

Conjuntos e Fundamentos

Fernando Ferreira
Universidade de Lisboa

Janeiro de 2011

raSCumho

Chapter 1

Estruturas de Dedekind-Peano

Definição 1. Uma estrutura de Dedekind-Peano é um triplo $(N, S, 0)$ em que N é um conjunto, S é uma função de N para N e 0 é um elemento de N de tal modo que:

1. $\forall x \in N (S(x) \neq 0)$.
2. $\forall x \in N \forall y \in N (S(x) = S(y) \rightarrow x = y)$.
3. Para todo o conjunto $X \subseteq N$ tem-se

$$0 \in X \wedge \forall x \in N (x \in X \rightarrow S(x) \in X) \rightarrow X = N.$$

A condição (3) denomina-se de princípio de indução.

O seguinte teorema, que demonstraremos mais tarde, é essencial para o desenvolvimento da aritmética:

Teorema (Recursão de Dedekind). Seja $(N, S, 0)$ uma estrutura de Dedekind-Peano, X um conjunto, $a \in X$ e $f : X \mapsto X$ uma função. Então existe uma (única) função $h : N \mapsto X$ tal que $h(0) = a$ e, para todo $m \in N$, $h(S(m)) = f(h(m))$.

Como iremos ver, este teorema permite mostrar que duas quaisquer estruturas de Dedekind-Peano são isomorfas. Nesta conformidade, a menos de isomorfismo, existe (quanto muito) apenas uma única estrutura de Dedekind-Peano. Também iremos ver que a axiomática da teoria dos conjuntos permite mostrar a existência de uma estrutura de Dedekind-Peano. A esta única (a menos de isomorfismo) estrutura chamamos a estrutura dos *números naturais* e denotamos o seu domínio por \mathbb{N} . Naturalmente, designa-se $S(0)$ por 1, $S(1)$ por 2, e assim sucessivamente.

Fixe-se n um número natural. Tomando $X = \mathbb{N}$, $a = n$ e $f = S$ no teorema de recursão de Dedekind, existe $h_n : \mathbb{N} \mapsto \mathbb{N}$ tal que $h_n(0) = n$ e, para todo $m \in \mathbb{N}$, $h_n(S(m)) = S(h_n(m))$. Que função é esta? Calculemos alguns valores: $h_n(0) = n$, $h_n(1) = h_n(S(0)) = S(h_n(0)) = S(n)$, $h_n(2) = h_n(S(1)) = S(h_n(1)) = S(S(n))$, etc. Intuitivamente, $h_n(k)$ é a soma de n com k , i.e.,

é $n + k$. Em vista disto, vamos utilizar o sinal '+' para denotar a função de $\mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ que satisfaz as condições:

- i. $n + 0 = n$, e
- ii. $n + S(m) = S(n + m)$.

Note-se que, trivialmente, se tem $S(n) = n + 1$. Assim, as condições acima também se podem escrever da seguinte maneira:

- i. $n + 0 = n$, e
- ii. $n + (m + 1) = (n + m) + 1$.

Proposição 1 (Lei associativa da adição). *Para todos os números naturais m , n e k , $m + (n + k) = (m + n) + k$.*

Demonstração. Sejam m e n números naturais. Vamos demonstrar, por indução em k , que $\forall k \in \mathbb{N} (m + (n + k) = (m + n) + k)$.

Caso base: Se $k = 0$, então $m + (n + 0) = m + n = (m + n) + 0$. Estas duas igualdades justificam-se por (i) da definição de adição.

Passo de indução: Seja k arbitrário e, assumamos (por hipótese de indução) que $m + (n + k) = (m + n) + k$. Então:

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

Note-se que apenas utilizámos as propriedades (i) e (ii) da definição de adição e a hipótese de indução. \square

Por que razão esta demonstração é justificada? Porque estamos a utilizar a terceira propriedade das estruturas de Dedekind-Peano! No caso acima, dados m, n números naturais, define-se $X = \{k \in \mathbb{N} : m + (n + k) = (m + n) + k\}$. Ora, mostrar que $\forall k \in \mathbb{N} (m + (n + k) = (m + n) + k)$ é o mesmo que ver que $X = \mathbb{N}$. Para ver isto basta, de acordo com a terceira propriedade mencionada, ver que $0 \in X$ e que $\forall k (k \in X \rightarrow k + 1 \in X)$ é verdadeiro. Ou seja, basta ver que $m + (n + 0) = m + n = (m + n) + 0$ (é o caso base acima) e que, para todo $k \in \mathbb{N}$, se $m + (n + k) = (m + n) + k$ (hipótese de indução) então $m + (n + (k + 1)) = (m + n) + (k + 1)$ (tese de indução). Ora, isto é precisamente o passo de indução acima.

Proposição 2 (Lei do corte para a adição). *Para quaisquer números naturais m, n e k , se $m + k = n + k$ então $m = n$.*

Demonstração. A demonstração é imediata por indução em k . \square

Proposição 3. *Para todo o natural $n \neq 0$ tem-se $\exists^1 m (m + 1 = n)$.*

Demonstração. Convém separar a asserção de existência da asserção de unicidade. Esta última resume-se a mostrar que

$$m + 1 = n \wedge r + 1 = n \rightarrow m = r.$$

Mas isto é imediato pela segunda propriedade das estruturas de Dedekind-Peano. A asserção de existência, $n \neq 0 \rightarrow \exists m(m + 1 = n)$ demonstra-se facilmente por indução em n . O caso base é trivial. O passo de indução nem sequer utiliza a hipótese de indução pois a tese de indução é claramente verdadeira: $n + 1 \neq 0 \rightarrow \exists m(m + 1 = n + 1)$. \square

Exercício 1. Mostre que, para quaisquer números naturais m e n :

1. $0 + m = m$.
2. $(m + 1) + n = (m + n) + 1$.
3. Lei comutativa da adição: $m + n = n + m$ (Sugestão: use a alínea anterior).

De maneira análoga ao caso da adição, podemos definir – com a ajuda do teorema da recursão – a operação de multiplicação:

- i. $n \cdot 0 = 0$, e
- ii. $n \cdot (m + 1) = (n \cdot m) + n$.

Mais concretamente: fixamos n . Considere-se a função $f_n : \mathbb{N} \mapsto \mathbb{N}$ definida por $f_n(m) = m + n$ e ponha-se $a = 0$. Pelo teorema da recursão, existe uma única função $h_n : \mathbb{N} \mapsto \mathbb{N}$ tal que $h_n(0) = 0$ e $h_n(m + 1) = f_n(h_n(m))$. Se escrevermos $n \cdot m$ em vez de $h_n(m)$ ficamos com as equações (i) e (ii) acima.

Proposição 4. Para todos os naturais n e m , $n \cdot m = 0 \rightarrow n = 0 \vee m = 0$.

Demonstração. Admitamos que $n \neq 0$ e $m \neq 0$. Pela Proposição 3, existem naturais l e r tais que $n = l + 1$ e $m = r + 1$. Vem:

$$nm = nS(r) = nr + n = nr + S(l) = S(nr + l) \neq 0. \quad \square$$

Proposição 5 (Lei distributiva da multiplicação em relação à adição). Para todos os números naturais m , n e k , $m \cdot (n + k) = m \cdot n + m \cdot k$.

Notação. Observe-se que não colocámos nem $m \cdot n$ nem $m \cdot k$ entre parêntesis pois, como é habitual, dá-se precedência às multiplicações em relação às adições.

Demonstração. Sejam m e n números naturais. Vamos demonstrar, por indução em k , que $\forall k \in \mathbb{N} (m \cdot (n + k) = m \cdot n + m \cdot k)$.

Caso base: Se $k = 0$, então $m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$. Todas estas igualdades se justificam por meio das definições.

Passo de indução: Seja k arbitrário e, assumamos (por hipótese de indução) que $m \cdot (n + k) = m \cdot n + m \cdot k$. Então:

$$\begin{aligned} m \cdot (n + (k + 1)) &= m \cdot ((n + k) + 1) \\ &= m \cdot (n + k) + m \\ &= (m \cdot n + m \cdot k) + m \\ &= m \cdot n + (m \cdot k + m) \\ &= m \cdot n + m \cdot (k + 1) \end{aligned}$$

onde utilizámos a propriedade associativa da adição na penúltima igualdade. \square

Exercício 2. Mostre que, para quaisquer números naturais m, n e k :

1. $n \cdot 1 = n$.
2. Lei associativa da multiplicação: $(m \cdot n) \cdot k = m \cdot (n \cdot k)$.
3. $(n + 1) \cdot m = (n \cdot m) + m$.
4. Lei comutativa da multiplicação: $m \cdot n = n \cdot m$ (Sugestão: use a alínea anterior).

Exercício 3. Defina a operação de exponenciação numa estrutura de Dedekind-Peano qualquer e demonstre as propriedades fundamentais desta operação.

Definição 2. Para números naturais n e m dizemos que n é menor do que m , e escreve-se $n < m$ se existe um número natural $k \neq 0$ tal que $n + k = m$.

Exercício 4. Mostre que, para quaisquer números naturais m, n e k :

1. $m < m + 1$.
2. $m < n + 1 \leftrightarrow m < n \vee m = n$.
3. Anti-reflexividade de $<$: $m \not< m$ (Sugestão: use a lei do corte).
4. Transitividade de $<$: $m < n \wedge n < k \rightarrow m < k$.

Proposição 6 (Tricotomia). Para todos os números naturais m e n ou se tem $m < n$, ou $m = n$ ou $n < m$. Além disso, os casos são mutuamente incompatíveis.

Demonstração. Fixemos m . Vamos demonstrar que $m < n \vee m = n \vee n < m$ vale para todo o número natural n por indução em n .

Caso base: Este é o caso em que $n = 0$. Neste caso, se m é 0, então é claro que $m = n$. Por outro lado, se $m \neq 0$, então $n < m$.

Passo de indução: Seja n arbitrário e, assumamos (por hipótese de indução) que $m < n \vee m = n \vee n < m$. Se $m < n$, como $n < n + 1$ sai, por transitividade, $m < n + 1$. Se $n = m$, então $m < n + 1$. Resta ver o caso em que $n < m$. Então, $n + (k + 1) = m$ para certo número natural k . Se $k = 0$, sai $m = n + 1$. Suponhamos que $k \neq 0$. Então $m = n + (k + 1) = (n + 1) + k$, donde $n + 1 < m$.

É claro que os três casos acima são mutuamente incompatíveis. \square

Uma *ordem total* (estrita) é uma relação binária anti-reflexiva, transitiva e tricotômica. Mostrámos acima que a relação $<$ numa estrutura de Dedekind-Peano é uma relação de ordem total. A seguinte lei é fundamental:

Proposição 7 (Lei do corte para a multiplicação). Para quaisquer números naturais m, n e k com $k \neq 0$, se $m \cdot k = n \cdot k$ então $m = n$.

Demonstração. Nas condições da hipótese da proposição, admitamos que $mk = nk$ e que $m \neq n$. Por tricotomia, sem perda de generalidade podemos supor que $m < n$. Tome-se $r \neq 0$ tal que $n = m + r$. Vem $mk = nk = (m + r)k = mk + rk$. Logo, pela lei do corte para a adição, sai $rk = 0$. Isto contradiz a Proposição 4. \square

Exercício 5. Para todos $n, m, r \in \mathbb{N}$, se $n < m$ então $n + r < m + r$ e, caso $r \neq 0$, $n \cdot r < m \cdot r$.

Chapter 2

Princípio do mínimo

Dados números naturais n e m , escrevemos $n \leq m$ para abreviar a disjunção $n < m \vee n = m$.

Teorema (Princípio do mínimo). *Seja X um subconjunto não vazio de números naturais. Então X tem elemento mínimo, i.e., existe $n \in X$ tal que, para todo $m \in X$, $n \leq m$.*

Demonstração. Suponhamos que não, i.e., que X não tem elemento mínimo. Vamos provar por indução em k que, para todo k , se tem $\forall m < k (m \notin X)$. Note que este facto implica imediatamente que $X = \emptyset$.

Caso base: Claro que $\forall m < 0 (m \notin X)$, pois a condição “ $m < 0$ ” nunca é verdadeira.

Passo da indução: Seja k arbitrário e suponhamos, por hipótese de indução, que $\forall m < k (m \notin X)$. Ora, não se pode ter $k \in X$ pois, então, k seria elemento mínimo de X . Logo, $\forall m < k + 1 (m \notin X)$, como se queria. \square

Proposição 8 (Princípio da indução completa). *Seja X um conjunto de números naturais. Suponhamos que para todo o número natural n se tem a condição $(\forall m < n (m \in X)) \rightarrow n \in X$ (condição de progressão). Então $X = \mathbb{N}$.*

Demonstração. Admitamos, com vista a um absurdo, que X é um subconjunto próprio de \mathbb{N} . Isto quer dizer que $\mathbb{N} \setminus X$ é não vazio. Pelo princípio do mínimo $\mathbb{N} \setminus X$ tem um elemento mínimo n . Logo, $\forall m < n (m \in X)$. Pela condição de progressão conclui-se que $n \in X$, o que é absurdo. \square

Exercício 6. *Mostre que todo o subconjunto não vazio e majorado de \mathbb{N} tem elemento máximo.*

Chapter 3

Teorema da recursão de Dedekind

Este capítulo é dedicado à demonstração do teorema da recursão e ao teorema do isomorfismo de Dedekind. Sejam dados $(N, S, 0)$ uma estrutura de Dedekind-Peano, X um conjunto, a um elemento de X e f uma função de X para X . Considere-se o seguinte conjunto \mathcal{F} :

$$\mathcal{F} = \{h : h \text{ é uma função parcial de } N \text{ para } X, 0 \in \text{dom}(h), h(0) = a \text{ e} \\ \forall k \in N (S(k) \in \text{dom}(h) \rightarrow k \in \text{dom}(h) \wedge h(S(k)) = f(h(k)))\},$$

onde por uma função *parcial* de N para X simplesmente se entende uma função dum subconjunto de N para X . Sejam $h_1, h_2 \in \mathcal{F}$. Argumenta-se por indução que, para todo $n \in N$, se $n \in \text{dom}(h_1) \cap \text{dom}(h_2)$ então $h_1(n) = h_2(n)$. Se $n = 0$, então $h_1(n) = a = h_2(n)$. Suponhamos que $S(n) \in \text{dom}(h_1) \cap \text{dom}(h_2)$. Então, $n \in \text{dom}(h_1) \cap \text{dom}(h_2)$ e, por hipótese de indução, $h_1(n) = h_2(n)$. Sai, $h_1(S(n)) = f(h_1(n)) = f(h_2(n)) = h_2(S(n))$. Do que se discutiu, conclui-se que $\tilde{h} := \bigcup \mathcal{F}$ é uma *função*. Note que, por definição, $(n, x) \in \tilde{h}$ se, e somente se, existe $h \in \mathcal{F}$ tal que $(n, x) \in h$. Vamos ver que \tilde{h} é a função que satisfaz os requisitos da conclusão do teorema de recursão.

Em primeiro lugar, verificamos que $\text{dom}(\tilde{h}) = N$. Mostramos por indução que, para todo $n \in N$, $n \in \text{dom}(\tilde{h})$. Claro que $0 \in \text{dom}(\tilde{h})$, pois a função $\{(0, a)\}$ (definida só em 0) está em \mathcal{F} . Suponhamos que $n \in \text{dom}(\tilde{h})$. Então existe $h \in \mathcal{F}$ tal que $n \in \text{dom}(h)$. É fácil de argumentar que $h \cup \{(S(n), f(h(n)))\}$ é uma função de \mathcal{F} . Daqui sai que $S(n) \in \text{dom}(\tilde{h})$.

Por construção, a função (total) \tilde{h} satisfaz as condições desejadas. A parte da unicidade do teorema da recursão argumenta-se facilmente por indução.

É, por vezes, útil enunciar o teorema da recursão numa forma mais geral, na qual o valor da função no sucessor dum dado número não depende apenas do valor da função no número mas também do próprio número em si:

Corolário 1. *Seja $(N, S, 0)$ uma estrutura de Dedekind-Peano, X um conjunto, $a \in X$ e $f : X \times N \mapsto X$ uma função. Então existe uma (única) função $h : N \mapsto X$ tal que $h(0) = a$ e, para todo $m \in N$, $h(S(m)) = f(h(m), m)$.*

Demonstração. Esta versão do teorema da recursão poder-se-ia mostrar de modo análogo ao próprio teorema da recursão. Aqui mostramos que é um

corolário do teorema da recursão. Considere-se a função $f' : X \times N \mapsto X \times N$ definida por $f'(x, n) = (f(x, n), S(n))$. Pelo teorema da recursão existe uma função $h' : N \mapsto X \times N$ tal que $h'(0) = (a, 0)$ e $h'(S(n)) = f'(h'(n))$. Note-se que a função h' é da forma $n \rightsquigarrow (h'_1(n), h'_2(n))$, onde $h'_1 : N \mapsto X$ e $h'_2 : N \mapsto N$. Ou seja, $h'(n) = (h'_1(n), h'_2(n))$ para todo $n \in N$. Tem-se pois:

$$\begin{cases} h'_1(0) = a \\ h'_2(0) = 0 \\ h'_1(S(n)) = f(h'_1(n), h'_2(n)) \\ h'_2(S(n)) = S(h'_2(n)) \end{cases}$$

Por indução, mostra-se facilmente que $h'_2(n) = n$, para todo $n \in N$. E, por definição, $h'_1(0) = a$ e $h'_1(S(n)) = f(h'_1(n), h'_2(n)) = f(h'_1(n), n)$. Logo a função h'_1 tem as propriedades desejadas.

A unicidade demonstra-se directamente por indução. \square

Exercício 7. Defina, por recursão, a função factorial $n \rightsquigarrow n!$ numa estrutura de Dedekind-Peano qualquer.

Teorema (Isomorfismo de Dedekind). Sejam $(N_1, S_1, 0_1)$ e $(N_2, S_2, 0_2)$ duas estruturas de Dedekind-Peano. Então existe um isomorfismo entre elas, i.e., existe uma bijecção $f : N_1 \mapsto N_2$ tal que $f(0_1) = 0_2$ e, para todo $n \in N_1$, $f(S_1(n)) = S_2(f(n))$. Além disso, o isomorfismo é único.

Demonstração. Pelo teorema da recursão aplicado à estrutura $(N_1, S_1, 0_1)$, existe uma função $f : N_1 \mapsto N_2$ tal que $f(0_1) = 0_2$ e, para todo $n \in N_1$, $f(S_1(n)) = S_2(f(n))$. Analogamente, pelo teorema da recursão aplicado agora à estrutura $(N_2, S_2, 0_2)$, existe uma função $g : N_2 \mapsto N_1$ tal que $g(0_2) = 0_1$ e, para todo $m \in N_2$, $g(S_2(m)) = S_1(g(m))$. É fácil de ver, por indução em n , que para todo $n \in N_1$ se tem $g(f(n)) = n$. I.e., $g \circ f = id_{N_1}$. Analogamente, $f \circ g = id_{N_2}$. Assim, f é uma bijecção.

A parte da unicidade é consequência do teorema da recursão. \square

Exercício 8. (Recursão completa) Seja n um número natural. Defina-se $[n] := \{k \in \mathbb{N} : k < n\}$. Dado X um conjunto, uma sequência finita de elementos de X é uma função $s : [n] \mapsto X$. Denota-se por $X^{<\mathbb{N}}$ o conjunto de todas as sequências finitas de elementos de X . Tome-se $f : X^{<\mathbb{N}} \mapsto X$ uma função. Mostre que existe uma (única) função $h : \mathbb{N} \mapsto X$ tal que, para todo $n \in \mathbb{N}$, $h(n) = f(\langle h(0), \dots, h(n-1) \rangle)$.

No enunciado acima, a notação $\langle h(0), \dots, h(n-1) \rangle$ é auto-explanatória.

Chapter 4

Racionais positivos

Denotamos por \mathbb{N}^+ o conjunto dos números naturais não nulos.

Proposição 9. *Considere-se a seguinte relação binária em $\mathbb{N}^+ \times \mathbb{N}^+$ definida por $(n, m) \approx (k, r)$ se, e somente se, $n \cdot r = k \cdot m$. Esta relação é uma relação de equivalência e a classe de equivalência de (n, m) denota-se por $\frac{n}{m}$.*

Deixamos a demonstração desta proposição como exercício. Definimos o conjunto \mathbb{Q}^+ dos números *racionais positivos* como sendo o conjunto $\mathbb{N}^+ \times \mathbb{N}^+ / \approx$ das classes de equivalência da relação \approx . Distinguimos o seguinte elemento de \mathbb{Q}^+ : denotamos por $1_{\mathbb{Q}^+}$ a classe de equivalência $\frac{1}{1}$.

Exercício 9. *Mostre que $1_{\mathbb{Q}^+} = \{(m, m) : m \in \mathbb{N}^+\}$.*

Em \mathbb{Q}^+ podemos definir as operações de adição e multiplicação da seguinte forma:

$$\frac{n}{m} + \frac{k}{r} := \frac{nr + km}{mr}$$
$$\frac{n}{m} \cdot \frac{k}{r} := \frac{nk}{mr}$$

Estamos a definir estas operações em \mathbb{Q}^+ à custa das operações em \mathbb{N}^+ . Mas, claro, temos que verificar que as definições não dependem dos representantes. Mais precisamente, temos que verificar que se $(n, m) \approx (n', m')$ e $(k, r) \approx (k', r')$ então $(nr + km, mr) \approx (n'r' + k'm', m'r')$ e $(nk, mr) \approx (n'k', m'r')$. Deixamos estas verificações como exercícios.

Geralmente omitimos o subscrito \mathbb{Q}^+ da expressão $1_{\mathbb{Q}^+}$.

Proposição 10. *As operações de adição e multiplicação em \mathbb{Q}^+ são comutativas e associativas, vale a lei do corte para a adição e, além disso, a multiplicação é distributiva em relação à adição. Tem-se também que 1 é elemento neutro para a operação de multiplicação e que todo o elemento de \mathbb{Q}^+ tem inverso multiplicativo: $\forall a \in \mathbb{Q}^+ \exists b \in \mathbb{Q}^+ (a \cdot b = 1)$.*

Demonstração. As demonstrações são muito simples, reduzindo-se às propriedades dos números naturais. Vamos apenas verificar que todo o elemento de \mathbb{Q}^+ tem inverso multiplicativo, seja dado $a = \frac{n}{m}$ um elemento arbitrário de \mathbb{Q}^+ . Pondo $b = \frac{m}{n}$ obtém-se o que se quer. \square

É fácil de ver que o inverso multiplicativo dum elemento é único. O inverso multiplicativo de a denota-se por a^{-1} ou, um pouco abusivamente, por $\frac{1}{a}$.

Exercício 10. *Mostre que em \mathbb{Q}^+ se tem a lei do corte para a multiplicação, i.e., para todos $a, b, c \in \mathbb{Q}^+$, $ac = bc \rightarrow a = b$.*

Definição 3. *Dados elementos a e b de \mathbb{Q}^+ , dizemos que $a < b$ se existe $c \in \mathbb{Q}^+$ tal que $a + c = b$.*

Proposição 11. *A relação $<$ em \mathbb{Q}^+ é uma ordem total.*

Demonstração. Mostra-se facilmente o seguinte. Dados $n, m, l, r \in \mathbb{N}^+$, $a = \frac{n}{m}$ e $b = \frac{l}{r}$, tem-se que $a < b$ se, e somente se, $n \cdot r < l \cdot m$. A totalidade da ordem é uma consequência imediata deste facto. \square

Exercício 11. *Dados $a, b, c \in \mathbb{Q}^+$ com $a < b$ mostre que $a + c < b + c$ e $a \cdot c < b \cdot c$.*

Exercício 12. *Dados $a, b \in \mathbb{Q}^+$ com $a < b$, mostre que $b^{-1} < a^{-1}$.*

A seguinte injeção explica por que razão podemos considerar os números naturais não nulos como elementos de \mathbb{Q}^+ .

Proposição 12. *A função $j : \mathbb{N}^+ \mapsto \mathbb{Q}^+$ definida por $j(n) := \frac{n}{1}$ é injectiva e verifica as seguintes propriedades: $j(1) = 1$, $j(n + m) = j(n) + j(m)$, $j(n \cdot m) = j(n) \cdot j(m)$ e $n < m \mapsto j(n) < j(m)$.*

Chapter 5

A insuficiência dos números racionais

Em 1817 Bernard Bolzano propôs-se demonstrar – sem fazer apelo a intuições geométricas – que toda a função contínua, real de variável real, que toma dois valores então toma todos os valores intermédios. Trata-se de um acontecimento importante na História da Matemática pois, para conseguir obter uma tal demonstração, é mister que se articulem logicamente conceitos que, até então, se tomavam como fundamentados em intuições geométricas ou mecânicas (p. ex., a continuidade). Na sua demonstração, Bolzano utiliza uma propriedade que falha em \mathbb{Q}^+ . Trata-se do *princípio do supremo*, que vamos discutir adiante. Nesta medida, os números racionais – ainda que satisfazendo a propriedade da *densidade* (entre dois racionais há sempre um número racional) – são insuficientes para dar conta duma propriedade fundamental que decorre da noção intuitiva do *continuum* da recta. Para ilustrar esta insuficiência, torna-se conveniente trabalhar com os números racionais – positivos, negativos e zero – e não apenas com os positivos. É o que faremos de seguida, assumindo como garantidas algumas propriedades elementares dos números racionais (como veremos no Capítulo 7, não é difícil introduzir o conjunto \mathbb{Q} dos racionais a partir de \mathbb{Q}^+ e demonstrar essas propriedades).

Bolzano foi a primeira pessoa a definir rigorosamente a noção de continuidade. Vamos relembrar esta definição no contexto das funções de \mathbb{Q} para \mathbb{Q} . Uma função $f : \mathbb{Q} \mapsto \mathbb{Q}$ diz-se *contínua no ponto* a , $a \in \mathbb{Q}$, se

$$\forall \varepsilon \in \mathbb{Q}^+ \exists \delta \in \mathbb{Q}^+ \forall x \in \mathbb{Q} (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon).$$

Exercício 13. Mostre que a função $f : \mathbb{Q} \mapsto \mathbb{Q}$ definida por $f(x) = x^2$ é contínua em todos os pontos.

Exercício 14. Mostre que a função $f : \mathbb{Q}^+ \mapsto \mathbb{Q}^+$ definida por $f(x) = x^{-1}$ é contínua em todos os pontos.

Exercício 15. Suponha que a função $f : \mathbb{Q} \mapsto \mathbb{Q}$ é contínua no ponto a . Sejam $a, b \in \mathbb{Q}$ tais que $f(a) < b$. Mostre que existe $\varepsilon \in \mathbb{Q}^+$ tal que, para todo $c \in \mathbb{Q}$ com $|c - a| < \varepsilon$, $f(c) < b$.

O valor da função $x \rightsquigarrow x^2$ no ponto 1 é 1 e no ponto 2 é 4. Porém, a função não toma o valor 2, i.e., não existe um número racional b tal que $b^2 = 2$.

Este resultado já era conhecido dos Pitagóricos, os quais se surpreenderam com o facto da hipotenusa de um triângulo rectângulo isósceles ser incomensurável com os catetos.

Proposição 13. *A equação $x^2 = 2$ não tem solução racional.*

Demonstração. Suponhamos, com vista a um absurdo, que existe um par $m, n \in \mathbb{N}^+$ tal que $m^2 = 2n^2$. Tome-se um par $m, n \in \mathbb{N}^+$ nas condições acima tal que o valor $m + n$ é mínimo. Note-se que $n < m$ e que $m < 2n$. Facilmente se vê que o par $2n - m, m - n$ também satisfaz a igualdade acima. Como a soma destes dois valores é n , isto contradiz a condição de minimalidade do par m, n . \square

O facto da curva $y = x^2$ não intersectar o eixo racional de cota 2, ainda que intersecte os eixos de cota 1 e 4, ilustra a insuficiência dos números racionais para modelar a noção intuitiva de contínuo.

Definição 4. *Diz-se que uma ordem total satisfaz o princípio do supremo se todo o seu subconjunto não vazio e majorado tem supremo.*

Vamos recordar alguns dos conceitos presentes na definição acima. Dado um conjunto X , munido duma ordem parcial \leq , e dado $Y \subseteq X$, diz-se que $m \in X$ é um *majorante* de Y se $\forall y \in Y (y \leq m)$. Diz-se que Y é *majorado* se tiver majorantes. Se o conjunto dos majorantes de Y tem elemento mínimo, a este elemento chama-se o *supremo* de Y , e denota-se por $\sup(Y)$. Numa fórmula:

$$\sup(Y) := \min\{m \in X : m \text{ é majorante de } Y\}.$$

Exercício 16. *Considere-se X um conjunto munido duma ordem parcial \leq . Tome-se $Y \subseteq X$.*

- Mostre que se Y tem máximo então tem supremo (que é o máximo de Y).*
- Dê um exemplo dum subconjunto de \mathbb{Q}^+ sem máximo mas com supremo.*

Exercício 17. *Considere-se X um conjunto munido duma ordem parcial \leq . Tomem-se $Y, Z \subseteq X$ e suponha-se que $\forall y \in Y \exists z \in Z (y \leq z)$. Mostre que se $\sup Y$ e $\sup Z$ existem, então $\sup Y \leq \sup Z$.*

No próximo capítulo vamos construir os números reais positivos \mathbb{R}^+ . Terminamos este capítulo mostrando rigorosamente que em \mathbb{Q}^+ não vale o princípio do supremo. Seja $Y := \{a \in \mathbb{Q}^+ : a^2 < 2\}$. Este conjunto é majorado mas não tem supremo. Com efeito, admitamos por absurdo que Y tem supremo m . Poder-se-á dar o caso de $m^2 < 2$? Neste caso, por continuidade da função $x \rightsquigarrow x^2$ no ponto m , existiria $a \in Y$ tal que $m < a$ (veja-se o exercício 15), o que contradiria o facto de m ser majorante de Y . Poder-se-á dar o caso de $2 < m^2$? Novamente por continuidade da função $x \rightsquigarrow x^2$ no ponto m , haveria $a \in \mathbb{Q}^+$ tal que $a \notin Y$ e $a < m$. Mas, então, concluir-se-ia que a seria um majorante de Y , contradizendo o facto de m ser o mínimo de tais majorantes. Resta a alternativa $m^2 = 2$ que, como vimos, é impossível.

