Parte I

Teoria Ingênua dos Conjuntos

The material in this part is an introduction to basic naive set theory. With the inclusion of Tim Button's Teoria dos Conjuntos Aberta, this also covers the construction of number systems, and discussion of infinity, which are not required for the logical parts of the OLP.

Capítulo 1

Conjuntos

1.1 Extensionalidade

sfr:set:bas:sec

Um *conjunto* é uma coleção de objetos, considerada como um único objeto. Os objetos que compõem o conjunto chamam-se *elementos* ou *membros* do conjunto. Se x é um membro de um conjunto A, escrevemos $x \in A$; caso contrário, escrevemos $x \notin A$. O conjunto que não tem membros chama-se o *conjunto vazio* e denota-se "$\emptyset$".

Não importa como *especificamos* o conjunto, ou como *ordenamos* os seus membros, ou mesmo quantas *vezes* contamos os seus membros. Só importa quais são os seus membros. Codificamos isto no princípio seguinte. explanation

Definição 1.1 (Extensionalidade). Se A e B são conjuntos, então $A = B$ se e só se todo membro de A é também um membro de B, e vice-versa.

A extensionalidade autoriza certa notação. Em geral, quando temos objetos $a_1, \ldots, a_n$, então $\{a_1, \ldots, a_n\}$ é *o* conjunto cujos membros são $a_1, \ldots, a_n$. Enfatizamos a palavra "*o*", pois a extensionalidade nos diz que só pode haver *um* tal conjunto. De fato, a extensionalidade também autoriza o seguinte:

$$\{a, a, b\} = \{a, b\} = \{b, a\}.$$

Isto traduz a ideia de que, quando consideramos conjuntos, não nos importa a ordem dos seus membros, nem quantas vezes são especificados.

Exemplo 1.2. Sempre que temos vários objetos, podemos reuni-los num conjunto. O conjunto dos irmãos de Richard, por exemplo, é um conjunto que contém uma pessoa, e podemos escrevê-lo como $S = \{\text{Ruth}\}$. O conjunto dos inteiros positivos menores que 4 é $\{1, 2, 3\}$, mas também se pode escrever como $\{3, 2, 1\}$ ou mesmo como $\{1, 2, 1, 2, 3\}$. São todos o mesmo conjunto, pela extensionalidade. De fato, todo membro de $\{1, 2, 3\}$ é também um membro de $\{3, 2, 1\}$ (e de $\{1, 2, 1, 2, 3\}$), e vice-versa.

Com frequência especificaremos um conjunto por alguma propriedade que os seus membros compartilham. Usaremos a seguinte notação abreviada para

isso: $\{x : \varphi(x)\}$, onde $\varphi(x)$ representa a propriedade que x tem de satisfazer para ser contado entre os membros do conjunto.

Exemplo 1.3. No nosso exemplo, também poderíamos ter especificado S como

$$S = \{x : x \text{ é irmão de Richard}\}.$$

Exemplo 1.4. Diz-se que um número é *perfeito* se e só se for igual à soma dos seus divisores próprios (isto é, números que o dividem sem resto mas não são iguais ao próprio número). Por exemplo, 6 é perfeito porque os seus divisores próprios são 1, 2, e 3, e $6 = 1+2+3$. De fato, 6 é o único inteiro positivo menor que 10 que é perfeito. Assim, usando a extensionalidade, podemos dizer:

$$\{6\} = \{x : x \text{ é perfeito e } 0 \leq x \leq 10\}$$

Lemos a notação à direita como "o conjunto dos x tais que x é perfeito e $0 \leq x \leq 10$". A identidade aqui confirma que, quando consideramos conjuntos, não nos importa como são especificados. E, mais em geral, a extensionalidade garante que há sempre apenas um conjunto dos x tais que $\varphi(x)$. Logo, a extensionalidade justifica chamar a $\{x : \varphi(x)\}$ *o* conjunto dos x tais que $\varphi(x)$.

A extensionalidade nos dá um modo de mostrar que conjuntos são idênticos: para mostrar que $A = B$, mostre que sempre que $x \in A$ então também $x \in B$, e sempre que $y \in B$ então também $y \in A$.

Problema 1.1. Prove que há no máximo um conjunto vazio, isto é, mostre que se A e B são conjuntos sem membros, então $A = B$.

1.2 Subconjuntos e conjuntos potência

explanation

Com frequência quereremos comparar conjuntos. E um tipo óbvio de comparação que se pode fazer é o seguinte: *tudo o que está num conjunto está também no outro*. Esta situação é suficientemente importante para introduzirmos nova notação.

sfr:set:sub:sec

Definição 1.5 (Subconjunto). Se todo membro de um conjunto A é também um membro de B, então dizemos que A é um *subconjunto* de B, e escrevemos $A \subseteq B$. Se A não é subconjunto de B, escrevemos $A \nsubseteq B$. Se $A \subseteq B$ mas $A \neq B$, escrevemos $A \subsetneq B$ e dizemos que A é um *subconjunto próprio* de B.

Exemplo 1.6. Todo conjunto é subconjunto de si próprio, e $\emptyset$ é subconjunto de todo conjunto. O conjunto dos números naturais pares é subconjunto do conjunto dos números naturais. Também $\{a, b\} \subseteq \{a, b, c\}$. Mas $\{a, b, e\}$ não é subconjunto de $\{a, b, c\}$.

Exemplo 1.7. O número 2 é um membro do conjunto dos inteiros, ao passo que o conjunto dos números pares é subconjunto do conjunto dos inteiros. Contudo, um conjunto pode tanto ser um membro quanto subconjunto de algum outro conjunto, por exemplo, $\{0\} \in \{0, \{0\}\}$ e também $\{0\} \subseteq \{0, \{0\}\}$.

A extensionalidade dá um critério de identidade para conjuntos: $A = B$ se e só se todo membro de A é também um membro de B e vice-versa. A definição de "subconjunto" define $A \subseteq B$ precisamente como a primeira metade deste critério: todo membro de A é também um membro de B. Claro que a definição também se aplica se trocarmos A e B: isto é, $B \subseteq A$ se e só se todo membro de B é também um membro de A. E isso, por sua vez, é exatamente a parte "vice-versa" da extensionalidade. Em outras palavras, a extensionalidade implica que conjuntos são iguais se e só se são subconjuntos um do outro.

Proposição 1.8. *$A = B$ se e só se $A \subseteq B$ e $B \subseteq A$.*

Agora é também boa ocasião para introduzir mais alguma notação útil. Ao definir quando A é subconjunto de B dissemos que "todo membro de A é ...," e preenchemos os "..." com "um membro de B". Mas esta é uma *forma* tão comum de expressão que convém introduzir notação formal para ela.

sfr:set:sub:forallxina

Definição 1.9. $(\forall x \in A)\varphi$ abrevia $\forall x(x \in A \to \varphi)$. Do mesmo modo, $(\exists x \in A)\varphi$ abrevia $\exists x(x \in A \wedge \varphi)$.

Com esta notação, podemos dizer que $A \subseteq B$ se e só se $(\forall x \in A)x \in B$.

Passamos agora a considerar um certo tipo de conjunto: o conjunto de todos os subconjuntos de um dado conjunto.

Definição 1.10 (Conjunto potência). O conjunto constituído por todos os subconjuntos de um conjunto A chama-se o *conjunto potência* de A, e denota-se $\wp(A)$.

$$\wp(A) = \{B : B \subseteq A\}$$

Exemplo 1.11. Quais são todos os subconjuntos possíveis de $\{a, b, c\}$? São: $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$. O conjunto de todos estes subconjuntos é $\wp(\{a, b, c\})$:

$$\wp(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

Problema 1.2. Liste todos os subconjuntos de $\{a, b, c, d\}$.

Problema 1.3. Mostre que se A tem n membros, então $\wp(A)$ tem 2^n membros.

1.3 Alguns Conjuntos Importantes

sfr:set:imp:sec

Exemplo 1.12. Trabalharemos sobretudo com conjuntos cujos membros são objetos matemáticos. Quatro desses conjuntos são tão importantes que têm

nomes específicos:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
o conjunto dos números naturais

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
o conjunto dos números inteiros

$$\mathbb{Q} = \{m/n : m, n \in \mathbb{Z} \text{ e } n \neq 0\}$$
o conjunto dos números racionais

$$\mathbb{R} = (-\infty, \infty)$$
o conjunto dos números reais (o contínuo)

São todos conjuntos *infinitos*, isto é, cada um tem infinitos membros.

À medida que percorremos estes conjuntos, vamos acrescentando *mais* números ao nosso repertório. De fato, deve ficar claro que $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$: afinal, todo número natural é um inteiro; todo inteiro é racional; e todo racional é real. Igualmente, deve ficar claro que $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, pois -1 é inteiro mas não natural, e $1/2$ é racional mas não inteiro. É menos óbvio que $\mathbb{Q} \subsetneq \mathbb{R}$, isto é, que há números reais que não são racionais.

Também usaremos por vezes o conjunto dos inteiros positivos $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ e o conjunto que contém apenas os dois primeiros naturais $\mathbb{B} = \{0, 1\}$.

Exemplo 1.13 (Cadeias). Outro exemplo interessante é o conjunto A^* das *cadeias finitas* sobre um alfabeto A: qualquer sequência finita de elementos de A é uma cadeia sobre A. Incluímos a *cadeia vazia* Λ entre as cadeias sobre A, para todo alfabeto A. Por exemplo,

$$\mathbb{B}^* = \{\Lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \ldots\}.$$

Se $x = x_1 \ldots x_n \in A^*$ é uma cadeia constituída por n "letras" de A, então dizemos que o *comprimento* da cadeia é n e escrevemos $\text{len}(x) = n$.

Exemplo 1.14 (Sequências infinitas). Para qualquer conjunto A podemos também considerar o conjunto A^ω das sequências infinitas de membros de A. Uma sequência infinita $a_1 a_2 a_3 a_4 \ldots$ consiste numa lista infinita numa só direção de objetos, cada um dos quais é um membro de A.

1.4 Uniões e Interseções

explanation Na Seção 1.1, introduzimos definições de conjuntos por abstração, isto é, definições da forma $\{x : \varphi(x)\}$. Aqui invocamos alguma propriedade φ, e essa propriedade pode mencionar conjuntos que já definimos. Assim, por exemplo, se A e B são conjuntos, o conjunto $\{x : x \in A \vee x \in B\}$ consiste em todos aqueles objetos que são membros de A ou de B, isto é, é o conjunto que reúne

sfr:set:uni:sec

os membros de A e B. Podemos visualizar isto como na Figura 1.1, onde a área realçada indica os membros dos dois conjuntos A e B juntos.

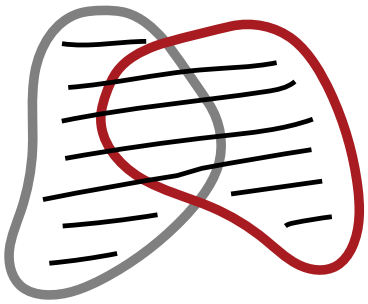


Figura 1.1: A união $A \cup B$ de dois conjuntos é o conjunto dos membros de A juntamente com os de B.

sfr:set:uni:
fig:union

Esta operação sobre conjuntos—combiná-los—é muito útil e comum, e por isso damos-lhe um nome formal e um símbolo.

Definição 1.15 (União). A *união* de dois conjuntos A e B, escrita $A \cup B$, é o conjunto de todas as coisas que são membros de A, de B, ou de ambos.

$$A \cup B = \{x : x \in A \vee x \in B\}$$

Exemplo 1.16. Como a multiplicidade de membros não importa, a união de dois conjuntos que têm um membro em comum contém esse membro apenas uma vez, por exemplo, $\{a, b, c\} \cup \{a, 0, 1\} = \{a, b, c, 0, 1\}$.

A união de um conjunto com um dos seus subconjuntos é simplesmente o conjunto maior: $\{a, b, c\} \cup \{a\} = \{a, b, c\}$.

A união de um conjunto com o conjunto vazio é idêntica ao conjunto: $\{a, b, c\} \cup \emptyset = \{a, b, c\}$.

Problema 1.4. Prove que se $A \subseteq B$, então $A \cup B = B$.

explanation

Também podemos considerar uma operação "dual" à união. É a operação que forma o conjunto de todos os membros que são membros de A e são também membros de B. Esta operação chama-se *interseção*, e pode representar-se como na Figura 1.2.

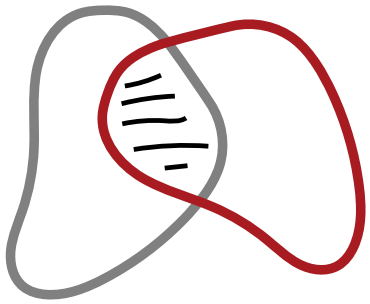


Figura 1.2: A interseção $A \cap B$ de dois conjuntos é o conjunto dos membros que têm em comum.

sfr:set:uni: fig:intersection

Definição 1.17 (Interseção). A *interseção* de dois conjuntos A e B, escrita $A \cap B$, é o conjunto de todas as coisas que são membros de ambos A e B.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

Dois conjuntos dizem-se *disjuntos* se a sua interseção é vazia. Isso significa que não têm membros em comum.

Exemplo 1.18. Se dois conjuntos não têm membros em comum, a sua interseção é vazia: $\{a, b, c\} \cap \{0, 1\} = \emptyset$.

Se dois conjuntos têm membros em comum, a sua interseção é o conjunto de todos esses membros: $\{a, b, c\} \cap \{a, b, d\} = \{a, b\}$.

A interseção de um conjunto com um dos seus subconjuntos é simplesmente o conjunto menor: $\{a, b, c\} \cap \{a, b\} = \{a, b\}$.

A interseção de qualquer conjunto com o conjunto vazio é vazia: $\{a, b, c\} \cap \emptyset = \emptyset$.

Problema 1.5. Prove rigorosamente que se $A \subseteq B$, então $A \cap B = A$.

explanation

Também podemos formar a união ou a interseção de mais de dois conjuntos. Uma forma elegante de tratar disso em geral é a seguinte: suponhamos que reunimos num único conjunto todos os conjuntos dos quais queremos formar a união (ou a interseção). Então podemos definir a união de todos os nossos conjuntos originais como o conjunto de todos os objetos que pertencem a pelo menos um membro desse conjunto, e a interseção como o conjunto de todos os objetos que pertencem a todo membro desse conjunto.

Definição 1.19. Se A é um conjunto de conjuntos, então $\bigcup A$ é o conjunto dos membros dos membros de A:

$$\begin{aligned} \bigcup A &= \{x : x \text{ pertence a um membro de } A\}, \text{ isto é,} \\ &= \{x : \text{existe um } B \in A \text{ tal que } x \in B\} \end{aligned}$$

Definição 1.20. Se A é um conjunto de conjuntos, então $\bigcap A$ é o conjunto dos objetos que todos os elementos de A têm em comum:

$$\begin{aligned}\bigcap A &= \{x : x \text{ pertence a todo membro de } A\}, \text{ isto é,}\\ &= \{x : \text{para todo } B \in A, x \in B\}\end{aligned}$$

Exemplo 1.21. Suponha $A = \{\{a, b\}, \{a, d, e\}, \{a, d\}\}$. Então $\bigcup A = \{a, b, d, e\}$ e $\bigcap A = \{a\}$.

Problema 1.6. Mostre que se A é um conjunto e $A \in B$, então $A \subseteq \bigcup B$.

Também poderíamos fazer o mesmo para uma sequência de conjuntos A_1, A_2, ...

$$\begin{aligned}\bigcup_i A_i &= \{x : x \text{ pertence a um dos } A_i\}\\ \bigcap_i A_i &= \{x : x \text{ pertence a todos os } A_i\}.\end{aligned}$$

Quando temos um *índice* de conjuntos, isto é, algum conjunto I tal que consideramos A_i para cada $i \in I$, podemos também usar estas abreviaturas:

$$\begin{aligned}\bigcup_{i\in I} A_i &= \bigcup\{A_i : i \in I\}\\ \bigcap_{i\in I} A_i &= \bigcap\{A_i : i \in I\}\end{aligned}$$

Finalmente, podemos querer pensar no conjunto de todos os membros em A que não estão em B. Podemos representá-lo como na Figura 1.3.

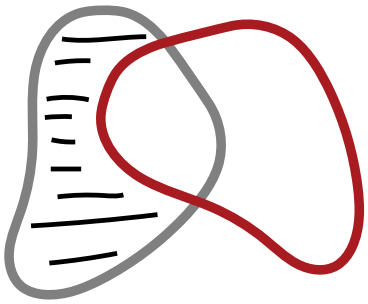


Figura 1.3: A diferença $A \setminus B$ de dois conjuntos é o conjunto dos membros de A que não são também membros de B.

sfr:set:uni:difference

Definição 1.22 (Diferença). A *diferença* de conjuntos $A \setminus B$ é o conjunto de todos os membros de A que não são também membros de B, isto é,

$$A \setminus B = \{x : x \in A \text{ e } x \notin B\}.$$

Problema 1.7. Prove que se $A \subsetneq B$, então $B \setminus A \neq \emptyset$.

1.5 Pares, Tuplas, Produtos Cartesianos

explanation

Da extensionalidade segue-se que os conjuntos não têm ordem entre os seus elementos. Por isso, se queremos representar ordem, usamos *pares ordenados* $\langle x, y\rangle$. Num par não ordenado $\{x, y\}$, a ordem não importa: $\{x, y\} = \{y, x\}$. Num par ordenado, importa: se $x \neq y$, então $\langle x, y\rangle \neq \langle y, x\rangle$.

sfr:set:pai:sec

Como devemos pensar os pares ordenados na teoria dos conjuntos? O essencial é preservar a ideia de que pares ordenados são idênticos se e só se compartilham o mesmo primeiro elemento e o mesmo segundo elemento, isto é:

$$\langle a, b\rangle = \langle c, d\rangle \text{ se e só se } a = c \text{ e } b = d.$$

Podemos definir pares ordenados na teoria dos conjuntos usando a definição de Wiener–Kuratowski.

Definição 1.23 (Par ordenado). $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$.

sfr:set:pai:wienerkuratowski

Problema 1.8. Usando Definição 1.23, prove que $\langle a, b\rangle = \langle c, d\rangle$ se e só se $a = c$ e $b = d$.

explanation

Tendo fixado uma definição de par ordenado, podemos usá-la para definir outros conjuntos. Por exemplo, por vezes queremos sequências ordenadas de mais de dois objetos, p.ex., *triplos* $\langle x, y, z\rangle$, *quádruplos* $\langle x, y, z, u\rangle$, e assim por diante. Podemos pensar nos triplos como pares ordenados especiais, em que o primeiro elemento é ele próprio um par ordenado: $\langle x, y, z\rangle$ é $\langle\langle x, y\rangle, z\rangle$. O mesmo vale para quádruplos: $\langle x, y, z, u\rangle$ é $\langle\langle\langle x, y\rangle, z\rangle, u\rangle$, e assim por diante. Em geral, falamos de *n-tuplas ordenadas* $\langle x_1, \ldots, x_n\rangle$.

Certos conjuntos de pares ordenados, ou outras n-tuplas ordenadas, serão úteis.

Definição 1.24 (Produto cartesiano). Dados conjuntos A e B, o seu *produto cartesiano* $A \times B$ é definido por

$$A \times B = \{\langle x, y\rangle : x \in A \text{ e } y \in B\}.$$

Exemplo 1.25. Se $A = \{0, 1\}$, e $B = \{1, a, b\}$, então o seu produto é

$$A \times B = \{\langle 0, 1\rangle, \langle 0, a\rangle, \langle 0, b\rangle, \langle 1, 1\rangle, \langle 1, a\rangle, \langle 1, b\rangle\}.$$

Exemplo 1.26. Se A é um conjunto, o produto de A consigo próprio, $A \times A$, também se escreve A^2. É o conjunto de *todos* os pares $\langle x, y\rangle$ com $x, y \in A$. O conjunto de todos os triplos $\langle x, y, z\rangle$ é A^3, e assim por diante. Podemos dar uma definição recursiva:

$$A^1 = A$$
$$A^{k+1} = A^k \times A$$

Problema 1.9. Liste todos os membros de $\{1, 2, 3\}^3$.

sfr:set:pai: cardnmprod **Proposição 1.27.** *Se A tem n membros e B tem m membros, então $A \times B$ tem $n \cdot m$ elementos.*

Prova. Para todo membro x em A, há m membros da forma $\langle x, y\rangle \in A \times B$. Seja $B_x = \{\langle x, y\rangle : y \in B\}$. Como sempre que $x_1 \neq x_2$, $\langle x_1, y\rangle \neq \langle x_2, y\rangle$, tem-se $B_{x_1} \cap B_{x_2} = \emptyset$. Mas se $A = \{x_1, \ldots, x_n\}$, então $A \times B = B_{x_1} \cup \cdots \cup B_{x_n}$, e portanto tem $n \cdot m$ membros.

Para visualizar isto, dispomos os membros de $A \times B$ numa grade:

$$\begin{array}{rccccc} B_{x_1} = & \{\langle x_1, y_1\rangle & \langle x_1, y_2\rangle & \ldots & \langle x_1, y_m\rangle\} \\ B_{x_2} = & \{\langle x_2, y_1\rangle & \langle x_2, y_2\rangle & \ldots & \langle x_2, y_m\rangle\} \\ \vdots & & \vdots & & \\ B_{x_n} = & \{\langle x_n, y_1\rangle & \langle x_n, y_2\rangle & \ldots & \langle x_n, y_m\rangle\} \end{array}$$

Como os x_i são todos distintos, e os y_j são todos distintos, quaisquer dois pares nesta grade são distintos, e há $n \cdot m$ deles. □

Problema 1.10. Mostre, por indução em k, que para todo $k \geq 1$, se A tem n membros, então A^k tem n^k membros.

Exemplo 1.28. Se A é um conjunto, uma *palavra* sobre A é qualquer sequência de membros de A. Uma sequência pode ser vista como uma n-tupla de membros de A. Por exemplo, se $A = \{a, b, c\}$, então a sequência "bac" pode ser vista como o triplo $\langle b, a, c\rangle$. Palavras, isto é, sequências de símbolos, são de importância crucial na ciência da computação. Por convenção, contamos os membros de A como sequências de comprimento 1, e $\emptyset$ como a sequência de comprimento 0. O conjunto de *todas* as palavras sobre A é então

$$A^* = \{\emptyset\} \cup A \cup A^2 \cup A^3 \cup \ldots$$

1.6 Paradoxo de Russell

sfr:set:rus: sec A extensionalidade autoriza a notação $\{x : \varphi(x)\}$, para *o* conjunto dos x tais que $\varphi(x)$. Contudo, tudo o que a extensionalidade *realmente* autoriza é o seguinte pensamento. *Se* há um conjunto cujos membros são exatamente os que satisfazem φ, *então* há apenas um tal conjunto. Dito de outro modo: fixada alguma φ, o conjunto $\{x : \varphi(x)\}$ é único, *se existir*.

Mas este condicional é importante! Crucialmente, nem toda propriedade se presta à *compreensão*. Isto é, algumas propriedades *não* definem conjuntos. Se todas definissem, cairíamos em contradições flagrantes. O exemplo mais famoso disso é o Paradoxo de Russell.

Os conjuntos podem ser membros de outros conjuntos—por exemplo, o conjunto potência de um conjunto A é constituído por conjuntos. Por isso faz sentido perguntar ou investigar se um conjunto é um membro de outro conjunto. Pode um conjunto ser membro de si próprio? Nada na ideia de conjunto parece excluir isso. Por exemplo, se *todos* os conjuntos formam uma coleção de objetos,

alguém poderia pensar que podem reunir-se num único conjunto—o conjunto de todos os conjuntos. E ele, sendo conjunto, seria um membro do conjunto de todos os conjuntos.

O Paradoxo de Russell surge quando consideramos a propriedade de não ter a si próprio como um membro, de ser *não auto-membro*. E se supusermos que há um conjunto de todos os conjuntos que não têm a si próprios como um membro? Será que

$$R = \{x : x \notin x\}$$

existe? Verifica-se que podemos provar que não.

Teorema 1.29 (Paradoxo de Russell). *Não há conjunto* $R = \{x : x \notin x\}$. *sfr:set:rus: thm:russells-paradox*

Prova. Se $R = \{x : x \notin x\}$ existisse, então $R \in R$ se e só se $R \notin R$, o que é uma contradição. □

explanation Vamos percorrer esta prova mais devagar. Se R existe, faz sentido perguntar se $R \in R$ ou não. Suponhamos que de fato $R \in R$. Agora, R foi definido como o conjunto de todos os conjuntos que não são membros de si próprios. Logo, se $R \in R$, então R não tem a propriedade definidora de R. Mas só os conjuntos que têm essa propriedade estão em R, logo R não pode ser um membro de R, isto é, $R \notin R$. Mas R não pode ao mesmo tempo ser e não ser um membro de R, logo temos uma contradição.

Como a suposição de que $R \in R$ leva a uma contradição, temos $R \notin R$. Mas isto também leva a uma contradição! Pois se $R \notin R$, então R tem a propriedade definidora de R, e assim R seria um membro de R, tal como todos os outros conjuntos não auto-membros. E de novo, R não pode ao mesmo tempo não ser e ser um membro de R.

digression Como montar uma teoria dos conjuntos que evite cair no Paradoxo de Russell, isto é, que evite afirmar de modo *inconsistente* que $R = \{x : x \notin x\}$ existe? Teríamos de estabelecer axiomas que nos dêem condições muito precisas para dizer quando os conjuntos existem (e quando não existem).

A teoria dos conjuntos esboçada neste capítulo não faz isso. É *genuinamente ingênua*. Diz apenas que os conjuntos obedecem à extensionalidade e que, se temos alguns conjuntos, podemos formar a sua união, interseção, etc. É possível desenvolver a teoria dos conjuntos com mais rigor do que isto.

Capítulo 2

Relações

2.1 Relações como Conjuntos

sfr:rel:set:sec

Na Seção 1.3, mencionamos alguns conjuntos importantes: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Sem dúvida que se lembram de algumas relações interessantes entre os membros de alguns destes conjuntos. Por exemplo, cada um destes conjuntos tem uma *relação de ordem* completamente padrão sobre si. Há também a relação *ser idêntico a*, segundo a qual cada objeto só se relaciona consigo próprio e com nenhum outro. Há muitas outras relações interessantes que encontraremos, e ainda mais relações possíveis. Antes de as revermos, contudo, começaremos por observar que podemos ver relações como um tipo especial de conjunto. explanation

Para isso, recordemos duas coisas da Seção 1.5. Primeiro, recordemos a noção de *par ordenado*: dados a e b, podemos formar $\langle a, b\rangle$. É importante notar que a ordem dos elementos *importa* aqui. Assim, se $a \neq b$ então $\langle a, b\rangle \neq \langle b, a\rangle$. (Contrastemos isto com pares não ordenados, isto é, conjuntos de 2 elementos, onde $\{a, b\} = \{b, a\}$.) Segundo, recordemos a noção de *produto cartesiano*: se A e B são conjuntos, então podemos formar $A \times B$, o conjunto de todos os pares $\langle x, y\rangle$ com $x \in A$ e $y \in B$. Em particular, $A^2 = A \times A$ é o conjunto de todos os pares ordenados de A.

Consideremos agora uma relação particular num conjunto: a relação $<$ no conjunto $\mathbb{N}$ dos números naturais. Seja o conjunto de todos os pares de números $\langle n, m\rangle$ onde $n < m$, isto é,

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}.$$

Há uma ligação estreita entre n ser menor que m, e o par $\langle n, m\rangle$ ser membro de R, nomeadamente:

$$n < m \text{ se e só se } \langle n, m\rangle \in R.$$

De fato, sem qualquer perda de informação, podemos considerar o conjunto R como *sendo* a relação $<$ em $\mathbb{N}$.

