Análise I – DEX 001114
Notas de aula

Renan M. Mezabarba

Última atualização: 27 de agosto de 2024.

Quis custodiet ipsos custodes?[0]

Juvenal, Sátiras, VI, linha 347.

[0]Quem vigia os vigilantes?

Sumário

Prefácio (É PRA LER!)

O presente material é uma versão reformulada (de partes) do texto "`Um curso fechado e limitado de Análise Real`" [14], que comecei a escrever tempos atrás, mas cuja narrativa não é apropriada para, efetivamente, acompanhar um curso de Análise, por diversos motivos[0]. Por isso, aqui você encontrará os assuntos distribuídos de forma diferente e mais amigável.

Cada capítulo corresponde a um terço do curso, enquanto as seções correspondem aos conteúdos das aulas. Tais seções serão divididas em duas partes: a subseção "`Essencial`" apresenta o que será abordado em aula, enquanto a subseção "`Extras`" contêm discussões adicionais, cuja leitura é opcional (mas recomendada)[1]. Exercícios serão propostos tanto ao longo do texto quanto em subseções específicas para atividades ("`Exercícios adicionais`"). Por falar nos exercícios, eles serão classificados em três tipos principais ($\star$, $\overset{\star}{\star}$ e $\overset{\star}{\star\star}$) descritos a seguir.

($\star$) Verificações (que deveriam ser) corriqueiras. Embora nem todos os exercícios nesta classe sejam imediatos, a maioria consiste em "abrir" as definições e fazer as "contas" naturais ao contexto em questão. Não é o tipo de problema que "cai em prova", mas são bons aquecimentos caso você ainda não tenha prática em escrever demonstrações mais complicadas.

($\overset{\star}{\star}$) Exercícios típicos de listas e provas. Consistem em aplicar resultados previamente demonstrados (tanto em aula quanto em questões anteriores), ou reciclar ideias vistas anteriormente a fim de testar o seu entendimento do assunto: quanto maior sua familiaridade, mais fácil será para você fazer os malabarismos necessários.

($\overset{\star}{\star\star}$) Estes geralmente são mais difíceis ou elaborados e não costumam fazer parte de listas ou provas (exceto, possivelmente, como questões bônus). Eles "testam" não apenas a familiaridade com o assunto, mas também dão a oportunidade de exercitar um pouco mais a criatividade.

Tente fazer exercícios de todos os tipos: fazer os fáceis te ajudará a ganhar ritmo para fazer os médios, e ao fazer alguns difíceis você *pode* aprender técnicas para transformar os exercícios médios em fáceis. Outra dica: se já souber EXATAMENTE como fazer um exercício, pule para o próximo.

Por fim, uma sugestão: sempre que possível, estude (ou ao menos leia) o "essencial" da aula antes da aula, pois isto tornará ~~possivelmente~~ as aulas bem mais proveitosas para você – e para mim.

[0] A principal razão é o propósito: [14] se destina a estudantes que pretendem estudar (!) o assunto de maneira independente, sem vínculo com o cronograma de uma disciplina de graduação.

[1] Algumas discussões realizadas nas seções extras serão importantes para o desenrolar de outras seções essenciais. Tais ocorrências serão devidamente indicadas, não se preocupe.

Capítulo 0

A reta real

Intuitivamente, a *reta real* é um objeto geométrico: um *segmento retilíneo sem saltos*, i.e., *contínuo*. Por outro lado, como segmentos dessa reta podem ser *somados* (copiados e justapostos) e *multiplicados*[0], segue que a reta também é um objeto *algébrico*. Daí, uma pergunta natural a se fazer é: como conciliar as duas noções a fim de *descrever*, matematicamente, a reta real?

A resposta usual faz uso da *linguagem de conjuntos*: a reta real será definida como *um conjunto* (de pontos), cujos *aspectos geométricos* desejados serão abstraídos por uma *relação de ordem* que deverá capturar, de alguma forma, as noções de *linearidade* e *continuidade*; os *aspectos algébricos*, por sua vez, serão descritos por meio de *operações binárias* que imitarão as operações usuais que aprendemos na *escola*. Nesta parte do curso lidaremos com todos esses aspectos, a fim de entender a definição matemática da reta real.

0.0 Linguagem: revisão de conjuntos e funções

0.0.0 Essencial

Conjuntos

A palavra "conjunto" é uma daquelas típicas expressões (*atômicas*) que não se explicam por meio de outras expressões mais simples, como *tempo*, *espaço*, *ser*, etc. Costuma ficar a cargo da (vida em) sociedade ensinar o significado dessas coisas: no caso, conjuntos podem ser entendidos como *agrupamentos de objetos* ou *coleções de indivíduos* que partilham algum tipo de característica comum num certo contexto. **Exemplos**: conjunto das pessoas numa sala, conjunto dos torcedores de um time, conjunto dos times de algum esporte coletivo num campeonato, conjunto dos campeonatos desse esporte coletivo, etc. Porém, usaremos tais noções em contexto matemático, e trataremos apenas de conjuntos formados por objetos de natureza matemática.

Dados *objetos matemáticos* x e A, vamos assumir que apenas dois casos podem ocorrer (e necessariamente um deles ocorrerá):"$x \in A$" (lido como "x pertence a A", "x é elemento de A" ou "x é membro de A") ou o contrário, indicado por "$x \notin A$" (lido como "x não pertence a A", "x não é elemento de A" ou "x não é membro de A"). **Porém, como não se define explicitamente o que significa *ser* conjunto** e, muito menos, o que é a relação de pertinência "$\in$", precisa-se, pelo menos, indicar os comportamentos esperados.

[0]Como feito por Descartes na infância da Geometria Analítica. Para saber mais, confira a obra de Tatiana Roque [15].

Definição 0.0.0. Para conjuntos A e B:

(i) escreveremos "$A \subseteq B$" para abreviar a afirmação "para todo x, se $x \in A$, então $x \in B$", lida como "A é **subconjunto** de B", ou "A **está contido em** B";

(ii) escreveremos "$A \not\subseteq B$" para abreviar a negação de "$A \subseteq B$", i.e., para indicar que "existe $x \in A$ tal que $x \notin B$";

(iii) escreveremos "$A \subsetneq B$" para abreviar "$A \subseteq B$ e $A \neq B$" e, em tais situações, diremos que A é **subconjunto próprio** de B. ¶

Axioma da Extensão. *Dois conjuntos são iguais se, e somente se, têm os mesmos elementos. Em notação mais econômica:* $A = B \Leftrightarrow (A \subseteq B)$ *e* $(B \subseteq A)$.

Exercício 0.0 ($\star$)**.** Sejam A o conjunto dos números inteiros pares, B o conjunto dos números inteiros múltiplos de 3 e C o conjunto dos números inteiros múltiplos de 6. Determine as relações de inclusão entre A, B e C. ■

Entre outras coisas, o exercício acima indica que precisamos de um modo mais prático para *descrever* conjuntos. A seguir, listam-se modos comuns de descrever o conjunto A do exercício anterior:

- $A = \{x : x \in \mathbb{Z} \text{ e } x \text{ é par}\}$;
- $A = \{x \in \mathbb{Z} : x \text{ é par}\}$;
- $A = \{x \in \mathbb{Z} : \text{existe } n \in \mathbb{Z} \text{ tal que } x = 2n\}$;
- $A = \{2z : z \in \mathbb{Z}\}$.

Em geral, ao descrever um conjunto no formato

$$\underbrace{\{\dots}_{1^{\underline{a}} \text{ parte}} : \underbrace{\dots\}}_{2^{\underline{a}} \text{ parte}}$$

entende-se que o conjunto considerado é formado pelos elementos que satisfazem o que se escreve na primeira parte, **tais que** as condições impostas na segunda parte são satisfeitas. Assim, na primeira descrição de A, entende-se que seus elementos são todas as coisas (já que não há restrições) que são números inteiros pares (a condição imposta na segunda parte). Analogamente, na segunda descrição, A é descrito como a coleção de todos os números inteiros (como imposto na primeira parte) que são pares (já que está é a condição da segunda parte).

Exercício 0.1 ($\star$)**.** Descreva os conjuntos B e C do exercício anterior nos formatos acima. ■

Observação 0.0.1. É comum encontrar a notação "$\{\dots \mid \dots\}$" em vez de "$\{\dots : \dots\}$". Você pode usá-la em seus exercícios, desde que não implique com a minha forma de escrever, padrão nos textos de Teoria dos Conjuntos, e que será adotada aqui. △

Outra alternativa prática de descrição, geralmente utilizada para conjuntos *finitos*[1], consiste em listar os elementos do conjunto. Por exemplo: para $S := \{a, 4, \triangle\}$, temos $a \in S$, $4 \in S$ e $\triangle \in S$, enquanto $0 \notin S$, $\nabla \notin S$ etc. Importante destacar o uso do símbolo "$:=$" acima: a ideia é usá-lo para indicar que S foi "definido" ou "declarado" como o conjunto escrito após o símbolo "$:=$". Para ilustrar, observe que no próximo exercício faz sentido usar "$=$" pois S já foi declarado acima.

[1]Finitude é um tópico que será discutido ainda neste capítulo.

Exercício 0.2 ($\star$)**.** Mostre que $S = \{\triangle, 4, a\}$. ■

Preciosismos à parte[2], o exercício acima indica que a ordem em que os elementos de um conjunto são descritos é irrelevante. É por essa razão que conjuntos do tipo $\{a, b\}$ são chamados de **pares não-ordenados**.

Exercício 0.3 ($\star$)**.** Mostre que $\{x, x\} = \{x\}$ para qualquer x. **Observação**: por conta deste resultado, é de "bom tom" não grafar duas vezes o mesmo elemento ao descrever um conjunto com a notação "$\{\dots\}$". ■

Exercício 0.4 ($\star$)**.** Descreva o conjunto $\{0, 1\}$ por meio da notação $\{\dots : \dots\}$. ■

A fim de encerrar esta primeira parte da revisão, a próxima definição trás o restante das notações e operações usuais entre conjuntos.

Definição 0.0.2.

(i) Denota-se $\emptyset \coloneqq \{x : x \neq x\}$, *coleção* que será chamada de **conjunto vazio** por razões *óbvias*: não existe x com $x \in \emptyset$, já que o contrário daria $x \neq x$.

(ii) Para X e Y conjuntos, considera-se $X \setminus Y \coloneqq \{x \in X : x \notin Y\}$, que denota a **diferença** entre X e Y, também chamada de **complementar de Y em X**.

(iii) Para conjuntos A e B, $A \cap B \coloneqq \{x : x \in A \text{ e } x \in B\}$ e $A \cup B \coloneqq \{x : x \in A \text{ ou } x \in B\}$ denotam os conjuntos chamados, respectivamente, de **interseção** e (**re**) **união** dos conjuntos A e B. Em particular, A e B são **disjuntos** se $A \cap B = \emptyset$. ¶

Observação 0.0.3. Lembre-se: na linguagem comum, "e" funciona como um *agregador*, enquanto "ou" indica *alternativa*: por exemplo, os pontos da reta nos intervalos $(-\infty, 1)$ *e* $(3, +\infty)$ constituem a solução da inequação $x^2 - 4x + 3 > 0$, o que em linguagem de conjuntos se expressa por meio da reunião $(-\infty, 1) \cup (3, +\infty)$. No entanto, **não** faz sentido dizer que tal reunião é composta por todo x tal que $x \in (-\infty, 1)$ **e** $x \in (3, +\infty)$, pois este "e" (da linguagem matemática usual) indica *simultaneidade* – e não há x com as duas propriedades *ao mesmo tempo*: o correto é dizer que $x \in (-\infty, 1)$ **ou** $x \in (3, +\infty)$. Cabe ainda destacar que o "ou" matemático não é exclusivo: sempre que dissermos "$x \in A$ ou $x \in B$", deve-se entender que *pelo menos* um dos casos deve ocorrer, o que não inviabiliza a ocorrência de ambos. △

Proposição 0.0.4. *Para todo conjunto A ocorre $\emptyset \subseteq A$.*

Demonstração. Dado x qualquer, a implicação "$x \in \emptyset \Rightarrow x \in A$" é verdadeira por *vacuidade*, já que "$x \in \emptyset$" é falso. Alternativamente: se a *inclusão* fosse falsa, deveria existir $x \in \emptyset$ com $x \notin A$, mas não existe $x \in \emptyset$, absurdo[3]. □

Observação 0.0.5 (Contido vs. pertence)**.** Cuidado para não confundir *pertinência* e *continência*:

- "$x \in y$" significa que "x" é um dos elementos de "y";
- "$x \subseteq y$" significa que "todo elemento de x é também elemento de y".

[2]Ninguém reprovará na matéria por escrever "=" em vez de "$\coloneqq$". CALMA.

[3]Por exemplo: a sentença "todas as piscinas da minha casa são olímpicas" é verdadeira se a minha casa não tiver piscinas.

Assim, embora $\emptyset \subseteq A$ ocorra para qualquer conjunto A, nem sempre ocorre $\emptyset \in A$. Na verdade, fora de contextos mais formais, é raro que se tenha $\emptyset \in A$. Veja que, por exemplo, $\emptyset \notin \emptyset$, já que o contrário é dizer que $\emptyset$ tem um elemento. Mesmo assim, $\emptyset \subseteq \emptyset$. A raiz dessa confusão é, possivelmente, oriunda do fato de que muitas vezes se diz "y contém x" a fim de expressar "$x \in y$". △

Exercício 0.5 ($\star$)**.** Convença-se de que $\emptyset \neq \{\emptyset\}$. ■

Exercício 0.6 ($\star$)**.** Sejam A, B e C conjuntos. Mostre as identidades, inclusões, equivalências e implicações a seguir.

a) $A \cup B = B \cup A$ e $A \cap B = B \cap A$.

b) $A \cup (B \cup C) = (A \cup B) \cup C$ e $A \cap (B \cap C) = (A \cap B) \cap C$.

c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

d) $A \subseteq A$, $A \subseteq B$ e $B \subseteq C \Rightarrow A \subseteq C$.

e) $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.

f) $A \subseteq B \Rightarrow C \setminus B \subseteq C \setminus A$.

g) $A \setminus B = \emptyset \Leftrightarrow A \subseteq B$.

h) $A \setminus A = \emptyset$, $A \setminus \emptyset = A$ e $A \setminus (A \setminus B) = A \cap B$.

i) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$. ■

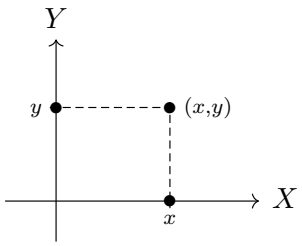
Funções

O advento das *funções*, seja por invenção ou descoberta, deflagrou uma das maiores mudanças de paradigma na Matemática por permitir incorporar as noções de movimento e variação aos *modelos* que, até então, tratavam apenas de situações estáticas e posicionais. Embora hoje se apresente como um conceito simples, alguns séculos separam as primeiras menções explícitas às funções da "definição" apresentada por Dedekind na segunda metade do Século XIX:

Conceito de função. *Uma função é uma regra f que associa cada elemento x de um conjunto X a um único elemento $f(x)$ de um conjunto Y.*

Se, por um lado, a conceituação acima parece englobar os casos clássicos aprendidos na infância (funções *polinomiais*, *trigonométricas*, etc.), por outro lado ela empurra para debaixo do tapete a definição de "regra". Um modo mais honesto consiste em apelar para *pares ordenados*.

Diferente do que ocorre no caso não-ordenado, em que $\{a, b\} = \{b, a\}$ mesmo com $a \neq b$, pode-se *convencionar* escrever (a, b) com o intuito de ter o seguinte comportamento: $(a, b) = (c, d)$ se, e somente se, $a = c$ e $b = d$. Com tal *dispositivo*, usualmente xingado de **par ordenado**, passa a fazer sentido definir o **produto cartesiano** $X \times Y \coloneqq \{(x, y) : x \in X \text{ e } y \in Y\}$ entre os conjuntos X e Y, cujos membros são todos os pares ordenados da forma (x, y) com $x \in X$ e $y \in Y$: noutras palavras, $X \times Y$ apenas abstrai um típico plano *cartesiano*.



Dado que um par ordenado (x, y) pode ser interpretado como uma *mini-regra* que faz sua *primeira coordenada* x corresponder à sua *segunda coordenada* y, é natural pensar em *regras* que associam elementos de X a Y como subconjuntos de $X \times Y$.

Definição 0.0.6 (Bourbaki, 1939)**.** Uma **função** (ou **mapa** ou **aplicação**) **de** X **em** Y é um subconjunto $f \subseteq X \times Y$ tal que:

(i) para todo $x \in X$ existe $y \in Y$ com $(x, y) \in f$ (cada x se associa a pelo menos um y);

(ii) se $(x, y), (x, z) \in f$, então $y = z$ (o y associado a x é único).

Escreve-se $f\colon X \to Y$ ou $X \xrightarrow{f} Y$ para indicar que f é uma função de X em Y. ¶

Acima, o conjunto X costuma ser chamado de **domínio** da função f, enquanto Y é o seu **codomínio** (também chamado de *contradomínio*). Uma vez que a cada $x \in X$ corresponde um único $y \in Y$ com $(x, y) \in f$, faz sentido atribuir a y uma notação que remeta ao elemento x: no caso, faz-se $y \coloneqq f(x)$ (ou ainda $x \overset{f}{\mapsto} f(x)$), e xinga-se $f(x)$ de **imagem de** x pela função f. Por sua vez, o subconjunto de Y formado por todos os elementos da forma $f(x)$, conforme x *varia* em X, é chamado de **imagem da função**, e denotado por $\operatorname{im}(f)$. Em símbolos: $\operatorname{im}(f) \coloneqq \{f(x) : x \in X\}$.

Exemplo 0.0.7 (Funções polinomiais)**.** Dado um *polinômio na indeterminada* t, i.e., uma *expressão* da forma $a_0 + a_1 t + \ldots + a_n t^n$, com $n \in \mathbb{N}$ e *números reais*[4] $a_0, \ldots, a_n$, onde t indica apenas um símbolo *indeterminado*, que abreviaremos com $p(t)$, passa a fazer sentido substituir cada ocorrência de "t" na expressão $p(t)$ por um *número real* x fixado, o que *produz* o *número real*

$$p(x) \coloneqq a_0 + a_1 x + \ldots + a_n x^n.$$

Dessa forma, pode-se dizer que $p \coloneqq \{(x, p(x)) : x \in \mathbb{R}\}$ relaciona cada $x \in \mathbb{R}$ ao número $p(x) \in \mathbb{R}$. Uma vez que tal associação é claramente *funcional*[5], ganha-se uma função $p\colon \mathbb{R} \to \mathbb{R}$, que faz $x \mapsto p(x)$ para cada $x \in \mathbb{R}$. Funções desse tipo são chamadas de (funções) **polinomiais**. ▲

Exemplo 0.0.8 (Funções racionais)**.** Mais geralmente, consideram-se expressões da forma $r(t) \coloneqq \frac{p(t)}{q(t)}$ em que ambos $p(t)$ e $q(t)$ são polinômios na indeterminada t. Desta vez, só faz *sentido* substituir "t" em $r(t)$ por um número real x fixado nas situações em que se garantir $q(x) \neq 0$, pois a divisão por 0 não é realizável em *corpos*. Assim, a expressão $r(t)$ induz uma função r cujo domínio é $\{x \in \mathbb{R} : q(x) \neq 0\}$, e que faz $r(x) \coloneqq \frac{p(x)}{q(x)}$ para cada x no domínio de r. Funções assim costumam ser chamadas de (funções) **racionais**. ▲

[4]Formalmente ainda não definimos o que é um número real. No entanto, você já fez Cálculo I. De modo geral, os exemplos farão uso de informações que nós já sabemos como são, embora ainda não estejam implementadas formalmente na disciplina. O Elon faz isso e ninguém reclama, então não é agora que isso vai virar um problema, certo?

[5]No sentido de que se $(x, y), (x, z) \in p$, então $y = z$.

Exercício 0.7 ($\star$)**.** Para funções f e g de X em Y, mostre que $f = g$ se, e somente se, $f(x) = g(x)$ para todo $x \in X$. ■

Definição 0.0.9. Se $f\colon X \to Y$ e $g\colon Y \to Z$ são funções, então fica *bem definida* uma função $g \circ f\colon X \to Z$ dada pela identidade

$$(g \circ f)(x) \coloneqq g \circ f(x) \coloneqq g(f(x)),$$

para todo $x \in X$, chamada de (função) **composta** (ou **composição**) entre f e g, em geral denotada apenas por $g \circ f$. ¶

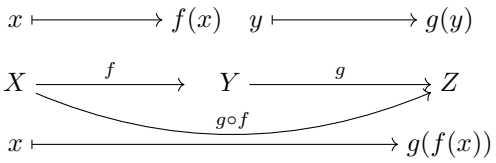


Figura 0.0: Esquematicamente, f vem antes de g, já que as setas costumam sair da direita para esquerda, no sentido de nossa escrita. Por outro lado, para descrever a regra da composição, precisamos escrever g primeiro, já que os cálculos são feitos "de dentro para fora": primeiro calcula-se $f(x)$, para daí calcular $g(f(x))$. Note que, apesar disso, as duas notações indicam a mesma coisa.

A definição acima faz sentido pois $f(x) \in Y$ para todo $x \in X$ e $Y = \operatorname{dom}(g)$, de modo que g *sabe* o que *fazer* com $f(x)$. Um pouco mais formalmente, podemos definir

$$g \circ f \coloneqq \{(x, z) \in X \times Z : g(f(x)) = z\},$$

que satisfaz as condições para ser uma função do tipo $X \to Z$:

- ✓ para cada $x \in X$ existe $z \in Z$ tal que $(x, z) \in g \circ f$, basta tomar $z \coloneqq g(f(x))$;
- ✓ se $(x, z), (x, z') \in g \circ f$, então $z = z'$ já que $z = g(f(x)) = z'$.

Exercício 0.8 ($\star$)**.** Sejam $f\colon W \to X$, $g\colon X \to Y$ e $h\colon Y \to Z$ funções. Mostre que as funções $h \circ (g \circ f)$ e $(h \circ g) \circ f$ são iguais. ■

Exercício 0.9 ($\star$)**.** Para um conjunto X, escreve-se $\mathrm{Id}_X\colon X \to X$ para denotar a **função identidade de** X, definida por $\mathrm{Id}_X(x) \coloneqq x$ para cada x em X. Mostre que $f \circ \mathrm{Id}_X = f$ para qualquer função f cujo domínio é X e $\mathrm{Id}_X \circ g = g$ para qualquer função g cujo codomínio é X.■

0.0.1 Extras

Análise para quê?

Os números naturais foram criados por Deus, todo o resto é trabalho da humanidade.

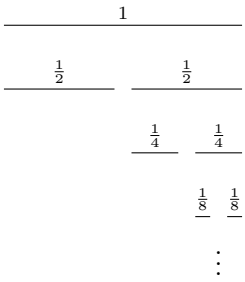
Leopold Kronecker (1886).

Faz parte do folclore matemático atribuir a frase anterior ao algebrista Leopold Kronecker (1823-1891), como uma síntese de seu ceticismo perante os diversos métodos *infinitários* e não-construtivos que se propagaram na Matemática a partir da segunda metade do Século XIX [4]. Longe de ser uma mera declaração teológica, ela expressa a confiabilidade que temos diante dos *métodos aritméticos* usuais, explicitamente ancorados na (aparente?) realidade imediata, em contraponto aos argumentos do *Cálculo*, que frequentemente dependem de suposições incomuns ao nosso cotidiano intrinsecamente *finito*, como no caso das *séries*.

Considere, por exemplo, a série

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} + \ldots \qquad (\dagger)$$

que manifesta a ideia de somar iteradamente parcelas da forma $\frac{1}{2^n}$ conforme toma-se n cada vez maior. Embora possa parecer artificial, esse tipo de animal surge naturalmente em problemas que envolvem o *cálculo* de áreas *curvilíneas*, por meio do chamado *método da exaustão*[6]. O ponto a chamar atenção, porém, é o seguinte: embora cada estágio finito desse processo seja facilmente calculável, não é completamente óbvio o que poderia *significar* realizar uma soma com infinitas parcelas.



Com argumentos aritmético-geométricos do tipo ilustrado acima, é razoável *convencionar* que o valor para (†) (seja lá qual for) deve corresponder ao *número* para o qual as *somas parciais* se *dirigem*: no caso, tal número *deveria* ser 1, já que $1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = \cdots$ Ainda assim, trata-se de uma convenção ou definição: não há vida suficiente para efetuar *todas* as somas e verificar uma igualdade legítima.

Agora, o que significa dizer que tais somas parciais se dirigem para algum valor? Além disso, o que impediria que certas somas se dirigissem para números diferentes? Mais ainda, como determinar os valores de tais somas infinitas?

Evidentemente, nada impede que tais perguntas sejam respondidas de forma vaga e intuitiva – ou apenas ignoradas. No caso da série proposta, por exemplo, um argumento muito comum para justificar as estimativas sem muito esforço (abanando as mãos) é o seguinte: ao escrever $S := \sum_{n=1}^{\infty} \frac{1}{2^n}$, chega-se a

$$2S = 2 \cdot \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots \right) = 1 + \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots \right) = 1 + S$$

e, consequentemente, $S = 1$, justamente o que o raciocínio intuitivo geométrico sugeria!

Não é difícil adaptar o *método* para mostrar que $\sum_{n=1}^{\infty} \frac{1}{3^n} = \frac{1}{2}$, $\sum_{n=1}^{\infty} \frac{1}{4^n} = \frac{1}{3}$ e, mais geralmente, $\sum_{n=1}^{\infty} \frac{1}{m^n} = \frac{1}{m-1}$ sempre que $m > 1$, identidades compatíveis com suas respectivas interpretações geométricas. O que acontece, porém, ao aplicar tal "metodologia" na determinação do valor da série $\sum_{n=1}^{\infty} 2^n$? Como antes, ao escrever $T := \sum_{n=1}^{\infty} 2^n$, chega-se a

$$2T = 4 + 8 + 16 + \ldots + 2^{n+1} + \ldots \Rightarrow 2T + 2 = 2 + 4 + 8 + \ldots = T \Rightarrow T = -2,$$

resultado que, desta vez, não parece *certo*, por discordar do que a interpretação geométrica sugere.

Finalmente encontramos uma pergunta mais inescapável do que as feitas um pouco acima: *por que o truque algébrico preguiçoso pareceu funcionar nos primeiros casos mas falhou no último?*

Responder a esse tipo de pergunta é, pelo menos historicamente, um dos papéis da Análise. Pode-se dizer que ela surgiu do processo natural de revisão metodológica, típico do *modus operandi* científico, no contexto do *Cálculo* de Leibniz-Newton. Embora, a princípio, tratasse-se de um movimento voltado a justificar (e expandir) os resultados da área com base em conceitos geométricos menos vagos, seus praticantes não tardaram a empregar a *linguagem de conjuntos* no processo de retraduzir e *sintetizar* o Cálculo a partir de noções aparentemente tão sólidas quanto os números criados pelo deus de Kronecker.

[6] É o que está por trás das ideias de *integração* que você estudou em Cálculo I.

Fundamentos debaixo do tapete

Conjuntos e, mais geralmente, *objetos matemáticos*, não existem da mesma forma que as entidades físicas existem. Por mais que você procure na sua casa ou em qualquer outro lugar, você nunca encontrará *o número 2*, por exemplo. É claro que você pode encontrar símbolos, desenhos ou pinturas que remetam ao *número 2*, mas nunca *o* próprio número 2, já que este é uma ideia, a abstração de um conceito. Dessa forma, diferente de alguém na Biologia ou na Geologia, cujos objetos de estudo são palpáveis e facilmente detectáveis, na Matemática é preciso tomar mais cuidado.

Conforme a Matemática se desenvolveu e amadureceu ao longo dos milênios, chegou-se ao consenso de utilizar *o método axiomático*. Na prática, isto consiste em assumir como válidas algumas afirmações básicas que parecem razoáveis o bastante para serem entendidas como "verdadeiras", e a partir delas deduzir "todo o resto". Como a discussão anterior indicou, isto é relativamente desnecessário para questões matemáticas corriqueiras, mas se torna indispensável quando problemas menos usuais entram em cena. Concomitantemente, a adaptabilidade dos conjuntos favoreceu o seu uso em praticamente todas as áreas da Matemática. Mas, novamente: conjuntos não existem.

Nesse sentido, há basicamente dois axiomas sobre conjuntos que as pessoas utilizam em seus primeiros contatos com o tema: o Axioma da Extensão, já postulado no começo da seção, e o Axioma da Abstração. Este último é usado implicitamente sempre que se emprega a notação $\{\dots:\dots\}$. Grosso modo, postula-se o seguinte: dada uma *propriedade* $\mathcal{P}$, existe o conjunto $\{x : x \text{ tem a propriedade } \mathcal{P}\}$. É claro que isto deixa o problema de explicar o que é *propriedade*, mas a intuição basta para a discussão: tudo o que se definiu na seção anterior poderia ser justificado por meio desses dois axiomas, até mesmo pares ordenados!

Exercício 0.10 $(^{\star}_{\star\star})$**.** Para x e y quaisquer, defina $(x, y) \coloneqq \{\{x\}, \{x, y\}\}$. Mostre que para a, b, c e d quaisquer, $(a, b) = (c, d)$ se, e somente se, $a = c$ e $b = d$. ■

Com um pouco mais de paciência, não seria difícil ver que funções podem ser interpretadas como conjuntos. Mais adiante, veremos que números também podem ser "definidos" via conjuntos, de modo que chega-se à conclusão inevitável: é razoável assumir, para propósitos formais, que tudo é conjunto. Do ponto de vista metodológico mencionado na página anterior, esta seria uma vitória enorme: a partir de dois axiomas básicos, *seríamos* capazes de justificar e reconstruir uma quantidade monumental de *fatos* matemáticos, o que tornaria bastante razoável aceitar as consequências menos intuitivas que encontrássemos pelo caminho. Contudo, há um problema.

Exercício 0.11 $(^{\star}_{\star\star})$**.** Considere $R \coloneqq \{x : x \notin x\}$. Mostre que $R \in R$ se, e somente se, $R \notin R$.■

O Axioma da Abstração diz que R deveria *existir*. Porém, se R existir, chega-se a uma contradição, pois tanto $R \in R$ quanto sua negação devem ocorrer simultaneamente.

Uma das soluções encontradas para resolver tal problema, conhecido como Paradoxo de Russell, foi abandonar o Axioma da Abstração e, em seu lugar, assumir o Axioma da Separação que, grosso modo, postula o seguinte: dada uma *propriedade* $\mathcal{P}$ e um conjunto A, existe o conjunto $\{x \in A : x \text{ tem a propriedade } \mathcal{P}\}$. Assim, em vez de assumir a habilidade irrestrita de definir conjuntos, supõe-se apenas a capacidade de determinar *subconjuntos* de conjuntos previamente conhecidos. O preço disso é que a lista de axiomas precisou ser estendida. Contudo, tais axiomas não serão abordados aqui – com exceção do Axioma da Escolha. Para saber mais, você pode conferir a referência [13].

0.1 Injeções, sobrejeções e a noção de cardinalidade

0.1.0 Essencial

Revisão: funções injetoras, sobrejetoras e bijetoras

Definição 0.1.0. Uma função $f\colon X \to Y$ será dita:

(i) **injetora** (ou *injetiva*, *injeção*, etc.) se para quaisquer $x, x' \in X$, a ocorrência de $f(x) = f(x')$ acarretar $x = x'$;

(ii) **sobrejetora** (ou *sobrejetiva*, *sobrejeção*, *sobre* Y, etc.) se $\operatorname{im}(f) = Y$ e

(iii) **bijetora** (ou *bijetiva*, *bijeção*, etc.) se $f\colon X \to Y$ for injetora e sobrejetora. ¶

Para aquecer, você pode começar com o próximo

Exercício 0.12 ($\overset{\star}{\star}$)**.** Sejam $f\colon X \to Y$ e $g\colon Y \to Z$ funções.

a) Mostre que se g e f são injetoras, então $g \circ f$ é injetora.

b) Mostre que se g e f são sobrejetoras, então $g \circ f$ é sobrejetora.

c) Conclua que se g e f são bijetoras, então $g \circ f$ é bijetora.

Bijeções estão intimamente ligadas com a noção de *invertibilidade*[7] para funções.

Definição 0.1.1. Dizemos que uma função $g\colon Y \to X$ é *uma* **inversa** de $f\colon X \to Y$ se $f \circ g = \mathrm{Id}_Y$ e $g \circ f = \mathrm{Id}_X$. A função f é **invertível** se tem uma inversa. ¶

Observação 0.1.2. Na prática, dizer que g é *uma* inversa de f equivale a dizer que $g\colon Y \to X$ satisfaz o seguinte

$$\text{para quaisquer } x \in X \text{ e } y \in Y,\ g(y) = x \Leftrightarrow f(x) = y. \tag{0.0}$$

De fato, se g é *uma* inversa de f, então a condição acima é satisfeita: por um lado, se $g(y) = x$, então $f(g(y)) = f(x)$, com $f(g(y)) = y$ pois $f \circ g = \mathrm{Id}_Y$ vale por hipótese; por outro lado, se $f(x) = y$, então $g(f(x)) = g(y)$, com $g(f(x)) = x$ pois $g \circ f = \mathrm{Id}_X$ vale por hipótese. Reciprocamente, se $g\colon Y \to X$ satisfaz a condição (0.0), então valem as identidades $g \circ f = \mathrm{Id}_X$ e $f \circ g = \mathrm{Id}_Y$: para a primeira, note que se $f(x) = y$, então (0.0) assegura $g(y) = g(f(x)) = x$; a segunda é *análoga*[8]. △

Em outras palavras, *uma* inversa de g desfaz tudo o que f faz. Como consequência:

Exercício 0.13 ($\star$)**.** Mostre que uma inversa, se existir, é única, ou seja: se g e g' são inversas de f, então $g = g'$. ■

Em certo sentido, o resultado acima diz que a inversa de uma função f fica completamente determinada por f (caso exista). Por isso, é comum indicá-la de modo a fazer alusão à função f: neste caso, a notação mais comum para a inversa de f é f^{-1}.

Exemplo 0.1.3. A função $f\colon \mathbb{Z} \to \mathbb{Z}$ dada por $f(z) := z + 1$ tem inversa dada por $g(z) := z - 1$. De fato,

$$g(f(z)) = f(z) - 1 = z + 1 - 1 = z \quad \text{e} \quad f(g(z)) = g(z) + 1 = z - 1 + 1 = z.$$

Futuramente, veremos que a função exponencial $\exp\colon \mathbb{R} \to (0, +\infty)$ tem a função logaritmo $\ln\colon (0, +\infty) \to \mathbb{R}$ como inversa: de suas aulas de Cálculo I, você deve se lembrar de que $e^x = y$ se, e somente se, $\ln(y) = x$. Compare isso com a condição (0.0). ▲

Exemplo 0.1.4. A função $h\colon \mathbb{Z} \to \mathbb{Z}$ dada por $h(z) := z^2$ não é invertível: por valer $h(-1) = h(1) = 1$, não pode haver g satisfazendo (0.0), pois $g(1)$ seria simultaneamente igual a -1 e 1. Em particular, note que h não é injetora e nem sobrejetora. ▲

O que tudo isso tem a ver com bijeções?

Proposição 0.1.5. *Uma função $f\colon X \to Y$ é bijetora se, e somente se, é invertível.*

[7] O verbo é "inverter" e não "inverser".

[8] Afirmações dessa natureza devem ser encaradas como exercícios do tipo ($\star$).

Demonstração. Assumindo que f é bijetora, vamos definir uma função $g\colon Y \to X$ que provaremos ser a inversa de f. Não há muito o que fazer: vamos definir

$$g := \{(y, x) \in Y \times X : f(x) = y\}.$$

Por f ser sobrejetora, para todo $y \in Y$ existe $x \in X$ tal que $f(x) = y$. Logo, para todo $y \in Y$ existe $x \in X$ tal que $(y, x) \in g$. Agora, se $(y, x), (y, x') \in g$, então $f(x) = f(x')$ (por quê?)*, donde a injetividade de f assegura $x = x'$. Isto mostra que g é função de $Y \to X$. Para verificar que g é a inversa de f, basta notar que g satisfaz a condição (0.0) da Observação 0.1.2 por construção.

A recíproca, isto é, "se $f\colon X \to Y$ é invertível, então f é bijetora", é consequência do próximo exercício. □

Exercício 0.14 ($\overset{\star}{\star}$)**.** Sejam $f\colon X \to Y$ e $g\colon Y \to Z$ funções.

a) Mostre que se $g \circ f$ é injetiva, então f é injetiva.

b) Mostre que se $g \circ f$ é sobrejetora, então g é sobrejetora.

c) Conclua que se $Z := X$ e $g := f^{-1}$, então f é bijetora. ■

Corolário 0.1.6. *Se $f\colon X \to Y$ é bijeção, então $f^{-1}\colon Y \to X$ é bijeção.*

A noção de cardinalidade

Os tipos de função discutidos no começo da seção permitem comparar o *tamanho* dos conjuntos de modo bastante prático.

Definição 0.1.7. Diremos que dois conjuntos **têm a mesma cardinalidade** ("quantidade de elementos") se existir uma bijeção entre os dois. ¶

Figura 0.1: É evidente que há tantos círculos quanto quadrados, mesmo sem saber *quantos*.

Proposição 0.1.8. *Sejam A, B e C conjuntos.*

(i) *Existe uma bijeção de A para A.*

(ii) *Se existe uma bijeção de A para B, então existe uma bijeção de B para A.*

(iii) *Se existe uma bijeção de A para B e outra bijeção de B para C, então existe uma bijeção de A para C.*

Demonstração. O primeiro item segue por Id_A ser bijeção, enquanto o terceiro item decorre do fato de que a composição de bijeções é bijeção (Exercício 0.12). O segundo item é o Corolário 0.1.6. □

Intuitivamente, a proposição acima diz que ao escrever

$$A \approx B \Leftrightarrow \text{existe bijeção } A \to B,$$

define-se uma *relação binária*[9] entre conjuntos que se comporta, essencialmente, como a relação de igualdade: $A \approx A$, $B \approx A$ sempre que $A \approx B$ e $A \approx C$ sempre que $A \approx B$ e $B \approx C$. Esse tipo de coisa tem um nome: trata-se de uma *relação de equivalência*[10].

[9] Primeiro tópico da Subseção 0.1.1.

[10] Segundo tópico da Subseção 0.1.1.

Em vez de determinar quando dois conjuntos *têm* a mesma cardinalidade, podemos usar funções para detectar quando um conjunto tem *mais elementos* do que outro.

Definição 0.1.9. Para conjuntos X e Y, vamos fixar as seguintes notações:

(i) "$X \precsim Y$" será usada para indicar a existência de injeção $X \to Y$;

(ii) "$X \prec Y$" será usada para indicar "$X \precsim Y$" e "$X \not\approx Y$";

(iii) "$Y \succsim X$" será usada para indicar a existência de sobrejeção $Y \to X$;

(iv) "$Y \succ X$" será usada para indicar "$Y \succsim X$" e "$X \not\approx Y$". ¶

A semelhança com os símbolos "$\leq$" e "$<$" usualmente empregados no contexto de ordenação numérica é intencional: ela serve para nos lembrar que as propriedades de $\precsim$ e $\prec$ se parecem com as propriedades de $\leq$ e $<$, respectivamente. E de fato, tais relações realmente comparam as *cardinalidades* dos conjuntos.

Exercício 0.15 $(\overset{\star}{\star})$**.** Para conjuntos X, Y e Z, mostre que

a) $X \precsim X$;

b) se $X \precsim Y$ e $Y \precsim Z$, então $X \precsim Z$;

c) se $X \approx Y$, então $X \precsim Z$ se, e somente se, $Y \precsim Z$.

Faça o mesmo trocando $\precsim$ por $\prec$, $\succsim$ e $\succ$. ■

Formalmente, tais relações remetem às ordens que serão abordadas na próxima seção. Todavia, com a terminologia que será utilizada, $\precsim$ não pode satisfazer a *antissimetria* para conjuntos: existem conjuntos X e Y com $X \neq Y$ tais que $X \precsim Y$ e $Y \precsim X$ (dê exemplos)*. Isto ocorre pois $\precsim$ é uma ordem não sobre os conjuntos, mas sobre suas *cardinalidades*.

Teorema 0.1.10 (Cantor-Bernstein)**.** *Se $X \precsim Y$ e $Y \precsim X$, então $X \approx Y$, i.e., se existem injeções da forma $X \to Y$ e $Y \to X$, então existe bijeção $X \to Y$.*

O resultado acima é uma banalidade nas situações em que X e Y são *finitos*: como veremos, em tais situações, $X \precsim Y$ se, e somente se, o *número de elementos de* X, digamos m, é menor do que ou igual ao *número de elementos de* Y, digamos n, de modo que a ocorrência simultânea de $Y \precsim X$ acarreta a desigualdade oposta $n \leq m$, resultando em $m = n$. Com isso dito, note que o enunciado não menciona números ou *finitude*, que ainda não foram formalmente introduzidos. O fato de ser possível demonstrá-lo no contexto que se desenrola pode ser interpretado como um indicativo de que as definições adotadas cumprem bem o papel de abstrair a noção de cardinalidade. Sua demonstração, porém, será postergada (cf. Subseção 0.4.1): há questões mais urgentes a serem discutidas.

Exercício 0.16 $(\overset{\star}{\star\star})$**.** Usando o Teorema de Cantor-Bernstein, mostre que $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$. ■

0.1.1 Extras

Relações binárias e inversas

Definição 0.1.11. Dados conjuntos X e Y, uma **relação** (**binária**) R entre X e Y é um subconjunto de $X \times Y$.

(i) Para um par $(x, y) \in X \times Y$, escreve-se $x \, R \, y$ para indicar que o par (x, y) é membro da relação R, enquanto x e y são ditos R**-relacionados**. A ocorrência de $(x, y) \notin R$ será indicada por $x \not R \, y$.

(ii) O **domínio** da relação R é o conjunto $\mathrm{dom}\,(R) \coloneqq \{x : \text{existe } y \in Y \text{ com } x \, R \, y\}$.

(iii) A **imagem** da relação R é o conjunto $\mathrm{im}\,(R) \coloneqq \{y : \text{existe } x \in X \text{ com } x \, R \, y\}$.

Quando $X = Y$, diz-se apenas que R é uma relação em X. ¶

Exemplo 0.1.12 (Relação de igualdade)**.** Fixado um conjunto X, $\Delta_X := \{(x, y) \in X \times X : x = y\}$ é chamada de *relação de igualdade* em X. Daí, de acordo com a definição anterior, pode-se escrever $x\,\Delta_X\,y$ para indicar que $(x, y) \in \Delta_X$, i.e., $x = y$. ▲

Exemplo 0.1.13 (Partes e inclusão)**.** Fixado um conjunto X, faz sentido considerar a *coleção* de *todos os subconjuntos de* X, denotada por $\wp(X)$ e chamada de **conjunto das partes de** X, simbolicamente: $\wp(X) := \{A : A \subseteq X\}$. Por exemplo:

(i) para $X := \emptyset$, $\wp(\emptyset) = \{\emptyset\}$, já que $\emptyset$ é o único subconjunto de $\emptyset$;

(ii) para $X := \{0, 2\}$, $\wp(X) = \{\emptyset, \{0\}, \{2\}, \{0, 2\}\}$, pois $\emptyset$ e X sempre são subconjuntos de X e, no caso, os demais subconjuntos possíveis são $\{0\}$ e $\{2\}$;

(iii) para $X := \mathbb{N}$, ocorre $\{0\}, \{1\}, \{2\}, \ldots, \{0, 1\}, \{0, 2\}, \ldots \in \wp(\mathbb{N})$, bem como $\{n : n \text{ é par}\}$, $\{n : n \text{ é ímpar}\}$, $\{n : n \text{ é primo}\}, \ldots \in \wp(\mathbb{N})$, além dos típicos $\emptyset, \mathbb{N} \in \wp(\mathbb{N})$. TODO subconjunto de $\mathbb{N}$ é, por definição, membro de $\wp(\mathbb{N})$; oportunamente, veremos que se trata de um conjunto bem grande.

De qualquer forma, para X fixado, a relação de inclusão entre subconjuntos de X define, como a frase sugere, uma relação binária $\subseteq$ na *família*[11] $\wp(X)$ de todos os subconjuntos de X: explicitamente, $\subseteq := \{(A, B) : A \subseteq B \subseteq X\}$. ▲

Exemplo 0.1.14 (*Curvas* e gráficos)**.** Em posse de *estruturas algébricas*, é possível utilizar expressões algébricas a fim de *relacionar variáveis*. Por exemplo, a *expressão polinomial* $x^2 + y^2 = 1$ induz a relação binária $S := \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$. Quando se representa $\mathbb{R} \times \mathbb{R}$ graficamente como o plano cartesiano usual, o subconjunto S *passa a corresponder* aos pontos do plano que *distam* precisamente 1 da origem $(0, 0)$.

