udf 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.

arith.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 arith.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 arith.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 arith.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 arith.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 $m, n \in \mathbb{N}$

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

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.

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

Problema arith.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 $m, n \in \mathbb{N}$.

arith.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 arith.2. Mostre que $\backsim$ é uma relação de equivalência.

Mas isto permite-nos dizer o seguinte:

Definição arith.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 arith.6. Mas de fato comportam-se! 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 arith.6 que tudo isto se comporta corretamente.

Problema arith.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 $i, j \in \mathbb{Z}$.

arith.3 A Reta Real

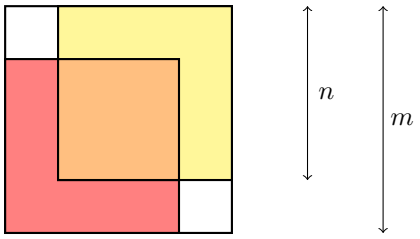
O passo seguinte é mostrar como construir os reais a partir dos racionais. Antes disso, há que perceber o que há de *distintivo* nos reais. sfr:arith:real:sec

Os reais comportam-se de modo muito parecido com os racionais. (Tecnicamente, ambos são exemplos de *corpos ordenados*; para a definição, ver Definição arith.9.) Agora, se resolveu os exercícios de **??**, 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:

Teorema arith.4. *$\sqrt{2}$ não é racional, isto é, $\sqrt{2} \notin \mathbb{Q}$* sfr:arith:real:root2irrational

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:



□

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.

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

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.

arith.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 arith.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 arith.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:

Teorema arith.6. *O conjunto dos cortes tem a propriedade de completude.* *sfr:arith:cuts:realcompleteness*

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 arith.6.

arith.5 Algumas Reflexões Filosóficas

sfr:arith:ref:sec

Quanto aos pormenores técnicos, por ora basta. Mas o que foi que alcançaram?

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 arith.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 arith.7). Mas eis uma forma trivial de obter construções diferentes: como em **??**, 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 **??**, 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 **??**, 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.

arith.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 arith.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 arith.7. Um *anel comutativo* é um conjunto S, equipado com elementos distintos 0 e 1 e operações $+$ e $\times$, que satisfazem estas oito condições:

$$\begin{aligned}
\textit{Associatividade} \qquad & a + (b + c) = (a + b) + c \\
& (a \times b) \times c = a \times (b \times c) \\
\textit{Comutatividade} \qquad & a + b = b + a \\
& a \times b = b \times a \\
\textit{Neutros} \qquad & a + 0 = a \\
& a \times 1 = a \\
\textit{Simétrico aditivo} \qquad & (\exists b \in S) 0 = a + b \\
\textit{Distributividade} \qquad & a \times (b + c) = (a \times b) + (a \times c)
\end{aligned}$$

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 arith.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 arith.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 arith.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 $\leq$:

Definição arith.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 arith.6. Mostre que $\mathbb{Q}$ é um corpo ordenado.

[3] Como na **??**, 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 $a \leq b \vee a = b \vee a \geq b$.

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 arith.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 arith.7. Mostre que $\mathbb{R}$ é um corpo ordenado.

Mas eis um pequeno fio solto a atar. Em Seção arith.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:

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

□

arith.7 Apêndice: os Reais como Sequências de Cauchy

Na Seção arith.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.)

sfr:arith:cauchy:sec

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.

sfr:arith:cauchy:
def:CauchySequence

Definição arith.10. Uma função $f : \mathbb{N} \to \mathbb{Q}$ é uma *sequência de Cauchy* sse, para qualquer $\varepsilon \in \mathbb{Q}$ positivo, se tem $(\exists \ell \in \mathbb{N})(\forall m, n > \ell)|f(m) - f(n)| < \varepsilon$.

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 arith.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 $\mathbb{N} \to \mathbb{Q}$.

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

Problema arith.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 $[f]_{\sim}$ 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:

Teorema arith.11. *As sequências de Cauchy constituem um corpo ordenado.* *sfr:arith:cauchy: thm:cauchyorderedfield*

Prova. Exercício. □

Problema arith.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 arith.12. *Todo o conjunto não vazio de sequências de Cauchy com majorante tem supremo (menor majorante).*

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 arith.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. □

Créditos das Imagens

Referências Bibliográficas

Benacerraf, Paul. 1965. What numbers could not be. *The Philosophical Review* 74(1): 47–73.

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`.

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`.

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