Do mesmo modo podemos construir um subconjunto de $\mathbb{N}^2$ para qualquer relação entre números. Reciprocamente, dado qualquer conjunto de pares de

números $S \subseteq \mathbb{N}^2$, há uma relação correspondente entre números, nomeadamente, a relação segundo a qual n se liga a m se e só se $\langle n, m\rangle \in S$. Isto justifica a definição seguinte:

Definição 2.1 (Relação binária). Uma *relação binária* num conjunto A é um subconjunto de A^2. Se $R \subseteq A^2$ é uma relação binária em A e $x, y \in A$, por vezes escrevemos Rxy (ou xRy) para $\langle x, y\rangle \in R$.

Exemplo 2.2. O conjunto $\mathbb{N}^2$ dos pares de números naturais pode ser listado numa matriz bidimensional assim: sfr:rel:set: relations

$$\begin{array}{ccccc} \langle \mathbf{0},\mathbf{0}\rangle & \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle & \dots \\ \langle 1,0\rangle & \langle \mathbf{1},\mathbf{1}\rangle & \langle 1,2\rangle & \langle 1,3\rangle & \dots \\ \langle 2,0\rangle & \langle 2,1\rangle & \langle \mathbf{2},\mathbf{2}\rangle & \langle 2,3\rangle & \dots \\ \langle 3,0\rangle & \langle 3,1\rangle & \langle 3,2\rangle & \langle \mathbf{3},\mathbf{3}\rangle & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Colocamos a diagonal, aqui, em negrito, pois o subconjunto de $\mathbb{N}^2$ constituído pelos pares que estão na diagonal, isto é,

$$\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \dots\},$$

é a *relação identidade em* $\mathbb{N}$. (Como a relação identidade é popular, definamos $\mathrm{Id}_A = \{\langle x, x\rangle : x \in A\}$ para qualquer conjunto A.) O subconjunto de todos os pares acima da diagonal, isto é,

$$L = \{\langle 0,1\rangle, \langle 0,2\rangle, \dots, \langle 1,2\rangle, \langle 1,3\rangle, \dots, \langle 2,3\rangle, \langle 2,4\rangle, \dots\},$$

é a relação *menor que*, isto é, Lnm se e só se $n < m$. O subconjunto dos pares abaixo da diagonal, isto é,

$$G = \{\langle 1,0\rangle, \langle 2,0\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \dots\},$$

é a relação *maior que*, isto é, Gnm se e só se $n > m$. A união de L com I, que podemos chamar $K = L \cup I$, é a relação *menor ou igual a*: Knm se e só se $n \leq m$. Do mesmo modo, $H = G \cup I$ é a *relação maior ou igual a*. Estas relações L, G, K, e H são tipos especiais de relações chamadas *ordens*. L e G gozam da propriedade de que nenhum número está em relação L ou G consigo próprio (isto é, para todo n, não se verifica nem Lnn nem Gnn). Relações com esta propriedade chamam-se *irreflexivas*, e, se também forem ordens, chamam-se *ordens estritas*.

explanation Embora ordens e identidade sejam relações importantes e naturais, convém enfatizar que, segundo a nossa definição, *qualquer* subconjunto de A^2 é uma relação em A, por mais artificial ou forçado que pareça. Em particular, $\emptyset$ é uma relação em qualquer conjunto (a *relação vazia*, que nenhum par de elementos satisfaz), e A^2 em si é também uma relação em A (uma que todo par de elementos satisfaz), chamada a *relação universal*. Mas também algo como $E = \{\langle n, m\rangle : n > 5 \text{ ou } m \times n \geq 34\}$ conta como relação.

Problema 2.1. Liste os membros da relação $\subseteq$ no conjunto $\wp(\{a, b, c\})$.

2.2 Reflexões Filosóficas

sfr:rel:ref:sec

Na Seção 2.1, definimos relações como certos conjuntos. Devemos fazer uma pausa e colocar uma questão filosófica rápida: o que é que tal definição *faz*? É extremamente duvidoso que devamos querer dizer que *descobrimos* fatos metafísicos de identidade; que, por exemplo, a relação de ordem em $\mathbb{N}$ *acabou por ser* o conjunto $R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}$ que definimos na Seção 2.1. Eis três razões para isso.

Primeiro: na Definição 1.23, definimos $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$. Consideremos em vez disso a definição $\|a, b\| = \{\{b\}, \{a, b\}\} = \langle b, a\rangle$. Quando $a \neq b$, temos que $\langle a, b\rangle \neq \|a, b\|$. Mas poderíamos com a mesma facilidade ter tomado $\|a, b\|$ como a nossa definição de par ordenado, em vez de $\langle a, b\rangle$. Ambas as definições teriam funcionado igualmente bem. Assim, temos dois candidatos igualmente bons a "ser" a relação de ordem nos números naturais, nomeadamente:

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}$$
$$S = \{\|n, m\| : n, m \in \mathbb{N} \text{ e } n < m\}.$$

Como $R \neq S$, pela extensionalidade, é claro que não podem *ambos* ser idênticos à relação de ordem em $\mathbb{N}$. Mas seria meramente arbitrário, e por isso um pouco embaraçoso, afirmar que R em vez de S (ou vice-versa) *é* a relação de ordenação, como questão de fato. (Isto é um caso muito simples de um argumento contra o reducionismo em teoria dos conjuntos que Benacerraf tornou famoso em 1965. Voltaremos a ele várias vezes.)

Segundo: se pensamos que *toda* a relação deve ser identificada com um conjunto, então a própria relação de pertinência a conjuntos, $\in$, deveria ser um conjunto particular. De fato, teria de ser o conjunto $\{\langle x, y\rangle : x \in y\}$. Mas será que este conjunto existe? Dado o Paradoxo de Russell, é uma afirmação não trivial que tal conjunto exista. De fato, é possível desenvolver a teoria dos conjuntos de modo rigoroso como teoria axiomática, e essa teoria de fato nega a existência deste conjunto. Logo, mesmo que algumas relações possam ser tratadas como conjuntos, a relação de pertinência a conjuntos terá de ser um caso especial.

Terceiro: quando "identificamos" relações com conjuntos, dissemos que nos permitiríamos escrever Rxy para $\langle x, y\rangle \in R$. Isto está bem, desde que a relação de pertinência, "$\in$", seja tratada *como* um predicado. Mas se pensamos que "$\in$" denota um certo tipo de conjunto, então a expressão "$\langle x, y\rangle \in R$" consiste apenas em três termos singulares que denotam conjuntos: "$\langle x, y\rangle$", "$\in$", e "R". E tal lista de nomes não é mais capaz de exprimir uma proposição do que a sequência sem sentido: "o copo porta-canetas a mesa". De novo, mesmo que algumas relações possam ser tratadas como conjuntos, a relação de pertinência a conjuntos tem de ser um caso especial. (Isto reúne num só argumento uma versão simples do paradoxo do conceito *cavalo* de Frege, e uma objeção célebre que Wittgenstein dirigiu a Russell.)

Então onde nos deixa isto? Bem, não há nada de *errado* em dizermos que as relações nos números são conjuntos. Só temos de compreender o espírito em

que tal observação é feita. Não enunciamos um fato metafísico de identidade. Limitamo-nos a notar que, em certos contextos, podemos (e iremos) *tratar* (certas) relações como certos conjuntos.

2.3 Propriedades Especiais das Relações

intro

sfr:rel:prp:sec

Alguns tipos de relações revelam-se tão comuns que receberam nomes especiais. Por exemplo, $\leq$ e $\subseteq$ relacionam os seus respectivos domínios (digamos, $\mathbb{N}$ no caso de $\leq$ e $\wp(A)$ no caso de $\subseteq$) de modos semelhantes. Para precisar exatamente como estas relações são semelhantes, e como diferem, as categorizamos segundo algumas propriedades especiais que as relações podem ter. Verifica-se que (combinações de) algumas destas propriedades especiais são especialmente importantes: ordens e relações de equivalência.

Definição 2.3 (Reflexividade). Uma relação $R \subseteq A^2$ é *reflexiva* se e só se, para todo $x \in A$, Rxx.

Definição 2.4 (Transitividade). Uma relação $R \subseteq A^2$ é *transitiva* se e só se, sempre que Rxy e Ryz, então também Rxz.

Definição 2.5 (Simetria). Uma relação $R \subseteq A^2$ é *simétrica* se e só se, sempre que Rxy, então também Ryx.

Definição 2.6 (Antissimetria). Uma relação $R \subseteq A^2$ é *antissimétrica* se e só se, sempre que tanto Rxy quanto Ryx, então $x = y$ (ou, noutras palavras: se $x \neq y$ então ou $\neg Rxy$ ou $\neg Ryx$).

explanation

Numa relação simétrica, Rxy e Ryx verificam-se sempre em conjunto, ou nenhuma se verifica. Numa relação antissimétrica, a única forma de Rxy e Ryx se verificarem em conjunto é que $x = y$. Note-se que isto não *exige* que Rxy e Ryx se verifiquem quando $x = y$, apenas que isso não está excluído. Assim, uma relação antissimétrica pode ser reflexiva, mas não é o caso que toda relação antissimétrica seja reflexiva. Note-se também que ser antissimétrica e ser meramente não simétrica são condições diferentes. De fato, uma relação pode ser ao mesmo tempo simétrica e antissimétrica (por exemplo, a relação identidade o é).

Definição 2.7 (Conexidade). Uma relação $R \subseteq A^2$ é *conexa* se para todos $x, y \in A$, se $x \neq y$, então ou Rxy ou Ryx.

Problema 2.2. Dê exemplos de relações que sejam (a) reflexivas e simétricas mas não transitivas, (b) reflexivas e antissimétricas, (c) antissimétricas, transitivas, mas não reflexivas, e (d) reflexivas, simétricas e transitivas. Não use relações sobre números ou conjuntos.

Definição 2.8 (Irreflexividade). Uma relação $R \subseteq A^2$ diz-se *irreflexiva* se, para todo $x \in A$, não Rxx.

Definição 2.9 (Assimetria). Uma relação $R \subseteq A^2$ diz-se *assimétrica* se para nenhum par $x, y \in A$ se tem tanto Rxy quanto Ryx.

Note-se que se $A \neq \emptyset$, então nenhuma relação irreflexiva em A é reflexiva e toda relação assimétrica em A é também antissimétrica. Contudo, há $R \subseteq A^2$ que não são reflexivas nem irreflexivas, e há relações antissimétricas que não são assimétricas.

2.4 Relações de Equivalência

sfr:rel:eqv:sec

A relação identidade num conjunto é reflexiva, simétrica e transitiva. Relações R que têm todas as três destas propriedades são muito comuns.

Definição 2.10 (Relação de equivalência). Uma relação $R \subseteq A^2$ que é reflexiva, simétrica e transitiva chama-se uma *relação de equivalência*. Membros x e y de A dizem-se *R-equivalentes* se Rxy.

As relações de equivalência dão origem à noção de *classe de equivalência*. Uma relação de equivalência "reparte" o domínio em partições distintas. Dentro de cada partição, todos os objetos estão relacionados uns com os outros; e objetos de partições diferentes não se relacionam entre si. Por vezes, é útil falar destas partições *diretamente*. Para esse fim, introduzimos uma definição:

sfr:rel:eqv:def:equivalenceclass

Definição 2.11. Seja $R \subseteq A^2$ uma relação de equivalência. Para cada $x \in A$, a *classe de equivalência* de x em A é o conjunto $[x]_R = \{y \in A : Rxy\}$. O *quociente* de A por R é $A/_R = \{[x]_R : x \in A\}$, isto é, o conjunto destas classes de equivalência.

O resultado seguinte justifica a definição de classe de equivalência, provando que as classes de equivalência são de fato as partições de A:

Proposição 2.12. *Se $R \subseteq A^2$ é uma relação de equivalência, então Rxy se e só se $[x]_R = [y]_R$.*

Prova. Para o sentido da esquerda para a direita, suponhamos Rxy, e seja $z \in [x]_R$. Por definição, então, Rxz. Como R é uma relação de equivalência, Ryz. (Explicando melhor: como Rxy e R é simétrica temos Ryx, e como Rxz e R é transitiva temos Ryz.) Logo $z \in [y]_R$. Generalizando, $[x]_R \subseteq [y]_R$. Mas de modo perfeitamente análogo, $[y]_R \subseteq [x]_R$. Logo $[x]_R = [y]_R$, pela extensionalidade.

Para o sentido da direita para a esquerda, suponhamos $[x]_R = [y]_R$. Como R é reflexiva, Ryy, logo $y \in [y]_R$. Assim também $y \in [x]_R$ pela suposição de que $[x]_R = [y]_R$. Logo Rxy. □

Exemplo 2.13. Um bom exemplo de relações de equivalência vem da aritmética modular. Para quaisquer a, b, e $n \in \mathbb{Z}^+$, digamos que $a \equiv_n b$ se e só se dividir a por n dá o mesmo resto que dividir b por n. (De modo um pouco mais

simbólico: $a \equiv_n b$ se e só se, para algum $k \in \mathbb{Z}$, $a - b = kn$.) Agora, $\equiv_n$ é uma relação de equivalência, para qualquer n. E há exatamente n classes de equivalência distintas geradas por $\equiv_n$; isto é, $\mathbb{N}/_{\equiv_n}$ tem n membros. São: o conjunto dos números divisíveis por n sem resto, isto é, $[0]_{\equiv_n}$; o conjunto dos números divisíveis por n com resto 1, isto é, $[1]_{\equiv_n}$; ...; e o conjunto dos números divisíveis por n com resto $n-1$, isto é, $[n-1]_{\equiv_n}$.

Problema 2.3. Mostre que $\equiv_n$ é uma relação de equivalência, para qualquer $n \in \mathbb{Z}^+$, e que $\mathbb{N}/_{\equiv_n}$ tem exatamente n membros.

2.5 Ordens

explanation

Muitas das nossas comparações envolvem descrever certos objetos como sendo "menores que", "iguais a" ou "maiores que" outros objetos, sob algum aspecto. Isso envolve relações de *ordem*. Mas há vários tipos de relação de ordem. Por exemplo, algumas exigem que quaisquer dois objetos sejam comparáveis, outras não. Algumas incluem a identidade (como $\leq$) e outras a excluem (como $<$). Ter aqui uma taxonomia ajuda-nos.

sfr:rel:ord:sec

Definição 2.14 (Pré-ordem). Uma relação que é ao mesmo tempo reflexiva e transitiva chama-se uma *pré-ordem*.

Definição 2.15 (Ordem parcial). Uma pré-ordem que também é antissimétrica chama-se uma *ordem parcial*.

Definição 2.16 (Ordem linear). Uma ordem parcial que também é conexa chama-se uma *ordem total* ou *ordem linear*.

sfr:rel:ord:def:linearorder

Exemplo 2.17. Toda ordem linear é também uma ordem parcial, e toda ordem parcial é também uma pré-ordem, mas as implicações recíprocas não valem. A relação universal sobre A é uma pré-ordem, pois é reflexiva e transitiva. Mas, se A tem mais de um membro, a relação universal não é antissimétrica e, portanto, não é uma ordem parcial.

Exemplo 2.18. Considere a relação *não mais longa que* $\preccurlyeq$ sobre $\mathbb{B}^*$: $x \preccurlyeq y$ sse $\text{len}(x) \leq \text{len}(y)$. Trata-se de uma pré-ordem (reflexiva e transitiva), e até conexa, mas não é uma ordem parcial, pois não é antissimétrica. Por exemplo, $01 \preccurlyeq 10$ e $10 \preccurlyeq 01$, mas $01 \neq 10$.

Exemplo 2.19. Uma ordem parcial importante é a relação $\subseteq$ sobre um conjunto de conjuntos. Em geral não é uma ordem linear: se $a \neq b$ e consideramos $\wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, vemos que $\{a\} \not\subseteq \{b\}$ e $\{a\} \neq \{b\}$ e $\{b\} \not\subseteq \{a\}$.

Exemplo 2.20. A relação de *divisibilidade sem resto* nos dá uma ordem parcial que não é linear. Para inteiros n e m, escrevemos $n \mid m$ para significar que n divide m (exatamente), isto é, sse existe algum inteiro k tal que $m = kn$. Sobre $\mathbb{N}$, isso é uma ordem parcial, mas não linear: por exemplo, $2 \nmid 3$ e também

$3 \nmid 2$. Vista como relação sobre $\mathbb{Z}$, a divisibilidade é apenas uma pré-ordem, pois não é antissimétrica: $1 \mid -1$ e $-1 \mid 1$ mas $1 \neq -1$.

Exemplo 2.21. A relação de *extensão* sobre um conjunto de sequências A^* é a seguinte: $s \sqsubseteq s'$ sse $s = \Lambda$ (a sequência vazia), $s = s'$, ou $s = \langle s_1, \ldots, s_n \rangle$ e $s' = \langle s_1, \ldots, s_n, s_{n+1}, \ldots, s_m \rangle$. Se $s \sqsubseteq s'$ dizemos também que s é um *segmento inicial* de s'. A relação de extensão sobre A^* é uma ordem parcial, mas não linear, p.ex., se $a \neq b$, então $ab \not\sqsubseteq ba$ e $ba \not\sqsubseteq ab$.

Definição 2.22 (Ordem estrita). Uma *ordem estrita* é uma relação irreflexiva, assimétrica e transitiva.

sfr:rel:ord: def:strictlinearorder **Definição 2.23 (Ordem linear estrita).** Uma ordem estrita que também é conexa chama-se *ordem total estrita* ou *ordem linear estrita.*

Exemplo 2.24. $\leq$ é a ordem linear correspondente à ordem linear estrita $<$. $\subseteq$ é a ordem parcial correspondente à ordem estrita $\subsetneq$.

Qualquer ordem estrita R sobre A pode transformar-se numa ordem parcial adicionando a diagonal Id_A, isto é, adicionando todos os pares $\langle x, x \rangle$. (Isto chama-se o *fecho reflexivo* de R.) Reciprocamente, a partir de uma ordem parcial obtém-se uma ordem estrita removendo Id_A. Os dois resultados seguintes tornam isto preciso.

sfr:rel:ord: prop:stricttopartial **Proposição 2.25.** *Se R é uma ordem estrita sobre A, então $R^+ = R \cup \mathrm{Id}_A$ é uma ordem parcial. Além disso, se R é uma ordem linear estrita, então R^+ é uma ordem linear.*

Prova. Suponhamos que R é uma ordem estrita, isto é, $R \subseteq A^2$ e R é irreflexiva, assimétrica e transitiva. Seja $R^+ = R \cup \mathrm{Id}_A$. Temos de mostrar que R^+ é reflexiva, antissimétrica e transitiva.

R^+ é claramente reflexiva, pois $\langle x, x \rangle \in \mathrm{Id}_A \subseteq R^+$ para todo $x \in A$.

Para mostrar que R^+ é antissimétrica, suponhamos, para redução ao absurdo, que R^+xy e R^+yx mas $x \neq y$. Como $\langle x, y \rangle \in R \cup \mathrm{Id}_A$, mas $\langle x, y \rangle \notin \mathrm{Id}_A$, temos de ter $\langle x, y \rangle \in R$, isto é, Rxy. Do mesmo modo, Ryx. Mas isto contradiz a hipótese de que R é assimétrica.

Para estabelecer a transitividade, suponhamos que R^+xy e R^+yz. Se tanto $\langle x, y \rangle \in R$ como $\langle y, z \rangle \in R$, então $\langle x, z \rangle \in R$, pois R é transitiva. Caso contrário, ou $\langle x, y \rangle \in \mathrm{Id}_A$, isto é, $x = y$, ou $\langle y, z \rangle \in \mathrm{Id}_A$, isto é, $y = z$. No primeiro caso, temos R^+yz por hipótese, $x = y$, logo R^+xz. Analogamente no segundo caso. Em qualquer caso, R^+xz; assim, R^+ é também transitiva.

Quanto à cláusula "além disso", suponhamos que R é também conexa. Então, para todo $x \neq y$, ou Rxy ou Ryx, isto é, ou $\langle x, y \rangle \in R$ ou $\langle y, x \rangle \in R$. Como $R \subseteq R^+$, isto continua a valer para R^+, logo R^+ é também conexa. □

sfr:rel:ord: prop:partialtostrict **Proposição 2.26.** *Se R é uma ordem parcial sobre A, então $R^- = R \setminus \mathrm{Id}_A$ é uma ordem estrita. Além disso, se R é uma ordem linear, então R^- é uma ordem linear estrita.*

Prova. Deixamos como exercício. □

Problema 2.4. Apresente uma prova da Proposição 2.26.

O resultado simples a seguir estabelece que ordens lineares estritas satisfazem uma propriedade no estilo da extensionalidade:

Proposição 2.27. *Se $<$ é uma ordem linear estrita sobre A, então:* sfr:rel:ord:prop:extensionality-strictlinearorra

$$(\forall a, b \in A)((\forall x \in A)(x < a \leftrightarrow x < b) \to a = b).$$

Prova. Suponhamos $(\forall x \in A)(x < a \leftrightarrow x < b)$. Se $a < b$, então $a < a$, o que contradiz o fato de $<$ ser irreflexiva; logo $a \not< b$. De forma totalmente análoga, $b \not< a$. Logo $a = b$, pois $<$ é conexa. □

2.6 Grafos

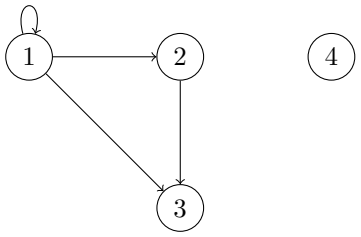
Um *grafo* é um diagrama no qual pontos—chamados "nós" ou "vértices" (plural de "vértice")—são conectados por arestas. Grafos são uma ferramenta onipresente em matemática discreta e em ciência da computação. São incrivelmente úteis para representar e visualizar relações e estruturas, desde coisas concretas como redes de vários tipos até estruturas abstratas como os possíveis resultados de decisões. Existem muitos tipos diferentes de grafos na literatura que diferem, p.ex., quanto a se as arestas são direcionadas ou não, têm rótulos ou não, se pode haver arestas de um nó para o mesmo nó, múltiplas arestas entre os mesmos nós, etc. *Grafos direcionados* têm uma conexão especial com relações. sfr:rel:grp:sec

Definição 2.28 (Grafo direcionado). Um *grafo direcionado* $G = \langle V, E\rangle$ é um conjunto de *vértices* V e um conjunto de *arestas* $E \subseteq V^2$.

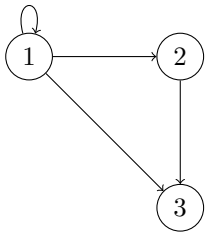
explanation

De acordo com nossa definição, um grafo é simplesmente um conjunto junto com uma relação nesse conjunto. Claro, ao falar de grafos, é natural esperar que sejam representados graficamente: podemos desenhar um grafo conectando dois vértices v_1 e v_2 por uma seta sse $\langle v_1, v_2\rangle \in E$. A única diferença entre uma relação por si só e um grafo é que um grafo especifica o conjunto de vértices, isto é, um grafo pode ter vértices isolados. O ponto importante, porém, é que toda relação R em um conjunto X pode ser vista como um grafo direcionado $\langle X, R\rangle$, e reciprocamente, um grafo direcionado $\langle V, E\rangle$ pode ser visto como uma relação $E \subseteq V^2$ com o conjunto V explicitamente especificado.

Exemplo 2.29. O grafo $\langle V, E\rangle$ com $V = \{1, 2, 3, 4\}$ e $E = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$ se parece com isto:



Este é um grafo diferente de $\langle V', E\rangle$ com $V' = \{1, 2, 3\}$, que se parece com isto:



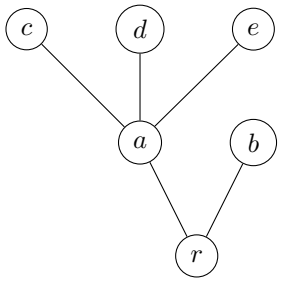
Problema 2.5. Considere a relação menor ou igual a $\leq$ no conjunto $\{1, 2, 3, 4\}$ como um grafo e desenhe o diagrama correspondente.

2.7 Árvores

sfr:rel:tre:sec

Um tipo particular de ordem parcial que desempenha um papel importante em todas as partes da lógica é uma *árvore*. Árvores finitas aparecem em partes elementares da lógica: por exemplo, fórmulas podem ser entendidas em termos de sua decomposição em uma árvore sintática, enquanto derivações em muitos sistemas de derivação também tomam a forma de árvores finitas. Árvores infinitas aparecem já na prova dos teoremas de completude para a lógica proposicional e de primeira ordem, e são usadas em toda a lógica matemática.

O conceito de árvore da teoria dos conjuntos está intimamente relacionado à noção de árvore na teoria dos grafos. Aqui está uma figura de uma árvore (finita):



O nó mais baixo r é a raiz. Todo nó diferente de r tem exatamente um nó pai imediatamente abaixo dele. Podemos pensar na relação em que um nó x está para um nó y se y pode ser alcançado a partir de x seguindo arestas para cima como x sendo um *ancestral* de y.

A relação de ancestralidade em uma árvore é uma ordem parcial estrita. Isso motiva a definição teórico-conjuntista. Para enunciá-la, precisamos de dois conceitos. Um *menor elemento* em um conjunto A parcialmente ordenado por $\leq$ é um membro $x \in A$ tal que para todo $y \in A$ temos que $x \leq y$. Um conjunto é *bem ordenado* por $\leq$ se cada um de seus subconjuntos não vazios tem um menor elemento.

Definição 2.30 (Árvore). Uma *árvore* é um par $T = \langle A, \leq \rangle$ tal que A é um conjunto e $\leq$ é uma ordem parcial em A com um único menor elemento $r \in A$ (chamado de *raiz*) tal que para todo $x \in A$, o conjunto $\{y : y \leq x\}$ é bem ordenado por $\leq$.

Definição 2.31 (Sucessores). Suponha $T = \langle A, \leq \rangle$ é uma árvore. Se $x, y \in A$, $x < y$, e não existe $z \in A$ tal que $x < z < y$, então dizemos que y é um *sucessor* de x.

Os sucessores de $x \in A$ também são chamados de seus *filhos*. Se y é um sucessor de x, então chamamos x de *predecessor* ou *pai* de y.

Proposição 2.32. *Se $\langle A, \leq \rangle$ é uma árvore, então todo $x \in A$ diferente da raiz tem no máximo um predecessor.*

Prova. Suponha $y_1 < x$ e $y_2 < x$ e $y_1 \neq y_2$. Então $\{y_1, y_2\} \subseteq \{z : z < x\}$. Como $\{z : z < x\}$ é bem ordenado por $\leq$, seu subconjunto $\{y_1, y_2\}$ tem um menor elemento, que obviamente deve ser ou y_1 ou y_2. Então ou $y_1 \leq y_2$ ou $y_2 \leq y_1$. Supusemos que $y_1 \neq y_2$, então na verdade ou $y_1 < y_2$ ou $y_2 < y_1$. Como supusemos que $y_1 < x$ e $y_2 < x$, temos ainda que ou $y_1 < y_2 < x$ ou $y_2 < y_1 < x$. Então y_1 e y_2 não podem ambos ser predecessores de x. □

Definição 2.33. Uma árvore $T = \langle A, \leq \rangle$ é dita *infinita* se A é um conjunto infinito, e *finita* caso contrário. Se T é tal que todo $x \in A$ tem apenas um número finito de sucessores, então dizemos que T é *finitamente ramificada*.

Definição 2.34 (Ramos). Dada uma árvore $T = \langle A, \leq \rangle$, um *ramo* de T é uma cadeia maximal em T, isto é, um conjunto $B \subseteq A$ tal que para quaisquer $x, y \in B$ ou $x \leq y$ ou $y \leq x$, e para qualquer $z \in X \setminus B$ existe $u \in B$ tal que nem $z \leq u$ nem $u \leq z$. Usamos $[T]$ para denotar o conjunto de todos os ramos de T.

Exemplo 2.35. Um exemplo clássico de árvore finitamente ramificada é a *árvore binária infinita* de sequências finitas de 0s e 1s, às vezes denotada $\{0,1\}^*$ ou $\mathbb{B}^*$, ordenada pela relação de extensão $\sqsubseteq$ (p.ex., $101 \sqsubseteq 101101$). Como qualquer cadeia binária pode sempre ser estendida adicionando um 0 ou um 1 no final, esta árvore contém infinitos elementos: todo elemento s tem exatamente dois sucessores, $s0$ e $s1$. Sua raiz é a sequência vazia Λ.