Em particular, S *não* determina uma função da forma $\mathbb{R} \to \mathbb{R}$ pois para um mesmo $x \in \mathrm{dom}\,(S)$ existem $y, y' \in \mathrm{im}\,(S)$ distintos e relacionados a x: explicitamente, se $x^2 + y^2 = 1$, então $y^2 = x^2 - 1$ e, como veremos, em tal situação pode-se concluir apenas que $|y| = \sqrt{x^2 - 1}$, o que dá margem a $y = \sqrt{x^2 - 1}$ e $y' = -\sqrt{x^2 - 1}$, ambos relacionados ao mesmo x. ▲

Definição 0.1.15. Dada uma relação binária R, a **relação inversa** de R, denotada por R^{-1}, é a relação $R^{-1} := \{(y, x) : x\ R\ y\}$. ¶

Exercício 0.17 ($\overset{\star}{\star}$)**.** Para uma relação binária R, mostre que:

a) $x\ R\ y \Leftrightarrow y\ R^{-1}\ x$ para quaisquer x e y;

b) $\mathrm{dom}\,(R) = \mathrm{im}\left(R^{-1}\right)$;

c) $\mathrm{im}\,(R) = \mathrm{dom}\left(R^{-1}\right)$; e

d) $(R^{-1})^{-1} = R$. ■

Exercício 0.18 ($\overset{\star}{\star\star}$)**.** Supondo que $X = Y$ e $R \subseteq X \times X$, interprete geometricamente a definição de R^{-1} como sendo a "rotação" de R em torno da "diagonal" Δ_X. ■

Esta discussão permite revisar a noção de função inversa. Como toda função é uma relação binária, vemos que toda função $f\colon X \to Y$ admite uma *relação inversa* f^{-1}. Assim, a Proposição 0.1.5 estabelece critérios para que tal relação inversa seja uma função (no sentido de Bourbaki).

Relações de equivalência, partições e cardinais

Definição 0.1.16. Uma relação binária $\sim$ num conjunto X é dita uma **relação de equivalência** se $\sim$ for

(i) **reflexiva**, i.e., se para todo $x \in X$ ocorrer $x \sim x$,

(ii) **simétrica**, i.e., se para quaisquer $x, y \in X$, a ocorrência de $x \sim y$ acarretar $y \sim x$, e

(iii) **transitiva**, i.e., se para quaisquer $x, y, z \in X$, a ocorrência simultânea de $x \sim y$ e $y \sim z$ acarretar $x \sim z$.

Diremos também que x e y são $\sim$-**equivalentes** sempre que ocorrer $x \sim y$, com a omissão do sufixo "$\sim$" quando a relação estiver clara pelo contexto. ¶

[11] Não custa frisar: neste texto, "conjunto", "coleção" e "família" são tratados como sinônimos!

Uma relação de equivalência $\sim$ estabelece um critério por meio do qual objetos a princípio distintos podem ser vistos como iguais, ao mesmo tempo em que separa outros objetos distintos pelo mesmo critério. Dessa forma, não espanta que a *relação de igualdade* ($x \sim y$ se, e somente se, $x = y$) seja o exemplo óbvio de equivalência.

Exemplo 0.1.17 (Horóscopo)**.** Frequentemente, praticantes da (pseudociência chamada de) `Astrologia` fazem uso implícito das relações de equivalência. De fato, de um ponto de vista informal, signos determinam uma "relação de equivalência" no "conjunto" de todas as pessoas:

- ✓ toda pessoa tem o mesmo signo de si mesma;
- ✓ se P tem o mesmo signo de P', então P' tem o mesmo signo de P;
- ✓ se P tem o mesmo signo de P' e esta tem o mesmo signo de P'', então P e P'' têm o mesmo signo.

Se a coisa parasse por aí, a `Astrologia` seria inofensiva. No entanto, é comum encontrar asserções do tipo "o comportamento X é característico do signo Y", o que sugere duas alternativas: ou a afirmação é falsa, ou *toda pessoa* do signo Y apresenta o comportamento X. Esse tipo de máxima ajuda a entender um dos usos mais comuns das relações de equivalência: a simplificação. Com efeito, se tais afirmações *astrológicas* fossem verdadeiras, então para entender os padrões comportamentais de *toda a humanidade* bastaria estudar os comportamentos de doze *representantes*, um de cada signo, algo bem mais simples do que estimar o comportamento individual dos oito bilhões de habitantes do planeta. Por *sorte*, signos estimam tão somente as datas de nascimento de seus portadores. ▲

Exemplo 0.1.18 (Paridade)**.** Recordemo-nos de que os números naturais podem ser classificados como *pares* ou *ímpares*: **pares** são os múltiplos de dois, **ímpares** são os outros. Isso pode ser usado para determinar uma relação de equivalência $\sim$ em $\mathbb{N}$: $m, n \in \mathbb{N}$ serão ditos $\sim$-equivalentes se tiverem a mesma *paridade*. Assim, $0, 2, 4, 6, \ldots$ são $\sim$-equivalentes entre si, $1, 3, 5, 7 \ldots$ são $\sim$-equivalentes entre si, enquanto 0 e 1 não são $\sim$-equivalentes, por exemplo. Note que há certos comportamentos *algébricos* que não dependem dos números escolhidos, e sim de suas paridades: a soma de *quaisquer* dois *ímpares* é *par*, o produto entre quaisquer *ímpares* é *ímpar*, etc. Isto sugere a possibilidade de realizar operações diretamente com as *classes* dos pares e dos ímpares em vez de lidar com seus *infinitos* representantes. ▲

Exemplo 0.1.19 (Restos da divisão por n)**.** Para generalizar o exemplo anterior, pode-se considerar a seguinte relação binária: para $n \in \mathbb{N}$ fixado e $x, y \in \mathbb{N}$, escreveremos $x \sim_n y$ a fim de indicar que x e y têm o mesmo *resto* na *divisão* por n. Verificar que tal relação $\sim_n$ é reflexiva, simétrica e transitiva é um bom exercício para quem se lembra de como fazer divisões. Ocorre que, como antes, certos comportamentos algébricos não dependem dos representantes escolhidos: por exemplo, a soma de quaisquer dois números com resto 2 na divisão por 3 terá resto 1, enquanto o produto de quaisquer dois números com resto 1 na divisão por 3 ainda terá resto 1. ▲

Um efeito colateral inevitável das relações de equivalência é a segregação dos elementos do conjunto em *classes de equivalência*. Mais precisamente:

Definição 0.1.20. Para uma relação de equivalência $\sim$ sobre um conjunto X, diremos que o conjunto $\{y : x \sim y\}$ é a **$\sim$-classe de equivalência de** x. A notação varia com o contexto: é comum escrever $[x]$, $[x]_\sim$, $\pi(x)$, $\overline{x}$, etc. Na dúvida, convêm explicitar a notação que será usada no começo das discussões. ¶

Com *relação* aos exemplos anteriores:

(i) a classe de equivalência de uma pessoa P com respeito aos signos astrológicos seria a coleção de todas as pessoas que têm o mesmo signo de P, consequentemente, existem apenas doze classes de equivalência (correspondentes aos signos possíveis);

(ii) a classe de equivalência de um número $n \in \mathbb{N}$ com respeito à paridade é a coleção dos naturais que têm a mesma paridade de n; logo, existem apenas duas classes, a dos pares e a dos ímpares;

(iii) a classe de equivalência de um número $p \in \mathbb{N}$ com respeito aos restos da divisão por n é a coleção dos números naturais que têm o mesmo resto na divisão, o que leva à conclusão de que existem precisamente n classes de equivalência (correspondentes aos restos possíveis na divisão por n).

Para facilitar a discussão de como uma relação de equivalência *particiona* o seu domínio, vamos introduzir brevemente a generalização do conceito de reunião.

Definição 0.1.21. Para um conjunto $\mathcal{S}$, define-se $\bigcup \mathcal{S} := \{x : \text{existe } S \in \mathcal{S} \text{ com } x \in S\}$, a **reunião da família** $\mathcal{S}$. Nas ocasiões em que $\mathcal{S} := \{S_i : i \in \mathcal{I}\}$ para algum conjunto $\mathcal{I}$ fixado, também é comum escrever $\bigcup_{i \in \mathcal{I}} S_i$ ou $\bigcup_{i \in \mathcal{I}} S_i$. ¶

O dispositivo acima apenas cria um modo bastante esperto de evitar abominações notacionais como "$S_0 \cup S_1 \cup \ldots$" quando se quer expressar uma reunião (possivelmente) *infinita* de conjuntos. Fora isso, ela não traz novidades: note, por exemplo, que para $\mathcal{S} := \{X, Y\}$, tem-se $\bigcup \mathcal{S} = X \cup Y$.

Exercício 0.19 ($\star$)**.** Note mesmo, isto é: verifique! ■

Proposição 0.1.22. *Sejam X um conjunto e $\sim$ uma relação de equivalência sobre X. Ao denotar por C_x a $\sim$-classe de equivalência de x para cada $x \in X$, valem as afirmações:*

(*i*) *para todo $y \in X$, existe $x \in X$ com $y \in C_x$ (i.e., $X = \bigcup_{x \in X} C_x$);*

(*ii*) *para quaisquer $x, y \in X$ ocorre $C_x = C_y$ ou $C_x \cap C_y = \emptyset$;*

(*iii*) *para quaisquer $x, y \in X$, $C_x = C_y$ se, e somente se, $x \sim y$.*

Demonstração. O primeiro item decorre da reflexividade de $\sim$: como $y \sim y$, tem-se $y \in C_y$. Os dois itens seguintes seguem do próximo exercício. □

Exercício 0.20 ($\overset{\star}{\star\star}$)**.** Sejam $\sim$ uma relação binária em X e $x, y \in X$ elementos quaisquer.

a) Mostre que se $\sim$ é transitiva, então "$x \sim y \Rightarrow C_y \subseteq C_x$".

b) Mostre que se $\sim$ é simétrica e transitiva, então "$x \sim y \Rightarrow C_x = C_y$".

c) Mostre que se $\sim$ é reflexiva, então "$C_x \subseteq C_y \Rightarrow x \sim y$".

d) Conclua que valem as condições (ii) e (iii) da proposição anterior. Dica: para (ii), o que ocorre com C_z se $z \in C_x \cap C_y$? ■

A última proposição mostra que $X/\!\sim := \{C_x : x \in X\}$, chamado de **quociente** de X por $\sim$, é uma família de subconjuntos de X que se enquadra como exemplo de *partição*.

Definição 0.1.23. Uma família $\mathcal{P}$ de subconjuntos não-vazios de X é uma **partição** de X se valerem as seguintes condições:

(i) para todo $x \in X$ existe $P \in \mathcal{P}$ com $x \in P$ (i.e., $X = \bigcup \mathcal{P}$); e

(ii) [12] se $P, Q \in \mathcal{P}$ e $P \neq Q$, então $P \cap Q = \emptyset$. ¶

Exercício 0.21 ($\overset{\star}{\star}$)**.** Mostre que se $\sim$ é uma relação de equivalência sobre X, então $X/\!\sim$ é uma partição de X. ■

Como o nome sugere, uma partição de X *particiona* o conjunto X em *partes* ou blocos *dois a dois disjuntos*, de modo que cada elemento de X está precisamente em apenas um membro de $\mathcal{P}$. Assim, faz sentido dizer que dois elementos de X são *$\mathcal{P}$-equivalentes* se pertencerem ao mesmo membro de $\mathcal{P}$. Como você deve ter suspeitado, isto define uma relação de equivalência legítima.

Proposição 0.1.24. *Se $\mathcal{P}$ for uma partição de X, então a relação $\sim_{\mathcal{P}}$ definida por*

$$u \sim_{\mathcal{P}} v \Leftrightarrow \exists P \in \mathcal{P} \text{ tal que } \{u, v\} \subseteq P$$

é uma relação de equivalência em X. Além disso, $\mathcal{P} = X/\!\sim_{\mathcal{P}}$.

Demonstração. A relação $\sim_{\mathcal{P}}$ é

✓ reflexiva, pois dado $x \in X$ existe $P \in \mathcal{P}$ com $x \in P$, e daí $\{x\} = \{x, x\} \subseteq P$,

✓ simétrica, pois se $\{x, y\} \subseteq P \in \mathcal{P}$, então $\{x, y\} = \{y, x\} \subseteq P \in \mathcal{P}$, e

[12] Costuma-se expressar a condição (ii) como "os membros de $\mathcal{P}$ são dois a dois disjuntos".

✓ transitiva, pois se $\{x, y\} \subseteq P \in \mathcal{P}$ e $\{y, z\} \subseteq P' \in \mathcal{P}$, então $P \cap P' \neq \emptyset$, acarretando $P = P'$ e, por conseguinte, $\{x, z\} \subseteq \{x, y\} \cup \{y, z\} \subseteq P \in \mathcal{P}$.

A igualdade $\mathcal{P} = X/\sim_{\mathcal{P}}$ segue pois $P = [x]_{\sim_{\mathcal{P}}}$ para quaisquer x e P com $x \in P \in \mathcal{P}$. □

Exemplo 0.1.25. Para a relação $\sim_n$ do Exemplo 0.1.19, as classes de equivalência correspondem precisamente a todos os possíveis restos pela divisão por n. Assim, chamando por R_i a coleção dos naturais que têm resto i na divisão por n, segue que $\mathbb{N}/\sim_n = \{R_0, R_1, \ldots, R_{n-1}\}$. Dito isso, observe que ao chamar por $\overline{i}$ a *classe* de equivalência de i, verifica-se $\overline{i} = R_i$. Desse modo, seria lícito escrever, por exemplo, $\mathbb{N}/\sim_2 = \{\overline{0}, \overline{1}\}$, ou ainda $\mathbb{N}/\sim_2 = \{\overline{12}, \overline{13}\}$, já que $\overline{0} = \overline{12}$ na relação $\sim_2$ (0 e 12 são divisíveis por 2) e $\overline{1} = \overline{13}$ (1 e 13 têm resto 1 na divisão por 2). Como você já deve ter imaginado, trata-se de um fenômeno mais geral. ▲

Definição 0.1.26. Um subconjunto $R \subseteq X$ é uma **classe de representantes** de uma

(*i*) relação de equivalência $\sim$ se para todo $x \in X$ existe um único $r \in R$ tal que $x \sim r$,

(*ii*) partição $\mathcal{P}$ de X se R for classe de representantes da relação $\sim_{\mathcal{P}}$, i.e., se para cada $P \in \mathcal{P}$ existe um único $r \in R$ tal que $r \in P$. ¶

Exercício 0.22 ($\star$)**.** Nas condições anteriores, mostre que $X/\sim = \{C_r : r \in R\}$, onde R é uma classe de representantes de $\sim$ e C_r indica a $\sim$-classe de equivalência de $r \in R$. ■

Agora parece um bom momento para uma pergunta ardilosa: quais partições (ou relações de equivalência) sobre *um conjunto* não-vazio admitem classes de representantes? Certamente, se X é tal conjunto e $\mathcal{P}$ é uma de suas partições, então cada $P \in \mathcal{P}$ é um subconjunto não-vazio de X, o que permite *escolher* um desses elementos $x_P \in P$ para então considerar o conjunto $\{x_P : P \in \mathcal{P}\}$. Dado que para $P, P' \in \mathcal{P}$ distintos ocorre $P \cap P' = \emptyset$, deve-se ter $x_P \neq x_{P'}$ sempre que $P \neq P'$. Em outras palavras, $\mathcal{R} := \{x_P : P \in \mathcal{P}\}$ é uma classe de representantes para $\mathcal{P}$. Se tal argumentação for honesta, significa que provamos o

Teorema 0.1.27 (Ⓒ)**.** *Se $\sim$ é uma relação de equivalência sobre um conjunto, então existe uma classe de representantes para $\sim$.*

Exercício 0.23 ((?))**.** A argumentação acima foi *honesta*? Se esta for a primeira vez que você se deparou com tal pergunta, pense nela pelo resto do seu dia. ■

As considerações acima ajudam a elucidar o que se *quis dizer* na discussão que sucedeu a Proposição 0.1.8. Para fixar notações:

Definição 0.1.28 (Ⓡ)**.** Vamos denotar por $\mathbb{V}$ o *conjunto de todos os conjuntos*[13], (provisoriamente) chamado de **conjunto universo**. ¶

Com a terminologia acima, a Proposição 0.1.8 *demonstra* que ao escrever "$A \approx B$" para indicar que existe bijeção da forma $A \to B$, obtém-se uma relação de equivalência em $\mathbb{V}$.

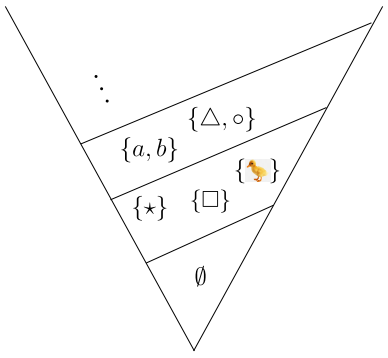


Figura 0.2: Cada $\approx$-classe de equivalência corresponde a uma noção de cardinalidade.

[13] Poderíamos definí-lo como $\mathbb{V} := \{x : x = x\}$, já que *todas as coisas são iguais a si mesmas*. Sim, isto é problemático de um ponto de vista formal, mas vamos ignorar essa treta por enquanto.

Portanto, na prática, uma das noções mais corriqueiras da matemática cotidiana é, na verdade, um dispositivo muito sofisticado: números são representantes de classes de equivalência! Ao dizer que $A := \{x, y\}$ e $B := \{a, b\}$ têm 2 elementos, por exemplo, o símbolo "2" codifica a classe de *todas as coisas com a mesma quantidade de elementos de* A (ou de B, ou de qualquer coisa que tenha... *dois elementos*). Nesse sentido, o que faremos nas próximas seções é encontrar um conjunto "canônico" para representar as cardinalidades dos conjuntos finitos: estes serão os *números naturais*.

0.2 Ordens, boas ordens e indução

0.2.0 Essencial

Ordens

O aparato das relações binárias (Subseção 0.1.1) permite abstrair o nosso entendimento de *ordenação*, que será usado posteriormente tanto na descrição da reta real quanto no tratamento das *nets*. Intuitivamente, os pontos da reta são *ordenados*, no sentido de que há uma *noção* de *antes* e *depois*, como em 3 que antecede 7 e 7 que antecede 9 (note que de nossa experiência diária, 3 também antecede 9). Mais do que isso, a *reta* está ordenada em forma de linha, no sentido de que dados dois pontos nela, algum deles deve anteceder o outro. Tais ideias se formalizam na próxima

Definição 0.2.0. Uma relação binária R num conjunto $\mathbb{X}$ é dita uma **relação de ordem** (**parcial**) se R for reflexiva, transitiva e, além disso, **antissimétrica**, i.e., se para quaisquer $x, y \in \mathbb{X}$, a ocorrência simultânea de $x \; R \; y$ e $y \; R \; x$ acarretar $x = y$, e Escreve-se $(\mathbb{X}, R)$ quando se busca enfatizar que o conjunto $\mathbb{X}$ é considerado com a ordem R, caso em que $\mathbb{X}$ é dito ser (**parcialmente**) **ordenado** pela ordem (parcial) R. ¶

Dada a óbvia inspiração nas ordenações usuais entre números, costuma-se utilizar símbolos como "$\preceq$", "$\sqsubseteq$" ou mesmo "$\leq$" para denotar ordens parciais – o que sugere uma generalização alternativa, desta vez com base em "$<$".

Definição 0.2.1. Diz-se que $\prec$ é uma **relação de ordem estrita** em $\mathbb{X}$ se $\prec$ for transitiva mas, em vez de reflexiva e antissimétrica, for

(i) **irreflexiva**, i.e., se para todo $x \in \mathbb{X}$ ocorrer $x \not\prec x$, e

(ii) **assimétrica**, i.e., se para quaisquer $x, y \in \mathbb{X}$, a ocorrência de $x \prec y$ acarretar $y \not\prec x$.

Como no caso parcial, escreve-se $(\mathbb{X}, \prec)$ para indicar que $\mathbb{X}$ *está* (**estritamente**) **ordenado** pela ordem (estrita) $\prec$. ¶

Observação 0.2.2. Na prática, podemos chamar ordens parciais e ordens estritas simplesmente de *ordens*. De fato:

✓ se $(\mathbb{S}, \prec)$ é uma ordem estrita, então a relação $\preceq$ definida por

$$x \preceq y \Leftrightarrow (x \neq y \text{ e } x \prec y) \text{ ou } x = y$$

é uma relação de ordem parcial em $\mathbb{S}$;

✓ se $(\mathbb{P}, \sqsubseteq)$ é uma ordem parcial, então a relação $\sqsubset$ definida por

$$x \sqsubset y \Leftrightarrow x \neq y \text{ e } x \sqsubseteq y$$

é uma relação de ordem estrita em $\mathbb{P}$.

Exercício 0.24 ($\star$)**.** Verifique as afirmações anteriores. ■

É claro que ao aplicar o primeiro procedimento à ordem estrita $\sqsubset$, retorna-se à ordem parcial original $\sqsubseteq$, enquanto o segundo procedimento aplicado à ordem parcial $\preceq$ resulta na ordem estrita original $\prec$. Assim, tem-se o direito de chamar tanto $(\mathbb{S}, \prec)$ quanto $(\mathbb{P}, \sqsubseteq)$ de **ordens**. Em tais situações, ficam implicitamente definidas a ordem parcial $\preceq$ e a ordem estrita $\sqsubset$ induzidas por $\prec$ e $\sqsubseteq$, respectivamente[14]. △

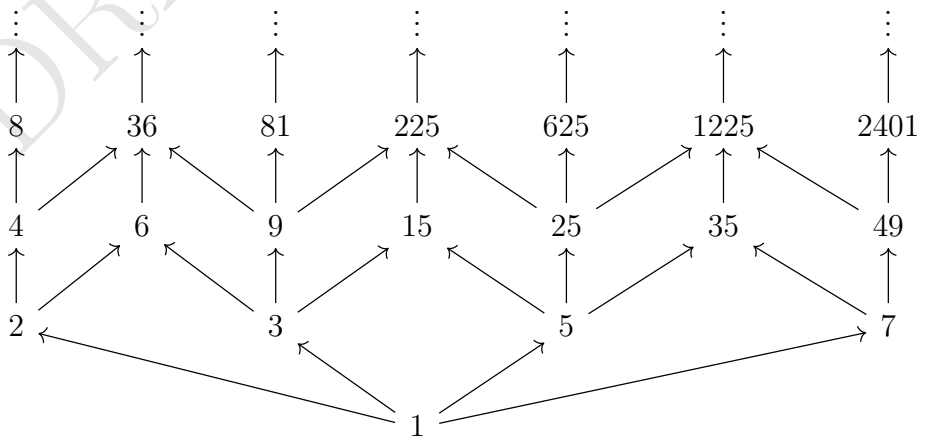
Exemplo 0.2.3. Quem já tem familiaridade com conjuntos numéricos ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, etc.) deve ter em mente as formas usuais de ordenação em tais cenários como exemplos de ordens. Apesar disso, é importante saber que mesmo conjuntos *ordinários* admitem ordenações incomuns.

Por exemplo, em $\mathbb{N}^* \coloneqq \mathbb{N} \setminus \{0\}$ (que será discutido na próxima seção), pode-se declarar $m \preceq n$ sempre que m for um divisor de n. Embora tal relação defina uma ordem parcial sobre $\mathbb{N}^*$ (verifique?)*, ela é bastante diferente de sua ordenação usual: note que $2 \not\preceq 3$ e $3 \not\preceq 2$, já que ambos são primos. Portanto, $(\mathbb{N}^*, \preceq)$ é uma ordem em que podem haver elementos *não-comparáveis* entre si, comportamento bem mais comum do que parece. ▲

Exemplo 0.2.4 (Confira o Exemplo 0.1.13)**.** A relação de inclusão $\subseteq$ sobre os membros de $\wp(X)$, para algum conjunto X fixado, faz de $(\wp(X), \subseteq)$ uma ordem, já que: $A \subseteq A$, $A \subseteq B$ e $B \subseteq A$ implicam $A = B$ e $A \subseteq B$ e $B \subseteq C$ implicam $A \subseteq C$, para quaisquer $A, B, C \in \wp(X)$. Como no caso anterior, podem existir $A, B \in \wp(X)$ não-comparáveis: para $X \coloneqq \mathbb{N}$ por exemplo, $A \coloneqq \{0, 1, 2\}$ e $B \coloneqq \{0, 1, 3\}$ não são comparáveis, já que $A \not\subseteq B$ (pois $2 \in A \setminus B$) e $B \not\subseteq A$ (pois $3 \in B \setminus A$). ▲

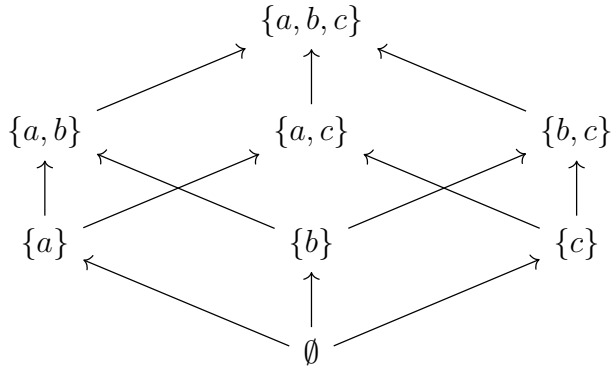
Observação 0.2.5 (Diagramas de Hasse)**.** Um modo bastante prático de *entender* certas ordens (ou *partes* delas) consiste em considerar seus *diagramas de Hasse*. A ideia é muito simples: a ocorrência de $x < y$ em $\mathbb{P}$ é representada por uma seta $(x \to y)$ que liga o vértice anterior (*menor*) x ao posterior (*maior*) y; quando $y < z$ e, por conseguinte, $x < z$, não se grafa uma seta entre ambos, pois subentende-se que as duas setas (entre x e y e entre y e z) compõem a seta entre x e z.

Assim, por exemplo, o diagrama de Hasse de $(\mathbb{N}^*, \preceq)$ com a ordem do Exemplo 0.2.3 poderia *começar* com



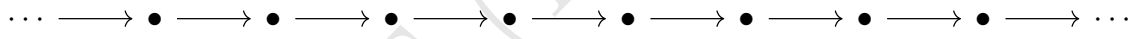
[14] Há uma exceção que será adotada neste texto: a inclusão estrita ainda será denotada por "$\subsetneq$" e não por "$\subset$". O motivo é muito simples: o uso do símbolo "$\subset$" para indicar a inclusão parcial está demasiado difundido, o que poderia causar confusão.

Evidentemente, *diversos* (*infinitos*!) números foram omitidos, como 12 (que deveria estar acima de 4 e 3), 10 (que deveria estar acima de 5 e 2), 11 (que deveria estar acima de 1 apenas), 13... Já para o caso de $X := \{a, b, c\}$ e $(\wp(X), \subseteq)$, o diagrama é mais simples, embora ainda intrincado.



Diagramas desse tipo ajudam a perceber que a ocorrência de elementos não-comparáveis se traduz em bifurcações. Uma vez que pretendemos usar ordens para capturar o comportamento das retas, é razoável considerar aquelas em que quaisquer dois elementos sejam comparáveis, condição usualmente chamada de *tricotomia*.

Definição 0.2.6. Uma ordem $(\mathbb{X}, <)$ é **total** se para quaisquer $x, y \in \mathbb{X}$ ocorrer somente um dos três casos a seguir: $x = y$, $x < y$ ou $y < x$. Se a ordem de $\mathbb{X}$ for parcial, basta dizer que para quaisquer $x, y \in \mathbb{X}$ ocorre $x \leq y$ ou $y \leq x$. ¶



Como o diagrama acima sugere, ordens totais[15] se comportam como linhas precisamente por não terem elementos incomparáveis (bifurcações). Os conjuntos $\mathbb{N}$ e $\mathbb{Z}$ com suas ordenações usuais são exemplos típicos de ordens totais. Os conjuntos $\mathbb{Q}$ e $\mathbb{R}$ também, mas seus diagramas são mais desonestos em virtude da *densidade* de suas ordens: dado que entre quaisquer $x, y \in \mathbb{Q}$ com $x < y$ existe $z \in \mathbb{Q}$ com $x < z < y$, torna-se *impossível* representar *fielmente*, por meio de um diagrama de Hasse, o comportamento linear de tais ordens. Na prática, a alternativa honesta de representação gráfica nesses casos é, justamente... uma linha reta. △

Em geral, costuma-se ler uma expressão do tipo "$x \preceq y$" como "x é **menor do que ou igual** a y", enquanto "$x \prec y$" é lida como "x é (**estritamente**) **menor** do que y" – a menos que o contexto sugira uma terminologia própria para os símbolos. *Alternativamente*, lê-se "$x \preceq y$" como "y é **maior do que ou igual** a x", o que esconde um fato que será importante: escrevendo "$a \succeq b$" para indicar que $b \preceq a$, segue que $\succeq$ também é uma relação de ordem sobre o conjunto em questão: explicitamente, $\succeq$ é apenas a *relação inversa* de $\preceq$ (Definição 0.1.15). Embora pareça banal, tal observação pode ser útil para quem se aventurar na exploração dos princípios de dualidade (Subseção 0.2.1).

Exercício 0.25 ($\star$)**.** Mostre que $(\mathbb{P}, \succeq)$ é ordem parcial sempre que $(\mathbb{P}, \preceq)$ é ordem parcial. ■

[15] Que com muita razão também são chamadas de ordens *lineares*.

Boas ordens e indução

Definição 0.2.7. Fixada uma *ordem* $(\mathbb{P}, \leq)$, um subconjunto A de $\mathbb{P}$ e um elemento $a \in A$, diremos que a é *um* **menor elemento** (ou **mínimo**) de A se $a \leq x$ ocorrer para todo $x \in A$. No caso de uma ordem estrita $<$, pede-se $a < x$ para todo $x \in A$ tal que $x \neq a$. ¶

Acima, o uso do artigo indefinido "um" foi puro preciosismo, já que um mínimo, quando existe, é único: se $a, a' \in A$ são mínimos de A, então ocorre $a \leq a'$ e $a' \leq a$, donde a antissimetria de $\leq$ acarreta $a = a'$. Isto justifica introduzir uma notação para indicar os mínimos: caso exista, o menor elemento de A será denotado $\min_{a \in A} a$, $\min_{\leq} A$ ou apenas $\min A$.

Definição 0.2.8. Uma ordem $\leq$ (ou $<$) sobre um conjunto $\mathbb{B}$ é chamada de **boa ordem** se todo subconjunto não-vazio de $\mathbb{B}$ admite menor elemento. Diz-se também que $\mathbb{B}$ está **bem ordenado** pela (boa) ordem $\leq$, ou ainda que $(\mathbb{B}, \leq)$ é uma boa ordem. ¶

Exemplo 0.2.9. Alguns conjuntos numéricos clássicos que você já viu na escola (ou em Cálculo I) não são bem ordenados: é o caso de $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ (por quê?)*. A situação de $\mathbb{C}$ é um pouco pior, mas ainda é cedo para discutir isso. Por outro lado, $\mathbb{N}$ é o exemplo típico de boa ordem, o que não é mero acidente, como veremos em breve. ▲

Moralmente, um conjunto está bem ordenado quando seus elementos podem ser *enfileirados* por meio da ordem $\leq$: há o *primeiro* elemento, digamos $b_0 := \min \mathbb{B}$, em seguida o seu *sucessor*, digamos $b_1 := \min(\mathbb{B} \setminus \{b_0\})$, em seguida... Como os índices "0" e "1" sugerem, parece haver alguma ligação com os *números naturais* que já conhecemos de longa data, o que suscita uma pergunta deliberadamente evitada até agora (pelo menos para quem pulou a Subseção 0.1.1: *o que são números (e o que poderiam ser)?*[16]

$$b_0 \longrightarrow b_1 \longrightarrow b_2 \longrightarrow b_3 \longrightarrow b_4 \longrightarrow \cdots$$

Evidentemente, esse tipo de pergunta não se refere ao símbolo utilizado para *denotar* um número, mas sim ao próprio número: por exemplo, qual o significado de "três" nas sentenças "A Argentina venceu três Copas do Mundo" e "Neymar rolou por três metros ao simular uma falta"? Quais as diferenças de significado, e quais as semelhanças?

Exercício 0.26 ((?))**.** Reflita (por pelo menos *três* minutos) sobre as questões acima. ■

Apesar da sugestão numérica anterior, é possível evitar o emprego explícito de números no entendimento das boas ordens – o que inclusive será útil quando voltarmos a discutir a *natureza* dos números. A grande sacada para fazer isso está escondida na seguinte

Proposição 0.2.10. *Sejam $(\mathbb{B}, \leq)$ uma boa ordem e $b \in \mathbb{B}$. Se existir $c \in \mathbb{B}$ com $c > b$, então existe $b' \in \mathbb{B}$ com as seguintes propriedades:*

(i) $b < b'$;

(ii) *se $d \in \mathbb{B}$ e $d > b$, então $b' \leq d$.*

[16] Referência ao clássico "*Was Sind Und Was Sollen Die Zahlen?*", de Richard Dedekind, em que *Ele* apresenta Sua construção para (o que hoje chamamos de) um corpo ordenado completo [4].

Demonstração. É mais simples do que parece: a existência de c com $c > b$ garante que $\mathbb{B}_{>b} := \{d \in \mathbb{B} : d > b\}$ é um subconjunto não-vazio de $\mathbb{B}$, justamente por ter c como elemento. Logo, a boa ordenação garante a existência de $\min \mathbb{B}_{>b}$, de modo que basta tomar $b' := \min \mathbb{B}_{>b}$. □

Definição 0.2.11. Nas condições da proposição anterior, vamos denotar b' por $\mathrm{suc}_{\mathbb{B}}(b)$, o **sucessor** de b na boa ordem $\mathbb{B}$. ¶

Assim como ocorre com sucessores nos diversos campos da vida real, o sucessor de b numa boa ordem $\mathbb{B}$, caso exista, é o primeiro elemento da ordem a ser maior do que b, o que em particular impede a existência de elementos *intermediários*. O próximo exercício deve esclarecer a ideia.

Exercício 0.27 ($\star$)**.** Seja $(\mathbb{B}, \leq)$ uma boa ordem. Mostre que se $b \in \mathbb{B}$ e existe $\mathrm{suc}_{\mathbb{B}}(b)$, então não existe $c \in \mathbb{B}$ tal que $b < c < \mathrm{suc}_{\mathbb{B}}(b)$. Dica: releia a definição de $\mathrm{suc}_{\mathbb{B}}(b)$. ■

Exercício 0.28 ($\overset{\star}{\star\star}$)**.** Seja $(\mathbb{B}, \leq)$ uma boa ordem. Mostre que se $x, y \in \mathbb{B}$ têm sucessores e $x \leq y$, então $\mathrm{suc}_{\mathbb{B}}(x) \leq \mathrm{suc}_{\mathbb{B}}(y)$. Dica: mostre antes que se $\emptyset \neq Y \subseteq X \subseteq \mathbb{B}$, então $\min X \leq \min Y$. ■

Observação 0.2.12 (Sucessores nem sempre existem)**.** Para quem tem familiaridade com os números racionais, por exemplo, note que não faz sentido perguntar qual o sucessor de 0 em $\mathbb{Q}$, já que não existe o *primeiro racional* maior do que 0: sempre que $q > 0$, existe outro q' com $0 < q' < q$. Em particular, a relação de ordem usual sobre $\mathbb{Q}$ não é uma boa ordem. △

Exemplo 0.2.13. Por mais sem graça que pareça, $\mathbb{B} := \emptyset$ pode ser considerado como um conjunto bem ordenado: no caso, sua boa ordem $\leq$ é o único subconjunto de $\emptyset \times \emptyset = \emptyset$, a saber, $\emptyset$! Apesar de sua simplicidade, $\emptyset$ é o gatilho de uma importante reação em cadeia, como veremos adiante. ▲

Definição 0.2.14. Fixada uma boa ordem $(\mathbb{B}, \leq)$, diremos que $u \in \mathbb{B}$ é o **último elemento** de $\mathbb{B}$ se $u = \max \mathbb{B}$. ¶

Proposição 0.2.15. *Se $(\mathbb{B}, \leq)$ é uma boa ordem e $u' \notin \mathbb{B}$, então existe uma boa ordem $(\mathbb{B}', \leq')$ tal que*

(i) $\mathbb{B} \subsetneq \mathbb{B}'$,

(ii) $x \leq y \Leftrightarrow x \leq' y$ *para quaisquer* $x, y \in \mathbb{B}$, *e*

(iii) u' *é o último elemento de* $\mathbb{B}'$.

Demonstração. Basta definir $\mathbb{B}' := \mathbb{B} \cup \{u'\}$ e, para quaisquer $x, y \in \mathbb{B}'$, escrever $x \leq' y$ para indicar a ocorrência de "$x, y \in \mathbb{B}$ e $x \leq y$" ou "$y = u'$". Na prática, $\leq'$ apenas *estende* a definição de $\leq$ sobre $\mathbb{B}' \times \mathbb{B}'$ ao declarar $x \leq' u'$ para todo $x \in \mathbb{B}'$, o que torna quase imediata a verificação das propriedades desejadas. □

Exercício 0.29 ($\overset{\star}{\star}$)**.** Complete a demonstração. ■

Exemplo 0.2.16. Fixado qualquer objeto u', tem-se por definição que $u' \notin \emptyset$, o que permite empregar a última proposição a fim de estender a boa ordem $\mathbb{B}$ do Exemplo 0.2.13: faz-se $\mathbb{B}' := \mathbb{B} \cup \{u'\} = \{u'\}$, que tem u' como seu último (e único!) elemento. Ora, por que parar? Certamente existe $u'' \neq u'$, donde a proposição anterior garante a boa ordem $\mathbb{B}'' := \mathbb{B}' \cup \{u''\}$, com $u' < u''$ e u'' como último elemento. Em particular, u'' é sucessor de u', mas u'' não tem sucessores em $\mathbb{B}''$. Ora, por que parar? Certamente existe $u''' \notin \{u', u''\}$, donde a proposição anterior garante... ▲

Como os exemplos acima sugerem, a noção de sucessor numa boa ordem torna supérfluo o uso explícito de números *alienígenas* para descrever o seu enfileiramento. Na verdade, mais do que isso, o comportamento dos sucessores é tão parecido com o da *progressão* esperada dos números naturais que chega a ser tentador utilizar a noção de boa ordenação para *descrever* o que os números *poderiam ser*. Para agravar ainda mais o sentimento:

Teorema 0.2.17 (Indução numa boa ordem)**.** *Seja* $(\mathbb{B}, \leq)$ *uma boa ordem. Suponha que* X *seja um subconjunto de* $\mathbb{B}$ *com a seguinte propriedade para qualquer* $c \in \mathbb{B}$*:*

$$\textit{sempre que ocorre } b \in X \textit{ para todo } b < c\textit{, também ocorre } c \in X.$$

Em tais condições, $\mathbb{B} = X$*.*

Demonstração. Nada precisa ser feito se ocorrer $\mathbb{B} = \emptyset$. Agora, se $\mathbb{B} \neq \emptyset$ e existir $b \in \mathbb{B}$ com $b \notin X$, então o conjunto $T := \{b \in \mathbb{B} : b \notin X\}$ é não-vazio e, pela boa ordenação, deve existir $t := \min T$; em particular, $t \in T$. Ora, isto impede que X tenha a propriedade do enunciado: com efeito, por t ser o menor elemento em T, todo $b < t$ deve ser membro de X, de modo que se X tivesse a propriedade, concluiríamos que $t \in X$, mas $t \in T := \mathbb{B} \setminus X$. □

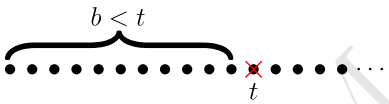


Figura 0.3: Se t fosse o *primeiro* tal que $t \notin X$, então todo $b < t$ pertenceria a X. Logo, $t \in X$!

No dia a dia, o subconjunto X costuma ser formado pelos elementos de $\mathbb{B}$ que têm alguma propriedade $\mathcal{P}$ fixada, i.e., $X := \{x \in \mathbb{B} : \text{vale } \mathcal{P}(x)\}$, de modo que a exigência feita sobre X se traduz na seguinte condição:

$$\textbf{\textit{sempre que vale } } \mathcal{P}(b) \textbf{\textit{ para todo }} b < c\textit{, também vale } \mathcal{P}(c).$$

Muito provavelmente você já se deparou com tal formulação do *Princípio da Indução* em alguma disciplina introdutória de Teoria dos Números ou Álgebra – neste caso, é comum dizer que esta é a "segunda forma da indução" [9, 10]. Como sempre, o intuito é provar que todo elemento c de $\mathbb{B}$ tem a propriedade $\mathcal{P}(c)$ e, nesse sentido, o Teorema 0.2.17 assegura que não precisamos provar $\mathcal{P}(c)$ *diretamente*, mas podemos fazer isso com o auxílio de uma *hipótese indutiva* (a parte em negrito na frase destacada acima): se conseguirmos garantir que $\mathcal{P}(c)$ vale sempre que se assumir a validade de $\mathcal{P}(b)$ para todo $b < c$, então todo c da boa ordem tem a propriedade em questão[17].

Note que o raciocínio da demonstração pode ser usado para provar que *cada* elemento de uma boa ordem não-vazia $\mathbb{B}$ pertence a X se a hipótese for satisfeita: como não existe $b < \min \mathbb{B}$, a hipótese indutiva é verdadeira (todo $b < \min \mathbb{B}$ pertence a X, por vacuidade!), logo $\min \mathbb{B} \in X$; se $\min \mathbb{B}$ tem sucessor, digamos c, então $c \in X$, pois no passo anterior verificou-se que todo $b < c$ pertence a X; se c tem sucessor...

Esse arquétipo de efeito dominó é equivalente ao que foi apresentado no teorema anterior, mas somente nas boas ordens em que todos os elementos, exceto o menor, são sucessores de *alguém*[18]. *Naturalmente*, isto será discutido depois. Para encerrar, faça o seguinte

Exercício 0.30 $(\overset{\star}{\star})$**.** Mostre que se $(\mathbb{B}, \leq)$ é boa ordem, então $(\mathbb{B}, \leq)$ é ordem total. ■

[17] "*Ah, mas não estaríamos supondo o que queremos provar?!*" Calma: ninguém está supondo que vale $\mathcal{P}(c)$, mas sim que $\mathcal{P}(b)$ vale para todo $b < c$!

[18] Cuidado: ter sucessor $\neq$ ser sucessor. O exemplo óbvio é o menor elemento de uma boa ordem com pelo menos *dois* elementos.

0.2.1 Extras

Elementos minimais e maximais

Definição 0.2.18. Fixada uma *ordem* $(\mathbb{P}, \leq)$, um subconjunto A de $\mathbb{P}$ e um elemento $a \in A$, diremos que $a \in A$ é **elemento minimal de** A se não existe $x \in A$ com $x < a$. De modo *dual*, diremos que $a \in A$ é **elemento maximal** de A se não existe $x \in A$ com $a < x$. ¶

Elementos minimais e maximais não costumam ser explorados em contextos introdutórios de Análise pois as ordens consideradas *geralmente* são totais – e, em tais casos, as definições coincidem com as noções de mínimos e *máximos*.

Proposição 0.2.19. *Sejam $(\mathbb{T}, \leq)$ uma ordem, $A \subseteq \mathbb{T}$ um subconjunto e $a \in A$ um elemento qualquer.*

(i) *Se $a = \min A$, então a é minimal.*

(ii) *Se $(\mathbb{T}, \leq)$ é uma ordem total, então vale a recíproca do item anterior.*

Demonstração. Para a primeira parte, não pode existir $x \neq a$ com $x < a$ e $x \in A$, pois por a ser mínimo deve-se ter $a \leq x$ (lembre-se: ordens estritas são assimétricas!). Para a segunda parte: a princípio, por a ser minimal, para nenhum $x \in A$ *ocorre* $x < a$ e, como x e a são comparáveis pela hipótese de tricotomia, *resta* apenas $a \leq x$. Logo, $a = \min A$. □

Exercício 0.31 $(\overset{\star}{\star\star})$**.** Enuncie e demonstre a versão da proposição anterior para elementos maximais. **Observação:** neste caso, você também precisará da definição de *maior elemento* (ou *máximo*)[19], apresentada um pouco mais abaixo (mas não é difícil adivinhar qual é). ■

Com isso dito, retorne para as ordens não-totais da Observação 0.2.5: no caso de $\wp(X)$, por exemplo, $A := \{\{a\}, \{b\}, \{c\}\}$ é tal que todos os seus elementos são minimais em $\wp(X)$ (e nenhum deles é mínimo!), comportamento similar ao dos números primos em $(\mathbb{N}^*, \preceq)$. Alguma delas apresenta subconjuntos com elementos maximais que não são máximos?

Dualidade

Considere $(\mathbb{P}, \leq)$ uma ordem (parcial). O fato de $(\mathbb{P}, \geq)$ ainda ser uma ordem parcial traz uma consequência curiosa: sempre que você tiver um resultado acerca de um conceito definível em ordens parciais $(\leq)$, você ganha automaticamente outro resultado acerca da versão *dual* do conceito, isto é, onde o conceito é reescrito com a ordem inversa $(\geq)$.

