todos os números naturais menores



do que  $n$  também não pertencem a  $A$ ). Como  $I_1 = \{1\} \subset \mathbb{N} - A$ , vemos que  $1 \in X$ . Por outro lado, como  $A$  não é vazio, concluímos que  $X \neq \mathbb{N}$ . Logo a conclusão do axioma da indução não é válido. Segue-se que deve existir  $n \in X$  tal que  $n + 1 \notin X$ . Então  $I_n = \{1, 2, \dots, n\} \subset \mathbb{N} - A$  mas  $n_0 = n + 1 \in A$ . Portanto  $n_0$  é o menor elemento do conjunto  $A$ , pois não existe número natural entre  $n$  e  $n + 1$ . (Outras formas de demonstração ver nas referências [2], [3] e [10])

### 2.2.3 Conjunto finitos e conjuntos infinitos

O estudo sistemático dos conjuntos, que acabou levando a uma teoria axiomática desse campo de estudo, começou com George Cantor, por volta de 1872. Nessa época, Cantor estava iniciando sua carreira profissional e se ocupava do estudo da representação de funções por meio de séries trigonométricas. Nessa ocupação ele foi levado a investigar os conjuntos de pontos de descontinuidade de tais funções, os mais simples dos quais são conjuntos com apenas um número finito de pontos. Mas o aparecimento de conjuntos cada vez mais complicados acabou levando Cantor a investigar conjuntos infinitos em sua generalidade. Nesse estudo ele introduziu um conceito simples, que logo se revelaria da maior importância. (O conceito de equivalência de conjuntos).

Segundo Cantor, dois conjuntos são *equivalentes*, ou tem a mesma *cardinalidade*, ou a mesma *potência*, quando é possível estabelecer uma correspondência que leve elementos distintos de um conjunto em elementos distintos do outro conjunto, todos os elementos de um e do outro conjunto sendo objeto dessa correspondência. Em termos precisos, a correspondência que estamos falando chama-se *bijecção*.

Observe que é essa noção de equivalência que dá origem ao conceito abstrato de número natural. De fato, o que faz uma criança de quatro ou cinco anos de idade constatar que numa cesta há três laranjas, noutra três maçãs, e ainda noutra três ovos? Ela chega a essa conclusão, mesmo sem perceber, por constatar que é possível “casar” os elementos de qualquer uma dessas cestas com os elementos de qualquer outra de maneira biunívoca. É essa abstração dos elementos concretos dos conjuntos equivalentes de diferentes objetos que nos leva a formar a noção de números naturais, um fenômeno que ocorre muito cedo em nossas vidas.

Assim vamos denotar por  $F_n$  o conjunto dos primeiros números naturais,  $F_n = \{1, 2, 3, \dots, n\}$ , é precisamente o fato de um conjunto  $A$  ser equivalente (ou equipotente) a  $F_n$  que nos faz dizer que  $A$  tem  $n$  elementos, ou que tem o mesmo número de elementos de  $F_n$ .

Daí definimos: Um conjunto  $A$  se diz *finito* quando existe um número natural  $n$  tal que  $A$  seja equipotente ao conjunto  $F_n$ .

Um conjunto se diz *infinito* quando não for finito.

No caso de conjuntos finitos, serem equipotentes corresponde a terem o mesmo número de elementos, de sorte que o conceito de cardinalidade é o recurso natural para estender, a conjuntos infinitos, o conceito de “número de elementos de um conjunto”

Diz-se que dois conjuntos quaisquer  $A$  e  $B$  têm a mesma *cardinalidade*, ou o mesmo *número*

de elementos, se eles forem equipotentes. Como se vê, essa definição, no caso de conjuntos finitos, não traz nada de novo, mas estende, para conjuntos infinitos, a noção de “números de elementos de um conjunto”. Tais números são chamados *números transfinitos*. (Ver mais na referência [6])

Podemos dizer que dado  $n \in \mathbb{N}$ , indiquemos com a notação  $I_n$  o conjunto dos números naturais de 1 até  $n$ . Assim,  $I_1 = \{1\}$ ,  $I_2 = \{1, 2\}$ ,  $I_3 = \{1, 2, 3\}$  e, mais geralmente, um número  $k$  pertence a  $I_n$  se, somente se,  $1 \leq k \leq n$ .

Seja  $X$  um conjunto. Diz-se que  $X$  é *finito*, e que  $X$  tem  $n$  elementos quando se pode estabelecer uma correspondência biunívoca  $f : I_n \rightarrow X$ . O número natural  $n$  chama-se então o *número cardinal* do conjunto  $X$  ou, simplesmente, o número de elementos de  $X$ . A correspondência  $f : I_n \rightarrow X$  chama-se uma *contagem* dos elementos de  $X$ . Pondo  $f(1) = x_1$ ,  $f(2) = x_2, \dots, f(n) = x_n$ , podemos escrever  $X = \{x_1, x_2, \dots, x_n\}$ . Para todo  $n$ ,  $I_n$  é finito e seu número cardinal é  $n$ . Assim, todo número  $n$  é o conjunto cardinal de algum conjunto finito.

A fim de evitar exceções, admite-se ainda incluir o conjunto vazio  $\emptyset$  entre os conjuntos finitos e diz-se que  $\emptyset$  tem zero elementos. Assim, por definição, zero é o número cardinal do conjunto vazio.

Diz-se que um conjunto  $X$  é *infinito* quando ele não é finito. Isto quer dizer que  $X$  não é vazio e que, não importa qual seja  $n \in \mathbb{N}$ , não existe correspondência biunívoca  $f : I_n \rightarrow X$ .

O conjunto  $\mathbb{N}$  dos números naturais é infinito. Com efeito, dada qualquer função  $f : I_n \rightarrow \mathbb{N}$ , não importa qual  $n$  fixou, podemos  $k = f(1) + f(2) + \dots + f(n)$  e vemos que, para todo  $x \in I_n$ , tem-se  $f(x) < k$ , logo não existe  $x \in I_n$  tal que  $f(x) = k$ . Assim, é impossível cumprir as condições de correspondência biunívoca.

O número cardinal de um conjunto finito  $X$ , que indicaremos com a notação  $n(X)$ , goza de qualquer propriedade básica, entre as quais destacaremos as seguintes:

1. O número de elementos de um conjunto finito é o mesmo, seja qual for a contagem que se adote.

Isto significa que se  $f : I_m \rightarrow X$  e  $g : I_n \rightarrow X$  são correspondências biunívocas então  $m = n$ .

2. Todo subconjunto  $Y$  de um conjunto finito  $X$  é finito e  $n(Y) \leq n(X)$ . Tem-se  $n(Y) = n(X)$  somente quando  $X = Y$ .

3. Se  $X$  e  $Y$  são finitos então  $X \cup Y$  é finito e tem-se  $n(X \cup Y) = n(X) + n(Y) - n(X \cap Y)$ .

4. Sejam  $X, Y$  conjuntos finitos. Se  $n(X) > n(Y)$ , nenhuma função  $f : X \rightarrow Y$  é injetiva e nenhuma função  $g : Y \rightarrow X$  é sobrejetiva.

A primeira parte do item 4 é conhecida como o *princípio da casa dos pombos*: se há mais pombos do que casas num pombal, qualquer modo de alojar os pombos deverá colocar pelo menos dois deles na mesma casa. Às vezes, o mesmo fato é chamado *o princípio das gavetas*: se  $m > n$ , qualquer maneira de distribuir  $m$  objetos em  $n$  gavetas deverá por ao menos dois desses objetos na mesma gaveta. (Para aprofundar o conhecimento referências [2], [3], [6] e [10]).

O princípio das casas dos pombos com toda sua simplicidade, possui interessantes aplicações. Vejamos os exemplos.

**Exemplo 2.9.** Tomemos um número natural de 1 a 9. Para fixar as ideias, seja 3 esse número. Vamos provar que todo número natural  $m$  possui um múltiplo cuja representação decimal contém apenas os algarismos 3 ou 0. Para isso considere o conjunto  $X = \{3, 33, \dots, 33\dots3\}$  cujos elementos são os  $m$  primeiros números naturais representados somente por algarismos iguais a 3. Se algum dos elementos de  $X$  for múltiplo de  $m$ , nosso trabalho acabou. Caso contrário, formamos o conjunto  $Y = \{1, 2, \dots, m - 1\}$  e definimos a função  $f : X \rightarrow Y$  pondo, para cada  $x \in X$ ,

$$f(x) = \text{resto da divisão de } x \text{ por } m.$$

Como  $X$  tem mais elementos do que  $Y$ , o princípio das casas de pombos assegura que existem elementos  $x_1 < x_2$  no conjunto  $X$  tais que  $f(x_1) = f(x_2)$ . Isto significa que  $x_1$  e  $x_2$ , quando divididos por  $m$ , deixam o mesmo resto. Logo  $x_2 - x_1$  é múltiplo de  $m$ . Mas é claro que  $x_1$  tem  $p$  algarismos e  $x_2$  tem  $p + q$  algarismos então a representação decimal de  $x_2 - x_1$  consiste em  $q$  algarismos iguais a 3 seguidos de  $p$  algarismos iguais a 0.

**Exemplo 2.10.** Vamos usar o princípio das gavetas para provar que, numa reunião com  $n$  pessoas ( $n \geq 2$ ), há sempre duas pessoas (pelo menos) que têm o mesmo número de amigos naquele grupo. Para ver isto, imaginemos  $n$  caixas, numeradas com  $0, 1, \dots, n - 1$ . A cada uma das  $n$  pessoas entregamos um cartão que pedimos para depositar na caixa correspondente ao número de amigos que ele tem naquele grupo. As caixas de números  $0$  e  $n - 1$  não podem ambas receber cartões pois se houver alguém que não tem amigos ali, nenhum dos presentes pode ser amigo de todos, e vice-versa. Portanto temos, na realidade,  $n$  cartões para serem depositados em  $n - 1$  caixas. Pelo princípio das gavetas, pelo menos uma das caixas vai receber dois ou mais cartões. Isto significa que duas ou mais pessoas ali têm o mesmo número de amigos entre os presentes.

## 2.2.4 Um pouco mais sobre conjuntos infinitos

Para encerrar estas considerações a respeito de números cardinais, faremos alguns comentários sobre conjuntos infinitos.

Em primeiro lugar, convém esclarecer que a maior contribuição de Cantor não foi a adoção da linguagem e da notação dos conjuntos e sim suas descobertas sobre os números cardinais de conjuntos infinitos. Ele foi o primeiro a descobrir que existem conjuntos infinitos com diferentes cardinalidade ao provar que não pode haver uma correspondência biunívoca entre  $\mathbb{N}$  e o conjunto  $\mathbb{R}$  dos números reais e que nenhum conjunto  $X$  pode estar em correspondência biunívoca com o conjunto  $\mathcal{P}(X)$  cujos elementos são os subconjuntos de  $X$ . Além disso, ele mostrou que a reta, o plano e o espaço tridimensional (ou mesmo espaço com dimensões superiores a três) têm o mesmo número cardinal. Estes fatos, que atualmente são considerados corriqueiros entre os matemáticos, causaram forte impacto na época (meados do século dezenove).

A segunda observação diz respeito a função  $f : X \rightarrow X$  de um conjunto em si mesmo. Quando  $X$  é finito,  $f$  é injetiva se, e somente se, é sobrejetiva. Mas isso não é verdade para  $X$  infinito. Por exemplo, se definirmos a função  $f : \mathbb{N} \rightarrow \mathbb{N}$  pondo para cada  $n \in \mathbb{N}$ ,  $f(n) =$  número de fatores primos distintos que ocorrem na decomposição de  $n$ , veremos que  $f$  é sobrejetiva mas não injetiva. (para cada  $b \in \mathbb{N}$  existe uma infinidade de números  $n$  tais que  $f(n) = b$ ). Além disso, as funções  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $g : \mathbb{N} \rightarrow \mathbb{N}$ ,  $h : \mathbb{N} \rightarrow \mathbb{N}$  e  $s : \mathbb{N} \rightarrow \mathbb{N}$ , definidas por

$$f(n) = n + 1$$

$$g(n) = n + 30$$

$$h(n) = 2n$$

$$s(n) = 3n$$

são injetivas mas não sobrejetivas. Estas quatro funções são protagonistas de seguinte história qua fecha a seção.

## FANTASIA MATEMÁTICA

O Grande Hotel de Georg Cantor tinha uma infinidade de quartos, numerados consecutivamente, um para cada número natural. Todos eram igualmente confortáveis. Num fim de semana prolongado, o hotel estava com seus quartos todos ocupados, quando chega um viajante. A recepcionista vai logo dizendo:

-Sinto muito, mas não há vagas.

Ouvindo isso o gerente interveio:

- Podemos abrigar o cavalheiro, sim senhora.

E ordena:

- Transfira o hóspede do quarto 1 para o quarto 2, passe o do quarto 2 para o quarto 3 e assim por diante. quem estiver no quarto  $n$ , mude para o quarto  $n + 1$ . Isto manterá todos alojados e deixará disponível o quarto 1 para o recém-chegado.

Logo depois chegou um ônibus com 30 passageiros, todos querendo hospedagem. A recepcionista, tendo aprendido a lição, removeu o hóspede de cada quarto  $n$  para o quarto  $n + 30$  e acolheu assim todos os passageiros do ônibus. Mas ficou sem saber o que fazer quando, horas depois, chegou um trem com uma infinidade de passageiros. Desesperada, apelou para o gerente que prontamente resolveu o problema dizendo: - passe cada quarto  $n$  para o quarto  $2n$ . Isto deixará vagos todos os apartamentos de número ímpar, nos quais poremos os novos hóspedes. - Pensando melhor: mude quem está no quarto  $n$  para o quarto  $3n$ . Os novos hóspedes, ponha-os nos quartos de número  $3n + 2$ . Deixaremos vagos os quartos de número  $3n + 1$ . Assim, sobrarão ainda infinitos quartos vazios e eu poderei ter sossego por algum tempo.

Para finalizar, é bom não confundirmos conjuntos infinitos com aquele que tem um número muito grande (podem finito) de elementos. Quando, na linguagem comum, se diz algo como “- Já ouvi isto uma infinidade de vezes”, trata-se de uma mera força de expressão. Não há distâncias infinitas (mesmo entre duas galáxias bem afastadas) e até o número de átomos do universo é finito. (o físico Arthur Eddington estimou o número de prótons do universo em  $136 \times 2^{256}$ . O número de átomos é certamente menos pois todo átomo contém ao menos um próton.)

É importante ter sempre em mente que nenhum número natural  $n$  é maior do que todos os demais: tem-se sempre  $n < n + 1$ .

## 2.2.5 Notas históricas sobre teoria dos conjuntos

### A teoria dos conjuntos

Foi por volta de 1960 que a noção de conjuntos foi introduzida no ensino básico, na maior parte dos países do mundo, inclusive no Brasil. E trouxe mais malefícios do que vantagens. Tanto assim que em países desenvolvidos, como os Estados Unidos, a abordagem de conjuntos declinou rapidamente já no final da década de 60, e estava praticamente eliminada no início dos anos 70. Já no Brasil o hábito de incluir conjuntos no ensino básico perdurou por muito mais tempo.

### Cantor e os conjuntos infinitos

Bernhard Bolzano foi quem primeiro falou livremente de conjuntos infinitos. Ele escreveu um livro sobre os paradoxos do infinito, publicado postumamente em 1859, no qual aborda várias questões de natureza filosófica e matemática acerca dos conjuntos infinitos. Richard Dedekind foi mais longe que Bolzano, utilizando a noção de conjunto na construção dos números reais. Mas foi Georg Cantor quem mais avançou no estudo dos conjuntos. Logo no início de um de seus trabalhos sobre os números transfinitos ele define conjunto com as seguintes palavras: *por conjuntos entendemos qualquer coleção numa totalidade  $M$  de objetos distintos, produto de nossa intuição ou pensamento.*

A rigor, isto não é bem uma definição, pois exige que já saibamos o que seja “coleção”, vocábulo esse que é sempre tomado como sinônimo de conjuntos. Na verdade, Cantor está apenas explicando, em linguagem imprecisa que seja, sua percepção do conceito de conjunto, que, diga-se de passagem, era a única que poderia ocorrer a qualquer matemático do seu tempo. Veremos que esse conceito, utilizado livremente, pode levar a sérias contradições.

### Teorema de Cantor e infinidade dos números transfinitos

A noção de cardinalidade ou potência de um conjunto permitiu que Cantor introduzisse e estudasse os “números transfinitos”, que nada mais são do que as potências dos conjuntos infinitos. Em particular, Cantor mostrou como ordenar os conjuntos segundo suas potências.

Assim, denotamos as potências com os mesmos símbolos com que estamos denotando os conjuntos, podemos escrever  $\mathbb{N} = \mathbb{P} = \mathbb{I} = \mathbb{Q} < \mathbb{R}$ , onde  $\mathbb{N}$ ,  $\mathbb{P}$ ,  $\mathbb{I}$ ,  $\mathbb{Q}$  e  $\mathbb{R}$  denotam os conjuntos dos números naturais, dos pares, dos Impares, dos Racionais e dos Reais. respectivamente.