Exemplo 2.36. De maneira um pouco mais geral, o conjunto de sequências finitas de números naturais $\mathbb{N}^*$ com a relação de extensão $\sqsubseteq$ também é uma árvore. É obviamente não finitamente ramificada: todo $s \in \mathbb{N}^*$ tem infinitos sucessores sn, um para cada $n \in \mathbb{N}$. Todo $A \subseteq \mathbb{N}^*$ que é fechado sob $\sqsubseteq$ é uma *subárvore* de $\mathbb{N}^*$. (Isto é, A é tal que se $s \in A$ e $s' \sqsubseteq s$, então também $s' \in A$.) Todas as árvores finitas podem ser representadas como subárvores finitas de $\mathbb{N}^*$.

Proposição 2.37 (Lema de Kőnig). *Se $T = \langle A, \leq \rangle$ é uma árvore infinita finitamente ramificada, então T tem um ramo infinito.*

Um caso especial do Lema de Kőnig amplamente usado em teoria da computabilidade, conhecido como *Lema Fraco de Kőnig*, é o seguinte: qualquer subárvore infinita de $\{0,1\}^*$ tem um ramo infinito.

2.8 Operações sobre Relações

sfr:rel:ops: sec

É frequentemente útil modificar ou combinar relações. Na Proposição 2.25, consideramos a *união* de relações, que é apenas a união de duas relações vistas como conjuntos de pares. Do mesmo modo, na Proposição 2.26, consideramos a diferença relativa de relações. Eis algumas outras operações que podemos efetuar sobre relações.

sfr:rel:ops: relationoperations

Definição 2.38. Sejam R e S relações, e A um conjunto qualquer.
A *inversa* de R é $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$.
O *produto relativo* de R e S é $(R \mid S) = \{\langle x, z\rangle : \exists y(Rxy \wedge Syz)\}$.
A *restrição* de R a A é $R{\restriction_A} = R \cap A^2$.
A *aplicação* de R a A é $R[A] = \{y : (\exists x \in A)Rxy\}$

Exemplo 2.39. Seja $S \subseteq \mathbb{Z}^2$ a relação sucessora sobre $\mathbb{Z}$, isto é, $S = \{\langle x, y\rangle \in \mathbb{Z}^2 : x + 1 = y\}$, de modo que Sxy sse $x + 1 = y$.
S^{-1} é a relação antecessora sobre $\mathbb{Z}$, isto é, $\{\langle x, y\rangle \in \mathbb{Z}^2 : x - 1 = y\}$.
$S \mid S$ é $\{\langle x, y\rangle \in \mathbb{Z}^2 : x + 2 = y\}$
$S{\restriction_{\mathbb{N}}}$ é a relação sucessora sobre $\mathbb{N}$.
$S[\{1, 2, 3\}]$ é $\{2, 3, 4\}$.

Definição 2.40 (Fecho transitivo). Seja $R \subseteq A^2$ uma relação binária.
O *fecho transitivo* de R é $R^+ = \bigcup_{0<n\in\mathbb{N}} R^n$, onde definimos recursivamente $R^1 = R$ e $R^{n+1} = R^n \mid R$.
O *fecho reflexivo transitivo* de R é $R^* = R^+ \cup \mathrm{Id}_A$.

Exemplo 2.41. Tome a relação sucessora $S \subseteq \mathbb{Z}^2$. S^2xy sse $x + 2 = y$, S^3xy sse $x + 3 = y$, etc. Logo S^+xy sse $x + n = y$ para algum $n \geq 1$. Em outras palavras, S^+xy sse $x < y$, e S^*xy sse $x \leq y$.

Problema 2.6. Mostre que o fecho transitivo de R é de fato transitivo.

Capítulo 3

Funções

3.1 Noções Básicas

explanation

Uma *função* é um mapa que envia cada membro de um dado conjunto para um membro específico em algum (outro) conjunto dado. Por exemplo, a operação de somar 1 define uma função: cada número n é mapeado para um único número $n+1$. sfr:fun:bas:sec

Mais em geral, funções podem tomar pares, triplos, etc., como entradas e devolver algum tipo de saída. Muitas funções nos são familiares da aritmética básica. Por exemplo, a adição e a multiplicação são funções. Tomam dois números e devolvem um terceiro.

Neste sentido matemático e abstrato, uma função é uma *caixa preta*: só importa que saída fica associada a que entrada, não o método de calcular a saída.

Definição 3.1 (Função). Uma *função* $f\colon A \to B$ é um mapeamento de cada membro de A para um membro de B.

Chamamos A de *domínio* de f e B de *contradomínio* de f. Os membros de A chamam-se entradas ou *argumentos* de f, e o membro de B que fica associado a um argumento x por f chama-se o *valor de* f para o argumento x, escrevendo-se $f(x)$.

A *imagem* $\mathrm{Im}(f)$ de f é o subconjunto do contradomínio constituído pelos valores de f para algum argumento; $\mathrm{Im}(f) = \{f(x) : x \in A\}$.

O diagrama na Figura 3.1 pode ajudar a pensar em funções. A elipse à esquerda representa o *domínio* da função; a elipse à direita representa o *contradomínio*; e uma seta aponta de um *argumento* no domínio para o *valor* correspondente no contradomínio.

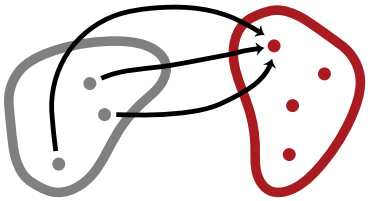


Figura 3.1: Uma função é um mapeamento de cada membro de um conjunto para um membro de outro. Uma seta vai de um argumento no domínio para o valor correspondente no contradomínio.

sfr:fun:bas: fig:function

Exemplo 3.2. A multiplicação toma pares de números naturais como entradas e mapeia-os para números naturais como saídas, logo vai de $\mathbb{N} \times \mathbb{N}$ (o domínio) para $\mathbb{N}$ (o contradomínio). Como se vê, a imagem é também $\mathbb{N}$, pois todo $n \in \mathbb{N}$ é $n \times 1$.

Exemplo 3.3. A multiplicação é uma função porque associa cada entrada—cada par de números naturais—a uma única saída: $\times : \mathbb{N}^2 \to \mathbb{N}$. Em contraste, mapear um número natural n para um real x tal que $x^2 = n$ não é funcional, pois cada inteiro positivo n tem duas raízes quadradas: $\sqrt{n}$ e $-\sqrt{n}$. Podemos torná-la funcional devolvendo só a raiz quadrada positiva: $\sqrt{\ } : \mathbb{N} \to \mathbb{R}$.

Exemplo 3.4. A relação que associa cada aluno de uma turma à sua nota final é uma função—nenhum aluno pode ter duas notas finais diferentes na mesma turma. A relação que associa cada aluno de uma turma aos seus progenitores não é uma função: os alunos podem ter zero, ou dois, ou mais progenitores.

Podemos definir funções especificando de modo preciso qual é o valor da função para cada argumento possível. Formas de o fazer são dar uma fórmula, descrever um método para calcular o valor, ou listar os valores para cada argumento. Como quer que as funções sejam definidas, temos de garantir que, para cada argumento, especificamos um, e apenas um, valor. explanation

Exemplo 3.5. Seja $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = x + 1$. Esta é uma definição que especifica f como uma função que toma números naturais e devolve números naturais. Diz-nos que, dado um número natural x, f devolverá o seu sucessor $x + 1$. Neste caso, o contradomínio $\mathbb{N}$ não é a imagem de f, pois o número natural 0 não é sucessor de nenhum número natural. A imagem de f é o conjunto de todos os inteiros positivos, $\mathbb{Z}^+$.

sfr:fun:bas: examplefunext

Exemplo 3.6. Seja $g : \mathbb{N} \to \mathbb{N}$ definida por $g(x) = x + 2 - 1$. Isto nos diz que g é uma função que toma números naturais e devolve números naturais. Dado um número natural n, g devolverá o predecessor do sucessor do sucessor de n, isto é, $n + 1$.

Acabamos de considerar duas funções, f e g, com *definições* diferentes. Contudo, são a *mesma função*. Afinal, para qualquer número natural n, temos explanation

$f(n) = n + 1 = n + 2 - 1 = g(n)$. Em outras palavras: as nossas definições de f e g especificam o mesmo mapeamento por meio de equações diferentes. Implicitamente, pois, estamos nos apoiando num princípio de extensionalidade para funções,

$$\text{se } \forall x\, f(x) = g(x), \text{ então } f = g$$

desde que f e g compartilhem o mesmo domínio e contradomínio.

Exemplo 3.7. Também podemos definir funções por casos. Por exemplo, poderíamos definir $h\colon \mathbb{N} \to \mathbb{N}$ por

$$h(x) = \begin{cases} \frac{x}{2} & \text{se } x \text{ é par} \\ \frac{x+1}{2} & \text{se } x \text{ é ímpar.} \end{cases}$$

Como todo número natural é par ou ímpar, a saída desta função será sempre um número natural. Basta lembrar que, se se define uma função por casos, cada entrada possível tem de cair em exatamente um caso. Em alguns casos, isto exigirá uma prova de que os casos são exaustivos e exclusivos.

3.2 Tipos de Funções

explanation Será útil introduzir uma espécie de taxonomia para alguns dos tipos de funções que encontramos com mais frequência. sfr:fun:kin:sec

Para começar, podemos querer considerar funções com a propriedade de que todo *membro* do contradomínio é um valor da função. Tais funções chamam-se sobrejetivas, e podem ser esquematizadas como na Figura 3.2.

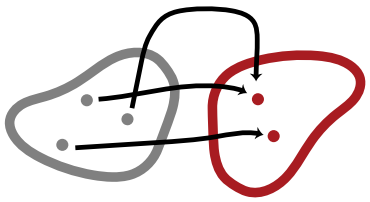


Figura 3.2: Uma função sobrejetiva tem todo membro do contradomínio como valor.

sfr:fun:kin:fig:surjective

Definição 3.8 (Função Sobrejetiva). Uma função $f\colon A \to B$ é *sobrejetiva* se e só se B é também a imagem de f, isto é, para todo $y \in B$ existe pelo menos um $x \in A$ tal que $f(x) = y$, ou em símbolos:

$$(\forall y \in B)(\exists x \in A) f(x) = y.$$

Chamamos a tal função uma sobrejeção de A para B.

explanation Se quiser mostrar que f é uma sobrejeção, tem de mostrar que todo objeto no contradomínio de f é o valor de $f(x)$ para alguma entrada x.

Note-se que qualquer função *induz* uma sobrejeção. Afinal, dada uma função $f\colon A \to B$, seja $f'\colon A \to \mathrm{Im}(f)$ definida por $f'(x) = f(x)$. Como $\mathrm{Im}(f)$ é *definida* como $\{f(x) \in B : x \in A\}$, esta função f' é garantidamente uma sobrejeção

Agora, qualquer função mapeia cada entrada possível para uma única saída. explanation
Mas há também funções que nunca mapeiam entradas diferentes para a mesma saída. Tais funções chamam-se injetivas, e podem ser esquematizadas como na Figura 3.3.

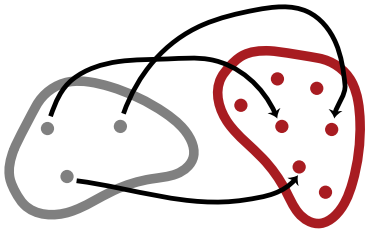


Figura 3.3: Uma função injetiva nunca mapeia dois argumentos diferentes para o mesmo valor.

sfr:fun:kin:
fig:injective

Definição 3.9 (Função Injetiva). Uma função $f\colon A \to B$ é *injetiva* se e só se, para cada $y \in B$, há no máximo um $x \in A$ tal que $f(x) = y$. Chamamos a tal função uma injeção de A para B.

Se quiser mostrar que f é uma injeção, tem de mostrar que, para quaisquer explanation
membros x e y do domínio de f, se $f(x) = f(y)$, então $x = y$.

Exemplo 3.10. A função constante $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = 1$ não é nem injetiva, nem sobrejetiva.

A função identidade $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = x$ é tanto injetiva quanto sobrejetiva.

A função sucessora $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = x + 1$ é injetiva mas não sobrejetiva.

A função $f\colon \mathbb{N} \to \mathbb{N}$ definida por:

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

é sobrejetiva, mas não injetiva.

Muitas vezes, queremos considerar funções que são tanto injetivas como explanation
sobrejetivas. Chamamos a tais funções bijetivas. Parecem-se com a função esquematizada na Figura 3.4. Bijeções são também por vezes chamadas *correspondências biunívocas*, pois associam de modo único elementos do contradomínio a elementos do domínio.

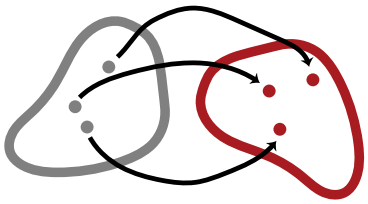


Figura 3.4: Uma função bijetiva associa de modo único os elementos do contradomínio aos do domínio.

sfr:fun:kin:
fig:bijective

Definição 3.11 (Bijeção). Uma função $f\colon A \to B$ é *bijetiva* se e só se é tanto sobrejetiva como injetiva. Chamamos a tal função uma bijeção de A para B (ou entre A e B).

3.3 Funções como Relações

explanation

sfr:fun:rel:
sec

Uma função que mapeia membros de A para membros de B define obviamente uma relação entre A e B, nomeadamente a relação que se verifica entre x e y se e só se $f(x) = y$. De fato, podemos até—se nos interessa reduzir os blocos de construção da matemática, por exemplo—*identificar* a função f com esta relação, isto é, com um conjunto de pares. Isto levanta então a questão: que relações definem funções deste modo?

Definição 3.12 (Gráfico de uma função). Seja $f\colon A \to B$ uma função. O *gráfico* de f é a relação $R_f \subseteq A \times B$ definida por

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

explanation

O gráfico de uma função fica unicamente determinado, pela extensionalidade. Além disso, a extensionalidade (sobre conjuntos) justifica de imediato o princípio implícito de extensionalidade para funções, segundo o qual, se f e g compartilham domínio e contradomínio, então são idênticas se coincidem em todos os valores.

Do mesmo modo, se uma relação é "funcional", então é o gráfico de uma função.

sfr:fun:rel:
prop:graph-function

Proposição 3.13. *Seja $R \subseteq A \times B$ tal que:*

1. *Se Rxy e Rxz, então $y = z$; e*
2. *para todo $x \in A$ existe algum $y \in B$ tal que $\langle x, y\rangle \in R$.*

Então R é o gráfico da função $f\colon A \to B$ definida por $f(x) = y$ se e só se Rxy.

Prova. Suponhamos que existe y tal que Rxy. Se existisse outro $z \neq y$ tal que Rxz, a condição sobre R seria violada. Logo, se existe y tal que Rxy, esse y é único, e assim f está bem definida. Obviamente, $R_f = R$. □

Toda função $f\colon A \to B$ tem um gráfico, isto é, uma relação em $A \times B$ definida por $f(x) = y$. Por outro lado, toda relação $R \subseteq A \times B$ com as propriedades dadas na Proposição 3.13 é o gráfico de uma função $f\colon A \to B$. Por causa desta ligação estreita entre funções e os seus gráficos, podemos pensar numa função simplesmente como o seu gráfico. Em outras palavras, funções podem identificar-se com certas relações, isto é, com certos conjuntos de tuplos. Note, contudo, que o espírito desta "identificação" é como na Seção 2.2: não é uma afirmação sobre a metafísica das funções, mas a observação de que é conveniente *tratar* funções como certos conjuntos. Uma razão pela qual isto é tão conveniente é que podemos agora considerar fazer operações semelhantes sobre funções às que fizemos sobre relações (ver Seção 2.8). Em particular: explanation

sfr:fun:rel: defn:funimage

Definição 3.14. Seja $f\colon A \to B$ uma função com $C \subseteq A$.

A *restrição* de f a C é a função $f{\restriction_C}\colon C \to B$ definida por $(f{\restriction_C})(x) = f(x)$ para todo $x \in C$. Em outras palavras, $f{\restriction_C} = \{\langle x, y\rangle \in R_f : x \in C\}$.

A *aplicação* de f a C é $f[C] = \{f(x) : x \in C\}$. Chamamos-lhe também a *imagem* de C por f.

Segue-se destas definições que $\mathrm{Im}(f) = f[\mathrm{dom}(f)]$, para qualquer função f. Estas noções são exatamente as que se esperaria, dadas as definições na Seção 2.8 e a nossa identificação de funções com relações. Mas outras duas operações—inversas e produtos relativos—exigem um pouco mais de detalhe. Trataremos disso na Seção 3.4 e na Seção 3.5. explanation

3.4 Inversas de Funções

sfr:fun:inv: sec

Pensamos nas funções como mapas. Uma pergunta natural sobre funções é, pois, se o mapeamento pode ser "invertido". Por exemplo, a função sucessora $f(x) = x + 1$ pode ser invertida, no sentido em que a função $g(y) = y - 1$ "desfaz" o que f faz. explanation

Mas é preciso ter cuidado. Embora a definição de g defina uma função $\mathbb{Z} \to \mathbb{Z}$, não define uma *função* $\mathbb{N} \to \mathbb{N}$, pois $g(0) \notin \mathbb{N}$. Assim, mesmo em casos simples, não é óbvio que uma função possa ser invertida; pode depender do domínio e do contradomínio.

Isto torna-se mais preciso com a noção de inversa de uma função.

Definição 3.15. Uma função $g\colon B \to A$ é uma *inversa* de uma função $f\colon A \to B$ se $f(g(y)) = y$ e $g(f(x)) = x$ para todo $x \in A$ e $y \in B$.

Se f tem uma inversa g, escrevemos muitas vezes f^{-1} em vez de g.

Agora determinaremos quando as funções têm inversas. Um bom candidato a inversa de $f\colon A \to B$ é $g\colon B \to A$ "definida por" explanation

$$g(y) = \text{"o" } x \text{ tal que } f(x) = y.$$

Mas as aspas em "definida por" (e em "o") sugerem que isto não é uma definição. Pelo menos, nem sempre funcionará com total generalidade. Pois, para

que esta definição especifique uma função, tem de haver um e apenas um x tal que $f(x) = y$—a saída de g tem de ficar unicamente determinada. Além disso, tem de estar especificada para todo $y \in B$. Se existirem x_1 e $x_2 \in A$ com $x_1 \neq x_2$ mas $f(x_1) = f(x_2)$, então $g(y)$ não ficaria unicamente determinada para $y = f(x_1) = f(x_2)$. E se não existir x algum tal que $f(x) = y$, então $g(y)$ nem sequer fica especificada. Em outras palavras, para g estar definida, f tem de ser tanto injetiva quanto sobrejetiva.

Vamos com calma. Dividiremos a questão em duas: dada uma função $f\colon A \to B$, quando existe uma função $g\colon B \to A$ tal que $g(f(x)) = x$? Tal g "desfaz" o que f faz, e chama-se *inversa à esquerda* de f. Em segundo lugar, quando existe uma função $h\colon B \to A$ tal que $f(h(y)) = y$? Tal h chama-se *inversa à direita* de f—f "desfaz" o que h faz.

Proposição 3.16. *Se $f\colon A \to B$ é injetiva, então existe uma* inversa à esquerda $g\colon B \to A$ *de f tal que $g(f(x)) = x$ para todo $x \in A$.*

Prova. Suponhamos que $f\colon A \to B$ é injetiva. Consideremos $y \in B$. Se $y \in \mathrm{Im}(f)$, existe $x \in A$ tal que $f(x) = y$. Como f é injetiva, há apenas um tal $x \in A$. Então podemos definir: $g(y) = x$, isto é, $g(y)$ é "o" $x \in A$ tal que $f(x) = y$. Se $y \notin \mathrm{Im}(f)$, podemos mapeá-lo para qualquer $a \in A$. Assim, podemos escolher $a \in A$ e definir $g\colon B \to A$ por:

$$g(y) = \begin{cases} x & \text{se } f(x) = y \\ a & \text{se } y \notin \mathrm{Im}(f). \end{cases}$$

Está definida para todo $y \in B$, pois para cada tal $y \in \mathrm{Im}(f)$ há exatamente um $x \in A$ tal que $f(x) = y$. Por definição, se $y = f(x)$, então $g(y) = x$, isto é, $g(f(x)) = x$. □

Problema 3.1. Mostre que, se $f\colon A \to B$ tem uma inversa à esquerda g, então f é injetiva.

Proposição 3.17. *Se $f\colon A \to B$ é sobrejetiva, então existe uma* inversa à direita $h\colon B \to A$ *de f tal que $f(h(y)) = y$ para todo $y \in B$.*

Prova. Suponhamos que $f\colon A \to B$ é sobrejetiva. Consideremos $y \in B$. Como f é sobrejetiva, existe $x_y \in A$ com $f(x_y) = y$. Então podemos definir: $h(y) = x_y$, isto é, para cada $y \in B$ escolhemos algum $x \in A$ tal que $f(x) = y$; como f é sobrejetiva há sempre pelo menos um de onde escolher.[1] Por definição, se $x = h(y)$, então $f(x) = y$, isto é, para todo $y \in B$, $f(h(y)) = y$. □

[1] Como f é sobrejetiva, para todo $y \in B$ o conjunto $\{x : f(x) = y\}$ é não vazio. A nossa definição de h exige que escolhamos um único x em cada um destes conjuntos. Que isto seja sempre possível não é de todo óbvio—a possibilidade de fazer estas escolhas é simplesmente assumida como axioma. Em outras palavras, esta proposição pressupõe o chamado Axioma da Escolha, questão a que aqui não damos destaque. Contudo, em muitos casos concretos, p.ex., quando $A = \mathbb{N}$ ou é finito, ou quando f é bijetiva, o Axioma da Escolha não é necessário. (No caso em que f é bijetiva, para cada $y \in B$ o conjunto $\{x : f(x) = y\}$ tem exatamente um membro, logo não há escolha a fazer.)

Problema 3.2. Mostre que, se $f\colon A \to B$ tem uma inversa à direita h, então f é sobrejetiva.

Combinando as ideias da prova anterior, obtemos agora que toda bijeção tem uma inversa, isto é, existe uma única função que é tanto inversa à esquerda quanto à direita de f. explanation

sfr:fun:inv: prop:bijection-inverse **Proposição 3.18.** *Se $f\colon A \to B$ é bijetiva, existe uma função $f^{-1}\colon B \to A$ tal que, para todo $x \in A$, $f^{-1}(f(x)) = x$ e, para todo $y \in B$, $f(f^{-1}(y)) = y$.*

Prova. Exercício. □

Problema 3.3. Prove Proposição 3.18. Tem de definir f^{-1}, mostrar que é uma função, e mostrar que é uma inversa de f, isto é, $f^{-1}(f(x)) = x$ e $f(f^{-1}(y)) = y$ para todo $x \in A$ e $y \in B$.

Há uma forma ligeiramente mais geral de extrair inversas. Vimos na Seção 3.2 que toda função f induz uma sobrejeção $f'\colon A \to \operatorname{Im}(f)$ pondo $f'(x) = f(x)$ para todo $x \in A$. Claramente, se f é injetiva, então f' é bijetiva, logo tem uma inversa única pela Proposição 3.18. Por um pequeno abuso de notação, chamamos por vezes à inversa de f' simplesmente "a inversa de f." explanation

sfr:fun:inv: prop:left-right **Proposição 3.19.** *Mostre que, se $f\colon A \to B$ tem uma inversa à esquerda g e uma inversa à direita h, então $h = g$.*

Prova. Exercício. □

Problema 3.4. Prove Proposição 3.19.

sfr:fun:inv: prop:inverse-unique **Proposição 3.20.** *Toda função f tem no máximo uma inversa.*

Prova. Suponhamos que g e h são ambas inversas de f. Então, em particular, g é uma inversa à esquerda de f e h é uma inversa à direita. Pela Proposição 3.19, $g = h$. □

3.5 Composição de Funções

sfr:fun:cmp: sec Vimos na Seção 3.4 que a inversa f^{-1} de uma bijeção f é ela própria uma função. Outra operação sobre funções é a composição: podemos definir uma nova função compondo duas funções, f e g, isto é, aplicando primeiro f e depois g. Claro que isto só é possível se as imagens e os domínios forem compatíveis, isto é, a imagem de f tem de ser um subconjunto do domínio de g. Esta operação sobre funções é o análogo da operação de produto relativo sobre relações na Seção 2.8. explanation

Um diagrama pode ajudar a explicar a ideia de composição. Na Figura 3.5, representamos duas funções $f\colon A \to B$ e $g\colon B \to C$ e a sua composição $(g \circ f)$. A função $(g \circ f)\colon A \to C$ associa cada membro de A a um membro de C.

Especificamos a que membro de C fica associado um membro de A do seguinte modo: dada uma entrada $x \in A$, aplicamos primeiro a função f a x, obtendo algum $f(x) = y \in B$, depois aplicamos a função g a y, obtendo algum $g(f(x)) = g(y) = z \in C$.

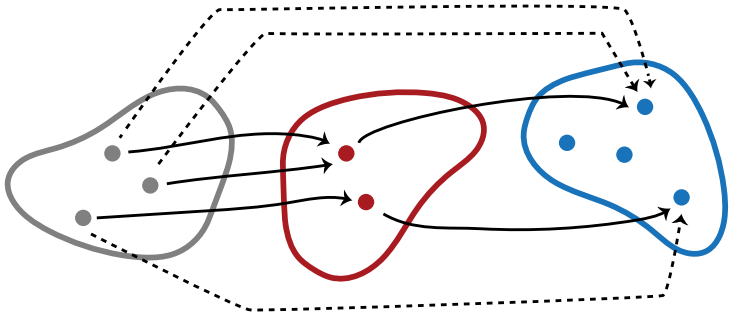


Figura 3.5: A composição $g \circ f$ de duas funções f e g.

sfr:fun:cmp: fig:composition

Definição 3.21 (Composição). Sejam $f\colon A \to B$ e $g\colon B \to C$ funções. A *composição* de f com g é $g \circ f\colon A \to C$, onde $(g \circ f)(x) = g(f(x))$.

Exemplo 3.22. Consideremos as funções $f(x) = x + 1$, e $g(x) = 2x$. Como $(g \circ f)(x) = g(f(x))$, para cada entrada x deve primeiro tomar-se o sucessor, depois multiplicar o resultado por dois. Logo a composição é dada por $(g \circ f)(x) = 2(x + 1)$.

Problema 3.5. Mostre que, se $f\colon A \to B$ e $g\colon B \to C$ são ambas injetiva, então $g \circ f\colon A \to C$ é injetiva.

Problema 3.6. Mostre que, se $f\colon A \to B$ e $g\colon B \to C$ são ambas sobrejetiva, então $g \circ f\colon A \to C$ é sobrejetiva.

Problema 3.7. Suponhamos $f\colon A \to B$ e $g\colon B \to C$. Mostre que o gráfico de $g \circ f$ é $R_f \mid R_g$.

3.6 Funções Parciais

explanation

sfr:fun:par: sec

Às vezes é útil relaxar a definição de função de modo que não seja exigido que a saída da função esteja definida para todas as entradas possíveis. Tais mapeamentos são chamados de *funções parciais*.

Definição 3.23. Uma *função parcial* $f\colon A \nrightarrow B$ é um mapeamento que associa a cada membro de A no máximo um membro de B. Se f associa um membro de B a $x \in A$, dizemos que $f(x)$ está *definido*, e caso contrário *indefinido*. Se $f(x)$ está definido, escrevemos $f(x)\downarrow$, caso contrário $f(x)\uparrow$. O *domínio* de uma função parcial f é o subconjunto de A onde ela está definida, isto é, $\mathrm{dom}(f) = \{x \in A : f(x)\downarrow\}$.

Exemplo 3.24. Toda função $f\colon A \to B$ é também uma função parcial. Funções parciais que estão definidas em todo A—isto é, o que até agora chamávamos simplesmente de função—também são chamadas de funções *totais*.