Por exemplo: caso não tenha *adivinhado* a definição de máximo, ela se faz assim.

Definição 0.2.20. Fixada uma *ordem* $(\mathbb{P}, \leq)$, um subconjunto A de $\mathbb{P}$ e um elemento $a \in A$, diremos que a é *um* **maior elemento** (ou **máximo**) de A se $x \leq a$ ocorrer para todo $x \in A$. No caso de uma ordem estrita $<$, pede-se $x < a$ para todo $x \in A$ tal que $x \neq a$. ¶

Agora, esqueça a definição acima e considere $(\mathbb{P}, \geq)$, onde $\geq$ é a inversa de $\leq$. O que significa dizer que $a \in A$ é menor elemento de A com respeito à ordem $\geq$? Checando a Definição 0.2.7, deve-se ter o seguinte: $a \geq x$ ocorre para todo $x \in A$. Como "$a \geq x$" significa "$x \leq a$", resulta que a é máximo de A com respeito à ordem $\leq$. Neste caso, as definições de máximo e mínimo são ditas duais.

Exercício 0.32 $(\overset{\star}{\star\star})$**.** Mostre que as definições de elementos minimais e maximais são duais. ■

Uma das vantagens desse tipo de abordagem é reciclar demonstrações. Por exemplo: como já sabemos que mínimos em ordens parciais são únicos quando existem, resulta que máximos em ordens parciais também são únicos quando existem, simplesmente por eles podem ser expressos como mínimos nas ordens inversas. Se você duvida, faça o próximo exercício, e perceba que, na prática, você precisa apenas trocar todas as ocorrências de "$<$" e "$\leq$" na demonstração da Proposição 0.2.19 por "$>$" e "$\geq$", respectivamente. Abaixo, $\max A$ indica o máximo de A, caso exista.

Exercício 0.33 $(\overset{\star}{\star\star})$**.** Sejam $(\mathbb{T}, \leq)$ uma ordem, $A \subseteq \mathbb{T}$ um subconjunto e $a \in A$ um elemento qualquer.

(i) Mostre que se $a = \max A$, então a é maximal.

(ii) Mostre que se $(\mathbb{T}, \leq)$ é uma ordem total, então vale a recíproca do item anterior. ■

[19] Note que máximos, assim como mínimos, quando existem, são únicos $(\star)$.

0.3 Os axiomas de Dedekind-Peano

0.3.0 Essencial: boas ordens naturais

Na última seção discutiu-se uma forma de indução válida em boas ordens quaisquer. Agora, vamos nos restringir às boas ordens que remetem diretamente ao entendimento que temos dos *números naturais*, a começar com o

Corolário 0.3.0 (Indução "clássica")**.** *Sejam* $(\mathbb{B}, \leq)$ *uma boa ordem com* $\mathbb{B} \neq \emptyset$*, considere* $p := \min \mathbb{B}$ *e suponha que para todo* $b' \in \mathbb{B} \setminus \{p\}$ *exista* $b \in \mathbb{B}$ *tal que* $b' = \mathrm{suc}_{\mathbb{B}}(b)$*. Em tais condições, se* $X \subseteq \mathbb{B}$ *for tal que*

- ✓ $p \in X$*, e*
- ✓ $\mathrm{suc}_{\mathbb{B}}(b) \in X$ *sempre que* $b \in X$*,*

então $\mathbb{B} = X$*.*

Demonstração. Basta verificar que X tem a propriedade do Teorema 0.2.17, i.e., que para qualquer $c \in \mathbb{B}$, tenha-se a ocorrência de $c \in X$ sempre que $b \in X$ para todo $b < c$: ora, se $c := p$, então $p \in X$ por hipótese; se $c > p$ e $b \in X$ para todo $b < c$, então em particular para $b \in \mathbb{B}$ com $c = \mathrm{suc}_{\mathbb{B}}(b)$ (que existe pela hipótese sobre $\mathbb{B}$), deve-se ter $b < c$, donde segue que $b \in X$ e, pela hipótese sobre X, $c = \mathrm{suc}_{\mathbb{B}}(b) \in X$, como desejado. □

Exercício 0.34 $(^{\star}_{\star\star})$**.** Prove o corolário anterior sem apelar para o Teorema 0.2.17. Dica: suponha $\mathbb{B} \setminus X \neq \emptyset$ e note que seu menor elemento *deveria* ser da forma $\mathrm{suc}_{\mathbb{B}}(b)$ para algum $b \in X$. ■

O corolário acima mostra que se $\mathbb{B}$ é uma boa ordem em que todo elemento maior do que $\min \mathbb{B}$ é sucessor de *alguém*, então vale o *princípio da indução* em sua forma convencional. Tal propriedade de fato remete aos naturais, mas não completamente: com $\mathbb{B} := \{a, a', a'', a'''\}$, por exemplo, obtemos uma boa ordem ao declarar $a < a' < a'' < a'''$ onde $a = \min \mathbb{B}$, $a' = \mathrm{suc}_{\mathbb{B}}(a)$, $a'' = \mathrm{suc}_{\mathbb{B}}(a')$ e $a''' = \mathrm{suc}_{\mathbb{B}}(a'')$, ou seja, todo elemento diferente de $\min \mathbb{B}$ é sucessor de alguém. Porém, $\mathbb{B}$ não é o que esperaríamos de $\mathbb{N}$, pois ainda faltam sucessores: deveria haver $a'''' := \mathrm{suc}_{\mathbb{B}}(a''')$, $a''''' := \mathrm{suc}_{\mathbb{B}}(a'''')$ e *assim por diante*. Pois bem:

Definição 0.3.1. Diremos que uma boa ordem $(\mathbb{B}, \leq)$ é **natural** se as seguintes condições forem satisfeitas:

- (i) $\mathrm{suc}_{\mathbb{B}}(b)$ existe para todo $b \in \mathbb{B}$,
- (ii) para todo $b' \in \mathbb{B} \setminus \{\min \mathbb{B}\}$ existe $b \in \mathbb{B}$ com $b' = \mathrm{suc}_{\mathbb{B}}(b)$. ¶

A expressão "natural" acima faz, finalmente, alusão ao *conjunto dos números naturais*, frequentemente denotado por $\mathbb{N}$, que você certamente conhece de sua vida fora da disciplina. Veremos que, para efeitos práticos, qualquer boa ordem natural pode fazer o *papel* de $\mathbb{N}$.

Definição 0.3.2. Diremos que $(\mathcal{N}, i, s)$ é um **sistema natural**[20] se $\mathcal{N}$ for um conjunto, i for um elemento de $\mathcal{N}$ e $s \colon \mathcal{N} \to \mathcal{N}$ for uma função satisfazendo os seguintes axiomas:

[20] Nos cânones brasileiros de Análise Real redigidos por Lima [9, 10], diz-se apenas que "$\mathbb{N}$ é um conjunto dotado de uma função s tal que...", onde as retiscências repetem as condições (i), (ii) e (iii) apresentadas para sistemas naturais. Aqui, o emprego do artigo indefinido (um) em vez do definido (o) visa chamar sua atenção para o seguinte: a princípio, nada impede que existam diversos sistemas naturais *diferentes*.

(DP$_i$) $\mathcal{N} \setminus \operatorname{im}(s) = \{i\}$;

(DP$_{ii}$) s é injetora; e

(DP$_{iii}$) (*indutivo*) se um subconjunto $X \subseteq \mathcal{N}$ for tal que

(C.I.) $i \in X$, e
(H.I.) $s(n) \in X$ sempre que $n \in X$,

então $X = \mathcal{N}$. ¶

Os axiomas (DP$_i$), (DP$_{ii}$) e (DP$_{iii}$), elaborados independentemente por Dedekind e Peano, buscam capturar o *mínimo* que se espera dos *números naturais* dentro de um cenário regido por conjuntos[21]. Nesse sentido, boas ordens naturais cumprem bem o papel.

Teorema 0.3.3. *Se* $(\mathbb{B}, \leq)$ *é uma boa ordem natural, então* $(\mathbb{B}, \min \mathbb{B}, \operatorname{suc}_{\mathbb{B}})$ *é um sistema natural, ou seja:*

(i) $\mathbb{B} \setminus \operatorname{im}(\operatorname{suc}_{\mathbb{B}}) = \{\min \mathbb{B}\}$;

(ii) *a função* $\operatorname{suc}_{\mathbb{B}} \colon \mathbb{B} \to \mathbb{B}$ *é injetora; e*

(iii) *se* $X \subseteq \mathbb{B}$ *for tal que* $\min \mathbb{B} \in X$ *e* $\operatorname{suc}_{\mathbb{B}}(b) \in X$ *sempre que* $b \in X$, *então* $X = \mathbb{B}$.

Demonstração. A verificação do axioma (DP$_i$) fica por sua conta ($\star$). O axioma indutivo (DP$_{iii}$), por sua vez, já foi demonstrado (confira o Corolário 0.3.0 em caso de dúvida). Resta apenas verificar a validade de (DP$_{ii}$), i.e., que a função $\operatorname{suc}_{\mathbb{B}} \colon \mathbb{B} \to \mathbb{B}$ é injetora.

Explicitamente, deve-se mostrar que se $x, y \in \mathbb{B}$ são distintos, então $\operatorname{suc}_{\mathbb{B}}(x) \neq \operatorname{suc}_{\mathbb{B}}(y)$. Como toda boa ordem é total (Exercício 0.30), a ocorrência de $x \neq y$ acarreta $x < y$ ou $y < x$, de modo que basta mostrar o seguinte: se $x < y$, então $\operatorname{suc}_{\mathbb{B}}(x) < \operatorname{suc}_{\mathbb{B}}(y)$. Ora, pelo Exercício 0.28, já sabemos que $\operatorname{suc}_{\mathbb{B}}(x) \leq \operatorname{suc}_{\mathbb{B}}(y)$. Se tal desigualdade não fosse estrita, teríamos $\operatorname{suc}_{\mathbb{B}}(x) = \operatorname{suc}_{\mathbb{B}}(y)$, resultando em

$$x < y < \operatorname{suc}_{\mathbb{B}}(y) = \operatorname{suc}_{\mathbb{B}}(x),$$

o que viola o Exercício 0.27. □

Há quem não goste da abordagem via boas ordens pois ela demanda *mais estrutura* para capturar parte do comportamento dos sistemas naturais. Todavia, um sistema natural $(\mathcal{N}, i, s)$ vem de fábria com uma boa ordem natural[22] que tem i como menor elemento e cuja função sucessor é, precisamente, a função s. Caso tenha se interessado, confira o Exercício 0.73. Assim, toda essa discussão traz a seguinte conclusão:

existe uma boa ordem natural se, e somente se, existe um sistema natural.

E daí a grande questão: existe?

Intuitivamente, a resposta é sim. Porém, *demonstrar* que a resposta é sim envolveria construir uma boa ordem natural *infinita*, o que poderia ser problemático num contexto em que as demonstrações precisam ser *finitas*. O que se faz então é *postular* a existência de ao menos uma boa ordem natural (ou sistema natural, se preferir):

[21] Em certo sentido, eles funcionam como os axiomas que descrevem os *grupos*, que por sua vez buscam capturar as propriedades básicas das noções de simetria. A ideia é que se tal mínimo for satisfeito, então todos os resultados de Aritmética Básica podem ser recuperados via dedução, paciência e um pouco de conjuntos.

[22] Que inclusive precisa ser explicitada em algum momento mesmo por quem opta pelos sistemas naturais, vide [9, 10] por exemplo.

Axioma de Dedekind-Peano. *Existe um sistema natural.*

Deste ponto em diante, é prática comum fixar *algum* sistema natural e, por meio de *argumentações indutivas*, construir *recursivamente* as operações de *adição* e *multiplicação* de forma precisa e verificar todas as propriedades operatórias esperadas, num árduo, doloroso e ~~gratificante?~~ demorado processo que, na prática, *recria* a Aritmética Básica. É nesse sentido que se costuma dizer que os Axiomas de Dedekind-Peano capturam o básico dos *naturais*: a partir deles e das construções conjuntistas (!)[23], recuperam-se todos os dispositivos aritméticos usuais e, *a posteriori*, todos os outros conjuntos numéricos! Há, porém, um elefante na sala: o vermelho que eu vejo é tão vermelho quanto o que você vê?

Explicitamente, o Axioma de Dedekind-Peano não assegura *o* sistema natural, mas apenas *um* sistema natural. Poderia haver vários? Se sim, então os processos descritos acima dependem do sistema natural escolhido? Cada sistema natural tem sua própria Aritmética? Será que essas preocupações realmente fazem sentido?

Comecemos pela última: a rigor, os questionamentos são pertinentes. Por exemplo: assim como um *grupo* é um conjunto dotado de funções que satisfazem certos axiomas, sistemas naturais também são conjuntos dotados de funções que satisfazem certos axiomas. Dado que existem grupos definitivamente *incompatíveis* entre si, há precedente para questionar a possibilidade de sistemas naturais *incompatíveis* em algum sentido. Feita a ressalva, não se preocupe: embora existam (*infinitos*!) sistemas naturais distintos, todos eles são *rigorosamente* compatíveis entre si, o que na prática garante que a Aritmética desenvolvida em um seja *indistinguível* da Aritmética desenvolvida em outro.

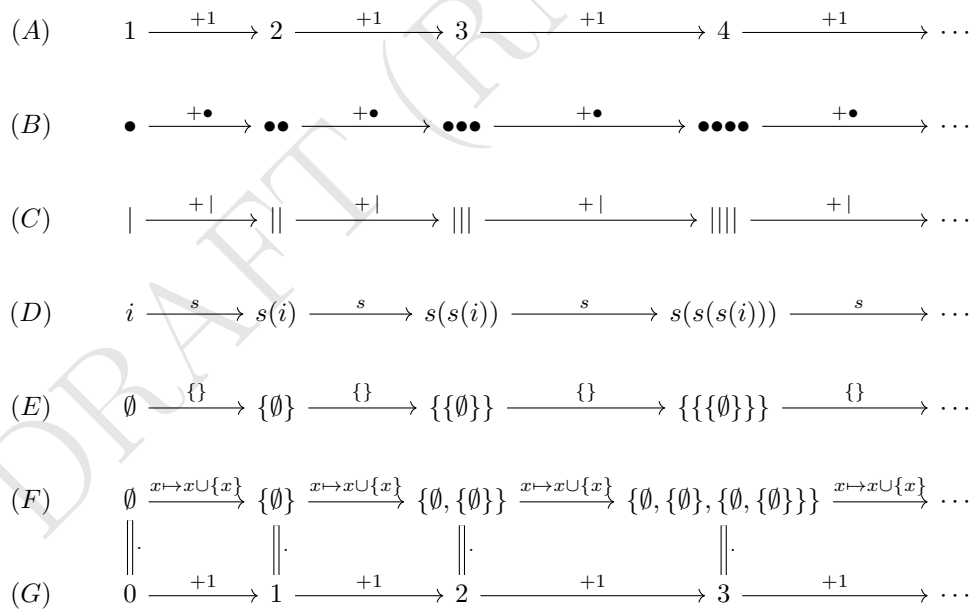


Figura 0.4: Vários sistemas naturais.

[23] É relativamente comum encontrar quem propague máximas como "os Axiomas de (Dedekind-) Peano permitem construir a Matemática!", num indicativo claro de amnésia, já que os axiomas usados na descrição de sistemas naturais descrevem apenas tais sistemas. Por exemplo, se $(\mathcal{N}, i, s)$ é um sistema natural, não são os seus axiomas que *permitem* construir o conjunto $\mathcal{N} \times (\mathcal{N} \setminus \{i\})$ a partir do qual se obtém os *inteiros*, mas sim as suposições tácitas (axiomas acerca de conjuntos!) de que tais procedimentos podem ser realizados. Para mais detalhes, confira [13].

Teorema 0.3.4 (Dedekind). *Se $(\mathcal{N}, i, s)$ e $(\mathcal{M}, j, t)$ são sistemas naturais, então existe uma única bijeção $\varphi\colon \mathcal{N} \to \mathcal{M}$ tal que $\varphi(i) = j$ e $\varphi(s(n)) = t(\varphi(n))$ para todo $n \in \mathcal{N}$.*

O teorema acima[24] mostra, entre outras coisas, a *irrelevância* de se apegar a um começo particular na descrição de um sistema natural: o importante é que exista *algum* começo. Também fica justificada a tranquilidade com que profissionais em Matemática *escolhem* um sistema natural arbitrário para desenvolver Aritmética, com a certeza de que os resultados obtidos valerão em qualquer outro sistema[25]. É lícito, portanto, fazer a seguinte

Definição 0.3.5. Vamos denotar por $\mathbb{N}$ *um* sistema natural dado pelo Axioma de Dedekind-Peano, cujos elementos serão chamados de *números naturais*. Além disso:

- $0 \coloneqq \min \mathbb{N}$;
- $1 \coloneqq \mathrm{suc}_{\mathbb{N}}(0)$;
- $2 \coloneqq \mathrm{suc}_{\mathbb{N}}(1)$;
- $3 \coloneqq \mathrm{suc}_{\mathbb{N}}(2)$;
- $4 \coloneqq \mathrm{suc}_{\mathbb{N}}(3)$;
- $5 \coloneqq \mathrm{suc}_{\mathbb{N}}(4)$;
- $6 \coloneqq \mathrm{suc}_{\mathbb{N}}(5)$;
- $7 \coloneqq \mathrm{suc}_{\mathbb{N}}(6)$;
- $8 \coloneqq \mathrm{suc}_{\mathbb{N}}(7)$;
- $9 \coloneqq \mathrm{suc}_{\mathbb{N}}(8)$;

e assim por diante[26]. ¶

O método usado para justificar o Teorema 0.3.4 (chamado de recursão) permite definir de maneira rigorosa as operações usuais de adição e multiplicação em $\mathbb{N}$, bem como verificar suas propriedades principais por indução. Embora seja edificante investir algum período da vida na verificação rigorosa dessas coisas, trata-se de algo mais pertinente a um curso de Aritmética ou de (Introdução a) Teoria dos Números do que a um curso de Análise *Real*. Por isso, todo o arcabouço básico de Aritmética será assumido como conhecido – e, apenas por preciosismo, a verificação de algumas propriedades será sugerida na Subseção "Extras", a seguir. Em particular: $\mathrm{suc}_{\mathbb{N}}(n) \coloneqq n + 1$ de agora em diante.

0.3.1 Extras

Recursão

De acordo com a suposição feita no final da subseção anterior, nós já *sabemos* somar e multiplicar números naturais, o que formalmente consiste em assumir conhecidas funções $(+)\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e $(\cdot)\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ com as propriedades *operatórias* que aprendemos na escola. Com isso em mente, suponha que agora quiséssemos definir a famosa função **fatorial** $F\colon \mathbb{N} \to \mathbb{N}$, que associa cada $n \in \mathbb{N}$ ao número $n!$, de acordo com os seguintes critérios: $0! \coloneqq 1$ e $(n+1)! \coloneqq (n+1) \cdot n!$. Da forma como está posta, é como se a função F fosse usada em sua própria definição, já que

$$F(n+1) = (n+1) \cdot F(n),$$

algo circular e que poderia trazer dor de cabeça.

[24] Cuja demonstração será apresentada na próxima Subseção "Extras".

[25] Por exemplo, fixados sistemas naturais $(\mathcal{N}, i, s)$ e $(\mathcal{M}, j, t)$, suponha que seja verdadeira a asserção "não existe $n \in \mathcal{N}$ tal que $s(n) = n$". Neste caso, também deverá valer que "não existe $m \in \mathcal{M}$ tal que $t(m) = m$": de fato, se existisse m com $t(m) = m$, então ao tomar o único $n \in \mathcal{N}$ com $\varphi(n) = m$, teria-se $t(\varphi(n)) = \varphi(s(n)) = \varphi(n)$, donde a injetividade de φ garantiria $s(n) = n$.

[26] Em posse das operações de adição, multiplicação e *potenciação*, definem-se rigorosamente os sistemas de representação numérica posicional. Em particular, o sistema em base 10 permite descrever todos os números naturais a partir dos números fixados acima.

Porém, secretamente, a função F acima é a *colagem* de uma *família de funções* cuja *existência* é demonstrada por indução: prova-se que para cada $n \in \mathbb{N}$ existe uma função

$$F_n \colon \{m : m \in \mathbb{N} \text{ e } m < n\} \to \mathbb{N}$$

de tal forma que F_{n+1} *estende* F_n para cada $n \in \mathbb{N}$. Daí, para *colar* todas as F_n's numa única F, faz-se $F(m) \coloneqq F_n(m)$ para qualquer $n \in \mathbb{N}$ com $m < n$, o que torna F uma função pois, nas inevitáveis ocorrências de $n, n' > m$ com $n \neq n'$, ou F_n estende $F_{n'}$ (caso $n > n'$) ou $F_{n'}$ estende F_n (caso $n' > n$) e, portanto, $F_n(m) = F_{n'}(m)$. Implicitamente, F é a *reunião* de *todas* as F_n's.

Observação 0.3.6 (Funções revisitadas)**.** Seguindo a Definição 0.0.6 à risca, a descrição de uma função exige que sejam informados domínio e codomínio. No entanto, pode-se relaxar isso: é lícito dizer que uma **função** é meramente um conjunto de pares ordenados com a seguinte propriedade: $y = y'$ sempre que $(x, y), (x, y') \in f$. Em posse de uma função segundo tais critérios, recupera-se uma função no sentido da Definição 0.0.6 fazendo $\operatorname{dom}(f) \coloneqq \{x : \text{existe } y \text{ tal que } (x, y) \in f\}$ e $\operatorname{im}(f) \coloneqq \{y : \text{existe } x \text{ tal que } (x, y) \in f\}$, pois assim f se revela uma função do tipo $\operatorname{dom}(f) \to \operatorname{im}(f)$. A vantagem dessa reformulação é puramente técnica: ela permite falar de conjuntos de funções sem que precisemos explicitar o domínio de cada uma delas, o que deixa a escrita mais limpa. △

Definição 0.3.7. Dadas funções f e g, diz-se que g **estende** f, ou g é uma **extensão** de f, se ocorrer $\operatorname{dom}(f) \subseteq \operatorname{dom}(g)$ e $g(x) = f(x)$ para todo $x \in \operatorname{dom}(f)$. ¶

A seguir, a notação $\bigcup \mathcal{F}$ indica a *reunião* da *família* $\mathcal{F}$, introduzida na Definição 0.1.21.

Lema 0.3.8. *Seja $\mathcal{F}$ uma família de funções. Se, para quaisquer $f, g \in \mathcal{F}$ valer que $f(x) = g(x)$ sempre que $x \in \operatorname{dom}(f) \cap \operatorname{dom}(g)$, então $F \coloneqq \bigcup \mathcal{F}$ é uma função cujo domínio é $\bigcup_{f \in \mathcal{F}} \operatorname{dom}(f)$. Em particular, $F(x) = f(x)$ para qualquer $f \in \mathcal{F}$ com $x \in \operatorname{dom}(f)$.*

Exercício 0.35 $\binom{\star}{\star}$**.** Demonstre o lema acima. Dica: perceba que todo elemento de $\bigcup \mathcal{F}$ é um par ordenado; depois, para $(x, y), (x, z) \in \bigcup \mathcal{F}$, note que devem existir $f, g \in \mathcal{F}$ com $(x, y) \in f$ e $(x, z) \in g$, acarretando $x \in \operatorname{dom}(f) \cap \operatorname{dom}(g)$; conclua que $y = z$. ■

Teorema 0.3.9 (Recursão)**.** *Sejam $(\mathbb{B}, \leq)$ uma boa ordem natural, X um conjunto e $R \colon \mathbb{B} \times X \to X$ uma função*[27]*. Para cada $x \in X$ fixado, existe uma única função $R_x \colon \mathbb{B} \to X$ tal que $R_x(\min \mathbb{B}) = x$ e $R_x(\operatorname{suc}_{\mathbb{B}}(b)) = R(b, R_x(b))$ para cada $b \in \mathbb{B}$.*

Antes de provar o teorema acima, convém observar como ele permite construir funções *na prática*. Para o caso do fatorial, uma vez em posse dos naturais $\mathbb{N}$ e da operação de multiplicação $\cdot \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, tomam-se $\mathbb{B} \coloneqq X \coloneqq \mathbb{N}$, $R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $R(n, m) \coloneqq (n + 1) \cdot m$ e $x \coloneqq 1$. Note então que a função $R_1 \colon \mathbb{N} \to \mathbb{N}$ correspondente é tal que $R_1(0) = 1$ e $R_1(n + 1) = (n + 1) \cdot R_1(n)$ para todo $n \in \mathbb{N}$, i.e., R_1 é a função que faz $n \mapsto n!$, como desejado.

Demonstração. Para cada $b \in \mathbb{B}$, seja $\mathbb{B}_{<b} \coloneqq \{c \in \mathbb{B} : c < b\}$. Vamos dizer que uma função $f \colon \mathbb{B}_{<b} \to X$ é *R_x-recursiva em b* se:

- $b = \min \mathbb{B}$, ou
- $b > \min \mathbb{B}$, $f(\min \mathbb{B}) = x$ e $f(\operatorname{suc}_{\mathbb{B}}(c)) = R(c, f(c))$ para cada $c < b$ tal que $\operatorname{suc}_{\mathbb{B}}(c) < b$.

Observe que para cada elemento $b > \min \mathbb{B}$, existe no máximo uma função R_x-recursiva em b: se tanto f quanto g são R_x-recursivas em b e $c < b$ é tal que $f(c) \neq g(c)$, então existe

$$c'' \coloneqq \min\{c : c < b \text{ e } f(c) \neq g(c)\},$$

com $c'' > \min \mathbb{B}$ (pois $f(\min \mathbb{B}) = g(\min \mathbb{B})$); logo, existe $c' < c''$ com $\operatorname{suc}_{\mathbb{B}}(c') = c''$ e, consequentemente,

$$f(c'') = f(\operatorname{suc}_{\mathbb{B}}(c')) = R(c', f(c')) = R(c', g(c')) = g(\operatorname{suc}_{\mathbb{B}}(c')) = g(c'').$$

Em particular, como uma função R_x-recursiva em b' é também R_x-recursiva em $b \leq b'$ (por quê?!)$^{\star}_{\star}$, segue que se f e g forem R_x-recursivas em b e b', respectivamente, então g estende f. Agora, provaremos que para cada $b \in \mathbb{B}$ *existe* uma função R_x-recursiva em b.

[27] Nesse tipo de situação, escreveremos $R(b, x)$ em vez de $R((b, x))$.

- ✓ (C.I.) Para $b \coloneqq \min \mathbb{B}$, a função R_x-recursiva em b é $\emptyset$.
- ✓ (H.I.) Supondo que existe uma função R_x-recursiva em b, mostraremos que existe função R_x-recursiva em $\mathrm{suc}_{\mathbb{B}}(b)$:
  - ✓ se $b \coloneqq \min \mathbb{B}$, então $\mathbb{B}_{<\mathrm{suc}_{\mathbb{B}}(b)} = \{b\}$ e, assim, basta definir $f(b) \coloneqq x$;
  - ✓ se $b > \min\{\mathbb{B}\}$, então existe $c < b$ com $\mathrm{suc}_{\mathbb{B}}(c) = b$, de modo que $\mathbb{B}_{<b} = \mathbb{B}_{<c} \cup \{c\}$ e $\mathbb{B}_{<\mathrm{suc}_{\mathbb{B}}(b)} = \mathbb{B}_{<c} \cup \{c, b\}$; daí, se $f\colon \mathbb{B}_{<b} \to X$ é a função R_x-recursiva existente por hipótese, basta definir $g\colon \mathbb{B}_{<\mathrm{suc}_{\mathbb{B}}(b)} \to X$ fazendo $g(d) \coloneqq f(d)$ se $d < b$ (i.e., $d \leq c$) e $g(b) \coloneqq R(c, f(c))$.

Ao aliar a indução acima com a argumentação do primeiro parágrafo, resulta que para todo $b \in \mathbb{B}$ existe uma única função R_x-recursiva em b, digamos f_b, de tal forma que $f_{b'}$ estende f_b sempre que $b \leq b'$. Isso *permite considerar a família de funções* $\mathcal{F} \coloneqq \{f_b : b \in \mathbb{B}\}$, que satisfaz as exigências do Lema 0.3.8. Logo, $R_x \coloneqq \bigcup_{b\in\mathbb{B}} f_b$ é uma função da forma $\mathbb{B} \to X$ (verifique!)[28] tal que $R_x(\min \mathbb{B}) = x$ e $R_x(\mathrm{suc}_{\mathbb{B}}(b)) = f_c(\mathrm{suc}_{\mathbb{B}}(b))$ para *qualquer* $c > b$, acarretando

$$R_x(\mathrm{suc}_{\mathbb{B}}(b)) = R(b, f_c(b)) = R(b, R_x(b)),$$

como desejado. Nesta altura do campeonato, você já deve saber como provar que R_x é a única com tal propriedade, certo? □

Exercício 0.36 $(\overset{\star}{\star\star})$**.** Complete a demonstração. ■

Para ilustrar um pouco mais o método da recursão (e tornar este texto mais honesto), vamos ver como definir as operações de adição e multiplicação precisamente – e sem as abanações de mão cometidas em [9, 10].

(+) Para cada $m \in \mathbb{N}$, seja $+_m\colon \mathbb{N} \to \mathbb{N}$ a função que faz $+m(0) = m$ e $+_m(\mathrm{suc}_{\mathbb{N}}(n)) = \mathrm{suc}_{\mathbb{N}}(+_m(n))$ para cada $n \in \mathbb{N}$. Daí, defina $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ por $+(m, n) \coloneqq +_m(n)$, que por simplicidade será denotado por $m + n$.

(·) Para cada $m \in \mathbb{N}$, seja $\cdot_m\colon \mathbb{N} \to \mathbb{N}$ a função que faz $\cdot_m(0) = 0$ e $\cdot_m(\mathrm{suc}_{\mathbb{N}}(n)) = \cdot_m(n) + m$. Daí, defina $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ por $\cdot(m, n) \coloneqq \cdot_m(n)$, que por simplicidade será denotado por $m \cdot n$.

Exercício 0.37 $(\overset{\star}{\star})$**.** Use o Teorema 0.3.9 para garantir a existência das funções acima. Dica: para $+_m$, tome $\mathbb{B} = X = \mathbb{N}$ no enunciado original, com $R\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $R(n, y) \coloneqq \mathrm{suc}_{\mathbb{B}}(y)$ e $x \coloneqq m$; para $\cdot_m$, faça $R(n, y) \coloneqq y + m$ (que existe pelo passo anterior!) e tome $x \coloneqq 0$. ■

A rigor, as funções anteriores são regras arbitrárias que descrevem diferentes formas de iterar a função sucessor de $\mathbb{N}$. Porém, uma vez investigadas as propriedades de tais operações, percebe-se que elas agem de acordo com a experiência empírica. Por exemplo:

Proposição 0.3.10. *Para quaisquer $m, n \in \mathbb{N}$, tem-se $m + n = n + m$.*

Demonstração. Primeiro, tem-se $0 + n = n + 0$ para todo $n \in \mathbb{N}$: por definição, $n + 0 = n$ para todo $n \in \mathbb{N}$; por outro lado, $0 + 0 = 0$ e, se ocorrer $0 + n = n$, então $0 + \mathrm{suc}_{\mathbb{N}}(n) = \mathrm{suc}_{\mathbb{N}}(0 + n) = \mathrm{suc}_{\mathbb{N}}(n)$, donde segue, por indução, que $0 + n = n$ para todo $n \in \mathbb{N}$. Agora, se para $m \in \mathbb{N}$ fixado ocorrer $m + n = n + m$ para todo $n \in \mathbb{N}$, então o mesmo valerá para $\mathrm{suc}_{\mathbb{N}}(m)$, pois... □

Exercício 0.38 $(\overset{\star}{\star\star})$**.** Complete a demonstração anterior. ■

Exercício 0.39 $(\overset{\star}{\star}\star\overset{\star}{\star})$**.** Se estiver com paciência, reconstrua a Aritmética. ■

Observação 0.3.11. Sim, foram cinco estrelas: estas se reservam a exercícios que devem ser feitos no máximo uma vez na vida. △

[28] $(\overset{\star}{\star\star})$: será útil notar que $\bigcup_{b\in\mathbb{B}} \mathbb{B}_{<b} = \mathbb{B}$.

Recursão mais uma vez: demonstração do Teorema 0.3.4

Há pelo menos duas formas de demonstrar o Teorema 0.3.4 (de Dedekind): a primeira, braçal e honesta, e a segunda, rápida e malandra.

Demonstração braçal. Primeiro, note que *se existir* uma função com as propriedades impostas, então ela é única: com efeito, se $\psi\colon \mathcal{N} \to \mathcal{M}$ satisfaz as mesmas condições, então $X := \{n \in \mathcal{N} : \varphi(n) = \psi(n)\}$ é tal que

- ✓ $i \in X$, pois $\varphi(i) = j = \psi(i)$, e
- ✓ se $n \in X$, então $s(n) \in X$, já que $\varphi(s(n)) = t(\varphi(n)) = t(\psi(n)) = \psi(s(n))$,

donde a suposição de $(\mathcal{N}, i, s)$ ser um sistema natural assegura $X = \mathcal{N}$.[29] O restante da prova consiste em fazer uma série de argumentações semelhantes.

Supondo que exista uma função φ satisfazendo $\varphi(i) = j$ e $\varphi(s(n)) = t(\varphi(n))$ para todo $n \in \mathcal{N}$, provaremos que ela deve ser bijetora.

- ✓ É sobrejetora pois $Y := \{m \in \mathcal{M} : \text{existe } n \in \mathcal{N} \text{ com } \varphi(n) = m\}$ é tal que $j \in Y$ (pois $\varphi(i) = j$) e $t(m) \in Y$ sempre que $m \in Y$ (pois se $n \in \mathcal{N}$ é tal que $\varphi(n) = m$, então $s(n) \in \mathcal{N}$ e $\varphi(s(n)) = t(\varphi(n)) = t(m)$), donde segue que $Y = \mathcal{M}$ (já que $(\mathcal{M}, j, t)$ é um sistema natural).
- ✓ Para verificar a injetividade, a ideia é mostrar que se $n \neq n'$, então $\varphi(n) \neq \varphi(n')$.

Em outras palavras, para $n \in \mathcal{N}$ fixado, busca-se provar que $D_n := \{n' \in \mathcal{N} : n' \neq n \Rightarrow \varphi(n') \neq \varphi(n)\}$ satisfaz $D_n = \mathcal{N}$. Tem início a *primeira indução*: mostraremos que $D_i = \mathcal{N}$ (Caso Inicial) bem como $D_{s(n)} = \mathcal{N}$ sempre que $D_n = \mathcal{N}$ (Hipótese Indutiva). Ocorre que para mostrar $D_i = \mathcal{N}$, também precisa-se argumentar por indução! Tem início a segunda indução:

- ✓ $i \in D_i$ (já que a implicação "$i \neq i \Rightarrow \varphi(i) \neq \varphi(i)$" é verdadeira[30]);
- ✓ se $n \in D_i$ para algum $n \in \mathcal{N}$, pode-se ter $n = i$ ou $n \neq i$; no primeiro caso, $s(i) \neq i$ (certo?) e $\varphi(s(i)) = t(\varphi(i)) = t(j) \neq j$ (por quê?!), mostrando que $s(i) \in D_i$; no segundo caso, existe $n' \in \mathcal{N}$ com $s(n') = n$ (pois $(\mathcal{N}, i, s)$ é sistema natural) e $\varphi(s(n)) = t(\varphi(n)) = t(\varphi(s(n'))) = t(t(\varphi(n'))) \neq j$ (pois $t(m) \neq j$ para todo $m \in \mathcal{M} \setminus \{j\}$), mostrando que $s(n) \in D_i$.

O argumento acima encerra a segunda indução, mas não a primeira: mostrou-se apenas que $D_i = \mathcal{N}$; falta provar a segunda parte, i.e., que $D_{s(n)} = \mathcal{N}$ sempre que $D_n = \mathcal{N}$! E para surpresa de ninguém, tal igualdade será mostrada... na terceira indução:

- ✓ como antes, tem-se $s(n) \in D_{s(n)}$ por conta da igualdade $s(n) = s(n)$;
- ✓ agora, se $k \in D_{s(n)}$, deve-se provar que $s(k) \in D_{s(n)}$; se ocorrer $s(k) = s(n)$, nada precisa ser feito; se $s(k) \neq s(n)$, então $k \neq n$ (pois s é função!), enquanto o modo como tomamos n, i.e., satisfazendo $D_n = \mathcal{N}$, garante que $\varphi(k) \neq \varphi(n)$, donde finalmente a injetividade de t atesta $t(\varphi(k)) \neq t(\varphi(n))$, com a suposição sobre φ encerrando o trabalho, já que $\varphi(s(k)) = t(\varphi(k))$ e $\varphi(s(n)) = t(\varphi(n))$.

Portanto, mostrou-se que $D_i = \mathcal{N}$ (C.I.) e $D_{s(n)} = \mathcal{N}$ sempre que $D_n = \mathcal{N}$ (H.I.), exatamente o que se desejava. Falta apenas provar que *existe* uma função $\varphi\colon \mathcal{N} \to \mathcal{M}$ satisfazendo $\varphi(i) = j$ e $\varphi(s(n)) = t(\varphi(n))$ para todo $n \in \mathcal{N}$. Isto se faz via recursão: no enunciado do Teorema da Recursão, substitui-se $\mathbb{B}$ pelo sistema natural $(\mathcal{N}, i, s)$ com a boa ordem descrita no Exercício 0.73, toma-se $X := \mathcal{M}$, $x := j$ e faz-se $R_j : \mathcal{N} \times \mathcal{M} \to \mathcal{M}$ a função dada por $R(n, m) := t(m)$. Logo, $R_j(i) = j$ e

$$R_j(s(n)) = R(n, R_j(n)) = t(R_j(n))$$

para todo $n \in \mathcal{N}$, mostrando que a função φ procurada é, tão somente, R_j. □

A demonstração "rápida e malandra", por sua vez, apenas extrapola o uso do Exercício 0.73 na demonstração anterior: já que sistemas naturais podem ser substituídos por boas ordens naturais, basta provar a "versão bem ordenada" do Teorema de Dedekind.

[29] Na prática, o que se fez foi um argumento indutivo nos moldes da indução clássica descrita no Corolário 0.3.0, porém adaptada para sistemas naturais: provou-se o caso inicial ($i \in X$) e, supondo-se que $n \in X$ (hipótese indutiva), concluiu-se que $s(n) \in X$.

[30] Posto que o seu *antecedente* é falso. Lembre-se de que afirmações do tipo "se P, então Q" só são falsas na ocorrência de *premissas* (P) verdadeiras com *conclusões* (Q) falsas.

Teorema 0.3.12 (de Dedekind, para boas ordens)**.** *Quaisquer duas boas ordens naturais são isomorfas. Além disso, o isomorfismo é único.*

As expressões "isomorfas" e "isomorfismo", que aparecerão no texto com certa frequência, têm definições bem gerais. Porém, por ora, basta saber que, no contexto acima, significam *bijeção crescente*. Mais precisamente, um **isomorfismo entre boas ordens** $(\mathbb{A}, \leq)$ e $(\mathbb{B}, \leq)$ é uma bijeção $\varphi\colon \mathbb{A} \to \mathbb{B}$ tal que $x \leq y \Rightarrow \varphi(x) \leq \varphi(y)$. Moralmente, a única diferença entre boas ordens isomorfas são os nomes de seus elementos, e o isomorfismo faz justamente o processo de *transliteração*[31].

Demonstração. Como de costume, convém começar a prova pela unicidade: se $\varphi, \psi\colon \mathbb{A} \to \mathbb{B}$ fossem isomorfismos distintos, então o conjunto

$$T := \{a \in \mathbb{A} : \varphi(a) \neq \psi(a)\}$$

seria não-vazio e, portanto, existiria $t := \min T$. A pergunta é: quem é t? Note que t não pode ser o menor elemento de $\mathbb{A}$, pois $\varphi(\min \mathbb{A}) = \min \mathbb{B}$ e $\psi(\min \mathbb{A}) = \min \mathbb{B}$ (por quê?)*. Logo, por $\mathbb{A}$ ser boa ordem natural, existe $s \in \mathbb{A}$ tal que $t = \mathrm{suc}_{\mathbb{A}}(s)$. Agora, por minimalidade, deve-se ter $s \notin T$ e, por conseguinte, $\varphi(s) = \psi(s)$. Qual o problema? Este: por φ ser isomorfismo, $\varphi(\mathrm{suc}_{\mathbb{A}}(s)) = \mathrm{suc}_{\mathbb{B}}(\varphi(s))$ (verifique)* e, pela mesma razão, $\psi(\mathrm{suc}_{\mathbb{A}}(s)) = \mathrm{suc}_{\mathbb{B}}(\psi(s))$, ou seja, $\varphi(t) = \psi(t)$.

Resta assim exibir um isomorfismo, o que é bem simples: pelo Teorema da Recursão, a função

$$\begin{aligned} \Phi\colon \mathbb{A} \times \mathbb{B} &\to \mathbb{B} \\ (a, b) &\mapsto \mathrm{suc}_{\mathbb{B}}(b) \end{aligned}$$

induz uma única função $\varphi\colon \mathbb{A} \to \mathbb{B}$ tal que $\varphi(\min \mathbb{A}) = \min \mathbb{B}$ e $\varphi(\mathrm{suc}_{\mathbb{A}}(a)) = \mathrm{suc}_{\mathbb{B}}(\varphi(a))$ para todo $a \in \mathbb{A}$. Onde está a rapidez e malandragem? Resposta: veja abaixo. □

Exercício 0.40 $(^\star_{\star\star})$**.** Mostre que a função φ acima é uma bijeção crescente. ■

Boas ordens não-naturais

Exercício 0.41 $(^\star_{\star\star})$**.** Mostre que a função sucessor $\mathrm{suc}_{\mathbb{B}}\colon \mathbb{B} \to \mathbb{B}$ é injetora em qualquer boa ordem $(\mathbb{B}, \leq)$ em que todo elemento tenha sucessor. ■

A sutileza do exercício anterior é notar que na parte final da demonstração do Teorema 0.3.3, utilizou-se apenas o fato de todo elemento de $\mathbb{B}$ ter sucessor – e não a suposição de que todo elemento $\neq \min \mathbb{B}$ é sucessor de alguém. Isto levanta a pergunta: existem boas ordens satisfazendo a primeira condição mas não a segunda? Certamente!

Exemplo 0.3.13. Embora tenhamos pouca informação acerca de $\mathbb{N}$ (assumimos apenas que se trata de uma boa ordem/sistema natural), parace razoável dizer que existe $u' \notin \mathbb{N}$. Acontece que em posse disso, a Proposição 0.2.15 nos diz que $\mathbb{N}' := \mathbb{N} \cup \{u'\}$ admite uma boa ordem que tem u' como último elemento! É claro que, agora, nem todo elemento de $\mathbb{N}'$ tem sucessor: justamente por u' ser o último elemento, *ninguém* está acima dele. Porém, note que curioso: u' também não é sucessor (imediato) de ninguém! De fato, se $x \in \mathbb{N}'$ é tal que $x < u'$, então $x \in \mathbb{N}$ e, dessa forma, $\mathrm{suc}_{\mathbb{N}}(x) := x + 1 \in \mathbb{N}$ e, por isso, $x + 1 < u'$ (reveja a Definição 0.2.11 ou o Exercício 0.27 caso tenha se esquecido do que *significa* ser sucessor). ▲

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow \cdots \longrightarrow n+1 \longrightarrow \cdots \qquad u'$$

Figura 0.5: Se uma boa ordem não tem último elemento, basta acrescentá-lo.

Embora pareça artificial, o cenário acima é bem comum na verdade: ao encontrar *sequências convergentes em* $\mathbb{R}$, por exemplo, podemos pensar nos termos da sequência *ordenados* por $\mathbb{N}$, de modo que o ponto adicional acrescentado acima faz meramente o papel de *limite*.

Por que parar? Chamando $\mathbb{N}_0 := \mathbb{N}$ e $\mathbb{N}_1 := \mathbb{N} \cup \{u'\}$, ainda parece razoável a existência de algum objeto $u'' \notin \mathbb{N}_1$, o que permite definir $\mathbb{N}_2 := \mathbb{N}_1 \cup \{u''\}$. Analogamente, parecece razoável definir $\mathbb{N}_3$, $\mathbb{N}_4$... Ao repetir esse processo para todo $n \in \mathbb{N}$, chega-se a uma boa ordem $\mathbb{B}$ em que todo elemento tem sucessor, mas tal que $\mathbb{B}$ não é natural! Caso tenha achado interessante, confira [13] para mais detalhes.

[31] Como na Figura 0.4 da página 32.

Afinal, zero é natural?