Vamos mostrar como cantor logrou construir toda uma infinidade de números transfinitos, ou seja, uma infinidade de conjuntos infinitos, todos com diferentes potências.

Primeiro vamos ilustrar a construção no caso de um conjunto finito bem simples, com apenas três elementos, digamos o conjunto  $M = \{a, b, c\}$ . Vamos formar o conjunto de todos os subconjuntos de  $M$ . Denotando, como de costume, o conjunto vazio por  $\emptyset$ , esses subconjuntos são os oito conjuntos seguintes:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$$

O conjunto de todos esses subconjuntos, chamado o *conjunto das partes de  $M$* , costuma ser denotado com o símbolo  $\mathcal{P}(M)$ . Assim,

$$\mathcal{P}(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Já observamos que a noção de potência permite ordenar os conjuntos. Assim, no caso do conjunto  $M$  que estamos considerando, temos, em termos de suas potências,  $M < \mathcal{P}(M)$ . Este fato, aqui ilustrado no caso de um conjunto de três elementos, pode ser facilmente demonstrado para qualquer conjunto finito; e pode ser demonstrado, sem muita dificuldade, para conjuntos quaisquer, finitos ou infinitos. Esse resultado de Cantor permite construir, a partir de um conjunto infinito inicial  $M$  toda uma infinidade de conjuntos infinitos com cardinalidade crescente:

$$M < \mathcal{P}(M) < \mathcal{P}(\mathcal{P}(M)) < \mathcal{P}(\mathcal{P}(\mathcal{P}(M))) < \dots$$

resultado esse que também é devido a Cantor.

**Teorema 2.2.2. Teorema de Cantor.** *Qualquer que seja o conjunto  $M$ , sua potência é sempre menor do que a potência de  $\mathcal{P}(M)$ , isto é,  $\#M < \#\mathcal{P}(M)$ .*

**Demonstração** A aplicação de  $m \in M \rightarrow \{m\} \in \mathcal{P}(M)$  é injetiva, portanto prova que,  $\#M \leq \#\mathcal{P}(M)$

Para efetivamente provar que  $\#M < \#\mathcal{P}(M)$ , seja  $m \in M \rightarrow M_m$  uma aplicação qualquer de  $M$  em  $\mathcal{P}(M)$ , onde  $M_m$  é o subconjunto de  $M$  que é a imagem de  $m$  pela referida aplicação. Em seguida consideremos o conjunto  $B = \{x \in M; x \notin M_x\}$ , que é um subconjunto de  $M$ , podendo mesmo ser o conjunto vazio. Vamos mostrar que ele difere de qualquer  $M_m$ , com  $m$  variando em  $M$ . De fato, qualquer que seja  $m \in M$ ,  $B$  e  $M_m$  diferem pelo mesmo elemento  $m$ , pois

$$m \in B \implies m \notin M_m$$

e

$$m \notin B \implies m \in M_m$$

Sendo  $B$  diferente de todo  $M_m$ , com  $m$  variando em  $M$ , vemos que não existe aplicação de  $M$  sobre  $\mathcal{P}(M)$ , muito menos biunívoca (ou bijetora). concluímos, pois, que  $\#M < \#\mathcal{P}(M)$ , como queríamos provar.

### O paradoxo de Cantor

Vamos descrever agora um dos primeiros paradoxos da teoria dos conjuntos, surgido com o próprio Cantor. Aceitado a definição de conjuntos dado por Cantor, podemos conceber o conjunto  $U$  de todos os conjuntos. Esse conjunto  $U$  seria, por assim dizer, *o conjunto universal*, portanto, teria potência máxima, já que reuniria todos os conjuntos passíveis de consideração. Em particular, ele teria de ser um elemento de si mesmo, o que já é, em si, um pouco estranho. Pior que isto é que, ao considerarmos o conjunto das partes de  $U$ , isto é, o conjunto  $P(U)$ , somos levados, pelo próprio teorema de Cantor, a concluir que  $P(U) > U$ . Ora, isto contradiz a suposição inicial, de que existe um conjunto universal  $U$ , ou conjunto de todos os conjuntos.

### Frege e o paradoxo de Russell

Dentre os muitos outros paradoxos que foram sendo descobertos, merece especial atenção o chamado paradoxo de Russell, que está contido em uma carta que Bertrand Russell escreveu a Gottlob Frege em 1902. Frege recebeu a carta de Russell no momento em que estava para publicar o segundo volume de uma obra em que fundamentava toda a aritmética na teoria dos conjuntos. Ele reagiu com as seguintes palavras: “nada mais indesejável para um cientista do que ver ruir os fundamentos do edifício, justamente no momento em que ele está sendo construído. Foi nessa incômoda situação que me encontrei ao receber uma carta do Sr. Bertrand Russell no momento em que meu trabalho já estava indo para o prelo”.

Para explicar o paradoxo de Russell, começamos observando que um conjunto pode ser elemento de outro conjunto, como já vimos atrás, no caso do conjunto das partes de um dado conjunto. Outro exemplo: Uma reta é um conjunto de pontos; e podemos formar o conjunto das retas de um dado plano, portanto, um conjunto de conjunto.

Um conjunto pode ser elementos de si mesmo, como o conjunto de todas as ideias abstratas, pois tal conjunto também é uma ideia abstrata; portanto, ele é um elemento de si mesmo. Outro exemplo: o conjunto dos conjuntos que possuem mais de dois elementos é um elemento de si mesmo, pois ele com certeza possui mais de dois elementos.

Não se pertube o leitor se achar muito estranha essa ideia de um conjunto pertencer a si mesmo. Falamos dela somente porque desejamos, isto sim, considerar conjuntos que não pertencem a si mesmos, como o conjunto dos números naturais, dos inteiros, dos divisores de 360, o conjunto dos vértices de um poliedro, etc.

Vamos considerar o conjunto de todos os conjuntos que não pertencem a si mesmos, e que

denotaremos por  $M$ . Assim, de maneira simbólica e explicada,

$$M = \{x; x \notin x\}.$$

Pergunta:  $M \in M$  ? Não, pois  $M$  seria um certo  $x$  tal que  $x \in x$ , donde, pela definição de  $M$ ,  $x \notin M$ , isto é,  $M \notin M$ . Será então que  $M \notin M$  ? Também não, pois  $M$  seria um certo  $x$  tal que  $x \notin x$ , donde, pela definição de  $M$ ,  $x \in M$ , isto é,  $M \in M$ .

Em resumo,

$$M \in M \Leftrightarrow M \notin M$$

Estamos diante de um paradoxo, que surgiu da consideração do conjunto  $M$  de todos os conjuntos que não pertencem a si mesmo.

### **Por que surgem os paradoxos ?**

Nada há de errado com o raciocínio que acaba nos levando, tanto ao paradoxo de cantor como ao de Russell. Se não há nada de errado, como então fomos chegar a esses paradoxos?

Os paradoxos surgem porque o universo do discurso é muito amplo; e acaba abarcando essas contradições. O próprio conceito de conjuntos, segundo Cantor, foi originalmente concebido de maneira muito livre, e acabou levando o próprio Cantor a um paradoxo insuperável.

Veja este exemplo, mostrando a que nos leva o uso muito livre da linguagem: um rei mandou dizer a um condenado que ele morreria na fogueira se as últimas palavras do condenado encerrassem uma verdade; e morreria na forca se falasse uma falsidade. O condenado disse: vou morrer na forca. Em consequencia, o rei não pode executá-lo nem na fogueira (se não o condenado teria dito uma falsidade), nem na forca (se não o condenado teria falado uma verdade). E por que esse impasse? Simplesmente porque a decisão final depende de algo fluido, aquilo que o condenado ainda vai falar. Isso não pode ser permitido; o universo do discurso tem de ser devidamente restrito para não abrigar possíveis contradições ou impasses.

Por causa dos paradoxos, alguma coisa tinha de ser feito. Foi então que vários matemáticos cuidaram de formular um sistema de axiomas, a partir dos quais fosse possível estabelecer os resultados da teoria, libertando-a, ao mesmo tempo, dos paradoxos que vinham surgindo e de outros mais que pudessem aparecer.

### **Zermelo e o axioma da especificação**

Ernst Zermelo foi um dos matemáticos que mais sucesso tiveram nesse empreendimento de axiomatizar devidamente a teoria dos conjuntos. Nascido em Berlim, Zermelo estudou Matemática, Física e Filosofia nas universidades de Berlim, Halle e Freiburg. Foi professor em Gotingen e Zuruque. Ainda cedo em sua vida profissional, Zermelo teve de interromper sua carreira por problemas de saúde e, mais tarde, por problemas com o regime nazista de Hitler. Embora seus principais trabalhos situem-se na área de lógica e fundamentos da matemática, Zermelo também possui contribuições em Mecânica e Análise Aplicada.



Em suas considerações sobre os paradoxos, notadamente os de Cantor e Russell, Zermelo percebeu que duas coisas não poderiam coexistir: a consideração livre de conjuntos, como o conjunto universal, e a caracterização de um conjunto por uma propriedade de seus elementos (sem maiores restrições). Ora, esta última condição era muito natural e não deveria ser descartada. Zermelo optou pela impossibilidade de se considerar conjuntos sem qualquer restrição, como no caso do conjunto de todos os conjuntos, ou o conjunto de todos os conjuntos que não pertence a si mesmo. Ele teve a intuição de que seria possível considerar conjuntos infinitos, porém, sempre a partir de algum conjunto pre-existente. Assim, de posse do conjunto dos números naturais  $\mathbb{N}$ , podemos considerar o conjunto de pares de números naturais  $(a, b)$ , com  $b \neq 0$ , a partir dos quais construímos o conjunto dos números racionais; a partir deste conjunto podemos construir o conjunto dos números reais, depois o dos complexos. Conjuntos mais e mais amplos, em termos de cardinalidade, podem ser formados a partir de qualquer conjunto  $M$ , em particular a sequência crescente

$$M < P(M) < P(P(M)) < P(P(P(M))) < \text{etc.}$$

Foi seguindo essa linha de raciocínio que Zermelo formulou o seguinte axioma, que veio a ser chamado *axioma da especificação*:

*Dado um conjunto  $A$  e uma propriedade  $P(x)$ , existe um conjunto  $M$  cujos elementos são os elementos de  $A$  que satisfazem a propriedade  $P(x)$ . Simbolicamente.*

$$M = \{x \in A; P(x)\}$$

É interessante observar que estamos, a toda hora, usando este axioma na formação de novos conjuntos a partir de um conjunto dado, frequentemente sem perceber a interveniência do axioma. Considere, por exemplo, as afirmações: “o conjunto das raízes reais do polinômio  $x^5 - 7x^3 + 1$ ”; “o conjunto dos triângulos de base  $AB$  e altura  $h$ ”; “o conjunto dos coeficientes binomiais de ordem 7”. Em todos esses casos estamos formando conjuntos com a ajuda do axioma da especificação.

Vários outros axiomas são necessários para construir axiomáticamente a teoria dos conjuntos. E o conceito de conjuntos aparece então como *conceito primitivo*, sem definição em termos de noções precedentes, sendo delimitado apenas pelos axiomas.

### **O paradoxo de Richard**

Mas será mesmo que o axioma da especificação terá exorcizado todo e qualquer paradoxo da teoria dos conjuntos? Faremos um teste, tentando construir o conjunto de todos os conjuntos de números naturais que podem ser descritos com menos de 20 palavras na língua portuguesa. Exemplo de tais: o maior divisor primo do número 4056; o número de pessoas registrada no cartório de Goiânia; o número de gols válidos marcados em partidas jogadas no estádio do Maracanã desde 1950. Todos estes números estão bem definidos com menos palavras da língua

portuguesa.

Seja  $M$  o conjunto que estamos especificando, isto é,  $M$  é o conjunto dos números naturais que podem ser descritos com menos de 20 palavras. Trata-se de um conjunto finito, pois finito é o número de arranjos de todas as palavras da língua portuguesa em grupo de menos de 20 palavras; e de todos esses grupos interessa considerar apenas uma fração, justamente aqueles grupos que resultam em definições significativas de números naturais. Portanto, o complementar de  $M'$  de  $M$  é um subconjunto infinito do conjunto dos números naturais; e, como tal possui um menor elemento. Seja  $m$  esse menor elemento de  $M'$ . O que é  $m$ ? Resposta: “ $m$  é o menor número natural que não pode ser descrito com menos de 20 palavras da língua portuguesa”. Ora, acabamos de descrever  $m$  com apenas 18 palavras!

Como se vê estamos diante de um paradoxo (paradoxo de Richard), resultante da construção de um conjunto com axiomas da especificação. como podemos evitar mais esse paradoxo da teoria?

### **As imprecisões da linguagem**

O paradoxo anterior nos põe diante de um problema sério, que é a linguagem que usamos para nos comunicar. Ora, a linguagem, por mais correta que seja, contém muitas imprecisões e ambiguidades. Vejamos alguns exemplos:

*As testemunhas forneceu informações aos membros da CPI que poderão ajudar na descoberta do esquema de corrupção.* O que ou quem vai ajudar, as informações ou os membros da CPI?

*O importante na matemática são as ideias, não a notação e o formalismo, como pensam muitos professores.* O que pensam os professores, que o importante são as ideias ou a notação e o formalismo?

*A diretora pediu que o professor comunicasse aos alunos sua alegria pelo progresso que eles vinham fazendo nos estudos.* Alegria da diretora ou do professor?

*A oposição acha que o governo está dividido e quer impedir a votação da matéria.* Quem quer impedir, a oposição ou o governo?

Todas essas frases são perfeitamente normais na linguagem correta; nada de errado com elas, embora não resistam as demandas do rigor lógico. E não é por isso que vão deixar de ser usadas. Pelo contrário, às vezes até certas omissões no uso da linguagem são necessárias para valorizar um trecho escrito ou falado. Isto é frequente em obras literárias, prosa ou poesia. E mesmo quando se conta uma anedota, é comum usar de meias palavras ou omitir algumas coisa, para deixar a esperteza do ouvinte uma parte na interpretação do resultado final.

Kurt Godel, um dos maiores lógicos do século XX, disse certa vez: “quanto mais reflito sobre a linguagem, tanto mais me admiro que as pessoas consigam se entender umas com as outras”.

### **A linguagem formal**

A conclusão é simples: a linguagem corrente não atende às exigências do rigor lógico. Alguma coisa tinha de ser feita para evitar paradoxo como o último que mencionamos atrás. Isso aconteceu em 1922, quando dois matemáticos, Adolf Fraenkel e Albert Skolem propuseram que a linguagem corrente fosse completamente banida da Matemática e substituída por uma linguagem formal, construída com poucos símbolos e as regras de sintaxe necessárias para se conduzir ao raciocínio dedutivo. Os símbolos incluem os conhecidos símbolos matemáticos, como os sinais de adição, subtração, igualdade, etc. além de outros, como “ $\implies$ ”(significa “implica”), “ $\exists$ ”(significa “existe”), “ $\forall$ ”(significa “para todo”), “ $\in$ ”(significa “pertence”), os sinais de parênteses, símbolos para as variáveis, etc. Por exemplo, lidando como o conjunto dos números naturais  $\mathbb{N}$ , quando escrevemos

$$n \in \mathbb{N} \implies \exists a, b, c, d \in \mathbb{N}, n = a^2 + b^2 + c^2 + d^2,$$

estamos expressando, em linguagem formal, o seguinte teorema de Euler: “todo número natural é a soma de quatro quadrados”. A mesma proposição pode ser ainda escrita assim:

$$\forall n \in \mathbb{N}, \exists a, b, c, d, \in \mathbb{N}, n = a^2 + b^2 + c^2 + d^2$$

. A propriedade que utilizamos acima para definir um conjunto, qual seja, “conjunto de todos os números naturais que podem ser descritos com menos de 20 palavras na língua portuguesa” não é passível de ser escrito em linguagem formal, portanto, está excluído de considerações matemáticas. E desde a proposta de Fraenkel e Skolem em 1922 ninguém conseguiu ainda formular uma propriedade em linguagem formal que conduzisse a algum paradoxo.

### **Linguagem formal e linguagem corrente**

Dissemos acima que a linguagem corrente ficaria banida do universo matemático, sendo permitida apenas a linguagem formal. Isso apenas em tese. A importância da linguagem formal é a de ser um instrumento para estudar a consistência das teorias matemáticas, não para ser usado no dia a dia do matemático. Nem os lógicos que estudam os fundamentos da Matemática insistem no desatino de fazer tudo em linguagem formal; nem isso é possível! No mais das vezes é difícil, ou mesmo uma tarefa hercúlea, traduzir um teorema em linguagem formal. E não perturbe também seus alunos como exemplos esdrúxulos de conjuntos, que só podem causar dificuldades ao próprio professor. Não queira, pois, falar do conjunto dos fios da barba do imperador, pois não há como saber, ao certo, onde termina a barba e onde começam os fios

do pescoço... ou os cabelos da cabeça! E esse conjunto seria aquele de quando o imperador tinha 23 anos de idade? ou 47? No dia do aniversário? ou três meses depois ? Afinal, por que perturbar seus alunos com essas coisas que não tem nada haver com a matemática?... Também não queira falar no conjunto dos dígitos que aparecem infinitas vezes na expansão decimal de  $\sqrt{2}$ ; você não tem nem como saber se 3 está ou não nesse conjunto, como pode então saber se isso é mesmo um conjunto?