Exemplo 3.25. A função parcial $f\colon \mathbb{R} \nrightarrow \mathbb{R}$ dada por $f(x) = 1/x$ é indefinida para $x = 0$ e definida em todo o restante.

Problema 3.8. Dada $f\colon A \nrightarrow B$, defina a função parcial $g\colon B \nrightarrow A$ por: para qualquer $y \in B$, se existe um único $x \in A$ tal que $f(x) = y$, então $g(y) = x$; caso contrário $g(y)\uparrow$. Mostre que se f é injetiva, então $g(f(x)) = x$ para todo $x \in \mathrm{dom}(f)$ e $f(g(y)) = y$ para todo $y \in \mathrm{Im}(f)$.

Definição 3.26 (Gráfico de uma função parcial). Seja $f\colon A \nrightarrow B$ uma função parcial. O *gráfico* de f é a relação $R_f \subseteq A \times B$ definida por

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

Proposição 3.27. *Suponha que $R \subseteq A \times B$ tem a propriedade de que sempre que Rxy e Rxy' então $y = y'$. Então R é o gráfico da função parcial $f\colon A \nrightarrow B$ definida por: se existe um y tal que Rxy, então $f(x) = y$, caso contrário $f(x)\uparrow$. Se R também é* serial*, isto é, para cada $x \in A$ existe um $y \in B$ tal que Rxy, então f é total.*

Prova. Suponha que existe um y tal que Rxy. Se existisse outro $y' \neq y$ tal que Rxy', a condição sobre R seria violada. Portanto, se existe um y tal que Rxy, esse y é único, e assim f é bem definida. Obviamente, $R_f = R$ e f é total se R é serial. □

Capítulo 4

O Tamanho dos Conjuntos

Este capítulo discute enumerações e conjuntos contáveis e incontáveis. Várias seções vêm em duas versões: uma mais elementar, que toma enumerações como listas, ou sobrejeções de $\mathbb{Z}^+$; e uma mais abstrata que define enumerações como bijeções com $\mathbb{N}$.

4.1 Introdução

sfr:siz:int:sec

Quando Georg Cantor desenvolveu a teoria dos conjuntos na década de 1870, um dos seus objetivos era tornar aceitável a ideia de uma coleção infinita—um infinito *atual*, como diriam os medievais. Parte central disto foi o seu tratamento do *tamanho* de conjuntos diferentes. Se a, b e c são todos distintos, então o conjunto $\{a, b, c\}$ é intuitivamente *maior* que $\{a, b\}$. Mas e os conjuntos infinitos? Serão todos do mesmo tamanho? Acontece que não.

A primeira ideia importante aqui é a de *enumeração*. Podemos listar qualquer conjunto finito enumerando todos os seus membros. Para alguns conjuntos infinitos, também podemos listar todos os seus membros se permitirmos que a própria lista seja infinita. Tais conjuntos chamam-se enumeráveis. O resultado surpreendente de Cantor, que compreenderemos completamente no fim deste capítulo, foi que alguns conjuntos infinitos *não* são enumeráveis.

4.2 Enumerações e Conjuntos Enumeráveis

sfr:siz:enm:sec

Esta seção discute enumerações de conjuntos, definindo-as como sobrejeções de $\mathbb{Z}^+$. Faz as coisas devagar, para leitores com pouca formação matemática. Uma versão alternativa, mais concisa, é dada na Seção 4.11,

que define enumerações de outro modo: como bijeções com $\mathbb{N}$ (ou um segmento inicial).

Já demos exemplos de conjuntos listando seus membros. Discutamos agora, de maneira mais geral, como e quando podemos listar os membros de um conjunto, mesmo que esse conjunto seja infinito. explanation

Definição 4.1 (Enumeração, informalmente). Informalmente, uma *enumeração* de um conjunto A é uma lista (possivelmente infinita) de membros de A tal que todo membro de A aparece na lista em alguma posição finita. Se A tem uma enumeração, então diz-se que A é *enumerável*.

Alguns pontos sobre enumerações: explanation

1. Contamos como enumerações apenas listas que têm um começo e em que todo membro além do primeiro tem um único membro imediatamente anterior. Em outras palavras, há apenas um número finito de elementos entre o primeiro membro da lista e qualquer outro membro. Em particular, isso significa que todo membro de uma enumeração tem uma posição finita: o primeiro membro tem posição 1, o segundo posição 2, etc.

2. Podemos ter enumerações diferentes do mesmo conjunto A que diferem pela ordem em que os membros aparecem: 4, 1, 25, 16, 9 enumera os (conjunto dos) cinco primeiros quadrados tão bem quanto 1, 4, 9, 16, 25.

3. Enumerações redundantes ainda são enumerações: 1, 1, 2, 2, 3, 3, ... enumera o mesmo conjunto que 1, 2, 3, ...

4. Ordem e redundância *importam* quando especificamos uma enumeração: podemos enumerar os inteiros positivos começando com 1, 2, 3, 1, ..., mas o padrão é mais fácil de ver quando enumerados da maneira padrão como 1, 2, 3, 4, ...

5. Enumerações devem ter um começo: ..., 3, 2, 1 não é uma enumeração dos inteiros positivos porque não tem primeiro membro. Para ver como isso segue da definição informal, pergunte a si mesmo: "em que posição na lista o número 76 aparece?"

6. O seguinte não é uma enumeração dos inteiros positivos: 1, 3, 5, ..., 2, 4, 6, ... O problema é que os números pares ocorrem nas posições $\infty+1$, $\infty+2$, $\infty+3$, em vez de em posições finitas.

7. O conjunto vazio é enumerável: é enumerado pela lista vazia!

Proposição 4.2. *Se A tem uma enumeração, tem uma enumeração sem repetições.*

Prova. Suponha que A tem uma enumeração $x_1, x_2, \ldots$ em que cada x_i é um membro de A. Podemos remover repetições de uma enumeração removendo membros repetidos. Por exemplo, podemos transformar a enumeração em uma nova na qual listamos x_i se ele é um membro de A que não está entre $x_1, \ldots, x_{i-1}$ ou removemos x_i da lista se já aparece entre $x_1, \ldots, x_{i-1}$. □

O último argumento mostra que, para obter um bom controle sobre enumerações e conjuntos enumeráveis e provar coisas sobre eles, precisamos de uma definição mais precisa. O seguinte a fornece.

Definição 4.3 (Enumeração, formalmente). Uma *enumeração* de um conjunto $A \neq \emptyset$ é qualquer função sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

explanation

Convençamo-nos de que a definição formal e a definição informal usando uma lista possivelmente infinita são equivalentes. Primeiro, qualquer função sobrejetiva de $\mathbb{Z}^+$ para um conjunto A enumera A. Tal função determina uma enumeração conforme definido informalmente acima: a lista $f(1)$, $f(2)$, $f(3)$, ... Como f é sobrejetiva, todo membro de A é garantidamente o valor de $f(n)$ para algum $n \in \mathbb{Z}^+$. Logo, todo membro de A aparece em alguma posição finita na lista. Como a função pode não ser injetiva, a lista pode ser redundante, mas isso é aceitável (como observado acima).

Por outro lado, dada uma lista que enumera todos os membros de A, podemos definir uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$ fazendo $f(n)$ ser o n-ésimo membro da lista, ou o último membro da lista se não há n-ésimo membro. O único caso em que isso não produz uma função sobrejetiva é quando A é vazio, e portanto a lista é vazia. Assim, toda lista não vazia determina uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

Definição 4.4. Um conjunto A é enumerável sse é vazio ou tem uma enumeração.

sfr:siz:enm:defn:enumerable

Exemplo 4.5. Uma função que enumera os inteiros positivos ($\mathbb{Z}^+$) é simplesmente a função identidade dada por $f(n) = n$. Uma função que enumera os números naturais $\mathbb{N}$ é a função $g(n) = n - 1$.

Exemplo 4.6. As funções $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ e $g\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ dadas por

$$f(n) = 2n \text{ e}$$
$$g(n) = 2n - 1$$

enumeram os inteiros positivos pares e os inteiros positivos ímpares, respectivamente. Contudo, nenhuma das funções é uma enumeração de $\mathbb{Z}^+$, já que nenhuma é sobrejetiva.

Problema 4.1. Defina uma enumeração dos quadrados positivos 1, 4, 9, 16, ...

Exemplo 4.7. A função $f(n) = (-1)^n \lceil \frac{(n-1)}{2} \rceil$ (onde $\lceil x \rceil$ denota a função *teto*, que arredonda x para cima até o inteiro mais próximo) enumera o conjunto dos inteiros $\mathbb{Z}$. Note como f gera os valores de $\mathbb{Z}$ "saltando" de um lado para outro entre inteiros positivos e negativos:

$$\begin{array}{cccccccc} f(1) & f(2) & f(3) & f(4) & f(5) & f(6) & f(7) & \dots \\ -\lceil \frac{0}{2} \rceil & \lceil \frac{1}{2} \rceil & -\lceil \frac{2}{2} \rceil & \lceil \frac{3}{2} \rceil & -\lceil \frac{4}{2} \rceil & \lceil \frac{5}{2} \rceil & -\lceil \frac{6}{2} \rceil & \dots \\ 0 & 1 & -1 & 2 & -2 & 3 & \dots & \end{array}$$

Você também pode pensar em f como definida por casos da seguinte forma:

$$f(n) = \begin{cases} 0 & \text{se } n = 1 \\ n/2 & \text{se } n \text{ é par} \\ -(n-1)/2 & \text{se } n \text{ é ímpar e} > 1 \end{cases}$$

Problema 4.2. Mostre que se A e B são enumeráveis, então $A \cup B$ também é. Para isso, suponha que há funções sobrejetivas $f\colon \mathbb{Z}^+ \to A$ e $g\colon \mathbb{Z}^+ \to B$, e defina uma função sobrejetiva $h\colon \mathbb{Z}^+ \to A \cup B$ e mostre que ela é sobrejetiva. Considere também os casos em que A ou $B = \emptyset$.

Problema 4.3. Mostre que se $B \subseteq A$ e A é enumerável, então B também é. Para isso, suponha que há uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Defina uma função sobrejetiva $g\colon \mathbb{Z}^+ \to B$ e mostre que ela é sobrejetiva. O que acontece se $B = \emptyset$?

Problema 4.4. Mostre por indução em n que se A_1, A_2, ..., A_n são todos enumeráveis, então $A_1 \cup \dots \cup A_n$ também é. Você pode assumir o fato de que se dois conjuntos A e B são enumeráveis, então $A \cup B$ também é.

Embora seja talvez mais natural ao listar os membros de um conjunto começar a contar a partir do 1º membro, os matemáticos gostam de usar os números naturais $\mathbb{N}$ para contar coisas. Eles falam do 0º, 1º, 2º, e assim por diante, membro de uma lista. Correspondentemente, podemos definir uma enumeração como uma função sobrejetiva de $\mathbb{N}$ para A. É claro que as duas definições são equivalentes.

sfr:siz:enm: prop:enum-shift

Proposição 4.8. *Há uma sobrejeção $f\colon \mathbb{Z}^+ \to A$ sse há uma sobrejeção $g\colon \mathbb{N} \to A$.*

Prova. Dada uma sobrejeção $f\colon \mathbb{Z}^+ \to A$, podemos definir $g(n) = f(n+1)$ para todo $n \in \mathbb{N}$. É fácil ver que $g\colon \mathbb{N} \to A$ é sobrejetiva. Reciprocamente, dada uma sobrejeção $g\colon \mathbb{N} \to A$, defina $f(n) = g(n-1)$. □

Isso nos dá o seguinte resultado:

Corolário 4.9. *Um conjunto A é enumerável sse é vazio ou há uma função sobrejetiva $f\colon \mathbb{N} \to A$.* *sfr:siz:enm: cor:enum-nat*

Discutimos acima que uma lista de membros de um conjunto A pode ser transformada em uma lista sem repetições. Isso também vale para enumerações, mas é um pouco mais difícil de formular e provar rigorosamente. Qualquer função $f\colon \mathbb{Z}^+ \to A$ deve estar definida para todo $n \in \mathbb{Z}^+$. Se há apenas um número finito de membros em A, então claramente não podemos ter uma função definida nos infinitos membros de $\mathbb{Z}^+$ que toma como valores todos os membros de A mas nunca toma o mesmo valor duas vezes. Nesse caso, isto é, no caso em que a lista sem repetições é finita, devemos escolher um domínio diferente para f, um com apenas um número finito de membros. Não ter repetições significa que f deve ser injetiva. Como também é sobrejetiva, estamos procurando uma bijeção entre algum conjunto finito $\{1, \ldots, n\}$ ou $\mathbb{Z}^+$ e A.

Proposição 4.10. *Se $f\colon \mathbb{Z}^+ \to A$ é sobrejetiva (isto é, uma enumeração de A), há uma bijeção $g\colon Z \to A$ onde Z é $\mathbb{Z}^+$ ou $\{1, \ldots, n\}$ para algum $n \in \mathbb{Z}^+$.* *sfr:siz:enm: prop:enum-bij*

Prova. Definimos a função g recursivamente: seja $g(1) = f(1)$. Se $g(i)$ já foi definido, seja $g(i+1)$ o primeiro valor de $f(1), f(2), \ldots$ que ainda não está entre $g(1), \ldots, g(i)$, se houver um. Se A tem apenas n membros, então $g(1), \ldots, g(n)$ estão todos definidos, e assim definimos uma função $g\colon \{1, \ldots, n\} \to A$. Se A tem infinitos membros, então para qualquer i deve haver um membro de A na enumeração $f(1), f(2), \ldots$, que ainda não está entre $g(1), \ldots, g(i)$. Nesse caso definimos uma função $g\colon \mathbb{Z}^+ \to A$.

A função g é sobrejetiva, já que qualquer elemento de A está entre $f(1), f(2), \ldots$ (pois f é sobrejetiva) e assim eventualmente será um valor de $g(i)$ para algum i. Também é injetiva, já que se houvesse $j < i$ tal que $g(j) = g(i)$, então $g(i)$ já estaria entre $g(1), \ldots, g(i-1)$, contrariamente à forma como definimos g. □

Corolário 4.11. *Um conjunto A é enumerável sse é vazio ou há uma bijeção $f\colon N \to A$ onde $N = \mathbb{N}$ ou $N = \{0, \ldots, n\}$ para algum $n \in \mathbb{N}$.* *sfr:siz:enm: cor:enum-nat-bij*

Prova. A é enumerável sse A é vazio ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Pela Proposição 4.10, o último vale sse há uma função bijetiva $f\colon Z \to A$ onde $Z = \mathbb{Z}^+$ ou $Z = \{1, \ldots, n\}$ para algum $n \in \mathbb{Z}^+$. Pelo mesmo argumento da prova da Proposição 4.8, isso por sua vez é o caso sse há uma bijeção $g\colon N \to A$ onde $N = \mathbb{N}$ ou $N = \{0, \ldots, n-1\}$. □

Problema 4.5. De acordo com a Definição 4.4, um conjunto A é enumerável sse $A = \emptyset$ ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Também é possível definir "conjunto enumerável" precisamente por: um conjunto é enumerável sse há uma função injetiva $g\colon A \to \mathbb{Z}^+$. Mostre que as definições são equivalentes, isto é, mostre que há uma função injetiva $g\colon A \to \mathbb{Z}^+$ sse $A = \emptyset$ ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

4.3 Método do Zigue-Zague de Cantor

sfr:siz:zigzag:sec

Já consideramos algumas enumerações "fáceis". Vejamos algo um pouco mais difícil. Considere-se o conjunto dos pares de números naturais, que definimos na Seção 1.5 assim: explanation

$$\mathbb{N} \times \mathbb{N} = \{\langle n, m\rangle : n, m \in \mathbb{N}\}$$

Podemos organizar estes pares ordenados numa *matriz*, assim:

	0	**1**	**2**	**3**	...
0	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 0,2\rangle$	$\langle 0,3\rangle$	...
1	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 1,2\rangle$	$\langle 1,3\rangle$	...
2	$\langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 2,2\rangle$	$\langle 2,3\rangle$	...
3	$\langle 3,0\rangle$	$\langle 3,1\rangle$	$\langle 3,2\rangle$	$\langle 3,3\rangle$	...
⋮	⋮	⋮	⋮	⋮	⋱

Claramente, cada par ordenado em $\mathbb{N} \times \mathbb{N}$ aparece exatamente uma vez na matriz. Em particular, $\langle n, m\rangle$ aparece na n-ésima linha e na m-ésima coluna. Mas como organizar os elementos de tal matriz numa lista "unidimensional"? O padrão na matriz abaixo demonstra uma forma de o fazer (embora haja, claro, muitas outras):

	0	**1**	**2**	**3**	**4**	...
0	0	1	3	6	10	...
1	2	4	7	11	...	...
2	5	8	12	...	...	...
3	9	13	...	...	...	...
4	14	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	⋮	⋱

Este padrão chama-se *método do zigue-zague de Cantor*. Enumera $\mathbb{N} \times \mathbb{N}$ do seguinte modo:

$$\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 0,2\rangle, \langle 1,1\rangle, \langle 2,0\rangle, \langle 0,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \ldots$$

Isto estabelece o seguinte:

sfr:siz:zigzag:natsquaredenumerable

Proposição 4.12. $\mathbb{N} \times \mathbb{N}$ *é enumerável.*

Prova. Seja $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ a função que a cada $k \in \mathbb{N}$ associa o tuplo $\langle n, m\rangle \in \mathbb{N} \times \mathbb{N}$ tal que k é o valor na n-ésima linha e m-ésima coluna da matriz do zigue-zague de Cantor. □

Esta técnica generaliza-se bem. Por exemplo, podemos usá-la para enumerar o conjunto dos triplos ordenados de números naturais, isto é: explanation

$$\mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{\langle n, m, k\rangle : n, m, k \in \mathbb{N}\}$$

Pensamos em $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ como o produto cartesiano de $\mathbb{N} \times \mathbb{N}$ com $\mathbb{N}$, isto é,

$$\mathbb{N}^3 = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} = \{\langle\langle n, m\rangle, k\rangle : n, m, k \in \mathbb{N}\}$$

e assim podemos enumerar $\mathbb{N}^3$ com uma matriz rotulando um eixo com a enumeração de $\mathbb{N}$ e o outro com a enumeração de $\mathbb{N}^2$:

	0	**1**	**2**	**3**	...
$\langle \mathbf{0}, \mathbf{0}\rangle$	$\langle 0,0,0\rangle$	$\langle 0,0,1\rangle$	$\langle 0,0,2\rangle$	$\langle 0,0,3\rangle$	...
$\langle \mathbf{0}, \mathbf{1}\rangle$	$\langle 0,1,0\rangle$	$\langle 0,1,1\rangle$	$\langle 0,1,2\rangle$	$\langle 0,1,3\rangle$	...
$\langle \mathbf{1}, \mathbf{0}\rangle$	$\langle 1,0,0\rangle$	$\langle 1,0,1\rangle$	$\langle 1,0,2\rangle$	$\langle 1,0,3\rangle$	...
$\langle \mathbf{0}, \mathbf{2}\rangle$	$\langle 0,2,0\rangle$	$\langle 0,2,1\rangle$	$\langle 0,2,2\rangle$	$\langle 0,2,3\rangle$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Assim, com um método como o zigue-zague de Cantor, obtemos analogamente uma enumeração de $\mathbb{N}^3$. E podemos continuar, obtendo enumerações de $\mathbb{N}^n$ para qualquer número natural n. Logo:

Proposição 4.13. *$\mathbb{N}^n$ é enumerável, para todo $n \in \mathbb{N}$.*

Problema 4.6. Mostre que $(\mathbb{Z}^+)^n$ é enumerável, para todo $n \in \mathbb{N}$.

Problema 4.7. Mostre que $(\mathbb{Z}^+)^*$ é enumerável. Pode assumir Problema 4.6.

4.4 Funções de Pareamento e Códigos

explanation

O método do zigue-zague de Cantor torna visualmente evidente a enumerabilidade de $\mathbb{N}^n$. Mas vamos concentrar-nos na nossa matriz que representa $\mathbb{N}^2$. Seguindo a linha em zigue-zague na matriz e contando as posições, podemos verificar que $\langle 1, 2\rangle$ fica associado ao número 7. Seria útil, contudo, poder calcular isto de modo mais direto. Ou seja, seria útil dispor da *inversa* da enumeração em zigue-zague, $g\colon \mathbb{N}^2 \to \mathbb{N}$, tal que

sfr:siz:pai:sec

$$g(\langle 0,0\rangle) = 0,\ g(\langle 0,1\rangle) = 1,\ g(\langle 1,0\rangle) = 2,\ \ldots, g(\langle 1,2\rangle) = 7,\ \ldots$$

Isto permitir-nos-ia calcular exatamente em que posição da enumeração cai $\langle n, m\rangle$.

De fato, podemos definir g diretamente com base em duas observações. Primeiro: se a n-ésima linha e a m-ésima coluna contêm o valor v, então a $(n+1)$-ésima linha e a $(m-1)$-ésima coluna contêm o valor $v+1$. Segundo: a primeira linha da nossa enumeração consiste nos números triangulares, começando por 0, 1, 3, 6, etc. O k-ésimo número triangular é a soma dos números naturais $< k$, que se pode calcular como $k(k+1)/2$. Juntando estas duas observações, consideremos a função:

$$g(n, m) = \frac{(n+m+1)(n+m)}{2} + n$$

Escreve-se frequentemente $g(n, m)$ em vez de $g(\langle n, m\rangle)$, já que é mais fácil para os olhos. Isto diz-nos que se determine primeiro o $(n + m)$-ésimo número triangular e depois que lhe somemos n. A função preenche a matriz exatamente da maneira que desejamos. Em particular, o par $\langle 1, 2\rangle$ é enviado para $\frac{4\times 3}{2} + 1 = 7$.

Esta função g é a *inversa* de uma enumeração de um conjunto de pares. Tais funções chamam-se *funções de emparelhamento*.

Definição 4.14 (Função de emparelhamento). Uma função $f\colon A \times B \to \mathbb{N}$ é uma *função de emparelhamento* aritmética se f for injetiva. Dizemos também que f *codifica* $A \times B$, e que $f(x, y)$ é o *código* de $\langle x, y\rangle$.

Podemos usar funções de emparelhamento para codificar, por exemplo, pares de números naturais; ou, em outras palavras, podemos representar cada *par* de elementos por um *único* número. Usando a inversa da função de emparelhamento, podemos *descodificar* o número, isto é, determinar que par representa. explanation

Problema 4.8. Dê uma enumeração do conjunto de todos os números racionais não negativos.

Problema 4.9. Mostre que $\mathbb{Q}$ é enumerável. Recordemos que qualquer número racional se pode escrever como uma fração z/m com $z \in \mathbb{Z}$, $m \in \mathbb{N}^+$.

Problema 4.10. Defina uma enumeração de $\mathbb{B}^*$.

Problema 4.11. Recordando o curso introdutório de lógica, cada tabela de verdade possível exprime uma função de verdade. Em outras palavras, as funções de verdade são todas as funções de $\mathbb{B}^k \to \mathbb{B}$ para algum k. Prove que o conjunto de todas as funções de verdade é enumerável.

Problema 4.12. Mostre que o conjunto de todos os subconjuntos finitos de um conjunto infinito enumerável arbitrário é enumerável.

Problema 4.13. Um subconjunto de $\mathbb{N}$ diz-se *confinito* sse for o complemento de um conjunto finito; isto é, $A \subseteq \mathbb{N}$ é confinito sse $\mathbb{N} \setminus A$ for finito. Seja I o conjunto cujos membros são exatamente os subconjuntos finitos e confinitos de $\mathbb{N}$. Mostre que I é enumerável.

Problema 4.14. Mostre que a união enumerável de conjuntos enumeráveis é enumerável. Isto é, sempre que A_1, A_2, ... são conjuntos e cada A_i é enumerável, então a união $\bigcup_{i=1}^{\infty} A_i$ de todos eles também é enumerável. [Nota: isto é difícil!]

Problema 4.15. Seja $f\colon A \times B \to \mathbb{N}$ uma função de emparelhamento arbitrária. Mostre que a inversa de f é uma enumeração de $A \times B$.

Problema 4.16. Especifique uma função que codifique $\mathbb{N}^3$.

4.5 Uma Função de Emparelhamento Alternativa

explanation

Há outras enumerações de $\mathbb{N}^2$ que facilitam descobrir quais são suas inversas. Eis uma. Em vez de visualizar a enumeração em uma matriz, comece com a lista de inteiros positivos associados a espaços (inicialmente) vazios. Imagine preencher esses espaços sucessivamente com pares $\langle n, m\rangle$ da seguinte forma. Começando com os pares que têm 0 na primeira posição (isto é, pares $\langle 0, m\rangle$), coloque o primeiro (isto é, $\langle 0, 0\rangle$) no primeiro espaço vazio, depois pule um espaço vazio, coloque o segundo (isto é, $\langle 0, 2\rangle$) no próximo espaço vazio, pule outro, e assim por diante. O começo (incompleto) de nossa enumeração agora se parece com isto

sfr:siz:pai-alt:sec

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0,0\rangle$		$\langle 0,1\rangle$		$\langle 0,2\rangle$		$\langle 0,3\rangle$		$\langle 0,4\rangle$		...

Repita isso com pares $\langle 1, m\rangle$ nos lugares que ainda permanecem vazios, novamente pulando cada outro espaço vazio:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0,0\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$		$\langle 0,2\rangle$	$\langle 1,1\rangle$	$\langle 0,3\rangle$		$\langle 0,4\rangle$	$\langle 1,2\rangle$	...

Insira pares $\langle 2, m\rangle$, $\langle 2, m\rangle$, etc., da mesma forma. Nossa enumeração completa assim começa assim:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	...
$\langle 0,0\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 2,0\rangle$	$\langle 0,2\rangle$	$\langle 1,1\rangle$	$\langle 0,3\rangle$	$\langle 3,0\rangle$	$\langle 0,4\rangle$	$\langle 1,2\rangle$	...

Se numerarmos as células na matriz acima de acordo com essa enumeração, não encontraremos uma linha zigue-zague arrumada, mas este arranjo:

	0	**1**	**2**	**3**	**4**	**5**	...
0	1	3	5	7	9	11	...
1	2	6	10	14	18	...	...
2	4	12	20	28	...	...	...
3	8	24	40	...	...	...	...
4	16	48	...	...	...	...	...
5	32	...	...	...	...	...	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Podemos ver que os pares na linha 0 estão nas posições ímpares de nossa enumeração, isto é, o par $\langle 0, m\rangle$ está na posição $2m + 1$; os pares na segunda linha, $\langle 1, m\rangle$, estão em posições cujo número é o dobro de um número ímpar, especificamente, $2\cdot(2m+1)$; os pares na terceira linha, $\langle 2, m\rangle$, estão em posições cujo número é quatro vezes um número ímpar, $4 \cdot (2m + 1)$; e assim por diante. Os fatores de $(2m + 1)$ para cada linha, 1, 2, 4, 8, ..., são exatamente as potências de 2: $1 = 2^0$, $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, ... De fato, o expoente

relevante é sempre o primeiro membro do par em questão. Assim, para o par $\langle n, m\rangle$ o fator é 2^n. Isso nos dá a fórmula geral: $2^n \cdot (2m + 1)$. Contudo, isso é um mapeamento de pares para inteiros *positivos*, isto é, $\langle 0, 0\rangle$ tem posição 1. Se quisermos começar na posição 0 devemos subtrair 1 do resultado. Isso nos dá:

Exemplo 4.15. A função $h\colon \mathbb{N}^2 \to \mathbb{N}$ dada por

$$h(n, m) = 2^n(2m + 1) - 1$$

é uma função de emparelhamento para o conjunto de pares de números naturais $\mathbb{N}^2$.

explanation

De acordo com nossa segunda enumeração de $\mathbb{N}^2$, o par $\langle 0, 0\rangle$ tem código $h(0, 0) = 2^0(2 \cdot 0 + 1) - 1 = 0$; $\langle 1, 2\rangle$ tem código $2^1 \cdot (2 \cdot 2 + 1) - 1 = 2 \cdot 5 - 1 = 9$; $\langle 2, 6\rangle$ tem código $2^2 \cdot (2 \cdot 6 + 1) - 1 = 51$.