É comum haver certo debate acerca da corretude de se assumir que $0 \in \mathbb{N}$. Embora se trate apenas de um símbolo utilizado para indicar o menor elemento de $\mathbb{N}$, as definições recursivas adotadas para a soma e a multiplicação escondem um *viés* ideológico: *naturalizar* o *vazio* (confira o Exercício 0.74).

Mais precisamente, na próxima seção, em que a noção de *cardinalidade* entre conjuntos arbitrários será, finalmente, apresentada, os elementos de $\mathbb{N}$ serão usados como *parâmetros* de finitude, num procedimento formal que apenas imita a noção de contagem. E é justamente aí que começa o problema: como contar os elementos do vazio?

- ✗ Quem defende "$0 \notin \mathbb{N}$" argumenta que ao *contar* os elementos em $\{a, b, c\}$, escolhe-se o *primeiro*, o *segundo* e, finalmente, o *terceiro*, de modo que ao término do processo se chega ao *número de elementos do conjunto*: 3. Há também quem apele a fatores históricos e etimológicos, já que a "noção do zero" ocorreu de maneira relativamente tardia, justificando assim que não se trate de uma ideia *natural*. Moral da história: não se contam os elementos de $\emptyset$.
- ✓ Já quem defende "$0 \in \mathbb{N}$" costuma pensar nos números naturais mais como *registradores* do processo de contagem: ao se iniciar a indexação a partir do 0, o *número de elementos do conjunto* será o menor número maior que os índices utilizados na indexação. Assim, por exemplo, como nem se começa a contagem dos elementos do vazio, o conjunto vazio deve ter $\min\{n \in \mathbb{N} : n > x \text{ para todo } x \in \emptyset\} = 0$ elementos (pense a respeito!). Já no caso de $\{a, b, c\}$, tem-se o 0-ésimo elemento, o 1-ésimo elemento e, finalmente, o 2-ésimo elemento, de modo que $\{a, b, c\}$ terá $\min\{n \in \mathbb{N} : n > 0, n > 1 \text{ e } n > 2\} = 3$ elementos.

Certamente, a postura "$0 \notin \mathbb{N}$" tem a vantagem de ser conceitualmente mais simples, talvez por sua proximidade com a experiência empírica. No entanto, ela é tecnicamente limitada: fica relativamente mais custoso descrever, por exemplo, o sistema numérico posicional utilizado corriqueiramente para dar sentido a coisas como "19", essencialmente pela *ausência* de um *neutro* aditivo que *anule* a multiplicação; também ao expressar fórmulas de *cardinalidade*, como $|A \cup B| = |A| + |B| - |A \cap B|$ para conjuntos finitos A e B, por exemplo, precisa-se excluir os casos que envolvem o conjunto vazio, já que não se define $|\emptyset|$ como um número *digno* de ser operado com os *naturais*.

Porém, acredito que o argumento mais forte em favor de se adotar $0 \in \mathbb{N}$ seja o da *azeitona*[32]. Como você pode verificar por indução, para todo $n \in \mathbb{N}$ (com 0 incluso), existe bijeção entre $\mathbb{N}_{<n} := \{m : m \in \mathbb{N} \text{ e } m < n\}$ e $\mathbb{N}_{<n+1} \setminus \{0\}$, o que na prática significa o que você sempre soube: "contar de 1 até n e gritar n" é equivalente a "contar de 0 até $n-1$ e gritar n". Em outras palavras: se não quiser a azeitona na pizza, basta tirá-la da sua fatia e, se quiser depois, basta pegá-la de volta! Inclusive, isto será feito com frequência ao longo do texto.

0.4 As diferentes noções de (in) finitude

0.4.0 Essencial

Conjuntos finitos

O final da discussão realizada na Subseção 0.1.1 sugeriu definir *número cardinal* como um tipo de *representante* da relação $\approx$ que declara dois conjuntos A e B como equivalentes quando existe uma bijeção entre eles. Aqui, vamos executar esta ideia – pelo menos para conjuntos *finitos*. Por falar neles:

Definição 0.4.0. Diremos que um conjunto X é **finito** se para algum $n \in \mathbb{N}$ existir bijeção entre X e $\mathbb{N}_{<n} := \{m : m \in \mathbb{N} \text{ e } m < n\}$. Conjuntos *não*-finitos serão xingados de **infinitos**. ¶

Exercício 0.42 ($\star$)**.** Sejam X e Y conjuntos tais que $X \approx Y$. Mostre que X é finito se, e somente se, Y é finito. ■

[32] Há outros, relativamente mais abstratos que fogem ao escopo deste material.

Note que pela definição acima, $\emptyset$ é finito, posto que $\mathbb{N}_{<0} = \emptyset$. Também são finitos os conjuntos unitários, i.e., da forma $\{x\}$, por estarem em bijeção com $\mathbb{N}_{<1} = \{0\}$, bem como os conjuntos da forma $\{x, y\}$ com $x \neq y$, por estarem em bijeção com $\mathbb{N}_{<2} = \{0, 1\}$, etc. Como os casos iniciais sugerem, se X é finito, então o número $n \in \mathbb{N}$ na definição de *finitude* é único, precisamente o tipo de comportamento esperado dos representantes de uma relação de equivalência.

Teorema 0.4.1. *Se X é finito, então existe um único $n \in \mathbb{N}$ com $X \approx \mathbb{N}_{<n}$.*

Demonstração. A definição garante a existência do número natural n. Para provar sua unicidade, considere $m, n \in \mathbb{N}$ com $X \approx \mathbb{N}_{<m}$ e $X \approx \mathbb{N}_{<n}$. Como a *relação* $\approx$ é simétrica e transitiva, resulta que $\mathbb{N}_{<m} \approx \mathbb{N}_{<n}$. Logo, basta argumentar pela contrapositiva: vamos supor $m \neq n$ a fim de concluir que não existe bijeção entre $\mathbb{N}_{<m}$ e $\mathbb{N}_{<n}$. Isto encerrará a prova, posto que pela observação inicial, a ocorrência de $X \approx \mathbb{N}_{<m}$ e $X \approx \mathbb{N}_{<n}$ *acarretará* $m = n$, como desejado.

⌜**Afirmação.** *Se $Y \subsetneq \mathbb{N}_{<n}$, então não existe bijeção entre $\mathbb{N}_{<n}$ e Y.*

Demonstração. O argumento será feito por indução em n, com o caso $n := 0$ imediato (certo?). Supondo a afirmação verdadeira para $n \in \mathbb{N}$ fixado, veremos que a existência de uma bijeção φ entre $\mathbb{N}_{<n+1} = \mathbb{N}_{<n} \cup \{n\}$ e $Y \subsetneq \mathbb{N}_{<n+1}$ resultaria numa bijeção entre $\mathbb{N}_{<n}$ e um subconjunto próprio de $\mathbb{N}_{<n}$, contrariando a *hipótese de indução*[33]:

- ✓ se $n \notin Y$, então $Y \subsetneq \mathbb{N}_{<n}$ e, portanto, a restrição de φ a $\mathbb{N}_{<n}$ seria uma bijeção entre $\mathbb{N}_{<n}$ e $Y' := Y \setminus \{\varphi(n)\}$, um subconjunto próprio de $\mathbb{N}_{<n}$;
- ✓ se $n \in Y$, então existe $k \leq n$ com $\varphi(k) = n$, de modo que a função $g\colon \mathbb{N}_{<n} \to Y \setminus \{n\}$, que faz $g(i) := \varphi(i)$ para $i \neq k$ e $g(k) := \varphi(n)$ caso $k < n$, é uma bijeção – e $Y \setminus \{n\} \subsetneq \mathbb{N}_{<n}$. ⌟

Agora, note que por $(\mathbb{N}, \leq)$ ser uma boa ordem, não há perda de generalidade em supor $m < n$, já que a ordem é total. Daí, $\mathbb{N}_{<m} \subsetneq \mathbb{N}_{<n}$, o que segue pois $m \in \mathbb{N}_{<n} \setminus \mathbb{N}_{<m}$ (e todo $k < m$ também satisfaz $k < n$, pela transitividade da ordem). Logo, pela afirmação, não existe bijeção entre $\mathbb{N}_{<m}$ e $\mathbb{N}_{<n}$, como queríamos. □

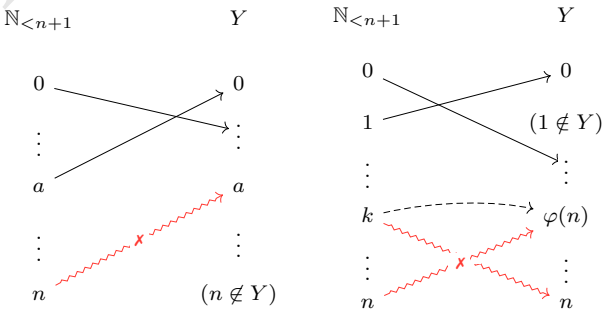


Figura 0.6: A demonstração anterior, em cores.

Definição 0.4.2. Dado um conjunto X finito, indicaremos por $|X|$ o único número natural em bijeção com X, que será chamado de **número cardinal de** X. ¶

[33] Em outras palavras, trata-se do passo indutivo usual, porém escrito na contrapositiva: "se **não** vale o caso $n + 1$, então também **não** vale o caso n".

Observação 0.4.3 (Alerta)**.** É comum encontrar obras que utilizam "$\#X$" para indicar o número cardinal de X. Porém, isto não será feito aqui – mas você é livre para escrever assim se preferir[34]. △

Portanto, como prometido, os números naturais cumprem o papel de representantes (das cardinalidades) dos conjuntos finitos, por meio de bijeções que abstraem os processos de contagem. Como efeito colateral, todas as *ferramentas* típicas de $\mathbb{N}$, desde suas operações até as argumentações por indução, ficam disponíveis para analisar questões que envolvam a cardinalidade de conjuntos finitos. Para praticar, confira o Exerício 0.63.

Conjuntos infinitos enumeráveis e não-enumeráveis

Além de firmar a posição dos números naturais como os cardinais de conjuntos finitos, a demonstração do último teorema também sugere, sem alarde, um critério para decidir se um conjunto é infinito. A seguir, $\varphi[Y] \coloneqq \{\varphi(y) : y \in Y\}$ indica a *imagem de um subconjunto* $Y \subseteq X$ por uma função φ que tem X como domínio[35].

Corolário 0.4.4 (da demonstração do Teorema 0.4.1)**.** *Se X admite bijeção com um subconjunto próprio $Y \subsetneq X$, então X é infinito.*

Demonstração. O diagrama a seguir resume a ideia:

$$\begin{array}{ccc} Y & \xrightarrow{\text{bijeção}} & X \\ {\scriptstyle \varphi|_Y}\downarrow \uparrow {\scriptstyle (\varphi|_Y)^{-1}} & & \downarrow{\scriptstyle \varphi} \\ \varphi[Y] & \subsetneq & \mathbb{N}_{<n} \end{array}$$

Se existisse uma bijeção $\varphi\colon X \to \mathbb{N}_{<n}$ para *algum* $n \in \mathbb{N}$, então existiria uma bijeção entre $\varphi[Y] \subsetneq \mathbb{N}_{<n}$ e $\mathbb{N}_{<n}$, contrariando a afirmação provada ao longo da demonstração do Teorema 0.4.1. Os detalhes ficam por sua conta $\binom{\star}{\star}$. □

Corolário 0.4.5. *$\mathbb{N}$ é infinito.*

Demonstração. A correspondência $n \mapsto n+1$ define uma bijeção entre $\mathbb{N}$ e $\mathbb{N} \setminus \{0\}$. □

A constatação de que existe um conjunto infinito cria um problema *momentâneo* na definição dos números cardinais: como nenhum número natural serve para representar a *cardinalidade* de $\mathbb{N}$, não parece haver uma noção natural de número que mereça ser xingada de $|\mathbb{N}|$. *Mas isto não deveria ser um problema, já que apenas os conjuntos infinitos ficaram sem cardinais e todos eles têm a mesma cardinalidade, justamente por serem infinitos... certo? Não bastaria fazer $|\mathbb{N}| \coloneqq \infty$?* A situação não é tão simples.

Teorema 0.4.6 (Cantor)**.** *Dado um conjunto X, não existe sobrejeção $X \to \wp(X)$.*

Demonstração. Para uma função $\varphi\colon X \to \wp(X)$, o conjunto $T \coloneqq \{x \in X : x \notin \varphi(x)\}$ atesta a não-sobrejetividade de φ: se ocorresse $\varphi(t) = T$ para algum $t \in X$, a definição de T daria "$t \in T \Leftrightarrow t \notin \varphi(t) = T$", uma contradição. Logo, não há sobrejeção $X \to \wp(X)$. □

[34] Eu ficarei triste? Sim. Mas vou sobreviver.

[35] Caso precise revisar esse assunto, confira o Exercício 0.54.

Exercício 0.43 ($\overset{\star}{\star\star}$)**.** Mostre que se $X \subseteq Y$ e Y é finito, então X é finito. Observação: este é o terceiro item do Exercício 0.63. ■

Corolário 0.4.7. *Se X é infinito, então $\wp(X)$ é infinito e $X \not\approx \wp(X)$.*

Demonstração. Como a correspondência $x \mapsto \{x\}$ define uma função injetora $X \to \wp(X)$, segue que se $\wp(X)$ fosse finito, então X estaria em bijeção com um subconjunto (finito!) de $\wp(X)$ e, portanto, X seria finito. O restante segue do Teorema de Cantor. □

Em particular, $\mathbb{N}$ e $\wp(\mathbb{N})$ são conjuntos infinitos que *não* têm a mesma cardinalidade, ou seja: existem cardinalidades infinitas distintas entre si, o que mostra a inefetividade de se escrever "$|X| = \infty$" para representar os números cardinais de conjuntos infinitos[36]. Para contornar o problema, costuma-se fazer o seguinte.

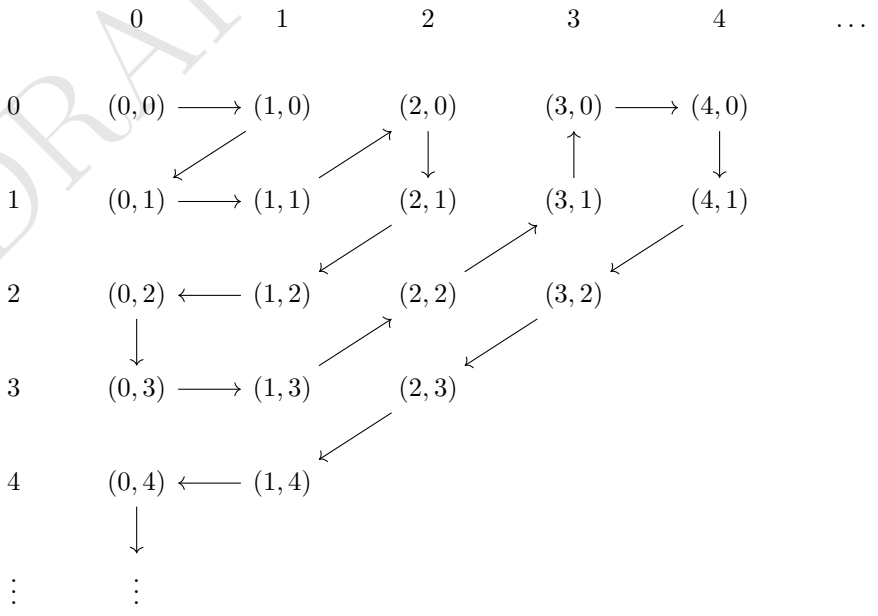
Definição 0.4.8. Diremos que X é **enumerável** se existir função injetora da forma $X \to \mathbb{N}$. Nas situações em que se puder garantir a existência de bijeção $X \to \mathbb{N}$ (e isto precisar ser explicitado), X será dito **infinito enumerável**. Por fim, diremos que X é **não-enumerável** se X *não for* enumerável, i.e., se não existir injeção $X \to \mathbb{N}$. ¶

Exercício 0.44 ($\star$)**.** Mostre que se X é não-enumerável, então X é infinito. ■

Proposição 0.4.9. *$\mathbb{N} \times \mathbb{N}$ é (infinito!) enumerável.*

Demonstração. A função $n \mapsto (0, n)$ define uma injeção $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Por outro lado, como você deve saber de suas aulas de Aritmética (ou afins), a correspondência $(m, n) \mapsto 2^m 3^n$ define uma função injetora $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Logo, o resultado segue do Teorema de Cantor-Bernstein. □

Os primeiros contatos com esse tipo de resultado costumam ser estranhos, já que parece ser claro que $\mathbb{N} \times \mathbb{N}$ deveria ter bem mais elementos do que $\mathbb{N}$: com efeito, $\mathbb{N} \times \mathbb{N} = \bigcup_{n \in \mathbb{N}} \mathbb{N} \times \{n\}$, i.e., é uma *reunião* enumerável de conjuntos enumeráveis dois a dois disjuntos e, mesmo assim, sua cardinalidade não excede a cardinalidade de $\mathbb{N}$. Contudo, uma simples ilustração ajuda a tornar a coisa toda mais palatável.



[36] Pelo menos se a intenção for fazer tal atribuição com o mínimo de decência.

Como o diagrama acima sugere, pode-se determinar uma bijeção da forma $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ ao *percorrer* $\mathbb{N} \times \mathbb{N}$ num zigue-zague maroto. O mesmo tipo de *percurso* também ajuda a perceber que o *conjunto dos números racionais* é infinito enumerável: a única diferença é que precisa-se evitar representações *equivalentes* de um mesmo número racional já *percorrido*, pois sem isso a injetividade se perde. Mas isto não é um problema, na verdade.

Teorema 0.4.10 (©)**.** *Uma função $f\colon X \to Y$ é sobrejetora se, e somente se, existe uma injeção $g\colon Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$. Em particular, $Y \precsim X$ se, e somente se, $X \succsim Y$.*

Demonstração. Se a função g existe como no enunciado, então a sobrejetividade de f segue do Exercício 0.14 (a menos da ordem das letras). A parte delicada é a recíproca: como cozinhar uma função $g\colon Y \to X$ satisfazendo $f \circ g = \mathrm{Id}_Y$? Note que a identidade procurada se traduz em pedir $f(g(y)) = y$ para todo $y \in Y$. Na prática, isto significa dizer que $g(y) \in X$ é *algum* elemento de X que é *levado* até y por f.

Algum $x \in X$ satisfaz $f(x) = y$, posto que f é sobrejetora por hipótese, o que garante $P_y := f^{-1}[\{y\}] \neq \emptyset$ para todo $y \in Y$. Ocorre que $\mathcal{P} := \{P_y : y \in Y\}$ é uma partição de X (certo?!)*, de tal maneira que o *insuspeito* Teorema 0.1.27 assegura uma classe de representantes para $\mathcal{P}$, digamos $\mathcal{R}$. Com isso, basta definir $g(y) := r$, onde r é o único elemento de $\mathcal{R}$ pertencente a $\mathcal{P}_y$, que satisfaz a identidade $f(g(y)) = y$ por *construção*. □

Corolário 0.4.11 (©)**.** *Se $f\colon X \to Y$ é sobrejetora, então $Y \precsim X$.*

Corolário 0.4.12 (©)**.** *Seja $\mathcal{X} := \{X_n : n \in \mathbb{N}\}$ uma família de conjuntos enumeráveis. Então $\bigcup \mathcal{X}$ é enumerável.*

Demonstração. Para cada $n \in \mathbb{N}$, seja $\mathrm{Sob}(\mathbb{N}, X_n)$ o conjunto das funções sobrejetoras da forma $\mathbb{N} \to X_n$. Como $\mathrm{Sob}(\mathbb{N}, X_n) \neq \emptyset$, podemos *escolher* $f_n \in \mathrm{Sob}(\mathbb{N}, X_n)$ para cada $n \in \mathbb{N}$ (como na demonstração do Teorema 0.1.27). Com isso, pode-se definir $f\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} X_n$ a função que faz $(m, n) \mapsto f_m(n)$. Note que se $x \in \bigcup_{n\in\mathbb{N}} X_n$, então existe $m \in \mathbb{N}$ com $x \in X_m$, bem como $n \in \mathbb{N}$ tal que $f_m(n) = x$, i.e., $f(m, n) = x$. Logo, f é sobrejetora, acarretando $\bigcup \mathcal{X} \precsim \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$. □

Tais resultados podem ser usados para mostrar que os típicos conjuntos $\mathbb{Z}$ (dos números inteiros) e $\mathbb{Q}$ (dos números racionais), embora infinitos, têm a mesma caradinalidade de $\mathbb{N}$, o que pode parecer muito estranho. Por um lado, isto se deve ao fato de a *construção* dos conjuntos em questão ter sido feita por meio de métodos que não *aumentam* cardinalidades infinitas (vide Proposição 0.4.9). Por outro lado, a *menor* cardinalidade infinita é a de $\mathbb{N}$, no seguinte sentido:

Teorema 0.4.13 (©)**.** *Se X é infinito, então $\mathbb{N} \precsim X$.*

Demonstração. A ideia é simples: por X ser infinito, não existe $n \in \mathbb{N}$ com uma bijeção $\mathbb{N}_{<n} \to X$; logo, se $n \in \mathbb{N}$ e $\varphi\colon \mathbb{N}_{<n} \to X$ for uma função injetora, então $X \setminus \mathrm{im}\,(\varphi)$ é não-vazio, o que permite *escolher*, *recursivamente*, sequências finitas *cada vez maiores* de modo a obter uma injeção $\mathbb{N} \to X$. Parece honesto, certo? □

Exercício 0.45 ($\overset{\star}{\star}$)**.** Para um conjunto X, mostre que as seguintes afirmações são equivalentes:

a) o conjunto X é infinito (não existe $n \in \mathbb{N}$ com uma bijeção $\mathbb{N}_{<n} \to X$);

b) existe uma função injetora $\mathbb{N} \to X$;

c) existe uma função bijetora $X \to Y$, com $Y \subsetneq X$. ■

Saber que $\mathbb{N}$ tem "*a menor cardinalidade infinita*" sugere a pergunta *natural*: qual é a *próxima* cardinalidade? Certamente, aplicações sucessivas do Teorema de Cantor resultam em diversas cardinalidades não-enumeráveis: $\mathbb{N} \prec \wp(\mathbb{N}) \prec \wp(\wp(\mathbb{N})) \prec \ldots$, o que não responde a pergunta, já que *poderia existir* X com $\mathbb{N} \prec X \prec \wp(\mathbb{N})$, caso em que a cardinalidade de $\wp(\mathbb{N})$ não seria a "*próxima*"[37]. Voltaremos a isso, mas não agora. Em todo caso, resta apenas um fato inócuo sobre conjuntos não-enumeráveis para ser apresentado – e, devido à sua simplicidade, a verificação ficará por sua conta.

Exercício 0.46 (Princípio da Casa dos Pombos ($\star_\star$))**.** Sejam X um conjunto não-enumerável e $A, B \subseteq X$ subconjuntos disjuntos satisfazendo $X = A \cup B$. Mostre que deve ocorrer $\mathbb{N} \prec A$ ou $\mathbb{N} \prec B$, i.e., (pelo menos) um deles deve ser não-enumerável. Dica: suponha que não. ■

0.4.1 Extras

Uma demonstração para o Teorema de Cantor-Bernstein

É importante ter em mente que a demonstração que veremos não é terrivelmente difícil e muito menos feia – ela é belíssima. No entanto, ela requer atenção e tempo, e o segundo recurso costuma ser escasso nas disciplinas de Análise. Recordemo-nos de seu enunciado:

Teorema de Cantor-Bernstein. Se existem funções injetoras $X \to Y$ e $Y \to X$, então existe bijeção $X \to Y$.

Você não deve esperar que a demonstração do Teorema de Cantor-Bernstein envolva a prova de que as injeções são sobrejetivas[38]: a ideia é *construir* uma "nova" função (bijetora) a partir das injeções dadas. Embora a coisa seja mais simples do que parece, alguns ingredientes preliminares devem ser introduzidos.

Definição 0.4.14. Para um conjunto $\mathcal{S}$, define-se $\bigcap \mathcal{S} := \{x : x \in S \text{ para todo } S \in \mathcal{S}\}$, a **interseção da família** $\mathcal{S}$. Nas ocasiões em que $\mathcal{S} := \{S_i : i \in \mathcal{I}\}$ para algum conjunto $\mathcal{I}$ fixado, também é comum escrever $\bigcap_{i\in\mathcal{I}} S_i$ ou $\bigcap_{i\in\mathcal{I}} S_i$. ¶

O dispositivo acima apenas cria um modo bastante esperto de evitar abominações notacionais como "$S_0 \cap S_1 \cap \ldots$" quando se quer expressar uma interseção (possivelmente) infinita de conjuntos. Fora isso, ela *quase* não traz novidades: note, por exemplo, que para $\mathcal{S} := \{X, Y\}$, tem-se $\bigcap \mathcal{S} = X \cap Y$.

Lema 0.4.15 (Leis de De Morgan)**.** *Sejam X e $\mathcal{Y}$ conjuntos, com $\mathcal{Y} \neq \emptyset$.*

(i) $\displaystyle\bigcap_{B\in\mathcal{Y}} (X \setminus B) = X \setminus \bigcup_{B\in\mathcal{Y}} B.$

(ii) $\displaystyle\bigcup_{B\in\mathcal{Y}} (X \setminus B) = X \setminus \bigcap_{B\in\mathcal{Y}} B.$

Demonstração. Se $x \in \bigcap_{B\in\mathcal{Y}}(X \setminus B)$, então para todo $B \in \mathcal{Y}$ tem-se $x \in X \setminus B$, donde segue que $x \in X$ e não existe $B \in \mathcal{Y}$ tal que $x \in B$, i.e., $x \in X$ e $x \notin \bigcup_{B\in\mathcal{Y}} B$, precisamente $x \in X \setminus \bigcup_{B\in\mathcal{Y}} B$. Pela arbitrariedade do x tomado, segue que $\bigcap_{B\in\mathcal{Y}}(X \setminus B) \subseteq X \setminus \bigcup_{B\in\mathcal{Y}} B$. A recíproca é análoga (faça!)$^\star_\star$.

Para provar o segundo item, note que se $x \in \bigcup_{B\in\mathcal{Y}}(X \setminus B)$, então existe $B' \in \mathcal{Y}$ com $x \in X \setminus B'$, i.e., $x \in X$ e $x \notin B'$ para algum $B' \in \mathcal{Y}$, donde se infere que $x \notin \bigcap_{B\in\mathcal{Y}} B$ e, por conseguinte, $x \in X \setminus \bigcap_{B\in\mathcal{Y}} B$. Logo, $\bigcup_{B\in\mathcal{Y}}(X \setminus \mathcal{Y}) \subseteq X \setminus \bigcap_{B\in\mathcal{Y}} B$. Novamente, a recíproca é análoga (já sabe né?)$^\star_\star$. □

Exercício 0.47 ($\star$)**.** Para conjuntos A, B e C, mostre que $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ e $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$. ■

[37] Em particular fica o **alerta**: afirmações do tipo "X e Y são não-enumeráveis" não significam, *a priori*, que X e Y tenham a mesma cardinalidade, mas apenas que ambas as cardinalidades são *maiores* do que a cardinalidade de $\mathbb{N}$.

[38] Lembre-se da função sucessor!

Lema 0.4.16. *Sejam $f\colon X \to Y$ uma função e considere famílias $\mathcal{U}$ e $\mathcal{V}$ de subconjuntos de X e de Y, respectivamente. Então:*

(i) $f\left[\bigcup \mathcal{U}\right] = \bigcup_{U\in\mathcal{U}} f[U]$ *e* $f\left[\bigcap \mathcal{U}\right] \subseteq \bigcap_{U\in\mathcal{U}} f[U]$*, com igualdade garantida no último caso se f for injetora;*

(ii) $f^{-1}\left[\bigcup \mathcal{V}\right] = \bigcup_{V\in\mathcal{V}} f^{-1}[V]$ *e* $f^{-1}\left[\bigcap \mathcal{V}\right] = \bigcap_{V\in\mathcal{V}} f^{-1}[V]$.

Exercício 0.48 $\left(\overset{\star}{\star}\right)$**.** Demonstre o lema anterior. ■

Demonstração do Teorema de Cantor-Bernstein. Fixadas funções injetoras $f\colon X \to Y$ e $g\colon Y \to X$, vamos obter partições $\{S, S'\}$ e $\{T, T'\}$ de X e Y, respectivamente, tais que $f[S] = T$ e $g[T'] = S'$ pois, se isso for feito, o teorema estará demonstrado (confira o Exercício 0.49). Para obter tal partição, note que qualquer subconjunto $S \subseteq X$ induz tanto uma partição em X quanto uma partição em Y: basta definir $S' := X \setminus S$, $T := f[S]$ e $T' := Y \setminus T$. Isso resolve *metade* do problema, dado que ainda é preciso garantir a identidade $g[T'] = S'$, essencial para definir a bijeção h. Ao se reescrever a igualdade $g[T'] = S'$ em *função* de S, obtém-se a identidade $g\left[Y \setminus f[S]\right] = X \setminus S$, equivalentemente exprimível como $S = X \setminus g\left[Y \setminus f[S]\right]$. Como obter tal S?

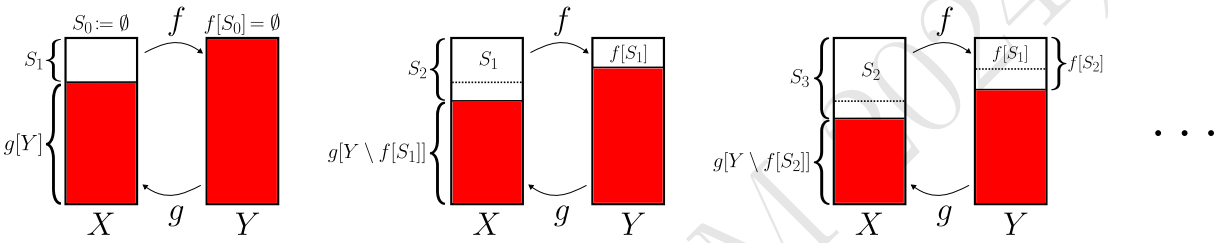


Figura 0.7: Heurística da construção recursiva do conjunto S.

Seja $S_0 := \emptyset$ e, para $n \in \mathbb{N}$ qualquer, $S_{n+1} := X \setminus g\left[Y \setminus f[S_n]\right]$. O subconjunto $S := \bigcup_{n\in\mathbb{N}} S_n$ satisfaz a identidade desejada, pois

$$\begin{aligned} S := \bigcup_{n\in\mathbb{N}} S_n = \bigcup_{n\in\mathbb{N}} S_{n+1} = \bigcup_{n\in\mathbb{N}} \left(X \setminus g\left[Y \setminus f[S_n]\right]\right) = X \setminus \bigcap_{n\in\mathbb{N}} g\left[Y \setminus f[S_n]\right] \overset{*}{=} \\ \overset{*}{=} X \setminus g\left[\bigcap_{n\in\mathbb{N}} \left(Y \setminus f[S_n]\right)\right] = X \setminus g\left[Y \setminus \bigcup_{n\in\mathbb{N}} f[S_n]\right] = X \setminus g\left[Y \setminus f\left[\bigcup_{n\in\mathbb{N}} S_n\right]\right] = \\ = X \setminus g\left[Y \setminus f\left[S\right]\right], \end{aligned}$$

onde a igualdade $(*)$ decorre da injetividade de g (lema anterior), enquanto as outras seguem das leis de De Morgan. □

Exercício 0.49 $\left(\overset{\star}{\star}\right)$**.** Mostre que se $F\colon A \to B$ e $G\colon C \to D$ são bijeções com $A \cap C = B \cap D = \emptyset$, então $F \cup G$ é uma bijeção da forma $A \cup C \to B \cup D$. Use isto para obter a bijeção procurada no teorema anterior. Dica: faça $A := S$, $B := f[S]$, $C := g[T']$ e $D := T'$, com $F := f|_S$ e $G := (g|_{T'})^{-1}$. ■

Portanto, a fim de estabelecer a *existência* de uma bijeção entre conjuntos X e Y, basta exibir injeções $X \to Y$ e $Y \to X$, sem a necessidade de explicitar uma bijeção particular. Isto será feito, por exemplo, quando provarmos a *não-enumerabilidade* de $\mathbb{R}$ por meio de uma bijeção entre $\mathbb{R}$ e $\wp(\mathbb{N})$, cuja *existência* será garantida por funções injetoras da forma $\mathbb{R} \to \wp(\mathbb{N})$ e $\wp(\mathbb{N}) \to \mathbb{R}$.

Construção dos inteiros e dos racionais

Um dos modos de *motivar* a *introdução* dos números inteiros é dar *significado* a expressões como "$5 - 7$", que não têm sentido no contexto natural: tipicamente, uma expressão da forma "$m - n$" em $\mathbb{N}$ corresponde à cardinalidade resultante de um conjunto com m elementos após a exclusão de n elementos; logo, se $m < n$, então não se pode realizar tal procedimento. Todavia, como os Bancos nos ensinam desde tempos imemoriais, é possível registrar "quanto falta": no caso, faz-se "$7 - 5 = 2$", e escreve-se "$5 - 7 = -2$" para indicar a natureza "negativa" do resultado[39].

[39] A aceitação dos números negativos pela comunidade matemática foi relativamente tardia – ainda no Século XIX havia quem encrencasse com eles. Quem gostar de aspectos históricos pode conferir [15].

Para *descrever* o nosso entendimento do que os inteiros *deveriam* ser dentro do cenário formal que se desenrola, pode-se observar o seguinte: embora coisas como "$5-7$" e "$3-5$" (que deveriam resultar em -2) não tenham significado em $\mathbb{N}$, a *informação* transmitida por tais expressões pode ser *codificada* em $\mathbb{N}$: em vez de escrever $5-7=3-5$, redistribuem-se as parcelas de modo a se obter uma igualdade entre somas positivas, i.e., $5+5=7+3$. Em outras palavras, duas *expressões* $a-b$ e $c-d$ são iguais (no que gostaríamos que fosse $\mathbb{Z}$) se, e somente se, $a+d$ e $b+c$ são iguais em $\mathbb{N}$. Em linguajar técnico:

Exercício 0.50 $\binom{\star}{\star\star}$**.** Sobre $Z \coloneqq \mathbb{N}\times\mathbb{N}$, considere a relação $\sim$ que declara $(a,b)\sim(c,d)$ se, e somente se, $a+d=b+c$.

a) Mostre que $\sim$ é uma relação de equivalência. Dica: para a transitividade, use a *lei do cancelamento*, i.e., "$a=b$ sempre que $a+c=b+c$, para quaisquer $a,b,c\in\mathbb{N}$".

b) Mostre que se $(a,b)\sim(a',b')$ e $(c,d)\sim(c',d')$, então $(a+c,b+d)\sim(a'+c',b'+d')$.

c) Mostre que ao definir $\overline{(a,b)}+'\overline{(c,d)}\coloneqq\overline{(a+c,b+d)}$, o resultado *independe da escolha de representantes*. Dica: encare o item anterior até que ele te encare de volta[40]. ■

Definição 0.4.17. O quociente $Z/\!\sim$ do exercício acima será denotado por $\mathbb{Z}$ e xingado de **conjunto dos números inteiros**. ¶

No caso, a classe de equivalência $\overline{(a,b)}$ representa o que gostaríamos de escrever como $a-b$, razão pela qual vamos escrever assim! Desse modo, a *operação* $+'$ definida no exercício anterior apenas estipula

$$(a-b)+'(c-d)\coloneqq(a+c)-(b+d),$$

tal qual aprendemos na escola.

Exercício 0.51 $\binom{\star}{\star}\star\binom{\star}{\star}$**.** Verifique as propriedades usuais da soma de números inteiros. ■

O "exercício" acima empurra para debaixo do tapete a verificação de diversas propriedades importantes do conjunto $\mathbb{Z}$ como construído aqui, mas que essencialmente permitem tratá-lo como já estamos acostumados – em particular, o apóstrofo empregado no símbolo de adição já pode ser abandonado. De maneira similar, ao definir

$$(a-b)\cdot'(c-d)\coloneqq(ac+bd)-(ad+bc),$$

verifica-se que o resultado da expressão acima (a rigor, uma classe de equivalência em $Z/\!\sim$), não depende da escolha dos representantes das classes, essencialmente como no caso da adição "$+'$". Após verificar que tal operação $\cdot'$ tem o comportamento que se esperaria da multiplicação em $\mathbb{Z}$, a construção de $\mathbb{Q}$ se torna inevitável.

Exercício 0.52 $\binom{\star}{\star\star}$**.** Sobre $Q\coloneqq\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$, considere a relação $\sim$ que declara $(a,b)\sim(c,d)$ se, e somente se, $ad=bc$.

a) Mostre que $\sim$ é uma relação de equivalência.

b) Chamando por $\frac{a}{b}$ a classe de equivalência de um par (a,b), mostre que $Q/\!\sim$ se comporta, essencialmente, como o ***conjunto* dos números racionais** que conhecemos na escola, e que passará a ser denotado por $\mathbb{Q}$. Em particular, defina as operações de adição e multiplicação e verifique suas propriedades usuais. ■

Com $\mathbb{Z}$ e $\mathbb{Q}$ *formalmente* apresentados, já é possível determinar suas *cardinalidades* por meio dos resultados vistos na subseção anterior (entre outros exercícios elementares propostos no final do capítulo):

(i) como existem funções injetoras $\mathbb{N}\to\mathbb{Z}$ e $\mathbb{Z}\to\mathbb{Q}$, resulta que $\mathbb{N}\precsim\mathbb{Z}\precsim\mathbb{Q}$;

(ii) por construção, $\mathbb{Q}$ vem de fábrica com uma sobrejeção da forma $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})\to\mathbb{Q}$, mostrando que $\mathbb{Q}\precsim\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$;

[40] Por exemplo: por um lado, $\overline{(1,2)}+'\overline{(2,5)}=\overline{(3,7)}$, enquanto $\overline{(2,3)}+'\overline{(3,6)}=\overline{(5,9)}$ e, de fato, $\overline{(3,7)}=\overline{(5,9)}$, já que $3+9=7+5$. Elaborar exemplos particulares para entender afirmações aparentemente abstratas é algo que você deve se acostumar a fazer por conta própria.

(iii) em geral, se $A \approx A'$ e $B \approx B'$, então $A \times B \approx A' \times B'$, de modo que por valer $\mathbb{Z} \approx \mathbb{Z} \setminus \{0\}$, resulta $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \approx \mathbb{Z} \times \mathbb{Z}$;

(iv) finalmente, $\mathbb{Z} = \bigcup_{n\in\mathbb{N}}\{-n, n\}$, com $\{-n, n\} \precsim \mathbb{N}$ para todo $n \in \mathbb{N}$, resultando em $\mathbb{Z} \precsim \mathbb{N}$ (logo, $\mathbb{Z} \approx \mathbb{N}$) e, como acima, $\mathbb{Z} \times \mathbb{Z} \approx \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

Em suma:

$$\mathbb{N} \precsim \mathbb{Z} \precsim \mathbb{Q} \precsim \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \approx \mathbb{Z} \times \mathbb{Z} \approx \mathbb{N},$$

donde o Teorema de Cantor-Bernstein assegura as clássicas *identidades* $\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q}$, i.e., tanto $\mathbb{Z}$ quanto $\mathbb{Q}$ são enumeráveis.

O problema da escolha e o sentido da existência

Talvez você tenha notado o símbolo "©" perdido em alguns pontos do texto. Caso tenha passado batido, sua primeira ocorrência foi no Teorema 0.1.27. *Será que tal teorema está protegido por direitos autorais?* Resposta: não. A ideia foi marcar no texto os pontos em que *fomos* displicentes com os *problemas de escolha* – e, em inglês, "escolha" se escreve "*choice*" (©hoice).

Por mais que tenhamos firmado o *compromisso* de *aceitar* conjuntos infinitos, as ferramentas que temos para compreendê-los são *finitárias*: a vida, os símbolos, o papel, a paciência... são recursos indiscutivelmente finitos, o que leva à exigência (bastante) razoável de que *demonstrações* também devem ser *finitas* em algum sentido. Certamente, dado que textos empregam, invariavelmente, apenas finitos caracteres, a noção de finitude que se espera de uma demonstração não deve ser pensada apenas textualmente, mas *computacionalmente*.

Exemplo 0.4.18 (Fundamental)**.** Para ilustrar, considere a demonstração do Teorema 0.4.13. Secretamente, o argumento *sugere* como definir, recursivamente, uma injeção da forma $\mathbb{N} \to X$ sempre que X for infinito:

- ✓ por X ser infinito, tem-se $X \neq \emptyset$, o que permite *escolher* $x_0 \in X$;
- ✓ por X ser infinito, tem-se $X \neq \{x_0\}$, o que permite *escolher* $x_1 \in X \setminus \{x_0\}$;
- ✓ por X ser infinito...
- ✓ por fim, a função $\mathbb{N} \to X$ que faz $n \mapsto x_n$ é injetora.

Implicitamente, o raciocínio acima descreve um processo de construção *infinitamente arbitrário*: cada novo passo *exige* um `input`, uma escolha *indeterminada* que deve ser feita por quem executa a demonstração. Para ilustrar uma situação que não sofre deste problema, suponha que X seja bem ordenado: neste caso, bastaria definir $x_0 := \min X$, $x_1 := \min X \setminus \{x_0\}$, *e assim sucessivamente*. Pode parecer a mesma coisa, mas não é: no último caso, o argumento explicita que a escolha deve ser feita por meio da boa ordem nativa de X, tomando-se *o* menor dentre os elementos ainda não escolhidos, o que independe de quem executa a demonstração[41]. ▲

O que fazer diante disso? Infelizmente, não há resposta *filosoficamente* fácil, uma vez que o questionamento atinge diretamente a *ontologia matemática*: afinal, quando usamos o verbo "existir" numa sentença matemática, como em "existe solução para a equação $x^2 + 1 = 0$", qual o sentido da palavra "existe"?

Exemplo 0.4.19. Futuramente, veremos que o tipo de objeto que se convenciona chamar de reta real, $\mathbb{R}$, é não-enumerável e, além disso, pode ser escrito como $\mathbb{R} = \mathbb{A} \cup \mathbb{T}$, onde $\mathbb{A}$ é a coleção dos números reais que são raízes de polinômios cujos coeficientes são racionais[42], e $\mathbb{T} := \mathbb{R} \setminus \mathbb{A}$. Com alguma paciência, pode-se mostrar que $\mathbb{A}$ é enumerável, ao que você provavelmente se pergunta: e daí? Como $\mathbb{R}$ é não-enumerável, conclui-se que $\mathbb{T}$, além de ser não-vazio, deve ser não-enumerável, pois o contrário acarretaria a enumerabilidade de $\mathbb{R}$, violando o Princípio da Casa dos Pombos (Exercício 0.46). Portanto, sem exibir ao menos um elemento de $\mathbb{T}$, provou-se que $\mathbb{T} \neq \emptyset$. ▲

[41] Trata-se de uma versão menos divertida da *anedota das meias*, criada por Russell para ilustrar o uso do Axioma da Escolha: numa coleção infinita de pares de meias, a fim de tomar uma meia de cada par, precisa-se escolher arbitrariamente uma meia de cada par (já que meias de um mesmo par costumam ser indistinguíveis); já para uma coleção infinita de pares de sapato, basta escolher o pé esquerdo de cada par.

[42] Como $\sqrt{2}$, raiz do polinômio $x^2 - 2$.

A aceitação desse tipo de argumento não é unanimidade entre a comunidade matemática: há quem defenda que por mais abstratas que sejam, as entidades matemáticas devem ser *exibidas*. Para essas pessoas, não basta provar que a inexistência de algo leva a uma contradição, é preciso argumentar diretamente a fim de justificar a *existência*. Porém, tal postura construtivista não é predominante: o mais comum, na verdade, é encarar *existência* como *ausência de contradições* perante algum sistema axiomático fixado, o que não resolve o problema ontológico[43], mas pelo menos possibilita um sono tranquilo para quem pratica Matemática.

De volta ao problema da escolha: como aprendi com Hugo C. Botós,

"para quem só *sabe* martelo, todo parafuso é prego".