### **Ainda a linguagem e o simbolismo**

A Matemática depende muito de sua linguagem e simbolismo específicos. Mas é também a linguagem e o simbolismo próprio da Matemática que a torna tão inacessível, principalmente ao leigo, mesmo o leigo “ culto ”. Assim, podemos dizer, em certo sentido, que a linguagem e o simbolismo da Matemática são “ mal necessário ”. E por causa mesmo dessas dificuldades inerentes a linguagem e ao simbolismo é que se torna tão necessário o devido cuidado na boa utilização desses instrumentos para que eles exerçam o desejado papel no aprendizado e não o prejudiquem.

É preciso que o professor tenha sempre presente que o objetivo de todo ensino, seja de matemática ou de qualquer outra disciplina, é transmitir ideias, estimular o pensamento independente e a criatividade. Linguagem e simbolismo são muito úteis e indispensáveis enquanto ajudam na transmissão e agilização das ideias. Infelizmente, o que muito acontece no ensino é que a linguagem de conjuntos e o excesso de simbolismo e terminologia, além de não ajudarem, só atrapalhem. Por exemplo, não há benefícios algum em insistir com as crianças sobre a diferença entre número e numeral; isto só traz prejuízos, pois cria uma preocupação desnecessária na mente do aluno. Do mesmo modo, para introduzir a ideia de função não é preciso apelar para produto cartesiano de conjuntos, muito menos para a noção de relação, como ainda costuma ser feito no ensino médio, e nada tem de motivador. Em situações como essas, o excesso de linguagem obstrui o mais importante, que são as ideias. Por exemplo, é muito mais natural e fácil dizer “ 2 e 5 são as raízes da equação  $x^2 - 7x + 10 = 0$ ” do que “ o conjunto verdade da sentença  $x^2 - 7x + 10 = 0$  é  $V(2, 5)$ ”. Por que introduzir as noções de “sentença aberta” se tudo pode ser feito sem isso? Nenhum matemático profissional utiliza essa linguagem! E o natural é seguir o costume dos matemáticos profissionais, e não ficar inventando pedantices artificiais que só fazem obstruir o caminho do aprendizado.

É importante observar que linguagem não motiva ninguém, ideias sim. Nenhum aluno pode se interessar por qualquer coisa onde não vê elemento que lhe satisfaça ou aguace a curiosidade. O mesmo é verdade no caso dos matemáticos que contribuíram para o desenvolvimento de sua ciência. Eles estavam sempre interessados nas ideias e nos métodos e técnicas delas resultante. Foram introduzindo linguagem e simbolismo por necessidade prática. O mesmo devemos fazer no ensino: só introduzir esses elementos quando eles se fizerem necessários para auxiliar no aprendizado de coisas verdadeiramente relevantes.

# Capítulo 3

## Conjuntos enumeráveis

Neste capítulo trabalharemos uma construção mais formal sobre enumerabilidade e uma outra menos formal, por entendermos que ambas são importantes para o entendimento do conceito de enumerabilidade, exemplificando e mostrando como certos conjuntos podem ser considerados enumeráveis. Para maior entendimento, ou extensão deste trabalho indicamos as referências [2], [3], [8], [9], [11] e [12]

### 3.1 Uma forma de construir enumerabilidade

Um conjunto *enumerável*, ou *contável*, é um conjunto cujos elementos podem ser enumerados: disposto em uma única lista, tendo um primeiro item, um segundo item, e assim por diante, de modo que todos os elementos do conjunto apareça mais cedo ou mais tarde na lista.

Exemplo: Como já foi dito os números naturais  $\mathbb{N}$  é enumerado pela lista

$$1, 2, 3, \dots$$

ao passo que o conjunto  $P^-$  dos inteiros negativos é enumerado pela lista

$$-1, -2, -3, -4, \dots$$

Note que os itens dessas listas não são números (classes de equivalência), mas numerais, ou nomes de números. Em geral, ao listar os elementos de um conjunto você manipula nomes, não as coisas nomeadas. Por exemplo, ao nomear os membros do Senado do Brasil, você não obriga os senadores a formarem uma fila; ao contrário você organiza seus nomes em uma lista, talvez alfabeticamente. ( pode-se argumentar que uma exceção ocorre no caso em que os elementos do conjunto sendo enumerado são, eles próprios, expressões linguísticas. Nesse caso, podemos plausivelmente falar em dispor os próprios elementos em uma lista. mas também poderíamos

falar dos itens como *nomes de si mesmos*, para podermos continuar insistindo que, ao enumerar um conjunto, são os nomes dos elementos do conjunto que são arranjados em uma lista.)

Por cortesia, consideremos enumerável o conjunto vazio,  $\emptyset$ , que não tem elementos. (o conjunto vazio; há somente um. A terminologia é um pouco enganosa: ela sugere a comparação de conjunto vazio com recipiente vazio. É mais conveniente, porém, comparar a conteúdos, e deve-se-ia considerar que todos os recipientes vazios têm os mesmo conteúdo nulo.)

Uma lista que enumera um conjunto pode ser finita ou interminável. Um conjunto infinito que é enumerável é chamado *enumeravelmente infinito* ou *denumerável*. Sejam claros a respeito de que elementos contam como listas infinitas, e que outros elementos não são contáveis. Os números naturais podem ser dispostos em uma única lista infinita, como indicado anteriormente, mas o arranjo a seguir não é aceitável como uma lista dos números naturais.

$$1, 3, 5, 7, \dots, 2, 4, 6, \dots$$

Aqui são listados todos os naturais ímpares e depois todos os pares. Isso não serve. Em uma lista aceitável, cada item deve aparecer cedo ou tarde como o  $n$ -ésimo elemento, para algum  $n$  finito. No arranjo inaceitável acima, contudo, nenhum dos naturais pares é representado dessa maneira. Em vez disso, eles aparecem (por assim dizer) como itens número  $\infty + 1, \infty + 2$  etc.

Para que esse ponto fique perfeitamente claro, poderíamos definir uma enumeração de um conjunto não como uma lista, mas como um arranjo no qual cada elemento do conjunto é *associado* a um número natural  $1, 2, 3, \dots$ . Na verdade, uma lista é um tal arranjo. A coisa nomeada pelo primeiro item da lista é associada ao natural 1, a coisa nomeada pelo segundo item da lista é associada ao natural 2, e, em geral, a coisa associada pelo  $n$ -ésimo item da lista é associada ao natural  $n$ . Isso motiva a seguinte definição de conjuntos enumeráveis.

**Definição 3.1.** *Um conjunto  $X$  diz-se enumerável quando é finito ou quando existe uma bijeção  $f : \mathbb{N} \rightarrow X$ . No segundo caso,  $X$  diz-se infinito enumerável e, pondo-se  $x_1 = f(1), x_2 = f(2), \dots, x_n = f(n), \dots$ , tem-se  $X = \{x_1, x_2, x_3, \dots, x_n, \dots\}$ . Cada bijeção  $f : \mathbb{N} \rightarrow X$  chama-se uma enumeração dos elementos de  $X$ .*

Essa definição pode ser entendida como a que estabelece equivalência entre o conjunto dos números naturais e o conjunto  $X$ . Eles tem a mesma cardinalidade, ou seja, o mesmo número de elementos. Este fenômeno é uma peculiaridade dos conjuntos infinitos e em nada contradiz o que já sabemos sobre conjuntos finitos.

No jargão matemático, uma lista infinita  $X$  determina uma *função*  $f : \mathbb{N} \rightarrow X$ , o valor da função  $f$  para o argumento  $n$  é denotado por  $f(n)$ . Esse valor é simplesmente os objetos denotada pelo  $n$ -ésimo item da lista. No nosso caso, os objetos são números, Assim, a lista

$$2, 4, 6, 8, \dots,$$

que enumera o conjunto  $E$  dos naturais pares, determina a função  $f$  para a qual temos

$$f(1) = 2, f(2) = 4, f(3) = 6, f(4) = 8, \dots$$

Inversamente, a função  $f$  determina a lista, exceto pela notação. (A mesma lista teria a seguinte aparência, em números romanos: II, IV, VI, VIII, ..., por exemplo). Assim, poderíamos ter definido a função  $f$  primeiro, dizendo que, para qualquer número natural  $n$ , o valor de  $f$  é  $f(n) = 2n$ ; e poderíamos então ter descrito a lista dizendo que, para cada natural  $n$ , seu  $n$ -ésimo item é a representação decimal do número  $f(n)$ , ou seja, do número  $2n$ .

Podemos então falar de conjuntos como sendo enumerados tanto por função quanto por listas. Em vez de enumerar os números naturais ímpares pela lista  $1, 3, 5, 7, \dots$ , podemos enumerá-los pela função que associa a cada número natural  $n$  o valor  $2n - 1$ . Em vez de enumerar o conjunto  $\mathbb{N}$  de todos os números naturais pela lista  $1, 2, 3, \dots$ , podemos enumerar  $\mathbb{N}$  pela função que associa a cada número natural  $n$  o próprio valor  $n$ . Já vimos a *função identidade*. Se a dominarmos por  $id$ , temos que  $id(n) = n$  para cada inteiro positivo  $n$ .

Se uma função enumera um conjunto não vazio, alguma outra também o faz; de fato, também o fazem infinitamente muitas outras. Assim, o conjunto dos números naturais é enumerado não somente pela função identidade, mas também pela função (vamos chama-la  $g$ ) determinada pela seguinte lista:

$$2, 1, 4, 3, 6, 5, \dots$$

Essa lista é obtida da lista  $1, 2, 3, 4, 5, 6, \dots$  permutando os itens em pares: 1 com 2, 3 com 4, 5 com 6, e assim por diante. Essa lista é uma enumeração estranha, mas perfeitamente aceitável, do conjunto dos números naturais: cada número natural aparece nela, cedo ou tarde. A função correspondente,  $g$ , pode ser definida como:

$$g(n) = \begin{cases} n + 1 & \text{se } n \text{ é ímpar} \\ n - 1 & \text{se } n \text{ é par} \end{cases}$$

Essa definição não é tão elegante como as definições  $f(n) = 2n$  e  $id(n) = n$  das funções  $f$  e  $id$ , mas faz o mesmo: ela associa um e somente um elemento de  $\mathbb{N}$  a cada número natural  $n$ . E a função  $g$  assim definida de fato enumera  $\mathbb{N}$ : para cada elemento  $m$  de  $\mathbb{N}$ , a um número natural  $n$  para o qual temos  $g(n) = m$ .

Ao enumerar um conjunto listando seus elementos, é perfeitamente legítimo que um elemento do conjunto apareça mais de uma vez na lista. A exigência é, mais precisamente, que cada elemento apareça *pelo menos uma vez*. não importa que a lista seja redundante: tudo que exigimos é que seja completa. De fato, uma lista redundante pode sempre ser reduzida para que se obtenha uma lista não redundante, uma vez que poderíamos percorrê-la e apagar os itens que

repetem itens anteriores. É também perfeitamente legítimo que uma lista contenha lacunas, uma vez que poderíamos percorrê-la e preencher as lacunas. A exigência é que todo elemento do conjunto enumerado seja associado a um número natural, e não que todo número natural tenha um elemento do conjunto associado a ele. Assim, enumeração repetidas dos números naturais são dadas pela seguinte lista:

$$1, 1, 2, 2, 3, 3, 4, 4, \dots$$

e pela seguinte lista cheia de lacunas:

$$1, -, 2, -, 3, -, 4, -, \dots$$

A função correspondente a essa última lista (vamos chama-la de  $h$ ) atribui valores correspondentes à primeira, terceira, quinta,... posição da lista, mas não atribui valor algum correspondente às lacunas (segunda, quarta, sexta,...posições). Assim, temos  $h(1) = 1$ , mas  $h(2)$  não é absolutamente nada, pois a função  $h$  é *indefinida* para o argumento 2;  $h(3) = 2$ , mas  $h(4)$  é indefinida;  $h(5) = 3$ , mas  $h(6)$  é indefinida. E assim por diante:  $h$  é uma função parcial de números naturais; ou seja, é definida somente para argumentos que sejam números naturais, mas não para todos esses argumentos. Explicitamente, poderíamos definir a função parcial  $h$  como segue:

$$h(n) = \frac{(n+1)}{2} \text{ se } n \text{ é ímpar}$$

Ou, para deixar claro que não esquecemos de dizer que valores  $h$  associa a números naturais pares, Poderíamos formular a definição como segue:

$$h(n) = \begin{cases} \frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \\ \text{indefinida} & \text{caso contrário} \end{cases}$$

Ora, a função parcial  $h$  é uma enumeração estranha, mas perfeitamente aceitável do conjunto  $\mathbb{N}$  dos números naturais.

Seria perverso escolher escolher  $h$  em vez simplesmente sa função *id* como enumeração dos números naturais; mas outros conjuntos são enumerados de modo mais natural por funções parciais. Assim, o conjunto  $E$  dos números naturais pares é convenientemente enumerar pela função parcial (vamos chama-la de  $j$ ) que concorda com *id* para argumentos pares, e é indefinida para argumentos ímpares:

$$j(n) = \begin{cases} n & \text{se } n \text{ é par} \\ \text{indefinida} & \text{caso contrário.} \end{cases}$$



A lista correspondente, com lacunas, é (em notação decimal):

$$-, 2, -, 4, -, 6, -, 8, \dots$$

É claro, a função  $f$  considera anteriormente, definida por  $f(n) = 2n$  para todos os números naturais  $n$ , era enumeração igualmente aceitável de  $E$ , correspondendo à lista sem lacunas 2, 4, 6, 8 e assim por diante.

Esse raciocínio é análogo ao feito no capítulo dois no Grande Hotel de Georg Cantor, onde as lacunas são os quartos ímpares o qual os novos hospedes poderão ser hospedados.

Qualquer conjunto  $S$  de números naturais é enumerado de maneira bastante simples pela função parcial  $s$  definida como segue:

$$h(n) = \begin{cases} n & \text{se } n \text{ está no conjunto } S \\ \text{indefinida} & \text{caso contrário.} \end{cases}$$

Um conjunto é não-enumerável, quando não existe uma bijeção entre os naturais e esse conjunto. Embora o conjunto dos números naturais seja enumerável, há conjuntos de outros tipos que não são enumeráveis. Dizer que um conjunto  $A$  é enumerável é dizer que há uma função cujos argumentos todos são números naturais e cujos valores todos são elementos de  $A$ , e que cada elemento de  $A$  é um valor dessa função: para cada elemento de  $a$  de  $A$  há ao menos um número natural  $n$  ao qual a função associa  $a$  como seu valor.

Note que nada nessa definição exige que  $A$  seja um subconjunto de números naturais ou de números de qualquer espécie. Em vez disso,  $A$  poderia ser um conjunto de pessoas; ou um conjunto de expressões linguísticas; ou um conjunto de conjuntos, como quando  $A$  é o conjunto  $\{\mathbb{N}, E, \emptyset\}$ . Aqui,  $A$  é um conjunto com três elementos, sendo que cada um é um conjunto. Um elemento de  $A$  é um conjunto infinito  $\mathbb{N}$ ; um outro elemento de  $A$  é o conjunto infinito  $E$  de todos os números naturais pares; e o terceiro é o conjunto vazio  $\emptyset$ . O conjunto  $A$  é certamente enumerável; por exemplo, pela seguinte lista finita:  $\mathbb{N}, E, \emptyset$ . Cada item desta lista nomeia um elemento de  $A$ , e todo elemento de  $A$  é cedo ou mais tarde nomeado nesta lista. Essa lista determina uma função (vamos chama-la de  $f$ ), que pode ser definida pelos três enunciados:  $f(1) = \mathbb{N}, f(2) = E, f(3) = \emptyset$ . Para sermos precisos,  $f$  é uma *função parcial ou definida por mais de uma sentença* de números naturais, sendo indefinida para argumentos maiores deo que 3.

Podemos usar também a seguinte terminologia. Uma *função*  $f$  é uma regra de *valores a argumentos*. O conjunto de todos aqueles argumentos aos quais a função associa valores é de-

nominado o *domínio* da função. O conjunto de todos aqueles valores que a função associa a seus argumentos é chamado a *imagem* da função. No caso de funções cujos argumentos são números naturais, distinguiremos entre funções *totais* e *função parcial ou definida por mais de uma sentença*. Uma função total de números naturais é uma cujo domínio é o conjunto  $\mathbb{N}$ . Uma função parcial de números naturais é uma cujo domínio é algo menos do que todo o conjunto  $\mathbb{N}$ . Geralmente na quando se fala em função, associa-se a funções totais, mas na verdade podemos estar tratando de funções totais ou parciais.