Chapter 6

Cortes de Dedekind

Dado um conjunto A munido duma ordem total $<$, diz-se que um subconjunto X de A é um *segmento inicial* de A se, sempre que $a, b \in A$ com $a < b$ e $b \in X$ então $a \in X$.

Definição 5. Um corte inferior de Dedekind em \mathbb{Q}^+ ou, simplesmente, um corte de Dedekind, é um segmento inicial de \mathbb{Q}^+ , não vazio, majorado e sem máximo. Designa-se por \mathbb{R}^+ o conjunto dos cortes de Dedekind.

Um corte de Dedekind diz-se *racional* se é da forma $\{c \in \mathbb{Q}^+ : c < a\}$, para certo $a \in \mathbb{Q}^+$. Denotamos este corte de Dedekind por $a_{\mathbb{R}^+}$ ou, quando não há confusão, simplesmente usamos também a . Caso o corte de Dedekind não seja desta forma, dizemos que se trata dum corte *irracional*.

Exercício 18. Mostre que um corte de Dedekind X é irracional se, e somente se, X não tem supremo em \mathbb{Q}^+ .

Pelo discutido no capítulo anterior, o conjunto $\{c \in \mathbb{Q}^+ : c^2 < 2\}$ é um corte de Dedekind irracional (denotada, por vezes, por $\sqrt{2}$).

Exercício 19. Seja X um segmento inicial de \mathbb{Q}^+ , não vazio e majorado. Denota-se por \hat{X} o próprio conjunto X se este não tiver máximo; caso contrário, \hat{X} é o conjunto X sem o seu elemento máximo. Mostre que \hat{X} é um corte de Dedekind.

Exercício 20. Seja X um corte de Dedekind.

1. Se $a \in \mathbb{Q}^+ \setminus X$ e $a < b$, então $b \in \mathbb{Q}^+ \setminus X$.
2. Mostre que o conjunto $Y := \{a^{-1} : a \in \mathbb{Q}^+ \setminus X\}$ é um segmento inicial de \mathbb{Q}^+ , não vazio e majorado.
3. Admita que o corte X é irracional. Mostre que Y é um corte de Dedekind.

Proposição 14. Dados X e Y cortes de Dedekind, diz-se que $X < Y$ se X é um subconjunto próprio de Y . A relação de $<$ é uma relação de ordem total entre cortes de Dedekind.

Demonstração. Claramente $<$ é anti-reflexiva e transitiva. Resta ver que é tricotómica. Sejam X e Y cortes de Dedekind distintos. Sem perda de generalidade, seja $a \in X \setminus Y$. Vamos ver que $Y \subseteq X$, o que demonstra o pretendido.

Tome-se $c \in Y$. Visto que $a \notin Y$ e que Y é um corte de Dedekind, conclui-se que não se tem $a \leq c$. Logo $c < a$. Por sua vez, como X é um corte de Dedekind, conclui-se $c \in X$. \square

Proposição 15. *O conjunto dos cortes de Dedekind munido da ordem $<$ satisfaz o princípio do supremo.*

Demonstração. Seja \mathcal{C} um conjunto majorado de cortes de Dedekind. Vamos ver que $\bigcup \mathcal{C} := \{a \in \mathbb{Q}^+ : \exists X \in \mathcal{C} (a \in X)\}$ é um corte de Dedekind. É claro que $\bigcup \mathcal{C}$ é um segmento inicial de \mathbb{Q}^+ que não tem máximo. Por hipótese, existe um corte de Dedekind Z tal que, para todo $X \in \mathcal{C}$ se tem $X \subseteq Z$. Tome-se $b \in \mathbb{Q}^+ \setminus Z$. É claro que todos os elementos de $\bigcup \mathcal{C}$ são majorados por c .

O facto de $\bigcup \mathcal{C}$ ser o supremo de \mathcal{C} é imediato. \square

Exercício 21. *Um subconjunto \mathcal{C} de \mathbb{R}^+ diz-se afastado de zero se existe $I \in \mathbb{R}^+$ tal que, para todo $X \in \mathcal{C}$, $I < X$. Mostre que todo o conjunto, não vazio, afastado de zero tem ínfimo.*

A teoria da ordem dos cortes de Dedekind é muito simples, como vimos. A aritmetização de \mathbb{R}^+ e a sua relação com a ordem requerem, por outro lado, algum trabalho.

Proposição 16. *Sejam X e Y cortes de Dedekind. Definem-se:*

$$X + Y := \{a + b : a \in X \text{ e } b \in Y\}$$

$$X \cdot Y := \{a \cdot b : a \in X \text{ e } b \in Y\}$$

Então $X + Y$ e $X \cdot Y$ são cortes de Dedekind.

Demonstração. É fácil mostrar que $X + Y$ e $X \cdot Y$ são conjuntos não vazios, majorados e sem máximo. Vamos ver que $X + Y$ é um segmento inicial de \mathbb{Q}^+ . Sejam $a \in X$, $b \in Y$ e $c < a + b$. Pretendemos ver que $c \in X + Y$. Dividimos em dois casos. Em primeiro lugar, supomos que $c \in X$. Tome-se $\epsilon \in \mathbb{Q}^+$ com $\epsilon < c$ e $\epsilon \in Y$. Vem $c = c' + \epsilon$, para certo $c' \in \mathbb{Q}^+$. Ora, $c' < c$, donde $c' \in X$. Sai $c \in X + Y$. Agora estudamos o caso em que $c \notin X$. Como $a \in X$, vem $a < c$. Seja d com $a + d = c$. Ora, $a + d = c < a + b$ e, portanto, $d < b$. Sai $d \in Y$. Logo, $c = a + d \in X + Y$. Resta ver que $X \cdot Y$ é segmento inicial de \mathbb{Q}^+ . Sejam $a \in X$, $b \in Y$ e $c < a \cdot b$. Ora, $c = a \cdot (c \cdot a^{-1}) < a \cdot b$. Logo, $c \cdot a^{-1} < b$ e, portanto, $c \cdot a^{-1} \in Y$. Logo $c \in X \cdot Y$. \square

Necessitamos agora do seguinte resultado. Intuitivamente, o resultado afirma que há elementos nos cortes de Dedekind e fora destes tão próximos quanto se queira:

Lema 1. *Sejam X um corte de Dedekind e $\epsilon \in \mathbb{Q}^+$. Então existem $a \in X$ e $b \in \mathbb{Q}^+ \setminus X$ tais que $b < a + \epsilon$.*

Demonstração. Dados X e ϵ nas condições do lema, tome-se $m \in \mathbb{N}^+$ tal que $\frac{1}{m} < \epsilon$ e $\frac{1}{m} \in X$. Considere-se o conjunto dos números naturais positivos k tais que $\frac{k}{m} \notin X$. Como X é majorado, este conjunto é não vazio e, consequentemente, tem elemento mínimo k_0 . Claro que $k_0 = r + 1$, para certo $r \in \mathbb{N}^+$. Tomamos $a = \frac{r}{m}$ e $b = \frac{r+1}{m}$. \square

Exercício 22. Mostre que $\sqrt{2} \cdot \sqrt{2} = 2$.

Estamos em condições de relacionar a ordem com a aritmética:

Proposição 17. *Sejam X e Y cortes de Dedekind. Então*

$$X < Y \Leftrightarrow \exists Z \in \mathbb{R}^+ (X + Z = Y).$$

Demonstração. Suponhamos que $X + Z = Y$. Claramente, $X \subseteq Y$. Resta mostrar que $Y \setminus X \neq \emptyset$. Tome-se $e \in Z$. Pelo Lema 1, existem $b \in X$ e $c \in \mathbb{Q}^+ \setminus X$ tais que $c < b + e$. Vem que $b + e \in X + Z = Y$. Porém, $b + e \notin X$.

Argumentemos a direção contrária. Suponhamos que $X < Y$. Considere-se o conjunto $W := \{a \in \mathbb{Q}^+ : \forall c \in X (c + a \in Y)\}$. Este conjunto é um segmento inicial de \mathbb{Q}^+ , não vazio e majorado. Tome-se Z o corte de Dedekind \bar{W} (ver exercício acima). É óbvio que $X + Z \subseteq Y$. Tome-se agora $b \in Y$, com vista a mostrar que $b \in X + Z$. Dividimos em dois casos: $b \in X$ ou $b \notin X$. Deixamos o primeiro caso ao leitor. Assuma-se, pois, que $b \in Y \setminus X$. Tome-se $b' \in Y$ com $b < b'$ e seja $\epsilon \in \mathbb{Q}^+$ tal que $b' = b + \epsilon$. Pelo Lema 1, existem $d \in X$ e $e \in \mathbb{Q}^+ \setminus X$ tais que $e < d + \epsilon$. Como $d \in X$ e $b \notin X$, vem $d < b$. Então existe $a \in \mathbb{Q}^+$ tal que $b = d + a$. Para terminar com a demonstração basta argumentar que $a \in Z$. Para ver isto, tome-se $c \in X$. Vem:

$$c + a < c + b < (d + \epsilon) + a = (d + a) + \epsilon = b + \epsilon = b' \in Y.$$

Logo, $a \in W$. Como b' não é máximo de Y , conclui-se facilmente que a não é máximo de W . Logo, $a \in Z$. \square

Proposição 18. *As operações de adição e multiplicação em \mathbb{R}^+ são comutativas e associativas, vale a lei do corte para a adição e, além disso, a multiplicação é distributiva em relação à adição. Tem-se também que $1_{\mathbb{R}^+}$ é elemento neutro para a operação de multiplicação e que todo o elemento de \mathbb{R}^+ tem inverso multiplicativo.*

Demonstração. A verificação das propriedades comutativas e associativas é imediata. A lei do corte para a adição é consequência da Proposição 17. Com efeito, suponhamos que $X \neq Y$, com vista a mostrar que $X + Z \neq Y + Z$ (onde X, Y e Z são cortes de Dedekind). Sem perda de generalidade, $X < Y$. Pela Proposição 17, existe um corte de Dedekind W tal que $Y = X + W$. Pelas associatividade e comutatividade da adição sai $Y + Z = (X + Z) + W$. Usando mais uma vez a Proposição 17, conclui-se que $X + Z < Y + Z$ e, portanto, $X + Z \neq Y + Z$.

Vamos agora estudar a propriedade distributiva. Sejam X, Y e Z cortes de Dedekind. É óbvio que $X \cdot (Y + Z) \subseteq (X \cdot Y) + (X \cdot Z)$. A inclusão contrária vê-se do seguinte modo. Tome-se um elemento arbitrário d de $(X \cdot Y) + (X \cdot Z)$. Necessariamente $d = ab + a'c$, com $a, a' \in X, b \in Y$ e $c \in Z$. Sem perda de generalidade, $a' \leq a$. Logo $d \leq ab + ac = a(b + c) \in X \cdot (Y + Z)$. Como $X \cdot (Y + Z)$ é um segmento inicial, sai $d \in X \cdot (Y + Z)$.

Deixa-se como exercício mostrar que $1_{\mathbb{R}^+}$ é elemento neutro para a multiplicação. Finalmente, vamos ver que todo o elemento de \mathbb{R}^+ tem inverso multiplicativo. Seja X um corte de Dedekind. Se X é racional da forma $a_{\mathbb{R}^+}$, com $a \in \mathbb{Q}^+$, então é fácil de ver que $X \cdot Y = 1_{\mathbb{R}^+}$, com $Y := (a^{-1})_{\mathbb{R}^+}$. Consideremos, pois, o caso em que X é um corte irracional. Tome-se $Y := \{a^{-1} : a \in \mathbb{Q}^+ \setminus X\}$.

Sabemos que Y é um corte de Dedekind e, claramente, $X \cdot Y \subseteq 1_{\mathbb{R}^+}$ (se $a \in X$ e $b \notin X$ vem $a < b$ e, portanto, $ab^{-1} < 1$). Tem-se mais trabalho em mostrar que $1_{\mathbb{R}^+} \subseteq X \cdot Y$. Com vista a isto, seja dado $c \in 1_{\mathbb{R}^+}$, i.e., seja dado um racional positivo c tal que $c < 1$. Queremos encontrar $a \in X$ e $b \in \mathbb{Q}^+ \setminus X$ tais que $c < ab^{-1}$. Fixe-se $a_0 \in X$. Seja $\delta \in \mathbb{Q}^+$ tal que $1 = c + \delta$ e tome-se $\epsilon := c^{-1}\delta a_0$. Pelo Lema 1, existem elementos $a \in X$ e $b \in \mathbb{Q}^+ \setminus X$ tais que $b < a + \epsilon$. É claro que podemos supor que $a_0 \leq a$. Vamos ver que $cb < a$, o que mostra o pretendido. Ora:

$$cb < c(a + \epsilon) = ca + c\epsilon = ca + \delta a_0 \leq ca + \delta a = (c + \delta)a = a. \quad \square$$

Exercício 23. Mostre que em \mathbb{R}^+ se tem a lei do corte para a multiplicação.

Exercício 24. Sejam X, Y e Z cortes de Dedekind com $X < Y$. Então $X + Z < Y + Z$ e $X \cdot Z < Y \cdot Z$.

A seguinte injeção explica por que razão podemos considerar os números racionais positivos como elementos de \mathbb{R}^+ .

Proposição 19. A função $j : \mathbb{Q}^+ \mapsto \mathbb{R}^+$ definida por $j(a) := a_{\mathbb{R}^+}$ é injectiva e verifica as seguintes propriedades: $j(1) = 1$, $j(a + b) = j(a) + j(b)$, $j(a \cdot b) = j(a) \cdot j(b)$ e $a < b \rightarrow j(a) < j(b)$.

Chapter 7

Números reais

Tendo introduzido os números reais positivos através dos cortes de Dedekind, vamos neste capítulo definir todos os reais. A forma como o vamos fazer também se poderia aplicar para definir os inteiros \mathbb{Z} a partir dos naturais positivos \mathbb{N}^+ , ou para definir os racionais \mathbb{Q} a partir dos racionais positivos \mathbb{Q}^+ .

Proposição 20. *Considere-se a relação binária em $\mathbb{R}^+ \times \mathbb{R}^+$ definida por $(X, Y) \sim (W, Z)$ se, e somente se, $X + Z = W + Y$. Esta relação é uma relação de equivalência.*

Demonstração. Deixamos as propriedades reflexiva e simétrica como exercício. Para demonstrar a propriedade transitiva, admita-se que $(X, Y) \sim (W, Z)$ e $(W, Z) \sim (U, V)$. Então, $X + Z = W + Y$ e $W + V = U + Z$. Somando ambos os membros de cada equação ficamos com $X + Z + W + V = W + Y + U + Z$. Utilizando a propriedade comutativa e a lei do corte podemos concluir que $X + V = U + Y$, i.e., $(X, Y) \sim (U, V)$. \square

O conjunto \mathbb{R} dos números reais é, por definição, o conjunto $\mathbb{R}^+ \times \mathbb{R}^+ / \sim$ das classes de equivalência da relação \sim . A classe dum par (X, Y) , com X e Y cortes de Dedekind, denota-se por $[(X, Y)]_\sim$ ou, simplesmente, por $[(X, Y)]$. Intuitivamente, $[(X, Y)]$ representa o número real $X - Y$. Distinguímos dois elementos em \mathbb{R} : o elemento $0_{\mathbb{R}} := [(1, 1)]$ e o elemento $1_{\mathbb{R}} := [(2, 1)]$.

Exercício 25. *Mostre que $0_{\mathbb{R}} = \{(X, X) : X \in \mathbb{R}^+\}$. Determine o conjunto $1_{\mathbb{R}}$.*

Em \mathbb{R} podemos definimos as operações de adição e multiplicação assim:

$$[(X, Y)] + [(W, Z)] := [(X + W, Y + Z)] \text{ e,}$$

$$[(X, Y)] \cdot [(W, Z)] := [(XW + YZ, XZ + YW)].$$

Observe-se que estamos a definir estas operações em \mathbb{R} à custa das operações em \mathbb{R}^+ . Claro que temos que verificar que as receitas acima definem, de facto, operações em \mathbb{R} . Mais precisamente, temos que verificar que se $(X, Y) \sim (X', Y')$ e $(W, Z) \sim (W', Z')$ então $(X + W, Y + Z) \sim (X' + W', Y' + Z')$ e $(XW + YZ, XZ + YW) \sim (X'W' + Y'Z', X'Z' + Y'W')$. Vamos verificar o caso da multiplicação (o caso da adição é muito simples). Para este caso, facilita mostrar que $(XW + YZ, XZ + YW) \sim (X'W + Y'Z, X'Z + Y'W)$ e que $(X'W + Y'Z, X'Z + Y'W) \sim (X'Z' + Y'Z', X'Z' + Y'W')$. Por transitividade, conclui-se o pretendido. Ora,

$$XW + YZ + X'Z + Y'W = W(X + Y') + Z(Y + X') \text{ e,}$$

$$X'W + Y'Z + XZ + YW = W(X' + Y) + Z(Y' + X).$$

Como, por hipótese, $X + Y' = X' + Y$ sai a primeira equivalência. A outra equivalência é análoga.

Para tornar a notação mais simples vamos, a partir de agora, omitir por vezes o subscrito \mathbb{R} dos elementos $0_{\mathbb{R}}$ e $1_{\mathbb{R}}$. Pelo contexto será claro de que 0 ou 1 se trata.

Proposição 21. *O conjunto \mathbb{R} com os elementos 0 e 1, munido das operações de adição e multiplicação, é um corpo, i.e.:*

1. $\forall x, y, z ((x + y) + z = x + (y + z)).$
2. $\forall x (x + 0 = x).$
3. $\forall x \exists y (x + y = 0).$
4. $\forall x, y (x + y = y + x).$
5. $\forall x, y, z (x \cdot (y \cdot z) = (x \cdot y) \cdot z).$
6. $\forall x (x \cdot 1 = x).$
7. $\forall x, y (x \cdot y = y \cdot x).$
8. $\forall x, y, z (x \cdot (y + z) = x \cdot y + x \cdot z).$
9. $0 \neq 1.$
10. $\forall x (x \neq 0 \rightarrow \exists y (x \cdot y = 1)).$

Demonstração. As demonstrações são simples e deixamo-las como exercícios. Vamos apenas verificar (3), (6) e (10). Seja dado $x = [(X, Y)]$ um elemento arbitrário de \mathbb{R} . É claro que $[(X, Y)] + [(Y, X)] = [(X + Y, Y + X)] = [(0, 0)] = 0_{\mathbb{R}}$. Quanto a (6), dado $x = [(X, Y)]$, note-se que $x \cdot 1 = [(X, Y)] \cdot [(2, 1)] = [(2X + Y, X + 2Y)] = [(X, Y)] = x$. Vamos agora verificar (10). Suponhamos que $x = [(X, Y)]$, $x \neq 0_{\mathbb{R}}$. Então, ou $X < Y$ ou $Y < X$. Suponhamos que se tem o primeiro caso (o segundo é similar). Neste caso, existe um corte de Dedekind Z tal que $Y = X + Z$. Tome-se um corte de Dedekind W tal que $Z \cdot W = 1$ e defina-se $y := [(1, W + 1)]$ Não é difícil de verificar que $x \cdot y = 1$. \square

Dadas as propriedades acima, podemos, de ora em diante, utilizar todas as definições e propriedades da teoria dos corpos. Por exemplo, todo $x \in \mathbb{R}$ tem um único elemento *simétrico*, que se denota por $-x$. Igualmente, dados $x, y \in \mathbb{R}$, $y - x$ denota o real $y + (-x)$.

De seguida vamos introduzir a ordem nos números reais. Sejam X e Y cortes de Dedekind. O número real $[(X, Y)]$ diz-se *positivo* se $Y < X$. Deixa-se ao cuidado verificar a correcção desta definição. O seguinte lema é útil:

Lema 2. *Têm-se as seguintes propriedades:*

- a. $0_{\mathbb{R}}$ não é um numero real positivo.
- b. Se x é um real não nulo, então ou x é positivo ou $-x$ é positivo.

c. Se x e y são reais positivos, então também o são $x + y$ e $x \cdot y$.

Demonstração. A primeira alínea é imediata e a segunda decorre da observação de que $-[(X, Y)] = [(Y, X)]$ (e da tricotomia entre cortes de Dedekind). Admitamos que $x = [(X, Y)]$ e $y = [(W, Z)]$ são números reais positivos. Vê-se facilmente que $x + y$ também é positivo. Estudemos a multiplicação. Por hipótese, $Y < X$ e $Z < W$. Pela Proposição 17, existem $U, V \in \mathbb{R}^+$ tais que $X = Y + U$ e $W = Z + V$. Observe-se que $x \cdot y = [(XW + YZ, XZ + YW)]$ e que:

$$XW + YZ = (Y + U)(Z + V) + YZ = YZ + YV + UZ + UV + YZ \text{ e}$$

$$XZ + YW = (Y + U)Z + Y(Z + V) = YZ + UZ + YZ + YV.$$

Usando a Proposição 17, sai imediatamente que $XZ + YW < XW + YZ$, i.e., que o número real $x \cdot y$ é positivo. \square

Proposição 22. Diz-se que o número real x é menor do que o número real y (escreve-se $x < y$) se $y - x$ é um número real positivo. A relação binária $<$ entre números reais é uma relação de ordem total e, além disso, tem as seguintes propriedades:

11. $\forall x, y, z (y < z \rightarrow x + y < x + z)$.

12. $\forall x, y, z (y < z \wedge 0 < x \rightarrow xy < xz)$.

Demonstração. O facto da relação binária ser uma ordem total sai imediatamente do lema anterior: (a) justifica a anti-reflexividade; (c) a transitividade e (b) a tricotomia. A primeira alínea acima é trivial enquanto que a outra é consequência de (c). \square

Um corpo munido duma ordem total que verifique as propriedades (11) e (12) denomina-se de *corpo ordenado*.

Exercício 26. Mostre que num corpo ordenado se têm as seguintes propriedades:

1. $x \neq 0 \rightarrow 0 < x^2$ e $0 < 1$.

2. $0 < x \wedge y < 0 \rightarrow xy < 0$ e $x < 0 \wedge y < 0 \rightarrow 0 < xy$.

3. $0 < x \rightarrow 0 < x^{-1}$ e $x < 0 \rightarrow x^{-1} < 0$.

4. $0 < x < y \rightarrow y^{-1} < x^{-1}$.

Teorema 1 (Números reais). *O corpo ordenado dos reais satisfaz o princípio do supremo.*

Demonstração. Verifica-se facilmente que a função $k : \mathbb{R}^+ \mapsto \mathbb{R}$ dada por $X \rightsquigarrow [(X + 1, 1)]$ preserva a ordem. Além disso, a imagem de k é constituída exactamente pelos números reais positivos. Assim, k é um isomorfismo de ordem entre \mathbb{R}^+ e os reais positivos. Note-se que os restantes reais ou são o elemento $0_{\mathbb{R}}$ ou são menores do que $0_{\mathbb{R}}$ (os denominados reais *negativos*).

Se S é um conjunto de reais positivos, o supremo existe por causa do isomorfismo de ordem k e da Proposição 15. Se S tem números reais positivos, este caso reduz-se facilmente ao anterior. Se S não tem números positivos tem-se

um de dois casos. Ou $0_{\mathbb{R}}$ é o supremo de S , ou não. No segundo caso, é fácil de ver que o conjunto $\{-x : x \in S\}$ tem apenas números reais positivos e que a sua imagem por k está afastada de zero. Logo, pelo exercício 21 esta imagem tem ínfimo. Assim, $\{-x : x \in S\}$ também tem ínfimo, digamos u . É fácil de verificar que $-u$ é o supremo de S . \square

O seguinte exercício permite ver \mathbb{R}^+ como subconjunto de \mathbb{R} :

Exercício 27. *Mostre que a função k definida na demonstração do teorema anterior verifica as seguintes propriedades: $k(1) = 1$, $k(n + m) = k(n) + k(m)$ e $k(n \cdot m) = k(n) \cdot k(m)$.*

Terminamos este capítulo com a demonstração do teorema do valor intermédio de Bolzano. Recorde-se que uma função real f definida no intervalo real fechado $[0, 1]$ é contínua em todos os pontos se

$$\forall a \in [0, 1] \forall \varepsilon \in \mathbb{R}^+ \exists \delta \in \mathbb{R}^+ \forall x \in [0, 1] (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon).$$

Teorema 2 (Valor intermédio). *Toda a função contínua $f : [0, 1] \mapsto \mathbb{R}$ tal que $f(0) < 0$ e $f(1) > 0$ tem um valor em que se anula.*

Demonstração. Considere-se $X := \{x \in [0, 1] : f(x) < 0\}$. Este conjunto é não vazio e majorado. Logo, tem supremo a . Se $f(a) < 0$ então $a < 1$ e, pela continuidade de f em a , tem-se $f(x) < 0$ numa vizinhança de a . Em particular, $f(x) < 0$ para valores x com $x > a$. Isto contradiz o facto de a ser majorante de X . Se $f(a) > 0$ então $0 < a$ e, pela continuidade de f em a , ter-se-ia também $f(x) > 0$ numa vizinhança de a . Daqui conclui-se que a não é o mínimo dos majorantes de X . Portanto, $f(a) = 0$. \square

Exercício 28. *Seja $(x_n)_{n \in \mathbb{N}}$ uma sucessão crescente (i.e., $n \leq m \rightarrow x_n \leq x_m$) e majorada de números reais. Mostre que o conjunto $\{x_n : n \in \mathbb{N}\}$ tem supremo e a sucessão $(x_n)_{n \in \mathbb{N}}$ converge para esse supremo.*

Exercício 29. *Seja $([a_n, b_n])_{n \in \mathbb{N}}$ uma sucessão de intervalos encaixados de números reais (i.e., $[a_{n+1}, b_{n+1}] \subseteq [a_n, b_n]$ para todo $n \in \mathbb{N}$). Seja $a = \sup_{n \in \mathbb{N}} a_n$ e $b = \inf_{n \in \mathbb{N}} b_n$. Mostre que $a \leq b$ e que $\bigcap_{n \in \mathbb{N}} [a_n, b_n] = [a, b]$. Mostre que se $\lim_n (b_n - a_n) = 0$, então a intersecção dos intervalos encaixados reduz-se a um ponto (este é o chamado Princípio do Encaixe).*

Chapter 8

A unicidade dos números reais

Em teoria dos corpos, dado $n \in \mathbb{N}$ e x um elemento dum corpo K podemos considerar informalmente o elemento

$$\underbrace{x + x + \dots + x}_{n \text{ vezes}}$$

do corpo K , denotado provisoriamente por $n \bullet x$ (convencionou-se que $0 \bullet x$ é 0_K , o elemento zero do corpo). Rigorosamente, fixa-se x um elemento do corpo em causa e efectua-se uma definição por recursão em que, no teorema da recursão de Dedekind, X é K , $f : X \mapsto X$ está definida por $f(w) = w + x$ e a é 0_K . Fica, pois:

- i. $0 \bullet x = 0_K$.
- ii. $(n + 1) \bullet x = (n \bullet x) + x$.

Exercício 30. Dado um corpo K e $x \in K$ mostre que, para todos $n, m \in \mathbb{N}$, se tem $(m + n) \bullet x = (m \bullet x) + (n \bullet x)$ e que $m \bullet (n \bullet x) = (m \cdot n) \bullet x$.

A função $(n, x) \rightsquigarrow n \bullet x$ não é uma operação do corpo, visto que n não tem que ser elemento do corpo em questão. As propriedades do exercício acima não se podem, com correcção, denominar de propriedades distributiva e associativa. O mesmo se passa com as seguintes propriedades:

Exercício 31. Dados x, y elementos dum corpo mostre que, para todo $n \in \mathbb{N}$, se tem $n \bullet (x + y) = (n \bullet x) + (n \bullet y)$ e $n \bullet (x \cdot y) = (n \bullet x) \cdot y$.

A correspondência \bullet generaliza-se facilmente aos números inteiros negativos: se n é um inteiro negativo, define-se $n \bullet x$ como sendo $-((-n) \bullet x)$.

Exercício 32. Mostre que num corpo ordenado K se tem, para todo $n \in \mathbb{N}^+$, $0_K < n \bullet 1_K$.

O exercício acima mostra, em particular, que $n \bullet 1_K \neq 0_K$ para $n \in \mathbb{N}^+$. Um corpo K nestas condições diz-se que tem *característica zero* (é esta a infeliz terminologia em vigor – há quem, com mais propriedade, diga que a característica é *infinita*). Mostrámos, pois, que todo o corpo ordenado tem característica zero.

Em corpos K de característica zero, podemos mesmo estender a correspondência \bullet a todos os números racionais. Dado um número racional $\frac{n}{m}$ ($n \in \mathbb{Z}$, $m \in \mathbb{N}^+$) e um elemento $x \in K$, denotamos por $\frac{n}{m} \bullet x$ o elemento $(n \bullet x)(m \bullet 1_K)^{-1}$. De ora em diante escrevemos simplesmente $\frac{n}{m}x$. Deixamos como exercício mostrar que esta operação está bem definida.

Proposição 23. *Seja K um corpo de característica zero. Então a função de \mathbb{Q} para K dada por $\frac{n}{m} \rightsquigarrow \frac{n}{m}1_K$ é um monomorfismo de corpos.*

A demonstração é simples. Observe que esta proposição permite ver o corpo \mathbb{Q} como subcorpo – de facto o mais pequeno subcorpo – dum corpo K de característica zero (diz-se que \mathbb{Q} é o *corpo primo* de K). Aos elementos de K da forma $\frac{n}{m}1_K$, com $n \in \mathbb{Z}$ e $m \in \mathbb{N}^+$, chamamos os *racionais* de K . Também se denotam estes elementos por $\frac{n}{m}$.

Definição (Propriedade Arquimediana). *Um corpo ordenado K diz-se Arquimediano se, para todo $x \in K$, existe $m \in \mathbb{N}^+$ tal que $x < m$.*

Proposição 24. *Todo o corpo ordenado que satisfaz o princípio do supremo é Arquimediano.*

Demonstração. Seja K um corpo nas condições da proposição. Vamos ver que se x é majorante de \mathbb{N}^+ então $x - 1$ também o é. Com efeito, se $x - 1$ não é majorante de \mathbb{N}^+ , então existe $n \in \mathbb{N}^+$ tal que $x - 1 < n$. Sai, $x < n + 1$ o que mostra que x também não é majorante de \mathbb{N}^+ . Desta discussão conclui-se que se \mathbb{N}^+ é majorado então não tem supremo. Como K satisfaz o princípio do supremo, conclui-se que \mathbb{N}^+ não é majorado.

