

Chapter 9

Equipotência

Definição 1. *Dois conjuntos X e Y dizem-se equipotentes ou equinumeros 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 1. *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 2. *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 1. *Mostre que, para todo o conjunto X , $X \leq_c \mathcal{P}(X)$.*

Proposição 2. *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 .*

Demonstração. Suponhamos que $f : X \mapsto Y$ é uma injeção. Então este mesmo f mostra que há uma bijecção entre X e o subconjunto $\text{im} f$ de Y . Reciprocamente, seja $Z \subseteq Y$ e $f : X \mapsto Z$ uma bijecção. Claro que f se pode considerar uma injeção de X para Y . \square

O seguinte é imediato:

Proposição 3. Para todos os conjuntos X , Y e Z tem-se:

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

O seguinte resultado é crucial e de demonstração não imediata:

Teorema de Schröder-Bernstein. 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 2. 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 4. 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 3. Não é necessário apelar ao axioma da escolha para obter uma função escolha para \mathbb{N} . Porquê?

O axioma da escolha é hoje comumente 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 3. 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.

Exercício 4. Mostre que todo o subconjunto finito de \mathbb{N} tem máximo.

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 1. Sejam $n, m \in \mathbb{N}$ e $f : [n] \mapsto [m]$ uma injecção não sobrejectiva. Então $m \neq 0$ e existe uma injecção 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 5. Sejam $n, m \in \mathbb{N}$ com $m < n$. Não há injecções 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, $f|_{[n_0-1]}$ é uma injecção de $[n_0-1]$ para $[m]$ que não é sobrejectiva, pois $f(n_0-1) \notin \text{im} f|_{[n_0-1]}$. Pelo Lema 1, existe uma injecção de $[n_0-1]$ em $[m-1]$. Note que $m-1 < n_0-1$. Isto contradiz a minimalidade de n_0 . □

Corolário 1. 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 $\text{card}(X) = n$.

Exercício 5. *Seja $n \in \mathbb{N}$ e $X \subseteq [n]$. Mostre que X é finito e a sua cardinalidade é menor ou igual a n . Conclua que um subconjunto dum conjunto finito ainda é finito e de cardinalidade menor ou igual a este.*

Exercício 6. *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 da X e Y serem disjuntos, mostre que se tem a igualdade. [Sugestão: mostre primeiro o caso particular.]*

Exercício 7. *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 8. *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 1) existiria uma injectão de $[n]$ em $[n - 1]$, o que contradiz a proposição 5. \square

Exercício 9. *Seja X um conjunto finito e $f : X \mapsto X$ uma sobrejectão. Mostre que f é injectiva. [Sugestão: use a demonstração da Proposição 4 e o princípio dos cacifos.]*

Um conjunto X diz-se *infinito à Dedekind* se existir uma injectão 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 2. *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 $f(0) \notin \text{img}$. \square

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

Proposição 6. *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 tome-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 $n \rightsquigarrow a_n$ é uma função injectiva. \square

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

Exercício 10. *Mostre, sem utilizar o axioma da escolha, que se um conjunto X é infinito à Dedekind então $\mathbb{N} \leq_c X$.*

Chapter 11

Enumerabilidade

Definição 4. Um conjunto X diz-se enumerável ou contável se é vazio ou existe uma sobrejecção de \mathbb{N} em X .

Quando se considera um conjunto enumerável (não vazio), tomamo-lo na forma $\{a_0, a_1, a_2, \dots\}$. O que isto realmente significa é que a função $k \rightsquigarrow a_k$ é uma sobrejecção de \mathbb{N} sobre o conjunto em causa. Note que a lista a_0, a_1, a_2, \dots pode ter repetições, pois não se exige que a função seja injectiva.

Proposição 7. A imagem sobrejectiva de um conjunto enumerável ainda é enumerável.

Demonstração. Seja X um conjunto enumerável e $f : X \mapsto Y$ uma função sobrejectiva. Se $X = \emptyset$, então $Y = \emptyset$ e, portanto, Y é enumerável. Se $X \neq \emptyset$, então existe uma função sobrejectiva $h : \mathbb{N} \mapsto X$. Claro que $f \circ h$ é uma sobrejecção de \mathbb{N} sobre Y . \square

Corolário 3. Se X é enumerável e $Y \leq_c X$ então Y é enumerável.

Demonstração. Supomos $Y \neq \emptyset$. Como sabemos, se existe uma injeção de Y em X então existe uma sobrejecção de X em Y . O resultado sai pela proposição anterior. \square

É claro que \mathbb{N} é enumerável, o mesmo acontecendo com os conjuntos finitos. O conjunto \mathbb{Z} também é enumerável, bastando para tal considerar a enumeração $0, -1, 1, -2, 2, -3, 3, \dots$. Em geral, vê-se facilmente que a união de dois conjuntos enumeráveis é enumerável.