## 3.2 Exemplos de conjuntos enumeráveis

Vejamos alguns exemplos de conjuntos enumeráveis

### 3.2.1 Enumerabilidade de $\mathbb{N}$ , $\mathbb{Z}$ e seus subconjuntos

**Exemplo 3.1.** O conjunto dos números naturais  $\mathbb{N}$  é enumerável, pois a função identidade  $id_{\mathbb{N}}$ , definida por  $id_{\mathbb{N}}(n) = n$  é uma função bijetiva.

**Exemplo 3.2.** O conjunto dos números pares positivos  $2\mathbb{N}$  é enumerável, pois

$$f : \mathbb{N} \rightarrow 2\mathbb{N}, \quad f(n) = 2n$$

é uma função bijetiva.

**Exemplo 3.3.** O conjunto dos inteiros é enumerável.

$$\begin{array}{cccccccc} \dots-3, & -2, & -1, & 0, & 1, & 2, & 3, & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \dots 7, & 5, & 3, & 1, & 2, & 4, & 6, & \dots \end{array}$$

A lista mais simples é  $0, 1, -1, 2, -2, 3, -3, \dots$ . Então, se a função correspondente é denominada  $f$ , temos  $f(1) = 0, f(2) = 1, f(3) = -1, f(4) = 2, f(5) = -2$ , e assim por diante.

Podemos determinar função  $f : \mathbb{N} \rightarrow \mathbb{Z}$ .

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ \frac{1-n}{2} & \text{se } n \text{ é ímpar.} \end{cases}$$

a função  $f$  é bijetiva.

### 3.2.2 Enumerabilidade das $n$ -uplas e do conjunto $\mathbb{Q}$ pela tabela de Cantor

Precisaremos do seguinte teorema.

**Teorema 3.2.1.** *Dados os conjuntos  $A_1, A_2, A_3, \dots$ , todos eles enumeráveis, então, sua união  $A = A_1 \cup A_2 \cup A_3 \cup \dots$  também é enumerável.*

**Demonstração** Como os conjuntos  $A_1, A_2, A_3, \dots$  são enumeráveis, vamos escrevê-lo na forma

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \dots, a_{1n}, \dots\} \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \dots, a_{2n}, \dots\} \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \dots, a_{3n}, \dots\} \\ &\vdots \\ A_n &= \{a_{n1}, a_{n2}, a_{n3}, \dots, a_{nn}, \dots\} \\ &\vdots \end{aligned}$$

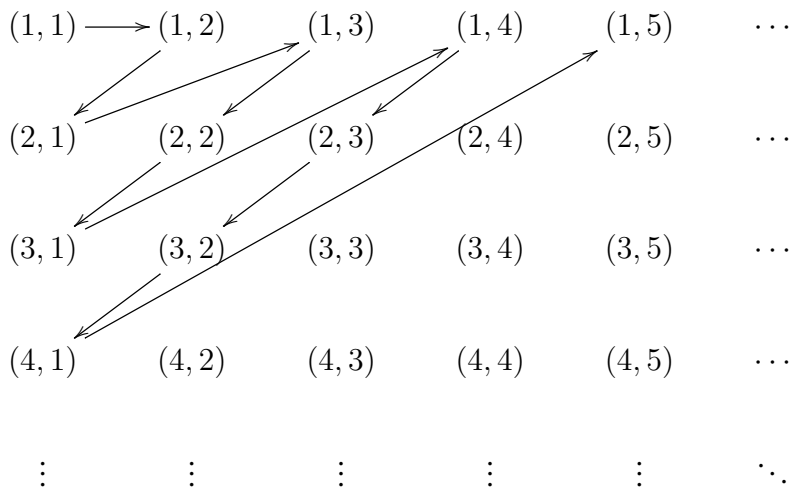
Repare agora que podemos escrever os elementos da união  $A$  da seguinte maneira: começamos com  $a_{11}$ , depois  $a_{12}$  e  $a_{21}$ , depois  $a_{13}$ ,  $a_{22}$  e  $a_{31}$ , etc. Isto equivale a tomar os elementos do conjunto  $A_i$  segundo as diagonais secundárias do quadro acima. Dito de outra maneira,  $A$  é a união dos conjuntos

$$\{a_{11}\}, \{a_{12}, a_{21}\}, \{a_{13}, a_{22}, a_{31}\}, \{a_{14}, a_{23}, a_{32}, a_{41}\}$$

Como todos esses conjuntos são finitos, podemos enumerar o conjunto  $A$ .

**Exemplo 3.4.** O conjunto dos pares ordenados de inteiros positivos é enumerável.

**Demonstração** Antes de fazer a enumeração, vamos organizar os pares em uma tabela retangular. Vamos então percorrer a tabela no estilo *em zigue-zague de Cantor*,



Isso nos dá a lista:

$$(1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1), (1, 4), (2, 3), (3, 2), (4, 1), \dots$$

Se chamarmos a função aqui envolvida de  $G$ , temos  $G(1) = (1, 1), G(2) = (1, 2), G(3) = (2, 1)$ , e assim por diante. O padrão é: primeiro vem o par cuja soma dos elementos é 2, então vêm os pares cuja soma dos elementos é 3, então vêm os pares cuja soma dos elementos é 4, e assim por diante. Podemos formar os seguintes grupos  $\{(1, 1)\}, \{(1, 2), (2, 1)\}, \{(1, 3), (2, 2), (3, 1)\}, \dots$

Logo pelo teorema 3.2.1 a união desses pares ordenados é enumerável.

Vejamos uma função que enumere esses pares ordenados. Dada uma função  $f$  que enumera os pares de inteiros positivos, tal como  $G$ , dado um  $n \in \mathbb{N}$  tal que  $f(n) = (a, b)$ , onde  $n$  representa a  $n$ -ésima posição deste par ordenado. Por exemplo  $f(4) = (1, 3)$ , ou seja, o par ordenado  $(1, 3)$  está na quarta posição.

É de fato possível obter fórmulas matemáticas para tal função (possível, mas não necessário: o que dissemos até agora é mais do que suficiente como uma prova de que o conjunto de pares ordenados de inteiros positivos é enumerável.)

Começemos verificando o *zigue-zague* na tabela, antes de chegar ao par  $(a, b)$ , teremos que passar pelo par cujos elementos somam 2, os dois pares cujo elemento somam 3, os três pares cujo os elementos somam 4, e assim por diante, até inclusive os  $a + b - 2$  pares cujos elementos somam  $a + b - 1$ , ou seja.

O par cujo a soma é 2

$$a + b = 3, \text{ temos } a + b - 2 = 1, \text{ um par em que a soma é dois}$$

O par cujo a soma é 3

$$a + b = 4, \text{ temos } a + b - 2 = 2, \text{ dois pares em que a soma é 3}$$

e assim por diante.

Então o par  $(a, b)$  aparecerá no  $n$ -ésimo lugar depois de todos esses pares. Assim, a posição do par  $(a, b)$  será dada por

$$[1 + 2 + \dots + (a + b - 2)] + a.$$

Por exemplo, a posição do par  $(1, 3)$  soma-se

os pares ordenados que a soma é dois = 1

os pares ordenados que a soma é três = 2

mais  $a = 1$ , logo o par ordenado  $(1, 3)$  está na posição 4. Onde podemos verificar sem dificuldade na tabela.

Neste ponto, recordemos a fórmula para a soma dos  $k$  inteiros positivos demonstrada por indução no capítulo 2, no exemplo 2.6:

$$1 + 2 + \dots + k = \frac{k(k + 1)}{2}.$$

Assim, a posição do par  $(a, b)$  será dada por

$$\frac{(a + b - 2)(a + b - 1)}{2} + a.$$

Isso pode ser simplificado para

$$\text{Posição de } (a, b) = \frac{a^2 + 2ab + b^2 - a - 3b + 2}{2}.$$

Por exemplo, o par  $(3, 2)$  deve estar na posição

$$\frac{3^2 + 2 \cdot 3 \cdot 2 + 2^2 - 3 - 3 \cdot 2 + 2}{2} = \frac{9 + 12 + 4 - 3 - 6 + 2}{2} = \frac{18}{2} = 9,$$

e pode-se de fato ver (relembrando a enumeração exibida acima) que está  $G(9) = (3, 2)$ .

**Exemplo 3.5.** O conjunto dos números racionais positivos é enumerável.

**Demonstração** Um número racional positivo é um número que pode ser expresso como uma razão de inteiros positivos, isto é, na forma  $\frac{m}{n}$ , em que  $m$  e  $n$  são inteiros positivos e  $n \neq 0$ . Portanto, podemos obter uma enumeração de todos os números racionais positivos começando com nossa enumeração de todos os pares de inteiros positivos e substituindo o par  $(m, n)$  pelo número racional dá lista

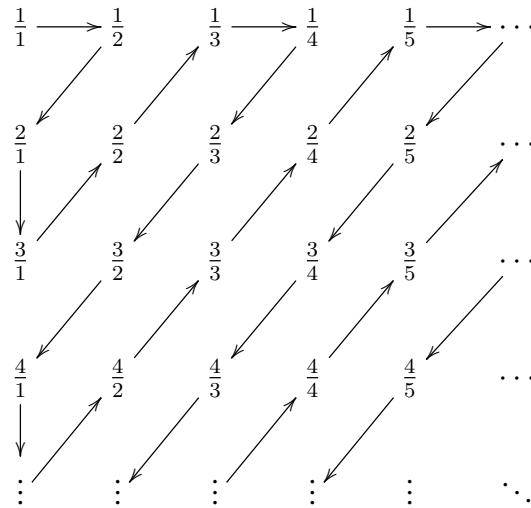
$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4}, \frac{1}{5}, \dots$$

ou, simplificada,mente,

$$1, \frac{1}{2}, 2, \frac{3}{1}, 1, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, 4, 5, 2, 1, \frac{1}{2}, \frac{1}{5}, \dots$$

todo número racional aparece de fato infinitamente muitas vezes, já que, por exemplo,  $\frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \dots$  e  $\frac{1}{2} = \frac{2}{4} = \dots$  e  $\frac{2}{1} = \frac{4}{2} = \dots$  e analogamente para todos os outros números racionais. Mas não há problema nisso: nossa definição de enumerabilidade permite repetições.

Podemos ver também essa enumeração através da tabela de Cantor, adaptando para os racionais positivos.



Portanto de forma análoga ao exemplo 3.4, podemos formar grupos de frações

$$\left\{ \frac{1}{1} \right\}, \left\{ \frac{1}{2}, \frac{2}{1} \right\}, \left\{ \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1} \right\}, \dots$$

formamos grupos de frações que a soma do numerador com o denominador é dois, três, quatro, ... e pelo teorema 3.2.1, conclui-se que o conjunto dos números racionais positivos é enumerável.

**Exemplo 3.6.** O conjunto dos números racionais é enumerável.

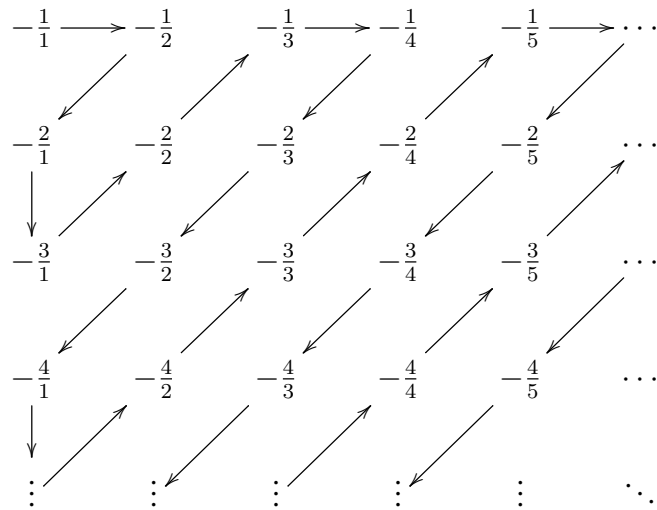
**Demonstração** Combinamos as ideias dos exemplos 3.3 e do exemplo 3.5, sabemos que no exemplo 3.5, como dispor os racionais positivos em uma lista única, infinita. Escrevendo um zero na frente desta lista e depois escrevendo todos os racionais positivos de modo inverso e com sinal de menor na frente dele, temos agora:

$$\dots, -\frac{1}{3}, -2, -\frac{1}{2}, -1, 0, 1, \frac{1}{2}, 2, \frac{1}{3}$$

Finalmente usando o método do exemplo 3.3 para transformar isso em uma lista apropriada:

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, \frac{1}{3}, -\frac{1}{3}, \dots$$

Podemos chegar a essa mesma conclusão que o conjunto dos números racionais é enumerável, partindo por outro raciocínio, tome a tabela dos números simétricos aos racionais positivos (os racionais negativos).



Desta maneira conseguimos também uma enumeração para os racionais negativos.

Temos pelo teorema 3.2.1 que  $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$  é também enumerável.

**Exemplo 3.7.** O conjunto das triplas ordenadas de inteiros positivos é enumerável.

**Demonstração** No exemplo 3.4 apresentamos duas maneiras de enumerar todos os pares de inteiros positivos. Por clareza, vamos trabalhar aqui com a primeira delas:

$$(1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1) \dots$$

Percorreremos agora esta lista, e em cada par substituímos o segundo elemento ou componente  $n$  pelo par que aparece no  $n$ -ésimo termo lugar nessa própria lista. Em outras palavras, substituímos cada 1 que aparece no segundo lugar de um par por  $(1, 1)$ , cada 2 por  $(1, 2)$ , e assim por

diante. Isso nos dá a lista

$$(1, (1, 1)), (1, (1, 2)), (2, (1, 1)), (1, (2, 1)), (2, (1, 2)), (3, (1, 1))\dots$$

a qual nos dá a lista de triplas

$$(1, 1, 1), (1, 1, 2), (2, 1, 1), (1, 2, 1), (2, 1, 2), (3, 1, 1)\dots$$

Em termos de função, essa enumeração pode ser descrita como segue. A enumeração original de pares corresponde a uma função associando a cada inteiro positivo  $n$  um par  $G(n) = (K(n), L(n))$  de inteiros positivos. A enumeração de triplas que acabamos de definir corresponde a associar, em vez disso, a cada inteiro positivo  $n$  a tripla

$$(K(n), K(L(n)), L(L(n)))$$

Não deixamos escapar nenhuma tripla  $(p, q, r)$  dessa maneira, porque sempre haverá um  $m = J(q, r)$  tal que  $(K(m), L(m)) = (q, r)$ , e então haverá um  $n = J(p, m)$  tal que  $(K(n), L(n)) = (p, m)$ , e a tripla associada a esse  $n$  será precisamente  $(p, q, r)$ .

**Exemplo 3.8.** O conjunto da  $k$ -uplas ordenadas positivas, para qualquer  $k$  fixo.

**Demonstração** O método pelo qual acabamos de obter uma enumeração de triplas a partir de uma enumeração de pares nos dá uma enumeração de quadruplas a partir de uma enumeração de triplas. Retorne a enumeração original de pares, e substitua cada segundo elemento  $n$  do par pela tripla que aparece no  $n$ -ésimo lugar na enumeração de triplas, de modo a obter uma quadrupla. As primeiras quadruplas nessa lista serão

$$(1, 1, 1, 1), (1, 1, 1, 2), (2, 1, 1, 1), (1, 2, 1, 1), (2, 1, 1, 2), \dots$$

Obviamente, podemos continuar daqui com quádruplas, sêxtuplas, ou  $k$ -uplas para qualquer  $k$  fixado.

Os exemplos 3.8 é equivalente a dizer que o produto cartesiano  $\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}$  é enumerável.

### 3.2.3 Enumerabilidade do produto cartesiano de qualquer conjunto enumerável

Para mostrarmos que o produto cartesiano de qualquer conjunto enumerável é enumerável precisaremos de alguns teoremas da análise matemática.

**Teorema 3.2.2.** *Todo subconjunto  $X \subset \mathbb{N}$  é enumerável.*



**Demonstração** Devemos mostrar que a  $f : \mathbb{N} \rightarrow X$  é injetiva e sobrejetiva. Se  $X$  for finito, é enumerável. Se for infinito, definiremos indutivamente uma bijeção  $f : \mathbb{N} \rightarrow X$ . Poremos:

$$f(1) = x_1$$

$$f(2) = x_2$$

$$\vdots$$

$$f(n) = x_n$$

Tomamos  $f(1) = x_1$  como menor elemento de  $X$ . Suponhamos  $f(1), \dots, f(n)$  definidos de modo a satisfazerem as seguintes condições:

a)  $f(1) < f(2) < \dots < f(n)$

b) Pondo  $B_n = X - \{f(1), \dots, f(n)\}$ .

Tem-se que  $f(n) < x$  para todo  $x \in B_n$ . Como  $B_n \neq \emptyset$  (pois  $X$  é infinito) definiremos  $f(n+1) =$  menor elemento de  $B_n$ . Temos  $f(n+1) > f(n)$ , ou seja, a função é estritamente crescente, logo temos que a função  $f : \mathbb{N} \rightarrow X$  é injetiva.