Seja agora $x \in K$. Então x não majora \mathbb{N}^+ . Por tricotomia, existe $m \in \mathbb{N}^+$ tal que $x < m$. Como se queria. \square

Lema 3. *Num corpo ordenado Arquimediano há sempre números racionais estritamente entre elementos distintos.*

Demonstração. Como observação preliminar note-se que para todo o elemento positivo w dum corpo ordenado Arquimediano K , existe $n \in \mathbb{N}^+$ tal que $0_K < \frac{1}{n} < w$. Isto sai imediatamente do facto de existir $n \in \mathbb{N}^+$ tal que $w^{-1} < n$.

Sejam x e y elementos dum corpo ordenado K com $x < y$. Podemos supor, sem perda de generalidade, que $x > 0$. Visto que $y - x > 0$, tome-se $m \in \mathbb{N}^+$ tal que $\frac{1}{m} < y - x$. Pela propriedade Arquimediana, seja $n \in \mathbb{N}^+$ mínimo tal que $mx < n$. Logo, $n - 1 \leq mx$. Por um lado sai $x < \frac{n}{m}$. Por outro, $\frac{n}{m} \leq x + \frac{1}{m} < x + (y - x) = y$. Como se queria. \square

Exercício 33. *Seja K um corpo ordenado e A e B subconjuntos de K . Suponha que $\sup A$ e $\sup B$ existem.*

1. *Seja $A + B := \{x + y : x \in A \wedge y \in B\}$. Mostre que $\sup(A + B)$ existe e que é igual a $\sup A + \sup B$.*
2. *Suponha que A e B apenas têm elementos positivos. Defina-se $A \cdot B := \{x \cdot y : x \in A \wedge y \in B\}$. Mostre que $\sup(A \cdot B)$ existe e é igual a $\sup A \cdot \sup B$.*

Estamos preparados para demonstrar o seguinte resultado fundamental:

Teorema (Unicidade dos reais). *Dois corpos ordenados que satisfaçam o princípio do supremo são isomorfos, i.e., existe uma bijecção entre eles que preserva a estrutura de corpo ordenado. Além disso o isomorfismo é único.*

Demonstração. Seja K um corpo ordenado que satisfaz o princípio do supremo. Vamos ver que \mathbb{R}^+ e K^+ são isomorfos (K^+ é o conjunto dos elementos positivos de K). Para ver isso, considere-se a aplicação $\phi : \mathbb{R}^+ \mapsto K^+$ definida por $X \rightsquigarrow \sup\{q \cdot 1_K : q \in X\}$. Note-se que, dado X um corte de Dedekind, o supremo anterior faz sentido, pois trata-se do supremo dum conjunto majorado em K . É óbvio que ϕ é injectiva. Seja dado $x \in K^+$. Considere-se $X := \{q \in \mathbb{Q}^+ : q \cdot 1_K < x\}$. É fácil de ver que X é um segmento inicial de \mathbb{Q}^+ . Pela propriedade Arquimediana de K , X é majorado e não vazio. Pelo Lema 3, sai que este segmento não tem máximo. Logo, X é um corte de Dedekind. Vamos ver que $\phi(X) = x$, ou seja, que $\sup\{q \cdot 1_K : q \in X\} = x$. Claro que o primeiro elemento não excede o segundo. Suponhamos, com vista a um absurdo, que $\sup\{q \cdot 1_K : q \in X\} = y < x$. Pelo Lema 3, existe $r \in \mathbb{Q}^+$ tal que $y < r \cdot 1_K < x$. Logo, $r \in X$. Isto dá origem a uma contradição.

Sejam X e Y cortes de Dedekind. É fácil de ver que se $X < Y$ então $\phi(X) < \phi(Y)$. Usando o exercício anterior, tem-se:

$$\begin{aligned} \phi(X + Y) &= \sup\{q \cdot 1_K + r \cdot 1_K : q \in X \wedge r \in Y\} = \\ &= \sup\{q \cdot 1_K : q \in X\} + \sup\{r \cdot 1_K : r \in Y\} = \phi(X) + \phi(Y). \end{aligned}$$

Vê-se, de modo análogo, que $\phi(X \cdot Y) = \phi(X) \cdot \phi(Y)$. Claramente, ϕ estende-se a um isomorfismo entre \mathbb{R} e K .

Deixamos a unicidade do isomorfismo ao cuidado do leitor. □

Chapter 9

Equipotência

Definição 6. *Dois conjuntos X e Y dizem-se equipotentes ou equinúmericos e escreve-se $X =_c Y$ se existir uma função $f : X \mapsto Y$ bijectiva.*

Nas condições acima também se diz que X e Y têm a mesma *cardinalidade*. Um exemplo importante de equipotência é o seguinte. Dados conjuntos X e Y denota-se por Y^X o conjunto de todas as funções de X para Y . Em particular, $\{0, 1\}^X$ é o conjunto de todas as funções de X para o conjunto $\{0, 1\}$. O conjunto de todos os subconjuntos de X , também chamado o conjunto das partes de X e denotado por $\mathcal{P}(X)$ é equipotente a $\{0, 1\}^X$ via a bijecção que a cada $Z \subseteq X$ faz corresponder a sua *função característica* $\chi_Z : X \mapsto \{0, 1\}$:

$$\chi_Z(x) := \begin{cases} 1 & \text{se } x \in Z \\ 0 & \text{se } x \notin Z \end{cases}$$

O seguinte resultado é óbvio:

Proposição 25. *Para todos os conjuntos X, Y e Z tem-se:*

- (a) $X =_c X$;
- (b) $X =_c Y \rightarrow Y =_c X$;
- (c) $X =_c Y \wedge Y =_c Z \rightarrow X =_c Z$.

Definição 7. *Diz-se que um conjunto X tem cardinalidade menor ou igual que Y , e escreve-se $X \leq_c Y$, se existir uma injeção de X para Y . Diz-se que X tem cardinalidade estritamente menor que Y , e escreve-se $X <_c Y$, se $X \leq_c Y$ e X não é equipotente a Y .*

Exercício 34. *Mostre que, para todo o conjunto X , $X \leq_c \mathcal{P}(X)$.*

Os dois resultados seguintes são claros:

Proposição 26. *Sejam dados conjuntos X e Y . Tem-se que $X \leq_c Y$ se, e somente se, existe um subconjunto Z de Y equipotente a X .*

Proposição 27. *Para todos os conjuntos X, Y e Z tem-se:*

- (a) $X \leq_c X$;

$$(b) X \leq_c Y \wedge Y \leq_c Z \rightarrow X \leq_c Z.$$

Segue-se um teorema importante e de demonstração não trivial:

Teorema de Cantor-Schröder-Bernstein. *Sejam dados conjuntos X e Y . Se $X \leq_c Y$ e $Y \leq_c X$ então $X =_c Y$.*

Demonstração. Sejam $f : X \mapsto Y$ e $g : Y \mapsto X$ injecções. Definem-se, por recursão, subconjuntos X_n de X e subconjuntos Y_n de Y da seguinte forma: por um lado, $X_0 = X$, $X_{n+1} = g[f[X_n]]$; por outro lado, $Y_0 = Y$ e $Y_{n+1} = f[g[Y_n]]$. Tem-se:

$$X_n \supseteq g[Y_n] \supseteq X_{n+1} \quad \text{e} \quad Y_n \supseteq f[X_n] \supseteq Y_{n+1},$$

para todo o número natural n . As propriedades acima mostram-se, cada qual, por indução. Consideremos a primeira propriedade. O caso base é claro. Quanto ao passo de indução, observe-se que, por hipótese de indução, se infere $X_{n+2} = g[f[X_{n+1}]] \subseteq g[f[g[Y_n]]] = g[Y_{n+1}]$ e $g[Y_{n+1}] = g[f[g[Y_n]]] \subseteq g[f[X_n]] = X_{n+1}$. A segunda propriedade verifica-se analogamente. Temos, pois, as seguintes inclusões:

$$X_0 \supseteq g[Y_0] \supseteq X_1 \supseteq g[Y_1] \supseteq X_2 \supseteq g[Y_2] \supseteq X_3 \dots \quad \text{e}$$

$$Y_0 \supseteq f[X_0] \supseteq Y_1 \supseteq f[X_1] \supseteq Y_2 \supseteq f[X_2] \supseteq Y_3 \dots$$

Definem-se as intersecções: $X^\infty := \bigcap_{n \in \mathbb{N}} X_n$ e $Y^\infty := \bigcap_{n \in \mathbb{N}} Y_n$. Ora:

$$Y^\infty = \bigcap_{n \in \mathbb{N}} Y_n \supseteq \bigcap_{n \in \mathbb{N}} f[X_n] \supseteq \bigcap_{n \in \mathbb{N}} Y_{n+1} = Y^\infty.$$

Logo, $\bigcap_{n \in \mathbb{N}} f[X_n] = Y^\infty$. Dado que f é injectiva, $f[X^\infty] = f[\bigcap_{n \in \mathbb{N}} X_n] = \bigcap_{n \in \mathbb{N}} f[X_n] = Y^\infty$. Assim, a função $f|_{X^\infty}$ é uma bijecção de X^∞ sobre Y^∞ . Agora, para obter uma bijecção entre X e Y , basta arranjar uma bijecção entre $X \setminus X^\infty$ e $Y \setminus Y^\infty$. Tem-se:

$$X \setminus X^\infty = (X_0 \setminus g[Y_0]) \cup (g[Y_0] \setminus X_1) \cup (X_1 \setminus g[Y_1]) \cup (g[Y_1] \setminus X_2) \cup \dots \quad \text{e}$$

$$Y \setminus Y^\infty = (Y_0 \setminus f[X_0]) \cup (f[X_0] \setminus Y_1) \cup (Y_1 \setminus f[X_1]) \cup (f[X_1] \setminus Y_2) \cup \dots$$

em que estas uniões são mutuamente disjuntas. Logo, se fizermos corresponder biunivocamente as ‘parcelas’ da primeira união às da segunda união de modo que ‘parcelas’ em correspondência sejam equipotentes, temos o resultado desejado. À ‘parcela’ $X_n \setminus g[Y_n]$ da união de cima fazemos corresponder a ‘parcela’ $f[X_n] \setminus Y_{n+1}$ da união de baixo; por outro lado, à ‘parcela’ $g[Y_n] \setminus X_{n+1}$ da união de cima fazemos corresponder a ‘parcela’ $Y_n \setminus f[X_n]$ da união de baixo. Pela injectividade de f , $f[X_n \setminus g[Y_n]] = f[X_n] \setminus f[g[Y_n]] = f[X_n] \setminus Y_{n+1}$. Por outro lado, pela injectividade de g , $g[Y_n \setminus f[X_n]] = g[Y_n] \setminus g[f[X_n]] = g[Y_n] \setminus X_{n+1}$. Assim, $X_n \setminus g[Y_n] =_c f[X_n] \setminus Y_{n+1}$ e $g[Y_n] \setminus X_{n+1} =_c Y_n \setminus f[X_n]$. \square

Exercício 35. *Mostre que se $X <_c Y$ e $Y <_c Z$ então $X <_c Z$.*

O seguinte resultado fornece uma caracterização alternativa da existência de injecções:

Proposição 28. *Sejam dados conjuntos X e Y com $X \neq \emptyset$. Então, $X \leq_c Y$ se, e somente se, existe uma sobrejecção de Y para X .*

Demonstração. Seja $X \neq \emptyset$ e $f : X \mapsto Y$ uma injecção. Fixe-se $x_0 \in X$. Defina-se $g : Y \mapsto X$ da seguinte forma:

$$g(y) := \begin{cases} x & \text{se } f(x) = y \\ x_0 & \text{se não existe } x \in X \text{ tal que } f(x) = y \end{cases}$$

Note-se que g está bem definida pois, dado $y \in Y$, a existir $x \in X$ tal que $f(x) = y$ este valor x é, por injectividade, único. Claramente, g é uma sobrejecção.

Reciprocamente, seja $g : Y \mapsto X$ uma sobrejecção. Então, para cada $x \in X$ existe pelo menos um elemento $y \in Y$ tal que $g(y) = x$. Escolha-se para $f(x)$ um tal elemento (i.e., $f(x)$ é escolhido de modo a que $g(f(x)) = x$). Vamos ver que $f : X \mapsto Y$ definido desta maneira é uma injecção. Com efeito, se $f(x) = f(x')$ então $x = g(f(x)) = g(f(x')) = x'$. \square

O modo como se escreveu a segunda parte do argumento anterior esconde um princípio fundamental que deve ser explicitado. Trata-se do *axioma da escolha*. Podemos formular este axioma da seguinte maneira: Dado um conjunto X existe uma função $\epsilon_X : \mathcal{P}(X) \setminus \{\emptyset\} \mapsto X$ tal que, para todo o subconjunto não vazio Z de X , se tem $\epsilon_X(Z) \in Z$. Ou seja, a função ϵ_X , que se diz uma *função de escolha* para X , “escolhe” um elemento de cada subconjunto não vazio de X . Destarte, no argumento acima, fixa-se uma função escolha ϵ_Y para Y e define-se $f(x) := \epsilon_Y(\{y \in Y : g(y) = x\})$.

Exercício 36. *Não é necessário apelar ao axioma da escolha para obter uma função escolha para \mathbb{N} . Porquê?*

O axioma da escolha é hoje comunmente aceite como fazendo parte da axiomática da teoria dos conjuntos mas, historicamente, levantou bastantes objecções por causa do seu carácter não construtivo. Com efeito, o axioma postula simplesmente a existência de funções escolhas. Como iremos ver mais tarde, o *teorema da comparabilidade das cardinalidades* pode demonstrar-se com a ajuda do axioma da escolha (de facto, é-lhe equivalente). O teorema diz o seguinte: Dados conjuntos X e Y , tem-se $X \leq_c Y$ ou $Y \leq_c X$.

No que se segue, chamaremos frequentemente a atenção para resultados cujas demonstrações façam uso do axioma da escolha.

Chapter 10

Finitude e infinitude

Dado n um número natural, denota-se por $[n]$ o conjunto $\{i \in \mathbb{N} : i < n\}$. Note que $[0] = \emptyset$.

Definição 8. Um conjunto X diz-se finito se existir $n \in \mathbb{N}$ tal que $X =_c [n]$. Caso contrário, diz-se que X é infinito.

Comumente, quando consideramos um conjunto finito tomamo-lo da forma $\{a_0, a_1, \dots, a_{n-1}\}$, para certo $n \in \mathbb{N}$. Sob o entendimento de que não há repetições, isto significa que a função $k \rightsquigarrow a_k$ é uma bijecção de $[n]$ para o conjunto em causa.

Lema 4. Sejam $n, m \in \mathbb{N}$ e $f : [n] \mapsto [m]$ uma injeção não sobrejectiva. Então $m \neq 0$ e existe uma injeção de $[n]$ para $[m-1]$.

Demonstração. Claro que $m \neq 0$. Se $m-1 \notin \text{im} f$ não há nada a demonstrar. Caso contrário, tome-se $r \in [n]$ com $f(r) = m-1$. Dado que f não é sobrejectiva, tome-se $k \in [m]$ com $k \notin \text{im} f$. Faz-se uma troca, definindo $g : [n] \mapsto [m-1]$ da seguinte forma:

$$g(x) := \begin{cases} f(x) & \text{se } x \neq r \\ k & \text{se } x = r \end{cases}$$

É claro que g está nas condições pretendidas. □

Proposição 29. Sejam $n, m \in \mathbb{N}$ com $m < n$. Não há injeções de $[n]$ para $[m]$.

Demonstração. Suponhamos, com vista a um absurdo, que existem números naturais n, m com $m < n$ e uma função injectiva $f : [n] \mapsto [m]$. Pelo princípio do mínimo, tome-se n_0 o menor natural com a propriedade acima. Claro que $n_0 \neq 0$. Ora, $f \upharpoonright_{[n_0-1]}$ é uma injeção de $[n_0-1]$ para $[m]$ que não é sobrejectiva, pois $f(n_0-1) \notin \text{im} f \upharpoonright_{[n_0-1]}$. Pelo Lema 4, $m \neq 0$ e existe uma injeção de $[n_0-1]$ em $[m-1]$. Note que $m-1 < n_0-1$. Isto contradiz a minimalidade de n_0 . □

Corolário 2. Para $n, m \in \mathbb{N}$ tem-se:

- (a) $m = n$ se, e somente se, $[m] =_c [n]$.

(b) $m \leq n$ se, e somente se, $[m] \leq_c [n]$.

A alínea (a) acima permite associar a cada conjunto finito X o único número natural n cujo conjunto associado $[n]$ é equipotente a X . Chama-se a este n a *cardinalidade* de X e escreve-se $\text{card}(X) = n$.

É trivial mostrar que se X é um conjunto finito de cardinalidade n e se $w \notin X$, então $X \cup \{w\}$ também é finito e tem cardinalidade $n + 1$.

Proposição 30. *Um subconjunto dum conjunto finito ainda é finito e de cardinalidade menor ou igual a este.*

Demonstração. Seja $n \in \mathbb{N}$ e $X \subseteq [n]$. Basta mostrar que X é finito e de cardinalidade menor ou igual a n . Este resultado demonstra-se facilmente por indução em n . O caso $n = 0$ é óbvio. Admitamos que $X \subseteq [n + 1]$. Então, $X \setminus \{n\} \subseteq [n]$. Por hipótese de indução, $X \setminus \{n\}$ é finito e de cardinalidade menor ou igual a n . O resultado segue-se da observação que antecede esta proposição. \square

Os três exercícios que se seguem pedem para se mostrar propriedades muito elementares dos conjuntos finitos.

Exercício 37. *Sejam X e Y conjuntos finitos. Mostre que $X \cup Y$ é finito e $\text{card}(X \cup Y) \leq \text{card}(X) + \text{card}(Y)$. No caso particular de X e Y serem disjuntos, mostre que se tem a igualdade. [Sugestão: mostre primeiro o caso particular.]*

Exercício 38. *Sejam X e Y conjuntos finitos. Mostre que $X \times Y$ é finito e $\text{card}(X \times Y) = \text{card}(X) \cdot \text{card}(Y)$. [Sugestão: por indução na cardinalidade de Y .]*

Exercício 39. *Sejam X e Y conjuntos finitos. Mostre que Y^X é finito e $\text{card}(Y^X) = \text{card}(Y)^{\text{card}(X)}$. Conclua que se X é finito então $\mathcal{P}(X)$ também é finito e $\text{card}(\mathcal{P}(X)) = 2^{\text{card}(X)}$.*

Teorema (Princípio dos cacifos). *Seja X um conjunto finito e $f : X \mapsto X$ uma função injectiva. Então f é sobrejectiva.*

Demonstração. Basta ver que, para todo $n \in \mathbb{N}$, sempre que $f : [n] \mapsto [n]$ é injectiva então é sobrejectiva. Com efeito, se f não fosse sobrejectiva, então $n \neq 0$ e (pelo Lema 4) existiria uma injeção de $[n]$ em $[n - 1]$, o que contradiz a proposição 29. \square

Esta formulação do princípio dos cacifos não é a mais conhecida. Geralmente, formula-se o princípio do seguinte modo: dados conjuntos finitos com $n + 1$ elementos e n elementos, respectivamente, então não existe uma aplicação injectiva do primeiro no segundo. Alternativamente, se X é um conjunto finito e $x \in X$ então não existe uma injeção de X em $X \setminus \{x\}$. Note-se que esta formulação é equivalente ao princípio tal como o formulámos no teorema acima (basta notar que uma tal injeção, quando considerada como aplicação em X , não é sobrejectiva).

Exercício 40. *Seja X um conjunto finito e $f : X \mapsto X$ uma sobrejecção. Mostre que f é injectiva.*

Um conjunto X diz-se *infinito à Dedekind* se existir uma injeção de X em si próprio que não é sobrejectiva. O princípio dos cacifos garante que os conjuntos infinitos à Dedekind são infinitos. O recíproco também é verdade na presença do axioma da escolha, como veremos.

Lema 5. *Se $\mathbb{N} \leq_c X$ então X é infinito à Dedekind.*

Demonstração. Seja $f : \mathbb{N} \rightarrow X$ uma função injectiva. Defina-se a função $g : X \mapsto X$ do seguinte modo:

$$g(x) := \begin{cases} f(n+1) & \text{se } x \in \text{im} f \text{ com } f(n) = x \\ x & \text{se } x \notin \text{im} f \end{cases}$$

Esta função está bem definida, é injectiva mas não é sobrejectiva, visto que $f(0) \notin \text{img}$. □

Conclui-se imediatamente que \mathbb{Z} , \mathbb{Q} e \mathbb{R} são infinitos à Dedekind.

Proposição 31. *Um conjunto X é infinito se, e somente se, $\mathbb{N} \leq_c X$.*

Demonstração. Já vimos que se $\mathbb{N} \leq_c X$ então X é infinito à Dedekind. Logo é infinito. Reciprocamente, suponhamos que X é infinito. Informalmente, o argumento é simples. Como $X \neq \emptyset$, tome-se $a_0 \in X$. Como $X \setminus \{a_0\} \neq \emptyset$ (visto que X é infinito), tome-se $a_1 \in X \setminus \{a_0\}$. Seguidamente toma-se $a_2 \in X \setminus \{a_0, a_1\}$. E por aí a fora ... Claramente, a função de \mathbb{N} em X dada por $n \mapsto a_n$ é uma função injectiva. □

Note que o argumento acima utiliza o axioma da escolha. A forma rigorosa de pôr o argumento é a seguinte. Fixe-se ϵ_X uma função de escolha para X . Define-se por recursão completa a função $f : \mathbb{N} \mapsto X$ do seguinte modo:

$$f(n) = \epsilon_X(X \setminus \{f(0), \dots, f(n-1)\}).$$

Note-se que f está bem definida e é injectiva.

Corolário 3. *Um conjunto é infinito se, e somente se, é infinito à Dedekind.*

Exercício 41. *Mostre, sem utilizar o axioma da escolha, que se um conjunto X é infinito à Dedekind então $\mathbb{N} \leq_c X$.*

O exercício acima, juntamente com o Lema 5, mostra (sem apelar ao axioma da escolha) que um conjunto X é infinito à Dedekind se, e somente se, o conjunto \mathbb{N} se injecta em X .

Chapter 11

Numerabilidade

Definição 9. Um conjunto X diz-se numerável se for equipotente a \mathbb{N} .

Exercício 42. Mostre que \mathbb{Z} é numerável.

Proposição 32. Um subconjunto de \mathbb{N} é finito ou numerável.

Demonstração. Seja $X \subseteq \mathbb{N}$. Se X é limitado então é finito (pois é subconjunto de um conjunto finito). Caso X seja ilimitado, define-se por recursão a função $f : \mathbb{N} \rightarrow X$ em que $f(0) = \min X$ e $f(n+1) = \min\{k \in X : f(n) < k\}$. Por definição, $f(n) < f(n+1)$ e, portanto, f é injectiva. Logo, $\mathbb{N} \leq_c X$. Pelo teorema de Cantor-Schröder-Bernstein, conclui-se que $X =_c \mathbb{N}$. \square

Corolário 4. Se $X \leq_c \mathbb{N}$, então X é finito ou numerável.

Proposição 33 (Cantor). $\mathbb{N} \times \mathbb{N}$ é numerável.

Demonstração. A seguinte sucessão é uma bijecção entre \mathbb{N} e $\mathbb{N} \times \mathbb{N}$:

$$(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3), (1, 2), (2, 1), (3, 0), (0, 4), \dots$$

Rigorosamente, mostra-se (ainda que seja um exercício de alguma delicadeza) que a função de $\mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ dada por $(n, m) \rightsquigarrow \frac{1}{2}(n+m)(n+m+1) + n$ é uma bijecção. (A sucessão acima é a função inversa desta bijecção.)

Alternativamente, a função $h : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ dada por $h(n, k) = 2^n 3^k$ é uma injecção (pela unicidade da factorização de um número natural em factores primos). Logo, $\mathbb{N} \times \mathbb{N} \leq_c \mathbb{N}$. Dado que $\mathbb{N} \leq_c \mathbb{N} \times \mathbb{N}$, tem-se a equipotência desejada pelo teorema de Cantor-Schröder-Bernstein. \square

Corolário 5. O produto cartesiano de dois conjuntos numeráveis é numerável.

Para ver que um conjunto infinito X é numerável o seguinte critério é muito conveniente: basta ver que existe uma sobrejecção dum conjunto numerável em X . Com efeito, pela Proposição 28, sai $X \leq_c \mathbb{N}$. Note que nesta aplicação da Proposição 28, não é necessário aplicar o axioma da escolha (ver exercício 36). Pode agora ver-se facilmente que \mathbb{Q} é numerável. Como \mathbb{Z} e \mathbb{N}^+ são numeráveis, pelo corolário anterior, $\mathbb{Z} \times \mathbb{N}^+$ é numerável. Ora, $(n, m) \rightsquigarrow \frac{n}{m}$ é uma sobrejecção de $\mathbb{Z} \times \mathbb{N}^+$ sobre \mathbb{Q} .

Exercício 43. *Mostre que a união de dois conjuntos numeráveis é numerável. Mostre que a união de um conjunto numerável com um conjunto finito é numerável.*

Proposição 34. *Uma união numerável de conjuntos numeráveis é numerável. Dito de outro modo, se $(X_n)_{n \in \mathbb{N}}$ é uma sucessão de conjuntos numeráveis, então $\bigcup_{n \in \mathbb{N}} X_n$ é numerável.*

Demonstração. Para cada $n \in \mathbb{N}$ escolha-se uma bijecção f_n de \mathbb{N} em X_n . Imediatamente, tem-se que $(n, m) \rightsquigarrow f_n(m)$ é uma sobrejecção de $\mathbb{N} \times \mathbb{N}$ em $\bigcup_{n \in \mathbb{N}} X_n$. \square

Exercício 44. *O leitor atento deve ter observado que, no argumento acima, se utiliza o axioma da escolha. Explícite o seu uso.*

Dado um conjunto X , seja $\mathcal{P}_{\text{fin}}(X)$ o conjunto de todos os subconjuntos finitos de X . Não é difícil de ver que $\mathcal{P}_{\text{fin}}(\mathbb{N})$ é numerável. Com efeito, $\mathcal{P}_{\text{fin}}(\mathbb{N}) = \bigcup_{n=0}^{\infty} \mathcal{P}_{\leq n}(\mathbb{N})$, onde $\mathcal{P}_{\leq n}(\mathbb{N})$ é o conjunto de todos os subconjuntos de \mathbb{N} que não excedem n elementos. Pela proposição acima, basta ver que, para todo $n \in \mathbb{N}^+$, $\mathcal{P}_{\leq n}(\mathbb{N})$ é numerável. Ora, dado $n \in \mathbb{N}^+$, a função de \mathbb{N}^n para $\mathcal{P}_{\leq n}(\mathbb{N})$ definida por:

$$(x_1, \dots, x_n) \rightsquigarrow \{x_1, \dots, x_n\}$$

tem como imagem $\mathcal{P}_{\leq n}(\mathbb{N}) \setminus \{\emptyset\}$. Como \mathbb{N}^n é numerável, conclui-se que $\mathcal{P}_{\leq n}(\mathbb{N})$ é numerável.

Um número real diz-se *algébrico* se for raiz dum polinómio da forma $a_0 + a_1X + \dots + a_nX^n$, onde os coeficientes são números inteiros e $a_n \neq 0$. Por exemplo, os números racionais são algébricos, assim como $\sqrt{2}$ ou $(1 + \sqrt{3})^2$. Também o é a única (porquê?) raiz real da equação $X^5 + X + 1 = 0$. NB por um teorema clássico do matemático norueguês Niels Abel, esta raiz não pode ser expressa em termos de radicais. Não é difícil de mostrar que o conjunto dos números algébricos reais é numerável. Com efeito, o conjunto de todos os polinómios não nulos de coeficientes inteiros é numerável visto que é constituído pela união numerável dos conjuntos de tais polinómios dum determinado grau n , sendo estes, por sua vez, imagens sobrejectivas de $\mathbb{Z}^n \times (\mathbb{Z} \setminus \{0\})$. Para cada polinómio não nulo de coeficientes inteiros, o conjunto das suas raízes reais é finito. Logo, o conjunto dos números algébricos é uma união numerável de conjuntos finitos. É, portanto, numerável.

Chapter 12

A cardinalidade do *continuum*

O seguinte argumento de *diagonalização* é famoso:

Proposição 35. *O conjunto $\{0, 1\}^{\mathbb{N}}$ não é numerável.*

Demonstração. Suponhamos, com vista a um absurdo, que existe uma bijecção f de \mathbb{N} em $\{0, 1\}^{\mathbb{N}}$. Considere-se a sucessão $d \in \{0, 1\}^{\mathbb{N}}$ definida por: $d(n) := 1 - (f(n))(n)$. Visto que f é sobrejectiva existe $n_0 \in \mathbb{N}$ tal que $f(n_0) = d$. Sai, $d(n_0) = 1 - (f(n_0))(n_0) = 1 - d(n_0)$, o que é absurdo. \square

O próximo passo consiste em mostrar que $\mathbb{R} =_c \{0, 1\}^{\mathbb{N}}$. Daqui se conclui que \mathbb{R} não é um conjunto numerável. Considere-se a função $x \rightsquigarrow \{q \in \mathbb{Q} : q < x\}$. É muito fácil de ver que esta função é uma injeção de \mathbb{R} em $\mathcal{P}(\mathbb{Q})$. Logo, $\mathbb{R} \leq_c \mathcal{P}(\mathbb{Q}) =_c \mathcal{P}(\mathbb{N})$, pois $\mathbb{Q} =_c \mathbb{N}$. Ora, $\mathcal{P}(\mathbb{N})$ é equipotente ao seu conjunto de funções características $\{0, 1\}^{\mathbb{N}}$. Portanto, $\mathbb{R} \leq_c \{0, 1\}^{\mathbb{N}}$. Pelo teorema de Cantor-Schröder-Bernstein, basta agora mostrar que $\{0, 1\}^{\mathbb{N}} \leq_c \mathbb{R}$. Isto pode ser feito de várias maneiras. Aqui optamos por um argumento que não é o mais simples mas que exhibe um conjunto importante de números reais: o *conjunto ternário de Cantor*.