Proposição 8 (Cantor). $\mathbb{N} \times \mathbb{N}$ é enumerável.

Demonstração. Pode enumerar-se $\mathbb{N} \times \mathbb{N}$ do seguinte modo:

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

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 enumeração acima é dada pela função inversa desta bijecção.) \square

Corolário 4. O produto cartesiano de dois conjuntos enumeráveis é enumerável.

Demonstração. Sejam X e Y enumeráveis (não vazios). Tomem-se f e g sobrejecções de \mathbb{N} sobre X e Y , respectivamente. Claro que $(n, m) \rightsquigarrow (f(n), g(m))$ é uma sobrejecção de $\mathbb{N} \times \mathbb{N}$ sobre $X \times Y$. Visto que $\mathbb{N} \times \mathbb{N}$ é enumerável, o resultado sai imediatamente. \square

Pode agora ver-se facilmente que \mathbb{Q} também é enumerável. Como \mathbb{Z} e \mathbb{N}^+ são enumeráveis, pelo corolário anterior, $\mathbb{Z} \times \mathbb{N}^+$ é enumerável. Ora, $(n, m) \rightsquigarrow \frac{n}{m}$ é uma sobrejecção de $\mathbb{Z} \times \mathbb{N}^+$ sobre \mathbb{Q} . Logo, \mathbb{Q} é enumerável. Iremos ver no início do próximo capítulo que \mathbb{R} não é enumerável.

Proposição 9. *Uma união enumerável de conjuntos enumeráveis é enumerável. Dito de outro modo, se $(X_n)_{n \in \mathbb{N}}$ é uma sucessão de conjuntos enumeráveis, então $\bigcup_{n \in \mathbb{N}} X_n$ é enumerável.*

Demonstração. Sem perda de generalidade, podemos supor que todos os conjuntos X_n são não vazios. Para cada $n \in \mathbb{N}$ escolha-se uma sobrejecção 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 11. *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 $P_{\text{fin}}(\mathbb{N})$ é enumerável. 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 enumerável. 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 $P_{\leq n}(\mathbb{N}) \setminus \{\emptyset\}$. Como \mathbb{N}^n é enumerável, conclui-se que $\mathcal{P}_{\leq n}(\mathbb{N})$ é enumerável.

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 $\sqrt{2}$, $(1 + \sqrt{3})^2$ (porquê?). 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 enumerável. Com efeito, o conjunto de todos os polinómios não nulos de coeficientes inteiros é enumerável visto que é constituído pela união enumerável 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 e, portanto, enumerável. Logo, o conjunto dos números algébricos é uma união enumerável de conjuntos enumeráveis. É, portanto, enumerável.

Definição 5. *Um conjunto diz-se numerável se for equipotente a \mathbb{N} .*

Proposição 10. *Um conjunto é enumerável se, e somente se, é finito ou numerável.*

Corolário 5. *Se $X \leq_c \mathbb{N}$ então X é finito ou numerável.*

O corolário é consequência imediata da proposição e do Corolário 3. A proposição tem uma demonstração imediata desde que se use o axioma da escolha. Basta mostrar que se X é enumerável e infinito então $X =_c \mathbb{N}$. Como X é infinito, então $\mathbb{N} \leq_c X$. Por outro lado, como X é imagem sobrejectiva de \mathbb{N} sai que $X \leq_c \mathbb{N}$. Pelo teorema de Schröder-Bernstein, $X =_c \mathbb{N}$. Há, no entanto, uma demonstração alternativa que não usa o axioma da escolha:

Lema 3. *Todo o subconjunto infinito de \mathbb{N} é enumerável.*

Demonstração. Seja $X \subseteq \mathbb{N}$ infinito. Define-se facilmente por recursão uma função $f : \mathbb{N} \rightarrow X$ tal que $f(0) = \min X$ e $f(n+1) = \min\{k \in X : f(n) < k\}$. Por definição, $f(n) < f(n+1)$ e daqui sai facilmente que f é injectiva. Admitamos, com vista a um absurdo, que $\text{im } f \neq X$. Tome-se m o menor elemento de X que não está em $\text{im } f$. Claro que $m \neq \min X$. Seja r o maior elemento de X menor do que m . Por minimalidade de m , $r = f(n)$ para algum $n \in \mathbb{N}$. Mas, então, $f(n+1) = \min\{k \in X : r < k\} = m$, o que é absurdo. \square