Às vezes basta codificar pares de números naturais $\mathbb{N}^2$ sem exigir que a codificação seja sobrejetora. Tais codificações têm inversas que são apenas funções parciais.

Exemplo 4.16. A função $j\colon \mathbb{N}^2 \to \mathbb{N}^+$ dada por

$$j(n, m) = 2^n 3^m$$

é uma função injetiva $\mathbb{N}^2 \to \mathbb{N}$.

4.6 Conjuntos Não enumeráveis

sfr:siz:nen:sec

Esta seção prova a não enumerabilidade de $\mathbb{B}^\omega$ e $\wp(\mathbb{Z}^+)$ usando a definição na Seção 4.2. Foi concebida para ser um pouco mais elementar e um pouco mais detalhada que a versão na Seção 4.11

Alguns conjuntos, como o conjunto $\mathbb{Z}^+$ dos inteiros positivos, são infinitos. Até agora vimos exemplos de conjuntos infinitos que eram todos enumerável. Contudo, há também conjuntos infinitos que não têm essa propriedade. Tais conjuntos são chamados de *não enumerável*.

Em primeiro lugar, talvez já seja surpreendente que existam conjuntos não enumerável. Para qualquer conjunto enumerável A há uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Se um conjunto é não enumerável, não há tal função. Isto é, nenhuma função mapeando os infinitos membros de $\mathbb{Z}^+$ para A pode esgotar todo A. Assim, há "mais" membros em A do que os infinitos inteiros positivos.

Como se provaria que um conjunto é não enumerável? É preciso mostrar que nenhuma tal função sobrejetora pode existir. Equivalentemente, é preciso mostrar que os elementos de A não podem ser enumerados em uma lista infinita

unidirecional. A melhor maneira de fazer isso é mostrar que toda lista de membros de A deve deixar de fora pelo menos um elemento; ou que nenhuma função $f\colon \mathbb{Z}^+ \to A$ pode ser sobrejetiva. Podemos fazer isso usando o *método diagonal* de Cantor. Dada uma lista de membros de A, digamos, x_1, x_2, ..., construímos outro elemento de A que, por sua construção, não pode estar naquela lista.

Nosso primeiro exemplo é o conjunto $\mathbb{B}^\omega$ de todas as sequências infinitas, sem lacunas, de 0s e 1s.

Teorema 4.17. *$\mathbb{B}^\omega$ é não enumerável.*

sfr:siz:nen:
thm:nonenum-bin-omega

Prova. Suponha, por absurdo, que $\mathbb{B}^\omega$ é enumerável, isto é, suponha que há uma lista s_1, s_2, s_3, s_4, ... de todos os membros de $\mathbb{B}^\omega$. Cada um desses s_i é em si uma sequência infinita de 0s e 1s. Chamemos o j-ésimo elemento da i-ésima sequência nessa lista de $s_i(j)$. Então a i-ésima sequência s_i é

$$s_i(1), s_i(2), s_i(3), \ldots$$

Podemos organizar essa lista, e os elementos de cada sequência s_i nela, em uma matriz:

	1	2	3	4	...
1	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	$s_1(4)$	...
2	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	$s_2(4)$	...
3	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	$s_3(4)$	...
4	$s_4(1)$	$s_4(2)$	$s_4(3)$	$\mathbf{s_4(4)}$	...
⋮	⋮	⋮	⋮	⋮	⋱

Os rótulos ao lado indicam o número da sequência na lista s_1, s_2, ...; os números no topo rotulam os membros das sequências individuais. Por exemplo, $s_1(1)$ é um nome para qualquer número, um 0 ou um 1, que é o primeiro membro na sequência s_1, e assim por diante.

Agora construímos uma sequência infinita, $\overline{s}$, de 0s e 1s que não pode estar nessa lista. A definição de $\overline{s}$ dependerá da lista s_1, s_2, ... Qualquer lista infinita de sequências infinitas de 0s e 1s dá origem a uma sequência infinita $\overline{s}$ que está garantidamente fora da lista.

Para definir $\overline{s}$, especificamos todos os seus membros, isto é, especificamos $\overline{s}(n)$ para todo $n \in \mathbb{Z}^+$. Fazemos isso lendo a diagonal da matriz acima (daí o nome "método diagonal") e depois trocando cada 1 por 0 e cada 0 por 1. De maneira mais abstrata, definimos $\overline{s}(n)$ como 0 ou 1 conforme o n-ésimo membro da diagonal, $s_n(n)$, é 1 ou 0.

$$\overline{s}(n) = \begin{cases} 1 & \text{se } s_n(n) = 0 \\ 0 & \text{se } s_n(n) = 1. \end{cases}$$

Se você prefere fórmulas a definições por casos, também pode definir $\overline{s}(n) = 1 - s_n(n)$.

Claramente $\overline{s}$ é uma sequência infinita de 0s e 1s, já que é apenas a sequência espelhada da sequência de 0s e 1s que aparecem na diagonal de nossa matriz. Assim $\overline{s}$ é um membro de $\mathbb{B}^\omega$. Mas não pode estar na lista s_1, s_2, ... Por quê?

Não pode ser a primeira sequência na lista, s_1, porque difere de s_1 no primeiro membro. Seja qual for $s_1(1)$, definimos $\overline{s}(1)$ como o oposto. Não pode ser a segunda sequência na lista, porque $\overline{s}$ difere de s_2 no segundo elemento: se $s_2(2)$ é 0, $\overline{s}(2)$ é 1, e vice-versa. E assim por diante.

Mais precisamente: se $\overline{s}$ estivesse na lista, haveria algum k tal que $\overline{s} = s_k$. Duas sequências são idênticas sse concordam em toda posição, isto é, para qualquer n, $\overline{s}(n) = s_k(n)$. Em particular, tomando $n = k$ como caso especial, $\overline{s}(k) = s_k(k)$ teria de valer. $s_k(k)$ é 0 ou 1. Se é 0, então $\overline{s}(k)$ deve ser 1—é assim que definimos $\overline{s}$. Mas se $s_k(k) = 1$, de novo por causa da forma como definimos $\overline{s}$, $\overline{s}(k) = 0$. Em ambos os casos $\overline{s}(k) \neq s_k(k)$.

Começamos supondo que há uma lista de membros de $\mathbb{B}^\omega$, s_1, s_2, ... A partir dessa lista construímos uma sequência $\overline{s}$ que provamos não poder estar na lista. Mas ela definitivamente é uma sequência de 0s e 1s se todos os s_i são sequências de 0s e 1s, isto é, $\overline{s} \in \mathbb{B}^\omega$. Isso mostra em particular que não pode haver lista de *todos* os membros de $\mathbb{B}^\omega$, já que para qualquer tal lista também poderíamos construir uma sequência $\overline{s}$ garantidamente fora da lista, de modo que a suposição de que há uma lista de todas as sequências em $\mathbb{B}^\omega$ leva a uma contradição. □

explanation

Esse método de prova é chamado de "diagonalização" porque usa a diagonal da matriz para definir $\overline{s}$. A diagonalização não precisa envolver a presença de uma matriz: podemos mostrar que conjuntos não são enumerável usando uma ideia semelhante mesmo quando não há matriz nem diagonal propriamente dita.

sfr:siz:nen: thm:nonenum-pownat

Teorema 4.18. *$\wp(\mathbb{Z}^+)$ não é enumerável.*

Prova. Procedemos da mesma forma, mostrando que para toda lista de subconjuntos de $\mathbb{Z}^+$ há um subconjunto de $\mathbb{Z}^+$ que não pode estar na lista. Suponha que a seguinte é uma lista dada de subconjuntos de $\mathbb{Z}^+$:

$$Z_1, Z_2, Z_3, \ldots$$

Agora definimos um conjunto $\overline{Z}$ tal que para qualquer $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ sse $n \notin Z_n$:

$$\overline{Z} = \{n \in \mathbb{Z}^+ : n \notin Z_n\}$$ □

$\overline{Z}$ é claramente um conjunto de inteiros positivos, já que por suposição cada Z_n o é, e assim $\overline{Z} \in \wp(\mathbb{Z}^+)$. Mas $\overline{Z}$ não pode estar na lista. Para mostrar isso, estabeleceremos que para cada $k \in \mathbb{Z}^+$, $\overline{Z} \neq Z_k$.

Seja $k \in \mathbb{Z}^+$ arbitrário. Definimos $\overline{Z}$ de modo que para qualquer $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ sse $n \notin Z_n$. Em particular, tomando $n = k$, $k \in \overline{Z}$ sse $k \notin Z_k$. Mas isso mostra que $\overline{Z} \neq Z_k$, já que k é um membro de um mas não do outro, e assim $\overline{Z}$ e Z_k têm membros diferentes. Como k foi arbitrário, $\overline{Z}$ não está na lista Z_1, Z_2, ...

explanation

A prova precedente não mencionou uma diagonal, mas você pode pensar nela como envolvendo uma diagonal se a imaginar assim: imagine os conjuntos Z_1, Z_2, ..., escritos em uma matriz, onde cada membro $j \in Z_i$ é listado na j-ésima coluna. Digamos que os primeiros quatro conjuntos nessa lista são $\{1, 2, 3, \dots\}$, $\{2, 4, 6, \dots\}$, $\{1, 2, 5\}$ e $\{3, 4, 5, \dots\}$. Então a matriz começaria com

$$\begin{array}{lccccccc}
Z_1 = \{ & \mathbf{1}, & 2, & 3, & 4, & 5, & 6, & \dots\} \\
Z_2 = \{ & & \mathbf{2}, & & 4, & & 6, & \dots\} \\
Z_3 = \{ & 1, & 2, & & & 5 & & \} \\
Z_4 = \{ & & & 3, & \mathbf{4}, & 5, & 6, & \dots\} \\
\vdots & & & & & \ddots & &
\end{array}$$

Então $\overline{Z}$ é o conjunto obtido percorrendo a diagonal, deixando de fora quaisquer números que aparecem ao longo da diagonal e incluindo aqueles j onde a matriz tem uma lacuna na j-ésima linha/coluna. No caso acima, deixaríamos de fora 1 e 2, incluiríamos 3, deixaríamos de fora 4, etc.

Problema 4.17. Mostre que $\wp(\mathbb{N})$ é não enumerável por um argumento diagonal.

Problema 4.18. Mostre que o conjunto de funções $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ é não enumerável por um argumento diagonal explícito. Isto é, mostre que se f_1, f_2, ..., é uma lista de funções e cada $f_i\colon \mathbb{Z}^+ \to \mathbb{Z}^+$, então há alguma $\overline{f}\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ fora dessa lista.

4.7 Redução

sfr:siz:red:sec

Esta seção prova a não enumerabilidade por redução, correspondendo aos resultados na Seção 4.6. Uma versão alternativa, ligeiramente mais condensada, correspondente aos resultados na Seção 4.12, é fornecida na Seção 4.13.

Mostramos $\wp(\mathbb{Z}^+)$ como não enumerável por um argumento de diagonalização. Já tínhamos uma prova de que $\mathbb{B}^\omega$, o conjunto de todas as sequências infinitas de 0s e 1s, é não enumerável. Eis outra maneira de provar que $\wp(\mathbb{Z}^+)$ é não enumerável: mostre que *se* $\wp(\mathbb{Z}^+)$ *é enumerável, então* $\mathbb{B}^\omega$ *também é enumerável*. Como sabemos que $\mathbb{B}^\omega$ não é enumerável, $\wp(\mathbb{Z}^+)$ também não pode ser. Isso é chamado de *reduzir* um problema a outro—neste caso, reduzimos o problema de enumerar $\mathbb{B}^\omega$ ao problema de enumerar $\wp(\mathbb{Z}^+)$. Uma solução para o último—uma enumeração de $\wp(\mathbb{Z}^+)$—daria uma solução para o primeiro—uma enumeração de $\mathbb{B}^\omega$.

Como reduzimos o problema de enumerar um conjunto B ao de enumerar um conjunto A? Fornecemos uma maneira de transformar uma enumeração

de A em uma enumeração de B. A maneira mais fácil de fazer isso é definir uma função sobrejetiva $f\colon A \to B$. Se x_1, x_2, ... enumera A, então $f(x_1)$, $f(x_2)$, ... enumeraria B. Em nosso caso, procuramos uma função sobrejetora $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$.

Problema 4.19. Mostre que se há uma função injetiva $g\colon B \to A$, e B é não enumerável, então A também é. Faça isso mostrando como você pode usar g para transformar uma enumeração de A em uma de B.

Prova do Teorema 4.18 por redução. Suponha que $\wp(\mathbb{Z}^+)$ fosse enumerável, e portanto que há uma enumeração dele, Z_1, Z_2, Z_3, ...

Defina a função $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$ fazendo $f(Z)$ ser a sequência s_k tal que $s_k(n) = 1$ sse $n \in Z$, e $s_k(n) = 0$ caso contrário. Isso define claramente uma função, já que sempre que $Z \subseteq \mathbb{Z}^+$, qualquer $n \in \mathbb{Z}^+$ ou é um membro de Z ou não é. Por exemplo, o conjunto $2\mathbb{Z}^+ = \{2, 4, 6, \dots\}$ dos pares positivos é mapeado para a sequência $010101\dots$, o conjunto vazio é mapeado para $0000\dots$ e o conjunto $\mathbb{Z}^+$ para $1111\dots$.

Também é sobrejetiva: toda sequência de 0s e 1s corresponde a algum conjunto de inteiros positivos, nomeadamente aquele que tem como membros os inteiros correspondentes às posições onde a sequência tem 1s. Mais precisamente, suponha $s \in \mathbb{B}^\omega$. Defina $Z \subseteq \mathbb{Z}^+$ por:

$$Z = \{n \in \mathbb{Z}^+ : s(n) = 1\}$$

Então $f(Z) = s$, como pode ser verificado consultando a definição de f.

Agora considere a lista

$$f(Z_1), f(Z_2), f(Z_3), \dots$$

Como f é sobrejetiva, todo membro de $\mathbb{B}^\omega$ deve aparecer como valor de f para algum argumento, e assim deve aparecer na lista. Essa lista portanto deve enumerar todo $\mathbb{B}^\omega$.

Assim, se $\wp(\mathbb{Z}^+)$ fosse enumerável, $\mathbb{B}^\omega$ seria enumerável. Mas $\mathbb{B}^\omega$ é não enumerável (Teorema 4.17). Logo $\wp(\mathbb{Z}^+)$ é não enumerável. □

explanation

É fácil confundir a direção em que a redução vai. Por exemplo, uma função sobrejetiva $g\colon \mathbb{B}^\omega \to B$ *não* estabelece que B é não enumerável. (Considere $g\colon \mathbb{B}^\omega \to \mathbb{B}$ definida por $g(s) = s(1)$, a função que mapeia uma sequência de 0s e 1s para seu primeiro membro. Ela é sobrejetiva, porque algumas sequências começam com 0 e outras começam com 1. Mas $\mathbb{B}$ é finito.) Note também que a função f deve ser sobrejetiva, caso contrário o argumento não se sustenta: $f(x_1)$, $f(x_2)$, ... não estariam garantidos de incluir todos os membros de B. Por exemplo,

$$h(n) = \underbrace{000\dots0}_{n\text{ 0s}}$$

define uma função $h\colon \mathbb{Z}^+ \to \mathbb{B}^\omega$, mas $\mathbb{Z}^+$ é enumerável.

Problema 4.20. Mostre que o conjunto de todos os *conjuntos de* pares de inteiros positivos é não enumerável por um argumento de redução.

Problema 4.21. Mostre que o conjunto X de todas as funções $f : \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento de redução (Dica: dê uma função sobrejetora de X para $\mathbb{B}^\omega$.)

Problema 4.22. Mostre que $\mathbb{N}^\omega$, o conjunto de sequências infinitas de números naturais, é não enumerável por um argumento de redução.

Problema 4.23. Seja P o conjunto de funções do conjunto dos inteiros positivos para o conjunto $\{0\}$, e seja Q o conjunto de funções *parciais* do conjunto dos inteiros positivos para o conjunto $\{0\}$. Mostre que P é enumerável e Q não é. (Dica: reduza o problema de enumerar $\mathbb{B}^\omega$ a enumerar Q).

Problema 4.24. Seja S o conjunto de todas as funções sobrejetivas do conjunto dos inteiros positivos para o conjunto $\{0,1\}$, isto é, S consiste de todas as sobrejetivas $f : \mathbb{Z}^+ \to \mathbb{B}$. Mostre que S é não enumerável.

Problema 4.25. Mostre que o conjunto $\mathbb{R}$ de todos os números reais é não enumerável.

4.8 Equinumerosidade

sfr:siz:equ:sec

Temos uma noção intuitiva do "tamanho" dos conjuntos, que funciona bem para conjuntos finitos. E quanto aos infinitos? Se quisermos uma forma formal de comparar os tamanhos de dois conjuntos de *qualquer* cardinalidade, é boa ideia começar por definir quando dois conjuntos têm o mesmo tamanho. Eis Frege:

> Se um garçom quer ter certeza de que pôs exatamente tantas facas quantos pratos sobre a mesa, não precisa contar nem uns nem outros, se simplesmente puser uma faca à direita de cada prato, de modo que cada faca na mesa fique à direita de algum prato. Os pratos e as facas ficam assim correlacionados de modo único, e de fato por essa mesma relação espacial. (Frege, 1884, § 70)

A intuição central desta passagem traduz-se numa definição formal:

sfr:siz:equ:comparisondef

Definição 4.19. A é *equinumeroso* a B, escrevendo-se $A \approx B$, sse existir uma bijeção $f : A \to B$.

sfr:siz:equ:equinumerosityisequi

Proposição 4.20. *A relação de equinumerosidade é uma relação de equivalência.*

Prova. É preciso mostrar que a equinumerosidade é reflexiva, simétrica e transitiva. Sejam A, B e C conjuntos.

Reflexividade. A aplicação identidade $\mathrm{Id}_A \colon A \to A$, com $\mathrm{Id}_A(x) = x$ para todo $x \in A$, é uma bijeção. Logo $A \approx A$.

Simetria. Suponhamos $A \approx B$, isto é, que existe uma bijeção $f \colon A \to B$. Como f é bijetiva, a inversa f^{-1} existe e também é bijetiva. Logo $f^{-1} \colon B \to A$ é uma bijeção, pelo que $B \approx A$.

Transitividade. Suponhamos $A \approx B$ e $B \approx C$, isto é, que existem bijeções $f \colon A \to B$ e $g \colon B \to C$. Então a composição $g \circ f \colon A \to C$ é bijetiva, logo $A \approx C$. □

Proposição 4.21. *Se $A \approx B$, então A é enumerável se e só se B o é.*

A prova seguinte usa Definição 4.4 se Seção 4.2 estiver incluída e Definição 4.27 caso contrário.

Prova. Suponhamos $A \approx B$, logo existe alguma bijeção $f \colon A \to B$, e suponhamos que A é enumerável. Então ou $A = \emptyset$ ou existe uma função sobrejetiva $g \colon \mathbb{Z}^+ \to A$. Se $A = \emptyset$, então $B = \emptyset$ também (caso contrário existiria um membro $y \in B$ sem $x \in A$ com $g(x) = y$). Se, por outro lado, $g \colon \mathbb{Z}^+ \to A$ for sobrejetiva, então $f \circ g \colon \mathbb{Z}^+ \to B$ é sobrejetiva. De fato, seja $y \in B$. Como f é sobrejetiva, existe $x \in A$ tal que $f(x) = y$. Como g é sobrejetiva, existe $n \in \mathbb{Z}^+$ tal que $g(n) = x$. Logo,

$$(f \circ g)(n) = f(g(n)) = f(x) = y$$

e portanto $f \circ g$ é sobrejetiva. Temos que $f \circ g$ é uma enumeração de B, logo B é enumerável.

Se B é enumerável, obtemos que A é enumerável repetindo o argumento com a bijeção $f^{-1} \colon B \to A$ em lugar de f. □

Problema 4.26. Mostre que, se $A \approx C$ e $B \approx D$, e $A \cap B = C \cap D = \emptyset$, então $A \cup B \approx C \cup D$.

Problema 4.27. Mostre que, se A é infinito e enumerável, então $A \approx \mathbb{N}$.

4.9 Conjuntos de Tamanhos Diferentes e o Teorema de Cantor

sfr:siz:car:sec

Apresentamos uma formulação precisa da ideia de que dois conjuntos têm o mesmo tamanho. Também podemos precisar a ideia de que um conjunto é menor que outro. A nossa definição de "é menor do que (ou equinumeroso)" exigirá, em vez de uma bijeção entre os conjuntos, uma injeção do primeiro para o segundo. Se tal função existir, o tamanho do primeiro conjunto é menor

explanation

ou igual ao do segundo. Intuitivamente, uma injeção de um conjunto em outro garante que a imagem da função tem pelo menos tantos membros quanto o domínio, pois não há dois membros do domínio que vão parar ao mesmo membro da imagem.

Definição 4.22. *A não é maior do que B*, escrevendo-se $A \preceq B$, sse existir uma injeção $f\colon A \to B$.

É claro que isto é uma relação reflexiva e transitiva, mas não simétrica (fica como exercício). Podemos ainda introduzir uma noção que diz que um conjunto é (estritamente) menor que outro.

Definição 4.23. A é *menor do que B*, escrevendo-se $A \prec B$, sse existir uma injeção $f\colon A \to B$ mas não existir bijeção $g\colon A \to B$, isto é, $A \preceq B$ e $A \not\approx B$.

É claro que esta relação é irreflexiva e transitiva. (Também fica como exercício.) Com esta notação, um conjunto A é enumerável sse $A \preceq \mathbb{N}$, e A é não enumerável sse $\mathbb{N} \prec A$. Isto permite reformular o Teorema 4.32 como a observação de que $\mathbb{N} \prec \wp(\mathbb{N})$. De fato, Cantor (1892) provou que este último ponto é *completamente geral*:

Teorema 4.24 (Cantor). *$A \prec \wp(A)$, para qualquer conjunto A.*

sfr:siz:car:thm:cantor

Prova. A aplicação $f(x) = \{x\}$ é uma injeção $f\colon A \to \wp(A)$, pois se $x \neq y$, então também $\{x\} \neq \{y\}$ por extensionalidade, logo $f(x) \neq f(y)$. Temos pois $A \preceq \wp(A)$.

> Apresentamos a prova longa se Seção 4.6 estiver presente; caso contrário, uma prova mais curta alinhada com a Seção 4.12.

Mostraremos agora que não pode existir função sobrejetiva $g\colon A \to \wp(A)$, quanto mais bijetiva, e portanto que $A \not\approx \wp(A)$. Suponhamos que $g\colon A \to \wp(A)$. Como g é total, todo $x \in A$ é mapeado para um subconjunto $g(x) \subseteq A$. Podemos mostrar que g não pode ser sobrejetora. Para isso, definimos um subconjunto $\overline{A} \subseteq A$ que, por definição, não pode estar no contradomínio de g. Seja

$$\overline{A} = \{x \in A : x \notin g(x)\}.$$

Como $g(x)$ está definido para todo $x \in A$, $\overline{A}$ é claramente um subconjunto bem definido de A. Mas não pode estar no contradomínio de g. Seja $x \in A$ arbitrário; mostramos que $\overline{A} \neq g(x)$. Se $x \in g(x)$, então não satisfaz $x \notin g(x)$, logo, pela definição de $\overline{A}$, temos $x \notin \overline{A}$. Se $x \in \overline{A}$, tem de satisfazer a propriedade definidora de $\overline{A}$, isto é, $x \in A$ e $x \notin g(x)$. Como x era arbitrário, isto mostra que, para cada $x \in A$, $x \in g(x)$ sse $x \notin \overline{A}$, logo $g(x) \neq \overline{A}$. Em outras palavras, $\overline{A}$ não pode estar no contradomínio de g, o que contradiz a suposição de que g é sobrejetora. □

É instrutivo comparar a prova do Teorema 4.24 com a do Teorema 4.18. Ali mostramos que, para qualquer lista Z_1, Z_2, ..., de subconjuntos de $\mathbb{Z}^+$, se pode construir um conjunto $\overline{Z}$ de números garantidamente fora da lista. Estava garantido que não estava na lista porque, para todo $n \in \mathbb{Z}^+$, $n \in Z_n$ sse $n \notin \overline{Z}$. Assim, há sempre algum número que é um membro de um entre Z_n ou $\overline{Z}$ mas não do outro. Seguimos a mesma ideia aqui, exceto que os índices n são agora membros de A em vez de $\mathbb{Z}^+$. O conjunto $\overline{A}$ está definido de modo a diferir de $g(x)$ para cada $x \in A$, porque $x \in g(x)$ sse $x \notin \overline{A}$. De novo, há sempre um membro de A que é um membro de um entre $g(x)$ e $\overline{A}$ mas não do outro. E tal como $\overline{Z}$ portanto não pode estar na lista Z_1, Z_2, ..., $\overline{A}$ não pode estar no contradomínio de g. explanation

É instrutivo comparar a prova do Teorema 4.24 com a do Teorema 4.32. Ali mostramos que, para qualquer lista N_0, N_1, N_2, ..., de subconjuntos de $\mathbb{N}$, podemos construir um conjunto D de números garantidamente fora da lista. Estava garantido que não estava na lista porque $n \in N_n$ sse $n \notin D$, para todo $n \in \mathbb{N}$. Seguimos a mesma ideia aqui, exceto que os índices n são agora membros de A em vez de $\mathbb{N}$. O conjunto D está definido de modo a diferir de $g(x)$ para cada $x \in A$, porque $x \in g(x)$ sse $x \notin D$.

A prova vale também a pena comparar com a do Paradoxo de Russell, Teorema 1.29. De fato, o Teorema de Cantor foi a inspiração para o paradoxo de Russell.

Problema 4.28. Mostre que não pode existir uma injeção $g\colon \wp(A) \to A$, para qualquer conjunto A. Sugestão: suponha $g\colon \wp(A) \to A$ injetiva. Considere $D = \{g(B) : B \subseteq A \text{ e } g(B) \notin B\}$. Seja $x = g(D)$. Use o fato de g ser injetiva para obter uma contradição.

4.10 A Noção de Tamanho e Schröder-Bernstein

sfr:siz:sb:sec

Eis um pensamento intuitivo: se A não é maior do que B e B não é maior do que A, então A e B são equinumerosos. Sejamos honestos: se isto estivesse *errado*, dificilmente poderíamos justificar que a noção definida de equinumerosidade tem a ver com comparações de "tamanhos" entre conjuntos. Felizmente, o pensamento intuitivo está certo. Isto justifica-se pelo Teorema de Schröder-Bernstein. explanation

sfr:siz:sb:thm:schroder-bernstein

Teorema 4.25 (Schröder-Bernstein). *Se $A \preceq B$ e $B \preceq A$, então $A \approx B$.*

Em outras palavras, se existir uma injeção de A para B e uma injeção de B para A, então existe uma bijeção de A para B. explanation

Este resultado é, contudo, realmente bastante *difícil* de provar. De fato, embora Cantor o tivesse enunciado, outros provaram-no.[1] Por agora, pode (e deve) aceitá-lo como verdadeiro.

Felizmente, Schröder-Bernstein é *correto* e legitima pensarmos nas relações que definimos, isto é, $A \approx B$ e $A \preceq B$, como tendo a ver com "tamanho". Além

[1] Para mais sobre a história, ver por exemplo Potter (2004, pp. 165–6).

disso, Schröder-Bernstein é muito *útil*. Pode ser difícil imaginar uma bijeção entre dois conjuntos equinumerosos. O Teorema de Schröder-Bernstein permite decompor a comparação em casos em que só precisamos de uma injeção do primeiro para o segundo e vice-versa.

As seções Seção 4.11, Seção 4.12, Seção 4.13 são versões alternativas da Seção 4.2, Seção 4.6, Seção 4.7 de Tim Button para uso em seu texto Open Set Theory. São um pouco mais avançadas e usam uma definição diferente de enumerabilidade mais adequada em um contexto de teoria dos conjuntos (isto é, bijeção com $\mathbb{N}$ ou um segmento inicial, em vez de ser listável ou ser a imagem de uma função sobrejetora de $\mathbb{Z}^+$).