Seja $2^{<\mathbb{N}}$ o conjunto de todas as funções cujo domínio é da forma $[n]$, para algum $n \in \mathbb{N}$, e cujo conjunto de chegada é $\{0, 1\}$. Aos elementos de $2^{<\mathbb{N}}$ chamam-se sequências binárias (finitas) e, muitas vezes, denotam-se por $\langle \sigma(0), \sigma(1), \dots, \sigma(n-1) \rangle$. O número n é o comprimento da sequência σ e escreve-se $\text{comp}(\sigma) = n$. Dada $\sigma \in 2^{<\mathbb{N}}$, definem-se as seguintes sequências de comprimento $n+1$:

$$\sigma 0 := \langle \sigma(0), \sigma(1), \dots, \sigma(n-1), 0 \rangle \text{ e}$$

$$\sigma 1 := \langle \sigma(0), \sigma(1), \dots, \sigma(n-1), 1 \rangle;$$

Note-se que estas sequências binárias são obtidas a partir de σ por concatenação do elemento 0, respectivamente, do elemento 1. Note, finalmente, que há uma única sequência de comprimento 0, por vezes denotada por $\langle \rangle$. Com esta notação podemos a descrever o conjunto ternário de Cantor.

Dado um intervalo $[a, b]$, fechado e limitado de \mathbb{R} (com $a < b$), sejam $\text{esq}([a, b]) := [a, a + \frac{b-a}{3}]$ e $\text{dir}([a, b]) := [b - \frac{b-a}{3}, b]$ (respectivamente, o primeiro

e o terceiro terço de $[a, b]$). Construimos, para cada sequência $\sigma \in 2^{<\mathbb{N}}$, um subconjunto C_σ de $[0, 1]$. Esta construção é descrita pelas seguintes equações: $C_{\langle \rangle} = [0, 1]$, $C_{\sigma 0} = \text{esq}(C_\sigma)$ e $C_{\sigma 1} = \text{dir}(C_\sigma)$. Assim, temos:

$$C_{\langle 0 \rangle} = [0, \frac{1}{3}], \quad C_{\langle 1 \rangle} = [\frac{2}{3}, 1];$$

$$C_{\langle 0,0 \rangle} = [0, \frac{1}{9}], \quad C_{\langle 0,1 \rangle} = [\frac{2}{9}, \frac{1}{3}], \quad C_{\langle 1,0 \rangle} = [\frac{2}{3}, \frac{7}{9}], \quad C_{\langle 1,1 \rangle} = [\frac{8}{9}, 1];$$

etc. Vamos, sucessivamente, tirando o terço do meio dos intervalos. A aplicação $\sigma \rightsquigarrow C_\sigma$ acima descrita existe pelo teorema da recursão, apesar da justificação não ser inteiramente óbvia.

Para cada $n \in \mathbb{N}$, seja $C^n := \bigcup_{\sigma \in \{0,1\}^{<\mathbb{N}}: \text{comp}(\sigma)=n} C_\sigma$. Temos:

$$C^0 = [0, 1];$$

$$C^1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1];$$

$$C^2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1];$$

etc. O conjunto ternário de Cantor é, por definição, $C := \bigcap_{n \in \mathbb{N}} C^n$.

Dado $\alpha \in \{0, 1\}^{\mathbb{N}}$, define-se $C'(\alpha) := \bigcap_{n \in \mathbb{N}} C_{\langle \alpha(0), \alpha(1), \dots, \alpha(n-1) \rangle}$. Note-se que $C'(\alpha)$ é a intersecção de uma sucessão de intervalos fechados encaixados cujos comprimentos tendem para 0. Pelo princípio do encaixe, $C'(\alpha)$ é um conjunto singular. Seja $C(\alpha)$ o seu único elemento, i.e., $C'(\alpha) = \{C(\alpha)\}$. Vamos argumentar que a aplicação $\alpha \rightsquigarrow C(\alpha)$ é uma injeção de $\{0, 1\}^{\mathbb{N}}$ em C (e, portanto, em \mathbb{R}).

Tomem-se $\alpha, \beta \in \{0, 1\}^{\mathbb{N}}$ com $\alpha \neq \beta$. Então existe um elemento mínimo $n \in \mathbb{N}$ tal que $\alpha(n) \neq \beta(n)$. Sem perda de generalidade, $\alpha(n) = 0$ e $\beta(n) = 1$. Note-se que, por minimalidade de n , $\alpha(0) = \beta(0), \dots, \alpha(n-1) = \beta(n-1)$. Vem:

$$C(\alpha) \in C_{\langle \alpha(0), \dots, \alpha(n-1), \alpha(n) \rangle} = C_{\sigma 0} = \text{esq}(C_\sigma);$$

$$C(\beta) \in C_{\langle \beta(0), \dots, \beta(n-1), \beta(n) \rangle} = C_{\sigma 1} = \text{dir}(C_\sigma);$$

onde σ é a sequência $\langle \alpha(0), \dots, \alpha(n-1) \rangle = \langle \beta(0), \dots, \beta(n-1) \rangle$. Como $\text{esq}(C_\sigma)$ e $\text{dir}(C_\sigma)$ são conjuntos disjuntos, vem que $C(\alpha) \neq C(\beta)$.

Exercício 45. Mostre que a correspondência $\alpha \rightsquigarrow C(\alpha)$ é uma bijecção entre $\{0, 1\}^{\mathbb{N}}$ e o conjunto ternário de Cantor.

Mostrámos, pois, o seguinte resultado:

Proposição 36. $\mathbb{R} \simeq_c \{0, 1\}^{\mathbb{N}}$. Em particular, \mathbb{R} não é numerável.

Exercício 46. Mostre que o conjunto de todos os abertos de \mathbb{R} é equipotente a \mathbb{R} . [Sugestão: faça corresponder a cada aberto U de \mathbb{R} o conjunto de todos os pares $(x, y) \in \mathbb{Q}^2$ tais que $]x, y[\subseteq U$.]

Será que há cardinalidades estritamente entre \mathbb{N} e $\mathcal{P}(\mathbb{N})$? Esta é a célebre hipótese do contínuo colocada por Georg Cantor. Desde os trabalhos de Kurt Gödel e Paul Cohen no final da década de trinta e no início da década de sessenta do século passado (respectivamente) que se sabe que esta questão é independente da axiomática usual da teoria dos conjuntos.

Chapter 13

O teorema de Cantor

O seguinte resultado, também devido a Cantor, generaliza o teorema 35.

Teorema de Cantor. *Para qualquer conjunto X , $X \neq_c \mathcal{P}(X)$.*

Demonstração. Admitamos, com vista a um absurdo, que existe uma bijecção f de X em $\mathcal{P}(X)$. Considere-se o conjunto $Z := \{x \in X : x \notin f(x)\}$. Como $Z \in \mathcal{P}(X)$, pela sobrejectividade de f existe $x_0 \in X$ tal que $f(x_0) = Z$. Agora:

$$x_0 \in f(x_0) \leftrightarrow x_0 \in Z \leftrightarrow x_0 \notin f(x_0),$$

o que é uma contradição. \square

Consequentemente, $X <_c \mathcal{P}(X)$. Há, pois, muitos infinitos de cardinalidade diferente:

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

É claro, as cardinalidades não se esgotam aqui. Em ZF há cardinalidades que se seguem a todas as cardinalidades listadas acima. Um exemplo é a cardinalidade do conjunto:

$$\mathcal{P}^\infty(\mathbb{N}) := \mathbb{N} \cup \mathcal{P}(\mathbb{N}) \cup \mathcal{P}(\mathcal{P}(\mathbb{N})) \cup \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \cup \dots$$

e isto não acaba aqui pois, pelo teorema de Cantor, $\mathcal{P}(\mathcal{P}^\infty(\mathbb{N}))$ tem cardinalidade superior a $\mathcal{P}^\infty(\mathbb{N})$, etc, etc. Também se pode perguntar se, para conjuntos infinitos X , há cardinalidades estritamente entre X e $\mathcal{P}(X)$ (a resposta é independente dos axiomas de ZFC). Ou, se dado um conjunto X , há uma cardinalidade imediatamente a seguir à cardinalidade de X (a resposta é afirmativa, em ZFC). Ou se

Terminamos este capítulo com uma generalização do teorema de Cantor. Na demonstração desta generalização usamos à saciedade o axioma da escolha. Recorde-se que, dada uma família de conjuntos $(Y_i)_{i \in I}$, o conjunto $\prod_{i \in I} Y_i$ é, por definição, o conjunto de todas as funções ϕ com domínio I tais que, para todo $i \in I$, $\phi(i) \in Y_i$. Frequentemente, os elementos de $(Y_i)_{i \in I}$ são denotados por $(y_i)_{i \in I}$, onde ϕ é dada por $\phi(i) = y_i$.

Proposição 37 (Teorema da cardinalidade de König). *Dadas famílias $(X_i)_{i \in I}$ e $(Y_i)_{i \in I}$ de conjuntos tais que $X_i <_c Y_i$, para todo $i \in I$, então*

$$\bigcup_{i \in I} X_i <_c \prod_{i \in I} Y_i.$$

Demonstração. Tome-se $(f_i)_{i \in I}$ uma família de injecções $f_i : X_i \mapsto Y_i$ e uma família $(y_i)_{i \in I}$ tal que $y_i \in Y_i \setminus \text{im} f_i$, para todo $i \in I$ (estas famílias existem por hipótese e pelo axioma da escolha). Dado $x \in \bigcup_{i \in I} X_i$ e $j \in I$ define-se:

$$g(x, j) := \begin{cases} f_j(x) & \text{se } x \in X_j \\ y_j & \text{caso contrário} \end{cases}$$

Para cada $x \in \bigcup_{i \in I} X_i$, a família $g(x) : j \rightsquigarrow g(x, j)$ é um elemento de $\prod_{i \in I} Y_i$. Vamos ver que $g : \bigcup_{i \in I} X_i \mapsto \prod_{i \in I} Y_i$ é uma injecção. Sejam $x, x' \in \bigcup_{i \in I} X_i$ com $x \neq x'$. Se existe $j \in I$ tal que $x, x' \in X_j$ então, pela injectividade de f_j , tem-se $g(x, j) = f_j(x) \neq f_j(x') = g(x', j)$ e, portanto, $g(x) \neq g(x')$. Caso contrário, x está nalgum X_j e $x' \notin X_j$. Neste caso, $g(x', j) = y_j \notin \text{im} f_j$ e $g(x, j) = f_j(x) \in \text{im} f_j$. Logo, $g(x, j) \neq g(x', j)$ e, igualmente, $g(x) \neq g(x')$.

Mostrámos que $\bigcup_{i \in I} X_i <_c \prod_{i \in I} Y_i$. Suponhamos agora, com vista a um absurdo, que existe uma bijecção $h : \bigcup_{i \in I} X_i \mapsto \prod_{i \in I} Y_i$. Para cada $j \in I$, considere-se a função $h_j : X_j \mapsto Y_j$ definida por $x \rightsquigarrow h(x)(j)$. Por hipótese, h_j não é sobrejectiva (axioma da escolha). Seja então $(y_i)_{i \in I}$ uma família tal que $y_i \in Y_i \setminus \text{im} h_i$, para todo $i \in I$ (axioma da escolha). Ora, por suposição, existe $x \in \bigcup_{i \in I} X_i$ tal que $h(x) = (y_i)_{i \in I}$. Tome-se $j \in I$ tal que $x \in X_j$. Vem, $y_j = h(x)(j) = h_j(x) \in \text{im} h_j$, o que contradiz a escolha de y_j . \square

O teorema de Cantor é um corolário do resultado acima. Com efeito, seja X um conjunto qualquer. Considere-se a família $X_i := \{i\}$ de conjuntos singulares (i.e., de um único elemento), onde o índice i varia em X . Considere-se também a família constante $Y_i := \{0, 1\}$, para $i \in X$. Pelo teorema da cardinalidade de König, $X = \bigcup_{i \in X} \{i\} <_c \prod_{i \in X} \{0, 1\} = \{0, 1\}^X$. Isto é uma reformulação do teorema de Cantor.

Chapter 14

Aritmética cardinal, sem cardinais...

A noção de cardinalidade é uma noção que exige alguma delicadeza de tratamento num desenvolvimento rigoroso em teoria dos conjuntos. O que é, em geral, o cardinal dum conjunto? Que objecto é este? Intuitivamente, o cardinal dum conjunto é *aquilo* que é comum a todos os conjuntos equipotentes a esse conjunto. Na prática matemática, este *aquilo* que é comum aos objectos que estão mutuamente em relação sob uma determinada relação de equivalência é a própria classe de equivalência do objecto. Mas tal pressupõe que a dada relação de equivalência esteja definida num determinado *conjunto*, o que não é o caso com a noção de equipotência. Com efeito, esta noção aplica-se a *todos* os conjuntos e, como veremos mais tarde, não é possível aglomerar todos os conjuntos num conjunto.

Desde que se tenham os números naturais, o problema da cardinalidade dum conjunto finito tem solução simples: o cardinal de um conjunto finito X é o (único) número natural n tal que $X =_c [n]$. Para além disto, dada a importância dos conjuntos \mathbb{N} e \mathbb{R} , adopta-se a terminologia de dizer que os conjuntos numeráveis têm cardinalidade \aleph_0 e que os conjuntos equipotentes ao *continuum* têm cardinalidade c . A solução para o problema de dar um sentido objectual às várias cardinalidades consiste no desenvolvimento duma teoria geral de números que estenda a teoria dos números naturais: os números *ordinais* de von Neumann. Mais tarde, iremos desenvolver esta teoria e, para isso, será necessário formular a axiomática da teoria dos conjuntos ZFC (notavelmente o axioma da substituição).

No entretanto, a noção de cardinalidade vai sempre aparecer no *contexto* duma asserção de tal modo que, convenientemente reinterpretada, a asserção não fala de cardinalidades mas apenas de equipotência e noções afins. Um exemplo ilustra este *modus operandi*. Informalmente, dadas cardinalidades κ e ρ , a cardinalidade produto, denotada por $\kappa \cdot \rho$, é a cardinalidade do produto cartesiano $A \times B$, onde A e B têm cardinalidade κ e ρ , respectivamente. Subjacente ao uso do produto de cardinalidades está a seguinte noção de congruência:

- (a) Se $A =_c A'$ e $B =_c B'$ então $A \times B =_c A' \times B'$.

Claro que se tem a seguinte lei: $\kappa \cdot \rho = \rho \cdot \kappa$. Encaramos esta lei como dizendo

o seguinte:

(b) $A \times B =_c B \times A$, para quaisquer conjuntos A e B .

Observe-se aquilo que realmente se está a passar: à lei que diz que o produto de duas cardinalidades não depende da ordem dos factores subjaz a propriedade (a), enquanto que a lei propriamente dita é uma forma de dizer (b). Neste entendimento, não faz sentido falar da cardinalidade de X isoladamente, mas já faz sentido dizer (p. ex.) que a cardinalidade dum conjunto X é estritamente menor que a cardinalidade dum conjunto Y . O discurso sobre cardinalidades faz sentido no *contexto* de asserções (convenientes), ainda que por enquanto não faça sentido fora delas. Diz-se, em filosofia, que é um discurso *sincategoremático* sobre cardinalidades. Vamos pois, neste capítulo, interpretar as asserções sobre cardinais deste modo sincategoremático (o que pressupõe que se possam interpretar desta forma). Por exemplo, o teorema de Cantor-Schröder-Bernstein tem a seguinte formulação: $\kappa \leq \rho \wedge \rho \leq \kappa \rightarrow \kappa = \rho$, para κ e ρ cardinais.

A soma das cardinalidades κ e ρ é a cardinalidade de $A \cup B$, onde A e B são conjuntos disjuntos e têm cardinalidades κ e ρ , respectivamente. Note-se que dados conjuntos A e B é sempre possível obter conjuntos *disjuntos* com as mesmas cardinalidades (respectivas): p. ex., $\{0\} \times A$ e $\{1\} \times B$ (ao conjunto $(\{0\} \times A) \cup (\{1\} \times B)$ dá-se o nome de *união disjunta* de A com B e denota-se por $A \uplus B$). Com estas noções de soma e produtos de cardinais é fácil de ver que as seguintes asserções sobre cardinalidades se podem interpretar do modo elíptico atrás descrito e, quando sujeitas a esta interpretação, são sempre verdadeiras:

1. $\kappa + 0 = \kappa$
2. $\kappa \cdot 0 = 0$
3. $\kappa \cdot 1 = \kappa$
4. $\kappa \cdot 2 = \kappa + \kappa$
5. $\kappa + (\rho + \mu) = (\kappa + \rho) + \mu$
6. $\kappa + \rho = \rho + \kappa$
7. $\kappa \cdot (\rho \cdot \mu) = (\kappa \cdot \rho) \cdot \mu$
8. $\kappa \cdot \rho = \rho \cdot \kappa$
9. $\kappa \cdot (\rho + \mu) = \kappa \cdot \rho + \kappa \cdot \mu$
10. $\kappa \leq \rho \rightarrow \kappa + \mu \leq \rho + \mu$
11. $\kappa \leq \rho \rightarrow \kappa \cdot \mu \leq \rho \cdot \mu$

Por exemplo, a quarta propriedade acima diz que $A \times \{0, 1\} =_c A \uplus A$, para todos os conjuntos A . Também utilizámos algumas abreviaturas naturais para omitir parêntesis. A verificação das propriedades é simples e fica como exercício.

A cardinalidade κ^ρ define-se como a cardinalidade do conjunto A^B , onde A tem cardinalidade κ e B tem cardinalidade ρ . Deste modo, é correcto dizer que se um conjunto A tem cardinalidade κ então $\mathcal{P}(A)$ tem cardinalidade 2^κ . Com efeito, isto advém do facto – já observado – de que $\mathcal{P}(A)$ é equipotente ao conjunto de todas as funções características de A . O teorema de Cantor pode enunciar-se assim: Para todo o cardinal κ , $\kappa < 2^\kappa$. O seguinte é válido:

12. $(\kappa \cdot \rho)^\mu = \kappa^\mu \cdot \rho^\mu$
13. $\kappa^{\rho+\mu} = \kappa^\rho \cdot \kappa^\mu$
14. $(\kappa^\rho)^\mu = \kappa^{\rho \cdot \mu}$
15. $\kappa \leq \rho \wedge \mu \neq 0 \rightarrow \mu^\kappa \leq \mu^\rho$
16. $\kappa \leq \rho \rightarrow \kappa^\mu \leq \rho^\mu$

para quaisquer cardinalidades κ , ρ e μ .

As cardinalidades finitas, assim como a cardinalidade numerável \aleph_0 e a cardinalidade do contínuo \mathfrak{c} , são extremamente importantes em matemática. Os exercícios 37, 38 e 39 mostram que a aritmética cardinal definida atrás, quando restringida a conjuntos finitos, coincide com a aritmética dos números naturais. Também temos as seguintes propriedades:

Proposição 38. *Abaixo, κ é um cardinal e n é um número natural.*

- (a) $\kappa < \aleph_0$ se, e somente se, $\exists m \in \mathbb{N}(\kappa = m)$.
- (b) $\mathfrak{c} = 2^{\aleph_0}$.
- (c) $\aleph_0 < \mathfrak{c}$.
- (d) $\aleph_0 + \aleph_0 = \aleph_0$ e $\aleph_0 \cdot \aleph_0 = \aleph_0$.
- (e) $\aleph_0 + n = \aleph_0$ e, se $n \neq 0$, $\aleph_0 \cdot n = \aleph_0$.
- (f) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$ e $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.
- (g) $\mathfrak{c} + n = \mathfrak{c}$ e, se $n \neq 0$, $\mathfrak{c} \cdot n = \mathfrak{c}$.
- (h) $\mathfrak{c} + \aleph_0 = \mathfrak{c} \cdot \aleph_0 = \mathfrak{c}$.
- (i) *Se B tem cardinalidade \mathfrak{c} e $A \subseteq B$ é finito ou numerável, então $B \setminus A$ tem cardinalidade \mathfrak{c} .*

Demonstração. A alínea (a) sai da Proposição 32. (b) é uma reformulação do facto de que $\mathbb{R} = {}_c\{0, 1\}^{\mathbb{N}}$. Por (b), (c) diz que $\aleph_0 < {}_c 2^{\mathbb{N}}$, o que já sabemos. $\aleph_0 \cdot \aleph_0 = \aleph_0$ é a Proposição 33. Por outro lado, $\aleph_0 \leq \aleph_0 + n \leq \aleph_0 + \aleph_0 = 2\aleph_0 \leq \aleph_0 \cdot \aleph_0 = \aleph_0$. Isto demonstra o resto de (d) e a primeira parte de (e). Para a segunda parte de (e), note-se que $\aleph_0 \leq \aleph_0 \cdot n \leq \aleph_0 \cdot \aleph_0 = \aleph_0$. A segunda parte de (f) sai do seguinte: $\mathfrak{c} \cdot \mathfrak{c} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$. A primeira parte de (f) assim como (g) e (h) concluem-se agora facilmente.

Resta mostrar a alínea (i). Sem perda de generalidade, podemos supor que B é $\mathbb{R} \times \mathbb{R}$. Considere-se a projecção

$$P := \{x \in \mathbb{R} : \exists y \in \mathbb{R} (x, y) \in A\}.$$

Como A é finito ou numerável, P é finito ou numerável. Logo, existe $x_0 \in \mathbb{R} \setminus P$. Seja X o conjunto $\{x_0\} \times \mathbb{R}$. Claro que X tem a cardinalidade do *continuum* e, por construção, $X \subseteq (\mathbb{R} \times \mathbb{R}) \setminus A$. Logo, $B \setminus A$ tem pelo menos a cardinalidade \mathfrak{c} . O resultado sai pelo teorema de Cantor-Schröder-Bernstein. \square

Proposição 39. *Os seguintes conjuntos têm cardinalidade \mathfrak{c} :*

1. *O conjunto dos números irracionais.*
2. *O conjunto dos números transcendentos (um número real diz-se transcendente se não é um número algébrico).*
3. *O conjunto de todos os subconjuntos infinitos de \mathbb{N} .*
4. *O conjunto de todas as funções contínuas de \mathbb{R} para \mathbb{R} .*

Demonstração. O conjunto dos racionais \mathbb{Q} é numerável. Logo, pela última alínea da proposição anterior, o conjunto complementar $\mathbb{R} \setminus \mathbb{Q}$ dos números irracionais tem cardinalidade \mathfrak{c} . De igual modo se demonstram as alíneas (2) e (3), pois como já vimos tanto o conjunto dos números algébricos como o conjunto de todos os subconjuntos finitos de \mathbb{N} são numeráveis.

O argumento para justificar a propriedade (4) é diferente. Considere-se a aplicação que a cada função contínua f de \mathbb{R} para \mathbb{R} faz corresponder a sua restrição $f \upharpoonright \mathbb{Q}$ ao conjunto \mathbb{Q} dos números racionais. Esta aplicação é injectiva pois se duas funções contínuas coincidem num subconjunto denso de \mathbb{R} , então são iguais. Logo, a cardinalidade do conjunto de todas as funções contínuas de \mathbb{R} para \mathbb{R} é menor ou igual à cardinalidade de $\mathbb{R}^{\mathbb{Q}}$. Ora, esta cardinalidade é $\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$. A desigualdade oposta é trivial. \square

Exercício 47. *Mostre que a cardinalidade de todas as funções de \mathbb{R} para \mathbb{R} é $2^{\mathfrak{c}}$.*

Por meio do axioma da escolha podem generalizar-se algumas propriedades de \aleph_0 e \mathfrak{c} a cardinalidades infinitas arbitrárias (note que a proposição 38 não usa o axioma da escolha).

Proposição 40 (Lei da absorção). *Sejam κ e ρ cardinais não nulos, o segundo dos quais infinito. Então*

$$\kappa \leq \rho \rightarrow \kappa + \rho = \kappa \cdot \rho = \rho.$$

Em particular, se ρ é um cardinal infinito então $\rho \cdot \rho = \rho$. Por outras palavras, para todo o conjunto infinito x , tem-se $x \times x =_c x$. Aliás, esta propriedade justifica a lei da absorção: vem, para $\kappa \geq 2$,

$$\rho \leq \kappa + \rho \leq \rho + \rho = 2 \cdot \rho \leq \kappa \cdot \rho \leq \rho \cdot \rho = \rho,$$

o que mostra o desejado. O caso $\kappa = 1$ também é claro. A propriedade invocada será demonstrada no capítulo 26.

Como já mencionámos, na presença do axioma da escolha, dados cardinais κ e ρ , tem-se $\kappa \leq \rho$ ou $\rho \leq \kappa$. Por isso, na presença do axioma da escolha, tem sentido falar em $\max\{\kappa, \rho\}$. Claramente, usando a lei da absorção:

Corolário 6. *Sejam κ e ρ cardinais não nulos, pelo menos um deles infinito. Então $\kappa + \rho = \kappa \cdot \rho = \max\{\kappa, \rho\}$.*

Corolário 7. *Sejam A e B conjuntos, $A \subseteq B$, de cardinalidades κ e ρ respectivamente. Suponhamos que ρ é infinito e que $\kappa < \rho$. Então $B \setminus A$ tem cardinalidade ρ .*

Demonstração. Seja λ a cardinalidade de $B \setminus A$. Visto que B é a união disjunta de A com $B \setminus A$, sai que $\kappa + \lambda = \rho$. Claro que ou κ ou λ é infinito. Pelo corolário anterior, $\rho = \max\{\kappa, \lambda\}$. Conclui-se que $\lambda = \rho$. \square

Chapter 15

Operações cardinais infinitárias

É também possível definir operações infinitárias sobre cardinais. Porém estas definições apenas fazem sentido na presença do axioma da escolha. Por exemplo, a soma $\sum_{i \in I} \kappa_i$ de cardinalidades é a cardinalidade de $\bigcup_{i \in I} (\{i\} \times A_i)$, onde cada A_i tem cardinalidade κ_i . O axioma da escolha é necessário para mostrar que se, para todo $i \in I$, $A_i =_c B_i$ então $\bigcup_{i \in I} (\{i\} \times A_i) =_c \bigcup_{i \in I} (\{i\} \times B_i)$.

Proposição 41. *Seja $(A_i)_{i \in I}$ uma família de conjuntos em que cada A_i tem cardinalidade κ_i . Então a união $\bigcup_{i \in I} A_i$ tem cardinalidade $\leq \sum_{i \in I} \kappa_i$.*

Demonstração. Note-se que há uma sobrejecção de $\bigcup_{i \in I} (\{i\} \times A_i)$ sobre $\bigcup_{i \in I} A_i$: basta associar a cada elemento (i, x) , onde $i \in I$ e $x \in A_i$ o elemento x . Logo, pela Proposição 28, $\bigcup_{i \in I} A_i \leq_c \bigcup_{i \in I} (\{i\} \times A_i)$. \square

Proposição 42. *Seja I um conjunto de cardinalidade μ e sejam $(\kappa_i)_{i \in I}$, $(\rho_i)_{i \in I}$ famílias de cardinais. Então:*

$$(a) \quad \forall i \in I (\kappa_i \leq \rho_i) \rightarrow \sum_{i \in I} \kappa_i \leq \sum_{i \in I} \rho_i;$$

$$(b) \quad \sum_{i \in I} \kappa_i = \mu \cdot \kappa, \text{ se } \forall i \in I (\kappa_i = \kappa).$$

Demonstração. Considerem-se famílias de conjuntos $(X_i)_{i \in I}$ e $(Y_i)_{i \in I}$ tais que, para cada $i \in I$, X_i tem cardinalidade κ_i e Y_i tem cardinalidade ρ_i . Suponhamos, também, que $X_i \leq_c Y_i$. Fixemos (através do axioma da escolha) uma família de injecções $f_i : X_i \mapsto Y_i$. É fácil de ver que a aplicação $(i, x) \rightsquigarrow (i, f_i(x))$ (onde $x_i \in X_i$) é uma injecção de $\bigcup_{i \in I} (\{i\} \times X_i)$ em $\bigcup_{i \in I} (\{i\} \times Y_i)$. Este argumento demonstra a primeira alínea da proposição. Para argumentar a segunda parte da proposição, seja X um conjunto de cardinalidade κ . Temos que ver que $\bigcup_{i \in I} (\{i\} \times X)$ é equipotente a $I \times X$. Ora, estes conjuntos são o mesmo. \square

Exercício 48. *Mostre que $\sum_{n \in \mathbb{N}} n = \aleph_0$. Conclua que na primeira alínea da proposição anterior não se pode substituir a desigualdade \leq pela desigualdade estrita $<$.*

Exercício 49. *Mostre a seguinte lei distributiva: $\lambda \cdot \sum_{i \in I} \kappa_i = \sum_{i \in I} (\lambda \cdot \kappa_i)$.*

O produto de cardinalidades $\prod_{i \in I} \kappa_i$ é a cardinalidade do conjunto $\prod_{i \in I} A_i$, onde cada A_i tem cardinalidade κ_i . Note-se, novamente, que esta definição apenas faz sentido na presença do axioma da escolha.

Proposição 43. *Seja I um conjunto de cardinalidade μ , sejam $(\kappa_i)_{i \in I}$, $(\rho_i)_{i \in I}$ famílias de cardinais seja λ um cardinal. Então:*

- (a) $\forall i \in I (\kappa_i \leq \rho_i) \rightarrow \prod_{i \in I} \kappa_i \leq \prod_{i \in I} \rho_i$;
- (b) $\prod_{i \in I} \kappa_i = \kappa^\mu$, se $\forall i \in I (\kappa_i = \kappa)$;
- (c) $(\prod_{i \in I} \kappa_i)^\lambda = \prod_{i \in I} \kappa_i^\lambda$;
- (d) $\prod_{i \in I} \lambda^{\kappa_i} = \lambda^{\sum_{i \in I} \kappa_i}$.