Na condição “b”, suponhamos que se existisse algum  $x \in X - F(\mathbb{N})$ , teríamos  $x \in B_n$  para todo  $n$  e, portanto  $x > f(n)$  qualquer que fosse  $n \in \mathbb{N}$ . Então o conjunto infinito  $F(\mathbb{N}) \subset \mathbb{N}$  seria limitado, uma contradição.

**Corolário 3.2.1.** *Seja  $f : X \rightarrow Y$  injetiva. Se  $Y$  é enumerável então  $X$  também é. Em particular, todo subconjunto de um conjunto enumerável é enumerável.*

**Demonstração** Temos que  $Y$  é enumerável, então existem as bijeções  $g : \mathbb{N} \rightarrow Y$  e  $h : Y \rightarrow \mathbb{N}$ . Dizer que  $h : Y \rightarrow \mathbb{N}$  é uma bijeção, é o mesmo que dizer que a cardinalidade de  $Y$  é igual a cardinalidade de  $\mathbb{N}$ . E como a função  $f : X \rightarrow Y$  é injetiva (cada elementos de  $Y$  tem apenas uma única correspondência com os elementos de  $X$ ), então podemos afirmar que a função  $h \circ f : X \rightarrow \mathbb{N}$  é uma bijeção de  $X$  sobre um subconjunto de  $\mathbb{N}$ , o qual é enumerável pelo teorema 3.2.2. No caso particular de  $X \subset Y$ , tomamos  $f : X \rightarrow Y$  igual a aplicação de inclusão.

**Corolário 3.2.2.** *Seja  $f : X \rightarrow Y$  sobrejetiva. Se  $X$  é enumerável então  $Y$  também é.*

**Demonstração** Para cada  $y \in Y$  podemos escolher um  $x = g(y) \in X$  tal que  $f(x) = y$ . Isto define uma aplicação  $g : Y \rightarrow X$  tal que  $f(g(y)) = y$  para todo  $y \in Y$ . Segue daí que  $g$  é injetiva. Pelo Corolário 3.2.1,  $Y$  é enumerável.

**Corolário 3.2.3.** *Sejam  $X, Y$  conjuntos enumeráveis. O produto cartesiano  $X \times Y$  é enumerável.*

**Demonstração** Como  $X$  e  $Y$  são enumeráveis então existem sobrejeções  $f : \mathbb{N} \rightarrow X$  e  $g : \mathbb{N} \rightarrow Y$ , logo  $\varphi : \mathbb{N} \times \mathbb{N} \rightarrow X \times Y$ , dada por  $\varphi(m, n) = (f(m), g(n))$  é sobrejetiva.

Então, pelo corolário 3.2.2, se provarmos que  $\mathbb{N} \times \mathbb{N}$  é enumerável, o produto cartesiano  $X \times Y$  também é enumerável. Para isto, consideremos a aplicação  $\psi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , dada por  $\psi(m, n) = 2^m \cdot 3^n$ . Pela unicidade da decomposição de um número em fatores primos,  $\psi$  é injetiva. Portanto pelo corolário 3.2.1 Segue que  $\mathbb{N} \times \mathbb{N}$  é enumerável.

**Corolário 3.2.4.** *A reunião de uma família enumerável de conjuntos enumeráveis é enumerável.*

**Demonstração** Dados,  $X_1, X_2, \dots, X_n, \dots$  enumeráveis, existem sobrejeções  $f_1 : \mathbb{N} \rightarrow X_1$ ,  $f_2 : \mathbb{N} \rightarrow X_2, \dots, f_n : \mathbb{N} \rightarrow X_n, \dots$ . Tomando  $X = \bigcup_{i=1}^{\infty} X_n$ , definiremos a sobrejeção  $f : \mathbb{N} \times \mathbb{N} \rightarrow X$  pondo  $f(m, n) = f_n(m)$ . O caso de uma reunião finita  $X = X_1 \cup \dots \cup X_n$  reduz-se ao anterior porque então  $X = X_1 \cup \dots \cup X_n \cup X_n \cup \dots$ .

O Corolário significa que o enumerável é o “menor” dos infinitos. Com efeito, ele pode ser reformulado assim:

*Todo conjunto infinito contém um subconjunto infinito enumerável.*

Com o teorema e seus corolários, temos argumentos para provar se um conjunto é enumerável. Por exemplo, vamos mostrar com esses argumentos que o conjunto  $\mathbb{Q}$  é enumerável.

**Exemplo 3.9.** O conjunto dos números racionais é enumerável.

**Demonstração** Se indicarmos  $\mathbb{Z}^*$  o conjunto dos números inteiros  $\mathbb{Z} - \{0\}$ , veremos que  $\mathbb{Z}^*$  é enumerável. Logo é também enumerável o produto cartesiano  $\mathbb{Z} \times \mathbb{Z}^*$ . Ora, a função  $f : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ , definida por  $f(m, n) = \frac{m}{n}$ , é sobrejetiva. Segue-se do corolário 3.2.2 que  $\mathbb{Q}$  é enumerável.

### 3.2.4 Enumerabilidade do conjunto dos polinômios com coeficiente em $\mathbb{Z}$

**Teorema 3.2.3.** *Se  $A_1, A_2, \dots, A_n$  são conjuntos enumeráveis, então  $A_1 \times A_2 \times \dots \times A_n$  é enumerável.*

**Demonstração** Usaremos indução sobre  $n$ .

Para  $n = 2$  é verdadeiro pelo corolário 3.2.3.

Por hipótese de indução suponhamos que:  $A_1, A_2, \dots, A_k$  enumeráveis  $\implies A_1 \times A_2 \times \dots \times A_k$  enumerável.

Se  $n = k + 1$ ,  $A_1 \times A_2 \times \dots \times A_k \times A_{k+1} = (A_1 \times A_2 \times \dots \times A_k) \times A_{k+1}$  é enumerável, pois por hipótese de indução  $A_1 \times A_2 \times \dots \times A_k$  é enumerável.

**Exemplo 3.10.** O conjunto dos polinômios  $P_n(x) = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n; a_i \in \mathbb{Z}\}$  com grau menor ou igual a  $n$  e coeficientes inteiros é enumerável.

**Demonstração** Cada elemento de  $P_n(x)$  está associado de forma única a uma sequência  $(a_0, a_1, \dots, a_n)$  de números inteiros, de tamanho  $n + 1$ . Isto é, existe uma função bijetora  $f : P_n(x) \rightarrow \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$  ( $n + 1$  vezes). Como  $\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$  é enumerável pelo teorema 3.2.3, então  $P_n(x)$  é enumerável.

**Exemplo 3.11.** Seja  $P(x)$  o conjunto de todos os polinômios com coeficientes em  $\mathbb{Z}$ . Então  $P(x)$  é enumerável.

**Demonstração** Como  $P(x) = \bigcup_{n=0}^{\infty} P_n(x)$ , ou seja, é a união de conjuntos enumeráveis, e a união de conjuntos enumeráveis é enumerável, pelo teorema 3.2.1. Portanto  $P(x)$  é enumerável.

### 3.2.5 Enumerabilidade das sequências finitas de inteiros positivos

**Exemplo 3.12.** O conjunto das sequências finitas de inteiros positivos menores que 10.

**Demonstração** Uma sequência finita cujos elementos sejam todos inteiros positivos menores que 10, tais como  $(1, 2, 3)$ , pode ser lida como um numeral ordinário 123 decimal ou base 10. O número que esse numeral denota, cento e vinte e três, pode então ser tomado como um número de código para a sequência dada. Na verdade, é conveniente, para propósitos posteriores, modificar ligeiramente esse procedimento e escrever a sequência *ao inverso* antes de lê-la como um numeral. Assim,  $(1, 2, 3)$  seria codificado por 321, e 123 codificaria  $(3, 2, 1)$ . Em geral, uma sequência

$$s = (a_0, a_1, a_2, \dots, a_k)$$

seria codificada por

$$a_0 + 10a_1 + 100a_2 + \dots + 10^k a_k,$$

que é o número que o número decimal  $a_k \dots a_2 a_1 a_0$  representa. Além disso, também será doravante conveniente denominar o elemento inicial de uma sequência o 0-ésimo elemento; o próximo elemento, o primeiro, e assim por diante. Para decodificar e obter o  $i$ -ésimo item da sequência codificada por  $n$ , tomamos o quociente de sua divisão por  $10^i$ , e então o resto da divisão por 10. Por exemplo, para encontrar o quinto item da sequência codificada por 12345789, nós a dividimos por  $10^5$  para obter o quociente 1234, e então o dividimos por 10 para obter o resto 4.

**Exemplo 3.13.** O conjunto das sequências finitas de inteiros positivos menores que  $b$ , para qualquer  $b$  fixado.

**Demonstração** Usamos um sistema decimal, ou base 10, porque, afinal de contas, seres humanos tipicamente tem 10 dedos, e a contagem começou pela contagem nos dedos. Um sistema

análogo de base  $b$  é possível para qualquer  $b > 1$ . Para um sistema binário, ou base 2, seria usado somente os algarismos 0 e 1, com  $a_k \dots a_2 a_1 a_0$  representando

$$a_0 + 2a_1 + 4a_2 + \dots + 2^k a_k$$

Assim, por exemplo, 1001 representa  $1 + 2^3 = 1 + 8 = 9$ . Para um sistema duodecimal, ou base 12, dois algarismos adicionais, digamos, \* e ‡ como em um telefone, seriam necessários para representar dez e onze. Então, por exemplo, 1\*‡ representa  $11 + 12 \cdot 10 + 144 \cdot 1 = 275$ . Se aplicarmos a ideia do problema anterior usando a base 12 em vez da 10, poderíamos codificar sequências finitas de inteiros positivos menores que 12, e não somente sequências finitas de inteiros positivos menores que 10. De modo mais geral, podemos codificar uma sequência finita

$$s = (a_0, a_1, a_2, \dots, a_k)$$

de inteiros positivos menores que  $b$  por

$$a_0 + ba_1 + b^2a_2 + \dots + b^k a_k.$$

Para obter o  $i$ -ésimo elemento da sequência codificada por  $n$ , tomamos o quociente da divisão por  $b^i$  e então o resto da divisão por  $b$ . Por exemplo, ao trabalhar com a base 12, para obter o quinto elemento da sequência codificada por 123456789 dividimos 123456789 por  $12^5$ , obtendo o quociente 496. Dividimos agora por 12, obtemos o resto 4. Em geral, ao trabalhar com a base  $b$ , o  $i$ -ésimo elemento - contando o elemento inicial como o 0-ésimo - da sequência codificada por  $(b, n)$  será

$$\text{elementos}(i, n) = \text{res}(\text{quo}(n, b^i), b),$$

em que  $\text{quo}(x, y)$  e  $\text{res}(x, y)$  são quociente e resto da divisão de  $x$  por  $y$ .

**Exemplo 3.14.** O conjunto das sequências finitas de inteiros positivos

**Demonstração** Utilizando essa linguagem de codificar e decodificar sequências, mostramos que podemos codificar sequências cujos elementos podem ser de qualquer tamanho, mas sejam de *comprimento fixo*. O que queremos agora é uma enumeração de todas as sequências finitas - pares, triplas, quádruplas etc. - em uma lista única e, de quebra, vamos incluir igualmente as 1-uplas ou sequências de termos (1),(2),(3),... Um primeiro método, baseado nos exemplos anteriores, é o seguinte. Seja  $G_1(n)$  a sequência de um termo ( $n$ ). Seja  $G_2 = G$  a função que enumera todas as 2-uplas ou pares. Seja  $G_3$  a função que enumera todas as triplas. Sejam  $G_4, G_5, \dots$  a enumeração de todas as quádruplas, quádruplas, e assim por diante. Podemos obter uma codificação de todas as sequências finitas por pares de inteiros positivos estipulando que qualquer sequência  $s$  de comprimento  $k$  seja codificada pelo par  $(k, a)$ , em que  $G_k(a) = s$ . Uma vez que pares de inteiros positivos podem ser codificados por números isolados, obtemos indiretamente uma codificação de sequências de números. Uma outra maneira de descrever

o que está acontecendo aqui é a seguinte. Retornamos à nossa listagem original de pares, e substituímos o par  $(k, a)$  pelo  $a$ -ésimo item da lista de  $k$ -uplas. Assim,  $(1, 1)$  será substituído pelo primeiro elemento (1) na lista de 1-uplas  $(1), (2), (3), \dots$ ; enquanto  $(1, 2)$  será substituído pelo segundo item (2) da mesma lista; ao passo que  $(2, 1)$  será substituído pelo primeiro item  $(1, 1)$  da lista de todos as 2-uplas ou pares; e assim por diante. Isso nos dá a lista

$$(1), (2), (1, 1), (3), (1, 2), (1, 1, 1), (4), (2, 1), (1, 1, 2), (1, 1, 1, 1), \dots$$

(Se desejarmos incluir também a 0-uplas ou a sequência vazia(), que podemos considerar simplesmente como o conjunto vazio  $\emptyset$ , podemos colocá-la no início da lista, no que podemos considerar como a 0-ésima posição.)

Os exemplos anteriores mostraram que podemos codificar sequências de qualquer comprimento cujos elementos sejam *menores que algum limite fixado*, mas o que queremos fazer agora é mostrar como codificar sequências cujos elementos possam ser *de qualquer tamanho*. Um segundo método, baseado nos exemplos anteriores, é começar codificando sequências de pares de inteiros positivos. Consideramos que uma sequência.

$$s = (a_0, a_1, a_2, \dots, a_k)$$

seja codificada por qualquer par  $(b, n)$  tal que todos os  $a_i$  sejam menos que  $b$ , e  $n$  codifica  $s$  no sentido de que

$$n = a_0 + ba_1 + b^2a_2 + \dots + b^ka_k.$$

Assim,  $(10, 275)$  codifica  $(5, 7, 2)$ , uma vez que  $275 = 5 + 7 \cdot 10 + 2 \cdot 10^2$ , enquanto  $(12, 275)$  codifica  $(11, 10, 1)$ , dado que  $275 = 11 + 10 \cdot 12 + 1 \cdot 12^2$ . Cada sequência  $s$  terá muitos códigos, visto que, por exemplo,  $(10, 234)$  e  $(12, 238)$  igualmente codificam  $(4, 3, 2)$ , uma vez que  $4 + 3 \cdot 10 + 2 \cdot 10^2 = 234$  e  $4 + 3 \cdot 12 + 2 \cdot 12^2 = 328$ . Como no método anterior, dado que pares de inteiros positivos podem ser codificados por números isolados, obtemos indiretamente uma codificação de sequências de números.

Uma terceira abordagem, totalmente diferente, também é possível baseada no fato de que todo inteiro maior do que 1 pode ser escrito de uma única maneira como produto de potências de primos cada vez maiores, uma representação chamada *decomposição em fatores primos*. Esse fato nos permite codificar uma sequência  $s = (1, j, k, m, n, \dots)$  pelo número  $2^i 3^j 5^k 7^m 11^n \dots$ . Assim, o número de códigos para a sequência  $(3, 1, 2)$  é  $2^3 3^1 5^2 = 8 \cdot 3 \cdot 25 = 600$ .

### 3.2.6 Enumerabilidade dos subconjuntos de conjuntos enumeráveis

**Exemplo 3.15.** O conjunto dos conjuntos finitos de inteiros positivos.

**Demonstração** É fácil obter uma enumeração de conjuntos finitos a partir de uma enumeração

de seqüências finitas. Usando a seguinte enumeração de conjuntos:

$$\{1\}, \{2\}, \{1, 1\}, \{3\}, \{1, 2\}, \{1, 1, 1\}, \{4\}, \{2, 1\}, \{1, 1, 2\}, \{1, 1, 1, 1\}, \dots$$

O conjunto  $\{1, 1\}$ , cujos elementos são 1 e 1, é simplesmente o conjunto  $\{1\}$ , cujo único elemento é 1, e analogamente nos outros casos, de modo que essas listas pode ser simplificada para ficar assim:

$$\{1\}, \{2\}, \{1\}, \{3\}, \{1, 2\}, \{1\}, \{4\}, \{1, 2\}, \{1, 2\}, \{1\}, \{5\}, \dots$$

As repetições não importam.

**Exemplo 3.16.** Qualquer subconjunto de um conjunto enumerável.

**Demonstração** Dado qualquer conjunto enumerável  $A$  e uma listagem dos elementos de  $A$ :

$$a_1 a_2 a_3, \dots,$$

obtemos facilmente uma listagem com lacunas dos elementos de qualquer subconjunto  $B$  de  $A$  pelo expediente de simplesmente apagar qualquer item da lista que não pertença a  $B$ , deixando em seu lugar uma lacuna.