Aqui, martelo é o modo finitário por meio do qual argumentamos, enquanto os parafusos são os conjuntos infinitos. É para tratá-los (minimamente) como ~~pregos~~ conjuntos finitos que se postula o

Axioma da Escolha. *Para uma família não-vazia $\mathcal{A}$ de conjuntos não-vazios, existe uma função $f\colon \mathcal{A} \to \bigcup \mathcal{A}$ tal que $f(A) \in A$ para cada $A \in \mathcal{A}$.*

Observação 0.4.20 (Um pouco de contexto, mas não muito)**.** Na tentativa de resolver o primeiro problema da *lista de exercícios* proposta por David Hilbert em 1900, um jovem chamado Ernst Zermelo *demonstrou*, em 1904, o que ficou conhecido como

Teorema 0.4.21 (da Boa Ordenação (©))**.** *Todo conjunto admite uma boa ordem.*

Mais precisamente, qualquer *conjunto* X admite pelo menos uma relação binária $\preceq$ que faz de $(X, \preceq)$ uma boa ordem[44]. O problema de Hilbert em questão era a *Hipótese do Contínuo*, que consiste em saber se existe (ou não) um conjunto infinito X com $\mathbb{N} \prec X \prec \wp(\mathbb{N})$: no caso, a relação com a noção de boa ordem se dá por um resultado de Cantor que estabelece o conjunto das boas ordens de $\mathbb{N}$ (a menos de *isomorfismo*) como um representante da *primeira* cardinalidade *maior* do que a cardinalidade de $\mathbb{N}$. No entanto, o que interessa para a presente discussão é o fato de Zermelo ter explicitado, pela primeira vez até então, a suposição de que escolhas arbitrárias poderiam ser feitas, i.e., o Axioma da Escolha[45]. △

Embora exista quem aponte tal axioma como incompatível com posturas finitárias, pode-se argumentar que foi justamente o comprometimento com tais posturas que levou à percepção de que escolhas infinitas não podem ser realizadas de maneira *construtiva*. Nesse sentido, em vez de banir os resultados que dependem de tais processos, Zermelo propôs aceitar a *existência* de *escolhas completas* sem a limitação de descrevê-las ou construí-las, algo bem mais *honesto*.

Enfim, vejamos esboços de como justificar as passagens marcadas com © (exceto pelo Teorema da Boa Ordenação, cuja demonstração foge do escopo deste trabalho)[46].

- ✓ No Teorema 0.1.27, a classe de representantes se obtém por meio do Axioma da Escolha ao considerar $\mathcal{A}$ como a família das classes de equivalência da relação (ou como a própria partição, a depender do caso), i.e., basta tomar $\mathcal{R} := \{f(A) : A \in \mathcal{A}\}$.
- ✓ O Teorema 0.4.10 e seu Corolário 0.4.11 apenas utilizaram o teorema anterior.
- ✓ Para o Corolário 0.4.12, ao fazer $\mathcal{B} := \{\mathrm{Sob}(\mathbb{N}, X_n) : n \in \mathbb{N}\}$, o Axioma da Escolha *assegura* uma função $f\colon \mathbb{N} \to \bigcup \mathcal{B}$ com $f(n) \in \mathrm{Sob}(\mathbb{N}, X_n)$ para cada $n \in \mathbb{N}$ (por quê?)$^{\star\star}_{\star}$.

[43] Por exemplo: o sistema axiomático fixado descreve entidades que existem de forma independente (num *universo platônico*) ou tudo não passa de um jogo artificial sofisticado? Eu não tenho uma resposta definitiva. Se quiser se aprofundar nesse tipo de discussão para tentar formular a sua própria resposta, você pode conferir o tratado [19] ou a envolvente discussão de Penelope Maddy [11] – se preferir algo mais modesto, o texto de Joel D. Hamkins [6] também é uma boa pedida.

[44] Tal ordem não tem qualquer tipo de comprometimento com *outras ordens* previamente existentes em X: no caso de $\mathbb{Z}$, por exemplo, poderia ocorrer $3 = \min_{\preceq} \mathbb{Z}$, $-1 = \mathrm{suc}_{\preceq}(3)$, $19 = \mathrm{suc}_{\preceq}(-1)$, etc.

[45] A rigor, em 1904, Zermelo tratou o Axioma da Escolha como mera suposição; foi apenas em 1908 que ele propôs uma axiomatização para a teoria de conjuntos que englobasse sua suposição como um dos axiomas.

[46] Para mais detalhes, confira [13].

✓ Finalmente, para o Teorema 0.4.13, com $\mathcal{A} \coloneqq \wp(X) \setminus \{\emptyset\}$, o Axioma da Escolha dá uma função $f\colon \mathcal{A} \to X$ com $f(A) \in A$ para todo $A \in \mathcal{A}$, de modo que ao chamar por $\operatorname{seq}(X)$ a família das funções da forma $\mathbb{N}_{<n} \to X$ para cada $n \in \mathbb{N}$, pode-se definir a função $\mathcal{O}\colon \operatorname{seq}(X) \to X$ que faz $\mathcal{O}(s) \coloneqq f(X \setminus \operatorname{im}(s))$, que explicitamente *escolhe* um elemento em X não pertencente à imagem da *sequência finita* $s \in \operatorname{seq}(X)$. Adaptando-se a ideia da demonstração do Teorema 0.3.9, mostra-se que existe uma (única) função $\psi\colon \mathbb{N} \to X$ tal que $\psi(n) = \mathcal{O}((\psi(m) : m < n))$ para cada $n \in \mathbb{N}$, que pelo modo com que a função $\mathcal{O}$ foi tomada, deve ser injetora.

Exercício 0.53 $(\overset{\star}{\star\star})$**.** Surpreendentemente, a demonstração do Teorema de Cantor-Bernstein não usou o Axioma da Escolha. Por quê? ■

Como representar os infinitos?

Outro símbolo foi empregado despretensiosamente no texto: "®". Sua ocorrência foi única, na Definição 0.1.28, mas não sem importância: ela indica que a definição está *condenada* pelo Paradoxo de ®ussell (Exercício 0.11). De fato, como se discutiu na subseção em questão, um dos modos de eliminar o Paradoxo de Russell consiste em substituir o Axioma da Abstração pelo Axioma da Separação: dada uma propriedade $\mathcal{P}$ e um conjunto A, existe $\{x \in A : x \text{ tem a propriedade } \mathcal{P}\}$. Uma consequência disso foi propositalmente omitida:

Teorema 0.4.22. *Não existe conjunto V para o qual se tenha $x \in V$ para todo x.*

Demonstração. Se existisse, então o Axioma da Separação permitiria definir $R \coloneqq \{x \in V : x \notin x\}$, que traria novamente o Paradoxo de Russell. □

Observação 0.4.23. A inexistência de um conjunto universo é menos problemática do que parece. Ao estudar Teoria dos Números, por exemplo, $\mathbb{Z}$ é o universo dos objetos estudados (os números!), e ninguém reclama de "$\mathbb{Z} \notin \mathbb{Z}$", i.e., $\mathbb{Z}$ não é um número inteiro. Da mesma forma, aqui, $\mathbb{V} \notin \mathbb{V}$, i.e., o universo dos conjuntos não é um conjunto. △

Apesar da observação acima, a impossibilidade de tratar $\mathbb{V}$ como conjunto atrapalha o tratamento que se faz das noções de cardinalidade, principalmente dos conjuntos infinitos: no caso de conjuntos finitos, os números naturais servem precisamente como representantes, mas nada foi apresentado aqui para cumprir tal papel no caso de conjuntos infinitos. O modo usual para resolver o problema faz uso dos chamados *ordinais de von Neumann*.

A ideia é quase simples: define-se $0 \coloneqq \emptyset$, $1 \coloneqq \{0\}$, $2 \coloneqq \{0, 1\}$, $3 \coloneqq \{0, 1, 2\}$, etc. Mais geralmente, um **ordinal** é um conjunto α com duas propriedades peculiares: α é *transitivo*, no sentido de que $x \subseteq \alpha$ sempre que $x \in \alpha$, e $(\alpha, \in_\alpha)$ é uma boa ordem (estrita), onde $\in_\alpha$ é a relação de ordem (estrita) em α dada por $x \in_\alpha y$ se, e somente se, $x \in y$. Com paciência, mostra-se que $0, 1, 2, 3, \ldots$ definidos como acima são ordinais, mas não só isso: ao considerar a coleção de todos os números naturais implementados dessa forma, ganha-se um conjunto ω que também é um ordinal. Ao repetir o processo de sucessão acima e definir $\omega + 1 \coloneqq \omega \cup \{\omega\}$, ganha-se novamente um ordinal, e ao definir $\omega + 2 \coloneqq \omega + 1 \cup \{\omega + 1\}$... Os *números cardinais* desejados *surgem* então como ordinais especiais: um ordinal α é **cardinal** se não existe $\beta \in \alpha$ que admita bijeção com α.

Ao desenvolver as ideias acima com tempo (num curso de Teoria dos Conjuntos, por exemplo), prova-se que todo número natural é um cardinal, assim como ω, que passa a ser chamado de $\aleph_0$, o primeiro cardinal infinito. Depois de argumentar um pouco mais, chega-se à conclusão de que deve existir $\aleph_1$, o primeiro cardinal maior do que $\aleph_0$, bem como $\aleph_2$, o primeiro cardinal maior do que $\aleph_1$, bem como $\aleph_3$, o primeiro... Após chegar a $\aleph_\omega$ (o primeiro cardinal maior do que $\aleph_n$ para todo n natural), chega-se à conclusão de que deve existir $\aleph_{\omega+1}$, o primeiro... Você pegou a ideia, certo? Para mais detalhes, confira [13].

Observação 0.4.24. No caso em que X é um conjunto finito, a expressão "$|X|$" indica o seu número cardinal. Agora, pelo que se discutiu acima, é lícito adotar a mesma notação para X infinito, mesmo que não tenhamos discutido cardinais em detalhes. Se isso te incomodar, ao encontrar expressões como "$|\mathbb{R}| \leq |\wp(\mathbb{N})|$", por exemplo, pense que se trata de uma abreviação estilosa para a afirmação "existe função injetora do tipo $\mathbb{R} \to \wp(\mathbb{N})$". Analogamente, "$|A| = |B|$" abrevia "existe bijeção entre A e B" e assim por diante. △

0.5 Exercícios adicionais

Importante: nos exercícios desta seção e pelo restante do texto, as notações para cardinalidades seguem o que se discutiu na Observação 0.4.24.

Exercício 0.54 (Imagens, pré-imagens, restrições, etc. $(\star)$)**.** Para uma função $f\colon X \to Y$ e um subconjunto $W \subseteq X$, a **restrição** da função f ao subconjunto W é a função $f|_W\colon W \to Y$ definida por $f|_W(w) := f(w)$ para todo $w \in W$. Dizemos que $g\colon Z \to Y$ **estende** f se $X \subseteq Z$ e $g|_X = f$. Mais ainda, para subconjuntos $A \subseteq X$ e $B \subseteq Y$ fixados, consideram-se:

(i) a **imagem direta** de A por f, definida como $f[A] := \{f(a) : a \in A\}$;

(ii) a **pré-imagem** de B por f, definida como $f^{-1}[B] := \{x \in X : f(x) \in B\}$.

Com base nas definições acima, faça o que se pede a seguir.

a) Mostre que $\operatorname{im}(f|_A) = f[A]$ para qualquer $A \subseteq X$.

b) Mostre que $f[A] \subseteq f[A']$ e $f^{-1}[B] \subseteq f^{-1}[B']$ sempre que $A \subseteq A' \subseteq X$ e $B \subseteq B' \subseteq Y$, respectivamente.

c) Mostre que $f[\emptyset] = \emptyset$ e $f^{-1}[\emptyset] = \emptyset$.

d) Mostre que $f^{-1}[Y] = X$.

e) Para $A \subseteq X$ e $B \subseteq Y$ quaisquer, mostre que valem as inclusões $A \subseteq f^{-1}[f[A]]$ e $f\left[f^{-1}[B]\right] \subseteq B$, com as igualdades garantidas se f for injetora (para o primeiro caso) ou sobrejetora (para o segundo caso). ■

Observação 0.5.0 (Importante). Explicitamente, $y \in f[A]$ se, e somente se, existe *algum* $a \in A$ com $f(a) = y$, enquanto $x \in f^{-1}[B]$ se, e somente se, $f(x) \in B$. Embora a pressa possa fazer você pensar o contrário, ao escrever "$f^{-1}[B]$", **não se supõe** que a função f seja *invertível*/bijetora: "f^{-1}" se refere à *relação inversa* de f, que pode não ser uma função (confira a discussão na Subseção 0.1.1). Na dúvida, use a definição dada para a notação – e não a sua intuição para o que a notação deveria ser. △

Exercício 0.55 ((!))**.** Leia a observação anterior novamente, mas preste atenção desta vez. ■

Definição 0.5.1. Para conjuntos X e Y, denotaremos por Y^X a família de todas as funções da forma $X \to Y$.[47] ¶

Exercício 0.56 $(\overset{\star}{\star})$**.** Para um conjunto X qualquer (possivelmente infinito!), exiba uma bijeção entre $\wp(X)$ e $\{0,1\}^X$. Dica: para um subconjunto $A \subseteq X$, associe uma função "óbvia" da forma $X \to \{0,1\}$; para facilitar, comece com X finito para daí generalizar. ■

Exercício 0.57 $(\overset{\star}{\star})$**.** Mostre que se $|A| = |B|$, então $|\wp(A)| = |\wp(B)|$. ■

Exercício 0.58 $(\overset{\star}{\star})$**.** Sejam A, B, C e D conjuntos. Mostre que se $|A| \leq |C|$ e $|B| \leq |D|$, então $|A^B| \leq |C^D|$. ■

Exercício 0.59 $(\overset{\star}{\star})$**.** Mostre que se $|A| = |C|$ e $|B| = |D|$, então $|A^B| = |C^D|$. ■

Observação 0.5.2. Note que o exercício anterior justifica definir potenciação entre cardinalidades/números cardinais: $|X|^{|Y|} := |X^Y|$. △

[47] O motivo da notação exponencial é sugerido, implicitamente, pelo último item do Exercício 0.63.

Observação 0.5.3. Independentemente do que será discutido nos próximos capítulos a cerca das chamadas *indeterminações*, a definição acima obriga que se tenha $0^0 = 1$, o que está de acordo com o fato de que existe uma única função da forma $\emptyset \to \emptyset$. △

Exercício 0.60 ($^\star_{\star\star}$)**.** Para conjuntos X, Y e Z *quaisquer*, exiba uma bijeção entre $(X^Y)^Z$ e $X^{Y\times Z}$. Qual a interpretação cardinal disso? ■

Exercício 0.61 ((!))**.** Se você fez o exercício acima apenas para os casos em que X, Y e Z são finitos, volte e faça de novo, para **conjuntos quaisquer**: a hipótese de finitude é irrelevante para a solução do exercício[48]. ■

Exercício 0.62 ($^\star_\star$)**.** Seja $f\colon X \to Y$ uma função. Mostre que $\mathcal{P} \coloneqq \{f^{-1}[\{y\}] : y \in \operatorname{im}(f)\}$ é uma partição de X. ■

Exercício 0.63 ($^\star_{\star\star}$)**.** Demonstre as seguintes afirmações.

a) Para todo $n \in \mathbb{N}$ ocorre $|\mathbb{N}_{<n}| = n$.

b) Se X é finito e $x \notin X$, então $|X \cup \{x\}| = |X| + 1$.

c) Se $X \subseteq Y$ e Y é finito, então X é finito e $|X| \leq |Y|$. Dica: indução em $|Y|$ + item anterior.

d) Se X e Y são finitos, então $X \cup Y$ é finito e $|X \cup Y| \leq |X| + |Y|$. Dica: indução em $|X|$ + item (b) para o subcaso do passo indutivo em que $X \not\subseteq Y$.

e) Se X e Y são finitos e disjuntos, então $|X \cup Y| = |X| + |Y|$.

f) Se $\mathcal{F}$ é finito e todo $F \in \mathcal{F}$ é finito, então $\bigcup \mathcal{F}$ é finito. Dica: indução em $|\mathcal{F}|$.

g) Se X e Y são finitos, então $X \times Y$ é finito e $|X \times Y| = |X| \cdot |Y|$. Dica: $X \times Y = \bigcup_{y\in Y} X \times \{y\}$.

h) Se X é finito e $f\colon X \to Y$ é uma função, então $\operatorname{im}(f)$ é finito e $|\operatorname{im}(f)| \leq |X|$.

i) Se $X \times Y$ é finito, então X e Y são finitos.

j) Se X é finito, então $\wp(X)$ é finito e $|\wp(X)| = 2^{|X|}$. Dica: combine o próximo item com o Exercício 0.56.

k) Se X e Y são finitos, então Y^X é finito e $|Y^X| = |Y|^{|X|}$. ■

Exercício 0.64 ($^\star_\star$)**.** Mostre que para $n \in \mathbb{N}$, uma função $f\colon \mathbb{N}_{<n} \to \mathbb{N}_{<n}$ é injetora se, e somente se, é sobrejetora. ■

Exercício 0.65 ($^\star_{\star\star}$)**.** Mostre que para X finito, uma função $f\colon X \to X$ é injetora se, e somente se, é sobrejetora. ■

Exercício 0.66 ($^\star_\star$)**.** O resultado acima permanece válido para X infinito? ■

Exercício 0.67 ($^\star_\star$)**.** Pense rápido: se $f\colon \mathbb{N} \to \mathbb{N}$ é uma função sobrejetora, então existe $n \in \mathbb{N}$ tal que $f^{-1}[\{n\}]$ é finito? ■

Exercício 0.68 ($^\star_\star$)**.** Seja $f\colon X \to Y$ uma função, com Y enumerável e X não-enumerável. Mostre que existe $y \in Y$ tal que $X' \coloneqq \{x \in X : f(x) = y\}$ é não-enumerável. ■

Exercício 0.69 ($^\star_\star$)**.** Seja $\psi\colon X \to Y$ uma função bijetora. Mostre que se $\mathcal{P}$ é uma partição de X, então $\psi(\mathcal{P}) \coloneqq \{\psi[P] : P \in \mathcal{P}\}$ é uma partição de Y. Em particular, tem-se $|\mathcal{P}| = |\psi(\mathcal{P})|$. ■

[48] De modo geral, só assuma que os conjuntos são finitos quando isso for explicitamente indicado.

Exercício 0.70 ($\overset{\star}{\star\star}$)**.** Mostre que existe uma partição $\mathcal{P} \coloneqq \{P_n : n \in \mathbb{N}\}$ de $\mathbb{N}$ com cada P_n infinito. Dica: arrume uma função sobrejetora $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ esperta – ou apele para Teoria dos Números. ■

Exercício 0.71 ($\overset{\star}{\star}$)**.** Sejam $(\mathbb{S}, \leq)$ e $(\mathbb{T}, \leq)$ ordens parciais. Uma função $f\colon \mathbb{S} \to \mathbb{T}$ é:

(i) **crescente** se para quaisquer $s, s' \in \mathbb{S}$ valer que $s \leq s' \Rightarrow f(s) \leq f(s')$;

(ii) **decrescente** se para quaisquer $s, s' \in \mathbb{S}$ valer que $s \leq s' \Rightarrow f(s) \geq f(s')$;

(iii) **monótona** se f for crescente ou decrescente.

Sabendo disso, suponha que a ordem de $\mathbb{S}$ seja total.

a) Mostre que se f é crescente e $f(s) < f(s')$, então $s < s'$.

b) Mostre que se f é decrescente e $f(s) < f(s')$, então $s > s'$.

c) Conclua que se f for monótona e bijetora, então a inversa $f^{-1}\colon \mathbb{T} \to \mathbb{S}$ também será monótona[49]. ■

Observação 0.5.4. Uma função crescente e injetora satisfaz a implicação *estrita*

$$s < s' \Rightarrow f(s) < f(s'),$$

já que deve ocorrer $f(s) \leq f(s')$, enquanto a injetividade proíbe $f(s) = f(s')$. Uma função em tal condição será chamada de **estritamente crescente**. A definição para funções **estritamente decrescentes** é análoga[50]. △

Exercício 0.72 ($\star$)**.** Convença-se de que funções estritamente monótonas são injetoras. ■

Exercício 0.73 ($\overset{\star\star}{\star\star}$)**.** Seja $(\mathcal{N}, i, s)$ um sistema natural. Diremos que $I \subseteq \mathcal{N}$ é **indutivo** se $s(n) \in I$ sempre que $n \in I$. Agora, para $m, n \in \mathcal{N}$, vamos escrever "$m \leq n$" a fim de indicar que "n pertence a todo conjunto indutivo que contém m". O propósito deste exercício é mostrar que $(\mathcal{N}, \leq)$ é uma boa ordem natural cujo sistema natural induzido é $(\mathcal{N}, i, s)$.

a) Convença-se de que $\leq$ é reflexiva e transitiva.

b) Mostre que se $I \subseteq \mathcal{N}$ é indutivo, então $s[I]$ também é.

c) Mostre que se $m, n \in \mathcal{N}$ e $m \not\leq n$, então $s(m) \not\leq s(n)$ e $s(m) \not\leq n$. Dica: pela definição de $\leq$, deve existir um subconjunto indutivo I satisfazendo $m \in I$ com $n \notin I$; use o item anterior para concluir.

d) Mostre que para todo $n \in \mathcal{N}$ ocorre $n \leq s(n)$ e $s(n) \not\leq n$. Dica: para a segunda parte, com $X \coloneqq \{n \in \mathcal{N} : s(n) \not\leq n\}$, note que $i \in X$ e $s(n) \in X$ sempre que $n \in X$.

e) Mostre que $(\mathcal{N}, \leq)$ é uma ordem parcial. Sugestão: verifique a antissimetria pela contrapositiva, i.e., mostre que se $m \neq n$, então $m \not\leq n$ ou $n \not\leq m$, o que pode ser feito por *indução* como no item anterior.

f) Mostre que se $m \leq n$, então $s(m) \leq s(n)$.

g) Mostre que se $I \subseteq \mathcal{N}$ é indutivo, então $s^{-1}[I]$ é indutivo.

[49] Na verdade, f é crescente/decrescente se, e somente se, f^{-1} é crescente/decrescente.

[50] A literatura também costuma xingar de *não-decrescente* as coisas que aqui foram chamadas de *crescentes*. Em tais textos, o adjetivo *crescente* se reserva para as situações de desigualdade estrita. Um comentário análogo é válido para funções *não-crescentes*.

h) Definindo "$m < n$" como abreviação para "$m \leq n$ e $m \neq n$", mostre que se $s(m) < s(n)$, então $m < n$. Dica: use o item anterior.

i) Mostre que $m < s(n)$ se, e somente se, $m \leq n$. Dica: primeiro, observe que se $m < s(i)$, então $m = i$; depois, note que se a tese valer para $n \in \mathcal{N}$ e ocorrer $s(k) < s(s(n))$ para algum k, então $k < s(n)$ em virtude do item anterior; conclua por *indução*.

j) Suponha que $X \subseteq \mathcal{N}$ tenha a seguinte propriedade: para todo $n \in \mathcal{N}$, a ocorrência de $m \in X$ para todo $m < n$ acarreta $n \in X$. Mostre que $X = \mathcal{N}$. Dica: considere $Y := \{n \in \mathcal{N} : \forall m \in \mathcal{N}\ m < n \Rightarrow m \in X\}$ e mostre por indução que $Y = \mathcal{N}$, ponto em que o item anterior será essencial; para concluir, lembre-se de que $n < s(n)$ para todo n.

k) Mostre que $(\mathcal{N}, \leq)$ é uma boa ordem. Dica: tome $S \subseteq \mathcal{N}$ sem menor elemento e use o item anterior para concluir que $\mathcal{N} \setminus S = \mathcal{N}$, i.e., $S = \emptyset$.

l) Mostre que $i = \min \mathcal{N}$ e $\mathrm{suc}_{\mathcal{N}}(n) = s(n)$ para todo $n \in \mathcal{N}$. ■

Observação 0.5.5. Sim. Foram quatro estrelas: estas se reservam a exercícios que devem ser feitos ao menos uma vez na vida. △

Exercício 0.74 ($\overset{\star\star}{\star\star}$)**.** Suponha que você tenha que dar um curso de Análise em que $0 \notin \mathbb{N}$. Como definir, recursivamente (no sentido do Exercício 0.37), as operações de soma e multiplicação em $\mathbb{N}$? ■

0.6 Linguagem: breve revisão de estruturas algébricas

0.6.0 Essencial

Operações binárias e elementos especiais

Definição 0.6.0. Fixado um conjunto X, uma função $*\colon X \times X \to X$ é chamada de **operação binária** em X. Porém, como não trataremos explicitamente de outras *aridades*, não há risco em chamar $*$ simplesmente de operação. Para $x, y \in X$, costuma-se escrever $x * y$ em vez de $*(x, y)$, em alusão às notações já bem estabelecidas para *adição* e *multiplicação*. ¶

A operação $*$ determina o que é $x * y$ em X. Independentemente disso, como $x * y \in X$, é legítimo operar tal elemento com algum $z \in X$, situação em que se escreve $(x * y) * z$. Os parênteses são necessários pois, a princípio, poderia ocorrer $(x * y) * z \neq x * (y * z)$, entre outros comportamentos *indesejados*. Porém, como o tempo é curto, vamos nos focar nos casos que interessam a este curso.

Definição 0.6.1. Seja $*\colon X \times X \to X$ uma operação num conjunto X.

(i) Diremos que a operação $*$ é **associativa** se para quaisquer $x, y, z \in X$ ocorrer $(x * y) * z = x * (y * z)$, o que na prática significa que pode-se escrever $x * y * z$ em vez de $(x * y) * z$ ou $x * (y * z)$.

(ii) Diremos que a operação $*$ é **comutativa** se para quaisquer $x, y \in X$ valer a identidade $x * y = y * x$.

(iii) Diremos que $e \in X$ é **elemento neutro**[51] da operação $*$ se para qualquer $x \in X$ ocorrer $e * x = x = x * e$. ¶

[51] Também chamado de **zero** ou **unidade** a depender do contexto.

Como você já deve saber, um elemento neutro de uma operação $*$, se existir, é único, o que permite o uso da expressão "o elemento neutro" da operação. Para aquecer os motores, convém destacar isso.

Lema 0.6.2. *Uma operação admite, no máximo, um único elemento neutro.*

Demonstração. Se $e, e' \in X$ são ambos elementos neutros da operação, então $e = e * e'$ por e' ser elemento neutro, enquanto $e * e' = e'$ por e ser elemento neutro. □

Definição 0.6.3. Diremos que $y \in X$ é um $*$-**inverso à direita** de x se valer $x * y = e$. Analogamente, y será dito um $*$-**inverso à esquerda** de x se ocorrer $y * x = e$. Se y for simultaneamente $*$-inverso à direita e à esquerda de x, diremos simplesmente que y é um $*$-**inverso**[52] de x. Naturalmente, o *prefixo* "$*$-" será abandonado sempre que o contexto permitir. ¶

Exercício 0.75 ($\star$)**.** Sejam X um conjunto e $*$ uma operação em X. Mostre que se $*$ é associativa e tem elemento neutro, então cada $x \in X$ admite, no máximo, um $*$-inverso. ■

Para quem gosta de colecionar terminologias, as próximas são um prato cheio:

- um **semigrupo** é um conjunto não-vazio munido de uma operação associativa;
- um **monóide** é um semigrupo com elemento neutro;
- um **grupo** é um monóide em que todo elemento tem um inverso;
- finalmente, um **grupo abeliano** é um grupo cuja operação é comutativa.

Observação 0.6.4. Tal qual se faz com ordens, quando se busca algum tipo de precisão exagerada, escreve-se algo como $(G, *, e)$ para indicar que $*$ é uma operação em G que tem e como elemento neutro, de modo que afirmações do tipo "$(G, *, e)$ *é um grupo abeliano*" abreviam a tediosa frase "$*\colon G \times G \to G$ é uma operação que faz de G um grupo comutativo cujo elemento neutro é e". △

Exemplo 0.6.5. As operações de adição e multiplicação em $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ constituem exemplos elementares das estruturas definidas acima, embora isso não tenha sido sempre óbvio[53].

- ✓ $(\mathbb{N}, +, 0)$ é um monóide comutativo, mas não é um grupo: não há, por exemplo, $n \in \mathbb{N}$ satisfazendo $n + 1 = 0$.
- ✓ $(\mathbb{Z}, +, 0)$ e $(\mathbb{Q}, +, 0)$ são grupos abelianos.
- ✓ $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ é um monóide comutativo, mas não é um grupo.
- ✓ $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ é um grupo abeliano.

Naturalmente, tais proposições só podem ser justificadas rigorosamente num cenário em que se tenha uma *construção* ou, pelo menos, uma definição explícita dos conjuntos e operações envolvidos. Se for de seu interesse verificar essas coisas, confira as construções de $\mathbb{Z}$ e $\mathbb{Q}$ na Subseção 0.4.1. ▲

[52] Ou oposto, simétrico, etc. Tudo depende do contexto.

[53] Historicamente, grupos de *permutações* foram os primeiros a dar as caras, entre as últimas décadas do século XVIII e as primeiras décadas do século XIX. Depois do aparecimento dessas estruturas, *percebeu-se* que entidades cotidianas compostas por *números* também constituíam *modelos* de grupos [7].

Praticamente todas as operações elementares consideradas ao longo do texto serão comutativas – a exceção mais marcante é a composição de funções, que em geral não será considerada do ponto de vista algébrico-estrutural. Apesar disso, no contexto que se aproxima, teremos que lidar com duas operações simultaneamente, que serão denotadas pelos símbolos $+$ e $\cdot$.

Em ambos os casos, as operações serão associativas, comutativas e dotadas de elemento neutro. No caso da operação $+$, o elemento neutro será denotado por 0, e o inverso de um elemento x, único em virtude do Lema 0.75, será denotado por $-x$ e chamado de **inverso aditivo** ou **simétrico**. Para a operação $\cdot$, o elemento neutro será denotado por 1, e o inverso de um elemento x, se existir, será denotado por x^{-1} ou $\frac{1}{x}$, caso em que x será dito **invertível**[54].

Proposição 0.6.6. *Sejam $(G, \cdot, 1)$ um monóide e $x \in G$. Para $n \in \mathbb{N}$, defina $x^n \in G$ recursivamente, fazendo $x^0 := 1$ e $x^{n+1} := x^n \cdot x$ para todo $n \in \mathbb{N}$. Se x admitir inverso, para cada $n \in \mathbb{N}$ com $n > 0$ defina ainda $x^{-n} := (x^{-1})^n$. Então, vale o seguinte:*

(i) $x^{m+n} = x^m \cdot x^n$ *para quaisquer* $m, n \in \mathbb{N}$;

(ii) $x^{mn} = (x^m)^n$ *para quaisquer* $m, n \in \mathbb{N}$;

(iii) se x admite inverso, então as identidades anteriores valem para $m, n \in \mathbb{Z}$.

Demonstração. O argumento é indutivo e depende das propriedades operatórias de $\mathbb{N}$ e $\mathbb{Z}$. Por exemplo: para $m \in \mathbb{N}$ fixado, tem-se:

- ✓ $x^{m+0} = x^m = x^m \cdot 1 = x^m \cdot x^0$;
- ✓ se $x^{m+n} = x^m \cdot x^n$ para algum $n \in \mathbb{N}$, então

$$x^{m+(n+1)} = x^{(m+n)+1} := x^{(m+n)} \cdot x = (x^m \cdot x^n) \cdot x = x^m \cdot (x^n \cdot x) := x^m \cdot x^{n+1},$$

donde a validade do primeiro item segue por indução.

Para o segundo item, o pulo do gato é notar que

$$x^{m(n+1)} = x^{mn+m} = x^{mn} \cdot x^m = (x^m)^n \cdot x^m := (x^m)^{n+1}.$$

A parte final segue, dentre outras coisas, de se observar que $x^{-n} = (x^n)^{-1}$. Os detalhes ficam por sua conta. □

Exercício 0.76 ($\star$)**.** Complete a demonstração da proposição anterior. Dica: além do que já foi mencionado, pode ser útil observar que $x^{n+1} = x \cdot x^n$. ■

Observação 0.6.7. Será cada vez mais comum utilizar o mesmo símbolo com significados que variam de acordo com o contexto. Na proposição anterior, por exemplo, o símbolo "1" em "$(G, \cdot, 1)$" denota o elemento neutro da operação "$\cdot$" de G. Já em "$x^{n+1} := x^n \cdot x$", o expoente "$n+1$" indica o sucessor de n em $\mathbb{N}$. Esta é a chamada *notação multiplicativa*, em que o *histórico* das iterações é registrado no expoente.

Alternativamente, quando a operação de G é denotada com o símbolo "$+$", seu elemento neutro é indicado por "0" (caso exista), enquanto o *histórico das iterações* é registrado à esquerda, como explicitado no próximo corolário – esta é a chamada *notação aditiva*. Note que, a seguir, o símbolo "0" em "$0x := 0$" também assume *dupla função*. △

Corolário 0.6.8. *Sejam $(G, +, 0)$ um grupo (abeliano) e $x \in G$. Para $n \in \mathbb{N}$, defina $nx \in G$ recursivamente, fazendo $0x := 0$ e $(n+1)x := nx + x$ para todo $n \in \mathbb{N}$. Além disso, defina $(-n)x := n(-x)$ para cada $n \in \mathbb{N}$. Então para quaisquer $m, n \in \mathbb{Z}$ valem as identidades $(m+n)x = mx + nx$ e $m(nx) = (mn)x$.*

[54] Como sempre, lembre-se: o verbo é "inverter" e não "inverser".

Anéis e corpos

Definição 0.6.9. Um **anel** consiste de um conjunto $A \neq \emptyset$ munido de duas operações, $+$ e $\cdot$, e elementos $0, 1 \in A$, onde

(i) $(A, +, 0)$ é um grupo abeliano, cuja operação $+$ é chamada de *adição*,

(ii) $(A, \cdot, 1)$ é um monóide comutativo, cuja operação $\cdot$ é chamada de *multiplicação*, e

(iii) as operações $+$ e $\cdot$ *comutam* entre si, i.e., para quaisquer $a, b, c \in A$ valem as identidades $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$. ¶

Costuma-se denotar o anel A como a *estrutura algébrica* $(A, +, \cdot, 0, 1)$. No entanto, quase sempre iremos nos referir simplesmente *ao anel* A, deixando as operações subentendidas no contexto.

Observação 0.6.10. A rigor, os anéis definidos acima deveriam ser chamados de *anéis comutativos com unidade*, dado que existem contextos que não exigem a comutatividade da multiplicação e tampouco a existência de elemento neutro multiplicativo. △

Exemplo 0.6.11. Os conjuntos numéricos $\mathbb{Z}$ e $\mathbb{Q}$ são anéis quando munidos das operações usuais, enquanto $\mathbb{N}$ não é anel, posto que a adição não define uma estrutura de grupo. ▲

Muitas propriedades operatórias com as quais estamos acostumados no cenário aritmético ainda são válidas no contexto de anéis[55].

Proposição 0.6.12. *Sejam A um anel e $a \in A$ um elemento qualquer. Então valem as seguintes identidades:*

(i) $0 \cdot a = 0$*;*

(ii) $-a = (-1) \cdot a$*.*

Demonstração. Tais identidades relacionando as operações $+$ e $\cdot$ decorrem diretamente da distributividade exigida na definição de anel. De fato,

$$a \cdot 0 = a \cdot (0+0) = (a \cdot 0) + (a \cdot 0) \Rightarrow 0 = (a \cdot 0) + (-(a \cdot 0)) = (a \cdot 0) + (a \cdot 0) + (-(a \cdot 0)) = a \cdot 0,$$

ao passo que

$$a + ((-1) \cdot a) = (1 + (-1)) \cdot a = 0 \cdot a = 0,$$

donde a igualdade $(-1) \cdot a = -a$ segue da unicidade do *oposto aditivo* de a. □

Observação 0.6.13. Em particular, como o inverso de $-a$ é a, segue que

$$(-1) \cdot (-a) = -(-a) = a,$$

identidade que será utilizada daqui em diante sem menções especiais. △

[55] E aqui cabe uma ressalva, possivelmente óbvia, mas que ainda assim merece ser feita. O comportamento que se observa nos números do "dia a dia" não decorre dos axiomas utilizados para *formalizá-los*, pelo contrário: os axiomas postulados para formalizar os números são "bons" justamente por reproduzirem os *comportamentos* observados.

Ao longo do texto, usaremos simultaneamente a Proposição 0.6.6 e o Corolário 0.6.8: a primeira com respeito à multiplicação do anel, e o segundo com respeito à adição do anel. Assim, se A é um anel, $a \in A$ e $m, n \in \mathbb{N}$, então ma^n indica o que, intuitivamente, seria escrito como

$$\underbrace{\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ vezes}} + \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ vezes}} + \ldots + \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ vezes}}}_{m \text{ vezes}},$$

com uma interpretação análoga para $m \in \mathbb{Z}$ e, se a for invertível, para $n \in \mathbb{Z}$.

Observação 0.6.14. Daqui em diante, como de costume, "ab" também será usado para denotar "$a \cdot b$", o produto entre a e b num anel A. Como o tempo é curto, "$a - b$" abreviará a expressão "$a + (-b)$". △

Definição 0.6.15. Um anel A é chamado de **corpo** se $1 \neq 0$ e todo $a \in A \setminus \{0\}$ é invertível, i.e, se existir $b \in A \setminus \{0\}$ com $ab = 1$. ¶

Exemplo 0.6.16. O primeiro corpo com o qual nos deparamos *explicitamente* é $\mathbb{Q}$, o conjunto dos números racionais com suas operações usuais. A reta real $\mathbb{R}$, protagonista deste curso, também é um corpo. Estes não são os únicos corpos que existem: a Álgebra Comutativa é repleta de tais entidades. Porém, em contextos *introdutórios* de Análise, não costuma ser importante saber disso[56]. ▲

Proposição 0.6.17 (Cancelamento para multiplicação[57])**.** *Se A é corpo e $\alpha, x, y \in A$ são tais que $\alpha x = \alpha y$ com $\alpha \neq 0_A$, então $x = y$.*

Demonstração. Basta multiplicar α^{-1} dos dois lados da igualdade $\alpha x = \alpha y$. □

Antes de encerrar esta subseção, cabe uma ressalva acerca da divisibilidade por zero, cuja *polêmica* só se justifica pela falta de discussão adequada: não há lei universal ou *mandamento* vindo das colinas que proíba dividir por zero em absolutamente qualquer contexto – o ponto é que fazer isso em anéis é, na prática, inútil.

De fato, uma identidade do tipo $\frac{\alpha}{0} = \beta$ num anel A depende, implicitamente, de se admitir a existência de $z := \frac{1}{0} \in A$, i.e., um elemento $z \in A$ que satisfaz $0 \cdot z = 1$. Ora, como também deve ocorrer $0 \cdot z = 0$, resulta que $0 = 1$ e, consequentemente, $0 = x$ para todo $x \in A$, ou seja, $A = \{0\}$. Algebricamente isto não é crime: um conjunto dotado de um único elemento admite tanto uma adição quanto uma multiplicação que o tornam um anel (verifique?)*. O *problema* é que ao se modelar axiomaticamente os números naturais, inteiros, etc., *espera-se* que ocorra $0 \neq 1$ (vide o Lema 0.7.2).

0.6.1 Extras

(Adiável) morfismos entre anéis

Definição 0.6.18. Dados anéis A e B, uma função $f\colon A \to B$ é chamada de **morfismo** *de anéis* (ou *de corpos* quando ambos forem corpos) se

(i) $f(1_A) = 1_B$,

(ii) $f(a + a') = f(a) + f(a')$, e

(iii) $f(aa') = f(a)f(a')$. ¶

[56] Não se engane: a Análise é intrinsecamente dependente da Álgebra, embora a recíproca seja falsa – exceto pelo *Teorema* (não tão) *Fundamental da Álgebra*, que *ainda* é importante em *algumas áreas*.

[57] Ou "Lema da Academia": corpo é *domínio*. Trata-se de uma piadoca do Prof. Eduardo Tengan.

Acima, por preciosismo, os elementos neutros multiplicativos de A e B foram distinguidos como 1_A e 1_B, respectivamente. Porém, ainda mais precisão poderia ser dada às notações: note que em "$f(a+a') = f(a) + f(a')$", por exemplo o símbolo "$+$" em "$a+a$" indica a adição do anel A, enquanto o mesmo símbolo em "$f(a) + f(a')$" indica a adição em B. Analogamente, a ausência de símbolos operacionais na última cláusula indica as multiplicações em A e B, respectivamente.

Em certo sentido, um morfismo de anéis $f\colon A \to B$ permite que A *manifeste* informações de natureza algébrica em B por meio de f. Por exemplo, se $a \in A$ é tal que $a^2 = 1$ em A, então o mesmo deve ocorrer com $f(a)$ em B, i.e., $f(a)^2 = 1_B$: de fato, deve-se ter

$$1_B = f(1_A) = f(a^2) = f(a)f(a) = f(a)^2.$$

No presente contexto, um tipo muito particular de morfismo de anéis será fundamental:

Proposição 0.6.19. *Para todo anel A existe um único morfismo de anéis $\zeta_A\colon \mathbb{Z} \to A$.*

Demonstração. Fazendo $(G, +, 0) := (A, +, 0_A)$ e $x := 1_A$ no Corolário 0.6.8, resulta que a função $\zeta_A\colon \mathbb{Z} \to A$, dada por $\zeta_A(n) := n \cdot 1_A$ e $\zeta(-n) := -(n \cdot 1_A)$ para qualquer $n \in \mathbb{N}$, é um morfismo de anéis. Fica por sua conta verificar, por indução, que qualquer *outro* morfismo $\psi\colon \mathbb{Z} \to A$ deve ser tal que $\psi = \zeta_A$. □

Exercício 0.77 ($\overset{\star}{\star}$)**.** Complete a demonstração acima. Dica: deve-se ter $\psi(1) = 1_A = \zeta_A(1)$, $\psi(1+1) = 1_A + 1_A = \zeta_A(2)$, ... ■

Ao longo deste capítulo, fixados um anel A e um número inteiro $z \in \mathbb{Z}$, a notação z_A indicará a imagem de z pelo morfismo ζ_A da última proposição, a **interpretação** de z em A. Na prática,

$$z_A = \underbrace{1_A + \ldots + 1_A}_{z \text{ vezes}} \text{ se } z > 0, \text{ enquanto } z_A = \underbrace{-1_A + \ldots + (-1_A)}_{z \text{ vezes}} \text{ se } z < 0.$$

Exercício 0.78 ($\overset{\star}{\star}$)**.** Mostre que para $z \in \mathbb{Z}$ e $a \in A$, o elemento $za \in A$ (como definido no Corolário 0.6.8) é tal que $za = z_A a$. Conclua que para quaisquer $a, b \in A$ e $m \in \mathbb{Z}$ deve-se ter $m(a+b) = ma + mb$. ■

Exemplo 0.6.20. Para $A := \mathbb{Q}$, o morfismo $\zeta_A\colon \mathbb{Z} \to A$ é, meramente, a inclusão. ▲

Exemplo 0.6.21 (Matrizes)**.** Se você tiver familiaridade com *matrizes*, note que se A denota o *anel das matrizes de ordem* $n \in \mathbb{N} \setminus \{0\}$ (e coeficientes *reais*, por exemplo), então $\zeta_A\colon \mathbb{Z} \to A$ associa cada inteiro $z \in \mathbb{Z}$ à matriz diagonal $(z\delta_{ij})$. ▲

Exercício 0.79 ($\star$)**.** Seja $f\colon A \to B$ um morfismo de anéis.

a) Mostre que $f(0_A) = 0_B$.

b) Mostre que $f(ma) = mf(a)$ para quaisquer $m \in \mathbb{Z}$ e $a \in A$.

c) Mostre que $f(-a) = -f(a)$ para qualquer $a \in A$.

d) Mostre que $f(a^m) = f(a)^m$ para quaisquer $m \in \mathbb{N}$ e $a \in A$. ■

Os últimos comentários, frequentemente úteis, seguem destacados nos próximos exercícios.

Exercício 0.80 ($\star$)**.** Dado um anel A, mostre que $\mathrm{Id}_A\colon A \to A$ é um morfismo de anéis. ■

Exercício 0.81 ($\star$)**.** Mostre que a composição de morfismos de anéis é um morfismo de anéis. ■

Exercício 0.82 (Núcleo e injetividade, ($\overset{\star}{\star}$))**.** Para um morfismo de anéis $f\colon A \to B$, chama-se de **núcleo** de f ao conjunto $\ker f := \{a \in A : f(a) = 0_B\}$.

a) Mostre que f é injetora se, e somente se, seu núcleo é *trivial*, i.e., se $\ker f = \{0_A\}$.

b) Mostre que se A e B são corpos, então f é injetora. ■

(Adiável) espaços vetoriais e transformações lineares

Se você já estudou Álgebra Linear ou, pelo menos, Geometria Analítica, já deve ter visto *espaços vetoriais*. Grosso modo, trata-se de um conjunto cujos elementos interpretamos como se fossem pontos/vetores *num espaço* em que algum sistema de coordenadas permite que façamos contas com esses pontos.