Demonstração. Apenas vamos argumentar a última alínea, já que os argumentos não são difíceis. Consideremos uma família $(X_i)_{i \in I}$ de conjuntos tal que, para cada $i \in I$, X_i tem cardinalidade κ_i ; considere-se também um conjunto Z de cardinalidade λ . Pretendemos ver que $\prod_{i \in I} Z^{X_i} =_c Z^{\cup_{i \in I} (\{i\} \times X_i)}$. Ora, é fácil de ver que a aplicação que a uma família $(f_i)_{i \in I}$ de funções (cada qual uma função de X_i para Z) faz corresponder a função de $\cup_{i \in I} (\{i\} \times X_i)$ para Z definida por $(i, x) \rightsquigarrow f_i(x)$ (onde $x \in X_i$), é a bijecção desejada. \square

Exercício 50. *Mostre que $\prod_{n \in \mathbb{N} \setminus \{0\}} n = 2^{\aleph_0}$.*

Exercício 51. *Mostre que na primeira alínea da proposição anterior não se pode substituir a desigualdade \leq pela desigualdade estrita $<$.*

O teorema da cardinalidade de König tem a seguinte reformulação: se $(\kappa_i)_{i \in I}$ e $(\lambda_i)_{i \in I}$ são famílias de números cardinais tais que $\kappa_i < \lambda_i$, para todo $i \in I$, então $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$.

Chapter 16

A teoria de Zermelo

O princípio não restrito de compreensão que permite passar *sempre* duma propriedade bem-determinada à sua extensão é inconsistente. O princípio diz que a cada propriedade bem-determinada $P(x)$ se pode associar a sua extensão $\{x : P(x)\}$, que é o conjunto que verifica a seguinte condição (*lei da concreção*):

$$z \in \{x : P(x)\} \leftrightarrow P(z),$$

para quaisquer z . Se considerarmos a propriedade ' $x \notin x$ ' então tem-se, para quaisquer z , $z \in \{x : x \notin x\} \leftrightarrow z \notin z$. Em particular, tomando para z o próprio conjunto $\{x : x \notin x\}$, obtém-se:

$$\{x : x \notin x\} \in \{x : x \notin x\} \leftrightarrow \{x : x \notin x\} \notin \{x : x \notin x\},$$

o que é uma contradição. Esta antinomia é hoje conhecida por *paradoxo de Russell*, tendo sido descoberta por Bertrand Russell (e Ernst Zermelo) no início do século passado.

Em 1908, Zermelo propôs uma axiomatização da teoria dos conjuntos que evita o paradoxo. Esta axiomatização é a raiz da moderna axiomática da teoria dos conjuntos: o sistema de Zermelo-Fraenkel munido do axioma da escolha, de sigla ZFC. O sistema ZFC é um sistema *puro* da teoria dos conjuntos, no sentido em que nesse sistema tudo é um conjunto (mais precisamente, as quantificações da teoria variam apenas sobre conjuntos). Vamos de seguida descrever o sistema de Zermelo (que é parte de ZFC) no âmbito duma teoria pura de conjuntos.

1. O **axioma da extensionalidade** diz que dois conjuntos são o mesmo se, e somente se, tiverem os mesmos elementos.
2. O **axioma esquema da separação** é uma restrição do (problemático) axioma da compreensão. O axioma da separação diz que para cada propriedade bem-determinada $P(x)$ então, dado um conjunto qualquer y , se pode formar o conjunto $\{x \in y : P(x)\}$. Isto quer dizer que, dado um conjunto y , a propriedade $P(x)$ *separa* os elementos de y que verificam a propriedade daqueles que a não verificam, aglomerando-os num conjunto. Este axioma também é conhecido pelo seu nome alemão: *Aussonderung axiom*.

Em virtude do axioma da extensionalidade, o conjunto $\{x \in y : P(x)\}$ está bem determinado por y e pela propriedade P . Com efeito, se z e u fossem conjuntos tais que, para todo x ,

$$x \in z \leftrightarrow x \in y \wedge P(x) \quad \text{e} \quad x \in u \leftrightarrow x \in y \wedge P(x)$$

então, por extensionalidade, $z = u$. De resto, este facto subjaz ao próprio bom uso da expressão ' $\{x \in y : P(x)\}$ '.

O que é feito do paradoxo de Russell com o axioma de compreensão assim restrito? O argumento de Russell dá, agora, origem ao seguinte teorema:

Proposição 44. *Não existe um conjunto z tal que, para todo x , $x \in z \leftrightarrow x \notin x$.*

Na teoria de Zermelo têm-se, pois, propriedades que não têm extensão, i.e., propriedades $P(x)$ para as quais não existe um conjunto z tal que, para todo x , $x \in z \leftrightarrow P(x)$. Dito de outro modo, a expressão ' $\{x : P(x)\}$ ' não está sempre bem definida. A uma propriedade bem-determinada que não tem extensão dá-se o nome de *classe própria*. Assim, a proposição anterior diz que a *classe de Russell* (i.e., a classe dada pela fórmula ' $x \notin x$ ') é uma classe própria. Em geral, falamos em *classes* como outro modo de falar em propriedades bem-determinadas. Note-se, que neste modo de falar, todo o conjunto é uma classe, nomeadamente a classe que advém da propriedade de pertencer a *esse* conjunto. Às classes que não têm extensão chamamos, como já fizemos, classes próprias.

Exercício 52. *Mostre que a classe de todos os conjuntos (a denominada classe universal) é uma classe própria.*

Como dissemos, a nossa teoria é uma teoria *pura* de conjuntos: tudo é conjunto. O que são então as classes próprias? São, como dissemos, um modo de falar em propriedades bem-determinadas. É, tecnicamente, um modo de falar na *metalinguagem*. Na *linguagem* da teoria dos conjuntos não se referem propriedades (não se quantificam), apenas se referem conjuntos. Que dizer então do enunciado do axioma da separação? Ele diz que para *cada* propriedade $P(x)$ se tem o seguinte: para todo o conjunto y existe o conjunto $\{x \in y : P(x)\}$. Mais precisamente, trata-se dum *esquema* de axiomas:

$$\forall y \exists z \forall x (x \in z \leftrightarrow x \in y \wedge P(x)),$$

um para cada propriedade bem-determinada P . O cabal esclarecimento do que é uma propriedade bem-determinada no nosso contexto da teoria dos conjuntos exigiria uma pequena introdução à Lógica Matemática. As linguagens naturais (como o português) não são suficientemente precisas para esclarecer esta problemática. Por exemplo, considere-se a propriedade de ser *o menor número natural que não se pode descrever com menos de quinze palavras*. Note que o número nessas condições foi descrito com catorze palavras! Há, pois, que tornar precisa a noção de propriedade que se usa para descrever os axiomas da teoria dos conjuntos. Sem entrar em detalhes técnicos da Lógica Matemática, podemos adiantar que as propriedades bem-determinadas de que falamos são dadas por *fórmulas* da linguagem formal da teoria dos conjuntos. Mais detalhadamente, fórmulas que se constroem a partir das fórmulas *atómicas* ' $x \in y$ ' e ' $x = y$ ' por meio dos conectivos Booleanos (conjunção, disjunção e negação) e dos quantificadores (existencial e universal). O axioma da separação é o esquema de axiomas

$$\forall y \exists z \forall x (x \in z \leftrightarrow x \in y \wedge \phi(x)),$$

um para cada fórmula $\phi(x)$ da linguagem formal da teoria dos conjuntos (possivelmente com *parâmetros*). Trata-se de um número infinito de axiomas, enunciados (metalinguisticamente) por meio da *formalização* da linguagem objecto (a linguagem da teoria dos conjuntos é uma linguagem *formal*).

Quando falamos sobre classes, é conveniente tomar certas liberdades notacionais. Dada uma classe C (i.e., uma fórmula $C(x)$), escrevemos $a \in C$ para dizer $C(a)$. De igual modo, falamos na classe complementar C^c (a classe associada à fórmula $\neg C(x)$) assim como na união e intersecção de duas classes. Com estas liberdades notacionais, o axioma da separação pode formular-se assim: Dado um conjunto y e uma classe C , então a classe $y \cap C$ é um conjunto. Note-se que, para conseguir formar um conjunto por separação, é mister ter *a priori* um conjunto y para ‘separar’. Os próximos axiomas dão um acervo básico de tais conjuntos.

Antes de entrarmos nos próximos quatro axiomas, devemos discutir um pequeno ponto. Nas formulações usuais da lógica, supõe-se sempre que há pelo menos um objecto no domínio do discurso. No nosso caso, este requisito diz que há pelo menos um conjunto. Seja ele z . Então, pelo axioma da separação, podemos formar o conjunto $\{x \in z : x \neq x\}$. Este conjunto não é mais do que o conjunto vazio, denotado por \emptyset (único, por extensionalidade). Em formulações menos usuais, existe explicitamente um axioma que garante a existência do conjunto vazio. Não o faremos aqui, pelas razões supras.

3. O **axioma do par** diz que dados conjuntos x e y existe um conjunto z cujos elementos são exactamente x e y . Pelo axioma da extensionalidade, este conjunto z é único, e denotamo-lo por $\{x, y\}$. Note que x e y podem ser o mesmo conjunto, caso em que ficamos com o conjunto *singular* $\{x\}$.

A noção de *par ordenado* pode definir-se em teoria dos conjuntos a partir da noção de par acima. Uma possível maneira de o fazer é a seguinte, devida a Kazimierz Kuratowski:

Definição 10. *Dados x e y define-se o par ordenado (x, y) como sendo o conjunto $\{\{x, y\}, \{x\}\}$.*

Proposição 45. *Se $(x, y) = (z, w)$ então $x = z$ e $y = w$.*

Demonstração. Suponhamos que $\{\{x, y\}, \{x\}\} = \{\{z, w\}, \{z\}\}$. Há dois casos a considerar: $x = y$ ou não. No caso afirmativo, vem $\{\{x\}\} = \{\{z, w\}, \{z\}\}$. Logo, $\{z, w\} = \{z\}$ e, por conseguinte, $z = w$. Sai $\{\{x\}\} = \{\{z\}\}$ e, sucessivamente, $\{x\} = \{z\}$, $x = z$. Logo, $x = y = z = w$. No caso em que $x \neq y$, tem-se necessariamente $\{x, y\} = \{z, w\}$ e $z \neq w$. Como $\{x\}$ é singular e $\{z, w\}$ não é, infere-se que $\{x\} = \{z\}$. Logo $x = z$. Ora, $y \in \{x, y\} = \{z, w\} = \{x, w\}$. Vem $y = w$. \square

4. O **axioma da união** diz que dado um conjunto z existe um conjunto cujos elementos são exactamente os *elementos de elementos* de z . Em símbolos, existe o conjunto $\{x : \exists v (v \in z \wedge x \in v)\}$. Pelo axioma da extensionalidade este conjunto é único. Denotamo-lo por $\bigcup z$.

O conjunto $\bigcup\{x, y\}$ denota-se habitualmente por $x \cup y$.

Exercício 53. *Mostre que a classe de todos os conjuntos singulares é uma classe própria.*

Uma *função* f é um conjunto de pares ordenados com a seguinte propriedade:

$$(x, y) \in f \wedge (x, z) \in f \rightarrow y = z.$$

O *domínio* da função f , denotado por $\text{dom}f$, é o conjunto $\{x : \exists y (x, y) \in f\}$. Note-se que este conjunto existe por separação, pois é o conjunto

$$\{x \in \bigcup \bigcup f : \exists y (x, y) \in f\}.$$

Dada f uma função e $x \in \text{dom}f$, existe um e um só elemento y tal que $(x, y) \in f$: como é costume, este elemento denota-se por $f(x)$. A *imagem* da função f , denotada por $\text{im}f$, é o conjunto $\{y : \exists x (x, y) \in f\}$ (este conjunto existe por separação: exercício). Como se sabe, uma função diz-se *injectiva* se se verifica o seguinte condicional: $f(x) = f(y) \rightarrow x = y$. Com estas definições não faz sentido definir a noção de *sobrejectividade*. Para que isso faça sentido tem que se especificar um conjunto de chegada B . Por vezes apresentam-se as funções especificando um conjunto de partida A , um conjunto de chegada B e a função propriamente dita f (i.e., o conjunto dos pares ordenados), em que $\text{dom}f = A$. Diz-se então que f é uma função de A em B e escreve-se $f : A \mapsto B$. Nestas circunstâncias já faz sentido dizer que f é sobrejectiva: é dizer que $\text{im}f = B$. Há quem reserve o termo ‘aplicação’ quando se especifica o conjunto de chegada (o conjunto de partida é, automaticamente, $\text{dom}f$), enquanto que o termo ‘função’ ficaria adstrito apenas ao conjunto dos pares ordenados. Nas presentes notas usamos indiferentemente a terminologia ‘função’ e ‘aplicação’, sendo claro pelo contexto aquilo a que nos referimos.

5. O **axioma das partes** diz que dado um conjunto z existe um conjunto cujos elementos são exactamente os subconjuntos de z . Em símbolos, existe o conjunto $\{x : x \subseteq z\}$. Pelo axioma da extensionalidade este conjunto é único. Como tem sido feito, denotamo-lo por $\mathcal{P}(z)$.

Dados conjuntos A e B , o *produto cartesiano* $A \times B$ é o conjunto $\{(x, y) : x \in A \wedge y \in B\}$. Este conjunto existe por separação pois é o conjunto

$$\{u \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists x \exists y (x \in A \wedge y \in B \wedge u = (x, y))\}.$$

Exercício 54. *Dados conjuntos A e B , mostre que existe o conjunto A^B de todas as funções de B para A .*

Exercício 55. *Dado um conjunto A e $R \subseteq A \times A$ uma relação de equivalência em A , mostre que existe o conjunto cociente A/R .*

Nenhum dos axiomas até agora garante a existência de conjuntos infinitos. Ora, é essencial que existam conjuntos infinitos em Matemática, pois as suas estruturas centrais – os números naturais e os números reais – são infinitas. O que vão ser os números naturais em teoria dos conjuntos? Há várias maneiras de responder a esta questão, mas uma – devida a von Neumann – é particularmente perspicaz (e, além disso, generaliza-se de modo a se obter os *números ordinais*). Vamos tomar cada número natural como o conjunto dos seus predecessores. Deste modo, o número zero é o conjunto vazio \emptyset . O número 1 é o conjunto

$\{0\}$. O número 2 é o conjunto $\{0, 1\}$, o 3 é o conjunto $\{0, 1, 2\}$, etc. Em geral, o sucessor do número n é o conjunto $n \cup \{n\}$. O seguinte axioma garante que todos estes “números” se podem aglomerar num conjunto:

6. O **axioma do infinito** diz que existe um conjunto I que tem o conjunto vazio \emptyset como elemento e que, sempre que tem um elemento x então também tem o elemento $x \cup \{x\}$. I.e., existe um conjunto I tal que

$$\emptyset \in I \wedge \forall x(x \in I \rightarrow x \cup \{x\} \in I).$$

Um conjunto que verifica a condição acima diz-se *indutivo* com respeito a \emptyset e à operação $x \rightsquigarrow x \cup \{x\}$. Nesta terminologia, o axioma do infinito diz que existe um conjunto indutivo.

É fácil de ver que podemos tomar a intersecção de todos os conjuntos indutivos. Com efeito, fixe-se I um conjunto indutivo. A intersecção procurada obtém-se agora por separação. É o conjunto

$$\{x \in I : \forall X(X \text{ é indutivo} \rightarrow x \in X)\}.$$

Por extensionalidade, este conjunto é único e denota-se por ω . Claramente, ω é indutivo. Além disso, ω é o menor conjunto nestas condições:

$$\forall X(\emptyset \in X \wedge \forall u(u \in X \rightarrow u \cup \{u\} \in X) \rightarrow \omega \subseteq X).$$

Denote-se por $S(x)$ o conjunto $x \cup \{x\}$. Podemos ver S como uma função de ω para ω , nomeadamente como o conjunto de pares ordenados $\{(x, y) \in \omega \times \omega : y = x \cup \{x\}\}$.

Lema 6. *Se $x \in \omega$ e $y \in x$ então $y \subseteq x$.*

Demonstração. Vamos mostrar que $X := \{x \in \omega : \forall y(y \in x \rightarrow y \subseteq x)\}$ é um conjunto indutivo, o que nos resolve o problema. Claramente, $\emptyset \in X$. Suponhamos que $x \in X$. Seja $y \in S(x)$. Se $y \in x$ então $y \subseteq x$ e, *a fortiori*, $y \subseteq S(x)$. Caso $y = x$, tem-se imediatamente, $y \subseteq S(x)$. \square

Exercício 56. *Mostre que se $x \in \omega$ então $x \subseteq \omega$.*

Proposição 46. *O triplo (ω, S, \emptyset) é uma estrutura de Dedekind-Peano.*

Demonstração. Claro que $S(x) \neq \emptyset$, pois $x \in S(x)$. A terceira propriedade das estruturas de Dedekind-Peano é imediata. Finalmente, suponhamos que $x, y \in \omega$ e $S(x) = S(y)$. Suponhamos, com vista a um absurdo, que $x \neq y$. Como $y \in S(y)$ sai $y \in x \cup \{x\}$. Logo, $y \in x$. Pelo lema anterior, $y \subseteq x$. Por um argumento simétrico, também se conclui que $x \subseteq y$. Logo $x = y$. \square

Com este resultado fechamos um círculo. O leitor pode convencer-se de que o desenvolvimento dos sistemas numéricos (números inteiros, racionais e reais) que efectuámos se pode formalizar na teoria de Zermelo constituída pelos seis axiomas discutidos. Um dos mais pasmosos legados da matemática do primeiro quartel do século passado é o facto de toda a matemática usual se poder formalizar num sistema dedutivo com apenas estes axiomas, juntamente com o axioma da escolha.

De agora em diante, quando falarmos de números naturais estamos a referir-nos aos elementos de ω .

Exercício 57. *Mostre que, na estrutura de Dedekind-Peano (ω, S, \emptyset) , se tem a equivalência: $x \in y \leftrightarrow x < y$. Conclua que se $x \in \omega$, então $x = \{y \in \omega : y < x\}$.*

Chapter 17

A teoria ZFC

No capítulo anterior distinguimos entre conjuntos e classes próprias. Estas últimas correspondem a propriedades bem-determinadas (dadas por fórmulas) que não dão origem a conjuntos. Para o que se segue devemos distinguir entre funções (*conjuntos* de pares ordenados) e, à falta de melhor nome, *operações*. Uma operação (unária) é dada por uma propriedade (binária) bem-determinada $P(x, y)$ para a qual se tem $\forall x \exists^1 y P(x, y)$. Por exemplo, a operação que a cada conjunto x faz corresponder o conjunto singular $\{x\}$ advém da propriedade $P(x, y)$ dada pela fórmula $\forall z (z \in y \leftrightarrow z = x)$. Note que não podemos considerar a operação $x \rightsquigarrow \{x\}$ como sendo uma *função* – um determinado conjunto de pares ordenados – pela simples razão que o seu “domínio” é a classe universal. Há muitos exemplos de operações úteis: $x \rightsquigarrow \bigcup x$, $x \rightsquigarrow \mathcal{P}(x)$, etc.

Exercício 58. *Mostre que $x \rightsquigarrow \{z \in x : z \notin z\}$ é uma operação que associa a cada conjunto x um conjunto que não é seu elemento.*

Por vezes, convém considerar operações restritas a uma certa classe. Não se perde generalidade por considerar o domínio da operação o universo inteiro, pois uma operação definida apenas numa sub-classe do universo pode estender-se facilmente a todo o universo (p. ex., fazendo corresponder o conjunto vazio aos conjuntos fora da sub-classe dada). Também se podem considerar operações binárias (poliádicas, em geral), tais como $x, y \rightsquigarrow \{x, y\}$ ou $x, y \rightsquigarrow x \times y$.

7. O **axioma da substituição** diz que dada uma operação $x \rightsquigarrow F(x)$ e um conjunto A , a imagem $F[A]$, constituída pelos elementos que são da forma $F(x)$ para algum $x \in A$, é um conjunto. Assim, o axioma permite formar o conjunto $\{y : \exists x \in A (y = F(x))\}$ ou, noutra notação, o conjunto $\{F(x) : x \in A\}$. Dito de outro modo (o qual explica o nome do axioma): se se *substituir* cada elemento x dum dado conjunto A por $F(x)$ obtém-se ainda assim um conjunto.

Nas condições das hipóteses do axioma da substituição, podemos formar o conjunto $\{z \in A \times F[A] : \exists x \exists y (z = (x, y) \wedge y = F(x))\}$. De facto, este conjunto é uma função: aquela que a cada elemento x de A faz corresponder o elemento $F(x)$. Note-se que esta função existe porque o axioma da substituição garante que $F[A]$ é um conjunto. Se nos permitirmos liberdades de expressão, podemos

enunciar o axioma da substituição do seguinte modo: uma operação restrita a um conjunto é uma função.

O axioma da substituição foi formulado por Abraham Fraenkel nos anos vinte do século passado e constitui um novo princípio, independente dos até agora formulados. Como veremos, este axioma desempenha um papel essencial no desenvolvimento da teoria dos ordinais de von Neumann.

Exercício 59. *Mostre que, na presença do axioma da substituição e do axioma do conjunto vazio, o axioma da separação é redundante.*

Exercício 60. *Mostre que, na presença dos axiomas até agora discutidos, o axioma do par é redundante.*

A seguinte consequência do axioma da substituição é muito útil:

Proposição 47. *Seja $x \rightsquigarrow F(x)$ uma operação e C uma classe própria. Suponhamos que F é injectiva em C . Então $F[C]$ também é uma classe própria.*

Demonstração. Suponhamos, com vista a um absurdo, que se pode formar o conjunto

$$z := \{y : \exists x(C(x) \wedge F(x) = y)\}.$$

Defina-se a operação $y \rightsquigarrow G(y)$ que, nos elementos y do conjunto z faz corresponder o único elemento x de C tal que $F(x) = y$ (nos restantes conjuntos faz corresponder o conjunto \emptyset). Pelo axioma da substituição, $G[z]$ é um conjunto. Mas os elementos de $G[z]$ são exactamente os elementos que estão na classe C . Isto contradiz a hipótese de que C é uma classe própria. \square

Será que podem existir conjuntos x tais que $x \in x$? Ou, mais geralmente, conjuntos $x, y_0, y_1, \dots, y_{n-1}$ em “círculo” $x \in y_0 \in y_1 \in \dots \in y_{n-1} \in x$? Como iremos discutir mais tarde, o seguinte axioma espelha a denominada “visão cumulativa” do universo dos conjuntos. Além disso, impede os casos “patológicos” referidos:

8. O **axioma da fundação** diz que dado um conjunto não vazio x existe um elemento $y \in x$ tal que $x \cap y = \emptyset$. Numa forma mais mnemónica: todo o conjunto não vazio tem um elemento minimal para a relação \in .

Exercício 61. *Mostre que, com o axioma da fundação, os casos patológicos descritos acima não se podem dar.*

Exercício 62. *Um conjunto x diz-se mal-fundado se existir uma função f de domínio ω tal que, $f(0) = x$ e, para todo $n \in \omega$, $f(n+1) \in f(n)$. Mostre que, na presença do axioma da fundação, não existem conjuntos mal-fundados.*

Os axiomas (1) a (8) acima constituem a teoria ZF de Zermelo-Fraenkel. A teoria ZFC obtém-se de ZF adicionando o axioma da escolha (o ‘C’, de *choice*, da sigla ‘ZFC’). A nossa formulação oficial deste axioma é:

9. O **axioma da escolha** diz que dados conjuntos X e Y e $P \subseteq X \times Y$ então

$$\forall x \in X \exists y \in Y [(x, y) \in P] \rightarrow \exists f \in Y^X \forall x \in X [(x, f(x)) \in P].$$

Este axioma abrevia-se pela sigla AC.

Exercício 63. *Mostre que em Z o axioma da escolha é equivalente à existência de funções escolhas para todos os conjuntos.*

Exercício 64. *Mostre que em Z o axioma da escolha é equivalente à existência de conjuntos de representantes para as relações de equivalência.*

O axioma da escolha numerável, de sigla AC_ω , é o caso particular do axioma da escolha em que X é ω :

$$\forall n \in \omega \exists y \in Y [(n, y) \in P] \rightarrow \exists f \in Y^\omega \forall n \in \omega [(n, f(n)) \in P].$$

O axioma das escolhas dependentes, de sigla DC, é o postulado que diz que, dados X um conjunto, $a \in X$ e $P \subseteq X \times X$ tais que $\forall x \in X \exists y \in X [(x, y) \in P]$, então existe uma função $f : \omega \rightarrow X$ tal que:

$$f(0) = a \wedge \forall n \in \omega [(f(n), f(n+1)) \in P].$$

Exercício 65. *Mostre que na presença de DC, o axioma da fundação é equivalente à inexistência de conjuntos mal-fundados (ver um exercício acima para a terminologia e para uma das direcções).*

Proposição 48. *A teoria Z demonstra as implicações: $AC \rightarrow DC \rightarrow AC_\omega$.*

Demonstração. Admita-se AC. Sejam dados X , $a \in X$ e $P \subseteq X \times X$ tais que $\forall x \in X \exists y \in X [(x, y) \in P]$. Pelo axioma da escolha, tome-se ϵ_X uma função escolha para X . Define-se $f : \omega \rightarrow X$ por recursão do seguinte modo: $f(0) = a$ e $f(n+1) = \epsilon_X(\{y \in X : (f(n), y) \in P\})$. Claramente, f satisfaz os requisitos pretendidos.

Suponhamos agora DC e admitamos o antecedente de AC_ω . Tome-se $X = \omega \times Y$ e defina-se a relação $Q \subseteq X \times X$ por

$$Q := \{((n, y), (m, z)) \in X \times X : m = n + 1 \wedge (m, z) \in P\}.$$

Claro que $\forall a \in X \exists b \in X [(a, b) \in Q]$. Fixe-se $y_0 \in Y$ com $(0, y_0) \in P$. Por DC, existe $h : \omega \rightarrow X$ tal que $h(0) = (0, y_0)$ e $(h(n), h(n+1)) \in Q$, para todo $n \in \omega$. Por construção, $h(n) \in P$, para todo $n \in \omega$. Seja $h(n) = (h_1(n), h_2(n))$. Ora, vê-se facilmente por indução que h_1 é a função identidade. Logo, h_2 é a função desejada. \square

O axioma da escolha AC é consistente relativamente a ZF. Isto quer dizer que se o sistema axiomático ZF é consistente, então ZFC também é consistente. Este resultado é consequência dos trabalhos de Gödel em 1938. A demonstração de Gödel é do mesmo género das demonstrações de consistência das geometrias não-Euclidianas relativamente à geometria Euclideana. Por exemplo, o disco de Klein mostra que se podem interpretar os termos primitivos da geometria planar Euclideana de modo a mostrar que os axiomas da geometria de Lobatchevski valem no disco de Klein. Assim, se aceitarmos a consistência da geometria Euclideana, necessariamente temos que aceitar a consistência da geometria de Lobatchevski. De modo semelhante, Gödel define um modelo *interno* em ZF a que deu o nome de *universo construtível* e mostrou, em ZF, que a axiomática ZFC vale no universo construtível, obtendo assim o resultado de consistência relativa há pouco mencionado.

Com os resultados de Gödel ficou ainda em aberto a possibilidade de ZF demonstrar o axioma da escolha. Apenas na sequência dos trabalhos de Cohen em 1963, inventor duma técnica de construção de modelos da teoria dos conjuntos conhecida por *método do forcing*, se demonstrou (através de *modelos simétricos*) que as teorias

$$\text{ZF} + \neg\text{AC}_\omega, \text{ZF} + \text{AC}_\omega + \neg\text{DC}, \text{ZF} + \text{DC} + \neg\text{AC}$$

são teorias consistentes relativamente a ZF.

As demonstrações destes resultados requerem técnicas de Lógica Matemática e não cabem numa introdução à teoria dos conjuntos.

rascunho

Chapter 18

Boas ordens

Definição 11. Uma boa ordem é uma ordem total estrita $(X, <)$ tal que todo o subconjunto não vazio de X tem mínimo para a relação \leq .

O conjunto dos números naturais ω munido da ordem usual (que, nos números naturais de von Neumann, é dada pela relação de pertença) constitui uma boa ordem. Para todo o número natural de von Neumann $n \in \omega$, n munido da relação de pertença é uma boa ordem finita. Dada uma boa ordem $(X, <)$ e dado $\mu \notin X$, podemos definir a seguinte boa ordem \prec em $X \cup \{\mu\}$:

$$x \prec y \iff (x, y \in X \wedge x < y) \vee (x \in X \wedge y = \mu).$$

Informalmente, a ordem $(X \cup \{\mu\}, \prec)$ obtém-se de $(X, <)$ colocando um novo elemento μ “à frente” de todos os elementos de X .

A seguinte boa ordem vai ser útil mais tarde:

Proposição 49. Seja $(X, <)$ uma boa ordem. Defina-se a relação $<_G$ em $X \times X$ em que $(x, y) <_G (x', y')$ se, e somente se:

$$[\max(x, y) < \max(x', y')] \vee [\max(x, y) = \max(x', y') \wedge x < x'] \\ \vee [\max(x, y) = \max(x', y') \wedge x = x' \wedge y < y']$$

A relação $<_G$ é uma boa ordem, denominada de ordem de Gödel em $X \times X$.

Demonstração. É fácil de ver que $<_G$ é uma ordem total. Seja Z um subconjunto não vazio de $X \times X$. Considere-se o seguinte subconjunto não vazio de X :

$$\{w \in X : \exists x, y ((x, y) \in Z \wedge \max(x, y) = w)\}.$$

Tome-se w_0 o mínimo elemento deste conjunto. Considere-se agora o subconjunto não vazio de X :

$$\{x \in X : \exists y ((x, y) \in Z \wedge \max(x, y) = w_0)\}.$$

Tome-se x_0 o mínimo elemento deste conjunto. Finalmente, tome-se o subconjunto não vazio de X : $\{y \in X : (x_0, y) \in Z \wedge \max(x_0, y) = w_0\}$. Seja y_0 o mínimo elemento deste conjunto. Pode agora argumentar-se sem dificuldade que (x_0, y_0) é o menor elemento de Z para a ordem \leq_G . \square

Toda a boa ordem não vazia $(X, <)$ tem um elemento mínimo, geralmente denotado por 0_X , ou simplesmente por 0 . Dado um elemento x de X que não seja máximo, podemos considerar o mínimo do conjunto $\{z \in X : x < z\}$. A este elemento chama-se o *sucessor* de x e denota-se por $S_X(x)$ ou, quando não há ambiguidade, por $S(x)$.

Exercício 66. *Nas condições acima, mostre que $w < S(x)$ se, e somente se, $w \leq x$.*

Um elemento x duma boa ordem $(X, <)$ diz-se um elemento *limite* se não for o elemento mínimo nem for um elemento sucessor.