**Exemplo 3.17.** A união de dois conjuntos enumeráveis quaisquer.

Como já vimos anteriormente, podemos exemplificar apenas com dois conjuntos também. Sejam  $A$  e  $B$  conjuntos enumeráveis, e consideremos listagem de seus elementos:

$$a_1 a_2 a_3, \dots b_1 b_2 b_3, \dots$$

Imitando a ideia de *embaralhamento*, visto nos exemplos anteriores, obtemos a seguinte listagem dos elementos da união  $A \cup B$  (o conjunto cujos elementos são todos e somente aqueles itens que são elementos ou de  $A$  ou de  $B$  ou de ambos):

$$a_1 b_2 a_2 b_2 a_3 b_3, \dots$$

Se a intersecção  $A \cap B$  (o conjunto cujos elementos estão tanto em  $A$  quanto em  $B$ ) não for vazio, então haverá redundância nessa lista: se  $a_m = b_n$ , então esse elemento irá aparecer tanto na posição  $2m - 1$  quanto na posição  $2n$ , mas isso não importa, como já vimos.

**Exemplo 3.18.** O conjunto das cadeias finitas de um alfabeto de símbolos finitos ou enumerável

**Demonstração** Dado um “alfabeto” de qualquer número finito, ou mesmo de uma infinidade enumerável, de símbolos  $S_1 S_2 S_3, \dots$ , podemos tomar como número de código para qualquer cadeia finita

$$S_{a_0} S_{a_1} S_{a_2} \dots S_{a_k}$$

O número de códigos para a sequência finita de inteiros

$$(a_1, a_2, a_3, \dots, a_k)$$

Podemos também utilizar o método da *decomposição em fatores primos*, por exemplo, com o alfabeto ordinário de 26 letras símbolos  $S_1 = A, S_2 = B$  etc., a cadeia ou palavra CAB seria codificada pelo código para (3,1,2), que teríamos  $2^3 \cdot 3 \cdot 5^2 = 600$ .

### 3.3 Números algébricos e transcendentos

#### 3.3.1 Números algébricos

**Definição 3.2.** Seja a equação polinomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ , onde os coeficientes  $a_i$  são inteiros. Qualquer solução desta equação é chamado um número algébrico. Esta definição também pode ser reescrita como, um número  $\alpha$  é algébrico se puder fabricar uma equação polinomial com coeficientes inteiros, da qual  $\alpha$  é a raiz.

Assim qualquer número racional,  $\alpha = \frac{p}{q}$ , é algébrico, porque  $\alpha$  é raiz da equação, ou seja, todo número racional é algébrico.

$$qx - p = 0$$

Pela definição podemos verificar que qualquer números irracionais na forma  $\sqrt[n]{a}$ , com  $a \in \mathbb{Z}$ , é solução da equação

$$x^n - a = 0$$

E o mais intrigante é que os números na forma  $i\sqrt{a}$  também são números algébricos, porque é soluções da equação

$$x^2 + a = 0$$

Vamos denotar o conjunto dos números algébricos por  $\overline{\mathbb{Q}}$ . O que mais chama atenção é que apesar de certos números irracionais estarem contidos no conjunto  $\overline{\mathbb{Q}}$ , ainda assim ele é enumerável. É o que mostraremos a seguir.

#### 3.3.2 Enumerabilidade do conjunto dos números algébricos

**Teorema 3.3.1.** O conjunto  $\overline{\mathbb{Q}}$  dos números algébricos é enumerável

**Demonstração** Como foi visto nos exemplos 3.10 e 3.11, Podemos tomar para cada polinômio  $P_i(x) \in P(x)$ , valores  $R_i = \{r_1, r_2, \dots, r_k\}$  conjunto de todas as raízes de  $P_i(x)$ , temos que  $R_i$  é um conjunto finito, pois todo polinômio tem um número finito de raízes. Sabendo que  $\overline{\mathbb{Q}} = \bigcup_{i=1}^{\infty} R_i$  a união de conjuntos enumeráveis. Portanto,  $\overline{\mathbb{Q}}$  é enumerável.

### 3.3.3 Os números transcendentos

**Definição 3.3.** *Um número é chamado transcendente quando ele não é algébrico*

Esses números são chamados assim por transcenderem as operações convencionais da álgebra. Nos capítulos seguintes faremos uma abordagem maior sobre esse interessante conjunto.



# Capítulo 4

## Conjuntos não enumeráveis

Neste capítulo introduziremos a distinção entre conjuntos enumeráveis e não enumeráveis, no capítulo anterior vimos muitos exemplos de conjuntos enumeráveis. Veremos alguns exemplos de conjuntos não enumeráveis. Demonstraremos, primeiro, a existência de tais conjuntos, e então examinaremos com um pouco mais de detalhe o método, chamado diagonalização, que é usado nesta demonstração.

### 4.1 A irracionalidade do número $e$ e $\pi$

#### 4.1.1 O número $e$ é irracional

O número  $e$ , que aparece nos estudos das funções logarítmicas, é definida como número tal que a área cinza abaixo é igual a 1.

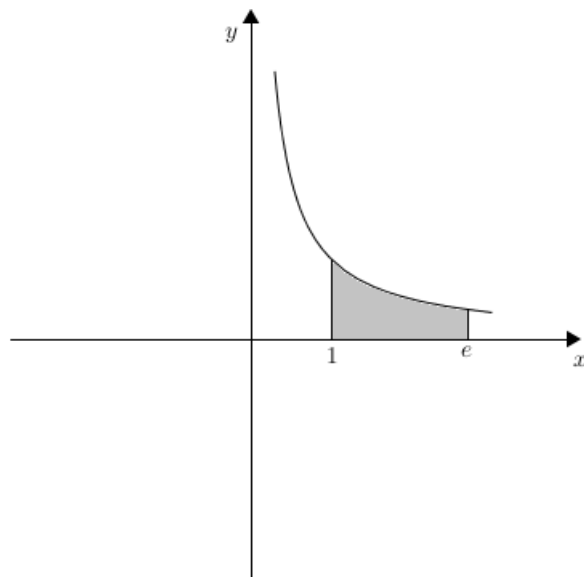


Figura 4.1: Gráfico da função  $f(x) = 1/x$  para  $x > 0$

Demonstra-se nos textos de cálculo que

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots$$

Suponha que  $e$  fosse um número racional, isto é,  $e = p/q$ , onde  $p, q \in \mathbb{N}$ , são primos entre si. Segue que

$$\frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!}\right) = \sum_{j=q+1}^{\infty} \frac{1}{j!}$$

Agora, faremos uma estimativa do segundo membro

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} = \frac{1}{q!} \left( \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \dots \right) < \frac{1}{q!} \left( \frac{1}{q+1} + \frac{1}{(q+1)^2} + \dots \right)$$

A expressão entre parênteses no último membro é uma série geométrica da forma

$$\sum_{n=1}^{\infty} r^n,$$

a qual para  $0 < r < 1$ , tem soma igual  $\frac{r}{1-r}$ . Usando este fato obtemos

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} < \frac{1}{q!} \frac{1}{q}$$

Então temos

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{q!}\right) < \frac{1}{q!} \frac{1}{q}$$

e daí

$$0 < q! \left( \frac{p}{q} - 1 - \frac{1}{1!} - \frac{1}{2!} \dots - \frac{1}{q!} \right) < \frac{1}{q}$$

Agora podemos observar que o termo do meio é inteiro pois  $q!$  cancela todos os denominadores das frações aí presentes. Mas isso é impossível, pois sendo  $\frac{1}{q} \leq 1$  a expressão acima diria que o termo médio é um inteiro positivo estritamente menos que 1. O absurdo provem da hipótese feita inicialmente que  $e$  fosse um número racional. Logo,  $e$  é irracional.

## 4.1.2 O número $\pi$ é irracional

Um dos primeiro número irracional que é nos apresentado, ainda no ensino fundamental, é o número  $\pi$ , razão do comprimento da circunferência pelo seu diâmetro. Mas, como a demonstração dessa irracionalidade desse número está fora do alcance da Matemática do ensino fundamental e médio, o aluno é apenas informado de que a expansão decimal desse número é

infinita e não periódica.

Mas com os nossos conhecimentos de cálculo diferencial podemos verificar a irracionalidade do número  $\pi$ . Considere a função

$$f(x) = \frac{x^n(1-x)^n}{n!},$$

onde  $n$  é um número natural.

Para demonstrar a irracionalidade de  $\pi$  precisaremos dos seguintes lemas.

**Lema 4.1.1.**  $D^k f(0)$  é um número inteiro para qualquer  $k = 0, 1, 2, 3, \dots$ , onde  $D^k f$  representa a  $k$ -ésima derivada de  $f$ , e  $D^0 f = f$

**Demonstração** Vamos utilizar a chamada fórmula de Leibnitz para derivadas de um produto de duas funções,  $g$  e  $h$ :

$$D^k(g \cdot h) = \sum_{j=0}^k \binom{k}{j} D^j g \cdot D^{k-j} h$$

Aplicando na fórmula  $f(x) = \frac{x^n(1-x)^n}{n!}$  temos

$$D^k(f) = \frac{1}{n!} \sum_{j=0}^k \binom{k}{j} D^j x^n \cdot D^{k-j}(1-x)^n$$

mas

$$D^j x^n|_{x=0} = \begin{cases} 0 & \text{se } j < n \\ n! & \text{se } j = n \\ 0 & \text{se } j > n \end{cases}$$

onde nossa função está restrita para  $x = 0$  quer dizer que a derivada é calculada no ponto  $x = 0$ , logo concluímos

$$D^k f(0) = 0, \text{ se } k < n$$

e

$$D^k f(0) = \frac{1}{n!} \binom{k}{n} n! D^{k-n}(1-x)^n|_{x=0}, \text{ se } k > n$$

Como os coeficientes binomiais são inteiros, segue que a expressão no segundo membro é um inteiro. Como queríamos demonstrar.

**Lema 4.1.2.**  $D^k f(1)$  é um número inteiro para qualquer  $k = 0, 1, 2, 3, \dots$

**Demonstração** Segue diretamente do lema anterior e da observação de que  $f(1-x) = f(x)$ .

A partir do que vimos vamos provar que o número  $\pi$  é irracional. Suponhamos que  $\pi^2 = \frac{p}{q}$ , onde  $\frac{p}{q}$  é uma fração irredutível, e chegarmos a um absurdo, mostrando assim que  $\pi^2$  não é racional. E, conseqüentemente,  $\pi$  também não pode ser racional, pois o quadrado de um número racional é também um racional.

Definiremos a função

$$F(x) = q^n \{ \pi^{2n} f(x) - \pi^{2n-2} D^2 f(x) + \dots + (-1)^n D^{2n} f(x) \}.$$

Como consequência dos lemas 4.1.1 e 4.1.2, e da hipótese  $\pi^2 = \frac{p}{q}$ , temos que

$$F(0) \text{ e } F(1) \text{ são números inteiros.}$$

A seguir observemos que

$$\{F'(x)\text{sen}\pi x - \pi F(x)\text{cos}\pi x\}' = \{F''(x)\text{sen}\pi x + \pi^2 F(x)\text{sen}\pi x\},$$

onde  $F'$  representa a derivada.

Um cálculo imediato da derivada segunda,  $F''$ , de  $F$  nos dá

$$\{F'(x)\text{sen}\pi x - \pi F(x)\text{cos}\pi x\}' = p^n \pi^2 f(x)\text{sen}\pi x.$$

Agora aplicando o teorema fundamental do cálculo integral que diz:

“ Se  $g : [0, 1] \rightarrow \mathbb{R}$  é uma função continuamente derivável em  $[0, 1]$ , então  $\int_0^1 g'(x)dx = g(1) - g(0)$ ”. Usaremos esse teorema para a função  $g(x) = F'(x)\text{sen}\pi x - \pi F(x)\text{cos}\pi x$  de maneira a obter

$$p^n \pi^2 \int_0^1 f(x)\text{sen}\pi x dx = \pi F(1) + \pi F(0),$$

ou seja

$$\pi p^n \int_0^1 f(x)\text{sen}\pi x dx = F(1) + F(0).$$

A ideia para finalizar a demonstração é a seguinte: o lado direito da última equação é inteiro em virtude de  $F(0)$  e  $F(1)$  serem números inteiros como já foi mostrado anteriormente. Portanto, se mostrarmos que para um  $n \in \mathbb{N}$  conveniente, o lado esquerdo é um número positivo estritamente menor que 1, teremos o absurdo procurado!

Ora, é claro que  $0 < x < 1$ , temos

$$0 < f(x) < \frac{1}{n!}$$

fazendo as devidas substituições temos

$$0 < \pi p^n \int_0^1 f(x) \operatorname{sen} \pi x dx < \pi \frac{p^n}{n!} \int_0^1 \operatorname{sen} \pi x dx = \frac{2p^n}{n!},$$

onde a última igualdade foi obtida fazendo-se a integração indicada. Como  $\lim_{x \rightarrow 2} \frac{2p^n}{n!} = 0$ , vê-se que podemos tomar um  $n \in \mathbb{N}$  tal que  $\frac{2p^n}{n!} < 1$ , encontramos o absurdo.

## 4.2 A Não-Enumeráveis de alguns conjuntos

Apresentaremos nessa secção os conjuntos não enumeráveis, em muitos casos utilizaremos os resultados já encontrados no capítulo que trata de conjuntos enumeráveis.

### 4.2.1 O conjunto das partes de $\mathbb{N}$ não é enumerável

Pelo teorema 2.2.2 que diz “Qualquer que seja o conjunto  $M$ , sua potência é sempre menor do que a potência de  $\mathcal{P}(M)$ ”. Então, se considerarmos o conjunto  $M = \mathbb{N}$  teremos que  $\#\mathbb{N} < \#\mathcal{P}(\mathbb{N})$ . Logo como não existe uma bijeção entre  $\mathbb{N}$  e suas partes, temos que o conjunto das partes de  $\mathbb{N}$  não é enumerável.

### 4.2.2 O conjunto dos números reais não é enumerável

Para provarmos que o conjunto dos números reais não é enumerável, basta provarmos que o intervalo  $(0, 1)$  também não é enumerável, pois existe uma equivalência entre este intervalo e o conjunto dos números reais.

A função

$$f(x) = \operatorname{tg}\left(\pi x - \frac{\pi}{2}\right)$$

é uma bijeção do intervalo  $(0, 1)$  com a reta toda.

Essa equivalência pode ser generalizada entre quaisquer intervalos, por exemplo

$$f : (0, 1) \longrightarrow (0, 2)$$

tomemos a função

$$f(x) = 2x$$

Generalizando,  $(0, 1)$  tem a mesma quantidade de números de  $(0, a)$  para todo número real  $a$ . De uma maneira mais geral, podemos encontrar uma equivalência entre qualquer intervalo (aberto ou fechado), com outros intervalos, ou também, com toda a reta. Para isto, temos que encontrar as funções adequadas. Esta é uma maneira de mostrar a equivalência entre os intervalos, veremos como os exemplos a seguir.

**Exemplo 4.1.**  $[a, b] \sim [0, 1]$  para todo  $a, b \in \mathbb{R}$ , de fato a função

$$f : [a, b] \longrightarrow [0, 1]$$

$$x \longrightarrow f(x) = \frac{x - a}{b - a}$$

é uma bijeção entre  $[a, b]$  e  $[0, 1]$ .

**Exemplo 4.2.**  $(-1, 1) \sim \mathbb{R}$  observemos a função

$$f : (-1, 1) \longrightarrow \mathbb{R}$$

$$x \longrightarrow \frac{x}{1 - |x|}$$

é uma bijeção.

**Exemplo 4.3.**  $(0, 1) \sim [0, 1] \sim (0, 1]$ . Para justificar consideremos os conjuntos

$$A = \left\{0, 1, \frac{1}{2}, \frac{1}{3}, \dots\right\}$$

$$B = \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$$

Temos que  $[0, 1] - A = (0, 1) - B$ ,  $[0, 1] = \{[0, 1] - A\} \cup A$  e  $(0, 1) = \{(0, 1) - B\} \cup B$ . Definiremos a função  $f : [0, 1] \longrightarrow (0, 1)$  por

$$f(x) = \begin{cases} x & \text{se } x \in [0, 1] - A; \\ \frac{1}{2} & \text{se } x = 0; \\ \frac{1}{n+2} & \text{se } x = \frac{1}{n}, n \geq 1 \end{cases}$$

assim temos uma bijeção, portanto  $[0, 1] \sim (0, 1)$ . Analogamente prova-se que  $(0, 1) \sim (0, 1]$  tomando-se  $A = \left\{1, \frac{1}{2}, \frac{1}{3}, \dots\right\}$  e  $B = \left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right\}$ . E pela propriedade transitiva podemos mostrar que  $[0, 1] \sim (0, 1]$ .

**Exemplo 4.4.** Segue dos exemplos anteriores que para todo  $a, b \in \mathbb{R}$ ,  $(a, b) \sim (a, b] \sim [a, b) \sim [a, b] \sim \mathbb{R}$

Vimos no capítulo anterior, que o conjunto  $\mathbb{Q}$  é enumerável. Isto poderia até sugerir que todos os conjuntos infinitos fossem enumeráveis, como de fato se acreditava fosse verdade. Em 1874 Cantor surpreendeu o mundo matemático sobre conjuntos, a de que o conjunto dos números reais não é enumerável, ou seja, tem cardinalidade diferente da do conjunto  $\mathbb{N}$  dos números naturais.