O exemplo clássico é $\mathbb{R}^n$, para $n \in \mathbb{N} \setminus \{0\}$, o conjunto das n-uplas de *números reais* – e Geometria Analítica consiste, essencialmente, em estudar os casos em que $n \leq 3$. Como tais n-uplas são da forma $(a_1, \dots, a_n)$, com $a_1, \dots, a_n \in \mathbb{R}$, é possível tanto somá-las umas com as outras quanto multiplicá-las entre si. Formalmente, definem-se operações

$$\begin{aligned} (+)\colon \mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ ((a_1, \dots, a_n), (b_1, \dots, b_n)) &\mapsto (a_1 + b_1, \dots, a_n + b_n) \end{aligned} \quad \text{e} \quad \begin{aligned} (\cdot)\colon \mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ ((a_1, \dots, a_n), (b_1, \dots, b_n)) &\mapsto (a_1 \cdot b_1, \dots, a_n \cdot b_n) \end{aligned}$$

No entanto, embora as duas operações sejam razoáveis de um ponto de vista puramente algébrico, apenas a soma tem uma interpretação geométrica clara: a saber, a translação. Ao fazer a multiplicação com a regra acima, verificam-se comportamentos inesperados incompatíveis com a multiplicação usual[58]. Apesar disso, recupera-se alguma intuição geométrica se, em vez de multiplicar vetores com a segunda regra, multiplicarmos apenas *escalares* por vetores, fazendo $\lambda \cdot (a_1, \dots, a_n) := (\lambda a_1, \dots, \lambda a_n)$. Ao considerar $\mathbb{R}^n$ com a soma $(+)$ e com essa multiplicação por escalares, tem-se um dos principais exemplos de *espaço vetorial*.

Definição 0.6.22. Fixado um corpo K, dizemos que um grupo abeliano $(V, +, 0)$ é um K-**espaço vetorial** se existir uma função

$$\begin{aligned} K \times V &\mapsto V \\ (k, v) &\mapsto kv \end{aligned}$$

chamada de *multiplicação* (ou *ação*), satisfazendo as seguintes condições:

(i) $1_K v = v$ para todo $v \in V$;

(ii) $(\alpha + \beta)v = (\alpha v) + (\beta v)$ para quaisquer $\alpha, \beta \in K$ e $v \in V$;

(iii) $k(u + v) = (ku) + (kv)$ para quaisquer $u, v \in V$ e $k \in K$. ¶

Em tal contexto, os elementos de V são chamados de *vetores*, enquanto os membros de K são xingados de *escalares*.

Após introduzirmos $\mathbb{R}$ como *um* corpo ordenado completo, as discussões acima servirão para entender $\mathbb{R}^n$ como um $\mathbb{R}$-espaço vetorial. Naturalmente, como $\mathbb{Q}$ é corpo, os mesmos argumentos já podem ser usados para justificar que $\mathbb{Q}^n$ é $\mathbb{Q}$-espaço vetorial. De modo geral, K^n é K-espaço vetorial, para qualquer $n \in \mathbb{N}$ e corpo K. Na verdade, pode-se extrapolar mais.

Exemplo 0.6.23. Se X é um conjunto e K é um corpo, então o conjunto K^X das funções da forma $X \to K$ tem uma estrutura natural de K-espaço vetorial com as operações herdadas de K em cada "coordenada". Mais precisamente, para $f, g \in K^X$ e $\lambda \in K$, definem-se $f + g, \lambda \cdot g \in K^X$ por

$$(f + g)(x) := f(x) + g(x) \quad \text{e} \quad (\lambda \cdot g)(x) := \lambda \cdot g(x)$$

para cada $x \in X$. Caso nunca tenha verificado que se trata de um espaço vetorial, faça isso $(\star)$. ▲

Espaços vetoriais aparecem com bastante frequência em cursos de Análise Real – embora geralmente sejam mantidos sob disfarce para turmas iniciantes. Aqui, os principais espaços vetoriais considerados serão o *plano cartesiano* $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ e o *espaço das funções contínuas de* $X \subseteq \mathbb{R}$ *em* $\mathbb{R}$, denotado por $\mathrm{C}(X, \mathbb{R})$, ambos intrinsecamente ligados a questões sobre a reta real. Para finalizar esta breve e bem-intencionada introdução aos espaços vetoriais, convém apresentar as funções que fazem o papel de *morfismos*:

Definição 0.6.24. Uma função $f\colon X \to Y$ entre K-espaços vetoriais X e Y é dita K-**linear** (ou **transformação** K-**linear**[59]) se for compatível com as operações de X e Y, i.e., se $f(\alpha u + v) = \alpha f(u) + f(v)$ para quaisquer $\alpha \in K$ e $u, v \in X$. ¶

[58] Como $u \cdot v = (0, \dots, 0)$ para $u, v \neq (0, \dots, 0)$. Há outros problemas de natureza geométrica que não convêm tratar aqui, mas você pode conferir em https://math.stackexchange.com/questions/185888.

[59] E como de costume, o sufixo "K" é abandonado nas situações em que o corpo é claro pelo contexto.

Exercício 0.83 ($\overset{\star}{\star}$)**.** Mostre que os seguintes resultados para morfismos de anéis permanecem válidos para transformações lineares:

a) itens (a) e (c) do Exercício 0.79;

b) item (b) do Exercício 0.79, para $m \in K$;

c) os Exercícios 0.80 e 0.81;

d) item (a) do Exercício 0.82. ■

0.7 Corpos ordenados

0.7.0 Essencial

Corpos ordenados

Definição 0.7.0. Um corpo $\mathbb{K}$ munido de uma relação de ordem (estrita) total $<$ é chamado de **corpo ordenado** se $<$ for compatível com sua estrutura algébrica, i.e.,

$(\mathrm{CO_i})$ $\forall a, b, c \in \mathbb{K} \quad a < b \Rightarrow a + c < b + c$,

$(\mathrm{CO_{ii}})$ $\forall a, b \in \mathbb{K} \quad a > 0_{\mathbb{K}}$ e $b > 0_{\mathbb{K}} \Rightarrow ab > 0_{\mathbb{K}}$. ¶

Exercício 0.84 (Caracterização alternativa via cones ($\overset{\star}{\star}$))**.** Dado um corpo $\mathbb{K}$, mostre que $\mathbb{K}$ admite uma ordem $<$ que torna $(\mathbb{K}, <)$ um corpo ordenado se, e somente se, existir um subconjunto $P \subseteq \mathbb{K}$ com $x + y, xy \in P$ sempre que $x, y \in P$ e tal que, para qualquer $x \in \mathbb{K}$, ocorra um, e somente um, dos seguintes casos: $x = 0_{\mathbb{K}}$, $x \in P$ ou $-x \in P$. Dica: com a ordem em mãos, faça $P := \{x \in \mathbb{K} : x > 0_{\mathbb{K}}\}$ e note que $x < y$ se, e somente se, $y - x \in P$; com P em mãos, use o passo anterior para definir a ordem em $\mathbb{K}$ de modo adequado. ■

Exemplo 0.7.1. O corpo dos números racionais é um corpo ordenado com sua ordem usual. Caso não se lembre: basta definir $P := \left\{\frac{a}{b} \in \mathbb{Q} : ab > 0\right\}$, que satisfaz as condições do exercício anterior (verifique!)$^{\star}_{\star}$, de modo que

$$\frac{\alpha}{\beta} < \frac{\gamma}{\delta} \Leftrightarrow \frac{\beta\gamma - \alpha\delta}{\beta\delta} \in P \Leftrightarrow \beta\delta(\beta\gamma - \alpha\delta) > 0$$

para quaisquer $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ com $\beta, \delta \neq 0$. Em particular, assumindo $\beta, \delta > 0$ como de costume, resulta que

$$\frac{\alpha}{\beta} < \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta < \beta\gamma,$$

e fica por sua conta testar alguns exemplos com números "de verdade". ▲

Lema 0.7.2 (Fundamental)**.** *Se $\mathbb{K}$ é um corpo ordenado, então $0_{\mathbb{K}} < 1_{\mathbb{K}}$.*

Demonstração. O contrário daria $0_{\mathbb{K}} > 1_{\mathbb{K}}$, posto que a ordem é total e $\mathbb{K}$ é corpo. Logo, a condição $(\mathrm{CO_i})$, com $c := -1_{\mathbb{K}}$, acarretaria $-1_{\mathbb{K}} > 0_{\mathbb{K}}$ e, consequentemente, teria-se $0_{\mathbb{K}} > 1_{\mathbb{K}} = (-1_{\mathbb{K}})(-1_{\mathbb{K}}) > 0_{\mathbb{K}}$ em virtude da condição $(\mathrm{CO_{ii}})$, uma contradição. □

Para o que se discutirá a seguir, é recomendável saber o que é um morfismo de anéis[60] (cf. Subseção 0.6.1).

[60] Se preferir ignorar o conselho: pense que $\rho\colon \mathbb{Q} \to \mathbb{K}$ é uma função que permite interpretar cada número racional q como um elemento de $\rho(q) \in \mathbb{K}$, de forma a respeitar as operações de $\mathbb{Q}$ em $\mathbb{K}$: assim, $\rho(q + q') = \rho(q) + \rho(q')$, etc.

Teorema 0.7.3. *Se $\mathbb{K}$ é corpo ordenado, então existe um único morfismo injetor de anéis $\rho\colon \mathbb{Q} \to \mathbb{K}$.*

Demonstração. Observe que o lema anterior garante que $n_{\mathbb{K}} > 0_{\mathbb{K}}$ para todo $n \in \mathbb{N} \setminus \{0\}$:

- ✓ como $\mathbb{K}$ é corpo, tem-se $1_{\mathbb{K}} > 0_{\mathbb{K}}$;
- ✓ supondo $n_{\mathbb{K}} > 0_{\mathbb{K}}$ para algum $n \geq 1$, tem-se $(n+1)_{\mathbb{K}} := n_{\mathbb{K}} + 1_{\mathbb{K}} > 0_{\mathbb{K}}$, onde a última desigualdade decorre da condição ($\mathrm{CO_i}$).

Logo, $z_{\mathbb{K}} \neq 0_{\mathbb{K}}$ para todo $z \in \mathbb{Z} \setminus \{0\}$. Agora, se $\sigma\colon \mathbb{Q} \to \mathbb{K}$ for *um* morfismo de anéis, então $\sigma|_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{K}$ também é um morfismo de anéis, donde a Proposição 0.6.19 obriga que se tenha $\sigma(z) = z_{\mathbb{K}}$ para todo $z \in \mathbb{Z}$. Por outro lado, da identidade

$$\sigma\left(\frac{a}{1} \cdot \frac{1}{a}\right) = \sigma(a) \cdot \sigma\left(\frac{1}{a}\right),$$

não é difícil concluir que $\sigma\left(\frac{1}{a}\right) = \frac{1}{\sigma(a)}$ para todo $a \in \mathbb{Z} \setminus \{0\}$ e, por conseguinte,

$$\sigma\left(\frac{m}{n}\right) = \frac{m_{\mathbb{K}}}{n_{\mathbb{K}}} := \left(\frac{m}{n}\right)_{\mathbb{K}}$$

deve valer para quaisquer $m, n \in \mathbb{Z}$ com $n \neq 0$. Portanto, tudo se resume a observar que a regra acima define, de fato, um morfismo de anéis da forma $\mathbb{Q} \to \mathbb{K}$, que será injetor por ter *núcleo trivial*. □

Exercício 0.85 ($^{\star}_{\star\star}$)**.** Complete os detalhes. ■

Moralmente, o elemento $q_{\mathbb{K}} \in \mathbb{K}$ descrito recursivamente na demonstração anterior *representa* ou *interpreta* o número racional $q \in \mathbb{Q}$. Para quem tem aversão à Álgebra ~~melhore!~~, pode-se pensar em $\mathbb{K}$ como um *ambiente virtual* no qual é possível *implementar* os números racionais: nesse sentido, a demonstração apenas descreve e justifica o algoritmo de implementação. Se ainda parecer abstrato demais: todo corpo ordenado contém uma *cópia* de $\mathbb{Q}$!

Definição 0.7.4. $\mathbb{Q}_{\mathbb{K}} := \{q_{\mathbb{K}} : q \in \mathbb{Q}\}$. ¶

Muitas propriedades operatórias corriqueiras dos números *reais* que introduziremos em breve são, na verdade, comuns a qualquer corpo ordenado. As mais *úteis* seguem listadas na próxima

Proposição 0.7.5. *Sejam $\mathbb{K}$ um corpo ordenado e $x, y, z \in \mathbb{K}$ elementos quaisquer. Então:*

(i) *$x > 0_{\mathbb{K}}$ se, e somente se, $-x < 0_{\mathbb{K}}$;*

(ii) *se $x > 0_{\mathbb{K}}$ e $y < z$, então $xy < xz$;*

(iii) *se $x < 0_{\mathbb{K}}$ e $y < z$, então $xy > xz$;*

(iv) *$x > 0_{\mathbb{K}}$ se, e somente se, $x^{-1} > 0_{\mathbb{K}}$;*

(v) *se $x \neq 0_{\mathbb{K}}$, então $x^2 > 0_{\mathbb{K}}$;*

(vi) *se $0_{\mathbb{K}} < x < y$, então $0_{\mathbb{K}} < y^{-1} < x^{-1}$.*

Demonstração. Se $x > 0_{\mathbb{K}}$, então $0_{\mathbb{K}} = x - x > 0_{\mathbb{K}} - x = -x$ por conta da condição ($\mathrm{CO_i}$), i.e., $-x < 0_{\mathbb{K}}$. Analogamente mostra-se a recíproca. Os itens (ii) e (iii) seguem de ($\mathrm{CO_{ii}}$) ao se observar que $y < z$ equivale a $y - z < 0_{\mathbb{K}}$. Para o item (iv), note que se $x > 0_{\mathbb{K}}$ e $x^{-1} < 0_{\mathbb{K}}$, então pelo item anterior resultaria $-1_{\mathbb{K}} = (-x)x^{-1} > -x0_{\mathbb{K}} = 0_{\mathbb{K}}$, contrariando o fato de que $0_{\mathbb{K}} < 1_{\mathbb{K}}$; a recíproca segue da identidade $(x^{-1})^{-1} = x$. O quinto item decorre da condição ($\mathrm{CO_{ii}}$) para $x > 0_{\mathbb{K}}$; para $x < 0_{\mathbb{K}}$, o mesmo raciocínio dá $(-x)^2 > 0_{\mathbb{K}}$, enquanto $(-x)^2 = (-1_{\mathbb{K}})^2 x^2 = x^2$. O último é o mais divertido e, por tal razão, ficará por sua conta. □

Exercício 0.86 ($\star_\star$)**.** Complete a demonstração anterior. Dica: para o item (vi), note que $x^{-1}y^{-1} > 0_{\mathbb{K}}$; daí, use a condição (CO$_{\text{ii}}$). ■

Exercício 0.87 ($\star$)**.** Nas condições anteriores, mostre que se $a < c$ e $b < d$ para certos $a, b, c, d \in \mathbb{K}$, então $a + b < c + d$. ■

Valor absoluto e a desigualdade triangular

Definição 0.7.6. Seja $\mathbb{K}$ um corpo ordenado. O **valor absoluto** em $\mathbb{K}$ é a função $|\cdot|_{\mathbb{K}} \colon \mathbb{K} \to \mathbb{K}$ que associa cada $x \in \mathbb{K}$ ao elemento $|x|_{\mathbb{K}} \coloneqq \max\{x, -x\}$. ¶

O valor absoluto constitui uma *maneira uniforme* de "medir" elementos de $\mathbb{K}$ por meio da *comparação* com os habitantes de seu **cone positivo**, i.e., do subconjunto $\mathbb{K}_{\geq 0} \coloneqq \{x \in \mathbb{K} : x \geq 0_{\mathbb{K}}\}$, posto que $|x|_{\mathbb{K}} \in \mathbb{K}_{\geq 0}$ para todo $x \in \mathbb{K}$. Essa "*maneira uniforme*" se refere, entre outras coisas, ao fato de que o valor absoluto é compatível tanto com a estrutura algébrica quanto com a ordem de $\mathbb{K}$, no seguinte sentido.

Proposição 0.7.7. *Sejam $\mathbb{K}$ um corpo ordenado e $x, y \in \mathbb{K}$. Então:*

(i) $|x|_{\mathbb{K}} \geq 0_{\mathbb{K}}$;

(ii) $|x|_{\mathbb{K}} = 0_{\mathbb{K}}$ *se, e somente se,* $x = 0_{\mathbb{K}}$;

(iii) $|xy|_{\mathbb{K}} = |x|_{\mathbb{K}}|y|_{\mathbb{K}}$;

(iv) $|x + y|_{\mathbb{K}} \leq |x|_{\mathbb{K}} + |y|_{\mathbb{K}}$.

Demonstração. Os três primeiros itens ficam por sua conta ($\star_\star$). Como a desigualdade (iv) acima, chamada de **desigualdade triangular**, será extremamente recorrente no texto, convém demonstrá-la aqui: como $-x \leq |x|_{\mathbb{K}}$ e $-y \leq |y|_{\mathbb{K}}$, tem-se $-(x + y) \leq |x|_{\mathbb{K}} + |y|_{\mathbb{K}}$; como também ocorre $x + y \leq |x|_{\mathbb{K}} + |y|_{\mathbb{K}}$, conclui-se que

$$|x + y|_{\mathbb{K}} = \max\{x + y, -(x + y)\} \leq |x|_{\mathbb{K}} + |y|_{\mathbb{K}}.$$ □

Exercício 0.88 ($\star_\star$)**.** Para $x, y \in \mathbb{K}$, com $\mathbb{K}$ corpo ordenado, mostre que são equivalentes:

(i) $-y \leq x \leq y$; (ii) $x \leq y$ e $-x \leq y$; (iii) $|x|_{\mathbb{K}} \leq y$.

Conclua que $|x - y|_{\mathbb{K}} \leq z$ se, e somente se, $y - z \leq x \leq y + z$. ■

Observação 0.7.8. O exercício acima permanece válido ao trocarmos "$\leq$" por "$<$" (verifique!)*. △

Teorema 0.7.9 (Truque fundamental da Análise)**.** *Para α e β elementos de um corpo ordenado $\mathbb{K}$, são equivalentes:*

(i) $\alpha = \beta$;

(ii) $|\alpha - \beta|_{\mathbb{K}} < \varepsilon$ *para todo* $\varepsilon \in \mathbb{K}$ *com* $\varepsilon > 0_{\mathbb{K}}$.

Demonstração. A direção (i) $\Rightarrow$ (ii) é clara. Para a recíproca, se ocorresse $\alpha \neq \beta$, teríamos $\alpha < \beta$ ou $\beta < \alpha$ e, consequentemente, $\beta - \alpha > 0_{\mathbb{K}}$ ou $\alpha - \beta > 0_{\mathbb{K}}$ (respectivamente), de modo que

$$|\alpha - \beta|_{\mathbb{K}} = \max\{\alpha - \beta, \beta - \alpha\} \coloneqq r > 0_{\mathbb{K}},$$

provando o resultado pela contrapositiva. □

Exercício 0.89 ($\star_\star$)**.** Considere $\mathbb{K}$ um corpo ordenado e $x, y \in \mathbb{K}$ quaisquer.

a) Mostre que se $x > y > 0_{\mathbb{K}}$, então $x^2 > y^2$.

b) Mostre que se $x < y < 0_{\mathbb{K}}$, então $x^2 > y^2$.

c) Mostre que se $x > 1_{\mathbb{K}}$, então $x^2 > x$ e, se $0_{\mathbb{K}} < x < 1_{\mathbb{K}}$, então $x^2 < x$. ■

0.7.1 Extras

Espaços vetoriais ordenados

Corpos não são as únicas estruturas algébricas que podem aparecer acompanhadas de uma ordem compatível. Um exemplo que será importante é o seguinte: fixados um corpo ordenado $\mathbb{K}$ e um conjunto X, diremos que uma função $f\colon X \to \mathbb{K}$ é **limitada** se existir $M \in \mathbb{K}$ com $M > 0_{\mathbb{K}}$ tal que $|f(x)|_{\mathbb{K}} \leq M$ para todo $x \in X$. Ao considerar $\mathcal{B}(X, \mathbb{K})$ a coleção de todas as funções limitadas de X em $\mathbb{K}$, obtém-se um legítimo $\mathbb{K}$-espaço vetorial[61] com as operações usuais para espaços de funções (cf. Exemplo 0.6.23):

- ✓ se $f, g \in \mathcal{B}(X, \mathbb{K})$, então $f + g \in \mathbb{K}$ pois, para $M, N \in \mathbb{K}_{>0}$ tais que $|f(x)|_{\mathbb{K}} \leq M$ e $|g(x)|_{\mathbb{K}} \leq N$ para todo $x \in X$, tem-se
$$|f(x) + g(x)|_{\mathbb{K}} \leq |f(x)|_{\mathbb{K}} + |g(x)|_{\mathbb{K}} \leq M + N;$$
- ✓ a função constante nula $\underline{0}\colon X \to \mathbb{K}$ que associa $\underline{0}(x) := 0_{\mathbb{K}}$ para todo x é, claramente, limitada;
- ✓ se $f \in \mathcal{B}(X, \mathbb{K})$ e $\lambda \in \mathbb{K}$, então para $M \in \mathbb{K}_{>0}$ satisfazendo $|f(x)|_{\mathbb{K}} \leq M$ para todo x se verifica
$$|\lambda f(x)|_{\mathbb{K}} = |\lambda|_{\mathbb{K}} |f(x)|_{\mathbb{K}} \leq |\lambda|_{\mathbb{K}} M.$$

A rigor, os pontos acima apenas mostram que obtemos operações legítimas em $\mathcal{B}(X, \mathbb{K})$ ao restringir as operações usuais de $\mathbb{K}^X$ a funções limitadas. No entanto, como as condições operatórias necessárias para elevar $\mathcal{B}(X, \mathbb{K})$ ao patamar de espaço vetorial já são satisfeitas em $\mathbb{K}^X$, segue que $\mathcal{B}(X, \mathbb{K})$ é, de fato, um espaço vetorial[62]. Mas não só isso: para $f, g \in \mathcal{B}(X, \mathbb{K})$, podemos declarar

$$f \leq g \Leftrightarrow f(x) \leq g(x) \quad \text{para todo } x \in X,$$

que se revela uma ordem (parcial) em $\mathcal{B}(X, \mathbb{K})$ com as seguintes propriedades:

(i) $f \leq g \Rightarrow f + h \leq g + h$ para quaisquer $f, g, h \in \mathcal{B}(X, \mathbb{K})$;

(ii) $f \leq g \Rightarrow rf \leq rg$ para quaisquer $f, g \in \mathcal{B}(X, \mathbb{K})$ e $r \in \mathbb{K}_{\geq 0}$.

Um $\mathbb{K}$-espaço vetorial V com uma ordem parcial $\leq$ satisfazendo condições análogas costuma ser chamado de **espaço vetorial ordenado**. É claro que assim como $\mathcal{B}(X, \mathbb{K})$ é espaço vetorial ordenado, o próprio $\mathbb{K}^X$ também é: o uso de $\mathcal{B}(X, \mathbb{K})$ como exemplo inicial foi apenas uma desculpa para mostrar valores absolutos em ação.

Exercício 0.90 $(\overset{\star}{\star\star})$**.** Por que a ordem em $\mathcal{B}(X, \mathbb{K})$ não é total? ■

Observação 0.7.10 (Cuidado com a desigualdade estrita)**.** Por definição, escrever "$f < g$" para funções f e g em $\mathcal{B}(X, \mathbb{K})$ (ou em $\mathbb{K}^X$) abrevia "$f \leq g$ e $f \neq g$". Portanto, trata-se uma afirmação que não é equivalente a "$f(x) < g(x)$ para todo $x \in X$". Reflita. △

Corpos não-ordenáveis

Exercício 0.91 $(\overset{\star}{\star})$**.** Mostre que se K é um corpo finito, então não existe ordem total $<$ sobre K segundo a qual $(K, <)$ seja um corpo ordenado. ■

O exercício acima mostra que existem corpos nos quais é *impossível* definir uma relação de ordem compatível com suas operações. Outro caso típico é $\mathbb{C}$, o **corpo dos números complexos**. Trata-se essencialmente do plano $\mathbb{R}^2$ com uma *multiplicação entre vetores* que torna $\mathbb{R}^2$ num corpo. Tipicamente, escreve-se $a + bi \in \mathbb{C}$ em vez de $(a, b) \in \mathbb{R}^2$, de modo que o produto entre dois elementos de $\mathbb{C}$ é feito de tal forma a valer $i^2 = -1$. Explicitamente:

$$(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i.$$

O problema é que, se $\mathbb{C}$ admitisse uma ordem compatível com suas operações, deveria ocorrer $i^2 > 0$. No entanto, $i^2 = -1$, e a desigualdade $-1 < 0$ vale em qualquer corpo ordenado.

[61] No futuro, trataremos apenas do caso $\mathbb{K} := \mathbb{R}$. Assim, você pode assumir que $\mathbb{K}$ é $\mathbb{R}$ se preferir.

[62] A terminologia correta é "$\mathcal{B}(X, \mathbb{K})$ é subespaço vetorial de $\mathbb{K}^X$".

0.8 Supremos e ínfimos

0.8.0 Essencial

Definição e exemplos

Já temos quase todo o ferramental necessário para *entender* definição da reta real que será apresentada: $\mathbb{R}$ será definido como um corpo ordenado *completo*. É para discutir completude que precisamos voltar alguns passos e introduzir *supremos e ínfimos*.

Definição 0.8.0. Fixada uma *ordem* $(\mathbb{P}, \leq)$, um subconjunto A de $\mathbb{P}$ e um elemento $p \in \mathbb{P}$, diremos que p é um **limitante superior** (ou **majorante**)[63] de A se $x \leq p$ ocorrer para todo $x \in A$. Adicionalmente, dizemos que p é o **supremo** de A se p é *o menor limitante superior* de A. Notação: $\sup A$ ou $\sup_{a \in A} a$. ¶

Observação 0.8.1. Não confunda sup com suc: o primeiro, que indica o supremo, é composto pelas letras **s**, **u**, **p**, enquanto o segundo, que indica o sucessor, é composto pelas letras **s**, **u**, **c**. △

Dualizando a definição de supremo (cf. Subseção 0.2.1), chega-se à noção de *ínfimo*.

Definição 0.8.2. Fixada uma *ordem* $(\mathbb{P}, \leq)$, um subconjunto A de $\mathbb{P}$ e um elemento $p \in \mathbb{P}$, diremos que p é um **limitante inferior** (ou **minorante**)[64] de A se $p \leq x$ ocorrer para todo $x \in A$. Adicionalmente, dizemos que p é o **ínfimo** de A se p é *o maior limitante inferior* de A. Notação: $\inf A$ ou $\inf_{a \in A} a$. ¶

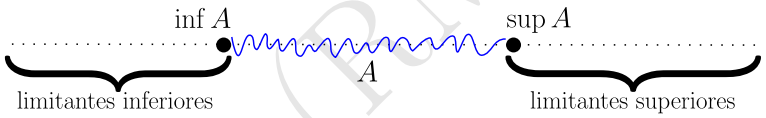


Figura 0.8: O supremo de um conjunto, quando existe, é o *melhor* limitante superior do conjunto. Analogamente, o ínfimo, se existir, é o *melhor* limitante inferior do conjunto.

Exemplo 0.8.3. Máximos são supremos, enquanto mínimos são ínfimos. De fato, se $A \subseteq \mathbb{P}$ tem máximo α, então:

- ✓ α é limitante superior de A por definição;
- ✓ se $\beta \in \mathbb{P}$ é algum outro limitante superior de A, então $a \leq \beta$ vale para todo $a \in A$ e, em particular, vale para α já que $\alpha \in A$.

O caso de mínimos é análogo. ▲

Exercício 0.92 $(\star)$**.** Para uma ordem $(\mathbb{P}, \leq)$ e um subconjunto $A \subseteq \mathbb{P}$, suponha que exista $\alpha := \min A$. Mostre que $\alpha = \inf A$. Dica: você pode imitar o argumento anterior ou apelar diretamente para "dualidade" (cf. Subseção 0.2.1). ■

Exemplo 0.8.4 (A recíproca é falsa!)**.** Em $\mathbb{Q}$, o subconjunto $A := \{q \in \mathbb{Q} : q > 0\}$ não tem menor elemento: dado qualquer $q \in A$, tem-se $\frac{q}{2} \in A$ com $\frac{q}{2} < q$ (por quê?!)*, mostrando que nenhum dos elementos de A pode tomar para si o papel de ser *o menor*. O "problema", como o você já deve ter percebido, é a ausência de 0 em A: se ocorresse $0 \in A$, então 0 seria, trivialmente, o menor elemento de A. Este é o indício de que 0, embora não seja o menor elemento de A, é o seu ínfimo! ▲

[63] Ou ainda **cota superior**.
[64] Ou ainda **cota inferior**.

Formalmente, a afirmação final do exemplo anterior pode se justificar com as seguintes observações:

- ✓ 0 é limitante inferior de A pela definição de A;
- ✓ se $s \in \mathbb{Q}$ e $s \leq q$ para todo $q \in A$, i.e., se s é limitante inferior de A, então $s \leq 0$, posto que *o contrário levaria a concluir* que $0 < s$, donde seguiria $\frac{s}{2} \in A$ com $\frac{s}{2} < s$, contrariando a suposição de s limitar A inferiormente.

Note que só foi possível concluir "$s > 0$" pois a totalidade da ordem impõe a ocorrência de "$s < 0$", "$s = 0$" ou "$s > 0$", de modo que a negação das duas primeiras forçou a validade da última. Noutras palavras, mostrou-se que nenhum $s > 0$ pode limitar A inferiormente, de modo que pela tricotomia, limitantes inferiores de A devem estar *abaixo* de 0. O fenômeno vale em geral.

Teorema 0.8.5. *Fixadas uma ordem <u>total</u> $(\mathbb{T}, \leq)$, um subconjunto $A \subseteq \mathbb{T}$ e $\alpha \in \mathbb{T}$ um limitante inferior de A, são equivalentes:*

(i) $\alpha = \inf A$;

(ii) *para todo $\beta \in \mathbb{T}$, se ocorrer $\beta > \alpha$, então existe $a \in A$ com $a < \beta$.*

Demonstração. Se vale (i), então $\alpha = \max\{l \in \mathbb{T} : l \text{ é limitante inferior de } A\}$, donde segue que se $\beta > \alpha$, então β não pode ser limitante inferior de A, i.e., tem que existir $a \in A$ com $b \not\leq a$, donde a tricotomia acarreta $a < b$, como desejado. Reciprocamente, se vale (ii), então nenhum $\beta > \alpha$ limita A inferiormente ou, equivalentemente (graças à tricotomia), todo β limitante inferior de A satisfaz $\beta \leq \alpha$, donde o restante segue por α ser limitante inferior de A (por hipótese). □

Exercício 0.93 ($\overset{\star}{\star}$)**.** Dualize o teorema anterior, i.e., enuncie (e demonstre) a versão para supremos. Dica: explicitamente, "se α é limitante superior de A, então $\alpha = \sup A$ se, e somente se, para todo $\beta < \alpha$ existir $a \in A$ com $\beta < a$". ■

Supremos e ínfimos em corpos ordenados

Feita esta primeira apresentação, vamos nos ater ao caso em que os supremos e ínfimos são tomados em corpos ordenados. Para aquecer os motores:

Exercício 0.94 ($\star$)**.** Num corpo ordenado $\mathbb{K}$, mostre que $0_{\mathbb{K}} = \inf\{x \in \mathbb{K} : x > 0_{\mathbb{K}}\}$. ■

É bem provável que sua solução para o exercício prove, na verdade, a identidade

$$k = \inf\{x \in \mathbb{K} : x > k\}$$

para qualquer $k \in \mathbb{K}$, o que está absolutamente correto. O ponto é que há mais coisas escondidas aí.

Definição 0.8.6. Para subconjuntos $A, B \subseteq \mathbb{K}$ e $x \in \mathbb{K}$, definimos:

(i) $A + B \coloneqq \{a + b : a \in A \text{ e } b \in B\}$ e $A + x \coloneqq \{a + x : a \in A\}$;

(ii) $AB \coloneqq \{ab : a \in A \text{ e } b \in B\}$ e $xA \coloneqq \{xa : a \in A\}$;

(iii) $-A \coloneqq \{-a : a \in A\}$. ¶

Exercício 0.95 ($\star$)**.** Pratique!

a) Mostre que $A + B = B + A$, $A \cdot B = B \cdot A$, $A + \emptyset = \emptyset$ e $A \cdot \emptyset = \emptyset$.

b) Mostre que $\{x \in \mathbb{K} : x > 0_{\mathbb{K}}\} + k = \{x \in \mathbb{K} : x > k\}$ para qualquer $k \in \mathbb{K}$.

c) Mostre que $0_{\mathbb{K}} A = \{0_{\mathbb{K}}\}$ e $xyA = x(yA)$ para quaisquer $x, y \in \mathbb{K}$.

d) Para $A \coloneqq \{x \in \mathbb{K} : |x|_{\mathbb{K}} < 1_{\mathbb{K}}\}$, mostre que $-A = A$.

e) Mostre que se $A, B \subseteq \mathbb{K}_{>0}$ (i.e., se $x \in A$ ou $x \in B$, então $x > 0_{\mathbb{K}}$), então $AB \subseteq \mathbb{K}_{>0}$. ■

Teorema 0.8.7. *Sejam $A, B \subseteq \mathbb{K}$ subconjuntos não-vazios e $r \in \mathbb{K}$. Supondo que todos os ínfimos e supremos abaixo existam, valem as seguintes afirmações:*

(i) *se $A \subseteq B$, então $\inf A \geq \inf B$ e $\sup A \leq \sup B$;*

(ii) *se $r \geq 0$, então $\inf(rA) = r \inf A$ e $\sup(rA) = r \sup A$;*

(iii) *se $r \leq 0$, então $\inf(rA) = r \sup A$ e $\sup(rA) = r \inf A$;*

(iv) *se $x \geq 0$ para todo $x \in A \cup B$, então $\inf(AB) = \inf A \inf B$ e $\sup(AB) = \sup A \sup B$;*

(v) $\inf(A + B) = \inf A + \inf B$ *e* $\sup(A + B) = \sup A + \sup B$.

Demonstração. Como diria Jack...

(i) Note que se l é limitante inferior de B, então l também é limitante inferior de A (por quê?)*. Logo, se $\beta \coloneqq \inf B$, então $\beta \in \{L' : L' \text{ é limitante inferior de } A\} \coloneqq C$ e, por valer $\inf A \coloneqq \max C$, segue que $\beta \leq \inf A$.

(ii) Note que o resultado é automático para $r \coloneqq 0_{\mathbb{K}}$. Com $r > 0_{\mathbb{K}}$, e chamando $\alpha \coloneqq \sup A$, temos $x \leq \alpha$ para todo $x \in A$ (pois α limita A superiormente). Logo, se $y \in rA$, então $y = rx$ para algum $x \in A$, acarretando em $y = rx \leq r\alpha$, donde a arbitrariedade de y mostra que $r\alpha$ limita rA superiormente. Logo, $\sup(rA) \leq r\alpha$. Por outro lado, com $\beta \coloneqq \sup(rA)$ e tomando $x \in A$ qualquer, obtemos $rx \leq \beta$ e, por conseguinte, $x \leq \frac{\beta}{r}$, donde segue que $\sup A \leq \frac{\beta}{r}$. Logo, $r \sup A \leq \beta$.

(iii) Nada precisa ser feito para $r \coloneqq 0_{\mathbb{K}}$. Supondo $r < 0_{\mathbb{K}}$ e fazendo $\delta \coloneqq \sup A$, mostra-se (como no item anterior) que $r\delta$ é limitante inferior de rA e, por isso, $r\delta \leq \inf(rA)$. Analogamente, com $\varepsilon \coloneqq \inf(rA)$, mostra-se que $\frac{\varepsilon}{r}$ é limitante superior de A, acarretando $\sup A \leq \frac{\varepsilon}{r}$ e, consequentemente, $r \sup A \geq \varepsilon$.

(iv) Primeiro, observe que sob as condições dadas, $AB = \{0_{\mathbb{K}}\}$ se, e somente se, $A = \{0_{\mathbb{K}}\}$ ou $\mathbb{B} = \{0_{\mathbb{K}}\}$, casos em que as identidades são triviais. Assim, podemos assumir que ambos A e B contêm elementos maiores do que $0_{\mathbb{K}}$. Agora, chamando $\alpha \coloneqq \sup A$, $\beta \coloneqq \sup B$ e $\gamma \coloneqq \sup AB$, mostraremos que $\gamma \leq \alpha\beta$ e $\alpha\beta \leq \gamma$. A primeira desigualdade segue pois $x \leq \alpha$ e $y \leq \beta$ para quaisquer $x \in A$ e $y \in B$, e daí $xy \leq \alpha\beta$ em virtude da hipótese sobre os *sinais*. Para a segunda desigualdade:

- ✓ fixado $y \in B$ com $y > 0_{\mathbb{K}}$, temos $xy \leq \gamma$ para todo $x \in A$, o que assegura $x \leq \frac{\gamma}{y}$ e, consequentemente, $\alpha \leq \frac{\gamma}{y}$;
- ✓ dado que $0_{\mathbb{K}} < \alpha$ (por quê?!)*, resulta $y \leq \frac{\gamma}{\alpha}$ e, como isto vale para qualquer $y' \in B$ com $y' > 0_{\mathbb{K}}$, conclui-se que $\beta \leq \frac{\gamma}{\alpha}$ e, portanto, $\alpha\beta \leq \gamma$.

(v) Novamente, façamos $\alpha := \inf A$, $\beta := \inf B$ e $\gamma := \inf(A+B)$. Como $\alpha \leq x$ e $\beta \leq y$ para quaisquer $x \in A$ e $y \in B$, resulta $\alpha+\beta \leq x+y$ e, consequentemente, $\alpha+\beta \leq \gamma$. Para a desigualdade restante, observe que $x \leq \gamma - y$ para quaisquer $x \in A$ e $y \in B$, o que resulta em $\alpha \leq \gamma - y$ e, consequentemente, $\beta \leq \gamma - \alpha$. □

Exercício 0.96 ($^{\star}_{\star\star}$)**.** Complete a demonstração do teorema anterior. ■

A demonstração do teorema anterior foi simplificada por uma hipótese preguiçosa: a suposição de que os supremos e ínfimos considerados *sempre* existem. Sem ela, os enunciados ficariam um pouco mais complicados. Por exemplo, no caso de (ii), para o supremo, seria preferível escrever "se $\sup A$ existe, então rA tem supremo e $\sup(rA) = r \sup A$ para qualquer $r \geq 0$": neste caso, seria necessário observar que rA é limitado superiormente para daí provar que $r \sup A$ é o menor limitante superior de rA. Após reler com atenção a demonstração, você perceberá que, no fundo, foi isso o que provamos – então, na prática, nada se perdeu[65]. Tais ressalvas se aplicam também a (iii), (iv) e (v). O item (i), como veremos, é mais delicado, e só se resolve com a hipótese de *completude*.

0.8.1 Extras

Supremos e ínfimos em ordens parciais

Supremos e ínfimos não são exclusividade de ordens totais. Porém, a vida sem tricotomia é um pouco menos óbvia: sem a tricotomia, o Teorema 0.8.5 não se aplica, por exemplo. Ainda assim, tais animais estão em todo lugar.

Exemplo 0.8.8. Dado um conjunto X e subconjuntos $A, B \subseteq X$, existem $\sup\{A,B\}$ e $\inf\{A,B\}$ em $(\wp(X), \subseteq)$? Se sim, quem são? Vejamos:

(i) se existir, $\sup\{A,B\}$ deve limitar superiormente o conjunto $\{A,B\}$, acarretando $A, B \subseteq \sup\{A,B\}$ e, além disso, se C for um subconjunto de X com $A, B \subseteq C$, também deverá ocorrer $\sup\{A,B\} \subseteq C$ (o supremo de um conjunto é o seu *menor* limitante superior!);

(ii) analogamente, se existir $\inf\{A,B\}$, este deverá não apenas limitar inferiormente $\{A,B\}$ (i.e., $\inf\{A,B\} \subseteq A, B$), como também satisfazer $D \subseteq \inf\{A,B\}$ para qualquer subconjunto D de X com $D \subseteq A, B$ (o ínfimo de um conjunto é o seu *maior* limitante inferior!).

Parece familiar, não? Explicitamente, $\sup\{A,B\}$ deve ser o menor subconjunto de X a conter tanto A quanto B, e já conhecemos um subconjunto que faz isso: $A \cup B$! E, de fato, tem-se $\sup\{A,B\} = A \cup B$:

✓ $A \cup B$ limita $\{A,B\}$ superiormente, pois ocorre $A, B \subseteq A \cup B$;

✓ $A \cup B$ é o menor limitante superior de $\{A,B\}$, já que $A \cup B \subseteq C$ sempre que $A, B \subseteq C$.

Talvez você possa estar se perguntando: como é possível que as linhas de argumentação acima tenham provado a identidade "$\sup\{A,B\} = A \cup B$", dado que a expressão "$\sup\{A,B\}$" nem sequer apareceu? Resposta: as condições verificadas acima são a *definição de supremo* que, quando existe, é único; assim, ao mostrar que $A \cup B$ tem as propriedades que $\sup\{A,B\}$ deveria ter, conclui-se que $A \cup B$ *é* o supremo procurado. ▲

Exercício 0.97 ($^{\star}_{\star\star}$)**.** Mostre que $A \cap B = \inf\{A,B\}$ em $\wp(X)$. ■

Após a introdução de corpos completos na próxima seção, será prática comum tomar supremos e ínfimos apenas de subconjuntos não-vazios e limitados. No entanto, a definição não proíbe tais casos, o que traz a pergunta: o que seriam $\sup_{\mathbb{P}} \emptyset$ e $\inf_{\mathbb{P}} \emptyset$ numa ordem $(\mathbb{P}, \leq)$?

[65] Explicitamente: se $\sup A$ existe, então $rx \leq r \sup A$ para todo $x \in A$, mostrando que $r \sup A$ limita rA superiormente; agora, se $rx \leq \mu$ para todo $x \in A$, então $x \leq \frac{\mu}{r}$, donde segue que $\sup A \leq \frac{\mu}{r}$ e, por conseguinte, $r \sup A \leq \mu$, mostrando que $r \sup A$ é o menor limitante superior de rA.

Explicitamente, $\sup_{\mathbb{P}} \emptyset$ é o menor dos limitantes inferiores de $\emptyset$. Agora, leia com calma: como todo elemento de $\mathbb{P}$ é limitante superior de $\emptyset$ (por vacuidade!), segue que $\emptyset$ tem supremo em $\mathbb{P}$ se, e somente se, $\mathbb{P}$ tem mínimo e, neste caso, $\sup_{\mathbb{P}} \emptyset = \min \mathbb{P}$. Analogamente, $\emptyset$ tem ínfimo em $\mathbb{P}$ se, e somente se, $\mathbb{P}$ tem máximo, e vale $\inf_{\mathbb{P}} \emptyset = \max \mathbb{P}$. É por isso que em corpos ordenados, não existem $\sup \emptyset$ nem $\inf \emptyset$: corpos ordenados são ilimitados inferior e superiormente (verifique)* e, em particular, não têm máximo e nem mínimo.

(Importante) corpos estendidos e intervalos

Em contraponto ao que se observou acima, é formalmente lícito *acrescentar* pontos num corpo ordenado $\mathbb{K}$ que sirvam como *extremos*. De modo geral, dada uma ordem parcial $(\mathbb{P}, \leq)$, é possível tomar elementos *artificiais*[66] distintos $p, q \notin \mathbb{P}$ e fazer $\overline{\mathbb{P}} := \mathbb{P} \cup \{p, q\}$, para daí definir uma ordem parcial $\preceq$ que estende $\leq$, declarando-se $p \preceq x$ e $x \preceq q$ para qualquer $x \in \overline{\mathbb{P}}$, e para $x, y \in \mathbb{P}$, $x \preceq y$ se, e somente se, $x \leq y$; em particular, obtém-se $p = \min \overline{\mathbb{P}}$ e $q = \max \overline{\mathbb{P}}$. Um *corpo estendido* é a ordem oriunda deste processo aplicado a um corpo ordenado.

Definição 0.8.9. Dado um corpo ordenado $\mathbb{K}$, denota-se por $\overline{\mathbb{K}}$ o conjunto $\mathbb{K} \cup \{-\infty, +\infty\}$, onde $-\infty, +\infty \notin \mathbb{K}$, com a ordem definida acima (com $p := -\infty$ e $q := +\infty$), que passa a ser chamado de **corpo estendido**. ¶

Observação 0.8.10. No futuro, tal definição se aplicará exclusivamente a $\mathbb{K} := \mathbb{R}$, caso em que $\overline{\mathbb{R}}$ será chamada de *reta estendida*. Então, se preferir, pode fingir que $\mathbb{K}$ é $\mathbb{R}$. △

A escolha do símbolo "∞" para indicar os pontos artificiais acrescentados ao corpo $\mathbb{K}$ é arbitrária e segue apenas a prática comum. Dito isso, é importante ressaltar que, embora seja frequente se referir a tais pontos como "infinitos", seria mais correto xingá-los de *ilimitados*, posto que "infinito" costuma se referir à cardinalidade de conjuntos, enquanto "$-\infty$" e "$+\infty$" apenas denotam *extremos* artificiais numa ordem, algo bem mais específico.