Exercício 67. *Nas condições acima, mostre que x é limite se, e somente se, $0 < x$ e $\forall z(z < x \rightarrow \exists w(z < w < x))$.*

Recorde a definição de segmento inicial do Capítulo 6. Se $y \in X$, então o conjunto $X_{<y}$ definido por $\{x \in X : x < y\}$ é um segmento inicial de $(X, <)$.

Proposição 50. *Seja $(X, <)$ uma boa ordem e I um segmento inicial próprio de X (i.e., I não é todo o X). Então existe $y \in X$ tal que $I = X_{<y}$.*

Demonstração. Como $I \subsetneq X$, tome-se y_0 o elemento mínimo de $X \setminus I$. Vamos argumentar que $I = X_{<y_0}$. Se $x \notin I$, vem $y_0 \leq x$ por minimalidade de y_0 . Logo, $x \notin X_{<y_0}$. Reciprocamente, se $y_0 \leq x$, não se pode ter $x \in I$ pois então viria $y_0 \in I$ por definição de segmento inicial. \square

Exercício 68. *Seja $(X, <)$ uma boa ordem que tenha elementos limite. Seja x o menor elemento limite de X . Mostre que $X_{<x}$ é, de forma natural, uma estrutura de Dedekind-Peano.*

Definição 12. *Sejam $(X, <)$ e (Y, \prec) duas boas ordens. Diz-se que uma função $f : X \mapsto Y$ é estritamente crescente se,*

$$\forall x, x' \in X (x < x' \rightarrow f(x) \prec f(x')).$$

Não é difícil de argumentar que se f é estritamente crescente então f é injectiva e tem-se mesmo o bicondicional $\forall x, x' \in X (x < x' \leftrightarrow f(x) \prec f(x'))$.

Proposição 51. *Seja $f : X \mapsto X$ uma função estritamente crescente duma boa ordem $(X, <)$ para si própria. Então, para todo $x \in X$, $x \leq f(x)$.*

Demonstração. Admitamos, com vista a um absurdo, que existe $x \in X$ tal que $f(x) < x$. Tome-se x_0 mínimo nestas circunstâncias. Seja $y_0 = f(x_0)$. Note que $y_0 < x_0$ e, por monotonicidade estrita, $f(y_0) < y_0$. Ora, isto contradiz a minimalidade de x_0 . \square

Corolário 8. *Seja $(X, <)$ uma boa-ordem e $f : X \mapsto X$ uma função estritamente crescente. Então $\text{im} f$ não está contida num segmento inicial próprio de X .*

Definição 13. *Um isomorfismo entre boas ordens $(X, <)$ e (Y, \prec) é uma bijecção $f : X \mapsto Y$ estritamente crescente. Duas boas ordens $(X, <)$ e (Y, \prec) dizem-se isomorfas se existir um isomorfismo entre elas, e escreve-se $(X, <) =_o (Y, \prec)$, ou simplesmente $X =_o Y$ desde que as boas ordens estejam implícitas.*

Corolário 9. *Nenhuma boa ordem é isomorfa a um seu segmento inicial próprio.*

Chapter 19

Indução e recursão transfinita

Como já vimos, existem princípios de indução e recursão na estrutura dos números naturais. As boas ordens são estruturas para as quais estes princípios, devidamente adaptados, também se aplicam.

Proposição 52 (Princípio da indução transfinita). *Seja $(X, <)$ uma boa ordem e Z um subconjunto de X . Se, para todo o elemento $x \in X$, se tiver o condicional $(\forall y < x (y \in Z)) \rightarrow x \in Z$ (condição de progressão), então $Z = X$.*

Demonstração. A demonstração é análoga ao princípio da indução completa em ω , usando a existência de mínimos de conjuntos não vazios. \square

Teorema (Princípio da recursão transfinita). *Seja $(X, <)$ uma boa ordem e $w, y \rightsquigarrow F(w, y)$ uma operação binária bem-determinada. Então existe exactamente uma função h de domínio X que verifica a seguinte propriedade recursiva: para todo $x \in X$,*

$$h(x) = F(h \upharpoonright_{X_{<x}}, x).$$

Demonstração. Considere-se o conjunto Z dos elementos $z \in X$ para os quais existe uma função σ_z de domínio $X_{<z} \cup \{z\}$ tal que

$$\sigma_z(x) = F(\sigma_z \upharpoonright_{X_{<x}}, x),$$

para todo $x \leq z$. Esta função é necessariamente única. Com efeito, dada também uma função $\hat{\sigma}_z$ de domínio $X_{<z} \cup \{z\}$ tal que $\hat{\sigma}_z(x) = F(\hat{\sigma}_z \upharpoonright_{X_{<x}}, x)$, para todo $x \leq z$, vê-se imediatamente por indução transfinita em x que, para todo $x \leq z$, se tem $\sigma_z(x) = \hat{\sigma}_z(x)$.

Vamos ver que este conjunto Z é todo o X . Se não fosse, existiria um elemento mínimo z_0 que não estaria no conjunto. Pelo axioma da substituição, existe o conjunto $\{\sigma_z : z < z_0\}$. Trata-se de um conjunto de funções em cadeia (i.e., dadas duas funções neste conjunto, uma delas é subconjunto da outra). A união deste conjunto, que designamos por f , é uma *função* cujo domínio é $\{x \in X : x < z_0\}$. Por construção, $f(x) = F(f \upharpoonright_{X_{<x}}, x)$, para todo $x \in \text{dom} f$. Assim, o conjunto $f \cup \{(z_0, F(f, z_0))\}$ é uma função de domínio $X_{<z_0} \cup \{z_0\}$ que verifica a propriedade de recursão, o que contradiz a definição de z_0 .

Definimos, pois, uma operação $z \rightsquigarrow \sigma_z$ em todo o elemento z de X . Pelos axiomas da substituição e da união, $\bigcup_{z \in X} \sigma_z$ é um conjunto e, claramente, uma função de domínio X . Claro que esta é a função h desejada.

A unicidade da função h é clara por indução transfinita. \square

Quando aplicamos o princípio da recursão transfinita a ω obtemos facilmente uma generalização do princípio da recursão dos números naturais:

Corolário 10. *Fixe-se a um conjunto e seja $x \rightsquigarrow F(x)$ uma operação bem-determinada. Então existe exactamente uma função h de domínio ω tal que $h(0) = a$ e, para todo $n \in \omega$, $h(n+1) = F(h(n))$.*

Exercício 69. *Justifique rigorosamente o corolário anterior.*

Exemplo. Dada a operação $x \rightsquigarrow \mathcal{P}(x)$, pelo corolário anterior existe uma função f de domínio ω tal que $f(0) = \omega$ e $f(n+1) = \mathcal{P}(f(n))$. Intuitivamente, $\text{im} f$ é o conjunto $\{\omega, \mathcal{P}(\omega), \mathcal{P}(\mathcal{P}(\omega)), \dots\}$.

O corolário anterior tem uma aplicação teórica importante pois permite definir o *fecho transitivo* dum dado conjunto.

Definição 14. *Um conjunto x diz-se transitivo se sempre que $y \in x$ então $y \subseteq x$.*

O conjunto $\{\{\emptyset\}\}$ não é transitivo. Pelo Lema 6, os elementos de ω são conjuntos transitivos. Pelo exercício 56, ω é um conjunto transitivo.

Exercício 70. *Mostre as seguintes propriedades:*

- (a) *Se x é um conjunto transitivo então $S(x)$ também é transitivo.*
- (b) *Se x e y são conjuntos transitivos então $x \cap y$ também é transitivo.*
- (c) *Se x é um conjunto transitivo então $\mathcal{P}(x)$ também é transitivo.*
- (d) *Se cada elemento dum conjunto X é transitivo, então $\bigcup X$ é transitivo.*

Definição 15. *Fixe-se x um conjunto. Define-se por recursão $TC_0(x) = x$ e $TC_{n+1}(x) = \bigcup TC_n(x)$. O fecho transitivo de x , denotado por $TC(x)$, é o conjunto $\bigcup_{n \in \omega} TC_n(x)$.*

O Corolário 10 é aqui usado através da operação $x \rightsquigarrow \bigcup x$. Intuitivamente, $TC(x)$ é $x \cup \bigcup x \cup \bigcup \bigcup x \cup \bigcup \bigcup \bigcup x \cup \dots$ constituído pelos elementos de x , os elementos dos elementos de x , os elementos dos elementos dos elementos de x e por aí adiante. Rigorosamente, dado um conjunto x , se denotarmos por f a função que a cada número natural n faz corresponder o conjunto $TC_n(x)$, então $TC(x)$ é $\bigcup \text{im} f$.

Proposição 53. *Dado um conjunto x , $TC(x)$ é um conjunto transitivo tal que $x \subseteq TC(x)$. Além disso, se z é um conjunto transitivo tal que $x \subseteq z$, então $TC(x) \subseteq z$.*

Demonstração. Claramente, $x \subseteq TC(x)$. Seja $y \in TC(x)$ e considere-se $w \in y$. Para algum $n \in \omega$ tem-se $y \in TC_n(x)$. Logo $w \in \bigcup TC_n(x)$, i.e., $w \in TC_{n+1}(x)$ e, portanto, $w \in TC(x)$. Para a segunda parte, demonstre-se facilmente, por indução em n , que $TC_n(x) \subseteq z$, para todo $n \in \omega$. Logo, $TC(x) \subseteq z$. \square

Chapter 20

Ordinais de von Neumann

Definição 16. Um ordinal de von Neumann ou, simplesmente, um ordinal, é um conjunto transitivo α tal que, para quaisquer elementos diferentes x e y de α , se tem $x \in y$ ou $y \in x$.

Na teoria dos conjuntos, usualmente reservam-se as letras minúsculas do início alfabeto grego para denotar ordinais. O seguinte é um exercício:

Proposição 54. Têm-se as seguintes propriedades.

- (a) \emptyset é um ordinal (também se escreve 0 em vez de \emptyset).
- (b) Se α é um ordinal, então $S(\alpha)$ é um ordinal.
- (c) Se α e β são ordinais, então $\alpha \cap \beta$ é um ordinal.

Note que todo o elemento de ω é um ordinal e que o próprio ω é um ordinal. Dado um ordinal α , podemos considerar a relação $\{(x, y) \in \alpha \times \alpha : x \in y\}$ em α , a que chamamos a relação de ‘pertença’ em α .

Proposição 55. Um ordinal munido da relação de ‘pertença’ constitui uma boa ordem.

Demonstração. Seja dado α um ordinal. A relação de ‘pertença’ em α é anti-reflexiva pelo axioma da fundação e é tricotómica por definição de ordinal. Para ver que é uma ordem total basta ver que é uma relação transitiva. Sejam $x, y, z \in \alpha$ com $x \in y$ e $y \in z$. Pelo axioma da fundação não se pode ter $x = z$. Logo, por definição de ordinal, $x \in z$ ou $z \in x$. Novamente pelo axioma da fundação, $z \in x$ é impossível. Resta $x \in z$.

Finalmente, temos que ver que todo o subconjunto não vazio X de α tem elemento mínimo para a relação de ‘pertença’. Pelo axioma da fundação, seja $x \in X$ tal que $x \cap X = \emptyset$. Vamos ver que x é o elemento mínimo de X para a relação de ‘pertença’. Tome-se $y \in X$ com $y \neq x$. Visto que $x \cap X = \emptyset$, não se pode ter $y \in x$. Resta $x \in y$, como se queria. \square

Corolário 11. Todo o elemento dum ordinal é um ordinal.

Demonstração. Seja α um ordinal e $x \in \alpha$. Como α é um conjunto transitivo e a relação de ‘pertença’ em α é transitiva, x é um conjunto transitivo. Por sua vez, o facto de que x é subconjunto de α claramente implica que quaisquer dois elementos de x são comparáveis com respeito à relação de ‘pertença’. \square

De ora em diante em diante, quando tratarmos um ordinal α como uma boa ordem, consideramo-lo munido da relação de ‘pertença’.

Lema 7. *Sejam α e β ordinais. Então, $\beta \subsetneq \alpha$ se, e somente se, $\beta \in \alpha$.*

Demonstração. Suponhamos que $\beta \subsetneq \alpha$. Por transitividade de β , β é um segmento inicial de α . Logo, existe $x \in \alpha$ tal que $\beta = \{z \in \alpha : z \in x\}$. Mas, claramente, $\{z \in \alpha : z \in x\} = x$. Logo, $\beta \in \alpha$. O recíproco é imediato por transitividade de α e por fundação. \square

Proposição 56. *Sejam α e β ordinais diferentes. Então $\alpha \in \beta$ ou $\beta \in \alpha$.*

Demonstração. Sejam α e β ordinais diferentes. Se $\alpha \subseteq \beta$, então pelo lema anterior, $\alpha \in \beta$. Se $\beta \subseteq \alpha$, vem $\beta \in \alpha$. Caso contrário, $\alpha \cap \beta \subsetneq \alpha$ e $\alpha \cap \beta \subsetneq \beta$. Ora, $\alpha \cap \beta$ é um ordinal. Logo, pelo lema anterior, vem $\alpha \cap \beta \in \alpha$ e $\alpha \cap \beta \in \beta$. Vem $\alpha \cap \beta \in \alpha \cap \beta$, o que é impossível pelo axioma da fundação. \square

Corolário 12. *Se $\alpha \neq \beta$ então $\alpha \neq_o \beta$.*

Demonstração. Sem perda de generalidade, $\beta \in \alpha$. Sai $\beta \subsetneq \alpha$. Claramente, β é um segmento inicial próprio de α e, portanto, não é isomorfo a α . \square

Seja Ord a classe dos ordinais. Pelo que vimos, a relação de ‘pertença’ em Ord tem as propriedades de ordem total. Comumente, para ordinais α e β , escreve-se $\alpha < \beta$ em vez de $\alpha \in \beta$. Pelo Lema 7, tem-se $\alpha \leq \beta$ se, e somente se, $\alpha \subseteq \beta$. Note que, à semelhança dos ordinais de von Neumann finitos, cada ordinal α coincide com o conjunto dos seus predecessores, i.e., $\alpha = \{\beta : \beta < \alpha\}$.

Exercício 71. *Se X é um conjunto de ordinais então $\bigcup X$ é um ordinal. Mostre que $\bigcup X$ é o menor dos ordinais que majoram X (dito de outro modo, todo o conjunto X de ordinais tem supremo sendo este supremo o ordinal $\bigcup X$).*

Proposição 57 (Burali-Forti). *A classe Ord é uma classe própria.*

Demonstração. Se Ord fosse um conjunto então, pelo que vimos, Ord seria um ordinal de von Neumann. Viria $Ord \in Ord$, o que contradiz o axioma da fundação. \square

Corolário 13. *Seja C uma classe de ordinais tal que $\forall \alpha \exists \beta (\alpha < \beta \wedge C(\beta))$. Então C é uma classe própria.*

Demonstração. Suponhamos que C é um conjunto z . Vamos ver que o conjunto $\bigcup z$ é constituído por todos os ordinais, o que é um absurdo. Com efeito, dado α um ordinal qualquer, tome-se β tal que $\alpha < \beta$ e $C(\beta)$. Logo, $\alpha \in \beta \wedge \beta \in z$. Sai $\alpha \in \bigcup z$. \square

Corolário 14. *Seja dada uma operação $x \rightsquigarrow F(x)$ com valores nos ordinais. Fixe-se A um conjunto. Então $\exists \beta \forall x \in A (F(x) < \beta)$.*

Demonstração. Pelo axioma da substituição pode formar-se o conjunto $F[A]$ dos ordinais da forma $F(x)$, com $x \in A$. Pelo corolário anterior, existe um ordinal β que majora este conjunto. \square

Lema 8. *Seja C uma sub-classe não vazia da classe dos ordinais. Então C tem elemento mínimo.*

Demonstração. Tome-se α em C . Se α é elemento mínimo de C , já temos o que queremos. Caso contrário, considere-se o conjunto não vazio $\{x \in \alpha : C(x)\}$. Este conjunto tem elemento mínimo como subconjunto da boa ordem α . Este elemento mínimo é o elemento desejado. \square

O seguinte resultado é consequência imediata do Lema 8:

Proposição 58 (Princípio da indução transfinita nos ordinais). *Seja C uma classe de ordinais. Se*

$$(\text{Condição de Progressão}) \quad \forall \alpha ((\forall \beta < \alpha C(\beta)) \rightarrow C(\alpha)),$$

então C é a classe de todos os ordinais.

Os ordinais são de três tipos. Existe o ordinal 0. Há, também, os *ordinais sucessores*, i.e., ordinais da forma $S(\beta)$ para algum ordinal β . Os restantes ordinais são os *ordinais limite*.

Exercício 72. *Seja α um ordinal limite. Mostre que $\sup \alpha = \alpha$. O que se passa quando α não é ordinal limite?*

É útil ter o princípio da indução transfinita nos ordinais na seguinte forma:

Corolário 15. *Seja C uma classe de ordinais. Se*

1. $C(0)$
2. $\forall \alpha (C(\alpha) \rightarrow C(S(\alpha)))$
3. $(\forall \alpha < \gamma C(\alpha)) \rightarrow C(\gamma)$, para γ ordinal limite,

então C é a classe de todos os ordinais.

Demonstração. Basta observar que as condições acima implicam a condição de progressão. \square

Proposição 59 (Princípio da recursão transfinita nos ordinais). *Seja $w, \alpha \rightsquigarrow F(w, \alpha)$ uma operação binária bem-determinada. Então existe uma operação $\alpha \rightsquigarrow H(\alpha)$ tal que, para todo o ordinal α :*

$$H(\alpha) = F(H \upharpoonright_{\alpha}, \alpha),$$

onde $H \upharpoonright_{\alpha}$ é a função que se obtém ao se restringir a operação dada por H ao conjunto α .

Observação. *Note que $H \upharpoonright_{\alpha}$ é uma função graças ao Axioma da Substituição.*

Demonstração. Dado que cada ordinal α é uma boa ordem, pelo princípio da recursão transfinita para boas ordens, existe uma única função h_{α} de domínio α tal que, para todo $\beta < \alpha$:

$$h_{\alpha}(\beta) = F((h_{\alpha}) \upharpoonright_{\beta}, \beta) = F(h_{\beta}, \beta),$$

a última igualdade justificada pela unicidade das funções h_{β} . Definimos, pois, uma operação $\alpha \rightsquigarrow h_{\alpha}$. Agora toma-se simplesmente a operação $\alpha \rightsquigarrow_H h_{S(\alpha)}(\alpha)$. \square

No teorema anterior também se admite que a operação dada por H dependa de parâmetros, i.e., a operação pode ser da forma $w, y \rightsquigarrow H(w, y, p)$, onde p é um valor fixo. Se, por sua vez, $w, y, p \rightsquigarrow H(w, y, p)$ é uma operação *ternária*, ou seja, para cada parâmetro p a operação binária $w, y \rightsquigarrow H(w, y, p)$ está bem definida, então a operação correspondente $\alpha \rightsquigarrow F_p(\alpha)$ é dada por uma *fórmula* com parâmetro p , como facilmente se constata pela demonstração. Ou seja, neste caso temos uma operação *binária* $\alpha, p \rightsquigarrow F_p(\alpha)$. Claro que estas considerações também se aplicam a mais do que um parâmetro.

É conveniente ter o princípio da recursão transfinita na seguinte forma:

Corolário 16. *Fixe-se um conjunto a e sejam $z, \alpha \rightsquigarrow G(z, \alpha)$ e $w, \gamma \rightsquigarrow H(w, \gamma)$ operações. Então existe uma operação $\alpha \rightsquigarrow F(\alpha)$ definida nos ordinais tal que:*

$$\begin{cases} F(0) & = a \\ F(S(\alpha)) & = G(F(\alpha), \alpha) \\ F(\gamma) & = H(F \upharpoonright_{\gamma}, \gamma), \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Demonstração. Basta aplicar a Proposição 59 à operação J definida assim:

$$w, \alpha \rightsquigarrow_J \begin{cases} a & \text{se } \alpha = 0 \\ G(w(\beta), \beta) & \text{se } \alpha \text{ é da forma } S(\beta) \\ H(w, \alpha) & \text{se } \alpha \text{ é ordinal limite} \end{cases}$$

□

Chapter 21

Aritmética ordinal

Proposição 60 (Soma ordinal). *Existe uma operação binária $\alpha, \beta \rightsquigarrow \alpha + \beta$ definida nos ordinais e tomando valores nos ordinais tal que:*

$$\begin{cases} \alpha + 0 & = \alpha \\ \alpha + S(\beta) & = S(\alpha + \beta) \\ \alpha + \gamma & = \sup\{\alpha + \beta : \beta < \gamma\}, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Demonstração. Define-se a soma ordinal por recursão transfinita em β , com parâmetro α . Dado que a operação $x \rightsquigarrow \sup x$ não está definida sempre (faz sentido apenas em conjuntos de ordinais), devemos substituir a terceira cláusula por $\bigcup\{\alpha + \beta : \beta < \gamma\}$. Nestas circunstâncias, temos uma definição correcta por recursão transfinita. Agora, *a posteriori*, vê-se (imediatamente) por indução transfinita, que esta operação toma afinal sempre valores nos ordinais. \square

Adoptamos as terminologias usuais. Assim, 1 é por definição $S(0)$. Vem, claramente, $S(\alpha) = \alpha + 1$, para qualquer ordinal α . Note que a soma ordinal não é comutativa. Por exemplo, $1 + \omega = \sup\{1 + n : n \in \omega\} = \omega \neq \omega + 1$.

Vamos ilustrar o método da demonstração por indução transfinita com a propriedade associativa da adição dos números ordinais.

Lema 9. *Sejam α, β e γ ordinais tais que $\alpha < \beta$. Então, $\gamma + \alpha < \gamma + \beta$.*

Demonstração. Fixemos γ e α . Vamos demonstrar, por indução transfinita em β , o condicional $\alpha < \beta \rightarrow \gamma + \alpha < \gamma + \beta$. O caso $\beta = 0$ é trivial. Se $\beta = S(\delta)$ e $\alpha < \beta$, então $\alpha < \delta$ ou $\alpha = \delta$. No primeiro caso, por hipótese de indução transfinita, $\gamma + \alpha < \gamma + \delta < S(\gamma + \delta) = \gamma + S(\delta) = \gamma + \beta$. No segundo caso, $\gamma + \alpha = \gamma + \delta < S(\gamma + \delta) = \gamma + S(\delta) = \gamma + \beta$.

Resta discutir o caso em que β é ordinal limite. Ora, se $\alpha < \beta$ então existe η tal que $\alpha < \eta < \beta$. Por hipótese de indução transfinita, $\gamma + \alpha < \gamma + \eta$. Por definição de soma ordinal, $\gamma + \eta \leq \gamma + \beta$. Isto mostra o que se quer. \square

Exercício 73. *Mostre que se $\gamma + \alpha < \gamma + \beta$ então $\alpha < \beta$.*

Exercício 74. *Mostre que se $\gamma + \alpha = \gamma + \beta$ então $\alpha = \beta$. O resultado ainda será verdade com as parcelas trocadas?*

Exercício 75. *Suponha que $\alpha \leq \beta$. Mostre que existe um único ordinal γ tal que $\alpha + \gamma = \beta$.*

Lema 10. *Se γ é um ordinal limite então, para todo o ordinal α , $\alpha + \gamma$ também é um ordinal limite.*

Demonstração. Visto que $0 < \gamma$, vem $\alpha + 0 < \alpha + \gamma$. Logo $\alpha + \gamma$ não é o ordinal nulo. Seja agora $\delta < \alpha + \gamma$. Por definição de soma ordinal, existe $\eta < \gamma$ tal que $\delta < \alpha + \eta$. Claro que $\alpha + \eta$ está entre δ e $\alpha + \gamma$. \square

Proposição 61. *Para todos os ordinais α, β, γ tem-se $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Demonstração. Fixam-se α e β e mostra-se a igualdade por indução transfinita em γ . O caso $\gamma = 0$ é claro. O caso sucessor também é fácil de verificar:

$$(\alpha + \beta) + S(\gamma) = S((\alpha + \beta) + \gamma) = S(\alpha + (\beta + \gamma)) = \alpha + S(\beta + \gamma) = \alpha + (\beta + S(\gamma)),$$

onde a segunda igualdade se justifica por hipótese de indução transfinita. Suponhamos agora que γ é ordinal limite e que, para todo $\delta < \gamma$ se tem

$$(\alpha + \beta) + \delta = \alpha + (\beta + \delta).$$

Dado δ com $\delta < \gamma$, pelo Lema 9 tem-se $\beta + \delta < \beta + \gamma$ e $\alpha + (\beta + \delta) < \alpha + (\beta + \gamma)$. Logo, $(\alpha + \beta) + \delta < \alpha + (\beta + \gamma)$. Pela arbitrariedade de δ e por definição de soma ordinal conclui-se a desigualdade $(\alpha + \beta) + \gamma \leq \alpha + (\beta + \gamma)$.

Reciprocamente, tome-se δ arbitrário tal que $\delta < \beta + \gamma$. Vamos ver que $\alpha + \delta \leq (\alpha + \beta) + \gamma$. Dada a arbitrariedade de δ e a definição de some ordinal (atendendo a que $\beta + \gamma$ é ordinal limite), sai a outra desigualdade. Então, dado que $\delta < \beta + \gamma$, por definição de soma ordinal, tome-se $\eta < \gamma$ tal que $\delta < \beta + \eta$. Sai,

$$\alpha + \delta < \alpha + (\beta + \eta) = (\alpha + \beta) + \eta < (\alpha + \beta) + \gamma$$

onde se tem a igualdade acima por hipótese de indução transfinita. \square

De modo análogo à soma ordinal, também se pode definir o produto ordinal:

Proposição 62 (Produto ordinal). *Existe uma operação binária $\alpha, \beta \rightsquigarrow \alpha \cdot \beta$ definida nos ordinais e tomando valores nos ordinais tal que:*

$$\begin{cases} \alpha \cdot 0 & = 0 \\ \alpha \cdot (\beta + 1) & = (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \gamma & = \sup\{\alpha \cdot \beta : \beta < \gamma\}, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Exercício 76. *Calcule $2 \cdot \omega$ e $\omega \cdot 2$.*

Exercício 77. *Mostre que $0 \cdot \alpha = 0$, para todo o ordinal α .*

Lema 11. *Sejam α, β e γ ordinais tais que $\gamma \neq 0$ e $\alpha < \beta$. Então, $\gamma \cdot \alpha < \gamma \cdot \beta$.*

Demonstração. Fixemos α e γ , este último não nulo. Vamos demonstrar, por indução transfinita em β , o condicional $\alpha < \beta \rightarrow \gamma \cdot \alpha < \gamma \cdot \beta$. O caso $\beta = 0$ é trivial. Se $\beta = \delta + 1$ e $\alpha < \beta$, então $\alpha < \delta$ ou $\alpha = \delta$. No primeiro caso, por hipótese de indução transfinita, $\gamma \cdot \alpha < \gamma \cdot \delta < (\gamma \cdot \delta) + \gamma = \gamma \cdot (\delta + 1) = \gamma \cdot \beta$. No segundo caso, $\gamma \cdot \alpha < (\gamma \cdot \alpha) + \gamma = \gamma \cdot (\alpha + 1) = \gamma \cdot \beta$.

Resta discutir o caso em que β é ordinal limite. Ora, se $\alpha < \beta$ então existe η tal que $\alpha < \eta < \beta$. Por hipótese de indução transfinita, $\gamma \cdot \alpha < \gamma \cdot \eta$. Por definição de produto ordinal, $\gamma \cdot \eta \leq \gamma \cdot \beta$. Isto mostra o que se quer. \square

O seguinte lema demonstra-se sem dificuldade:

Lema 12. *Se γ é um ordinal limite então, para todo o ordinal não nulo α , $\alpha \cdot \gamma$ também é um ordinal limite.*

Proposição 63. *Para todos os ordinais α, β, γ tem-se $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.*

Demonstração. Podemos supor que α é não nulo. Agora, fixam-se α e β e mostra-se a igualdade por indução transfinita em γ . Os caso zero e sucessor são fáceis de argumentar. Vamos debruçar-nos sobre o caso em que γ é ordinal limite. Tome-se η arbitrário tal que $\eta < \beta + \gamma$. Por definição de soma ordinal existe δ tal que $\delta < \gamma$ e $\eta < \beta + \delta$. Sai,

$$\alpha \cdot \eta < \alpha \cdot (\beta + \delta) = \alpha \cdot \beta + \alpha \cdot \delta < \alpha \cdot \beta + \alpha \cdot \gamma$$

onde se tem a igualdade acima por hipótese de indução transfinita. Pela arbitrariedade de η e pela definição de produto ordinal, sai $\alpha \cdot (\beta + \gamma) \leq \alpha \cdot \beta + \alpha \cdot \gamma$.

Reciprocamente, tome-se δ ao arbitrário tal que $\delta < \alpha \cdot \gamma$. Vamos ver que $\alpha \cdot \beta + \delta \leq \alpha \cdot (\beta + \gamma)$. Dada a arbitrariedade de δ e a definição de soma ordinal (atendendo a que $\alpha \cdot \gamma$ é ordinal limite), sai a outra desigualdade. Então, dado que $\delta < \alpha \cdot \gamma$, por definição de produto ordinal, tome-se $\eta < \gamma$ tal que $\delta < \alpha \cdot \eta$. Sai,

$$\alpha \cdot \beta + \delta < \alpha \cdot \beta + \alpha \cdot \eta = \alpha \cdot (\beta + \eta) < \alpha \cdot (\beta + \gamma)$$

onde se tem a igualdade acima por hipótese de indução transfinita. \square

Exercício 78. *Será que a distributividade à direita também vale? Justifique.*

Exercício 79. *Mostre que $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.*

Finalmente, também definimos a exponenciação ordinal:

Proposição 64 (Exponenciação ordinal). *Existe uma operação binária $\alpha, \beta \rightsquigarrow \alpha^\beta$ definida nos ordinais (com $\alpha > 1$) e tomando valores nos ordinais tal que:*

$$\begin{cases} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha \\ \alpha^\gamma &= \sup\{\alpha^\beta : \beta < \gamma\}, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Exercício 80. *Sejam α, β e γ ordinais tais que $1 < \gamma$ e $\alpha < \beta$. Mostre que $\gamma^\alpha < \gamma^\beta$.*

Exercício 81. *Seja γ um ordinal limite e $\alpha > 1$. Mostre que α^γ é ordinal limite.*

Nos dois seguintes exercícios, considere que se define 1^β como sendo 1, que 0^0 é 1 e que, para $\beta \neq 0$, 0^β é 0.