Para provar isso, trabalharemos com os números do intervalo  $(0, 1)$ , já que este intervalo tem cardinalidade da reta toda, como vimos anteriormente. Observemos que alguns desses números

têm mais de uma representação decimal, como 0,4 e 0,399999...., para que isto não aconteça, adotaremos, para cada número, sua representação decimal infinita. Assim,

$$0,437 = 0,4369999\dots; \quad 0,052 = 0,051999\dots$$

E com esse procedimento cada número terá uma única representação decimal infinita.

**Teorema 4.2.1.** *O conjunto dos números reais não é enumerável*

**Demonstração** Suponhamos que fosse possível estabelecer uma correspondência biunívoca dos números do intervalo  $(0, 1)$  com os números naturais. Isso é o mesmo que supor que os números desse intervalo sejam os elementos de uma sequência infinita  $x_1, x_2, x_3, \dots$ . Escritos em sua representação decimal, esses números seriam, digamos

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}a_{13}\dots a_{1n}\dots \\ x_2 &= 0, a_{21}a_{22}a_{23}\dots a_{2n}\dots \\ x_3 &= 0, a_{31}a_{32}a_{33}\dots a_{3n}\dots \\ &\dots\dots\dots \\ x_n &= 0, a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots \\ &\dots\dots\dots \end{aligned}$$

onde os  $a_{ij}$  são algarismos de zero a 9. O último passo que nos levará a uma contradição, consiste em produzir um número no intervalo  $(0, 1)$  que não esteja na lista. Isso é feito pelo processo diagonal de Cantor, usado em muitas outras situações. Construímos um número que seja diferente de  $x_1$  na primeira casa decimal, diferente de  $x_2$  na segunda casa decimal, diferente de  $x_3$  na terceira casa decimal, e assim por diante, de sorte que esse número não coincidirá com nenhum dos números da lista.

De maneira mais precisa seja o número

$$y = 0, b_1b_2b_3\dots b_n\dots$$

construído de maneira que,

$$\begin{aligned} b_1 &\neq a_{11} \text{ e } b_1 \neq 0 \\ b_2 &\neq a_{22} \text{ e } b_2 \neq 0 \\ b_3 &\neq a_{33} \text{ e } b_3 \neq 0 \\ &\vdots \\ b_n &\neq a_{nn} \text{ e } b_n \neq 0 \end{aligned}$$

com essa construção teremos  $y \neq x_n$ . Chegamos a contradição que  $y \notin (0, 1)$ .

Podemos chegar a esse mesmo resultado através do teorema 1.2.1 (Intervalos encaixados).

Suponhamos agora que o intervalo fechado  $[0, 1]$  possa ser enumerado, ou seja,

$$[0, 1] = \{x_1, x_2, x_3, \dots\}$$

poça ser disposta como uma sequência infinita.

Construamos, agora, uma sequência de intervalos fechados como segue: considerando os três subintervalos fechados de  $[0, 1]$ .

$$\left[0, \frac{1}{3}\right], \left[\frac{1}{3}, \frac{2}{3}\right], \left[\frac{2}{3}, 1\right],$$

cada um com amplitude  $\frac{1}{3}$ . Ora, existe um número real  $x$  que não pode pertencer a todos os três intervalos. Seja  $I_1 = [a_1, b_1]$  um dos três intervalos, tal que  $x_1 \notin I_1$ .

Consideremos, em seguida, os três seguintes subintervalos de  $I_1 = [a_1, b_1]$ ,

$$\left[a_1, a_1 + \frac{1}{9}\right], \left[a_1 + \frac{1}{9}, a_1 + \frac{2}{9}\right], \left[a_1 + \frac{2}{9}, b_1\right]$$

cada um com amplitude  $\frac{1}{9}$ . Analogamente, seja  $I_2$  um dos três intervalos dessa nova divisão, tal que  $x_2 \notin I_2$ . Continuando dessa maneira, obtemos uma sequência de intervalos fechados

$$I_1 \supset I_2 \supset I_3 \dots$$

tais que  $x_n \notin I_n$  para todo  $n \in \mathbb{N}$ . Então de acordo com o teorema dos intervalos encaixados, existe um real  $y \in [0, 1]$  tal que  $y$  pertence a todos os intervalos. Mas  $y \in \{x_1, x_2, \dots\}$ , logo  $y = x_m$  para algum  $m \in \mathbb{N}$ . Então, pela nossa construção,  $y = x_m \notin I_m$ , o que contradiz o fato de que  $y$  pertence a todo intervalo. Assim, a nossa hipótese de que  $[0, 1]$  é enumerável conduz a uma contradição. Logo,  $[0, 1]$  não é enumerável.

**Corolário 4.2.1.** *O conjunto dos números irracionais  $(\mathbb{R} - \mathbb{Q})$  não é enumerável.*

**Demonstração** Suponhamos que o conjunto dos números irracionais  $(\mathbb{R} - \mathbb{Q})$  seja enumerável. Então, teríamos que

$$\mathbb{R} = (\mathbb{R} - \mathbb{Q}) \cup \mathbb{Q}$$

é enumerável, o que é um absurdo pelo teorema 4.2.1.

**Corolário 4.2.2.** *O conjunto dos números transcendentais reais não é enumerável.*

Pela mesma justificativa do corolário anterior, se considerarmos os números reais como a união dos transcendentais reais com os algébricos reais, chegaremos ao mesmo absurdo. Já que o conjunto dos números algébricos é enumerável.





que é algébrico. Também do teorema de Gelfond-Schneider segue que

$$e^\pi = (e^{i\pi})^{-i} = (-1)^{-i} = 23,14069263\dots$$

é transcendente, chamado de *constante de Gelfond*

Outros transcendentos curiosos e famosos são:

O número de Morse-Thue: 0,0110101001...

A constante de Champernowne: 0,12345678910111213..., tem a interessante propriedade de conter em sua expansão decimal qualquer número que imaginarmos.

$$e^\pi$$

$$\ln 2$$

são também transcendentos.

Existe uma infinidade de números que não conhecemos a natureza transcendente deles, por exemplo:

$$e + \pi$$

$$e\pi$$

$$\pi^e$$

$$2^e$$

$$2^\pi$$

#### 4.2.4 Conjunto de Cantor não é enumerável

O conjunto de Cantor, que descreveremos agora, tem as seguintes propriedades:

- 1) É compacto.
- 2) Tem interior vazio (não contém intervalos).
- 3) Não contém pontos isolados ( todos os seus pontos são pontos de acumulação.)
- 4) É não-enumerável.

Estamos interessados na quarta propriedade, então vamos ver como é o conjunto de Cantor para mostrarmos que ele não é enumerável.

O conjunto de Cantor, representaremos por  $K$ , é um subconjunto fechado do intervalo  $[0, 1]$ , obtido como complementar de uma reunião de intervalos abertos, do seguinte modo. Retira-se do intervalo  $[0, 1]$  seu terço médio aberto  $(\frac{1}{3}, \frac{2}{3})$ . Depois retira-se o terço médio aberto de cada um dos intervalos restantes  $[0, \frac{1}{3}]$  e  $[\frac{2}{3}, 1]$ . Sobra então  $[0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$ . Em seguida, retira-se o terço médios aberto de cada um desses quatro intervalos. Repete-se o processo indefinidamente. O conjunto  $K$  dos pontos não retirados é o conjunto de Cantor.

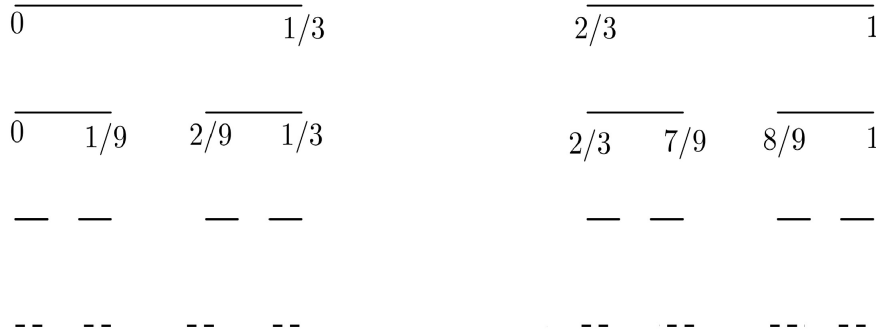


Figura 4.2: Construindo o conjunto de Cantor

Se indicarmos com  $I_1, I_2, \dots, I_n, \dots$  os intervalos abertos omitidos, veremos que  $F = \mathbb{R} - \bigcup_{n=1}^{\infty} I_n$  é um conjunto fechado logo  $K = [0, 1] \cap F$  é limitado e fechado, ou seja, o conjunto de Cantor é compacto.

Para mostra que  $K$  tem interior vazio, observamos que depois da  $n$ -ésima etapa de sua construção restam apenas intervalos de comprimento  $\frac{1}{3^n}$ . Portanto, dado qualquer intervalo  $J \subset [0, 1]$  de comprimento  $c > 0$ , se tomarmos  $n$  tal que  $\frac{1}{3^n} < c$ , o intervalo  $J$  estará mutilado depois da  $n$ -ésima etapa da formação de  $K$ . Assim,  $K$  não contém intervalos.

Os pontos extremos dos intervalos omitidos nas diversas etapas da construção do conjunto de Cantor, tais como  $\frac{1}{3}, \frac{2}{3}, \frac{1}{9}, \frac{2}{9}, \frac{7}{9}, \frac{8}{9}$ , etc, pertencem a  $K$ , pois em cada etapa são retirados apenas pontos interiores aos intervalos que restam na etapa anterior. Eles constituem um conjunto enumerável  $E$ , sem pontos isolados. Com efeito, seja  $c \in K$  extremidade de algum intervalo, digamos  $(c, b)$ , omitido de  $[0, 1]$  para formar  $K$ . Quando  $(c, b)$  foi retirado, restou um certo intervalo  $[a, c]$ . Nas etapas seguintes da construção de  $K$ , restaram sempre terços finais de intervalos, do tipo  $[a_n, c]$  com  $a_n \in E$ . O comprimento  $c - a_n$  tende a zero, logo  $a_n \rightarrow c$  e assim  $c$  não é ponto isolado de  $E$ .

Suponha agora que  $c \in K$  não seja extremo de intervalo retirado de  $[0, 1]$  durante a construção de  $K$ . (Até agora, não sabemos se de fato tais pontos existem, mas veremos logo mais que eles constituem a maioria dos pontos de  $K$ ). Provemos que  $c$  não é isolado em  $K$ . Com efeito, para cada  $n \in \mathbb{N}$ ,  $c$  pertence ao interior de um intervalo  $[x_n, y_n]$  que restou depois da  $n$ -etapa da construção de  $K$ . Temos  $x_n < c < y_n$  com  $x_n, y_n \in K$  e  $y_n - x_n = \frac{1}{3^n}$ . Logo  $c = \lim x_n = \lim y_n$  é ponto de acumulação de  $K$ .

Provaremos agora que o conjunto de Cantor  $K$  não é enumerável. Dado qualquer subconjunto enumerável  $\{x_1, x_2, \dots, x_3, \dots\} \subset K$ , obteremos um ponto  $c \in K$  tal que  $c \neq x_n$  para todo  $n \in \mathbb{N}$ . Para isso, com centro num ponto de  $K$ , tomamos um intervalo compacto não-degenerado  $I_1$  tal que  $x_1 \in I_1$ . Como nenhum ponto de  $K$  é isolado,  $I_1 \cap K$  é um conjunto infinito, compacto sem pontos isolados. Em seguida, com centro em algum ponto de  $K$  interior a  $I_1$ , tomamos um intervalo compacto não-degenerado  $I_2 \cap I_1$  tal que  $x_2 \in I_2$ . Prosseguimos analogamente, obtemos uma seqüência decrescente de intervalos compactos  $I_1 \supset I_2 \cdots \supset I_n \cdots$

tais que  $x_n \in I_n$  e  $I_n \cap K \neq \emptyset$ . Sem perda de generalidade, podemos supor que  $I_n$  tem comprimento  $< \frac{1}{n}$ . Então o ponto  $c$ , pertence a todos os  $I_n$  (cuja existência é garantida pelo teorema dos intervalos encaixados) é único, isto é,  $\bigcap_{n=1}^{\infty} I_n = \{c\}$ . Escolhendo, para  $n \in \mathbb{N}$  um ponto  $y_n \in I_n \cap K$ , teremos então  $|y_n - c| \leq \frac{1}{n}$ , donde  $\lim y_n = c$ . Como  $K$  é fechado, segue-se que  $c \in K$ . Por outro lado, para todo  $n \in \mathbb{N}$  temos  $c \in I_n$ , logo  $c \neq x_n$ , concluindo a demonstração.

Os pontos do conjunto de Cantor têm uma caracterização interessante e útil em termos de sua representação em base 3. Dado  $x \in [0, 1]$ , representar  $x$  na base 3 significa escrever  $x = 0, x_1x_2\dots$ , onde cada um dos dígitos  $x_n$  é igual a 0, 1 ou 2, de tal modo que

$$x = \frac{x_1}{3} + \frac{x_2}{3^2} + \dots + \frac{x_n}{3^n} + \dots$$

Afim de que se tenha  $x = 0, x_1x_2\dots x_n000\dots$  é necessário e suficiente que  $x$  seja um número na forma  $\frac{m}{3^n}$ , com  $m, n$  inteiros e  $m \leq 3^n$ . Por exemplo  $\frac{17}{27} = 0,122000\dots$  na base 3. Quando o denominador da fração irredutível  $\frac{p}{q}$  não é uma potência de 3 então a representação de  $\frac{p}{q}$  na base 3 é periódica. Por exemplo,  $\frac{1}{4} = 0,02020202\dots$  e  $\frac{1}{7} = 0,010212010212\dots$  na base 3. Os números irracionais tem representação não-periódica.

Na primeira etapa da formação do conjunto de Cantor, ao retirar-se o intervalo aberto  $(\frac{1}{3}, \frac{2}{3})$  ficam excluído os números  $x \in [0, 1]$  cuja representação na base 3 tem  $x_1 = 1$ , com a única exceção de  $\frac{1}{3} = 0,1$  que permanece. Na segunda etapa, foram excluído os números dos intervalos  $(\frac{1}{9}, \frac{2}{9})$  e  $(\frac{7}{9}, \frac{8}{9})$  ou seja, aqueles da forma  $0,01x_3x_4\dots$  ou da forma  $0,21x_3x_4\dots$  (com exceção de  $\frac{1}{9} = 0,01$  e de  $\frac{7}{9} = 0,21$  que permanecem). De modo geral, podemos afirmar que os elementos do conjunto de Cantor são os números do intervalo  $[0, 1]$  cuja representação  $x = 0, x_1x_2\dots x_n\dots$  na base 3 só contém os algarismos 0 e 2, com exceção daqueles que contêm um único algarismo 1 como algarismo significativo final, como  $x = 0,20221$  por exemplo. Se observarmos que  $0,0222\dots = 0,1$  podemos sempre substituir o algarismo final 1 pela sequencia  $0222\dots$ . Por exemplo:  $0,20201 = 0,20200222\dots$

Com essa representação do conjunto de Cantor na base 3, podemos mostrar de outra maneira que o conjunto  $K$  não é enumerável.

Usaremos a mesma ideia da diagonal de cantor. Suponhamos que o conjunto  $K$  seja enumerável, ou seja, existe uma bijeção  $f : \mathbb{N} \rightarrow K$  tal que

$$\begin{aligned} f(1) &= 0, a_{11}a_{12}a_{13}\dots a_{1n}\dots \in K \\ f(2) &= 0, a_{21}a_{22}a_{23}\dots a_{2n}\dots \in K \\ f(3) &= 0, a_{31}a_{32}a_{33}\dots a_{3n}\dots \in K \\ &\dots\dots\dots \\ f(n) &= 0, a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots \in K \\ &\dots\dots\dots \end{aligned}$$

Seja  $c = 0, c_1c_2c_3\dots c_n\dots \in K$  tal que  $c_n \neq a_{nn}$

$$c \neq f(1) \text{ pois } c_1 \neq a_{11}$$

$$c \neq f(2) \text{ pois } c_2 \neq a_{22}$$

$\vdots$

$$c \neq f(n) \text{ pois } c_n \neq a_{nn}$$

qualquer que seja  $n$  natural.

Ou seja,  $c \in K$  e não é imagem pela  $f$  de nenhum  $n \in \mathbb{N}$ . Logo  $f$  não é sobrejetora. Contradição.

### 4.3 A Hipótese do Contínuo e sua impossibilidade de demonstração

Começaremos a secção mostrando que existe uma equivalência entre o conjunto das partes dos naturais e os números reais.