4.11 Enumerações e Conjuntos Enumeráveis

sfr:siz:enm-alt:sec

Esta seção define enumerações como bijeções com (segmentos iniciais) de $\mathbb{N}$, como se faz em teoria dos conjuntos. Por isso difere ligeiramente das definições em Seção 4.2 e repete os exemplos dessa seção. É também um pouco mais concisa.

Podemos especificar um conjunto finito simplesmente enumerando os seus membros. Fazemo-lo quando definimos um conjunto assim:

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Supondo que os membros $a_1, \ldots, a_n$ são todos distintos, obtemos uma bijeção entre A e os primeiros n números naturais $0, \ldots, n-1$. Reciprocamente, como todo o conjunto finito tem apenas finitos membros, todo o conjunto finito pode ser posto nessa correspondência. Em outras palavras, se A é finito, existe uma bijeção entre A e $\{0, \ldots, n-1\}$, onde n é o número de membros de A.

Se admitirmos certos tipos de conjuntos infinitos, admitiremos também que alguns conjuntos infinitos possam ser enumerados. Podemos precisar isto dizendo que um conjunto infinito é enumerado por uma bijeção entre ele e todo o $\mathbb{N}$.

Definição 4.26 (Enumeração, no sentido conjuntista). Uma *enumeração* de um conjunto A é uma bijeção cujo contradomínio é A e cujo domínio é ou um conjunto inicial de números naturais $\{0, 1, \ldots, n\}$ *ou* todo o conjunto dos números naturais $\mathbb{N}$.

explanation

Há uma base intuitiva para este uso da palavra *enumeração*. Dizer que enumeramos um conjunto A é dizer que existe uma bijeção f que nos permite *contar* os elementos do conjunto A. O elemento de índice 0 é $f(0)$, o de índice 1

é $f(1)$, ... o de índice n é $f(n)$....[2] O raciocínio fica ainda mais claro com o seguinte:

sfr:siz:enm-alt: defn:enumerable

Definição 4.27. Um conjunto A é enumerável se e só se $A = \emptyset$ ou existe uma enumeração de A. Dizemos que A é não enumerável se e só se A *não* é enumerável.

Logo um conjunto é enumerável se e só se é vazio ou se podemos usar uma enumeração para contar os seus membros. explanation

Exemplo 4.28. Uma função que enumera os números naturais é simplesmente a função identidade $\mathrm{Id}_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{N}$ dada por $\mathrm{Id}_{\mathbb{N}}(n) = n$. Uma função que enumera os números naturais *positivos*, $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, é a função $g(n) = n + 1$, isto é, a função sucessora.

Problema 4.29. Mostre que um conjunto A é enumerável se e só se $A = \emptyset$ ou existe uma sobrejeção $f \colon \mathbb{N} \to A$. Mostre que A é enumerável se e só se existe uma injeção $g \colon A \to \mathbb{N}$.

Exemplo 4.29. As funções $f \colon \mathbb{N} \to \mathbb{N}$ e $g \colon \mathbb{N} \to \mathbb{N}$ dadas por

$$f(n) = 2n \text{ e}$$
$$g(n) = 2n + 1$$

enumeram, respectivamente, os números naturais pares e os ímpares. Mas nenhuma é sobrejetiva, logo nenhuma é uma enumeração de $\mathbb{N}$.

Problema 4.30. Defina uma enumeração dos quadrados perfeitos 1, 4, 9, 16, ...

Exemplo 4.30. Seja $\lceil x \rceil$ a função *teto*, que arredonda x por excesso para o inteiro mais próximo. Então a função $f \colon \mathbb{N} \to \mathbb{Z}$ dada por:

$$f(n) = (-1)^n \left\lceil \tfrac{n}{2} \right\rceil$$

enumera o conjunto dos inteiros $\mathbb{Z}$ do seguinte modo:

$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	...
$\left\lceil \frac{0}{2} \right\rceil$	$-\left\lceil \frac{1}{2} \right\rceil$	$\left\lceil \frac{2}{2} \right\rceil$	$-\left\lceil \frac{3}{2} \right\rceil$	$\left\lceil \frac{4}{2} \right\rceil$	$-\left\lceil \frac{5}{2} \right\rceil$	$\left\lceil \frac{6}{2} \right\rceil$	...
0	-1	1	-2	2	-3	3	...

Repare como f gera os valores de $\mathbb{Z}$ "saltitando" entre inteiros positivos e negativos. Também se pode ver f definida por casos assim:

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

[2] Sim, contamos a partir de 0. Claro que também poderíamos começar em 1. Não faria grande diferença. Bastaria substituir $\mathbb{N}$ por $\mathbb{Z}^+$.

Problema 4.31. Mostre que se A e B são enumeráveis, então $A \cup B$ também é.

Problema 4.32. Mostre por indução em n que se A_1, A_2, ..., A_n são todos enumeráveis, então $A_1 \cup \cdots \cup A_n$ também é.

4.12 Conjuntos Não Enumeráveis

sfr:siz:nen-alt:sec

Esta seção prova a não enumerabilidade de $\mathbb{B}^\omega$ e de $\wp(\mathbb{N})$ usando as definições na Seção 4.11, isto é, exigindo uma bijeção com $\mathbb{N}$ em vez de uma sobrejeção a partir de $\mathbb{Z}^+$.

explanation

O conjunto $\mathbb{N}$ dos números naturais é infinito. Também é trivialmente enumerável. O fato notável, porém, é que existem conjuntos *não enumeráveis*, isto é, conjuntos que não são enumeráveis (ver Definição 4.27).

Isto pode surpreender. Afinal, dizer que A é não enumerável é dizer que *não* existe bijeção $f\colon \mathbb{N} \to A$; isto é, nenhuma função que mapeie os infinitos membros de $\mathbb{N}$ para A esgota todo A. Logo, se A é não enumerável, há "mais" membros em A do que números naturais.

Para provar que um conjunto é não enumerável, é preciso mostrar que não pode existir uma bijeção adequada. A melhor forma é mostrar que qualquer tentativa de enumerar membros de A tem de deixar pelo menos um membro de fora; isto mostra que nenhuma função $f\colon \mathbb{N} \to A$ é sobrejetiva. Uma estratégia geral para o estabelecer é usar o *método diagonal* de Cantor. Dada uma lista de membros de A, digamos x_1, x_2, ..., construímos outro membro de A que, pela sua construção, não pode estar nessa lista.

Tudo isto compreende-se melhor com um exemplo. O nosso primeiro exemplo é o conjunto $\mathbb{B}^\omega$ de todas as cadeias infinitas de 0s e 1s. (O símbolo '$\mathbb{B}$' significa binário, e podemos pensar nele como o conjunto de dois elementos $\{0, 1\}$.)

Teorema 4.31. *$\mathbb{B}^\omega$ é não enumerável.*

sfr:siz:nen-alt:thm:nonenum-bin-omega

Prova. Considere-se qualquer enumeração de um subconjunto de $\mathbb{B}^\omega$. Temos então uma lista s_0, s_1, s_2, ... em que cada s_n é uma cadeia infinita de 0s e 1s. Seja $s_n(m)$ o m-ésimo dígito da cadeia s_n. Podemos pois pensar na lista como uma matriz, colocando $s_n(m)$ na n-ésima linha e m-ésima coluna:

	0	1	2	3	...
0	$\mathbf{s_0(0)}$	$s_0(1)$	$s_0(2)$	$s_0(3)$	...
1	$s_1(0)$	$\mathbf{s_1(1)}$	$s_1(2)$	$s_1(3)$	...
2	$s_2(0)$	$s_2(1)$	$\mathbf{s_2(2)}$	$s_2(3)$	...
3	$s_3(0)$	$s_3(1)$	$s_3(2)$	$\mathbf{s_3(3)}$	...
⋮	⋮	⋮	⋮	⋮	⋱

Construiremos agora uma cadeia infinita, d, de 0s e 1s que não está nesta lista, especificando cada uma das suas entradas, isto é, $d(n)$ para todo $n \in \mathbb{N}$. Intuitivamente, lemos a diagonal da matriz acima (daí o nome "método diagonal") e trocamos cada 0 por 1 e cada 1 por 0. De modo mais abstrato, definimos $d(n)$ como 0 ou 1 consoante o n-ésimo membro da diagonal, $s_n(n)$, seja 1 ou 0, isto é:

$$d(n) = \begin{cases} 1 & \text{se } s_n(n) = 0 \\ 0 & \text{se } s_n(n) = 1 \end{cases}$$

Claramente $d \in \mathbb{B}^\omega$, pois é uma cadeia infinita de 0s e 1s. Mas construímos d de modo que $d(n) \neq s_n(n)$ para qualquer $n \in \mathbb{N}$, isto é, d difere de s_n na sua n-ésima entrada. Logo $d \neq s_n$ para qualquer $n \in \mathbb{N}$, pelo que d não pode estar na lista s_0, s_1, s_2, ...

Mostramos assim que, dada uma enumeração arbitrária de algum subconjunto de $\mathbb{B}^\omega$, ela omite algum membro de $\mathbb{B}^\omega$. Logo não existe enumeração do conjunto $\mathbb{B}^\omega$, isto é, $\mathbb{B}^\omega$ é não enumerável. □

Este método de prova chama-se "diagonalização" porque usa a diagonal da matriz para definir d. Contudo, a diagonalização não exige necessariamente uma matriz. De fato, podemos mostrar que um conjunto é não enumerável por uma ideia semelhante mesmo quando não há matriz nem diagonal literal. O resultado seguinte ilustra como. explanation

sfr:siz:nen-alt: thm:nonenum-pownat

Teorema 4.32. *$\wp(\mathbb{N})$ não é enumerável.*

Prova. Procedemos da mesma forma, mostrando que qualquer lista de subconjuntos de $\mathbb{N}$ omite algum subconjunto de $\mathbb{N}$. Suponhamos, pois, que temos uma lista $N_0, N_1, N_2, \ldots$ de subconjuntos de $\mathbb{N}$. Definimos um conjunto D assim: $n \in D$ sse $n \notin N_n$:

$$D = \{n \in \mathbb{N} : n \notin N_n\}$$

Claramente $D \subseteq \mathbb{N}$. Mas D não pode estar na lista: por construção, $n \in D$ sse $n \notin N_n$, logo $D \neq N_n$ para qualquer $n \in \mathbb{N}$. □

A prova precedente não mencionou uma diagonal. Ainda assim, pode pensar-se nela como envolvendo uma diagonal, imaginando os conjuntos N_0, N_1, ... dispostos numa matriz em que escrevemos N_n na n-ésima linha colocando m na m-ésima coluna sse $m \in N_n$. Por exemplo, se os primeiros quatro conjuntos da lista são $\{0, 1, 2, \ldots\}$, $\{1, 3, 5, \ldots\}$, $\{0, 1, 4\}$ e $\{2, 3, 4, \ldots\}$, a matriz começaria com explanation

$$\begin{array}{lccccccc}
N_0 = \{ & \mathbf{0}, & 1, & 2, & & & & \ldots\} \\
N_1 = \{ & & \mathbf{1}, & & 3, & & 5, & \ldots\} \\
N_2 = \{ & 0, & 1, & & & 4 & & \} \\
N_3 = \{ & & & 2, & \mathbf{3}, & 4, & & \ldots\} \\
\vdots & & & & & & & \ddots
\end{array}$$

Então D é o conjunto obtido percorrendo a diagonal, pondo $n \in D$ sse n *não* está na diagonal. No caso acima, excluiríamos 0 e 1, incluiríamos 2, excluiríamos 3, etc.

Problema 4.33. Mostre que o conjunto de todas as funções $f\colon \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento diagonal explícito. Isto é, mostre que, se f_1, f_2, ... é uma lista de funções e cada $f_i\colon \mathbb{N} \to \mathbb{N}$, então existe alguma $g\colon \mathbb{N} \to \mathbb{N}$ que não está nesta lista.

4.13 Redução

sfr:siz:red-alt:sec

Esta seção prova a não enumerabilidade por redução, alinhada com os resultados na Seção 4.12. Uma versão alternativa, ligeiramente mais elaborada, alinhada com os resultados na Seção 4.6, encontra-se na Seção 4.7.

Provamos que $\mathbb{B}^\omega$ é não enumerável por um argumento de diagonalização. Usamos um argumento semelhante para mostrar que $\wp(\mathbb{N})$ é não enumerável. Há outra forma de provar que $\wp(\mathbb{N})$ é não enumerável: mostrar que *se* $\wp(\mathbb{N})$ *é enumerável então* $\mathbb{B}^\omega$ *também é enumerável*. Como sabemos que $\mathbb{B}^\omega$ é não enumerável, segue que $\wp(\mathbb{N})$ também o é.

Isto chama-se *reduzir* um problema a outro. Neste caso, reduzimos o problema de enumerar $\mathbb{B}^\omega$ ao problema de enumerar $\wp(\mathbb{N})$. Uma solução para este último—uma enumeração de $\wp(\mathbb{N})$—daria uma solução para o primeiro—uma enumeração de $\mathbb{B}^\omega$.

Para reduzir o problema de enumerar um conjunto B ao de enumerar um conjunto A, indicamos uma forma de transformar uma enumeração de A numa enumeração de B. A forma mais simples é definir uma sobrejeção $f\colon A \to B$. Se $x_1, x_2, \ldots$ enumeram A, então $f(x_1), f(x_2), \ldots$ enumerariam B. No nosso caso, procuramos uma sobrejeção $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$.

Problema 4.34. Mostre que, se existir uma função injetiva $g\colon B \to A$, e B for não enumerável, então A também o é. Faça-o mostrando como pode usar g para transformar uma enumeração de A numa de B.

Prova do Teorema 4.32 por redução. Para a redução, suponhamos que $\wp(\mathbb{N})$ é enumerável e portanto que existe uma enumeração $N_1, N_2, N_3, \ldots$

Definimos a função $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$ pondo $f(N)$ igual à cadeia s_k tal que $s_k(n) = 1$ sse $n \in N$, e $s_k(n) = 0$ caso contrário.

Isto define claramente uma função, pois sempre que $N \subseteq \mathbb{N}$, qualquer $n \in \mathbb{N}$ ou é um membro de N ou não é. Por exemplo, o conjunto $2\mathbb{N} = \{2n : n \in \mathbb{N}\} = \{0, 2, 4, 6, \ldots\}$ dos naturais pares é mapeado para a cadeia $1010101\ldots$; $\emptyset$ é mapeado para $0000\ldots$; $\mathbb{N}$ é mapeado para $1111\ldots$.

Também é sobrejetiva: toda a cadeia de 0s e 1s corresponde a algum conjunto de números naturais, nomeadamente aquele que tem como membros os naturais nas posições em que a cadeia tem um 1. Com mais precisão, se $s \in \mathbb{B}^\omega$, defina-se $N \subseteq \mathbb{N}$ por:

$$N = \{n \in \mathbb{N} : s(n) = 1\}$$

Então $f(N) = s$, como se verifica consultando a definição de f.

Consideremos agora a lista

$$f(N_1), f(N_2), f(N_3), \ldots$$

Como f é sobrejetiva, todo o membro de $\mathbb{B}^\omega$ tem de aparecer como valor de f para algum argumento, e portanto na lista. Esta lista teria de enumerar todo $\mathbb{B}^\omega$.

Logo, se $\wp(\mathbb{N})$ fosse enumerável, $\mathbb{B}^\omega$ seria enumerável. Mas $\mathbb{B}^\omega$ é não enumerável (Teorema 4.31). Logo $\wp(\mathbb{N})$ é não enumerável. □

Problema 4.35. Mostre que o conjunto X de todas as funções $f : \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento de redução (Sugestão: dê uma função sobrejetora de X para $\mathbb{B}^\omega$.)

Problema 4.36. Mostre que o conjunto de todos os *conjuntos de* pares de números naturais, isto é, $\wp(\mathbb{N} \times \mathbb{N})$, é não enumerável por um argumento de redução.

Problema 4.37. Mostre que $\mathbb{N}^\omega$, o conjunto das sequências infinitas de números naturais, é não enumerável por um argumento de redução.

Problema 4.38. Seja S o conjunto de todas as sobrejeções de $\mathbb{N}$ para o conjunto $\{0, 1\}$, isto é, S consiste em todas as sobrejeções $f : \mathbb{N} \to \mathbb{B}$. Mostre que S é não enumerável.

Problema 4.39. Mostre que o conjunto $\mathbb{R}$ de todos os números reais é não enumerável.

Capítulo 5

Aritmetização

O material deste capítulo apresenta a construção dos sistemas numéricos na teoria ingênua dos conjuntos. É retirado do texto *Open Set Theory* de Tim Button.

5.1 De $\mathbb{N}$ para $\mathbb{Z}$

sfr:arith:int:sec

Eis duas constatações básicas (no sentido de "ideias que retemos"):

1. Todo inteiro pode escrever-se na forma $n - m$, com $n, m \in \mathbb{N}$.
2. A informação codificada numa expressão $n-m$ pode igualmente codificar-se por um par ordenado $\langle n, m\rangle$.

Já sabemos que os pares ordenados de números naturais são os membros de $\mathbb{N}^2$; estamos a assumir, também, que compreendemos $\mathbb{N}$. Eis uma sugestão ingênua, fundada nestas duas constatações: *tratar os inteiros como pares ordenados de números naturais.*

De fato, esta sugestão é demasiado ingênua. Obviamente, queremos que seja verdade que $0 - 2 = 4 - 6$. Mas, evidentemente, $\langle 0, 2\rangle \neq \langle 4, 6\rangle$. Logo, não podemos simplesmente dizer que $\mathbb{N}^2$ é o conjunto dos inteiros.

Generalizando a partir do problema precedente, o que queremos é o seguinte:

$$a - b = c - d \text{ sse } a + d = c + b$$

(Deve ser óbvio que assim é que os inteiros *devem* comportar-se: basta somar b e d a ambos os lados.) A forma fácil de garantir este comportamento é definir uma relação de equivalência entre pares ordenados, $\sim$, do seguinte modo:

$$\langle a, b\rangle \sim \langle c, d\rangle \text{ sse } a + d = c + b$$

Resta-nos mostrar que isto é uma relação de equivalência.

Proposição 5.1. *$\sim$ é uma relação de equivalência.*

Prova. Há que mostrar que $\sim$ é reflexiva, simétrica e transitiva.

Reflexividade: Evidentemente $\langle a, b\rangle \sim \langle a, b\rangle$, pois $a + b = b + a$.

Simetria: Suponhamos $\langle a, b\rangle \sim \langle c, d\rangle$, logo $a+d = c+b$. Então $c+b = a+d$, pelo que $\langle c, d\rangle \sim \langle a, b\rangle$.

Transitividade: Suponhamos $\langle a, b\rangle \sim \langle c, d\rangle \sim \langle m, n\rangle$. Logo, $a + d = c + b$ e $c + n = m + d$. Assim, $a + d + c + n = c + b + m + d$, e portanto $a + n = m + b$. Logo, $\langle a, b\rangle \sim \langle m, n\rangle$. □

Podemos agora usar esta relação de equivalência para formar classes de equivalência:

Definição 5.2. Os inteiros são as classes de equivalência, sob $\sim$, dos pares ordenados de números naturais; isto é, $\mathbb{Z} = \mathbb{N}^2/_\sim$.

Agora, podem surgir várias reações *filosóficas* distintas face a esta definição estipulativa. Antes de as considerarmos, porém, vale a pena continuar com alguns pormenores técnicos.

Tendo dito o que são os inteiros, precisamos de definir funções e relações básicas sobre eles. Escrevamos $[m, n]_\sim$ para a classe de equivalência sob $\sim$ que tem $\langle m, n\rangle$ como um membro.[1] Isto é:

$$[m, n]_\sim = \{\langle a, b\rangle \in \mathbb{N}^2 : \langle a, b\rangle \sim \langle m, n\rangle\}$$

Apresentamos, pois, algumas definições:

$$\begin{aligned}
[a, b]_\sim + [c, d]_\sim &= [a + c, b + d]_\sim \\
[a, b]_\sim \times [c, d]_\sim &= [ac + bd, ad + bc]_\sim \\
[a, b]_\sim \leq [c, d]_\sim &\text{ sse } a + d \leq b + c
\end{aligned}$$

(Como é habitual, uso 'ab' no sentido de '$(a \times b)$', só para tornar os axiomas mais legíveis.) Há, ainda, que garantir que estas definições se comportam como *devem*. Explicitar o que isto significa, e verificá-lo, é trabalhoso; relegamos os pormenores a Seção 5.6. Em resumo, contudo: tudo funciona!

Resta um último ponto. Construímos os inteiros a partir dos números naturais. Isto significa que os naturais *não são, eles próprios, inteiros*. Voltaremos ao significado filosófico disto na Seção 5.5. Do ponto de vista puramente técnico, porém, precisamos de alguma forma de tratar números naturais *como* inteiros. A ideia é simples: para cada $n \in \mathbb{N}$, estipulamos $n_\mathbb{Z} = [n, 0]_\sim$. Há que confirmar que esta definição é bem comportada, isto é, que para quaisquer $m, n \in \mathbb{N}$

$$\begin{aligned}
(m + n)_\mathbb{Z} &= m_\mathbb{Z} + n_\mathbb{Z} \\
(m \times n)_\mathbb{Z} &= m_\mathbb{Z} \times n_\mathbb{Z} \\
m \leq n &\leftrightarrow m_\mathbb{Z} \leq n_\mathbb{Z}
\end{aligned}$$

[1] Nota: com a notação introduzida na Definição 2.11, escreveríamos $[\langle m, n\rangle]_\sim$ para o mesmo objeto; isso, porém, torna a leitura um pouco mais difícil.

Mas isto é bastante direto. Por exemplo, para mostrar que a segunda condição se verifica, podemos apoiar-nos no comportamento dos naturais e raciocinar assim:

$$\begin{aligned}(m \times n)_{\mathbb{Z}} &= [m \times n, 0]_{\sim} \\ &= [m \times n + 0 \times 0, m \times 0 + 0 \times n]_{\sim} \\ &= [m, 0]_{\sim} \times [n, 0]_{\sim} \\ &= m_{\mathbb{Z}} \times n_{\mathbb{Z}}\end{aligned}$$

Deixamos como exercício confirmar que as outras duas condições se verificam.

Problema 5.1. Mostre que $(m + n)_{\mathbb{Z}} = m_{\mathbb{Z}} + n_{\mathbb{Z}}$ e $m \leq n \leftrightarrow m_{\mathbb{Z}} \leq n_{\mathbb{Z}}$, para quaisquer $m, n \in \mathbb{N}$.

5.2 De $\mathbb{Z}$ para $\mathbb{Q}$

sfr:arith:rat:sec

Acabamos de ver como construir os inteiros a partir dos naturais, usando alguma teoria ingênua dos conjuntos. Veremos agora como construir os racionais a partir dos inteiros, de modo muito semelhante. As constatações iniciais são:

1. Todo racional pode escrever-se na forma $^{i}/_{j}$, onde i e j são inteiros, mas j é diferente de zero.

2. A informação codificada numa expressão $^{i}/_{j}$ pode igualmente codificar-se num par ordenado $\langle i, j\rangle$.

A abordagem óbvia seria pensar nos racionais *como* pares ordenados de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$. Como antes, porém, isso seria um pouco demasiado ingênuo, pois queremos $^{3}/_{2} = {}^{6}/_{4}$, mas $\langle 3, 2\rangle \neq \langle 6, 4\rangle$. Mais geralmente, quereremos o seguinte:

$$^{a}/_{b} = {}^{c}/_{d} \text{ sse } a \times d = b \times c$$

Para obter isto, definimos uma *relação de equivalência* em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$ assim:

$$\langle a, b\rangle \backsim \langle c, d\rangle \text{ sse } a \times d = b \times c$$

Há que verificar que isto é uma relação de equivalência. É muito parecido com o caso de $\sim$, e deixamo-lo como exercício.

Problema 5.2. Mostre que $\backsim$ é uma relação de equivalência.

Mas isto permite-nos dizer o seguinte:

Definição 5.3. Os racionais são as classes de equivalência, sob $\backsim$, dos pares de inteiros (cujo segundo elemento é não nulo). Isto é, $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\}))/_{\backsim}$.

Tal como para os inteiros, queremos também definir algumas operações básicas. Sendo $[i,j]_\backsim$ a classe de equivalência sob $\backsim$ com $\langle i,j\rangle$ como um membro, definimos:

$$[a,b]_\backsim + [c,d]_\backsim = [ad+bc, bd]_\backsim$$
$$[a,b]_\backsim \times [c,d]_\backsim = [ac, bd]_\backsim.$$

Para definir $r \leq s$ nestes racionais, usamos o fato de que $r \leq s$ sse $s - r$ não é negativo, isto é, $r - s$ pode escrever-se como $^i/_j$ com i não negativo e j positivo:

$$[a,b]_\backsim \leq [c,d]_\backsim \text{ sse } [c,d]_\backsim - [a,b]_\backsim = [i_\mathbb{Z}, j_\mathbb{Z}]_\backsim$$

para algum $i \in \mathbb{N}$ e $0 \neq j \in \mathbb{N}$.

Depois há que verificar que estas definições se comportam como *devem*; relegamo-lo a Seção 5.6. Mas de fato comportam-se bem! Por fim, queremos alguma forma de tratar inteiros *como* racionais; logo, para cada $i \in \mathbb{Z}$, estipulamos $i_\mathbb{Q} = [i, 1_\mathbb{Z}]_\backsim$. De novo, verificamos na Seção 5.6 que tudo isto se comporta corretamente.

Problema 5.3. Mostre que $(i+j)_\mathbb{Q} = i_\mathbb{Q} + j_\mathbb{Q}$ e $(i \times j)_\mathbb{Q} = i_\mathbb{Q} \times j_\mathbb{Q}$ e $i \leq j \leftrightarrow i_\mathbb{Q} \leq j_\mathbb{Q}$, para quaisquer $i, j \in \mathbb{Z}$.

5.3 A Reta Real

sfr:arith:real:sec

O passo seguinte é mostrar como construir os reais a partir dos racionais. Antes disso, há que perceber o que há de *distintivo* nos reais.

Os reais comportam-se de modo muito parecido com os racionais. (Tecnicamente, ambos são exemplos de *corpos ordenados*; para a definição, ver Definição 5.9.) Agora, se resolveu os exercícios de Capítulo 4, saberá que há estritamente mais reais do que racionais, isto é, que $\mathbb{Q} \prec \mathbb{R}$. Cantor foi o primeiro a provar isto. Há, contudo, cerca de dois milênios e meio que se conhecem números irracionais, isto é, reais que não são racionais. De fato:

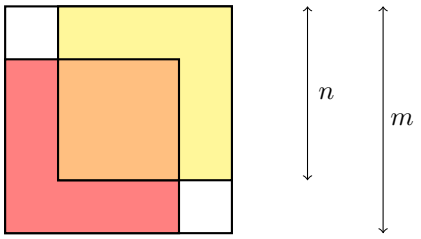
sfr:arith:real:root2irrational

Teorema 5.4. *$\sqrt{2}$ não é racional, isto é, $\sqrt{2} \notin \mathbb{Q}$*

Prova. Suponhamos, por *reductio*, que $\sqrt{2}$ é racional. Então $\sqrt{2} = {}^m/_n$ para alguns números naturais m e n. De fato, podemos escolher m e n de modo a que a fração não possa ser mais reduzida. Reorganizando, $m^2 = 2n^2$. A partir daqui, completamos a prova de duas formas:

Primeiro, geometricamente (seguindo Tennenbaum).[2] Consideremos estes quadrados:

[2] Esta prova é relatada por Conway (2006).