Exercício 82. *Mostre que $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$.*

Exercício 83. *Mostre que $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$.*

Exercício 84. *Mostre que se $\alpha, \beta < \omega_1$ então $\alpha + \beta, \alpha \cdot \beta, \alpha^\beta < \omega_1$.*

Chapter 22

O colapso numa boa ordem

Seja $(X, <)$ uma boa ordem. Por recursão transfinita (aplicado à operação $w, y \rightsquigarrow \text{in } w$), existe uma função f de domínio X tal que, para todo $x \in X$,

$$f(x) = \{f(y) : y < x\}.$$

A esta função dá-se o nome de *função colapso* da boa ordem $(X, <)$.

Exercício 85. *Considere uma boa ordem com três elementos. Calcule a função de colapso desta boa ordem.*

Teorema (Princípio do colapso). *A imagem da função colapso numa boa ordem é um ordinal e a própria função de colapso é um isomorfismo entre a boa ordem e esse ordinal.*

Demonstração. Vejamos que $\text{im } f$ é um conjunto transitivo. Seja $v \in \text{im } f$ e $u \in v$. Tem-se então que $v = f(x)$, para certo $x \in X$. Visto que $u \in f(x)$, sai que $u = f(z)$ com $z < x$. Logo, $u \in \text{im } f$. Vamos agora ver que quaisquer dois elementos $u, v \in \text{im } f$ são \in -comparáveis. Ora, $u = f(x)$ e $v = f(z)$, para certos $x, z \in X$. Se $u \neq v$, então $x \neq z$ e, portanto, $x < z$ ou $z < x$. No primeiro caso, $u \in v$. No segundo, $v \in u$.

É claro que se x e y são elementos de X com $y < x$, então $f(y) \in f(x)$. \square

Note que uma boa ordem não pode ser isomorfa a dois ordinais distintos. Portanto, podemos definir uma *operação* que a cada boa ordem $(X, <)$ faz corresponder o único ordinal $\text{ord}(X, <)$ a ela isomorfa. Esta operação $(X, <) \rightsquigarrow \text{ord}(X, <)$ goza das seguintes propriedades:

$$(X, <) =_o \text{ord}(X, <)$$

$$(X, <) =_o (Y, <) \text{ se, e somente se, } \text{ord}(X, <) = \text{ord}(Y, <)$$

Corolário 17. *Dois boas ordens são isomorfas, ou uma delas é isomorfa a um segmento inicial próprio da outra.*

Demonstração. Dadas duas boas ordens, cada uma delas é isomorfa a um ordinal. Se os ordinais forem o mesmo, então as boas ordens são isomorfas. Caso contrário, um dos ordinais é um segmento inicial do outro, o que implica que uma das boas ordens é isomorfa a um segmento inicial da outra. \square

Corolário 18. *Seja $(X, <)$ uma boa-ordem e $Y \subseteq X$. Então o conjunto Y munido da boa-ordem induzida por $<$ é isomorfo a $(X, <)$ ou a um segmento inicial de $(X, <)$.*

Demonstração. A boa-ordem $(X, <)$ não pode ser isomorfa a um segmento inicial próprio de Y . Um tal isomorfismo seria naturalmente uma aplicação estritamente crescente de X num segmento inicial próprio de X , o que contradiz a Proposição 51. O resultado sai pelo corolário anterior. \square

O seguinte resultado é agora imediato.

Corolário 19. *Sejam Y um conjunto e α um ordinal tais que $Y \subseteq \alpha$. Então existe $\beta \leq \alpha$ tal que $\beta =_c Y$.*

O seguinte resultado de ZF é importante pois assegura que há ordinais infinitos não numeráveis.

Lema 13. *Para todo o conjunto X existe um ordinal que não é equipotente a nenhum subconjunto de X .*

Demonstração. É fácil de argumentar que a classe \mathcal{C} de todas as boas ordens da forma $(Z, <)$ com $Z \subseteq X$ é um conjunto: note-se que um tal par está em $\mathcal{P}(X) \times \mathcal{P}(X \times X)$. Logo, pelo axioma da substituição, $\{ord(Z, <) : (Z, <) \in \mathcal{C}\}$ é um conjunto de ordinais, digamos H_X . Como Ord é uma classe própria, tome-se $\alpha \notin H_X$. Vamos ver que α não é equipotente a nenhum subconjunto de X . Suponhamos, por absurdo, que existe $Z \subseteq X$ tal que $Z =_c \alpha$. Através duma bijecção entre Z e α , podemos transportar a boa-ordem de α para X , obtendo aí uma boa-ordem isomorfa $<$ (ou seja $ord(Z, <) = \alpha$). Logo, α estaria em H_X , o que é absurdo. \square

Podemos agora definir a operação $X \rightsquigarrow h(X)$ que a cada conjunto X faz corresponder o menor ordinal que não é equipotente a nenhum subconjunto de X . A $h(X)$ dá-se o nome de *número de Hartogs* de X . Por exemplo, o número de Hartogs de ω é o menor ordinal que não é finito ou numerável. Este número $h(\omega)$ denota-se por ω_1 ou \aleph_1 . Note que pelo Corolário 19, um subconjunto de \aleph_1 ou é finito, ou é numerável ou é equipotente a \aleph_1 .

Pela definição da operação de Hartogs, $h(X)$ nunca é equipotente a um subconjunto de X . Como consequência, se X é infinito então $h(X)$ é um ordinal limite.

Chapter 23

Teorema do ponto fixo de Zermelo

Seja X um conjunto munido duma ordem parcial \leq . Um subconjunto Z de X diz-se uma *cadeia* se, para todos $x, y \in Z$, ou $x \leq y$ ou $y \leq x$.

Definição 17. *Um ordem parcial diz-se completa para cadeias se toda a cadeia tem supremo.*

Seja dado um conjunto A e $\mathcal{S} \subseteq \mathcal{P}(A)$. Vê-se facilmente que $\bigcup \mathcal{S}$ é o supremo de \mathcal{S} quando consideramos $\mathcal{P}(A)$ munido da ordem parcial " \subseteq ". Em particular, $\mathcal{P}(A)$ munido da ordem parcial " \subseteq " é completo para cadeias. Outro exemplo útil de ordem parcial completa para cadeias é o seguinte. Dada (X, \leq) uma ordem parcial, considere-se $Cadeias(X, \leq)$, ou simplesmente $Cadeias(X)$, o conjunto de todas as cadeias de X . Então, $Cadeias(X)$ munido da ordem parcial " \subseteq " é uma ordem completa para cadeias. Isto decorre do facto da união duma cadeia de cadeias ser uma cadeia.

Exercício 86. *Verifique a última afirmação acima.*

Definição 18. *Seja (X, \leq) uma ordem parcial. Uma função $f : X \mapsto X$ diz-se uma expansão se, para todo $x \in X$, $x \leq f(x)$.*

Note-se que toda a ordem parcial completa para cadeias tem elemento mínimo (o supremo do conjunto vazio), que abaixo denotamos por \perp .

Lema 14 (Iteração transfinita). *Seja (X, \leq) uma ordem parcial completa para cadeias e $f : X \mapsto X$ uma expansão. Então existe uma operação $\alpha \rightsquigarrow It(\alpha)$ definida nos ordinais e com valores em X tal que:*

$$\begin{cases} It(0) & = \perp \\ It(\alpha + 1) & = f(It(\alpha)) \\ It(\gamma) & = \sup\{It(\alpha) : \alpha < \gamma\}, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Além disso, se $\beta \leq \alpha$ então $It(\beta) \leq It(\alpha)$.

Demonstração. A definição de It seria uma consequência imediata do teorema de recursão transfinita nos ordinais excepto pelo facto da terceira cláusula não ter de estar definida *a priori*. Porém, a seguinte definição pode, evidentemente, ser feita:

$$\left\{ \begin{array}{l} It(0) = \perp \\ It(\alpha + 1) = f(It(\alpha)) \\ It(\gamma) = \sup\{It(\alpha) : \alpha < \gamma\}, \text{ se } \gamma \text{ é ordinal limite e} \\ \quad \text{este supremo existir} \\ It(\beta) = \perp, \text{ caso contrário} \end{array} \right.$$

Mostra-se, por indução transfinita em α , que se tem a propriedade $P(\alpha) := \forall \delta, \beta (\delta < \beta \leq \alpha \rightarrow It(\delta) \leq It(\beta))$. Claro que se tem $P(0)$. Suponhamos $P(\alpha)$ e tomem-se $\delta < \beta \leq \alpha + 1$. Se $\beta \leq \alpha$ a conclusão desejada sai de $P(\alpha)$. Seja, então, $\beta = \alpha + 1$. Tem-se $\delta \leq \alpha$ e conclui-se $It(\delta) \leq It(\alpha)$, novamente por se ter $P(\alpha)$. Ora, como $It(\alpha) \leq f(It(\alpha)) = It(\alpha + 1) = It(\beta)$, sai o pretendido. Finalmente, seja γ um ordinal limite e suponhamos que se tem $P(\alpha)$ para todo $\alpha < \gamma$. Daqui sai o condicional $\beta < \alpha < \gamma \rightarrow It(\beta) \leq It(\alpha)$. Logo, por definição da operação, vem que $It(\gamma) = \sup\{It(\alpha) : \alpha < \gamma\}$. Conclui-se, imediatamente, $P(\gamma)$.

Pelo discutido acima, tem-se que o “caso contrário” nunca se dá. A parte final do lema demonstra-se facilmente por indução transfinita. \square

Teorema (Ponto fixo de Zermelo). *Seja (X, \leq) uma ordem parcial completa para cadeias e $f : X \mapsto X$ uma expansão. Então f tem um ponto fixo, i.e., existe $x \in X$ tal que $f(x) = x$.*

Demonstração. Seja f uma expansão. É fácil de argumentar que não se tem o condicional $\alpha < \beta \rightarrow It(\alpha) < It(\beta)$. Com efeito, esta propriedade implicaria que f fosse uma injeção da classe própria Ord no conjunto X , o que é uma impossibilidade. Logo, existem ordinais α e β tais que $\alpha < \beta$ e $It(\alpha) = It(\beta)$. Como $\alpha \leq \alpha + 1 \leq \beta$, vem $It(\alpha) \leq It(\alpha + 1) \leq It(\beta)$. Logo, $It(\alpha) = It(\alpha + 1) = f(It(\alpha))$, i.e., $It(\alpha)$ é ponto fixo de f . \square

Chapter 24

O lema de Zorn e tudo isso

Relembremos que, dada uma ordem parcial (X, \leq) , uma *cadeia* C é um subconjunto de X tal que quaisquer dois elementos são comparáveis (i.e., se $x, y \in C$ então $x \leq y$ ou $y \leq x$). Uma cadeia diz-se *maximal* se não estiver contida propriamente noutra cadeia.

Proposição 65 (Princípio da maximalidade de Hausdorff). *Seja (X, \leq) uma ordem parcial. Então X tem uma cadeia maximal.*

Demonstração. Admitamos, com vista a um absurdo, que não há cadeias maximais em X . Então, $\forall C \in \text{Cadeias}(X) \exists C' \in \text{Cadeias}(X) [C \subsetneq C']$. Pelo axioma da escolha, existe uma função $f : \text{Cadeias}(X) \mapsto \text{Cadeias}(X)$ tal que $C \subsetneq f(C)$, para toda a cadeia C de X . Ora, como sabemos, o conjunto $\text{Cadeias}(X)$ munido da ordem “ \subsetneq ” é um conjunto completo para cadeias e, é claro, f é uma expansão neste conjunto completo para cadeias. Pelo teorema do ponto fixo de Zermelo, f tem um ponto fixo. Isto é absurdo. \square

O seguinte resultado, utilizado frequentemente em Matemática, é um corolário simples do teorema anterior:

Proposição 66 (Lema de Zorn). *Seja (X, \leq) uma ordem parcial em que toda a cadeia tem majorante. Então X tem elemento maximal.*

Demonstração. Pelo teorema anterior, seja C uma cadeia maximal de X . Tome-se x um majorante de C . Claramente, x é elemento maximal de X . \square

Proposição 67 (Princípio da boa ordenação). *Todo o conjunto pode ser bem ordenado.*

Demonstração. Sem perda de generalidade, podemos supor que X é infinito. Considere-se o conjunto \mathcal{F} de todas as funções injectivas da forma $f : \beta \mapsto X$, com $\beta < h(X)$, onde $h(X)$ é o número de Hartogs de X . Claro que (\mathcal{F}, \subseteq) é uma ordem parcial. Para além disso, se \mathcal{C} é uma cadeia de funções de \mathcal{F} , a união $\bigcup \mathcal{C}$ ainda é uma função injectiva e o seu domínio é claramente um segmento inicial de $h(X)$. Por definição de número de Hartogs, este segmento inicial não pode ser todo o $h(X)$. Argumentámos, portanto, que toda a cadeia de (\mathcal{F}, \subseteq) tem majorante. Pelo lema de Zorn, esta ordem tem um elemento maximal $f : \beta \mapsto X$. É fácil de argumentar que $\text{im} f = X$: com efeito, se não fosse, tomava-se um elemento $x_0 \in X \setminus \text{im} f$; então a função $f \cup \{(\beta, x_0)\}$ de

domínio $\beta + 1$ (note-se que $\beta + 1 < h(X)$, pois $h(X)$ é ordinal limite) estaria em \mathcal{F} ; isto entra em contradição com a maximalidade de f .

Agora, dado que o elemento maximal f é uma bijecção entre um ordinal e X , conclui-se que X pode ser bem-ordenado. \square

Exercício 87. *Mostre que a teoria Z juntamente com o princípio da boa ordenação demonstra o axioma da escolha.*

Proposição 68 (Comparabilidade das cardinalidades). *Dados conjuntos X e Y , então $X \leq_c Y$ ou $Y \leq_c X$.*

Demonstração. Pelo teorema anterior, podemos munir X e Y de boas ordens. Ora, como sabemos, as boas ordens ou são isomorfas ou uma delas é isomorfa a um segmento inicial da outra. O resultado sai agora trivialmente. \square

O axioma da escolha é necessário para demonstrar qualquer dos quatro teoremas acima. Com efeito:

Teorema (Equivalências ao axioma da escolha). *Na teoria ZF os seguintes princípios são equivalentes:*

1. *Axioma da escolha.*
2. *Princípio da maximalidade de Hausdorff.*
3. *Lema de Zorn.*
4. *Princípio da boa ordenação.*
5. *Princípio da comparabilidade das cardinalidades.*

Demonstração. Viu-se que $(1) \rightarrow (2) \rightarrow (3) \rightarrow (4) \rightarrow (5)$. É fácil mostrar que $(4) \rightarrow (1)$. Logo, basta ver que $(5) \rightarrow (4)$. Seja X um conjunto qualquer. Por (5), $X \leq_c h(X)$ ou $h(X) \leq_c X$, onde $h(X)$ é o número de Hartogs de X . Por definição de $h(X)$ não se tem o segundo caso. Logo, $X \leq_c h(X)$, i.e., existe uma injeção de X no ordinal $h(X)$. Então, claramente que X pode ser bem ordenado. \square

Chapter 25

O axioma da escolha na prática matemática

O axioma da escolha é frequentemente usado na matemática, por vezes de modo quase imperceptível. Se bem que muitas vezes apenas se usem formas enfraquecidas do axioma (p. ex., AC_ω ou DC), outras vezes ele é usado em todo (ou quase todo) o seu poder. Nesta secção, vamos apresentar alguns exemplos de argumentos que ocorrem na prática matemática e que utilizam o axioma da escolha.

Um primeiro exemplo, já discutido anteriormente, é o da equivalência entre as noções de conjunto infinito e infinito à Dedekind. A primeira propriedade implica a segunda com a ajuda do axioma da escolha. O argumento que usámos na demonstração da Proposição 30 apenas necessita do axioma DC das escolhas dependentes. De facto, pode mesmo argumentar-se que AC_ω já é suficiente:

Proposição 69. *Em $Z + AC_\omega$, todo o conjunto infinito é infinito à Dedekind.*

Demonstração. Dado que X é um conjunto infinito, tem-se

$$\forall n \in \omega \exists Z \in \mathcal{P}(X) (\text{card}(Z) = 2^n).$$

Por AC_ω , existe uma sucessão $n \rightsquigarrow Z_n$ de subconjuntos de X cada qual com 2^n elementos. Ora,

$$\text{card}(\bigcup_{i=0}^n Z_i) \leq \sum_{i=0}^n \text{card}(Z_i) = \sum_{i=0}^n 2^i = 2^{n+1} - 1 < 2^{n+1}.$$

Tem-se, pois, que $\forall n \in \omega \exists x \in X (x \in Z^{n+1} \setminus (\bigcup_{i=0}^n Z_i))$. Novamente por AC_ω , existe uma sucessão $n \rightsquigarrow x_n$ de elementos de X tais que, para todo $n \in \omega$, $x_n \in Z^{n+1} \setminus (\bigcup_{i=0}^n Z_i)$. Claro que esta sucessão é uma injeção de ω em X . Logo, X é infinito à Dedekind. \square

Dado w um número real e X um subconjunto de \mathbb{R} , diz-se que w é *ponto aderente* de X se $\forall \varepsilon > 0 \exists x \in X |x - w| < \varepsilon$. Na presença de AC_ω , esta noção é equivalente a dizer que existe uma sucessão $(x_n)_{n \in \omega}$ de elementos de X a convergir para w . Com efeito, admitamos que w é ponto aderente de X . Então, $\forall n \in \omega \exists x \in X |x - w| < \frac{1}{n+1}$. Por AC_ω , existe $f : \omega \mapsto X$ tal que, para todo $n \in \omega$, $|f(n) - w| < \frac{1}{n+1}$. Claro que a sucessão $x_n = f(n)$, de elementos de X , converge para w . A implicação contrária é imediata e não necessita do axioma da escolha.

Exercício 88. Uma função $f : \mathbb{R} \mapsto \mathbb{R}$ diz-se sequencialmente contínua no ponto $x \in \mathbb{R}$ se, sempre que $(x_n)_{n \in \omega}$ é uma sucessão de números reais a convergir para x , então a sucessão $(f(x_n))_{n \in \omega}$ converge para $f(x)$. Mostre em $Z+AC_\omega$ que uma função real de variável real f é contínua num ponto $x \in \mathbb{R}$ se, e somente se, é sequencialmente contínua em x .

O axioma da escolha tem, por vezes, consequências desagradáveis. O axioma permite mostrar a existência de certos objectos “patológicos” que, de outro modo, não existiriam. Curiosamente, as formas enfraquecidas AC_ω ou DC da axioma da escolha não são geralmente suficientes para mostrar a existência das patologias.

Um problema importante da análise matemática consiste em prolongar a noção de comprimento dum intervalo a subconjuntos mais complicados de \mathbb{R} . Idealmente, gostaríamos de prolongar esta noção a todos os subconjuntos de \mathbb{R} . Põe-se o problema: será que existe uma função $\mu : \mathcal{P}(\mathbb{R}) \rightarrow [0, +\infty]$ de tal sorte que:

1. $\mu(\emptyset) = 0$ e $\mu(\mathbb{R}) = +\infty$.
2. se $(X_n)_{n \in \omega}$ é uma sucessão de subconjuntos mutuamente disjuntos de \mathbb{R} , então $\mu(\bigcup_{n \in \omega} X_n) = \sum_{n \in \omega} \mu(X_n)$.
3. se $a, b \in \mathbb{R}$ com $a \leq b$, então $\mu([a, b]) = b - a$.
4. se $a \in \mathbb{R}$ e $X \subseteq \mathbb{R}$, então $\mu(X) = \mu(a + X)$, onde $a + X = \{a + x : x \in X\}$.

Os dois primeiros requisitos garantem que μ é uma *medida* (definida em todos os subconjuntos de \mathbb{R}). A segunda propriedade é conhecida como σ -aditividade. O terceiro requisito diz que a medida dum intervalo é o seu comprimento. O último requisito diz que a medida é invariante para translações.

Lema 15. *Seja μ como acima. Têm-se as seguintes propriedades:*

- i. se $X, Y \subseteq \mathbb{R}$ são conjuntos disjuntos, então $\mu(X \cup Y) = \mu(X) + \mu(Y)$.*
- ii. se $X \subseteq Y \subseteq \mathbb{R}$, então $\mu(X) \leq \mu(Y)$.*
- iii. se $(X_n)_{n \in \omega}$ é uma sucessão crescente de subconjuntos de \mathbb{R} ($X_n \subseteq X_{n+1} \subseteq \mathbb{R}$, para todo $n \in \omega$), então $\mu(\bigcup_{n \in \omega} X_n) = \sup_{n \in \omega} \mu(X_n)$.*

Demonstração. A primeira propriedade é consequência da σ -aditividade de μ (e do facto de que $\mu(\emptyset) = 0$). A segunda propriedade sai da anterior: com efeito, se $X \subseteq Y$, então $\mu(Y) = \mu(X \cup (Y \setminus X)) = \mu(X) + \mu(Y \setminus X) \geq \mu(X)$. Finalmente, argumentemos (iii). Seja $(X_n)_{n \in \omega}$ uma sucessão crescente de subconjuntos de \mathbb{R} . Defina-se $Y_0 = X_0$ e $Y_{n+1} = X_{n+1} \setminus X_n$. Note-se que $\bigcup_{n \in \omega} X_n = \bigcup_{n \in \omega} Y_n$ e que esta última união é disjunta. Vem:

$$\mu(\bigcup_{n \in \omega} X_n) = \mu(\bigcup_{n \in \omega} Y_n) = \sum_{n \in \omega} \mu(Y_n) = \sup_{n \in \omega} \left(\sum_{i=0}^n \mu(Y_i) \right) = \sup_{n \in \omega} \mu(\bigcup_{i=0}^n Y_i) = \sup_{n \in \omega} \mu(X_n),$$

onde se utiliza o facto de que cada X_n é a união dos Y_i , com $i \leq n$. □

Vamos ver que, na presença do axioma da escolha, não há funções μ que satisfaçam (1)-(4). Mais especificamente, com a ajuda do axioma da escolha, vamos exibir um conjunto V – o chamado *conjunto de Vitali* – cuja existência de medida leva a uma contradição. Defina-se a seguinte relação de equivalência em \mathbb{R} : $x \sim y$ sse $x - y \in \mathbb{Q}$. Pelo axioma da escolha, seja V um conjunto de representantes para esta relação de equivalência. Sem perda de generalidade, podemos supor que $V \subseteq [0, 1]$ (pois toda a classe de equivalência intersecta $[0, 1]$). Claramente, $\mathbb{R} = \bigcup_{q \in \mathbb{Q}} (q + V)$. Além disso, esta união numerável é disjunta. Com efeito, suponhamos que $(q + V) \cap (q' + V) \neq \emptyset$, com $q, q' \in \mathbb{Q}$. Seja $x \in (q + V) \cap (q' + V)$. Então existem $r, r' \in V$ tais que $x = q + r = q' + r'$. Daqui sai que $r - r' = q' - q \in \mathbb{Q}$. Logo $r \sim r'$ e, portanto, $r = r'$ (já que ambos r e r' estão no conjunto de representantes V). Vem, $q = q'$. Por σ -aditividade, $\sum_{q \in \mathbb{Q}} \mu(q + V) = +\infty$. Pela invariância da translação, $\mu(q + V) = \mu(V)$, para todo $q \in \mathbb{Q}$. Conclui-se que $\mu(V) > 0$. Ora, $\bigcup_{q \in [0, 1] \cap \mathbb{Q}} (q + V) \subseteq [0, 2]$. Logo, $\sum_{q \in [0, 1] \cap \mathbb{Q}} \mu(V) \leq 2$. Isto é absurdo, pois a série à esquerda da desigualdade é soma infinita de um mesmo elemento não nulo.

Perante o exemplo de Giuseppe Vitali, os analistas escolhem manter as propriedades (1)-(4) mas admitir que a função μ não esteja definida em *todos* os subconjuntos de \mathbb{R} . Em análise matemática desenvolve-se a *medida de Lebesgue* com as propriedades (1)-(4), porém apenas definida nos denominados conjuntos *mensuráveis à Lebesgue*. Os conjuntos mensuráveis à Lebesgue contêm os intervalos e são fechados para complementações e uniões finitas ou numeráveis. Ao menor subconjunto de $\mathcal{P}(\mathbb{R})$ que contêm todos os intervalos de \mathbb{R} e que é fechado para complementações e uniões finitas ou numeráveis chama-se o conjunto dos *Borelianos* de \mathbb{R} . Assim, todo o conjunto Boreliano é mensurável à Lebesgue.

Exercício 89. Mostre que os abertos e fechados de \mathbb{R} são conjuntos Borelianos.

Exercício 90. Mostre que o conjunto ternário de Cantor é um conjunto de cardinalidade 2^{\aleph_0} , mensurável à Lebesgue e que tem medida zero.

Exercício 91. Defina, por recursão transfinita, a seguinte função $\alpha \rightsquigarrow \mathcal{B}_\alpha$ de domínio ω_1 :

$$\begin{aligned} \mathcal{B}_0 &= \mathcal{A} \cup \{\mathbb{R} \setminus U : U \in \mathcal{A}\} \\ \mathcal{B}_{\alpha+1} &= (\mathcal{B}_\alpha)^* \cup \{\mathbb{R} \setminus X : X \in (\mathcal{B}_\alpha)^*\} \\ \mathcal{B}_\lambda &= \bigcup_{\alpha < \lambda} \mathcal{B}_\alpha, \text{ se } \lambda \text{ é ordinal limite} \end{aligned}$$

onde \mathcal{A} é o conjunto de todos os abertos de \mathbb{R} e a operação $*$ está definida definida no exercício. Seja $\mathcal{B} = \bigcup_{\alpha < \omega_1} \mathcal{B}_\alpha$.

1. Mostre que \mathcal{B} é o conjunto dos Borelianos de \mathbb{R} .
2. Mostre que, para cada $\alpha < \omega_1$, a cardinalidade de \mathcal{B}_α é 2^{\aleph_0} .
3. Mostre que a cardinalidade de \mathcal{B} é 2^{\aleph_0} .

Na presença do axioma da escolha, o conjunto de Vitali é um exemplo dum conjunto que não é mensurável à Lebesgue. No início dos anos setenta do século passado, Robert Solovay exibiu um modelo de $ZF + DC$ em que todo o conjunto é mensurável à Lebesgue. O resultado de Solovay mostra que a existência de conjuntos não mensuráveis à Lebesgue necessita do axioma da escolha (nem sequer bastando formas enfraquecidas deste).

O exemplo de Vitali pode ser refinado de forma mais ou menos dramática. Um resultado de Stefan Banach e Alfred Tarski publicado em 1924 mostra que é possível particionar a bola unitária de \mathbb{R}^3 num número finito de pedaços de tal modo que seja possível re-arranjar esses pedaços, por meio de rotações e translações, e obter no final duas cópias da bola unitária. Este resultado é conhecido por *paradoxo de Banach-Tarski*. Não se trata realmente dum paradoxo, mas tão-somente dum resultado extremamente contra-intuitivo. Os pedaços de que o resultado de Banach-Tarski fala não são mensuráveis: o axioma da escolha desempenha um papel essencial nesta decomposição da bola unitária, à semelhança do que sucede no exemplo de Vitali.

Dado um espaço vectorial V sobre um corpo K , um conjunto X de vectores de V diz-se *linearmente independente* se, para toda a sequência finita x_1, \dots, x_n de elementos distintos de X , se tem:

$$\forall \lambda_1, \dots, \lambda_n \in K (\lambda_1 x_1 + \dots + \lambda_n x_n = 0 \rightarrow \lambda_1 = \dots = \lambda_n = 0).$$

Um conjunto de vectores X diz-se uma *base de Hamel* do espaço vectorial V se for linearmente independente e *gerar* V , no sentido em que, para todo $x \in V$, existem elementos $x_1, \dots, x_n \in X$ e escalares $\lambda_1, \dots, \lambda_n \in K$ tais que $x = \lambda_1 x_1 + \dots + \lambda_n x_n$. Um conjunto X de vectores linearmente independente diz-se *maximal* se nenhum conjunto Y de vectores que contenha propriamente X é linearmente independente. O seguinte lema é fundamental:

Lema 16. *Todo o conjunto de vectores linearmente independente maximal é uma base.*

Demonstração. Seja X um conjunto linearmente independente maximal. Considere-se x um elemento de V . Se $x \in X$, claramente x escreve-se como combinação linear de elementos de X . Se $x \notin X$, por maximalidade, $X \cup \{x\}$ já não é linearmente independente. Então existe uma combinação linear nula de elementos de $X \cup \{x\}$ sem que os coeficientes sejam todos nulos. Dado que X é linearmente independente, esta combinação linear nula é necessariamente da forma $\lambda x + \lambda_1 x_1 + \dots + \lambda_n x_n$, com $x_1, \dots, x_n \in X$ e $\lambda \neq 0$. Sai $x = -\lambda^{-1} \lambda_1 x_1 - \dots - \lambda^{-1} \lambda_n x_n$. \square

Teorema 3. *Todo o espaço vectorial tem uma base de Hamel.*

Demonstração. Seja V um espaço vectorial. Seja \mathcal{I} o conjunto de todos os subconjuntos X de V linearmente independentes. Vamos ver que \mathcal{I} munido da ordem parcial “estar contido” está nas condições de aplicação do lema de Zorn. Com efeito, seja \mathcal{C} uma cadeia de elementos de \mathcal{I} . Vamos ver que $\bigcup \mathcal{C}$ é um conjunto linearmente independente. Sejam $x_1, \dots, x_n \in \bigcup \mathcal{C}$. Dado que $\bigcup \mathcal{C}$ é uma cadeia, existe $X \in \mathcal{C}$ tal que $\{x_1, \dots, x_n\} \subseteq X$. Daqui sai que qualquer combinação linear nula de x_1, \dots, x_n tem necessariamente todos os coeficientes nulos. Pelo lema de Zorn, existe $B \in \mathcal{I}$ maximal. Pelo lema anterior, B é base de V . \square

Como se sabe, todo o corpo tem um fecho algébrico. Este resultado necessita, em geral, do axioma da escolha. A demonstração mais comum deste resultado usa o lema de Zorn. Porém, para ilustrar uma técnica importante, mas menos conhecida do que o lema de Zorn, vamos mostrar este resultado através duma recursão transfinita ao longo duma boa-ordem.