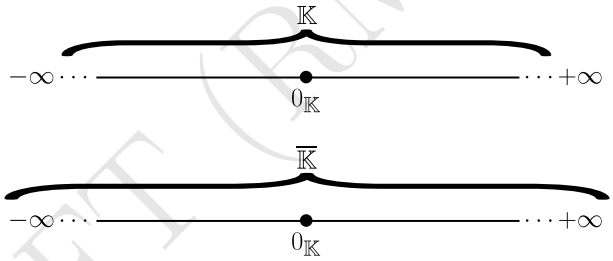


Figura 0.9: Se você já aceita o desenho de cima, por que não aceitar o desenho de baixo?

Definição 0.8.11 (Intervalos abertos)**.** Para $\alpha, \beta \in \overline{\mathbb{K}}$, os conjuntos

$$[-\infty, \beta)_{\mathbb{K}} := \{x \in \overline{\mathbb{K}} : x < \beta\}, \tag{0.1}$$

$$(\alpha, +\infty]_{\mathbb{K}} := \{x \in \overline{\mathbb{K}} : \alpha < x\} \tag{0.2}$$

serão chamados de *intervalos abertos fundamentais* de $\overline{\mathbb{K}}$. Diremos que $I \subseteq \overline{\mathbb{K}}$ é um **intervalo aberto** se I for interseção finita de intervalos fundamentais. Quando $\mathbb{K}$ for claro pelo contexto, os subíndices serão abandonados[67]. ¶

Sim: a notação acima não está errada, e os intervalos foram "fechados" nos pontos *infinitos*. Você não podia fazer isso em Cálculo I pois ainda não tinha idade para entender certas coisas, como a liberdade poética proporcionada pela Teoria dos Conjuntos. Mas esta fase da sua vida passou. Agora, por exemplo, é completamente lícito considerar o intervalo $[-\infty, 5)_{\mathbb{Q}}$ em $\overline{\mathbb{Q}}$, explicitamente composto pelo ponto $-\infty$ e todos os números racionais menores do que 5, ou seja:

$$[-\infty, 5)_{\mathbb{Q}} = \{-\infty\} \cup \{x \in \mathbb{Q} : x < 5\}.$$

O mesmo se aplica à definição dada para intervalo aberto: secretamente, ela generaliza os intervalos abertos que você já conhecia.

[66] Ou virtuais, fictícios, etc. Não faz diferença, dado que tudo aqui é algum tipo de ficção.

[67] Em particular, após a introdução de $\mathbb{R}$, sempre consideraremos $\mathbb{K} = \mathbb{R}$.

Proposição 0.8.12. *Para $a, b \in \overline{\mathbb{K}}$, o subconjunto*

$$(a,b)_{\mathbb{K}} := \left\{x \in \overline{\mathbb{K}} : a < x < b\right\}$$

é um intervalo aberto inteiramente contido em $\mathbb{K}$, i.e., $(a,b)_{\mathbb{K}} \subseteq \mathbb{K}$. Em particular, $\emptyset$, $\mathbb{K}$, (k,l), $(-\infty,k)_{\mathbb{K}}$ e $(k,+\infty)_{\mathbb{K}}$ são intervalos abertos contidos em $\mathbb{K}$, para quaisquer $k,l \in \mathbb{K}$.

Demonstração. A segunda parte segue da primeira ao se observar que $\emptyset = (a,b)_{\mathbb{K}}$ sempre que $b \leq a$ e $\mathbb{K} = (-\infty,+\infty)_{\mathbb{K}}$. Para a primeira parte, note que $(a,b)_{\mathbb{K}} = [-\infty,b)_{\mathbb{K}} \cap (a,+\infty]_{\mathbb{K}}$, ou seja, é uma interseção finita de intervalos abertos fundamentais e, por isso, é um intervalo aberto. A inclusão segue pois $-\infty \leq a, b \leq +\infty$, de modo que se $a < x < b$, então $x \notin \{-\infty,+\infty\}$ e, portanto, $x \in \mathbb{K}$. □

Observação 0.8.13. Embora a proposta seja elevar $-\infty$ e $+\infty$ ao patamar de *pontos*, eles não são elementos do corpo e, por isso, não podem ser operados livremente com os outros *elementos* do corpo. Em particular, não escreva atrocidades do tipo "$-\infty + \infty = 0$". Lembre-se: o mundo não vai acabar se você pensar um pouco antes de escrever uma abobrinha. △

O motivo para tais *intervalos* serem chamados de *abertos* só será abordado no próximo capítulo. Com isso dito, há outra palavra que deveria ter chamado sua atenção: por que tais animais são chamados de intervalos? Afinal, o que *significa* ser um intervalo?

Definição 0.8.14. Seja $(\mathbb{P},\leq)$ uma ordem. Dizemos que um subconjunto $I \subseteq \mathbb{P}$ é um **intervalo** se para quaisquer $a,b,c \in \mathbb{P}$ valer que $c \in I$ sempre que $a \leq c \leq b$ com $a,b \in I$. ¶

Figura 0.10: Na figura à esquerda, quaisquer dois pontos entre a e b estão na região destacada. Já na figura à direita, há pontos entre a e b que não estão na região destacada.

Exercício 0.98 $(\overset{\star}{\star})$**.** Seja $\mathbb{K}$ um corpo ordenado.

a) Mostre que os intervalos abertos fundamentais de $\overline{\mathbb{K}}$ são intervalos.

b) Mostre que a interseção de intervalos (numa ordem qualquer) é um intervalo.

c) Conclua que os intervalos abertos de $\overline{\mathbb{K}}$ são intervalos. ■

Em particular, após introduzirmos a reta real $\mathbb{R}$, poderemos classificar todos os subconjuntos de $\mathbb{R}$ e de $\overline{\mathbb{R}}$ que são intervalos, o que condiz com os exemplos usuais que você já conhece do Cálculo I. Um pouco mais adiante, em posse da noção de *conexidade*, veremos que os intervalos são, precisamente, os subconjuntos *conexos* de $\mathbb{R}$, como mandam o *bom senso* e a *intuição*. Isto sugere a pergunta: se, na prática, os intervalos serão exatamente os subconjuntos que já sabíamos ser intervalos, para que serve ter uma definição abstrata de intervalo? Resposta: para simplificar a vida, sempre[68]!

Exercício 0.99 $(\overset{\star}{\star\star})$**.** Supondo que $(\mathbb{T},\leq)$ é ordem total, sejam $\alpha,\beta \in \mathbb{T}$, com $\alpha < \beta$. Mostre que se $I,J \subseteq \mathbb{T}$ são intervalos tais que $\alpha \in I$, $\beta \in J$ e $I \cap J = \emptyset$, então para quaisquer $x \in I$ e $y \in J$ deve ocorrer $x < y$. ■

Futuramente, o exercício acima será usado na demonstração da clássica "lei da conservação do sinal", uma importante propriedade dos limites de ~~redes~~ funções e sequências em $\mathbb{R}$.

0.9 Completude (no sentido de Dedekind)

0.9.0 Essencial

Cortes e corpos completos

É chegada a hora de apresentar a reta real: a ideia é definir $\mathbb{R}$ como um corpo ordenado *sem buracos*. Evidentemente, isto pressupõe que saibamos o que é um *buraco*. No entanto, por questões estéticas e morais, buracos serão chamados de *cortes*.

[68] Como dizia o Prof. Alexandre "Sasha" Ananin, "a preguiça é a locomotiva do progresso".

Definição 0.9.0. Seja $\mathbb{K}$ um corpo ordenado. Um **corte** em $\mathbb{K}$ é um par (A, B) de subconjuntos não-vazios de $\mathbb{K}$ tais que

(i) $A \cap B = \emptyset$ e $A \cup B = \mathbb{K}$,

(ii) para quaisquer $a \in A$ e $b \in B$ ocorre $a < b$. ¶

Exemplo 0.9.1. Ampliando o leque de *intervalos* discutidos na Definição 0.8.11 e na Proposição 0.8.12 (cf. Subseção 0.8.1), fixado um corpo ordenado $\mathbb{K}$ e elementos $\alpha, \beta \in \overline{\mathbb{K}}$, definimos

(i) $[\alpha, \beta]_{\mathbb{K}} := \{x \in \overline{\mathbb{K}} : \alpha \leq x \leq \beta\}$,

(ii) $[\alpha, \beta)_{\mathbb{K}} := \{x \in \overline{\mathbb{K}} : \alpha \leq x < \beta\}$ e

(iii) $(\alpha, \beta]_{\mathbb{K}} := \{x \in \overline{\mathbb{K}} : \alpha < x \leq \beta\}$,

todos intervalos no sentido da Definição 0.8.14. Em particular, para $p \in \mathbb{K}$, ambos os intervalos $(-\infty, p]_{\mathbb{K}}$ e $[p, +\infty)_{\mathbb{K}}$ são subconjuntos de $\mathbb{K}$ (verifique?)* que induzem os chamados *cortes triviais*.

✓ (A, B) com $A := (-\infty, p]_{\mathbb{K}}$ e $B := (p, +\infty)_{\mathbb{K}}$, e

✓ (A, B) com $A := (-\infty, p)_{\mathbb{K}}$ e $B := [p, +\infty)_{\mathbb{K}}$.

Em geral, diremos que um corte (A, B) é **trivial** se existir $p \in \mathbb{K}$ tal que $p = \max A$ ou $p = \min B$. Desse modo, não é difícil perceber que (A, B) é trivial se, e somente se, (A, B) se enquadra em um dos casos acima para algum $p \in \mathbb{K}$ (verifique?)*. ▲

Como o exemplo acima sugere, os subconjuntos A e B na definição do corte (A, B) correspondem aos dois pedaços que se obteriam de $\mathbb{K}$ se este fosse *cortado* num determinado *ponto* de $\mathbb{K}$. É por essa razão que os cortes do exemplo anterior são triviais: para qualquer ponto $p \in \mathbb{K}$ fixado, é *trivial* cortar a reta em p, basta "inclinar a lâmina" para que p fique num dos lados do corte. A grande sacada vem agora: a depender do corpo considerado, podem haver "buracos" que permitam cortes sem extremos, i.e., não-triviais.

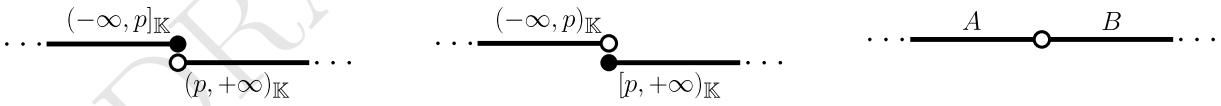


Figura 0.11: Um corte não-trivial é, na prática, um "buraco".

Exemplo 0.9.2 (Fundamental: $\sqrt{2}$)**.** Fixado um corpo ordenado $\mathbb{K}$, os subconjuntos

$$A := \{x \in \mathbb{K} : x < 0_{\mathbb{K}} \text{ ou } 0_{\mathbb{K}} \leq x^2 < 2_{\mathbb{K}}\} \text{ e } B := \{x \in \mathbb{K} : x > 0_{\mathbb{K}} \text{ e } x^2 \geq 2_{\mathbb{K}}\}$$

determinam um corte (A, B) em $\mathbb{K}$.

✓ $A \neq \emptyset$ pois $0_{\mathbb{K}}, 1_{\mathbb{K}} \in A$ e $B \neq \emptyset$ pois $2_{\mathbb{K}} \in B$.

✓ A tricotomia da ordem de $\mathbb{K}$ acarreta tanto $A \cap B = \emptyset$ quanto $A \cup B = \mathbb{K}$ (certo?)*.

✓ Finalmente, se $a \in A$ e $b \in B$, então $a < b$: isto é evidente para $a < 0_{\mathbb{K}}$; se ocorresse $a \geq 0_{\mathbb{K}}$ com $a \geq b$, teria-se $a^2 \geq ab \geq b^2 \geq 2_{\mathbb{K}}$, acarretando em $a \notin A$.

Pergunta-se: tal corte é, necessariamente, induzido por algum $\alpha \in \mathbb{K}$? Como a discussão no Exemplo 0.9.1 sugere, isto equivale a perguntar sobre a existência de máximo para A ou mínimo para B.

Lema 0.9.3. *Seja $\alpha \in \mathbb{K}$. Se $\alpha = \sup A$ ou $\alpha = \min B$, então $\alpha^2 = 2_{\mathbb{K}}$.*

Demonstração. A prova a seguir é adaptada de Rudin [16]. Essencialmente, a ideia é mostrar que se $\alpha^2 \neq 2_{\mathbb{K}}$, então α não pode ser supremo de A e tampouco pode ser mínimo de B. Algumas considerações iniciais:

(i) como $1_{\mathbb{K}} \in A$ e $b > 0_{\mathbb{K}}$ para todo $b \in B$, podemos supor $\alpha > 0_{\mathbb{K}}$;

(ii) como a ordem de $\mathbb{K}$ é total, de $\alpha^2 \neq 2_{\mathbb{K}}$ restam apenas as alternativas $\alpha^2 < 2_{\mathbb{K}}$ ou $\alpha^2 > 2_{\mathbb{K}}$;

(iii) se ocorrer o primeiro caso, então $\alpha \notin B$ e, portanto, α não pode ser o mínimo de B;

(iv) se ocorrer o segundo caso, então $\alpha \in B$;

(v) se $\alpha \in B$ mas $\alpha \neq \min B$, então existe $b \in B$ com $b < \alpha$, donde segue que α não pode ser o supremo de A (certo?)*.

Desta argumentação preliminar, resulta que basta mostrar duas afirmações.

Afirmação 0. *Se $\alpha^2 < 2_{\mathbb{K}}$, então α não é supremo de A.*

Afirmação 1. *Se $\alpha^2 > 2_{\mathbb{K}}$, então α não é mínimo de B.*

⌜*Demonstração.* Para mostrar que α não é supremo de A, basta obter $\beta \in A$ tal que $\alpha < \beta$ (pois assim α não limitará A superiormente). Para mostrar que α não é mínimo de B, basta obter $\beta \in B$ com $\beta < \alpha$. Ora, escrevendo $\beta := \alpha + \gamma$, precisamos determinar γ de modo que se $\alpha \in A$, então $\gamma > 0$ com $\alpha + \gamma \in A$, e se $\alpha \in B$, então $\gamma < 0$ com $\alpha + \gamma \in B$. Como Rudin [16], faremos

$$\gamma := -\frac{\alpha^2 - 2_{\mathbb{K}}}{\alpha + 2_{\mathbb{K}}}, \tag{!!}$$

o que assegura as identidades (verifique!)*

$$\underbrace{\beta = \alpha - \frac{\alpha^2 - 2_{\mathbb{K}}}{\alpha + 2_{\mathbb{K}}}}_{(A)} = \frac{2_{\mathbb{K}}\alpha + 2_{\mathbb{K}}}{\alpha + 2_{\mathbb{K}}} \quad \text{e} \quad \underbrace{\beta^2 - 2_{\mathbb{K}} = \frac{2_{\mathbb{K}}(\alpha^2 - 2_{\mathbb{K}})}{(\alpha + 2_{\mathbb{K}})^2}}_{(B)}.$$

Antes de prosseguir, observe que $\beta > 0_{\mathbb{K}}$ (o contrário daria $\alpha \leq -1_{\mathbb{K}}$). Agora, se $\alpha^2 < 2_{\mathbb{K}}$, então $\alpha^2 - 2_{\mathbb{K}} < 0_{\mathbb{K}}$, donde (A) acarreta $\beta > \alpha > 0_{\mathbb{K}}$, enquanto (B) garante $\beta \in A$. Por outro lado, se $\alpha^2 > 2_{\mathbb{K}}$, então $\alpha^2 - 2_{\mathbb{K}} > 0_{\mathbb{K}}$, donde (A) acarreta $0_{\mathbb{K}} < \beta < \alpha$, enquanto (B) implica $\beta^2 > 2_{\mathbb{K}}$, i.e., $\beta \in B$. ⌟

Enfim, se $\alpha^2 \neq 2_{\mathbb{K}}$ e:

✗ $\alpha < 2_{\mathbb{K}}$, então α não pode ser mínimo de B (por (iii)), enquanto a Afirmação 0 prova que α também não pode ser supremo de A;

✗ $\alpha > 2_{\mathbb{K}}$, então α não pode ser mínimo de B pela Afirmação 1, enquanto (v) prova que α também não pode ser supremo de A. □

Em posse do lema acima, observe que se $\mathbb{K}$ for um corpo em que *não existe* $\alpha \in \mathbb{K}$ satisfazendo $\alpha^2 = 2_{\mathbb{K}}$, então o corte (A, B) não poderá ser trivial: se algum $p \in \mathbb{K}$ fosse o máximo de A, então ocorreria $p = \sup A$ e, pelo lema, $p^2 = 2_{\mathbb{K}}$; analogamente, nenhum p pode ser mínimo de B. Em particular, $\mathbb{Q}$ tem buracos! ▲

Exercício 0.100 ($^\star_\star$)**.** Mostre que não existe $q \in \mathbb{Q}$ com $q^2 = 2$. ■

Observação 0.9.4 (De onde Rudin tirou aquele β?!)**.** Note que o *sinal* do γ procurado é dado, em ambos os casos, por $\alpha^2 - 2_{\mathbb{K}}$: no primeiro caso, temos $\alpha^2 - 2_{\mathbb{K}} < 0_{\mathbb{K}}$ e buscamos $\gamma > 0_{\mathbb{K}}$; no segundo caso, temos $\alpha^2 - 2_{\mathbb{K}} > 0_{\mathbb{K}}$ e buscamos $\gamma < 0_{\mathbb{K}}$. Assim, podemos fazer $\gamma := -(p^2 - 2_{\mathbb{K}})x$ a fim de encontrar valores de x que resolvam o problema. Em outras palavras: caímos na resolução de uma inequação de segundo grau!

`[Fingindo que estamos em` $\mathbb{R}$`]`. Com γ dado como acima, podemos reescrever $\beta^2 - 2$ fazendo

$$\beta^2 - 2 = (\alpha^2 - 2)(1 - 2\alpha x + (\alpha^2 - 2)x^2),$$

e para se ter $\beta^2 - 2 = 0$, há dois valores possíveis para x, a saber $\frac{1}{\alpha+\sqrt{2}}$ e $\frac{1}{\alpha-\sqrt{2}}$ (verifique!)[69]. Logo, basta tomar x no intervalo *real* $\left(0, \frac{1}{\alpha+\sqrt{2}}\right)$ (certo?)*. Ora, como espera-se implementar tal solução num corpo ordenado qualquer, precisa-se escolher um x racional neste intervalo. Enfim, como $\sqrt{2} < 2$, segue que basta tomar $x := \frac{1}{p+2}$. Brilhante[70]. △

Reconhecido o problema, precisa-se encontrar uma solução: o que exigir sobre um corpo ordenado a fim de não ter buracos?

Exercício 0.101 ($^\star_{\star\star}$)**.** Sejam $\mathbb{K}$ um corpo ordenado e (A, B) um corte em $\mathbb{K}$. Para $\alpha \in \mathbb{K}$ qualquer, mostre que $\alpha = \sup A$ se, e somente se, $\alpha = \inf B$. Dica: antes de qualquer outra coisa, faça um desenho. ■

Observe então que se $\alpha = \sup A$ (ou $\alpha = \inf B$), então de duas uma: ou $\alpha = \max A$ ou $\alpha = \min B$. Com efeito, por valer $\mathbb{K} = A \cup B$, tem-se $\alpha \in A$ ou $\alpha \in B$, donde segue que $\alpha = \max A$ ou $\alpha = \min B$. Descobrimos assim como tampar os buracos de um corpo ordenado.

Definição 0.9.5. Um corpo ordenado $\mathbb{K}$ é chamado de **completo**[71] se todo subconjunto não-vazio $A \subseteq \mathbb{K}$ limitado superiormente tem supremo. ¶

Exercício 0.102 ($^\star_\star$)**.** Mostre que se $\mathbb{K}$ é um corpo ordenado completo e (A, B) é um corte em $\mathbb{K}$, então (A, B) é trivial. ■

A condição arquimediana

A completude também traz outra consequência fundamental que você provavelmente pensou que era "de graça".

Teorema 0.9.6. *Se $\mathbb{K}$ é um corpo ordenado e completo, então o subconjunto*

$$\mathbb{N}_{\mathbb{K}} := \{n_{\mathbb{K}} : n \in \mathbb{N}\}$$

não é limitado superiormente, i.e., para qualquer $x \in \mathbb{K}$ existe $n \in \mathbb{N}$ tal que $x < n_{\mathbb{K}}$.

[69] Por "Bhaskara" mesmo! ($^\star_\star$)

[70] Rudin é conhecido por apresentar argumentos fantásticos sem enfatizar suas possíveis motivações. Nesse aspecto, ele não é melhor que o Elon. Em todo caso, para aprofundar a discussão sobre o que pode ter motivado as escolha do "γ de Rudin", confira https://math.stackexchange.com/questions/141774.

[71] Ou *Dedekind-completo*.

Demonstração. Se $\mathbb{N}_{\mathbb{K}}$ fosse limitado superiormente, existiria $\alpha := \sup \mathbb{N}_{\mathbb{K}} \in \mathbb{K}$. Como $\alpha - 1_{\mathbb{K}} < \alpha$, a minimalidade de α como limitante superior de $\mathbb{N}_{\mathbb{K}}$ acarreta a existência de $n \in \mathbb{N}$ tal que $\alpha - 1_{\mathbb{K}} < n_{\mathbb{K}}$. Mas daí $\alpha < n_{\mathbb{K}} + 1_{\mathbb{K}} \in \mathbb{N}_{\mathbb{K}}$, uma contradição. □

Definição 0.9.7. Um corpo ordenado $\mathbb{K}$ satisfazendo a tese do teorema acima é chamado de (corpo) **arquimediano**. ¶

Que grande porcaria a propriedade arquimediana, não é mesmo? O conjunto dos naturais é ilimitado?! O que de útil poderia decorrer de uma afirmação tão *trivial*? Resposta:

Proposição 0.9.8. *Dado um corpo ordenado $\mathbb{K}$, são equivalentes:*

(i) ($\mathbb{K}$ é arquimediano) *$\mathbb{N}_{\mathbb{K}}$ não é limitado superiormente em $\mathbb{K}$;*

(ii) (ausência de "ilimitados") *não existe $x \in \mathbb{K}$ com $n_{\mathbb{K}} < x$ para todo $n \in \mathbb{N}$;*

(iii) (ausência de "infinitésimos") *não existe $x \in \mathbb{K}$ com $x \neq 0_{\mathbb{K}}$ satisfazendo*

$$|x|_{\mathbb{K}} < \frac{1_{\mathbb{K}}}{n_{\mathbb{K}}}$$

para todo $n \in \mathbb{N} \setminus \{0\}$;

(iv) ($\mathbb{Q}$ é "denso" em $\mathbb{K}$) *se $x, y \in \mathbb{K}$ e $x < y$, então existe $q \in \mathbb{Q}$ tal que $x < q_{\mathbb{K}} < y$.*

Demonstração. Os três primeiros itens são *claramente* equivalentes entre si (já sabé, né?)$^{\star}_{\star}$. Agora, assumindo (iii), provaremos (iv). Como $x < y$, temos $y - x = |y - x|_{\mathbb{K}} > 0_{\mathbb{K}}$ e, por (iii), existe $n \in \mathbb{N}$ com

$$\frac{1_{\mathbb{K}}}{n_{\mathbb{K}}} < y - x$$

e, por conseguinte, $1_{\mathbb{K}} + nx < ny$. Se conseguirmos "encaixar" um $m_{\mathbb{K}}$ entre nx e $1_{\mathbb{K}} + nx$, fazendo $nx < m_{\mathbb{K}} \leq 1_{\mathbb{K}} + nx$, então a desigualdade desejada seguirá com $q := \frac{m_{\mathbb{K}}}{n_{\mathbb{K}}}$. Supondo $0_{\mathbb{K}} < x$, a condição (iii) novamente assegura $s \in \mathbb{N}$ com

$$\frac{1_{\mathbb{K}}}{s_{\mathbb{K}}} < \frac{1_{\mathbb{K}}}{nx},$$

de modo que ao tomar $m := \min\left\{s \in \mathbb{N} : \frac{1_{\mathbb{K}}}{s_{\mathbb{K}}} < \frac{1_{\mathbb{K}}}{nx}\right\}$ resulta $m_{\mathbb{K}} - 1_{\mathbb{K}} \leq nx < m_{\mathbb{K}}$ e, consequentemente, $nx < m_{\mathbb{K}} \leq nx + 1_{\mathbb{K}}$. Os casos em que $x \leq 0_{\mathbb{K}}$ ficam por sua conta ($^{\star}_{\star}$).

Finalmente, supondo (iv), mostraremos que $\mathbb{N}$ é ilimitado superiormente: para $r \in \mathbb{K}$ com $r > 0_{\mathbb{K}}$, existem $m, n \in \mathbb{N}$ tais que

$$0_{\mathbb{K}} < \frac{1_{\mathbb{K}}}{n_{\mathbb{K}}} \leq \frac{m_{\mathbb{K}}}{n_{\mathbb{K}}} < \frac{1_{\mathbb{K}}}{r},$$

donde segue que $r < n_{\mathbb{K}}$, como desejado. □

Exercício 0.103 ($\star$)**.** Sejam $\mathbb{K}$ um corpo arquimediano e $x, y \in \mathbb{K}$. Mostre que se $x, y > 0_{\mathbb{K}}$, então existe $N \in \mathbb{N}$ com $Nx > y$. ■

A proposição acima estabelece que para um corpo ordenado $\mathbb{K}$ fixado, são as cópias de $\mathbb{N}$ e $\mathbb{Q}$ em $\mathbb{K}$ que codificam a informação necessária para decidir se $\mathbb{K}$ é arquimediano ou não. Em particular, é de se esperar que o próprio corpo ordenado $\mathbb{Q}$ seja arquimediano, o que de fato ocorre: dados $p, q \in \mathbb{Q}$ distintos, não é difícil perceber que $s := p + r$ é tal que $p < s < q$, onde $r := \frac{|p-q|}{2}$. Em particular, por $\mathbb{Q}$ ter subconjuntos não-vazios, limitados superiormente e sem supremo, resulta que a condição arquimediana não garante completude.

0.9.1 Extras

Corpos não-arquimedianos

Definição 0.9.9. Dado um corpo ordenado $\mathbb{K}$, diremos que $x \in \mathbb{K}$ é **infinitesimal** em $\mathbb{K}$, ou é um **infinitésimo**, se para todo $n \in \mathbb{N}$ valer $|nx|_{\mathbb{K}} < 1_{\mathbb{K}}$. Analogamente, $x \in \mathbb{K}$ é **ilimitado**[72] em $\mathbb{K}$ se para todo $n \in \mathbb{N}$ valer $n_{\mathbb{K}} < |x|_{\mathbb{K}}$. ¶

É claro que $0_{\mathbb{K}} \in \mathbb{K}$ é infinitesimal em $\mathbb{K}$. Por outro lado, $x \neq 0_{\mathbb{K}}$ é infinitesimal em $\mathbb{K}$ se, e somente se, $\frac{1}{x}$ é ilimitado em $\mathbb{K}$. Logo, $\mathbb{K}$ tem infinitésimos não-nulos se, e somente se, $\mathbb{K}$ tem elementos ilimitados (verifique)*. Portanto, corpos arquimedianos são precisamente aqueles nos quais *não* existem infinitésimos não-nulos (certo?)*, o que sugere a pergunta: há algum corpo ordenado não-arquimediano? Sim.

Proposição 0.9.10. *Se $\mathbb{D}$ é um* domínio ordenado[73]*, então seu corpo de frações $\mathbb{K} := \mathrm{Frac}(\mathbb{D})$ admite uma relação de ordem total $\sqsubseteq$, compatível com a ordem de $\mathbb{D}$ e que faz de $\mathbb{K}$ um corpo ordenado.*

Demonstração. Basta encarar o Exemplo 0.7.1 até que ele te encare de volta. □

Portanto, a fim de obter um corpo ordenado dotado de infinitésimos, basta encontrar um domínio ordenado $\mathbb{D}$ dotado de um elemento ilimitado x, pois daí seu inverso multiplicativo x^{-1} (no corpo de frações $\mathbb{K}$) será um infinitésimo não-trivial.

Exercício 0.104 ($\overset{\star\star}{\star\star}$)**.** Para um domínio ordenado $(\mathbb{D}, \preceq)$, considere o *anel de polinômios* na indeterminada x e coeficientes em $\mathbb{D}$, denotado por $\mathbb{D}[x]$.

a) Mostre que $\mathbb{D}[x]$ é um domínio legítimo. Dica: avalie o grau de um produto de polinômios.

b) Dados $p, q \in \mathbb{D}[x]$, declare $p \sqsubseteq q$ se, e somente se, $p = q$ ou o coeficiente líder de $q - p$ é (estritamente!) maior do que $0 \in \mathbb{D}$. Mostre que tal relação faz de $\mathbb{D}[x]$ um domínio ordenado em que x é ilimitado.

c) Conclua que $\mathbb{D}(x)$, o corpo de frações do domínio $\mathbb{D}[x]$, é um corpo ordenado que contém infinitésimos. ■

Análise "não-*standard*"

O Cálculo não nasceu em sua formulação atual. Originalmente, para definir a *derivada* de uma função "$f(x)$", por exemplo, considerava-se a expressão

$$\frac{f(x+\varepsilon) - f(x)}{\varepsilon},$$

com ε um infinitesimal não-nulo, a fim de obter daí sua *parte não-infinitesimal*. Por exemplo: com $f(x) := x^2$, tem-se

$$\frac{(x+\varepsilon)^2 - x^2}{\varepsilon} = \frac{x^2 + 2x\varepsilon + \varepsilon^2 - x^2}{\varepsilon} = 2x + \varepsilon,$$

donde segue que a derivada de $f(x)$ é $f'(x) = 2x$. A questão é: como justificar isso? Afinal de contas, num certo momento do cálculo, trata-se $\varepsilon \neq 0$ para, posteriormente, agir como se $\varepsilon = 0$. Na época, as definições não se embasavam em entidades abstratas como conjuntos, mas sim em noções geométrico-físicas, de modo que tal tratamento "artificial" causava certo incômodo. O tempo passou e, aos poucos, infinitésimos foram substituídos por limites e a reta geométrica tornou-se um corpo arquimediano completo.

No entanto, nos anos 60 do século passado, técnicas avançadas de Lógica-Matemática foram utilizadas na elaboração do que passou a ser conhecido como *Nonstandard Analysis*, ou *Análise não-padrão*, que permite não apenas formalizar e, em certa medida, justificar a metodologia original, como também sistematizar métodos para transferir resultados da Análise não-padrão para a Análise usual – e vice-versa. Para saber mais, o texto de Keisler [8] é um excelente ponto de partida.

[72] Na Wikipedia, você encontrará tais números xingados como "*infinitos*", mas tal terminologia não é adequada, por confundir noções de ordem e cardinalidade.

[73] Cuja definição é a mesma dos corpos ordenados, trocando-se o corpo $\mathbb{K}$ por um *domínio* $\mathbb{D}$: um anel $\mathbb{D}$ é chamado de **domínio** se $0_{\mathbb{D}} \neq 1_{\mathbb{D}}$ e $xy \neq 0_{\mathbb{D}}$ sempre que $x, y \in \mathbb{D} \setminus \{0_{\mathbb{D}}\}$.

0.10 Unicidade da reta real e sua cardinalidade

0.10.0 Essencial

A unicidade de corpos completos (a menos de isomorfismo)

Assim como o Axioma de Dedekind-Peano postulou a existência de $\mathbb{N}$, vamos postular a existência ~~da reta real~~ de um corpo ordenado completo.

Axioma da Preguiça Infinita. Existe um corpo ordenado completo.

O nome dado ao axioma acima explicita a sua motivação: preguiça. Enquanto, no caso de $\mathbb{N}$, precisa-se realmente postular sua existência[74], aqui, um corpo ordenado completo poderia ser efetivamente construído, mas o custo seria demasiado alto[75] em comparação aos benefícios: na prática, apenas transformaríamos o axioma acima num teorema e nunca mais voltaríamos a aproveitar a demonstração (neste texto).

Com isso dito, parece mais razoável dar atenção ao problema da *unicidade*: como já se mencionou anteriormente, a ideia é definir a reta real $\mathbb{R}$ como *um* corpo ordenado completo. Ora, admitindo-se que existe pelo menos um objeto dessa natureza, surge a pergunta: e se existir outro? Se duas construções distintas para corpos ordenados completos forem apresentadas, pode-se garantir que os corpos em questão são similares em algum sentido? Resposta: sim.

Observação 0.10.0. Para o que segue, convém revisar a noção de morfismo de anel na Subseção 0.6.1. △

Definição 0.10.1. Dados corpos ordenados $\mathbb{K}$ e $\mathbb{K}'$, diremos que uma função $f\colon \mathbb{K} \to \mathbb{K}'$ é um **morfismo de corpos ordenados** se f for simultaneamente um morfismo de corpos e uma função crescente[76]. Diz-se que f é um **isomorfismo** de corpos ordenados se existir um morfismo de corpos ordenados $g\colon \mathbb{K}' \to \mathbb{K}$ com $g \circ f = \mathrm{Id}_{\mathbb{K}}$ e $f \circ g = \mathrm{Id}_{\mathbb{K}'}$. Em tais condições, $\mathbb{K}$ e $\mathbb{K}'$ são ditos **isomorfos**. ¶

Exercício 0.105 ($\overset{\star}{\star}$)**.** Mostre que se $\mathbb{K}$ é corpo ordenado, então existe um único morfismo de corpos ordenados $f\colon \mathbb{Q} \to \mathbb{K}$. ■

A definição de isomorfismo dada acima é bem mais geral e se aplica, naturalmente, a qualquer contexto no qual uma noção *apropriada* de morfismo estiver disponível. Em certo sentido, enquanto *morfismos* são meios pelos quais *objetos* de um mesmo *tipo* ou *categoria* se *comunicam*, *isomorfismos* são meios que permitem não apenas a troca de informação, mas também a fidelidade nas traduções de um lado para outro. Há, porém, um modo bem mais prático de verificar isomorfismos *no presente contexto*.

Exercício 0.106 ($\overset{\star}{\star}$)**.** Sejam A e B anéis e $f\colon A \to B$ um morfismo de anéis.

a) Mostre que se f é bijetora, então f é um isomorfismo de anéis. Dica: a inversa (que existe!) deve satisfazer as condições para ser morfismo.

b) Mostre que se A e B são corpos ordenados e f é bijeção crescente, então f é um isomorfismo de corpos ordenados. Dica: pelo item anterior, f já é um isomorfismo de corpos, enquanto o Exercício 0.71 permite concluir que f^{-1} também é crescente. ■

[74] Grosso modo, postular a existência de $\mathbb{N}$ equivale a assumir que existe ao menos um conjunto infinito. Detalhes mais precisos fogem do escopo do texto.

[75] Mesmo assim, uma breve discussão é apresentada na Subseção 0.10.1.

[76] Como definido no Exercício 0.71.

Observação 0.10.2. Apesar do que se estabeleceu acima, há outros contextos (ou *categorias*) nos quais a mera bijetividade não é suficiente para atestar o isomorfismo entre os objetos considerados. Por exemplo: na *categoria* dos *espaços topológicos*, que conheceremos superficialmente em breve, *funções contínuas* fazem o papel de morfismos, e nem toda função contínua bijetiva tem inversa contínua. △

Moralmente, dizer que A e B são anéis ou corpos (ordenados) isomorfos significa afirmar que embora A e B possam ter definições distintas, os *comportamentos* que suas estruturas modelam são os mesmos. O próximo exercício pode dar uma ideia mais clara sobre tudo isso no contexto específico dos corpos ordenados.

Exercício 0.107 ($\star$)**.** Sejam $\mathbb{K}$ e $\mathbb{K}'$ corpos ordenados e $f\colon \mathbb{K} \to \mathbb{K}'$ um isomorfismo de corpos ordenados.

a) Mostre que $S \subseteq \mathbb{K}$ é limitado superiormente se, e somente se, $f[S] \subseteq \mathbb{K}'$ é limitado superiormente.

b) Mostre que $S \subseteq \mathbb{K}$ admite um supremo $\alpha \in \mathbb{K}$ se, e somente se, $f[S]$ admite supremo $\beta \in \mathbb{K}'$. Além disso, tem-se $\beta = f(\alpha)$.

c) Mostre que a equação $x^2 - 2_{\mathbb{K}} = 0_{\mathbb{K}}$ tem solução em $\mathbb{K}$ se, e somente se, a equação $x^2 - 2_{\mathbb{K}'} = 0_{\mathbb{K}'}$ tem solução em $\mathbb{K}'$. ■

Pelo que se expôs acima, um modo legítimo de resolver o problema da "unicidade" seria mostrar que quaisquer dois corpos ordenados completos são isomorfos. É precisamente isso o que será feito a seguir.

Lema 0.10.3. *Sejam $\mathbb{A}$ e $\mathbb{K}$ corpos ordenados e, para cada $a \in \mathbb{A}$, considere o subconjunto $\mathbb{Q}_{\mathbb{K},a} \coloneqq \{q_{\mathbb{K}} \in \mathbb{Q}_{\mathbb{K}} : q_{\mathbb{A}} < a\}$. Se $\mathbb{A}$ é arquimediano e $\mathbb{K}$ é completo, então a correspondência*

$$\begin{aligned} \rho\colon \mathbb{A} &\to \mathbb{K} \\ a &\mapsto \sup \mathbb{Q}_{\mathbb{K},a} \end{aligned} \tag{0.3}$$

é um morfismo de corpos ordenados.

É mais fácil entender a prova do que escrevê-la. A coisa toda é bastante visual, como ilustrado a seguir.

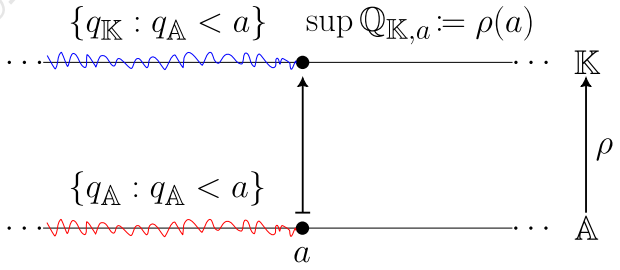


Figura 0.12: Sincronização de corpos.

Para cada $a \in \mathbb{A}$ considera-se, num primeiro momento, a coleção dos racionais (interpretados em $\mathbb{A}$) menores do que a. Ao *interpretar* tais números racionais em $\mathbb{K}$, obtém-se um conjunto limitado superiormente, que por sua vez admite um supremo em virtude da completude de $\mathbb{K}$. Finalmente, ρ apenas associa a ao supremo obtido no passo anterior. Mesmo que $\mathbb{A}$ e $\mathbb{K}$ sejam *construídos* de maneiras distintas, o fato de ambos *interpretarem* cópias *densas* de $\mathbb{Q}$ permite sincronizá-los entre si.

Demonstração. É edificante observar, antes de qualquer outra coisa, que a *relação* ρ é, na verdade, uma função:

- ✓ a propriedade arquimediana de $\mathbb{A}$ permite mostrar tanto que $\mathbb{Q}_{\mathbb{K},a} \neq \emptyset$ quanto a existência de um limitante superior em $\mathbb{K}$;
- ✓ logo, a completude de $\mathbb{K}$ assegura a existência de um único $\rho(a) \in \mathbb{K}$ digno de ser xingado como $\sup \mathbb{Q}_{\mathbb{K},a}$.

Em outras palavras: ρ associa a cada $a \in \mathbb{A}$ um único $\rho(a) \in \mathbb{K}$, como esperado. Você pode cuidar dos detalhes omitidos acima[77]. Agora, mostraremos que ρ é um morfismo de corpos. Para isso, para quaisquer $a, b \in \mathbb{A}$, precisa-se verificar que

$$\sup \mathbb{Q}_{\mathbb{K},1_{\mathbb{A}}} = 1_{\mathbb{K}}, \tag{0.4}$$
$$\sup \mathbb{Q}_{\mathbb{K},a+b} = \sup \mathbb{Q}_{\mathbb{K},a} + \sup \mathbb{Q}_{\mathbb{K},b} \tag{0.5}$$
$$\sup \mathbb{Q}_{\mathbb{K},ab} = \sup \mathbb{Q}_{\mathbb{K},a} \cdot \sup \mathbb{Q}_{\mathbb{K},b}. \tag{0.6}$$

Identidade (0.4). Ela vale mais geralmente, pois $\sup \mathbb{Q}_{\mathbb{K},q_{\mathbb{A}}} = q_{\mathbb{K}}$ para todo $q \in \mathbb{Q}$. Com efeito, $q_{\mathbb{K}}$ limita $\mathbb{Q}_{\mathbb{K},q_{\mathbb{A}}}$ superiormente e, se $\beta < q_{\mathbb{K}}$, então existe $r \in \mathbb{Q}$ com $r_{\mathbb{A}} < q_{\mathbb{A}}$ e $\beta < r_{\mathbb{K}}$, mostrando que $q_{\mathbb{K}}$ é, legitimamente, o menor limitante superior de $\mathbb{Q}_{\mathbb{K},q_{\mathbb{A}}}$.

Identidade (0.5). Tendo em vista o Teorema 0.8.7, basta mostrar que $\mathbb{Q}_{\mathbb{K},a+b} = \mathbb{Q}_{\mathbb{K},a} + \mathbb{Q}_{\mathbb{K},b}$, cuja verificação será apresentada a seguir.

Por um lado, se $q := r + s$ com $r_{\mathbb{A}} < a$ e $s_{\mathbb{A}} < b$, então $r_{\mathbb{A}} + s_{\mathbb{A}} < a + b$, acarretando $q_{\mathbb{K}} \in \mathbb{Q}_{\mathbb{K},a+b}$, donde a arbitrariedade de q implica em $\mathbb{Q}_{\mathbb{K},a} + \mathbb{Q}_{\mathbb{K},b} \subseteq \mathbb{Q}_{\mathbb{K},a+b}$. Por outro lado, se $q_{\mathbb{A}} < a+b$, então $0_{\mathbb{A}} < a+b-q_{\mathbb{A}}$ e, pela condição arquimediana satisfeita por $\mathbb{A}$, existem $r, s \in \mathbb{Q}$ com $0_{\mathbb{A}} < r_{\mathbb{A}} < a + b - q_{\mathbb{A}}$ e $a - r_{\mathbb{A}} < s_{\mathbb{A}} < a$. Logo, $q_{\mathbb{A}} - s_{\mathbb{A}} < q_{\mathbb{A}} + r_{\mathbb{A}} - a < b$, com $q_{\mathbb{A}} - s_{\mathbb{A}} \in \mathbb{Q}_{\mathbb{K},b}$, $s_{\mathbb{A}} \in \mathbb{Q}_{\mathbb{K},a}$, mostrando $q_{\mathbb{A}} = s_{\mathbb{A}} + q_{\mathbb{A}} - s_{\mathbb{A}} \in \mathbb{Q}_{\mathbb{K},a} + \mathbb{Q}_{\mathbb{K},b}$.

Identidade (0.6). A verificação das possíveis variações de *sinal* se reduz ao caso em que $a, b > 0_{\mathbb{A}}$, desde que se saiba da identidade auxiliar $\rho(-a) = -\rho(a)$. De fato, em posse disso, para $a < 0_{\mathbb{A}}$ e $b > 0_{\mathbb{A}}$, por exemplo, resulta

$$-\rho(ab) = \rho(-ab) = \rho((-a)b) = \rho(-a)\rho(b) = -\rho(a)\rho(b),$$

com um raciocínio análogo para o caso em que $a < 0_{\mathbb{A}}$ e $b < 0_{\mathbb{A}}$ (o caso em que $a = 0_{\mathbb{A}}$ ou $b = 0_{\mathbb{A}}$ é, em vista de (0.4), imediato). Tratemos então das identidades *suficientes*.

- ✓ Observe que se $x > 0_{\mathbb{A}}$, então o conjunto $D_x := \{q_{\mathbb{K}} \in \mathbb{Q}_{\mathbb{K},x} : q > 0_{\mathbb{A}}\}$ é tal que $\sup \mathbb{Q}_{\mathbb{K},x} = \sup D_x$ (certo?)*. Daí, observando que $D_{ab} = D_a \cdot D_b$ (verifique!)*, a identidade $\rho(ab) = \rho(a)\rho(b)$ para $a, b > 0_{\mathbb{A}}$ segue do Teorema 0.8.7.
- ✓ Para a identidade auxiliar $\rho(-a) = -\rho(a)$, note que não há perda de generalidade em supor $a \notin \mathbb{Q}_{\mathbb{A}}$ (por (0.4)). Daí, note que se $q_{\mathbb{A}} < a$, então $-a < -q_{\mathbb{A}}$, donde a definição de supremo acarreta $\sup \mathbb{Q}_{\mathbb{K},-a} \leq -q_{\mathbb{K}}$. Logo, $q_{\mathbb{K}} \leq -\sup \mathbb{Q}_{\mathbb{K},-a}$ e, novamente pela definição, $\sup \mathbb{Q}_{\mathbb{K},a} \leq -\sup \mathbb{Q}_{\mathbb{K},-a}$. Se a desigualdade fosse estrita, a condição arquimediana garantiria um $p \in \mathbb{Q}$ com $\sup \mathbb{Q}_{\mathbb{K},a} < p_{\mathbb{K}} < -\sup \mathbb{Q}_{\mathbb{K},-a}$, com $a > p_{\mathbb{A}}$ e, consequentemente, $-p_{\mathbb{A}} < -a$, o que implicaria em $-p_{\mathbb{K}} \leq \sup \mathbb{Q}_{\mathbb{K},-a}$, i.e., $-\sup \mathbb{Q}_{\mathbb{K},-a} \leq p_{\mathbb{K}}$, uma contradição. Portanto, $\sup \mathbb{Q}_{\mathbb{K},a} = -\sup \mathbb{Q}_{\mathbb{K},-a}$, como desejado.