□

Como $m^2 = 2n^2$, a região em que os dois quadrados de lado n se sobrepõem tem a mesma área que a região que nenhum dos dois quadrados cobre; isto é, a área do quadrado cor de laranja é igual à soma das áreas dos dois quadrados não sombreados. Logo, se o quadrado cor de laranja tem lado p e cada quadrado não sombreado tem lado q, então $p^2 = 2q^2$. Mas então $\sqrt{2} = {}^{p}/_{q}$, com $p < m$, $q < n$ e $p, q \in \mathbb{N}$. Isto contradiz o fato de m e n terem sido escolhidos tão pequenos quanto possível.

Segundo, formalmente. Como $m^2 = 2n^2$, segue-se que m é par. (É fácil mostrar que, se x é ímpar, então x^2 é ímpar.) Logo $m = 2r$, para algum $r \in \mathbb{N}$. Rearranjando, $2r^2 = n^2$, logo n também é par. Assim m e n são ambos pares, e portanto a fração ${}^{m}/_{n}$ *pode* ser ainda reduzida. Contradição!

De passagem, esta prova diagramática permite relembrar o material de **??**. Tennenbaum (1927–2006) era um matemático inequivocamente moderno; mas a prova é inegavelmente bela, completamente rigorosa e apela à intuição geométrica!

Em todo o caso: os reais são "mais extensos" do que os racionais. Nalgum sentido, há "lacunas" nos racionais, e os reais preenchem-nas. Weierstrass apercebeu-se de que isto descreve uma única propriedade dos números reais que os distingue dos racionais, nomeadamente a *propriedade de completude*: *Todo conjunto não vazio de números reais com majorante tem um supremo (menor majorante).*

É fácil ver que os racionais não têm a propriedade de completude. Por exemplo, considere-se o conjunto dos racionais menores que $\sqrt{2}$, isto é:

$$\{p \in \mathbb{Q} : p^2 < 2 \text{ ou } p < 0\}$$

Este conjunto tem um majorante nos racionais; os seus membros são todos menores que 3, por exemplo. Mas qual é o seu supremo? Queremos dizer "$\sqrt{2}$"; contudo, acabamos de ver que $\sqrt{2}$ *não* é racional. E não existe racional mínimo entre os que são estritamente maiores que $\sqrt{2}$. Logo, o conjunto tem majorante, mas não tem supremo. Assim, os racionais não satisfazem a propriedade de completude.

Em contraste, o contínuo "moralmente deveria" ter a propriedade de completude. Não queremos apenas que $\sqrt{2}$ seja um número real; queremos preencher todas as "lacunas" da reta racional. Queremos, ainda, que o próprio contínuo não tenha "lacunas". É exatamente isso que obteremos via completude.

5.4 De $\mathbb{Q}$ para $\mathbb{R}$

sfr:arith:cuts:sec

Em essência, a propriedade de completude mostra que qualquer ponto α da reta real divide essa reta em duas metades de modo perfeito: numa, α é o supremo; noutra, α é o ínfimo. Para *construir* os números reais a partir dos racionais, Dedekind sugeriu que pensássemos nos reais simplesmente como os *cortes* que particionam os racionais. Isto é, identificamos $\sqrt{2}$ com o *corte* que separa os racionais $< \sqrt{2}$ dos racionais $> \sqrt{2}$.

Vamos pôr isto em ordem. Se cortarmos os racionais em duas metades, podemos identificar de modo único a partição que fizemos considerando apenas a metade *inferior*. Sendo precisos, apresentamos a seguinte definição:

Definição 5.5 (Corte). Um *corte* α é qualquer segmento inicial próprio não vazio dos racionais sem máximo. Isto é, α é um corte sse:

1. *não vazio, próprio*: $\emptyset \neq \alpha \subsetneq \mathbb{Q}$
2. *inicial*: para todos $p, q \in \mathbb{Q}$: se $p < q \in \alpha$ então $p \in \alpha$
3. *sem máximo*: para todo $p \in \alpha$ existe $q \in \alpha$ tal que $p < q$

Então $\mathbb{R}$ é o conjunto dos cortes.

Podemos pois dizer que $\sqrt{2} = \{p \in \mathbb{Q} : p^2 < 2 \text{ ou } p < 0\}$. Claro que há que verificar que isto *é* de fato um corte, mas relegamo-lo a Seção 5.6.

Como antes, tendo definido certas entidades, precisamos a seguir de definir funções e relações básicas sobre elas. Começamos por uma fácil:

$$\alpha \leq \beta \text{ sse } \alpha \subseteq \beta$$

Esta definição de ordem permite *enunciar* o resultado central, a saber que o conjunto dos cortes tem a propriedade de completude. Por extenso, o enunciado tem esta forma. Se S é um conjunto não vazio de cortes com majorante, então S tem supremo. Com mais pormenor: existe um corte, λ, que é majorante de S, isto é, $(\forall \alpha \in S)\alpha \subseteq \lambda$, e λ é o menor tal corte, isto é, $(\forall \beta \in \mathbb{R})((\forall \alpha \in S)\alpha \subseteq \beta \to \lambda \subseteq \beta)$. Segue-se a prova do resultado:

sfr:arith:cuts:realcompleteness

Teorema 5.6. *O conjunto dos cortes tem a propriedade de completude.*

Prova. Seja S um conjunto não vazio de cortes com majorante. Seja $\lambda = \bigcup S$. Começamos por alegar que λ é um corte:

1. Como S tem majorante, pelo menos um corte pertence a S, logo $\emptyset \neq \lambda$. Como S é um conjunto de cortes, $\lambda \subseteq \mathbb{Q}$. Como S tem majorante, algum $p \in \mathbb{Q}$ está ausente de todo o corte $\alpha \in S$. Logo $p \notin \lambda$, e portanto $\lambda \subsetneq \mathbb{Q}$.
2. Suponhamos $p < q \in \lambda$. Então existe algum $\alpha \in S$ tal que $q \in \alpha$. Como α é um corte, $p \in \alpha$. Logo $p \in \lambda$.

3. Suponhamos $p \in \lambda$. Então existe algum $\alpha \in S$ tal que $p \in \alpha$. Como α é um corte, existe algum $q \in \alpha$ tal que $p < q$. Logo $q \in \lambda$.

Isto prova a alegação. Além disso, claramente $(\forall \alpha \in S)\alpha \subseteq \bigcup S = \lambda$, isto é, λ é majorante de S. Suponhamos agora que $\beta \in \mathbb{R}$ também é majorante, isto é, $(\forall \alpha \in S)\alpha \subseteq \beta$. Para qualquer $p \in \mathbb{Q}$, se $p \in \lambda$, então existe $\alpha \in S$ tal que $p \in \alpha$, logo $p \in \beta$. Generalizando, $\lambda \subseteq \beta$. Logo λ é o supremo de S. □

Temos pois um conjunto de entidades que satisfaz a propriedade de completude. Uma forma de o dizer é: não há "lacunas" nos nossos cortes. (Assim: tomar novos "cortes" de reais, em vez de racionais, não produziria objetos novos interessantes.)

Segue-se a definição de algumas operações sobre os reais. Começamos por embutir os racionais nos reais estipulando $p_{\mathbb{R}} = \{q \in \mathbb{Q} : q < p\}$ para cada $p \in \mathbb{Q}$. Definimos então:

$$\begin{aligned} \alpha + \beta &= \{p + q : p \in \alpha \wedge q \in \beta\} \\ \alpha \times \beta &= \{p \times q : 0 \leq p \in \alpha \wedge 0 \leq q \in \beta\} \cup 0^{\mathbb{R}} \qquad \text{se } \alpha, \beta \geq 0_{\mathbb{R}} \end{aligned}$$

Para tratar os outros casos da multiplicação, definamos primeiro:

$$-\alpha = \{p - q : p < 0 \wedge q \notin \alpha\}$$

e estipulemos:

$$\alpha \times \beta = \begin{cases} -\alpha \times -\beta & \text{se } \alpha < 0_{\mathbb{R}} \text{ e } \beta < 0_{\mathbb{R}} \\ -(-\alpha \times \beta) & \text{se } \alpha < 0_{\mathbb{R}} \text{ e } \beta > 0_{\mathbb{R}} \\ -(\alpha \times -\beta) & \text{se } \alpha > 0_{\mathbb{R}} \text{ e } \beta < 0_{\mathbb{R}} \end{cases}$$

Depois há que verificar que cada uma destas definições produz sempre um corte. E, por fim, há que fazer uma demonstração fácil (mas longa) de que os cortes, assim definidos, se comportam exatamente como devem. Mas relegamos tudo isto a Seção 5.6.

5.5 Algumas Reflexões Filosóficas

Quanto aos pormenores técnicos, por ora basta. Mas o que foi que alcançaram? sfr:arith:ref:sec

Bem, de forma pouco contestável, deram-nos uma matemática pura *belíssima*. Além disso, houve conquistas conceptuais profundas. Foi um insight profundo perceber que a propriedade de completude exprime a diferença crucial entre os reais e os racionais. Além disso, a construção explícita dos reais, como cortes de Dedekind, põe o objeto de estudo da análise em bases sólidas. Sabemos que a noção de *corpo ordenado completo* é coerente, pois os cortes formam precisamente um tal corpo.

Todavia, importa também levantar algumas reservas quanto a essas conquistas.

Primeiro, não é claro que pensar os reais em termos de cortes seja *mais* rigoroso do que pensá-los nas suas expansões decimais familiares (eventualmente infinitas). Esta última "construção" dos reais tem alguma semelhança com a construção via sequências de Cauchy; mas, de fato, era, essencialmente, conhecida dos matemáticos desde princípios do século XVII (ver Seção 5.7). O verdadeiro aumento de rigor veio da tomada de consciência de que os reais têm a propriedade de completude; a possibilidade de construir números reais como conjuntos particulares talvez não seja, por si só, tão interessante.

É ainda menos claro que a aritmetização (muito mais fácil) dos inteiros ou dos racionais aumente o rigor nessas áreas. Aqui, vale a pena uma observação simples. Tendo *construído* os inteiros como classes de equivalência de pares ordenados de naturais, e depois construído os racionais como classes de equivalência de pares ordenados de inteiros, e depois construído os reais como conjuntos de racionais, *nos esquecemos de imediato* das construções. Em particular: ninguém quereria *invocar* estas construções no decurso de uma prova matemática (exceto, claro, numa prova de que as construções se comportam como deviam). É muito mais fácil falar de um real diretamente do que falar de algum conjunto de conjuntos de conjuntos de conjuntos de conjuntos de conjuntos de conjuntos de naturais.

O mais duvidoso, porém, é que estas definições nos digam o que os inteiros, racionais ou reais *são*, *do ponto de vista metafísico*. Isto é, é duvidoso que os reais (digamos) *sejam* certos conjuntos (de conjuntos de conjuntos...). A principal barreira a tal visão é que a construção poderia ter sido feita de muitas maneiras diferentes. No caso dos reais, há construções genuinamente diferentes e interessantes (ver Seção 5.7). Mas eis uma forma trivial de obter construções diferentes: como em Seção 2.2, poderíamos ter definido pares ordenados de modo ligeiramente diferente; se tivéssemos usado essa noção alternativa de par ordenado, as nossas construções teriam funcionado exatamente tão bem como funcionaram, mas teríamos acabado com objetos diferentes. Assim, há muitas construções rivais, em teoria dos conjuntos, dos inteiros, racionais e reais. Seria, ademais, arbitrário (e embaraçoso) afirmar que os inteiros (digamos) são *estes* conjuntos, e não *aqueles*. (Como na Seção 2.2, isto é um caso de um argumento tornado célebre por Benacerraf 1965.)

Um outro ponto merece ser levantado: há algo de bastante *estranho* nas nossas construções. Começamos pelos números naturais. Depois, construímos os inteiros e construímos "o 0 dos inteiros", isto é, $[0,0]_\sim$. Mas $0 \neq [0,0]_\sim$. De fato, dadas as nossas construções, *nenhum* natural é um inteiro. Isto parece fortemente contraintuitivo. Na Seção 1.3, afirmamos, sem grande argumento, que $\mathbb{N} \subseteq \mathbb{Q}$. Agora, se as construções nos dissessem exatamente *o que* são os números, esta afirmação seria trivialmente falsa.

Recuando um pouco, onde chegamos? Trabalhando numa teoria ingênua dos conjuntos e tomando os naturais como dados, podemos *tratar* inteiros, racionais e reais como certos conjuntos. Nesse sentido, podemos *embutir* as teorias destas entidades numa teoria dos conjuntos. Mas a importância filosófica deste embutimento não é assim tão direta.

Claro que isto não é a última palavra! O ponto é apenas este: mostrar que a

aritmetização dos reais *é de* profunda significação filosófica exigiria argumento filosófico adicional.

5.6 Anéis e Corpos Ordenados

sfr:arith:check:sec

Ao longo deste capítulo, afirmamos que certas definições se comportam "como devem". Neste apêndice técnico, explicitaremos o que queremos dizer com isso e (esboçaremos como) mostrar que as definições se comportam "corretamente".

Na Seção 5.1, definimos adição e multiplicação em $\mathbb{Z}$. Queremos mostrar que, assim definidas, conferem a $\mathbb{Z}$ a estrutura que "quereríamos" que tivesse. Em particular, a estrutura em causa é a de um anel comutativo.

Definição 5.7. Um *anel comutativo* é um conjunto S, equipado com elementos distintos 0 e 1 e operações $+$ e $\times$, que satisfazem estas oito condições:

Associatividade	$a + (b + c) = (a + b) + c$
	$(a \times b) \times c = a \times (b \times c)$
Comutatividade	$a + b = b + a$
	$a \times b = b \times a$
Neutros	$a + 0 = a$
	$a \times 1 = a$
Simétrico aditivo	$(\exists b \in S) 0 = a + b$
Distributividade	$a \times (b + c) = (a \times b) + (a \times c)$

Implicitamente, todas estas fórmulas estão quantificadas universalmente sobre S. Note-se que os elementos 0 e 1 aqui não têm de ser os números naturais com o mesmo nome.

Logo, para verificar que os inteiros formam um anel comutativo, basta verificar estas oito condições. Nenhuma é *difícil* de estabelecer, mas o trabalho é um pouco laborioso. Por exemplo, eis como provar *associatividade*, no caso da adição:

Prova. Fixemos $i, j, k \in \mathbb{Z}$. Então existem $a_1, b_1, a_2, b_2, a_3, b_3 \in \mathbb{N}$ tais que $i = [a_1, b_1]$ e $j = [a_2, b_2]$ e $k = [a_3, b_3]$. (Por legibilidade, escrevemos "$[x, y]$" em vez de "$[x, y]_\sim$"; faremos o mesmo ao longo desta secção.) Então:

$$\begin{aligned} i + (j + k) &= [a_1, b_1] + ([a_2, b_2] + [a_3, b_3]) \\ &= [a_1, b_1] + [a_2 + a_3, b_2 + b_3] \\ &= [a_1 + (a_2 + a_3), b_1 + (b_2 + b_3)] \\ &= [(a_1 + a_2) + a_3, (b_1 + b_2) + b_3] \\ &= [a_1 + a_2, b_1 + b_2] + [a_3, b_3] \\ &= ([a_1, b_1] + [a_2, b_2]) + [a_3, b_3] \\ &= (i + j) + k \end{aligned}$$

apoiando-nos livremente no comportamento da adição em $\mathbb{N}$. □

Do mesmo modo, eis uma prova do *simétrico aditivo*:

Prova. Fixemos $i \in \mathbb{Z}$, de modo que $i = [a, b]$ para alguns $a, b \in \mathbb{N}$. Seja $j = [b, a] \in \mathbb{Z}$. Apoiando-nos no comportamento dos naturais, $(a+b)+0 = 0+(a+b)$, logo $\langle a+b, b+a\rangle \sim_{\mathbb{Z}} \langle 0, 0\rangle$ por definição, e portanto $[a+b, b+a] = [0, 0] = 0_{\mathbb{Z}}$. Assim $i + j = [a, b] + [b, a] = [a+b, b+a] = [0, 0] = 0_{\mathbb{Z}}$. □

E eis uma prova da *distributividade*:

Prova. Como acima, fixemos $i = [a_1, b_1]$ e $j = [a_2, b_2]$ e $k = [a_3, b_3]$. Então:

$$\begin{aligned}
i \times (j + k) &= [a_1, b_1] \times ([a_2, b_2] + [a_3, b_3]) \\
&= [a_1, b_1] \times [a_2 + a_3, b_2 + b_3] \\
&= [a_1(a_2 + a_3) + b_1(b_2 + b_3), a_1(b_2 + b_3) + b_1(a_2 + a_3)] \\
&= [a_1a_2 + a_1a_3 + b_1b_2 + b_1b_3, a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1] \\
&= [a_1a_2 + b_1b_2, a_1b_2 + a_2b_1] + [a_1a_3 + b_1b_3, a_1b_3 + a_3b_1] \\
&= ([a_1, b_1] \times [a_2, b_2]) + ([a_1, b_1] \times [a_3, b_3]) \\
&= (i \times j) + (i \times k)
\end{aligned}$$ □

Deixamos como exercício provar as cinco condições restantes. Tendo feito isso, mostramos que $\mathbb{Z}$ constitui um anel comutativo, isto é, que a adição e a multiplicação (assim definidas) se comportam como devem.

Problema 5.4. Mostre que $\mathbb{Z}$ é um anel comutativo.

Mas a tarefa não termina. Para além de definir adição e multiplicação em $\mathbb{Z}$, definimos uma relação de ordem, $\leq$, e há que verificar que esta se comporta como deve. Com mais pormenor, há que mostrar que $\mathbb{Z}$ constitui um *anel ordenado*.[3]

Definição 5.8. Um *anel ordenado* é um anel comutativo que está também equipado com uma relação de ordem total, $\leq$, tal que:

$$\begin{aligned}
a \leq b &\to a + c \leq b + c \\
(a \leq b \wedge 0 \leq c) &\to a \times c \leq b \times c
\end{aligned}$$

Problema 5.5. Mostre que $\mathbb{Z}$ é um anel ordenado.

Como antes, é laborioso mas rotineiro mostrar que $\mathbb{Z}$, tal como construído, é um anel ordenado. Deixamo-lo ao leitor.

Isto trata dos inteiros. Mas agora precisamos de mostrar coisas muito parecidas para os racionais. Em particular, há que mostrar que os racionais formam um *corpo ordenado*, com as nossas definições de $+$, $\times$ e $\leq$:

[3] Como na Definição 2.16, uma ordem total é uma relação reflexiva, transitiva, antissimétrica e conexa. No contexto de relações de ordem, a conexividade é por vezes chamada *tricotomia*, pois, para quaisquer a e b, temos $a \leq b \vee a = b \vee a \geq b$.

Definição 5.9. Um *corpo ordenado* é um anel ordenado que também satisfaz: sfr:arith:check:orderedfield

$$\textit{Inverso multiplicativo} \qquad (\forall a \in S \setminus \{0\})(\exists b \in S) a \times b = 1$$

Uma vez mostrado que $\mathbb{Z}$ constitui um anel ordenado, é fácil mas laborioso mostrar que $\mathbb{Q}$ constitui um corpo ordenado.

Problema 5.6. Mostre que $\mathbb{Q}$ é um corpo ordenado.

Tendo tratado dos inteiros e dos racionais, só restam os reais. Em particular, há que mostrar que $\mathbb{R}$ constitui um corpo ordenado *completo*, isto é, um corpo ordenado com a propriedade de completude. Agora, Teorema 5.6 estabeleceu que $\mathbb{R}$ tem a propriedade de completude. Contudo, cumpre ainda percorrer a tediosa verificação de que $\mathbb{R}$ é um corpo ordenado.

Antes de nos lançarmos a *esse* exercício laborioso, há que confirmar algumas coisas mais "imediatas". Por exemplo, precisamos de garantia de que $\alpha + \beta$, tal como definida, é de fato um *corte*, para quaisquer cortes α e β. Segue-se uma prova desse fato:

Prova. Como α e β são ambos cortes, $\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$ é um subconjunto próprio não vazio de $\mathbb{Q}$. Suponhamos agora $x < p + q$ para alguns $p \in \alpha$ e $q \in \beta$. Então $x - p < q$, logo $x - p \in \beta$, e $x = p + (x - p) \in \alpha + \beta$. Logo $\alpha + \beta$ é um segmento inicial de $\mathbb{Q}$. Finalmente, para qualquer $p + q \in \alpha + \beta$, como α e β são cortes, existem $p_1 \in \alpha$ e $q_1 \in \beta$ tais que $p < p_1$ e $q < q_1$; logo $p + q < p_1 + q_1 \in \alpha + \beta$; logo $\alpha + \beta$ não tem máximo. □

Esforços semelhantes permitem verificar que $\alpha - \beta$ e $\alpha \times \beta$ e $\alpha \div \beta$ são cortes (no último caso, ignorando o caso em que β é o corte zero). De novo, deixamo-lo ao leitor.

Problema 5.7. Mostre que $\mathbb{R}$ é um corpo ordenado.

Mas eis um pequeno fio solto a atar. Em Seção 5.4, sugerimos que podemos tomar $\sqrt{2} = \{p \in \mathbb{Q} : p < 0 \text{ ou } p^2 < 2\}$. Mas há que mostrar que este conjunto é de fato um *corte*. Segue-se uma prova desse fato:

Prova. Claramente isto é um segmento inicial próprio não vazio dos racionais; basta pois mostrar que não tem máximo. Em particular, basta mostrar que, sendo p um racional positivo com $p^2 < 2$ e $q = \frac{2p+2}{p+2}$, se tem $p < q$ e $q^2 < 2$. Para ver que $p < q$, basta notar:

$$\begin{aligned} p^2 &< 2 \\ p^2 + 2p &< 2 + 2p \\ p(p+2) &< 2 + 2p \\ p &< \tfrac{2+2p}{p+2} = q \end{aligned}$$

Para ver que $q^2 < 2$, basta notar:

$$\begin{aligned} p^2 &< 2 \\ 2p^2 + 4p + 2 &< p^2 + 4p + 4 \\ 4p^2 + 8p + 4 &< 2(p^2 + 4p + 4) \\ (2p+2)^2 &< 2(p+2)^2 \\ \tfrac{(2p+2)^2}{(p+2)^2} &< 2 \\ q^2 &< 2 \end{aligned}$$

□

5.7 Apêndice: os Reais como Sequências de Cauchy

sfr:arith:cauchy:sec

Na Seção 5.4, construímos os reais como cortes de Dedekind. Nesta secção, explicamos uma construção alternativa. Apoia-se na definição, devida a Cauchy, do que hoje chamamos *sequência de Cauchy*; mas o uso desta definição para *construir* os reais deve-se a outros autores do século XIX, nomeadamente Weierstrass, Heine, Méray e Cantor. (Para uma boa história, ver O'Connor and Robertson 2005.)

Antes de chegarmos ao século XIX, vale a pena considerar Simon Stevin (1548–1620). Em resumo, Stevin apercebeu-se de que podemos pensar cada real em termos da sua expansão decimal. Assim, mesmo um número irracional, como $\sqrt{2}$, tem uma expansão decimal agradável, que começa:

$$1.41421356237\ldots$$

É muito fácil modelar expansões decimais na teoria dos conjuntos: basta considerá-las como funções $d\colon \mathbb{N} \to \mathbb{N}$, onde $d(n)$ é o n-ésimo algarismo decimal que nos interessa. Depois precisamos de um pequeno ajuste, para tratar a parte do número real que vem antes da vírgula decimal (aqui, apenas 1). Precisaremos também de outro ajuste (uma relação de equivalência) para garantir que, por exemplo, $0.999\ldots = 1$. Mas não é difícil apresentar uma construção perfeitamente rigorosa dos números reais, à maneira de Stevin, dentro da teoria dos conjuntos.

Stevin não é o nosso foco. (Para mais sobre Stevin, ver Katz and Katz 2012.) Mas eis um pensamento estreitamente relacionado. Em vez de tratar diretamente a expansão decimal de $\sqrt{2}$, podemos antes considerar uma *sequência* de aproximações racionais cada vez mais precisas a $\sqrt{2}$, olhando para as expansões cada vez mais precisas:

$$1, 1.4, 1.414, 1.4142, 1.41421, \ldots$$

A ideia de que os reais podem ser considerados via "aproximações cada vez melhores" nos dá a base para outra sequência de insights, semelhante às constatações que retivemos ao construir $\mathbb{Q}$ a partir de $\mathbb{Z}$, ou $\mathbb{Z}$ a partir de $\mathbb{N}$. Os insights básicos são estes:

1. Todo o real pode escrever-se como uma expansão decimal (eventualmente infinita).

2. A informação codificada por uma expansão decimal (eventualmente infinita) pode igualmente codificar-se por uma sequência de números racionais.

3. Uma sequência de números racionais pode pensar-se como uma função de $\mathbb{N}$ para $\mathbb{Q}$; basta definir $f(n)$ como o n-ésimo racional na sequência.

Claro que nem *qualquer* função de $\mathbb{N}$ para $\mathbb{Q}$ nos dará um número real. Por exemplo, considere-se esta função:

$$f(n) = \begin{cases} 1 & \text{se } n \text{ é ímpar} \\ 0 & \text{se } n \text{ é par} \end{cases}$$

Essencialmente, a preocupação é que a sequência $0, 1, 0, 1, 0, 1, 0, \ldots$ não parece "convergir" para nenhum real. Logo: para garantir que consideramos sequências que de fato convergem para algum real, precisamos de restringir a atenção a sequências que tenham algum *limite*.

Já encontramos a ideia de limite em **??**. Mas não podemos usar *exatamente* a mesma definição que ali. A expressão "$(\forall \varepsilon > 0)$" envolvia tacitamente quantificação sobre os números reais; e estávamos a considerar limites de funções nos reais; logo, invocar essa definição seria valer-nos dos números reais — e eram precisamente eles que estávamos a tentar *construir*. Felizmente, podemos trabalhar com uma ideia estreitamente relacionada com a de limite.

Definição 5.10. Uma função $f : \mathbb{N} \to \mathbb{Q}$ é uma *sequência de Cauchy* sse, para qualquer $\varepsilon \in \mathbb{Q}$ positivo, se tem $(\exists \ell \in \mathbb{N})(\forall m, n > \ell)|f(m) - f(n)| < \varepsilon$. sfr:arith:cauchy:def:CauchySequence

A ideia geral de limite é a mesma de antes: se se quer um certo nível de precisão (medido por ε), há uma "região" onde olhar (qualquer entrada maior que ℓ). E é fácil ver que a nossa sequência 1, 1.4, 1.414, 1.4142, 1.41421... tem limite: se se quer aproximar $\sqrt{2}$ com erro inferior a $1/10^n$, basta olhar para qualquer entrada depois da n-ésima.

O pensamento óbvio seria então dizer que um número real *é* simplesmente qualquer sequência de Cauchy. Mas, como nas construções de $\mathbb{Z}$ e $\mathbb{Q}$, isso seria demasiado ingênuo: para um dado número real, várias sequências de Cauchy diferentes "indicam" esse número. Uma forma simples de ver isto é a seguinte. Dada uma sequência de Cauchy f, defina-se g como exatamente a mesma função que f, exceto que $g(0) \neq f(0)$. Como as duas sequências coincidem em todo o lado depois do primeiro número, quereremos, em última análise, dizer que têm o mesmo limite, no sentido de Definição 5.10, e portanto devem ser pensadas como "definindo" o mesmo real. Logo, devemos pensar nestas sequências de Cauchy como o mesmo número real.

Consequentemente, voltamos a precisar de definir uma relação de equivalência sobre as sequências de Cauchy, e identificar os números reais com *classes* de equivalência. Precisamos primeiro da ideia de uma função que tende

para 0 no limite. Para qualquer função $h : \mathbb{N} \to \mathbb{Q}$, digamos que h *tende para* 0 sse, para qualquer $\varepsilon \in \mathbb{Q}$ positivo, se tem que $(\exists \ell \in \mathbb{N})(\forall n > \ell)|h(n)| < \varepsilon$.[4] Além disso, sendo f e g funções $\mathbb{N} \to \mathbb{Q}$, definamos $(f - g)(n) = f(n) - g(n)$. Definimos agora:

$$f \fallingdotseq g \text{ sse } (f - g) \text{ tende para 0.}$$

Há que verificar que $\fallingdotseq$ é uma relação de equivalência; e de fato é. Podemos então, se quisermos, definir os reais como as classes de equivalência, sob $\fallingdotseq$, de todas as sequências de Cauchy de $\mathbb{N} \to \mathbb{Q}$.