Lema 4. *Todo o conjunto enumerável infinito é enumerável.*

Demonstração. Seja X um conjunto enumerável infinito e $f : \mathbb{N} \rightarrow X$ uma sobrejecção. Defina-se $I := \{n \in \mathbb{N} : \forall m \in \mathbb{N} (m < n \rightarrow f(m) \neq f(n))\}$. Vamos ver que $f|_I$ é uma bijecção de I sobre X . Isto demonstra o resultado pois, como X é infinito, vem que I é infinito e, pela proposição anterior, infere-se que I é enumerável. Ergo, X é enumerável. Claramente, $f|_I$ é injectiva. Tome-se agora $x \in X$. Considere-se o menor número natural n tal que $f(n) = x$. Trivialmente, $n \in I$. \square

Chapter 12

A cardinalidade do *continuum*

O seguinte argumento de *diagonalização* é famoso:

Proposição 11. *O conjunto $\{0, 1\}^{\mathbb{N}}$ não é enumerável.*

Demonstração. Suponhamos, com vista a um absurdo, que existe uma sobrejecção f de \mathbb{N} sobre $\{0, 1\}^{\mathbb{N}}$. 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

Proposição 12. $\mathbb{R} =_c \{0, 1\}^{\mathbb{N}}$. *Em particular, \mathbb{R} não é enumerável.*

Demonstração. Considere-se a função $x \rightsquigarrow \{q \in \mathbb{Q} : q < x\}$. É muito fácil de ver que esta função é uma injecção 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, $\mathbb{R} \leq_c \{0, 1\}^{\mathbb{N}}$. Por outro lado, a correspondência $f \rightsquigarrow \sum_{n=0}^{\infty} \frac{2f(n)}{3^n}$ é uma injecção de $\{0, 1\}^{\mathbb{N}}$ em \mathbb{R} (de facto, no intervalo real $[0, 3]$).

O resultado sai pelo teorema de Schröder-Bernstein. \square

Da discussão acima conclui-se que o conjunto dos números reais, também chamado de *continuum* real, não é numerável sendo, de facto, equipotente a $\mathcal{P}(\mathbb{N})$. O seguinte resultado, também devido a Georg Cantor, generaliza o teorema 11.

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 sobre $\mathcal{P}(X)$. 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:

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

mas, é claro, as cardinalidades não se esgotam aqui. Por exemplo, será que há cardinalidades estritamente entre \mathbb{N} e $\mathcal{P}(\mathbb{N})$? Por outro lado, em ZFC 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.

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 13 (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 $\bigcup_{i \in I} X_i \leq_c \prod_{i \in I} Y_i$. 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 13

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 a um objecto sob uma dada relação de equivalência é a 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 \mathfrak{c} . A solução geral para o problema da cardinalidade consiste no desenvolvimento duma teoria geral de números que estenda a teoria dos números naturais: os números *ordinais* de von Neumann. Iremos mais tarde desenvolver esta teoria e, para isso, necessitamos de formular a axiomática da teoria dos conjuntos ZFC (notavelmente o axioma da substituição). Deixamos esta tarefa para mais tarde.

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 elipse para 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. Vamos pois, neste capítulo, interpretar as asserções sobre cardinais deste modo elíptico (o que pressupõe que se possam interpretar desta forma). Por exemplo, teorema de 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 5, 6, 7 e 8 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 14. *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 enumerável, então $B \setminus A$ tem cardinalidade \mathfrak{c} .*

Demonstração. A alínea (a) é uma reformulação do Corolário 5. (b) é uma reformulação do facto de que $\mathbb{R} =_c \{0, 1\}^{\mathbb{N}}$. (c) sai do facto de que $\mathbb{N} \leq_c \mathbb{R}$, da Proposição 11 e da alínea anterior. $\aleph_0 \cdot \aleph_0 = \aleph_0$ sai da demonstração da Proposição 8. 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 enumerável, P é enumerável. 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 Schröder-Bernstein. \square

A última alínea da proposição anterior permite, por exemplo, mostrar que o conjunto dos números reais *transcendentes* (i.e., os números reais que não são algébricos) tem cardinalidade \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 anterior não usa o axioma da escolha). Com efeito, num capítulo subsequente demonstraremos, com a ajuda do axioma da escolha, a seguinte propriedade importante:

Proposição 15 (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 κ é um cardinal infinito então $\kappa \cdot \kappa = \kappa$. Por outras palavras, para todo o conjunto infinito X , tem-se $X \times X =_c X$. Como já discutimos, 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

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 $\bigcup_{i \in I} (\{i\} \times A_i) =_c \bigcup_{i \in I} (\{i\} \times B_i)$. 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 . Por exemplo, se κ é a cardinalidade do conjunto I , então $\prod_{i \in I} 2 = 2^\kappa$. Isto é trivial, pois esta igualdade diz literalmente que $\{0, 1\}^I =_c \{0, 1\}^I$. 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 $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$.