Considere-se um corpo K e seja $K[X]$ o seu anel de polinómios a uma variável. Recordemos alguns resultados de teoria dos corpos. Dado $p(X)$ um polinómio de grau positivo de $K[X]$ e F um corpo, extensão de K , sabemos que é possível definir explicitamente uma extensão algébrica F^+ de F onde o polinómio $p(X)$ tem (pelo menos) uma raiz. Neste ponto, o leitor recordar-se-á da construção do corpo de ruptura associado a um polinómio irreduzível (e do facto de que um polinómio de grau positivo se pode factorizar em produto de irreduzíveis).

Seja $(p_\alpha(X))_{\alpha < \kappa}$ uma boa-ordenação de todos os polinómios de grau positivo de $K[X]$ (aqui usa-se o axioma da escolha). Sem perda de generalidade, κ é um ordinal limite. Defina-se, por recursão transfinita, a seguinte cadeia de corpos $(K_\alpha)_{\alpha < \kappa}$:

$$\begin{cases} K_0 & = K \\ K_{\alpha+1} & = K_\alpha^+ \\ K_\gamma & = \varinjlim_{\alpha < \gamma} K_\alpha, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Nesta definição, K_α^+ é a extensão algébrica (discutida acima) de K_α em que o polinómio $p_\alpha(X)$ tem raízes. Seja dado $\gamma < \kappa$ ordinal limite. Então, $(K_\alpha)_{\alpha < \gamma}$ é uma cadeia de corpos (dada através de monomorfismos adequados) e, portanto, faz sentido falar no seu *limite directo* $\varinjlim_{\alpha < \gamma} K_\alpha$ (intuitivamente, $\varinjlim_{\alpha < \gamma} K_\alpha$ é a “união” de todos os corpos $(K_\alpha)_{\alpha < \gamma}$).

Por recursão transfinita, mostra-se que cada corpo K_α é uma extensão algébrica de K . Tome-se agora $\tilde{K} = \varinjlim_{\alpha < \kappa} K_\alpha$. Pelo discutido, \tilde{K} é uma extensão algébrica de K . Resta ver que \tilde{K} é algebricamente fechado. Por resultados da teoria dos corpos, basta ver que todo o polinómio de grau positivo com coeficientes em K tem raízes em \tilde{K} . Ora, um tal polinómio é um certo $p_\alpha(X)$, para algum $\alpha < \kappa$. Por construção, o polinómio $p_\alpha(X)$ tem raízes em $K_{\alpha+1}$ e, portanto, em \tilde{K} .

Esta demonstração mostra também que apenas se usa o axioma da escolha para obter uma boa ordem do anel de polinómios $K[X]$. Uma tal boa-ordenação é automática se K for finito ou numerável. Esta observação generaliza-se: como iremos ver no próximo capítulo, se K tiver uma boa-ordenação, então $K[X]$ também tem uma boa-ordenação (sem invocar o axioma da escolha). Portanto, ZF demonstra que todo o corpo bem ordenável tem fecho algébrico.

Os exemplos anteriores descrevem aplicações do axioma da escolha na área da álgebra abstracta. Como já observámos, em álgebra o axioma da escolha é frequentemente usado através do lema de Zorn. Isso acontece, p. ex., em álgebra comutativa, onde existem resultados sobre a existência de ideais maximais. No exemplo seguinte, vamos ilustrar novamente o uso do lema de Zorn.

Definição 19. *Seja X um conjunto. Um filtro sobre X é um conjunto \mathcal{F} de subconjuntos de X que satisfaz as seguintes condições:*

1. $X \in \mathcal{F}$ e $\emptyset \notin \mathcal{F}$;
2. se $F, G \in \mathcal{F}$ então $F \cap G \in \mathcal{F}$;
3. se $F \in \mathcal{F}$ e $F \subseteq G \subseteq X$ então $G \in \mathcal{F}$.

Dado um elemento a de um dado conjunto X , o conjunto de todos os subconjuntos de X de que a é elemento constitui um filtro. Aos filtros deste tipo chamam-se filtros *principais*. Outro exemplo importante de filtro é o seguinte. Dado um conjunto infinito X , o conjunto dos subconjuntos *co-finitos* (i.e., de complementar finito) de X forma um filtro.

Um conjunto não vazio \mathcal{C} de subconjuntos de X diz-se que tem a *propriedade de intersecção finita* (PIF) se toda a intersecção finita de elementos de \mathcal{C} é não vazia. É fácil de ver que se \mathcal{C} tem a PIF então

$$\mathcal{F} := \{F \subseteq X : \exists C_1, \dots, C_i \in \mathcal{C} (C_1 \cap \dots \cap C_i \subseteq F)\}$$

é um filtro.

Definição 20. Um ultrafiltro \mathcal{U} sobre X é um filtro sobre X com a seguinte propriedade: para qualquer subconjunto Z de X , ou $Z \in \mathcal{U}$ ou $X \setminus Z \in \mathcal{U}$.

Os filtros principais são ultrafiltros. Como iremos ver, na presença do axioma da escolha, há ultrafiltros que não são principais.

Proposição 70. Seja \mathcal{F} um filtro sobre X . \mathcal{F} é um ultrafiltro se, e somente se, não está contido propriamente em nenhum filtro.

Demonstração. Suponhamos que \mathcal{F} é um ultrafiltro e seja \mathcal{F}' um filtro tal que $\mathcal{F} \subseteq \mathcal{F}'$. Seja $Z \in \mathcal{F}'$. Não se pode ter $X \setminus Z \in \mathcal{F}$ pois, caso contrário, $X \setminus Z \in \mathcal{F}'$ o que implicaria que $\emptyset \in \mathcal{F}'$. Visto que \mathcal{F} é um ultrafiltro, vem $Z \in \mathcal{F}$. Dada a arbitrariedade de Z , demonstrou-se que $\mathcal{F} = \mathcal{F}'$.

Reciprocamente, suponhamos que \mathcal{F} é um filtro que não está contido propriamente em nenhum filtro. Seja dado $Z \subseteq X$. Admitamos que $X \setminus Z \notin \mathcal{F}$. É fácil de ver que $\mathcal{F} \cup \{Z\}$ tem a PIF. Seja \mathcal{F}' um filtro tal que $\mathcal{F} \cup \{Z\} \subseteq \mathcal{F}'$. Por hipótese, $\mathcal{F}' = \mathcal{F}$. Logo, $Z \in \mathcal{F}$. \square

Teorema do ultrafiltro. Todo o filtro sobre um conjunto está contido num ultrafiltro.

Demonstração. Seja X um conjunto e \mathcal{F} um filtro sobre X . Considere-se o conjunto \mathbb{P} de todos os filtros sobre X que contêm \mathcal{F} . Podemos munir este conjunto de filtros da ordem parcial “estar contido”. É fácil de argumentar que a união duma cadeia de filtros ainda é um filtro. Pelo lema de Zorn, \mathbb{P} tem elemento maximal. Um tal elemento maximal é um ultrafiltro. \square

(Considere-se o filtro dos conjuntos co-finitos de ω (o chamado filtro de Fréchet). Pelo teorema anterior, este filtro está contido num ultrafiltro. Claramente, este ultrafiltro não é principal. Assim, o teorema do ultrafiltro garante-nos a existência de ultrafiltros não principais sobre ω .)

Exercício 92. Seja \mathcal{F} um filtro sobre X e seja $G \subseteq X$ tal que $G \notin \mathcal{F}$. Então existe um ultrafiltro \mathcal{U} que contém \mathcal{F} e tal que $G \notin \mathcal{U}$. [Sugestão: mostre que $\mathcal{F} \cup \{X \setminus G\}$ tem a PIF.]

Chapter 26

Números aléfes

Definição 21. Um número cardinal, ou simplesmente um cardinal, é um ordinal que não é equipotente a nenhum ordinal inferior.

Exercício 93. Mostre que todo o cardinal infinito é um ordinal limite.

Pelo teorema dos cacifos, todo o ordinal finito é um número cardinal. Claro que ω é um cardinal, mas $\omega + 1$ não é um número cardinal. Também é claro que todo o ordinal é equipotente a um número cardinal. O enunciado de que todo o conjunto é equipotente a um número cardinal necessita obviamente do axioma da escolha (pois implica que todo o conjunto pode ser bem ordenado). Obviamente, o número de Hartogs $h(X)$ dum conjunto X é sempre um número cardinal.

Lema 17. Para todo o ordinal α existe um cardinal κ tal que $\alpha < \kappa$. Como consequência, a classe Card dos cardinais é uma classe própria.

Demonstração. Seja α um ordinal. O cardinal $h(\alpha)$ tem a propriedade pretendida (por tricotomia, a alternativa seria $h(\alpha) \leq \alpha$, o que conduz a um absurdo). \square

Definição 22. Seja κ um cardinal. Denota-se por κ^+ o menor cardinal que é maior que κ . A κ^+ dá-se o nome de cardinal sucessor de κ .

Claro que κ^+ é $h(\kappa)$.

Lema 18. Seja X um conjunto de cardinais. Então $\bigcup X$ é um cardinal.

Demonstração. Visto que X é um conjunto de ordinais, $\bigcup X$ é um ordinal. Suponhamos que $\alpha < \bigcup X$. Ora, como sabemos, $\bigcup X$ é o supremo ordinal do conjunto X . Logo, existe um cardinal $\kappa \in X$ tal que $\alpha < \kappa$. Isto acarreta $\alpha \neq_c \bigcup X$. \square

Observe-se que o lema anterior permite falar, sem ambiguidade, de $\sup X$ quando X é um conjunto de cardinais. O supremo de X na estrutura ordinal coincide com o supremo de X na estrutura cardinal.

Proposição 71 (Números aléfes). Existe uma operação $\alpha \rightsquigarrow \aleph_\alpha$ definida nos ordinais e tomando valores nos cardinais infinitos tal que:

$$\begin{cases} \aleph_0 & = \omega \\ \aleph_{\alpha+1} & = \aleph_\alpha^+ \\ \aleph_\gamma & = \sup\{\aleph_\alpha : \alpha < \gamma\}, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

Além disso, tem-se $\alpha < \beta \rightarrow \aleph_\alpha < \aleph_\beta$ e $\alpha \leq \aleph_\alpha$.

Demonstração. A operação existe pelo teorema da recursão transfinita nos ordinais. As propriedades demonstram-se facilmente por indução transfinita. Vejamos a segunda. Claro que $0 \leq \aleph_0$. E, $\alpha + 1 \leq \aleph_{\alpha+1} \leq \aleph_\alpha^+$, onde se usa a hipótese de indução na primeira desigualdade. Se γ é ordinal limite, vem para todo $\alpha < \gamma$, $\alpha \leq \aleph_\alpha \leq \aleph_\gamma$ (usou-se a hipótese de indução na primeira desigualdade). Pela arbitrariedade de α , sai $\gamma \leq \aleph_\gamma$. \square

Proposição 72. Para todo o cardinal infinito κ , existe um (necessariamente único) ordinal α tal que $\kappa = \aleph_\alpha$.

Demonstração. Seja α o menor ordinal tal que $\kappa \leq \aleph_\alpha$. Admitamos, com vista a um absurdo, que $\kappa < \aleph_\alpha$. Claro que $\alpha \neq 0$. Também não se pode ter $\alpha = \beta + 1$, pois nem se pode ter $\aleph_\beta < \kappa$ (por definição de $\aleph_{\beta+1}$), nem se pode ter $\kappa \leq \aleph_\beta$ (por minimalidade de α). Resta estudar o caso em que α é um ordinal limite. Neste caso, existe $\beta < \alpha$ com $\kappa < \aleph_\beta$, novamente contradizendo a minimalidade de α . \square

O seguinte resultado é fundamental para a aritmética cardinal:

Teorema (Produto de aléfes). Para todo o ordinal α tem-se $\aleph_\alpha \times \aleph_\alpha =_c \aleph_\alpha$.

Demonstração. Claramente, $\aleph_\alpha \leq_c \aleph_\alpha \times \aleph_\alpha$. Vamos mostrar, por indução transfinita em α , que $\aleph_\alpha \times \aleph_\alpha \leq_c \aleph_\alpha$. O caso $\alpha = 0$ é sabido. Tome-se $\alpha \neq 0$ e admita-se, por hipótese de indução transfinita, que $\aleph_\eta \times \aleph_\eta \leq_c \aleph_\eta$, para todo $\eta < \alpha$. Consideremos a boa ordem de Gödel $<_G$ no produto Cartesiano $\aleph_\alpha \times \aleph_\alpha$. Vamos argumentar que todo o segmento inicial próprio desta boa ordem tem cardinalidade estritamente inferior a \aleph_α . Evidentemente, isto mostra que $\aleph_\alpha \not\prec \text{Ord}(\aleph_\alpha \times \aleph_\alpha, <_G)$, concluindo-se $\text{Ord}(\aleph_\alpha \times \aleph_\alpha, <_G) \leq \aleph_\alpha$ e, portanto, $\aleph_\alpha \times \aleph_\alpha \leq_c \aleph_\alpha$. Seja (β, γ) um elemento ao arbítrio de $\aleph_\alpha \times \aleph_\alpha$ e considere-se $\delta = \max(\beta, \gamma)$. Note-se que $\delta + 1 < \aleph_\alpha$. Pela definição de ordem de Gödel, é claro que o segmento inicial de $\aleph_\alpha \times \aleph_\alpha$ determinado por (β, γ) está contido no produto Cartesiano $(\delta + 1) \times (\delta + 1)$. Sem perda de generalidade (pois $\alpha \neq 0$), podemos supor que δ é um ordinal infinito. Seja η tal que $\delta + 1 =_c \aleph_\eta$. Necessariamente, $\eta < \alpha$. Assim, o segmento inicial para a boa ordem de Gödel determinado por (β, γ) tem cardinalidade inferior ou igual a $\aleph_\eta \times \aleph_\eta =_c \aleph_\eta$ (aqui usamos a hipótese de indução transfinita). É, portanto, estritamente inferior a \aleph_α . Como se queria. \square

O desenvolvimento dos números aléfes acima efectuou-se em ZF. De agora em diante vamos necessitar do axioma da escolha. Como sabemos, em ZFC todo o conjunto pode ser bem ordenado e toda a boa ordem é isomorfa a um ordinal. Portanto, podemos efectuar a seguinte definição:

Definição 23. A cardinalidade de um conjunto x , denotada por $\text{Card}(x)$, é o menor ordinal equipotente a x .

Claramente, $\text{Card}(x)$ é um cardinal. Neste conformidade, temos uma operação $x \rightsquigarrow \text{Card}(x)$ definida em todo o universo e que toma valores nos números cardinais. Esta operação goza das seguintes propriedades:

$$\text{Card}(x) =_c x$$

$$x =_c y \text{ se, e somente se, } \text{Card}(x) = \text{Card}(y)$$

A operação $x \rightsquigarrow \text{Card}(x)$ associa a cada conjunto x um representante $\text{Card}(x)$ da sua “classe de equipotência”. Com esta definição, já se pode falar *literalmente* em cardinalidades e não apenas no contexto de certas asserções. Por exemplo, a igualdade cardinal $\kappa \cdot \rho = \rho \cdot \kappa$, que anteriormente interpretámos como significando que $x \times y =_c y \times x$ para todos os conjuntos x e y , tem agora o sentido literal que passamos a explicar. Dados cardinais κ e ρ define-se o cardinal $\kappa \cdot \rho$ como sendo $\text{Card}(\kappa \times \rho)$ e, com esta definição de *produto cardinal*, claro que se tem a lei $\kappa \cdot \rho = \rho \cdot \kappa$. Considerações análogas aplicam-se às outras operações aritméticas: $\kappa + \rho$ define-se como sendo $\text{Card}(\kappa \uplus \rho)$ e κ^ρ como sendo a cardinalidade do conjunto de todas as funções de ρ para κ . O mesmo se passa com operações infinitárias sobre cardinais.

Há um ponto subtil de linguagem para o qual é necessário chamar a atenção. Quando afirmamos que, para todo o cardinal infinito κ , se tem $\kappa \cdot \kappa = \kappa$ e a interpretamos literalmente, esta afirmação é verdadeira por causa do teorema do produto das aléfes (e da Proposição 72). Note-se que esta justificação não necessita do axioma da escolha. Porém, quando a interpretamos como afirmando que, para todo o conjunto infinito x , $x \times x =_c x$, então a justificação desta asserção invoca o axioma da escolha: $x =_c \text{Card}(x)$ e, como $\text{Card}(x) \times \text{Card}(x) =_c \text{Card}(x)$, vem $x \times x =_c x$.

Os números cardinais são ordinais mas a aritmética cardinal difere radicalmente da aritmética ordinal, ou seja, para cardinais (portanto, ordinais) κ e ρ , o produto cardinal de κ por ρ é (em geral) diferente do produto ordinal de κ por ρ , ainda que se costume usar a *mesma notação* para um e para outro, viz. $\kappa \cdot \rho$. O contexto deve permitir decidir qual a aritmética em causa. Geralmente reservam-se as letras minúsculas do meio do alfabeto grego (κ , λ , μ , ρ , etc) para denotar cardinais e, nestas circunstâncias, temos em mente a aritmética cardinal. Esse também é o caso quando usamos a notação dos aléfes.

Exercício 94. *Suponha que $\aleph_\alpha \leq 2^{\aleph_\beta}$. Mostre que $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$.*

Exercício 95. *Mostre que a cardinalidade do conjunto $\prod_{0 < \alpha < \omega_1} \alpha$ é 2^{\aleph_1} .*

O seguinte resultado é útil:

Proposição 73. *Seja λ um cardinal infinito e $(\kappa_\alpha)_{\alpha < \lambda}$ uma família de cardinais não nulos. Considere-se $\kappa := \sup\{\kappa_\alpha : \alpha < \lambda\}$. Então,*

$$\sum_{\alpha < \lambda} \kappa_\alpha = \lambda \cdot \kappa.$$

Demonstração. É claro que $\sum_{\alpha < \lambda} \kappa_\alpha \leq \sum_{\alpha < \lambda} \kappa = \lambda \cdot \kappa$. Para ver o recíproco, note-se que $\lambda = \sum_{\alpha < \lambda} 1 \leq \sum_{\alpha < \lambda} \kappa_\alpha$; note-se também que $\sum_{\alpha < \lambda} \kappa_\alpha$ majora cada κ_α e que, portanto, $\kappa \leq \sum_{\alpha < \lambda} \kappa_\alpha$. Assim, como ambos λ e κ são $\leq \sum_{\alpha < \lambda} \kappa_\alpha$, sai que o seu produto $\lambda \cdot \kappa$, que é o maior dos dois (ver Corolário 6), é também $\leq \sum_{\alpha < \lambda} \kappa_\alpha$. \square

Exercício 96. *Seja $(\kappa_i)_{i \in I}$ uma família de cardinais tal que a cardinalidade de I é infinita e $\leq \sup\{\kappa_i : i \in I\}$. Mostre que $\sum_{i \in I} \kappa_i = \sup\{\kappa_i : i \in I\}$.*

Dado um cardinal infinito \aleph_α , qual é o ordinal β que satisfaz a equação $2^{\aleph_\alpha} = \aleph_\beta$? A hipótese generalizada do contínuo diz que $\beta = \alpha + 1$:

$$\text{Hipótese generalizada do contínuo (HGC): } 2^{\aleph_\alpha} = \aleph_{\alpha+1}$$

A hipótese do contínuo é uma particularização de HGC:

$$\text{Hipótese do contínuo (HC): } 2^{\aleph_0} = \aleph_1$$

No modelo interno do universo construtível de Gödel, mencionado num capítulo anterior, também vale HGC pelo que a teoria $ZFC + HGC$ é consistente se ZF o for. Por sua vez, a técnica de *forcing* de Cohen permite construir modelos de ZFC em que HGC falha. De facto, já a teoria $ZFC + \neg HC$ é consistente relativamente a ZF .

Vamos finalizar esta secção demonstrando um resultado curioso: a fórmula de Hausdorff para cardinais.

Lema 19. *Toda a função $f : \omega_\alpha \mapsto \omega_{\alpha+1}$ é limitada, i.e., exists $\gamma < \omega_{\alpha+1}$ tal que $f(\beta) < \gamma$, para todo $\beta < \omega_\alpha$.*

Demonstração. Se f não é limitada, então $\omega_{\alpha+1} = \bigcup_{\beta < \omega_\alpha} f(\beta)$. Ora,

$$\text{card}\left(\bigcup_{\beta < \omega_\alpha} f(\beta)\right) \leq \sum_{\beta < \omega_\alpha} \aleph_\alpha = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha,$$

o que é um absurdo. □

Fórmula de Hausdorff. *Para todo α e β , tem-se $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$.*

Demonstração. Note-se que ambos os cardinais infinitos $\aleph_\alpha^{\aleph_\beta}$ e $\aleph_{\alpha+1}$ são $\leq \aleph_{\alpha+1}^{\aleph_\beta}$. Logo, o seu produto também é. Para mostrar a outra desigualdade, vamos dividir em dois casos. Suponhamos que $\alpha + 1 \leq \beta$. Vem:

$$\aleph_{\alpha+1}^{\aleph_\beta} \leq \aleph_\beta^{\aleph_\beta} \leq (2^{\aleph_\beta})^{\aleph_\beta} = 2^{\aleph_\beta \cdot \aleph_\beta} = 2^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}.$$

Resta estudar a desigualdade da esquerda para a direita para o caso em que $\beta \leq \alpha$. Pelo lema anterior, todo o elemento de $\omega_{\alpha+1}^{\omega_\beta}$ é uma função limitada. Logo:

$$\omega_{\alpha+1}^{\omega_\beta} = \bigcup_{\gamma < \omega_{\alpha+1}} \gamma^{\omega_\beta}.$$

Cada ordinal $\gamma < \omega_{\alpha+1}$ tem cardinalidade $\leq \aleph_\alpha$. Vem:

$$\aleph_{\alpha+1}^{\aleph_\beta} = \text{card}\left(\bigcup_{\gamma < \omega_{\alpha+1}} \gamma^{\omega_\beta}\right) \leq \sum_{\gamma < \omega_{\alpha+1}} \aleph_\alpha^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}. \quad \square$$

Exercício 97. *Dado $n < \omega$, mostre que $\aleph_n^{\aleph_\beta} = \aleph_n \cdot 2^{\aleph_\beta}$. [Sugestão: por indução em n , usando a fórmula de Hausdorff.]*

Exercício 98. *Mostre que $\aleph_\omega^{\aleph_1} = \aleph_\omega^{\aleph_0} \cdot 2^{\aleph_1}$. [Sugestão: $\aleph_\omega^{\aleph_1} \leq (\prod_{n < \omega} \aleph_n)^{\aleph_1} = \prod_{n < \omega} \aleph_n^{\aleph_1} = \prod_{n < \omega} \aleph_n \cdot 2^{\aleph_1} = (\prod_{n < \omega} \aleph_n) \cdot (2^{\aleph_1})^{\aleph_0} \leq \aleph_\omega^{\aleph_0} \cdot 2^{\aleph_1}$.]*

Chapter 27

O universo cumulativo

Definição 24 (Hierarquia cumulativa). *Define-se, por recursão transfinita nos ordinais, a seguinte operação $\alpha \rightsquigarrow V_\alpha$:*

$$\begin{cases} V_0 & = \emptyset \\ V_{\alpha+1} & = \mathcal{P}(V_\alpha) \\ V_\gamma & = \bigcup_{\beta < \gamma} V_\beta, \text{ se } \gamma \text{ é ordinal limite} \end{cases}$$

A classe constituída pelos conjuntos que estão nalgum V_α denota-se por V . Informalmente, $V = \bigcup_\alpha V_\alpha$.

Proposição 74. *Para ordinais α e β , têm-se as seguintes propriedades:*

1. $\forall x \forall y (x \in V_\alpha \wedge y \in x \rightarrow \exists \beta < \alpha (y \in V_\beta))$.
2. $\beta \leq \alpha \rightarrow V_\beta \subseteq V_\alpha$.
3. V_α é um conjunto transitivo.

Demonstração. A primeira propriedade demonstra-se por indução transfinita em α . Os casos em que α é 0 ou sucessor são imediatos. Suponhamos que α é ordinal limite. Por hipótese, $x \in V_\alpha$ e, portanto, $x \in V_\gamma$ para certo $\gamma < \alpha$. Por hipótese de indução transfinita, existe $\beta < \gamma$ tal que $y \in V_\beta$. Claro que $\beta < \alpha$.

A segunda propriedade também se demonstra por indução transfinita em α . Só o caso sucessor não é trivial. Seja $\beta \leq \alpha + 1$. Basta estudar o caso em que $\beta \leq \alpha$. Ora, por hipótese de indução transfinita, tem-se $V_\beta \subseteq V_\alpha$. Agora, basta mostrar que $V_\alpha \subseteq V_{\alpha+1}$. Tome-se $x \in V_\alpha$. Com vista a mostrar que $x \subseteq V_\alpha$, tome-se $y \in x$ ao arbítrio. Por (1), existe $\gamma < \alpha$ tal que $y \in V_\gamma$. Por hipótese de indução transfinita, $y \in V_\alpha$. Como se queria.

A terceira propriedade sai imediatamente das duas primeiras. \square

Exercício 99. *Seja ZF^- a teoria ZF sem o axioma da fundação. Mostre que ZF^- adicionado com a postulado $\forall x \exists \alpha (x \in V_\alpha)$ demonstra o axioma da fundação.*

Corolário 20. *Para todo o ordinal α , $\alpha \in V_{\alpha+1}$.*

Demonstração. A demonstração é por indução transfinita em α . O caso 0 é imediato, pois $V_1 = \{0\}$. Se, por hipótese de indução transfinita, $\alpha \in V_{\alpha+1}$

então, por (3) da proposição anterior, $\alpha \subseteq V_{\alpha+1}$. Conclui-se que $\alpha \cup \{\alpha\} \subseteq V_{\alpha+1}$, i.e., $\alpha + 1 \in V_{\alpha+2}$. Considere-se agora γ um ordinal limite. Por hipótese de indução transfinita, $\forall \alpha < \gamma (\alpha \in V_{\alpha+1})$. Logo, $\forall \alpha < \gamma (\alpha \in V_\gamma)$, ou seja, $\gamma \subseteq V_\gamma$. Portanto, $\gamma \in V_{\gamma+1}$. \square

Exercício 100. *Mostre que, para todo α , $\alpha \notin V_\alpha$.*

Do corolário acima conclui-se que a classe V contém todos os ordinais e, conseqüentemente, é uma classe própria. Vamos ver, de seguida, que a teoria ZF demonstra que a classe V é todo o universo dos conjuntos. Juntamente com o exercício 99, isto mostra que em ZF^- o axioma da fundação é equivalente a dizer que $\forall x \exists \alpha (x \in V_\alpha)$. Antes, porém, é conveniente demonstrar o seguinte lema que diz que o axioma da fundação também é verdadeiro para classes:

Lema 20. *Seja C uma classe não vazia. Então existe um elemento $y \in C$ tal que $y \cap C = \emptyset$.*

Demonstração. Tome-se $x \in C$. Seja $z = TC(\{x\})$, i.e., z é o fecho transitivo do conjunto singular $\{x\}$. Note-se que z é um conjunto transitivo e $x \in z$. Pelo axioma da separação, $z \cap C$ é um conjunto. Note-se que este conjunto é não vazio. Logo, pelo axioma da fundação, existe $y \in z \cap C$ tal que $y \cap z \cap C = \emptyset$. Como $y \subseteq z$ (visto que z é transitivo), vem $y \cap C = \emptyset$. \square

Proposição 75 (Princípio da \in -indução). *Seja C uma classe e admitamos que*

$$\text{(Condição de Progressão)} \quad \forall x ((\forall z \in x (z \in C)) \rightarrow x \in C),$$

então C é a classe universal.

Demonstração. Admitamos, com vista a um absurdo, que a classe complementar C^c é não vazia. Pelo lema anterior, existe $x \in C^c$ tal que $x \cap C^c = \emptyset$. Por outras palavras, se $z \in x$ então $z \in C$. Pela condição de progressão conclui-se que $x \in C$, o que é absurdo. \square

Teorema (Universo cumulativo). *Para todo o conjunto x , existe um ordinal α tal que $x \in V_\alpha$.*

Demonstração. Seja x um conjunto ao arbítrio e admitamos que, para todo $z \in x$, existe α tal que $z \in V_\alpha$. Então, podemos definir uma operação que, a cada elemento z de x , faz corresponder o menor número ordinal α tal que $z \in V_\alpha$. Pelo axioma da substituição, estes números ordinais formam um conjunto e, portanto, podemos tomar um ordinal β que os majore a todos. Temos, pois, $\forall z (z \in x \rightarrow z \in V_\beta)$, ou seja, $x \subseteq V_\beta$. Logo, $x \in V_{\beta+1}$. O resultado sai por \in -indução. \square

O teorema anterior mostra que todo o conjunto aparece numa certa etapa V_α da hierarquia cumulativa. O primeiro ordinal α tal que $x \in V_\alpha$ é, obviamente, um ordinal sucessor. Denota-se por $cota(x)$ o menor ordinal α tal que $x \in V_{\alpha+1}$. Note-se que $cota(\alpha) = \alpha$, para os ordinais α .

Exercício 101. *Mostre que, para todo o x , $cota(x) = \sup\{cota(y) + 1 : y \in x\}$.*

Contents

1	Estruturas de Dedekind-Peano	1
2	Princípio do mínimo	5
3	Teorema da recursão de Dedekind	6
4	Racionais positivos	8
5	A insuficiência dos números racionais	10
6	Cortes de Dedekind	12
7	Números reais	16
8	A unicidade dos números reais	20
9	Equipotência	23
10	Finitude e infinitude	26
11	Numerabilidade	29
12	A cardinalidade do <i>continuum</i>	31
13	O teorema de Cantor	33
14	Aritmética cardinal, sem cardinais...	35
15	Operações cardinais infinitárias	39
16	A teoria de Zermelo	41
17	A teoria ZFC	46
18	Boas ordens	50
19	Indução e recursão transfinita	52
20	Ordinais de von Neumann	54
21	Aritmética ordinal	58

<i>O universo cumulativo</i>	80
22 O colapso duma boa ordem	61
23 Teorema do ponto fixo de Zermelo	63
24 O lema de Zorn e tudo isso	65
25 O axioma da escolha na prática matemática	67
26 Números aléfes	73
27 O universo cumulativo	77

rescunho