Problema 5.8. Seja $f(n) = 0$ para todo n. Seja $g(n) = \frac{1}{(n+1)^2}$. Mostre que ambas são sequências de Cauchy e que o limite de ambas as funções é 0, de modo que também $f \sim_{\mathbb{R}} g$.

Feito isto, como de costume escrevemos $[f]_{\fallingdotseq}$ para a classe de equivalência que tem f como um membro. Porém, para manter a legibilidade, no que se segue omitimos o subscrito e escrevemos apenas $[f]$. Estipulamos também que, para cada $q \in \mathbb{Q}$, se tem $q_{\mathbb{R}} = [c_q]$, onde c_q é a função constante $c_q(n) = q$ para todo $n \in \mathbb{N}$. Definimos depois relações e operações básicas sobre os reais, por exemplo:

$$[f] + [g] = [(f + g)]$$
$$[f] \times [g] = [(f \times g)]$$

onde $(f + g)(n) = f(n) + g(n)$ e $(f \times g)(n) = f(n) \times g(n)$. Claro que também há que verificar que cada uma de $(f + g)$, $(f - g)$ e $(f \times g)$ é sequência de Cauchy quando f e g o são; mas o são, e deixamo-lo ao leitor.

Por fim, definimos uma noção de ordem. Dizemos que $[f]$ é *positivo* sse tanto $[f] \neq 0_{\mathbb{Q}}$ como $(\exists \ell \in \mathbb{N})(\forall n > \ell) 0 < f(n)$. Depois dizemos $[f] < [g]$ sse $[(g - f)]$ é positivo. Há que verificar que isto está bem definido (isto é, que não depende da escolha da função "representante" na classe de equivalência). Mas tendo feito isto, é bastante fácil mostrar que obtemos as propriedades algébricas certas; isto é:

sfr:arith:cauchy:thm:cauchyorderedfield

Teorema 5.11. *As sequências de Cauchy constituem um corpo ordenado.*

Prova. Exercício. □

Problema 5.9. Mostre que as sequências de Cauchy constituem um corpo ordenado.

É mais difícil provar que os reais, assim construídos, têm a propriedade de completude, pelo que daremos a prova.

Teorema 5.12. *Todo o conjunto não vazio de sequências de Cauchy com majorante tem supremo (menor majorante).*

[4] Compare-se com a definição de $\lim_{x\to\infty} f(x) = 0$ em **??**.

Esboço de prova. Seja S um conjunto não vazio de sequências de Cauchy com majorante. Então existe algum $p \in \mathbb{Q}$ tal que $p_{\mathbb{R}}$ é majorante de S. Seja $r \in S$; então existe algum $q \in \mathbb{Q}$ tal que $q_{\mathbb{R}} < r$. Logo, se existe supremo de S, este está entre $q_{\mathbb{R}}$ e $p_{\mathbb{R}}$ (inclusive).

Nos aproximaremos do supremo, abordando-o simultaneamente por baixo e por cima. Em particular, definimos duas funções, $f, g\colon \mathbb{N} \to \mathbb{Q}$, com a ideia de que f se irá aproximar do supremo por cima e g por baixo. Começamos por definir:

$$f(0) = p$$
$$g(0) = q$$

Então, sendo $a_n = \frac{f(n)+g(n)}{2}$, definamos:[5]

$$f(n+1) = \begin{cases} a_n & \text{se } (\forall h \in S)[h] \leq (a_n)_{\mathbb{R}} \\ f(n) & \text{caso contrário} \end{cases}$$
$$g(n+1) = \begin{cases} a_n & \text{se } (\exists h \in S)[h] \geq (a_n)_{\mathbb{R}} \\ g(n) & \text{caso contrário} \end{cases}$$

Tanto f como g são sequências de Cauchy. (Isto verifica-se com relativa facilidade, mas deixamo-lo como exercício.) Note-se que a função $(f-g)$ tende para 0, pois a diferença entre f e g reduz-se à metade a cada passo. Logo $[f] = [g]$.

Mostramos primeiro que $[f]$ é majorante de S, isto é, que $(\forall h \in S)[h] \leq [f]$. (Invocaremos Teorema 5.11 ao longo do argumento.) Seja $h \in S$ e suponhamos, por *reductio*, que $[f] < [h]$, de modo que $0_{\mathbb{R}} < [(h - f)]$. Como f é uma sequência de Cauchy monotonamente decrescente, existe algum $n \in \mathbb{N}$ tal que $[(c_{f(n)} - f)] < [(h - f)]$. Logo:

$$(f(n))_{\mathbb{R}} = [c_{f(n)}] < [f] + [(h - f)] = [h],$$

o que contradiz o fato de que, por construção, $[h] \leq (f(n))_{\mathbb{R}}$.

Mostramos a seguir que $[f] = [g]$ é o supremo de S. Seja j qualquer sequência de Cauchy e suponhamos $[j] < [g]$. Raciocinando como acima (usando o fato de g ser *crescente*), existe $n \in \mathbb{N}$ tal que $[j] < (g(n))_{\mathbb{R}}$. Mas, por construção, existe $h \in S$ tal que $(g(n))_{\mathbb{R}} \leq [h]$, logo $[j] < [h]$ e portanto $[j]$ não é majorante de S. □

[5] Isto é uma definição recursiva. Mas ainda *não* demos qualquer razão para crer que definições recursivas são legítimas.

Capítulo 6

Conjuntos Infinitos

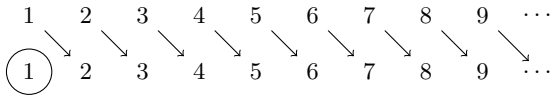
Este capítulo sobre conjuntos infinitos foi retirado de *Open Set Theory*, de Tim Button.

6.1 Hotel de Hilbert

sfr:infinite:hilbert:sec

O conjunto dos números naturais é obviamente infinito. Logo, se não quisermos *valer-nos* dos números naturais, o nosso primeiro passo é caracterizar um conjunto infinito em termos que não exijam mencionar os próprios números naturais. Eis uma abordagem agradável, apresentada por Hilbert numa conferência de 1924. Ele nos pede que imaginemos

> [...] um hotel com um número finito de quartos. Todos esses quartos devem estar ocupados por exatamente um hóspede. Se os hóspedes trocam de quarto de algum modo, [mas] de tal forma que cada quarto continua a conter no máximo uma pessoa, então nenhum quarto ficará livre, e o dono do hotel não pode, deste modo, criar um novo lugar para um hóspede que acaba de chegar [...¶...]
>
> Agora estipulamos que o hotel tem infinitos quartos numerados 1, 2, 3, 4, 5, ..., cada um ocupado por exatamente um hóspede. Logo que chega um novo hóspede, o dono só precisa de mudar cada um dos hóspedes antigos para o quarto associado ao número imediatamente superior, e o quarto 1 ficará livre para o recém-chegado.



(publicado em Hilbert 2013, 730; a nossa tradução)

O ponto crucial é que o Hotel de Hilbert tem infinitos quartos; e podemos tomar a sua explicação como definição do que significa dizer isto. De fato, foi esta a abordagem de Dedekind (apresentada aqui, claro, com enorme anacronismo; a definição de Dedekind é de 1888):

Definição 6.1. Um conjunto A é *infinito de Dedekind* sse existe uma injeção de A para um subconjunto próprio de A. Isto é, existe algum $o \in A$ e uma injeção $f : A \to A$ tal que $o \notin \mathrm{Im}(f)$. sfr:infinite:hilbert:defn:DedekindInfinite

6.2 Álgebras de Dedekind

Não queremos apenas que os números naturais sejam infinitos; queremos que tenham certas propriedades (algébricas): precisam de comportar-se bem sob adição, multiplicação, e assim por diante. sfr:infinite:dedekind:sec

A ideia de Dedekind foi tomar como primitiva a noção de *função sucessor* e depois caracterizar os números como aqueles que têm as seguintes propriedades:

1. Existe um número, 0, que não é sucessor de nenhum número
   isto é, $0 \notin \mathrm{Im}(s)$
   isto é, $\forall x\ s(x) \neq 0$

2. Números distintos têm sucessores distintos
   isto é, s é uma injeção
   isto é, $\forall x \forall y (s(x) = s(y) \to x = y)$

3. Todo o número se obtém de 0 por aplicações repetidas da função sucessor. sfr:infinite:dedekind:repeatedapplication

As duas primeiras condições são fáceis de lidar com, usando lógica de primeira ordem (ver acima). Mas não podemos tratar (3) apenas com lógica de primeira ordem. O avanço de Dedekind foi reformular a condição (3), em termos de teoria dos conjuntos, assim:

3′. Os números naturais são o menor conjunto que é *fechado para a função sucessor*: isto é, se aplicarmos s a qualquer membro do conjunto, obtemos outro membro do conjunto.

Mas precisamos de explicitar isto com calma.

Definição 6.2. Para qualquer função f, o conjunto X é *f-fechado* sse $(\forall x \in X) f(x) \in X$. Definimos agora, para qualquer o: sfr:infinite:dedekind:Closure

$$\mathrm{clo}_f(o) = \bigcap \{X : o \in X \text{ e } X \text{ é } f\text{-fechado}\}$$

Logo $\mathrm{clo}_f(o)$ é a interseção de todos os conjuntos f-fechados que têm o como um membro. Intuitivamente, então, $\mathrm{clo}_f(o)$ é o conjunto f-fechado *menor* que tem o como um membro. O resultado seguinte torna preciso esse pensamento intuitivo;

Lema 6.3. *Para qualquer função f e qualquer $o \in A$:* *sfr:infinite:dedekind:closureproperties*

sfr:infinite:dedekind: closurehaselem
1. $o \in \mathrm{clo}_f(o)$; *e*

sfr:infinite:dedekind: closureclosed
2. $\mathrm{clo}_f(o)$ *é* f*-fechado; e*

sfr:infinite:dedekind: closuresmallest
3. *se* X *é* f*-fechado e* $o \in X$*, então* $\mathrm{clo}_f(o) \subseteq X$

Prova. Note-se que existe pelo menos um conjunto f-fechado com o como um membro, nomeadamente $\mathrm{Im}(f) \cup \{o\}$. Logo $\mathrm{clo}_f(o)$, a interseção de *todos* os tais conjuntos, existe. Cumpre agora verificar (1)–(3).

Quanto a (1): $o \in \mathrm{clo}_f(o)$ pois é uma interseção de conjuntos que todos têm o como um membro.

Quanto a (2): suponhamos $x \in \mathrm{clo}_f(o)$. Se $o \in X$ e X é f-fechado, então $x \in X$, e agora $f(x) \in X$ pois X é f-fechado. Logo $f(x) \in \mathrm{clo}_f(o)$.

Quanto a (3): de modo geral, se $X \in C$ então $\bigcap C \subseteq X$. □

Com isto, podemos dizer:

Definição 6.4. Uma *álgebra de Dedekind* é um conjunto A juntamente com uma função $f\colon A \to A$ e algum $o \in A$ tal que:

sfr:infinite:dedekind: ded:proper
1. $o \notin \mathrm{Im}(f)$

sfr:infinite:dedekind: ded:injection
2. f é uma injeção

sfr:infinite:dedekind: ded:closure
3. $A = \mathrm{clo}_f(o)$

Como $A = \mathrm{clo}_f(o)$, o resultado anterior nos diz que A é o menor conjunto f-fechado com o como um membro. Claramente uma álgebra de Dedekind é infinita de Dedekind; basta olhar para as cláusulas (1) e (2) da definição. Mas o fato mais relevante é que qualquer conjunto infinito de Dedekind pode ser transformado numa álgebra de Dedekind.

sfr:infinite:dedekind: thm:DedekindInfiniteAlgebra
Teorema 6.5. *Se existe um conjunto infinito de Dedekind, então existe uma álgebra de Dedekind.*

Prova. Seja D infinito de Dedekind. Logo existe uma injeção $g\colon D \to D$ e um elemento $o \in D \setminus \mathrm{Im}(g)$. Seja agora $A = \mathrm{clo}_g(o)$; por Lema 6.3, A existe e $o \in A$. Seja $f = g{\restriction_A}$. Mostraremos que A, f, o formam uma álgebra de Dedekind.

Quanto a (1): $o \notin \mathrm{Im}(g)$ e $\mathrm{Im}(f) \subseteq \mathrm{Im}(g)$, logo $o \notin \mathrm{Im}(f)$.

Quanto a (2): g é injetiva em D; logo $f \subseteq g$ tem de ser injetiva.

Quanto a (3): por Lema 6.3, A é g-fechado; *a fortiori*, A é f-fechado. Logo $\mathrm{clo}_f(o) \subseteq A$ por Lema 6.3. Como também $\mathrm{clo}_f(o)$ é f-fechado e $f = g{\restriction_A}$, segue-se que $\mathrm{clo}_f(o)$ é g-fechado. Logo $A \subseteq \mathrm{clo}_f(o)$ por Lema 6.3. □

6.3 Álgebras de Dedekind e Indução Aritmética

Crucialmente, agora, uma álgebra de Dedekind—de fato, *qualquer* álgebra de Dedekind—servirá como substituto dos números naturais. Isto deve-se à seguinte consequência trivial: sfr:infinite:induction:sec

Teorema 6.6 (Indução aritmética). *Sejam N, s, o uma álgebra de Dedekind. Então, para qualquer conjunto X:* sfr:infinite:induction:thm:dedinfiniteinduction

$$\text{se } o \in X \text{ e } (\forall n \in N \cap X)s(n) \in X, \text{ então } N \subseteq X.$$

Prova. Pela definição de álgebra de Dedekind, $N = \mathrm{clo}_s(o)$. Ora, se tanto $o \in X$ como $(\forall n \in N)(n \in X \to s(n) \in X)$, então $N = \mathrm{clo}_s(o) \subseteq X$. □

Como a indução é característica dos números naturais, o ponto é este. Dado qualquer conjunto infinito de Dedekind, podemos formar uma álgebra de Dedekind e usar essa álgebra como substituto dos números naturais.

Admitidamente, Teorema 6.6 formula a indução em termos *de teoria dos conjuntos*. Mas podemos facilmente pôr o princípio em termos mais familiares:

Corolário 6.7. *Sejam N, s, o uma álgebra de Dedekind. Então, para qualquer fórmula $\varphi(x)$, que pode ter parâmetros:* sfr:infinite:induction:natinductionschema

$$\text{se } \varphi(o) \text{ e } (\forall n \in N)(\varphi(n) \to \varphi(s(n))), \text{ então } (\forall n \in N)\varphi(n)$$

Prova. Seja $X = \{n \in N : \varphi(n)\}$, e use-se agora Teorema 6.6 □

Neste resultado, falamos de uma fórmula "ter parâmetros". O que isto significa, em traços grosseiros, é que, para quaisquer objetos $c_1, \ldots, c_k$, podemos trabalhar com $\varphi(x, c_1, \ldots, c_k)$. Com mais precisão, podemos enunciar o resultado sem mencionar "parâmetros" do seguinte modo. Para qualquer fórmula $\varphi(x, v_1, \ldots, v_k)$, cujas variáveis livres são todas as exibidas, temos:

$$\begin{aligned}\forall v_1 \ldots \forall v_k((&\varphi(o, v_1, \ldots, v_k) \wedge \\ &(\forall x \in N)(\varphi(x, v_1, \ldots, v_k) \to \varphi(s(x), v_1, \ldots, v_k))) \to \\ &(\forall x \in N)\varphi(x, v_1, \ldots, v_k))\end{aligned}$$

Evidentemente, falar em "ter parâmetros" pode tornar a leitura muito mais fácil. (Na **??**, usaremos este expediente com frequência.)

Voltando às álgebras de Dedekind: dada qualquer álgebra de Dedekind, podemos também definir as habituais funções aritméticas de adição, multiplicação e exponenciação. Isto não é trivial, porém, e envolve a técnica de *definição recursiva*. É uma técnica que introduziremos e justificaremos muito mais tarde, e num contexto bem mais geral. (Os entusiastas podem querer voltar a isto depois de **??**, ou talvez ler um tratamento alternativo, como Potter

2004, pp. 95–8.) Mas, onde N, s, o formam uma álgebra de Dedekind, acabaremos por poder estipular o seguinte:

$$\begin{array}{lll} a + o = a & a \times o = o & a^o = s(o) \\ a + s(b) = s(a + b) & a \times s(b) = (a \times b) + a & a^{s(b)} = a^b \times a \end{array}$$

e mostrar que estas definições se comportam como se espera.

6.4 "Prova" de Dedekind da existência de um conjunto infinito

sfr:infinite:dedekindsproof:sec

Neste capítulo, apresentamos um tratamento em teoria dos conjuntos dos números naturais, em termos de álgebras de Dedekind. Em Seção 5.5, refletimos sobre o significado filosófico da aritmetização da análise (entre outras coisas). Cumpre agora refletir sobre o significado do que aqui alcançamos.

Ao longo de Capítulo 5, tomamos os números naturais como dados e os usamos para construir os inteiros, os racionais e os reais, de modo explícito. Neste capítulo, não demos uma construção explícita dos números naturais. Mostramos apenas que, *dado qualquer conjunto infinito de Dedekind*, podemos definir um conjunto que se comportará como queremos que $\mathbb{N}$ se comporte.

Obviamente, pois, não podemos pretender ter respondido a uma questão metafísica, como *quais os objetos que são os números naturais*. Mas isso é bom. Afinal, na Seção 5.5, sublinhamos que estaríamos errados se pensássemos na definição de $\mathbb{R}$ como conjunto de cortes de Dedekind como uma *descoberta*, em vez de uma estipulação conveniente. A observação crucial é que os cortes de Dedekind exemplificam as propriedades matemáticas centrais dos números reais. Assim também aqui: a observação crucial é que *qualquer* álgebra de Dedekind exemplifica as propriedades matemáticas centrais dos números naturais. (De fato, Dedekind insistiu neste ponto ao provar que todas as álgebras de Dedekind são *isomorfas* (1888, Theorems 132–3). Não surpreende, então, que muitos "estruturalistas" contemporâneos cite Dedekind como precursor.)

Além disso, mostramos como embutir a teoria dos números naturais numa teoria ingênua simples dos conjuntos, que ainda permanece bastante informal, mas que (aparentemente) não assume os números naturais como dados. Assim, podemos estar no caminho de realizar o próprio projeto ambicioso de Dedekind, que ele explicou assim:

> Na ciência nada que seja provável deve ser acreditado sem prova. Embora esta exigência pareça razoável, não posso considerá-la satisfeita sequer nos métodos mais recentes de lançar os fundamentos da ciência mais simples; a saber, aquela parte da lógica que trata da teoria dos números. Ao falar de aritmética (álgebra, análise) como mera parte da lógica, quero insinuar que considero o conceito de número totalmente independente das noções ou intuições de espaço e tempo—que o considero antes um produto imediato das leis puras do pensamento. (Dedekind, 1888, preface)

A ideia audaciosa de Dedekind é esta. Acabamos de mostrar como construir os números naturais usando só (ingenuamente) a teoria dos conjuntos. Em Capítulo 5, vimos como construir os reais dados os números naturais e alguma teoria dos conjuntos. Logo, talvez, "a aritmética (álgebra, análise)" acabe por ser "meramente parte da lógica" (no sentido alargado que Dedekind dá à palavra "lógica").

Essa é a ideia. Mas esperemos um momento. A nossa construção de uma álgebra de Dedekind (o nosso substituto dos números naturais) é condicional à existência de um conjunto infinito de Dedekind. (Basta olhar para trás, para Teorema 6.5.) A menos que a existência de um conjunto infinito de Dedekind possa ser estabelecida via "lógica" ou "as leis puras do pensamento", o projeto estagna.

Então, *pode* a existência de um conjunto infinito de Dedekind ser estabelecida pelas "leis puras do pensamento"? Eis o esforço de Dedekind:

> O meu próprio reino de pensamentos, isto é, a totalidade S de todas as coisas que podem ser objetos do meu pensamento, é infinita. Pois, se s designa um elemento de S, então o pensamento s' de que s pode ser objeto do meu pensamento é ele próprio um elemento de S. Se considerarmos isto como uma imagem $\varphi(s)$ do elemento s, então ... S é infinito de Dedekind, como queríamos ter provado. (Dedekind, 1888, §66)

Isto é algo de espantoso de encontrar no meio de um livro que em grande parte consiste em provas matemáticas altamente rigorosas. Duas observações valem a pena.

Primeiro: esta "prova" mal tem o que hoje reconheceríamos como caráter "matemático". Fala de objetos psicológicos (pensamentos), e apenas de objetos *possíveis*.

Segundo: pelo menos tal como apresentamos as álgebras de Dedekind, esta "prova" tem uma lacuna técnica direta. Se o argumento de Dedekind é bem-sucedido, estabelece só que há infinitas coisas (nomeadamente, infinitos pensamentos). Mas Dedekind também precisa de nos dar uma razão para ver S como um único *conjunto*, com infinitos membros, em vez de pensar em S como *algumas coisas* (no plural).

O fato de Dedekind não ver aqui uma lacuna pode sugerir que o seu uso da palavra "totalidade" não corresponde exatamente ao *nosso* uso da palavra "conjunto".[1] Mas isto não seria demasiado surpreendente. O projeto que perseguimos nos últimos dois capítulos—uma "construção" dos naturais e, a partir deles, uma "construção" dos inteiros, reais e racionais—foi todo ele feito de modo ingênuo. Nos apoiamos neste conjunto, ou naquele conjunto, sempre que precisamos, sem enunciar muitos princípios gerais sobre exatamente que conjuntos existem, e quando. Mas sabemos que precisamos de *alguns* princípios gerais, pois caso contrário caímos no Paradoxo de Russell.

Chegou a hora de superarmos a nossa ingenuidade.

[1] De fato, temos outras razões para pensar que não correspondia; ver Potter (2004, p. 23).

6.5 Apêndice: Provando Schröder-Bernstein

sfr:infinite:card-sb:sec

Antes de deixarmos a teoria ingênua dos conjuntos, há ainda uma última prova ingênua (mas sofisticada!) a considerar. Trata-se de uma prova de Schröder-Bernstein (Teorema 4.25): se $A \preceq B$ e $B \preceq A$ então $A \approx B$; isto é, dados injeções $f\colon A \to B$ e $g\colon B \to A$, existe uma bijeção $h\colon A \to B$.

Neste capítulo, seguimos a noção dedekindiana de *fechos*. De fato, Dedekind deu uma prova muito elegante de Schröder-Bernstein com esta noção, e aqui a apresentamos. A prova segue de perto Potter (2004, pp. 157–8), se quiser um tratamento ligeiramente diferente mas essencialmente semelhante. Uma breve pesquisa na Internet também convencerá o leitor de que este é um teorema—tal como a irracionalidade de $\sqrt{2}$—para o qual existem *muitas* provas interessantes e distintas.

Usando notação semelhante à de Definição 6.2, seja

$$\mathrm{Clo}_f(B) = \bigcap\{X : B \subseteq X \text{ e } X \text{ é } f\text{-fechado}\}$$

para cada conjunto B e função f. Assim definido, $\mathrm{Clo}_f(B)$ é o menor conjunto f-fechado que contém B, no sentido de que:

sfr:infinite:card-sb:Closureprops

Lema 6.8. *Para qualquer função f, e qualquer B:*

sfr:infinite:card-sb:Closurehaselem

1. $B \subseteq \mathrm{Clo}_f(B)$; *e*

sfr:infinite:card-sb:Closureclosed

2. $\mathrm{Clo}_f(B)$ *é f-fechado; e*

sfr:infinite:card-sb:Closuresmallest

3. *se X é f-fechado e $B \subseteq X$, então* $\mathrm{Clo}_f(B) \subseteq X$.

Prova. Exatamente como no Lema 6.3. □

Precisamos de mais um fato para chegar a Schröder-Bernstein:

sfr:infinite:card-sb:sbhelper

Proposição 6.9. *Se $A \subseteq B \subseteq C$ e $A \approx C$, então $A \approx B \approx C$.*

Prova. Dada uma bijeção $f\colon C \to A$, seja $F = \mathrm{Clo}_f(C \setminus B)$ e defina-se uma função g com domínio C do seguinte modo:

$$g(x) = \begin{cases} f(x) & \text{se } x \in F \\ x & \text{caso contrário} \end{cases}$$

Mostraremos que g é uma bijeção de C para B, donde seguirá que $g \circ f^{-1}\colon A \to B$ é uma bijeção, completando a prova.

Primeiro alegamos que, se $x \in F$ mas $y \notin F$, então $g(x) \neq g(y)$. Por reductio, suponhamos o contrário, de modo que $y = g(y) = g(x) = f(x)$. Como $x \in F$ e F é f-fechado por Lema 6.8, temos $y = f(x) \in F$, contradição.

Suponhamos agora $g(x) = g(y)$. Então, pelo que precede, $x \in F$ sse $y \in F$. Se $x, y \in F$, então $f(x) = g(x) = g(y) = f(y)$, logo $x = y$ pois f é uma bijeção. Se $x, y \notin F$, então $x = g(x) = g(y) = y$. Logo g é uma injeção.

Resta mostrar que $\mathrm{Im}(g) = B$. Fixemos $x \in B \subseteq C$. Se $x \notin F$, então $g(x) = x$. Se $x \in F$, então $x = f(y)$ para algum $y \in F$, pois caso contrário $F \setminus \{x\}$ seria f-fechado e estenderia $C \setminus B$, o que é impossível por Lema 6.8; agora $g(y) = f(y) = x$. □

Finalmente, eis a prova do resultado principal. Recordemos que, dada uma função h e um conjunto D, definimos $h[D] = \{h(x) : x \in D\}$.

Prova de Schröder-Bernstein. Sejam $f\colon A \to B$ e $g\colon B \to A$ injeções. Como $f[A] \subseteq B$, temos $g[f[A]] \subseteq g[B] \subseteq A$. Além disso, $g \circ f\colon A \to g[f[A]]$ é uma injeção, pois tanto g como f o são; e de fato $g \circ f$ é uma bijeção, apenas pela forma como definimos o seu contradomínio. Logo $g[f[A]] \approx A$, e portanto, por Proposição 6.9, existe uma bijeção $h\colon A \to g[B]$. Além disso, g^{-1} é uma bijeção $g[B] \to B$. Logo $g^{-1} \circ h\colon A \to B$ é uma bijeção. □

Créditos das Imagens

Referências Bibliográficas

Benacerraf, Paul. 1965. What numbers could not be. *The Philosophical Review* 74(1): 47–73.

Cantor, Georg. 1892. Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresbericht der deutschen Mathematiker-Vereinigung* 1: 75–8.

Conway, John. 2006. The power of mathematics. In *Power*, eds. Alan Blackwell and David MacKay, Darwin College Lectures. Cambridge: Cambridge University Press. URL `http://www.cs.toronto.edu/~mackay/conway.pdf`.

Dedekind, Richard. 1888. *Was sind und was sollen die Zahlen?* Braunschweig: Vieweg.

Frege, Gottlob. 1884. *Die Grundlagen der Arithmetik: Eine logisch mathematische Untersuchung über den Begriff der Zahl*. Breslau: Wilhelm Koebner. Translation in Frege (1953).

Frege, Gottlob. 1953. *Foundations of Arithmetic*, ed. J. L. Austin. Oxford: Basil Blackwell & Mott, 2nd ed.

Hilbert, David. 2013. *David Hilbert's Lectures on the Foundations of Arithmetic and Logic 1917–1933*, eds. William Bragg Ewald and Wilfried Sieg. Heidelberg: Springer.

Katz, Karin Usadi and Mikhail G. Katz. 2012. Stevin numbers and reality. *Foundations of Science* 17(2): 109–23.

O'Connor, John J. and Edmund F. Robertson. 2005. The real numbers: Stevin to Hilbert URL `http://www-history.mcs.st-and.ac.uk/HistTopics/Real_numbers_2.html`.

Potter, Michael. 2004. *Set Theory and its Philosophy*. Oxford: Oxford University Press.