[77] Será essencial lembrar que as correspondências $q \mapsto q_{\mathbb{A}}$ e $q \mapsto q_{\mathbb{K}}$ definem (únicos) morfismos de corpos da forma $\mathbb{Q} \to \mathbb{A}$ e $\mathbb{Q} \to \mathbb{K}$, respectivamente.

A enfadonha discussão acima mostra que ρ é um morfismo de corpos. Resta a ordem: se $a \leq b$ em $\mathbb{A}$, então $\mathbb{Q}_{\mathbb{K},a} \subseteq \mathbb{Q}_{\mathbb{K},b}$ e, novamente pelo Teorema 0.8.7, segue que $\rho(a) \leq \rho(b)$. □

Exercício 0.108 ($^\star_\star$)**.** Complete os detalhes da demonstração acima. ■

Observação 0.10.4. Convém destacar que o morfismo de corpos ρ é *estritamente crescente*, no sentido da Observação 0.5.4. Há dois modos simples de se convencer disso:

(i) por $\mathbb{A}$ ser arquimediano, existe $q \in \mathbb{Q}$ com $a < q_{\mathbb{A}} < b$ e

$$\rho(a) := \sup \mathbb{Q}_{\mathbb{K},a} < q_{\mathbb{K}} < \sup \mathbb{Q}_{\mathbb{K},b} := \rho(b);$$

(ii) alternativamente, como ρ é um morfismo de corpos, segue que ρ é injetor (item b) do Exercício 0.82). Logo, ρ deve ser estritamente crescente.

Embora o segundo argumento mostre que *qualquer* morfismo de corpos ordenados é estritamente crescente, o primeiro argumento será importante em breve, quando surgir o problema de estimar a cardinalidade de corpos arquimedianos. △

Teorema 0.10.5. *Se $\mathbb{A}$ e $\mathbb{K}$ são corpos ordenados e completos, então o mapa $\rho\colon \mathbb{A} \to \mathbb{K}$ definido em (0.3) é um isomorfismo de corpos ordenados.*

Demonstração. Desta vez o corpo $\mathbb{A}$ também é completo. Logo, o lema anterior permite conjurar *dois* morfismos de corpos ordenados, simultaneamente:

$$\begin{aligned} \rho\colon \mathbb{A} &\to \mathbb{K} \\ a &\mapsto \sup \mathbb{Q}_{\mathbb{K},a} \end{aligned} \qquad \text{e} \qquad \begin{aligned} \sigma\colon \mathbb{K} &\to \mathbb{A} \\ k &\mapsto \sup \mathbb{Q}_{\mathbb{A},k} \end{aligned}$$

Portanto, basta mostrar que um é o inverso do outro. Fixado $a \in \mathbb{A}$, tem-se

$$\sigma(\rho(a)) := \sup \mathbb{Q}_{\mathbb{A},\rho(a)},$$

e busca-se verificar $\sigma(\rho(a)) = a$. Ora, dado $q_{\mathbb{A}} \in \mathbb{Q}_{\mathbb{A},\rho(a)}$, tem-se $q_{\mathbb{K}} < \rho(a)$, e isso proíbe a ocorrência de $a \leq q_{\mathbb{A}}$: caso contrário, teria-se $\rho(a) \leq \rho(q_{\mathbb{A}}) = q_{\mathbb{K}}$. Agora, se $\beta \in \mathbb{A}$ é tal que $\beta < a$, então $\rho(\beta) < \rho(a)$, e existe $q \in \mathbb{Q}$ com $\rho(\beta) < q_{\mathbb{K}} < \rho(a)$, donde segue que $q_{\mathbb{A}} \in \mathbb{Q}_{\mathbb{A},\rho(a)}$ com $\beta < q_{\mathbb{A}}$. Portanto, a é o menor limitante superior de $\mathbb{Q}_{\mathbb{A},\rho(a)}$, i.e., $a = \sigma(\rho(a))$, como queríamos. Analogamente, mostra-se que $\rho(\sigma(k)) = k$ para todo $k \in \mathbb{K}$. □

Exercício 0.109 ($^\star_{\star\star}$)**.** Sejam $\mathbb{A}$ e $\mathbb{K}$ corpos ordenados, com $\mathbb{A}$ arquimediano e $\mathbb{K}$ completo.

a) Mostre que se $\varphi\colon \mathbb{A} \to \mathbb{K}$ é um morfismo de corpos ordenados, então $\varphi(q_{\mathbb{A}}) = q_{\mathbb{K}}$ para todo $q \in \mathbb{Q}$. Dica: as correspondências $q \mapsto q_{\mathbb{A}}$ e $q \mapsto q_{\mathbb{K}}$ determinam os únicos morfismos de corpos ordenados da forma $\mathbb{Q} \to \mathbb{A}$ e $\mathbb{Q} \to \mathbb{K}$, respectivamente; por outro lado, a composição entre $q \mapsto q_{\mathbb{A}}$ e φ também determina um morfismo da forma $\mathbb{Q} \to \mathbb{K}$.

b) Conclua que existe um único morfismo de corpos ordenados da forma $\mathbb{A} \to \mathbb{K}$. Em particular, os isomorfismos do teorema anterior são únicos. ■

As discussões acima resolvem o problema da "unicidade" mencionado anteriormente, e tornam quase honesta a próxima

Definição 0.10.6. Denota-se por $\mathbb{R}$ *qualquer* corpo ordenado e completo, que passa a ser chamado de **conjunto dos números reais**, ou apenas de **reta real**. ¶

Devido a tal escolha de notação, perde o sentido carregar "$\mathbb{R}$" como subíndice para indicar em qual corpo ordenado e completo um determinado procedimento ocorre, postura que será aplicada também para o valor absoluto de um número real x, que será denotado por $|x|$ de agora em diante[78].

Além disso, em contextos algébricos ou *analíticos*, será inofensivo considerar como verdadeiras as inclusões próprias $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$ embora, a rigor, existam apenas morfismos injetores que preservam as *estruturas algébricas e de ordem* subjacentes. Se, por um lado, isso soa demasiado arbitrário, por outro, a unicidade assegura que não haveria outra forma de *enxergar* um dentro do outro. É por isso que, na prática, tanto $\mathbb{N}$, quanto $\mathbb{Z}$ e $\mathbb{Q}$ são *substituídos* por suas cópias em $\mathbb{R}$.

A cardinalidade da reta real

Um dos fatos mais marcantes nos desenvolvimentos iniciais da Teoria dos Conjuntos e no estudo de coleções infinitas foi a *constatação* de que o *tipo de infinito* de $\mathbb{R}$ é *estritamente maior* do que o *tipo de infinito* de $\mathbb{N}$, i.e., $\mathbb{N} \prec \mathbb{R}$ ou $|\mathbb{N}| < |\mathbb{R}|$. Explicitamente, isto significa que existe função injetora $\mathbb{N} \to \mathbb{R}$ mas não existe função bijetora entre $\mathbb{N}$ e $\mathbb{R}$. Com o jargão típico dos textos básicos de Análise, isto se reduz a dizer que "$\mathbb{R}$ é não-enumerável".

A primeira parte é fácil: como $\mathbb{N}$ *é subconjunto* de $\mathbb{R}$, a inclusão $i\colon \mathbb{N} \to \mathbb{R}$ determina uma função automaticamente injetora. A parte não-trivial é mostrar que não pode existir função injetora $\mathbb{R} \to \mathbb{N}$ ou, equivalentemente (cf. Teorema 0.4.10), não existe função sobrejetora $\mathbb{N} \to \mathbb{R}$.

Há várias formas de demonstrar a não-enumerabilidade de $\mathbb{R}$. Um argumento bastante comum (conhecido como "diagonalização de Cantor") consiste em tomar *qualquer* função $\varphi\colon \mathbb{N} \to \mathbb{R}$ e definir um número $r := r_0, r_1 r_2 r_3 \ldots$ exigindo-se apenas que o número $r_n \in \{0, \ldots, 9\} \setminus \{a_{n,n}, 1, 9\}$ para todo $n \in \mathbb{N}$, onde

$$\varphi(n) := a_{n,0}, a_{n,1} a_{n,2} \ldots a_{n,n} \ldots$$

indica a expansão de $\varphi(n)$ em *base* 10. Como $r \notin \operatorname{im}(\varphi)$, segue que φ não pode ser sobrejetora.

Evidentemente, tal argumento depende de um estudo um pouco mais cuidadoso de *séries* e *representações* decimais, o que atrasaria a *formalização* do resultado no texto. Uma alternativa popular por aqui [9, 10], por exemplo, é apelar para a *compacidade* dos *intervalos fechados e limitados* de $\mathbb{R}$, disfarçada como a *propriedade dos intervalos encaixantes*. Porém, vejo como problemático se valer de propriedades *topológicas* da reta real sem avisar do que se trata, apenas para apresentar um argumento com gosto geométrico.

Aqui, a abordagem adotada será outra: mostraremos que $\mathbb{R}$ está em bijeção com $\wp(\mathbb{N})$, o conjunto das partes de $\mathbb{N}$. Daí, a não-enumerabilidade de $\mathbb{R}$ seguirá do Teorema de Cantor (cf. Teorema 0.4.6): como não existe sobrejeção $\mathbb{N} \to \wp(\mathbb{N})$, tampouco pode existir sobrejeção $\mathbb{N} \to \mathbb{R}$, já que $\wp(\mathbb{N}) \approx \mathbb{R}$. Como brinde pela transgressão imperdoável de não seguir o Elon, *ganharemos* a existência de bijeção entre $\mathbb{R}$ e $\mathbb{R}^n$ para qualquer $n \in \mathbb{N} \setminus \{0\}$ (cf. Subseção 0.10.1).

Exercício 0.110 ($\star_\star$)**.** Convença-se de que $|\wp(\mathbb{Q})| = |\wp(\mathbb{N})|$. Dica: Exercício 0.57 + $|\mathbb{N}| = |\mathbb{Q}|$.■

[78] O contexto deixará claro quando "$|x|$" representa o valor absoluto do *número real* x ou a cardinalidade do *conjunto* x. Pelo menos neste texto, conjuntos não são denotados por letras minúsculas, o que pode ajudar a acalmar os ânimos

Lema 0.10.7. *Se $\mathbb{A}$ é corpo arquimediano, então $|\mathbb{A}| \leq |\wp(\mathbb{N})|$, i.e., existe função injetora $\mathbb{A} \to \wp(\mathbb{N})$.*

Demonstração. A correspondência

$$\begin{aligned} \partial\colon \mathbb{A} &\to \wp(\mathbb{Q}) \\ a &\mapsto \{q \in \mathbb{Q} : q_{\mathbb{A}} < a\} \end{aligned}$$

é uma injeção: se $a, b \in \mathbb{A}$ são distintos, então ocorre $a < b$ ou $b < a$, donde a condição arquimediana assegura a existência de $q \in \mathbb{Q}$ *entre* a e b, acarretando em $\partial(a) \neq \partial(b)$. Portanto, existe função injetora $\mathbb{A} \to \wp(\mathbb{Q})$ e, pelo exercício anterior, existe injeção $\mathbb{A} \to \wp(\mathbb{N})$, como desejado. □

Como $\mathbb{R}$ é arquimediano (por ser completo), segue que $|\mathbb{R}| \leq |\wp(\mathbb{N})|$. O próximo passo é mostrar a desigualdade oposta, i.e., pois daí o Teorema 0.1.10 (Cantor-Bernstein) garantirá $|\mathbb{R}| = |\wp(\mathbb{N})|$. Embora este lado da desigualdade possa ser demonstrado de modo mais rápido por meio de *séries*, é possível maquiar os argumentos por meio de supremos de ~~séries~~ *somas* finitas. A seguir, assume-se que você tenha familiaridade com a notação de somatório ($\sum$). Se não for o caso, confira a Subseção 0.10.1.

Lema 0.10.8. *Se $0 < a < 1$, então $\sup\left\{\sum_{n\leq m} a^n : m \in \mathbb{N}\right\} = \frac{1}{1-a}$.*

Demonstração. Por indução, tem-se $a^{n+1} < a^n$ para todo $n \in \mathbb{N}$: $a < a^0 := 1$ e, supondo $a^{n+1} < a^n$, tem-se

$$a^{n+2} = a \cdot a^{n+1} < a \cdot a^n = a^{n+1}.$$

Por sua vez, tem-se

$$\sum_{n\leq m} a^n := \sum_{n=0}^{m} a^n = \frac{1 - a^{m+1}}{1 - a}$$

para qualquer $m \in \mathbb{N}$ (verifique!)*. Logo, pela primeira parte, $S := \{\sum_{n\leq m} a^n : m \in \mathbb{N}\}$ é limitado superiormente por $\frac{1}{1-a}$ (por quê?!)*, donde a completude de $\mathbb{R}$ garante que existe $s \in \mathbb{R}$ com $s = \sup S$. Para finalizar, o Teorema 0.8.7 se aplica e permite fazer

$$as = a\sup S = \underbrace{\sup\{ay : y \in S\} = \sup\{y - 1 : y \in S\}}_{\text{(por quê?!)}^\star} = \sup S - 1 = s - 1,$$

acarretando $S := \frac{1}{1-a}$. □

Exercício 0.111 ($\star$)**.** Mostre que $\sup\left\{\sum_{n\leq m} \frac{1}{10^n} : m \in \mathbb{N}\right\} = \frac{10}{9}$. ■

Lema 0.10.9. *Para cada $f\colon \mathbb{N} \to \{0, 1\}$, existe o número real $\psi(f) \in \mathbb{R}$ dado por*

$$\psi(f) := \sup\left\{\sum_{n\leq m} \frac{f(n)}{10^n} : m \in \mathbb{N}\right\}.$$

Além disso, ao denotar por $\{0, 1\}^{\mathbb{N}}$ o conjunto das funções da forma $\mathbb{N} \to \{0, 1\}$, a correspondência $\psi\colon \{0, 1\}^{\mathbb{N}} \to \mathbb{R}$ é injetora.

Demonstração. Fixada $f \in \{0,1\}^{\mathbb{N}}$, a ideia é usar a completude de $\mathbb{R}$ para garantir a existência de $\psi(f)$. Para tanto, é suficiente mostrar que o conjunto

$$S(f) := \left\{ \sum_{n \leq m} \frac{f(n)}{10^n} : m \in \mathbb{N} \right\}$$

é não-vazio e limitado superiormente: obviamente, tem-se $S(f) \neq \emptyset$; para verificar a limitação, observe que $0 \leq f(n) \leq 1$ para todo $n \in \mathbb{N}$, donde segue que

$$\frac{1}{10^n} f(n) \leq \frac{1}{10^n} \Rightarrow \sum_{n \leq m} \frac{f(n)}{10^n} \leq \sum_{n \leq m} \frac{1}{10^n} \leq \frac{10}{9},$$

para qualquer $m \in \mathbb{N}$.

Isso mostrou que $S(f) \neq \emptyset$ é limitado superiormente para cada $f \in \{0,1\}^{\mathbb{N}}$. Consequentemente, a correspondência $\psi \colon \{0,1\}^{\mathbb{N}} \to \mathbb{R}$ está bem definida, pois o supremo de $S(f)$ é único para cada $f \in \{0,1\}^{\mathbb{N}}$. Resta apenas verificar a injetividade de ψ.

Para $p \in \mathbb{N}$ e $f \in \{0,1\}^{\mathbb{N}}$ fixados, mostraremos que

$$\psi_p(f) := \sup \left\{ \sum_{n \leq m} \frac{f(n+p)}{10^{n+p}} : m \in \mathbb{N} \right\} \leq \frac{1}{9 \cdot 10^{p-1}}. \tag{0.7}$$

De fato, já que $f(j) \leq 1$ para todo $j \in \mathbb{N}$, pode-se fazer

$$\sum_{n \leq m} \frac{f(n+p)}{10^{n+p}} = \frac{1}{10^p} \sum_{n \leq m} \frac{f(n+p)}{10^n} \leq \frac{1}{10^p} \sum_{n \leq m} \frac{1}{10^n} \leq \frac{1}{10^p} \cdot \frac{10}{9} = \frac{1}{9 \cdot 10^{p-1}},$$

donde a desigualdade (0.7) segue.

O último ingrediente da prova consiste em observar que

$$\psi(f) = \sum_{n \leq m} \frac{f(n)}{10^n} + \psi_{m+1}(f) \tag{0.8}$$

para qualquer $m \in \mathbb{N}$, o que segue do Teorema 0.8.7 (por quê?)*.

Enfim, para $g \in \{0,1\}^{\mathbb{N}}$ com $f \neq g$, existe $m := \min\{j \in \mathbb{N} : f(j) \neq g(j)\}$ e, por falta de opções, não há perda de generalidade em supor $f(m) = 0$ e $g(m) = 1$. Segue então de (0.8), bem como da minimalidade de m, que existe $r \in \mathbb{R}$ tal que

$$\psi(f) = r + \psi_{m+1}(f) \text{ e } \psi(g) = r + \frac{1}{10^m} + \psi_{m+1}(g).$$

Por (0.7), finalmente, obtém-se

$$\begin{aligned} \psi(g) - \psi(f) = \frac{1}{10^m} + \psi_{m+1}(g) - \psi_{m+1}(f) \geq \frac{1}{10^m} + 0 - \psi_{m+1}(f) \geq \\ \geq \frac{1}{10^m} - \frac{1}{9 \cdot 10^m} = \frac{8}{9 \cdot 10^m} > 0, \end{aligned}$$

mostrando que $\psi(f) \neq \psi(g)$. □

Secretamente, a prova acima consiste apenas em tomar sequências infinitas de 0's e 1's e interpretá-las como números reais por meio da expansão decimal. Assim, a sequência constante $(1, \dots, 1, \dots)$, por exemplo, se torna o número real que, na rua[79], xingaríamos de $1,1111\dots$

Corolário 0.10.10. $\mathbb{R}$ *é não-enumerável.*

Demonstração. Pelo Exercício 0.56 temos $|\wp(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}|$. Logo, mostrou-se que $|\wp(\mathbb{N})| \leq |\mathbb{R}|$. Como já tínhamos $|\mathbb{R}| \leq |\wp(\mathbb{N})|$, a igualdade $|\mathbb{R}| = |\wp(\mathbb{N})|$ segue em virtude do Teorema de Cantor-Bernstein. Por fim, como $\wp(\mathbb{N})$ é não-enumerável pelo Teorema 0.4.6 (de Cantor), o resultado segue. □

Exercício 0.112 $(\overset{\star}{\star\star})$**.** Diz-se que $r \in \mathbb{R}$ é **transcendente** se não existe polinômio $p \in \mathbb{Q}[x]$ com $p(r) = 0$. Mostre que o conjunto dos números transcendentes é não-enumerável. Em particular, conclua que $\mathbb{R} \setminus \mathbb{Q}$, o conjunto dos **números irracionais**, é não-enumerável. ■

0.10.1 Extras

Somatórios e produtórios

A seguir, $\operatorname{seq}(\mathbb{R})$ denota a coleção das **sequências finitas** de números reais, i.e., $s \in \operatorname{seq}(\mathbb{R})$ se, e somente se, s é uma função da forma $\mathbb{N}_{<n} \to \mathbb{R}$ para algum $n \in \mathbb{N}$. Em particular, note que $\emptyset \in \operatorname{seq}(\mathbb{R})$. Para facilitar as notações, vamos escrever $(f_i : i \leq n)$ para indicar a sequência finita $f \colon \mathbb{N}_{n+1} \to \mathbb{R}$ que a cada $i \leq n$ associa f_i, enquanto $(g_i : i < n)$ indica uma função real g cujo domínio é $\mathbb{N}_{<n}$.

Definição 0.10.11 (Operadores Σ e Π)**.** Definem-se $\sum \colon \operatorname{seq}(\mathbb{R}) \to \mathbb{R}$ e $\prod \colon \operatorname{seq}(\mathbb{R}) \to \mathbb{R}$ da seguinte forma:

(i) $\sum \emptyset := 0$ e $\prod \emptyset := 1$;

(ii) $\sum (f_i : i \leq n) := f_n + \sum (f_i : i < n)$ e $\prod (f_i : i \leq n) := f_n \cdot \prod (f_i : i < n)$ para cada $n \in \mathbb{N}$ e $f := (f_i : i \leq n) \in \mathbb{R}^{n+1}$. ¶

É comum que o primeiro contato com as *definições* acima cause desconforto. Porém, a coisa é bastante simples, e consiste tão somente de um algoritmo de repetição. No caso de Σ, por exemplo, para se $x_n \in \mathbb{R}$ para todo $n \in \mathbb{N}$, tem-se

$$\begin{aligned} \sum \emptyset &:= 0; \\ \sum (x_0) &:= \sum \emptyset + x_0 = 0 + x_0; \\ \sum (x_0, x_1) &:= \sum (x_0) + x_1 = x_0 + x_1; \\ \sum (x_0, x_1, x_2) &:= \sum (x_0, x_1) + x_2 = (x_0 + x_1) + x_2; \\ \sum (x_0, x_1, x_2, x_3) &:= \dots \end{aligned}$$

Intuitivamente, $\sum (x_i : i \leq n)$ expressa aquilo que se escreveria como $x_0 + x_1 + \ldots + x_n$. Isto sugere notações bem mais práticas e *maleáveis* do que as anteriores.

Definição 0.10.12. Sejam $n \in \mathbb{N}$ e $f := (f_i : i \leq n) \in \mathbb{R}^{n+1}$.

(i) Tanto $\displaystyle\sum_{i \leq n} f_i$ quanto $\displaystyle\sum_{i=0}^{n} f_i$ serão usados para denotar $\sum (f_i : i \leq n)$.

(ii) Tanto $\displaystyle\prod_{i \leq n} f_i$ quanto $\displaystyle\prod_{i=0}^{n} f_i$ serão usados para denotar $\prod (f_i : i \leq n)$. ¶

A partir dessas definições, é relativamente simples adaptá-las a fim de dar sentido formal a variações típicas de *somatórios* e *produtórios*, como os listados a seguir:

[79] Talvez você se surpreenda ao efetuar o cálculo "$10 \div 9$", em sua calculadora, por exemplo.

(i) $\sum_{i=j}^{m} f_i$; (ii) $\prod_{i<m} a_i \sum_{j=0}^{n} b_j$; (iii) $\sum_{i=0}^{m} \sum_{j+k=i} a_j b_k c_i$

(iv) $\prod_{x\in X} h(x)$ para um conjunto finito X e uma função $h\colon X \to \mathbb{R}$;

(v) $\sum F$ para um subconjunto finito $F \subseteq \mathbb{R}$;

(vi) ...

Você provavelmente já tem familiaridade com esse tipo de notação e sabe como operá-las no dia a dia. Ainda assim, quando alguma propriedade for usada sem maiores explicações, fica o convite para que você a demonstre – são bons exercícios de indução.

Construções da reta real

Tipicamente, ao encontrar algum tipo de objeto matemático *incompleto* num sentido específico, a coleção das testemunhas da incompleteza/incompletude esconde um modo para completar o que faltava. Foi assim com $\mathbb{Z}$ e com $\mathbb{Q}$. Também é assim com $\mathbb{R}$. Há três modos clássicos para construir um corpo ordenado completo.

- ✓ *Cortes de Dedekind.* Considera-se a família

$$\mathcal{C} \coloneqq \{(A,B) \in \wp(\mathbb{Q}) \times \wp(\mathbb{Q}) : (A,B) \text{ é corte de } \mathbb{Q} \text{ e } A \text{ não tem máximo}\},$$

  conjunto que é munido de uma estrutura de corpo ordenado completo. A vantagem desta construção está na completude: como a ordem de $\mathcal{C}$ é, essencialmente, a inclusão, supremos se manifestam como reuniões de maneira quase automática. No entanto, a parte algébrica é terrível.

- ✓ *Sequências de Cauchy racionais.* Considera-se a família

$$\mathcal{S} \coloneqq \{(q_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} : (q_n)_{n\in\mathbb{N}} \text{ é de Cauchy}\},$$

  onde "ser de Cauchy" significa, *grosso modo*, que os termos da sequência se tornam arbitrariamente próximos uns dos outros. Daí, com uma relação de equivalência $\sim$ apropriada sobre $\mathcal{S}$, definem-se sobre o quociente $\mathcal{S}/\!\sim$ operações de adição e multiplicação, bem como uma ordem, que fazem de $\mathcal{S}/\!\sim$ um corpo ordenado completo.

- ✓ *Completamento uniforme.* Apela-se para a *teoria de espaços uniformes* e seus teoremas de *completamento*, que englobam tipos de estruturas chamadas de *grupos topológicos*, reino em que habita o grupo aditivo $(\mathbb{Q}; +; 0)$. Em tal cenário, mostra-se que o completamento uniforme de $\mathbb{Q}$ pode ser promovido ao patamar de corpo ordenado (completo).

Tecnicamente, o primeiro método é o menos exigente do ponto de vista terminológico: já teríamos bagagem suficiente para realizar a construção, se não tivéssemos mais o que fazer. Todavia, os meandros envolvidos nessa *implementação* não costumam contribuir para a prática da Análise no dia a dia. Nesse sentido, o segundo método tem a vantagem de utilizar *ecos* de definições que serão importantes *após* a construção, como as *sequências de Cauchy*. Mesmo assim, as enfadonhas verificações de que as *estruturas* definidas satisfazem as condições desejadas só servem para o contexto da construção da reta: no futuro, quando você *precisar* de *espaços métricos completos*, tudo deverá ser refeito.

O terceiro método não tem essa desvantagem: um único teorema de *completamento* de *espaços uniformes* dá conta de *completar* tanto $\mathbb{Q}$ quanto *espaços métricos* e outras *estruturas uniformes* encontradas na *natureza*. Porém, dado o escopo do texto, desenvolver esse ferramental *apenas* para construir um corpo ordenado completo e, posteriormente, *fazer* Análise, seria descabido[80].

[80] É a postura tomada por Bourbaki [1, 2], por exemplo. Porém, cabe a ressalva de que os textos de Bourbaki nunca almejaram servir como propostas didáticas, mas sim como fundamentação teórico-formal. Se quiser uma releitura em português, confira [12].

Outras bijeções curiosas

Observação 0.10.13. Você provavelmente já sabe, mas não custa lembrar: para um conjunto X e um número $n \in \mathbb{N}$ fixado, pode-se definir $X^n := X^{\mathbb{N}_{<n}}$, i.e., a coleção de todas as funções da forma $(x_i : i < n)$. Alternativamente, poderíamos definir $X^0 := \{\emptyset\}$, $X^1 := X$, $X^2 := X \times X$ e, mais geralmente, $X^{n+1} := X^n \times X$, o que essencialmente consiste em formalizar n-uplas como se fossem pares ordenados tomados iteradamente: assim, uma tripla (x_0, x_1, x_2) seria, formalmente, $((x_0, x_1), x_2)$. △

Entre outras coisas, o Exercício 0.58, que você provavelmente já fez, assegura que se existem funções injetoras $A \to C$ e $B \to D$, então existe uma função injetora $A^B \to C^D$, i.e., há uma correspondência injetiva que associa a cada função do tipo $B \to A$ outra função do tipo $C \to D$. Consequentemente:

$$|\mathbb{R}| = \left|\{0,1\}^{\mathbb{N}}\right| \leq \left|\mathbb{N}^{\mathbb{N}}\right| \leq \left|\left(\{0,1\}^{\mathbb{N}}\right)^{\mathbb{N}}\right|,$$

onde a primeira desigualdade segue pois existe função injetora $\{0,1\} \to \mathbb{N}$, enquanto a segunda decorre da existência de função injetora $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Mas você também fez o Exercício 0.60 e, por isso, sabe que existe bijeção entre as funções da forma $Y \times Z \to X$ e as funções da forma $Z \to X^Y$. Em particular, temos daí

$$|\mathbb{R}| \leq |\mathbb{R}^n| = \left|\left(\{0,1\}^{\mathbb{N}}\right)^n\right| = \left|\left(\{0,1\}^{\mathbb{N}}\right)^{\mathbb{N}_{<n}}\right| = \left|\{0,1\}^{\mathbb{N}\times\mathbb{N}_{<n}}\right| \quad \text{e} \quad \left|\left(\{0,1\}^{\mathbb{N}}\right)^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}\times\mathbb{N}}\right|$$

para qualquer $n \in \mathbb{N}$ com $n > 0$. Por fim, segue do Exercício 0.59 (que é consequência direta do Exercício 0.58) que X^Y e X^Z estão em bijeção sempre que Y e Z estão em bijeção. Portanto,

$$|\mathbb{R}| \leq |\mathbb{R}^n| \leq \left|\{0,1\}^{\mathbb{N}\times\mathbb{N}_{<n}}\right| = \left|\{0,1\}^{\mathbb{N}}\right| \leq \left|\left(\{0,1\}^{\mathbb{N}}\right)^{\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}\times\mathbb{N}}\right| = \left|\{0,1\}^{\mathbb{N}}\right| = |\mathbb{R}|$$

pois $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N} \times \mathbb{N}_{<n}$ têm todos a mesma cardinalidade para qualquer $n \in \mathbb{N}$ com $n > 0$ (por quê?)$^{\star}_{\star}$.

Corolário 0.10.14. *$\mathbb{R}$ e $\mathbb{R}^n$ têm a mesma cardinalidade para todo $n \in \mathbb{N}$ com $n > 0$.*

Corolário 0.10.15. *$\mathbb{R}$ e $\mathbb{R}^{\mathbb{N}}$ têm a mesma cardinalidade. Explicitamente: existem tantas funções da forma $\mathbb{N} \to \mathbb{R}$ quanto números reais.*

Exercício 0.113 $(^{\star}_{\star\star})$**.** Mostre que $|\mathbb{R}| < \left|\mathbb{R}^{\mathbb{R}}\right|$. ■

0.11 Exercícios adicionais

Adiante, $\mathbb{K}$ denota um corpo ordenado qualquer, enquanto $\mathbb{R}$ denota *a* reta real.

Exercício 0.114 $(^{\star}_{\star})$**.** Seja $A \subseteq \{x \in \mathbb{K} : x > 0_{\mathbb{K}}\}$ com $A \neq \emptyset$. Mostre que A é ilimitado superiormente se, somente se, $\inf\left\{a^{-1} : a \in A\right\} = 0_{\mathbb{K}}$. ■

Exercício 0.115 $(^{\star}_{\star})$**.** Mostre que se $\mathbb{K}$ é arquimediano, então $\inf_{n\in\mathbb{N}} (2_{\mathbb{K}})^{-n} = 0_{\mathbb{K}}$. Dica: primeiro, mostre que $\{(2_{\mathbb{K}})^n : n \in \mathbb{N}\}$ é ilimitado superiormente em $\mathbb{K}$. ■

Exercício 0.116 $(^{\star}_{\star})$**.** Mostre que

$$\frac{|x+y|_{\mathbb{K}}}{1_{\mathbb{K}} + |x+y|_{\mathbb{K}}} \leq \frac{|x|_{\mathbb{K}}}{1_{\mathbb{K}} + |x|_{\mathbb{K}}} + \frac{|y|_{\mathbb{K}}}{1_{\mathbb{K}} + |y|_{\mathbb{K}}}$$

para quaisquer $x, y \in \mathbb{K}$. Dica: considere separadamente os casos $|x+y|_{\mathbb{K}} \leq |x|_{\mathbb{K}}$, $|x+y|_{\mathbb{K}} \leq |y|_{\mathbb{K}}$ e $\max\{|x|_{\mathbb{K}}, |y|_{\mathbb{K}}\} \leq |x+y|_{\mathbb{K}}$. ■

Exercício 0.117 $(^{\star}_{\star})$**.** Sejam $\delta \in \mathbb{K}$ e $n \in \mathbb{N}$. Mostre que se $\delta > -1_{\mathbb{K}}$ e $n > 0$, então vale a *desigualdade de Bernoulli*: $(1_{\mathbb{K}} + \delta)^n \geq 1_{\mathbb{K}} + n_{\mathbb{K}}\delta$. Dica: $1_{\mathbb{K}} + \delta > 0_{\mathbb{K}}$ e $n_{\mathbb{K}}\delta^2 \geq 0_{\mathbb{K}}$. ■

Exercício 0.118 $(^{\star}_{\star})$**.** Dados $a, b \in \mathbb{R}$ com $a < b$, mostre que $|(a,b)| = |\mathbb{R}|$. ■

Exercício 0.119 ($\star$)**.** Dados $a, b \in \mathbb{R}$ com $a < b$, qual a cardinalidade de $\mathbb{Q} \cap (a, b)$? ■

Exercício 0.120 ($\star$)**.** Dados $x, y \in \mathbb{R}$ com $x < y$, mostre que existe um número real $z \in \mathbb{R} \setminus \mathbb{Q}$ com $x < z < y$. ■

Exercício 0.121 ($\overset{\star}{\star}$)**.** Mostre que $\varphi\colon (-1, 1) \to \mathbb{R}$ dada por $\varphi(x) \coloneqq \dfrac{x}{1 - |x|}$ é bijetora. ■

Exercício 0.122 ($\overset{\star}{\star}$)**.** Mostre que $[a, b]$ e (a, b) têm a mesma cardinalidade para quaisquer $a, b \in \mathbb{R}$ com $a < b$. Conclua que $\overline{\mathbb{R}} \coloneqq \mathbb{R} \cup \{-\infty, +\infty\}$ e $\mathbb{R}$ têm a mesma cardinalidade. ■

Exercício 0.123 ($\overset{\star}{\star}$)**.** Mostre que se $x^2 \leq y^2$, para $x, y \in \mathbb{R}$, então $|x| \leq |y|$. ■

Exercício 0.124 ($\overset{\star}{\star}$)**.** Assuma que para todo $r \in \mathbb{R}$ com $r \geq 0$ exista um único $\alpha \geq 0$ tal que $\alpha^2 = r$. O número α costuma ser indicado por $\sqrt{r}$.

a) Mostre que se $x, y \geq 0$, então deve ocorrer $\sqrt{xy} \leq \dfrac{x + y}{2}$. Dica: $\gamma^2 \geq 0$ para todo $\gamma \in \mathbb{R}$.

b) Com respeito ao item anterior: em que situações pode-se garantir a igualdade? Dica: observe que $\sqrt{x}^2 = x$ para todo $x \geq 0$.

c) Mostre que $\sqrt{x^2} = |x|$ para todo $x \in \mathbb{R}$.

d) Mostre que se $\alpha > \beta \geq 0$, então $\sqrt{\alpha} > \sqrt{\beta}$ ■

Exercício 0.125 ($\overset{\star}{\star\star}$)**.** Prove que $\sqrt{r}$ existe para todo $r \geq 0$. Dica: Para $r \coloneqq 2$ isto está feito no Exemplo 0.9.2. ■

Exercício 0.126 ($\overset{\star}{\star\star}$)**.** Mostre que vale a recíproca do Exercício 0.102. ■

Exercício 0.127 ($\overset{\star}{\star\star}$)**.** Para uma ordem parcial $(\mathbb{P}, \leq)$, mostre que são equivalentes:

(i) todo subconjunto não-vazio e limitado superiormente admite supremo;

(ii) todo subconjunto não-vazio e limitado inferiormente admite ínfimo. ■

Exercício 0.128 ($\star$)**.** Mostre que $\mathbb{K}$ é completo se, e somente se, todo subconjunto não-vazio e limitado inferiormente tem ínfimo. ■

Exercício 0.129 ($\overset{\star}{\star\star}$)**.** Uma **norma** num $\mathbb{R}$-espaço vetorial E é uma função $\|\cdot\|\colon E \to \mathbb{R}$ satisfazendo as condições a seguir para quaisquer $x, y \in E$ e $\lambda \in \mathbb{R}$:

(i) $\|x\| \geq 0$;

(ii) $\|x\| = 0$ se, e somente se, $x = 0$;

(iii) $\|\lambda x\| = |\lambda| \|x\|$;

(iv) $\|x + y\| \leq \|x\| + \|y\|$.

Para um conjunto X qualquer, mostre que a função

$$\begin{aligned} \|\cdot\|_\infty\colon \mathcal{B}(X, \mathbb{R}) &\to \mathbb{R} \\ f &\mapsto \sup\{|f(x)| : x \in X\} \end{aligned}$$

define uma norma no $\mathbb{R}$-espaço vetorial $\mathcal{B}(X, \mathbb{R})$ das funções limitadas da forma $X \to \mathbb{R}$ (cf. Subseção 0.7.1). ■

Capítulo 1

Limites e continuidade

Capítulo 2

Os teoremas fundamentais da Análise

Lista de símbolos e siglas

$\in$	símbolo de pertinência, 8
$A \subseteq B$	A está contido em/é subconjunto de B, 9
$A \not\subseteq B$	A não é subconjunto de B, 9
$A \subsetneq B$	A é subconjunto próprio de B, 9
$A = B$	igualdade entre os conjuntos A e B, 9
$\{x : \mathcal{P}(x)\}$	conjunto dos x's com a propriedade $\mathcal{P}$, 9
$\{a, b\}$	par não-ordenado, 10
$\emptyset$	conjunto vazio, 10
$X \setminus Y$	complementar de Y em X, 10
$A \cap B$	interseção entre A e B, 10
$A \cup B$	(re)união dos conjuntos A e B, 10
(x, y)	par ordenado, 11
$X \times Y$	produto cartesiano, 11
$f\colon X \to Y$ ou $X \xrightarrow{f} Y$	função f de X em Y, 12
$f(x)$	valor de f em x, 12
$x \overset{f}{\mapsto} y$	$f(x) = y$, 12
$g \circ f$	composição das funções g e f, 13
Id_X	função identidade de X, 13
f^{-1}	inversa de f, 16
$X \precsim Y$	cardinalidade de X menor do que a cardinalidade de Y, 18
$X \prec Y$	cardinalidade de X estrit. menor do que a cardinalidade de Y, 18
$Y \succsim X$	cardinalidade de Y maior do que a cardinalidade de X, 18
$Y \succ X$	cardinalidade de Y estrit. maior do que a cardinalidade de X, 18
$x \mathrel{R} y$	R-relação; x e y estão R-relacionados, 18
$x \not\mathrel{R} y$	negação de $x \mathrel{R} y$, 18
$\wp(X)$	conjunto das partes de X, 19
R^{-1}	relação inversa de R, 19
$\bigcup \mathcal{S}$ ou $\bigcup_{S \in \mathcal{S}} S$	reunião da família $\mathcal{S}$, 21

$A \approx B$	A e B têm a mesma cardinalidade, 22
$(\mathbb{X}, \preceq)$	ordem parcial, 23
$\min A$, $\min_{a \in A} a$ ou $\min_{\leq} A$	o menor elemento de A com respeito à ordem $\leq$, 26
$\mathrm{suc}_{\mathbb{B}}(b)$	sucessor de b em $\mathbb{B}$, 27
$\max A$, $\max_{a \in A} a$ ou $\max_{\leq} A$	o maior elemento de A com respeito à ordem $\leq$, 29
$n!$	fatorial de n, 33
$\mathbb{N}_{<n}$	conjunto dos naturais estritamente menores do que n, 38
$\lvert X \rvert$	número cardinal de X, 39
$\bigcap \mathcal{S}$ ou $\bigcap_{S \in \mathcal{S}} S$	interseção da família $\mathcal{S}$, 43
$\mathbb{Z}$	conjunto dos números inteiros, 45
$\mathbb{Q}$	conjunto dos números racionais, 45
$f[A]$	imagem direta de A por f, 49
$f^{-1}[B]$	pré-imagem de B por f, 49
Y^X	conjunto das funções de X em Y, 49
$(G, *, e)$	conjunto G munido de operação $*$ que tem e como elemento neutro, 53
0	elemento neutro aditivo, 54
$-x$	inverso aditivo de x, 54
1	elemento neutro multiplicativo, 54
x^{-1} ou $\frac{1}{x}$	inverso multiplicativo de x, 54
a^n	n-ésima potência de a, 56
z_A	para $z \in \mathbb{Z}$, interpretação de z em A, 57
$\ker f$	núcleo de f, 57
$\lvert x \rvert_{\mathbb{K}}$	valor absoluto de $x \in \mathbb{K}$, 61
$\mathbb{K}_{\geq 0}$	cone positivo, 61
$\mathcal{B}(X, \mathbb{K})$	espaço das funções limitadas de X em $\mathbb{K}$, 62
$\mathbb{C}$	corpo dos números complexos, 62
$\sup A$ ou $\sup_{a \in A} a$	supremo de A, 63
$\inf A$ ou $\inf_{a \in A} a$	ínfimo de A, 63
$A + B$ e $A + x$	soma dos subconjuntos A e B; translação de A por x, 64
AB e xA	produto dos subconjuntos A e B; produto de A por x, 64
$-A$	reflexão de A em torno da origem, 64
$-\infty$ e $+\infty$	pontos no infinito de um corpo estendido, 67
$\overline{\mathbb{K}}$	corpo estendido, 67
$[-\infty, \beta)$	intervalo na reta estendida, fechado em $-\infty$ e aberto em β, 67

$(\alpha, +\infty]$	intervalo na reta estendida, aberto em α e fechado em $+\infty$, 67
(a, b)	intervalo aberto em a e b, 68
$[a, b]$	intervalo fechado em a e b, 69
$[a, b)$	intervalo fechado em a e aberto em b, 69
$(a, b]$	intervalo aberto em a e fechado em b, 69
$\mathbb{R}$	conjunto dos números reais, 77
$\operatorname{seq}(\mathbb{R})$	conjunto das sequências finitas de números reais, 81
$\sum_{i \leq n} f_i$ ou $\sum_{i=0}^{n} f_i$	somatório, 81
$\prod_{i \leq n} f_i$ ou $\prod_{i=0}^{n} f_i$	produtório, 81

Referências Bibliográficas

[0] A. F. Beardon. *Limits: a new approach to real analysis*. Undergraduate Texts in Mathematics. Springer, 1997.

[1] N. Bourbaki. *General Topology, part 1*. Addison-Wesley, London, 1966.

[2] N. Bourbaki. *General Topology, part 2*. Addison-Wesley, London, 1966.

[3] L. Bukovský. *The structure of the real line*. Monografie Matematyczne 71. Birkhäuser Basel, 1 edition, 2011.

[4] J. Ferreirós. *Labyrinth of thought: A history of set theory and its role in modern mathematics*. Birkhäuser Basel, 2ª edition, 2007.

[5] J. F. Hall. *Completeness of Ordered Fields*. California Polytechnic State University, 2010. Monografia de graduação.

[6] J. D. Hamkins. *Lectures on the Philosophy of Mathematics*. MIT Press, 2021.

[7] V. J. Katz and K. H. Parshall. *Taming the Unknown: A History of Algebra from Antiquity to the Early Twentieth Century*. Princeton University Press, 2014.

[8] H. Keisler. *Elementary Calculus. An Infinitesimal Approach*. Dover, 2 edition, 2000.

[9] E. L. Lima. *Análise Real, Volume 1: Funções de uma Variável*. IMPA, 2006.

[10] E. L. Lima. *Curso de Análise, Volume 1*. IMPA, 14 edition, 2017.

[11] P. Maddy. *Defending the Axioms: On the Philosophical Foundations of Set Theory*. Oxford University Press, USA, 2011.

[12] R. M. Mezabarba. Fundamentos de Topologia Geral, 2023. manuscrito, disponível em https://github.com/mezabarbarm/Fund_Top_Geral.

[13] R. M. Mezabarba. Teoria maliciosa dos conjuntos, 2023. manuscrito, disponível em https://github.com/mezabarbarm/MaliciousSetTheory.

[14] R. M. Mezabarba. Um curso fechado e limitado de análise real, 2023. manuscrito, disponível em https://github.com/mezabarbarm/AnalysisZero.

[15] T. Roque. *História da Matemática - Uma Visão Crítica, Desfazendo Mitos e Lendas*. Zahar, 2012.

[16] W. Rudin. *Principles of Mathematical Analysis*. McGraw Hill, 3 edition, 1976.

[17] E. Schechter. *Handbook of Analysis and Its Foundations*. Academic Press, 1996.

[18] R. Shakarchi. *Problems and solutions for undergraduate analysis*. Undergraduate Texts in Mathematics. Springer, 1 edition, 1998.

[19] S. Shapiro, editor. *The Oxford Handbook of Philosophy of Mathematics and Logic*. Oxford Handbooks in Philosophy. Oxford University, 2005.

[20] T. Tao. *Analysis I*. Texts and Readings in Mathematics. Springer, 3 edition, 2016.

Índice Remissivo