**Lema 4.3.1.** *Seja  $C(A) = \{f : A \rightarrow \{0, 1\}; f \text{ é função}\}$ . Temos que  $C(A) \sim \mathcal{P}(A)$*

**Demonstração** De fato, vamos definir  $F : \mathcal{P}(A) \rightarrow C(A)$  por  $F(S) = f$  tal que  $f : A \rightarrow \{0, 1\}$  onde para cada  $a \in A$ ,

$$f(a) = \begin{cases} 1 & \text{se } a \in S; \\ 0 & \text{se } a \notin S \end{cases}$$

Temos que

(i)  $F$  está bem definida. De fato se  $S_1 = S_2$  temos que as funções  $f_1 : A \rightarrow \{0, 1\}$  e  $f_2 : A \rightarrow \{0, 1\}$  dadas por

$$f_1(a) = \begin{cases} 1 & \text{se } a \in S_1; \\ 0 & \text{se } a \notin S_1 \end{cases}$$

$$f_2(a) = \begin{cases} 1 & \text{se } a \in S_2; \\ 0 & \text{se } a \notin S_2 \end{cases}$$

são iguais. Assim  $F(S_1) = F(S_2)$ .

(ii)  $f$  é injetora pois se  $S_1 \neq S_2$  temos que  $S_1 \not\subseteq S_2$  ou  $S_2 \not\subseteq S_1$ . Sem perda de generalidade, suponhamos  $S_1 \not\subseteq S_2$ . Logo existe um  $s \in S_1$  tal que  $s \notin S_2$ . Daí, como  $F(S_1) = f_1$  e  $F(S_2) = f_2$ , temos que  $f_1(s) = 1$  (pois  $s \in S_1$ ) e  $f_2(s) = 0$  (pois  $s \notin S_2$ ). Assim  $f_1(s) \neq f_2(s)$  e temos  $f_1 \neq f_2$ . Portanto  $F(S_1) \neq F(S_2)$

(iii)  $f$  é sobrejetora. De fato para todo  $f \in C(A)$ ,  $f : A \rightarrow \{0, 1\}$  é uma função. Seja  $S = f^{-1}(\{1\}) = \{x \in A; f(x) = 1\}$ . Temos que  $S \subset A$  e assim  $S \in \mathcal{P}(A)$ . Agora

$$f(a) = \begin{cases} 1 & \text{se } a \in S; \\ 0 & \text{se } a \notin S \end{cases}$$

pela definição de  $S$ . Logo  $F(S) = f$ . Portanto existe um  $S \in \mathcal{P}(A)$  tal que  $F(S) = f$ .

Assim  $F$  é bijetora e temos  $\mathcal{P}(A) \sim C(A)$ .

**Teorema 4.3.1.** *A cardinalidade do conjunto das partes dos naturais é igual a cardinalidade dos reais ( $\#\mathcal{P}(\mathbb{N}) = \#\mathbb{R}$ ).*

**Demonstração** Consideremos  $\mathcal{X}_1 = \#\mathcal{P}(\mathbb{N}) = \mathcal{P}(\mathbb{Q})$ , pois  $\mathbb{N} \sim \mathbb{Q}$  e  $c = \#\mathbb{R}$ , mostraremos que  $\mathcal{X}_1 = c$

Seja  $\psi : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$  definida por  $\psi(a) = \{x \in \mathbb{Q}; x < a\}$  (subconjunto formado por todos os números racionais menores que  $a$ ). Temos que  $\psi$  é injetora. De fato sejam  $a, b \in \mathbb{R}$  com  $a < b$ . Logo existe um  $c \in \mathbb{Q}$  tal que  $a < c < b$ . Assim  $c \notin \psi(a)$  e  $c \in \psi(b)$ . Daí  $\psi(a) \neq \psi(b)$ . Temos então demonstrado que  $c \leq \mathcal{X}_1$ .

Pelo lema 4.3.1 e pela propriedade transitiva, temos que  $\mathcal{P}(\mathbb{N}) \sim \mathcal{P}(\mathbb{Q}) \sim \mathcal{P}(C) = \{f : \mathbb{N} \rightarrow \{0, 1\}; f \text{ é uma função}\}$ . Sabemos que qualquer elemento  $x \in (0, 1)$  pode ser escrito unicamente na forma  $0, x_1x_2x_3\dots$  (representação decimal de  $x$ ). Usando esse fato definimos  $F : C(\mathbb{N}) \rightarrow \{0, 1\}$  por  $F(f) = 0, f(1)f(2)f(3)\dots$ . Assim  $F(f)$  é uma representação decimal construída de zeros e uns.

Temos que  $F$  é injetora. De fato, se  $f, g \in C(\mathbb{N})$  com  $f \neq g$ , existe  $n \in \mathbb{N}$  tal que  $f(n) \neq g(n)$ . Logo  $(0, f(1)f(2)f(3)\dots f(n)\dots) \neq (0, g(1)g(2)g(3)\dots g(n)\dots)$ . Portanto  $F(f) \neq F(g)$ .

Assim  $\#C(\mathbb{N}) \leq \#(0, 1)$ . Mas  $\#C(\mathbb{N}) = \#\mathcal{P}(\mathbb{N}) = \mathcal{X}_1$  e  $\#(0, 1) = \#\mathbb{R} = c$ . Portanto  $\mathcal{X}_1 \leq c$ , temos então  $c = \mathcal{X}_1$ .

Cantor não estava satisfeito com a notação para números transfinitos e resolveu denota-los usando a primeira letra do alfabeto hebraico:

$\aleph$  (alef)

Assim Cantor denotou  $\aleph_0 = \#\mathbb{N}$  e  $\aleph_1 = c = \#\mathcal{P}(\mathbb{N}) = 2^{\aleph_0}$ . Mas qual a motivação que Cantor teve de denotar os números transfinitos por  $\aleph$ ?

A resposta é que Cantor conhecia a tradição judaica, o alfabeto hebraico.  $\aleph$  representa a natureza infinita.

Com o auxílio do seu teorema Cantor mostrou que havia muitos infinitos, cada vez maiores:

$$\#\mathbb{N} < \#\mathcal{P}(\mathbb{N}) < \#\mathcal{P}(\mathcal{P}(\mathbb{N})) < \dots$$

usando a notação de cantor

$$\aleph_0 < \aleph_1 < \aleph_2 \dots$$

Cantor levantou a hipótese de haver uma sequência de alefs:

$$\aleph_0, \aleph_1, \aleph_2, \dots, \aleph_n \dots$$

apesar de não saber a colocação correta de cada um.

Esses resultados constituíram um primeiro avanço na compreensão do infinito real, e mostraram que as descobertas eram dignas de interesse. Eles permitiram construir uma hierarquia de totalidades infinitas.

Os primeiros resultados de Cantor não deixaram de encontrar críticas e reprovações. O matemático italiano Leopold Kronecker chegou a negar a publicação de um manuscrito de Cantor no *Journal de Crelle*, uma das mais prestigiosas revistas de matemática da época, na qual Cantor nunca mais aceitou publicar seus trabalhos. O artigo em questão continha um resultado surpreendente. Cantor, sempre preocupado em classificar os infinitos, descobriu com assombro que objetos de dimensões diferentes tinham a mesma ordem de infinito. Em termos de tamanho (no sentido dos conjuntos infinitos), uma reta e um plano (ou mesmo um espaço de  $n$  dimensão) são idênticos. A respeito disso, ele escreveu, em 1877, para Dedekind “estou vendo mais não acredito”.

Vejam uma prova deste fato.

Primeiro vejamos que. Se  $A \sim C$  e  $B \sim D$  então  $A \times B \sim C \times D$ . Isto segue do fato que existem funções bijetoras  $f : A \rightarrow C$  e  $g : B \rightarrow D$ . Definimos por  $h : A \times B \rightarrow C \times D$  por  $h(a, b) = (f(a), g(b))$ , verifica-se facilmente que  $h$  é bijetora.

Vamos mostrar que para  $n \geq 1$ , temos que  $\mathbb{R}^n \sim \mathbb{R}$ . De fato, temos que  $\mathbb{R} \sim (0, 1)$ . Assim, como vimos,  $\mathbb{R}^2 \sim (0, 1) \times (0, 1)$ .

Vamos definir  $\psi : (0, 1) \times (0, 1) \rightarrow (0, 1)$  por  $\psi(0, x_1x_2x_3\dots, 0, y_1y_2y_3\dots) = 0, x_1y_1x_2y_2x_3y_3\dots$ . Claramente está bem definida.

$\psi$  é injetor, pois  $\psi(0, x_1x_2x_3\dots, 0, y_1y_2y_3\dots) = (0, z_1z_2z_3\dots, 0, w_1w_2w_3\dots) = 0, x_1y_1x_2y_2x_3y_3\dots = 0, z_1w_1z_2w_2z_3w_3\dots \implies x_1 = z_1, y_1 = w_1, x_n = z_n, y_n = w_n \implies 0, x_1x_2\dots = 0, z_1z_2\dots$  e  $0, y_1y_2\dots = 0, w_1w_2\dots \implies (0, x_1x_2x_3\dots, 0, y_1y_2y_3\dots) = (0, z_1z_2z_3\dots, 0, w_1w_2w_3\dots)$ .

$\psi$  é sobrejetiva. Para todo  $z \in (0, 1)$ , temos  $z = z_1z_2z_3\dots$ . Sejam  $x = z_1z_2z_3\dots$  e  $y =$

$z_2 z_4 z_6 \dots$ . Então  $\psi(x, y) = \psi(0, z_1 z_3 z_5 \dots, 0, z_2 z_4 z_6 \dots) = 0, z_1 z_2 z_3 \dots = z$ . Assim existe  $(x, y) \in (0, 1) \times (0, 1)$  tal que  $\psi(x, y) = z$ .

Logo  $\psi$  é bijetora e temos  $\mathbb{R} \sim (0, 1) \sim (0, 1) \times (0, 1) \sim \mathbb{R}^2$ .

Agora, por indução sobre  $n$ , mostra-se que  $\mathbb{R} \sim \mathbb{R}^n$ . Pela propriedade transitiva  $\mathbb{R} \sim \mathbb{R}^2 \sim \dots \sim \mathbb{R}^n$ , para todo  $n \geq 1$

### 4.3.1 A Hipótese do Contínuo

Cantor descobriu um problema de tamanha dificuldade, que até hoje não conseguimos dominar totalmente: a “Hipótese do Continuum”(Contínuo).

O cardinal do conjunto dos números reais,  $c = 2^{\aleph_0}$ , chamado de contínuo, é estritamente maior que o cardinal dos números naturais,  $\aleph_0$ . A hipótese do contínuo diz que entre esses dois tamanhos de conjuntos infinitos não há nenhum outro. Ou seja, “Não existe número cardinal  $u$  tal que  $\aleph_0 < u < c$ ”.

Como Cantor designou por  $\aleph_1$  o menor cardinal depois de  $\aleph_0$ , a hipótese do contínuo é simplesmente:

$$c = 2^{\aleph_0}$$

Generalizando, designando por  $\aleph_{n+1}$  o menor cardinal depois de  $\aleph_n$ , temos:

$$\aleph_0 < \aleph_1 < \aleph_2 < \dots < \aleph_n < \dots$$

A hipótese generalizada do contínuo é a afirmação que, Não existe número cardinal  $u$  tal que  $\aleph_n < u < \aleph_{n+1}$ .

Cantor morreu com transtornos mentais em uma clinica de repouso, em 1918, sem conseguir provar nem descartar a hipótese do contínuo.

Em 1938, o matemático austríaco Kurt Godel (1906-1978) mostrou que em qualquer sistema haverá proposições que não podem ser provadas (Teorema da Incompletude de Godel). Mostrou também que a Hipótese do Contínuo é consistente com os axiomas da Teoria dos Conjuntos (não produzia contradições). Godel, também desenvolveu transtornos mentais. Não conseguiu mostrar que a negação da Hipótese do Contínuo também era consistente com a Teoria dos Conjuntos.

Em 1963, Paul Cohen (1934-2007), deu o segundo passo. Mostrou que a Hipótese do Contínuo era independente de todos os axiomas da Teoria dos Conjuntos. Poderia ser tomada tanto verdadeira como falsa. Verdadeira ou não a Hipótese do Contínuo não poderia ser provada nem refutada no sistema atual. Ganhou a medalha Fields por esse trabalho em 1966.

Esses dois resultados afirmam que quem aceita a teoria usual dos conjuntos pode, sem risco de introduzir contradições, adotar tanto a hipótese do contínuo, como sua negação.

Algumas frases marcantes de grandes contemporâneos de Cantor.



*“Deus criou os números naturais. O resto é obra dos homens”. Leopold Kronecker  
(1823-1891)*

“A teoria dos conjuntos de Cantor é uma moléstia, uma doença perversa, da qual algum dia, os matemáticos estarão curados.”

Henri Poincaré(1854-1912)

“Ninguém nos expulsará do paraíso que Georg Cantor abriu para nós”

David Hilbert (1862-1943)

# Capítulo 5

## Considerações Finais

Conceitos e propriedades importantes da teoria dos conjuntos foram utilizados neste trabalho para definir enumerabilidade, não-enumerabilidade, cardinalidade e hipótese do contínuo. Este contexto, traduz a intenção de oferecer uma alternativa para os professores do ensino básico à abordagem de conjuntos numéricos. Essa alternativa centraliza-se em que alguns conjuntos podem ser posto em uma lista e outros não, isso fica muito interessante quando se trabalha com conjuntos infinitos.

A compreensão da abordagem sobre contar ou não contar conjuntos infinitos, é uma questão delicada, pois para tal, se faz necessário toda uma construção axiomática de certa forma com o rigor que a matemática exige. Por exemplo, o estudo sobre injetividade e sobrejetividade, cujo são essenciais para o nosso trabalho, geralmente encontra-se dificuldades em construir situações concretas e cotidianas para tais assuntos. E um dos objetivos desse trabalho é mostrar que esses tópicos são de fundamental importância para as construções matemáticas.

Através deste trabalho espera-se contribuir com professores e alunos da formação básica, tanto na parte conceitual trabalhando o rigor matemático, como também na parte motivacional. Espera-se realmente que sirva de motivação para a pesquisa do tema, já que é um tema que atiza a curiosidade daqueles que gostam de estudar matemática. É bom ressaltar, em especial para o professor do ensino básico, que não se espera a aplicabilidade total do assunto para os alunos, mas sim possa construir estratégias pedagógica de ensino referente ao tema, e que tais se demonstre eficientes e significativos para o amadurecimento matemático dos alunos.

# Referências Bibliográficas

- [1] LIPSCHUTZ, S. *Topologia Geral*. Coleção Schaum, Ed. McGraw-Hill do Brasil, LTDA. São Paulo, Brasil, 1979.
- [2] Lima, Elon Lages *Curso de análise; v.1.11.ed.* Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2006.
- [3] Lima, Elon Lages *Análise real volume 1. Funções de uma variável. 11.ed.* Rio de Janeiro: IMPA, 2011.
- [4] BOYER, C.B. *História da Matemática*. São Paulo: Editora da Universidade de São Paulo, 1974.
- [5] \_\_\_\_\_. *Análise Real/Compleitude*. Disponível em: <http://pt.wikibooks.org/wiki/An>. Acesso em: 15 nov. 2014.
- [6] ÁVILA, Geraldo Severo de Souza. *Análise matemática para licenciatura*. 3ª ed.rev. e ampl. São Paulo: Editora Blucher, 2006.
- [7] APOSTOL, Tom M. *Cálculo I, Cálculo com funções de uma variável, com uma introdução à Álgebra Linear*. Editorial Reverté. Janeiro de 2013.
- [8] \_\_\_\_\_. *Maria Gorete Carreira Andrade*. Disponível em: <http://www.lce.esalq.usp.br/arquivos/aulas/2012/LCE5806/C5.pdf>
- [9] NERI, Cassio. *Curso de Análise Real*. 1 ed - Rio de Janeiro.
- [10] Lima, Elon Lages, José Nicolau. *A matemática do ensino médio*. Vol 1/ Elon Lages. Lima, Paulo Cezar Pinto Carvalho, Eduardo Wagner, Augusto César Morgado. - 9.ed. - Rio de Janeiro: SBM 2006.
- [11] Boolos, George S. *Computabilidade e lógica*./ George S. Boolos, John P. Burgess, Richard C. Jeffrey; tradução de Cezar A. Mortari. - São Paulo Editora Unesp, 2012.
- [12] Figueiredo, Djairo Guedes. *Análise I*/ Djairo Guedes de Figueiredo. - 2. ed. - Rio de Janeiro: LTC-Livros Técnicos e Científicos Editora S.A, 1996.

- [13] Figueiredo, Djairo Guedes. *Números Irracionais e transcendentais.*/ Djairo Guedes de Figueiredo. - 3. ed. - Rio de Janeiro: SBM, 2011.
- [14] Hunter, David J. *Fundamentos da Matemática Discreta*/ David J. Hunter; tradução Paulo Porto Martins; revisão técnica Jairo da Silva Bochi. - Rio de Janeiro: LTC, 2011.