Análise I – DEX 001114
Notas de aula

Renan M. Mezabarba

Última atualização: 16 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`" [8], 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 ($\star$, $\overset{\star}{\star}$ 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: [8] 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 [9].

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 "$A \nsubseteq B$" 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

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

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 "$\{\ldots|\ldots\}$" em vez de "$\{\ldots : \ldots\}$". 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 "$\{\ldots\}$". ■

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

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 $\emptyset := \{x : x \neq x\}$, *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 $X \setminus Y := \{x \in X : x \notin Y\}$, que denota a **diferença** entre X e Y, também chamada de **complementar de** Y **em** X.

(iii) Para conjuntos A e B, $A \cap B := \{x : x \in A \text{ e } x \in B\}$ e $A \cup B := \{x : x \in A \text{ ou } x \in B\}$ 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 ":=". 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) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$. ■

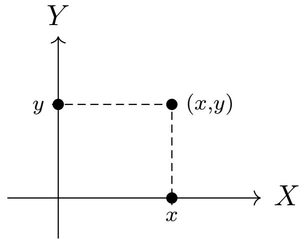
Funções

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** $X \times Y := \{(x, y) : x \in X \text{ e } y \in Y\}$ 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 $y := f(x)$ (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 $\mathrm{im}(f)$. Em símbolos: $\mathrm{im}(f) := \{f(x) : x \in X\}$.

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*

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

Dessa forma, pode-se dizer que $p := \{(x, p(x)) : x \in \mathbb{R}\}$ 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 $r(t) := \frac{p(t)}{q(t)}$ 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 $r(x) := \frac{p(x)}{q(x)}$ 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

$$(g \circ f)(x) := g \circ f(x) := g(f(x)),$$

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

$$\begin{tikzcd}
x \arrow[r, mapsto] & f(x) & y \arrow[r, mapsto] & g(y) \\
X \arrow[r, "f"] \arrow[rrr, bend right, "g\circ f"'] & Y \arrow[rr, "g"] & & Z \\
x \arrow[rrr, mapsto] & & & g(f(x))
\end{tikzcd}$$

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

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

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 $z := g(f(x))$;

✓ 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 $\mathrm{Id}_X(x) := x$ 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.

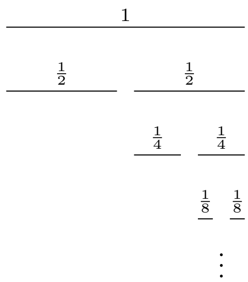
Leopold Kronecker (1886).

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 [2]. 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 $S \coloneqq \sum_{n=1}^{\infty} \frac{1}{2^n}$, 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 $T \coloneqq \sum_{n=1}^{\infty} 2^n$, 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 $\{\ldots : \ldots\}$. Grosso modo, postula-se o seguinte: dada uma *propriedade* $\mathcal{P}$, existe o conjunto $\{x : x$ 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 $(x, y) := \{\{x\}, \{x, y\}\}$. 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 $R := \{x : x \notin x\}$. 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 $\{x \in A : x$ 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 [7].

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 $f : X \to Y$ 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 $f : X \to Y$ for injetora e sobrejetora. ¶

Para aquecer, você pode começar com o próximo

Exercício 0.12 $({}^{\star}_{\star})$**.** 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. $\square$

Exercício 0.14 ($^\star_\star$)**.** 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. $\blacksquare$

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. ¶

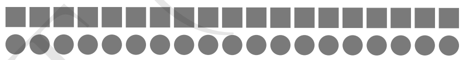


Figura 0.1: É evidente que há tantos círculos quanto quadrados, mesmo sem saber *quantos*.

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. $\square$

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 ($^{\star}_{\star}$)**.** 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: há questões mais urgentes a serem discutidas.

Exercício 0.16 ($^{\star}_{\star\star}$)**.** 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 $\operatorname{dom}(R) := \{x : \text{existe } y \in Y \text{ com } x \, R \, y\}$.

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

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 $\{n : n$ é par$\}$, $\{n : n$ é ímpar$\}$, $\{n : n$ 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 $x \in \operatorname{dom}(S)$ existem $y, y' \in \operatorname{im}(S)$ 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 $({}^{\star}_{\star})$**.** Para uma relação binária R, mostre que:

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

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

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

d) $(R^{-1})^{-1} = R$. ■

Exercício 0.18 $({}^{\star}_{\star\star})$**.** 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 $\displaystyle\bigcup_{i\in\mathcal{I}} S_i$ 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 $({}^{\star}_{\star\star})$**.** 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 $({}^{\star}_{\star})$**.** 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 $\bar{i}$ a *classe* de equivalência de i, verifica-se $\bar{i} = R_i$. Desse modo, seria lícito escrever, por exemplo, $\mathbb{N}/\sim_2 = \left\{\overline{0}, \overline{1}\right\}$, ou ainda $\mathbb{N}/\sim_2 = \left\{\overline{12}, \overline{13}\right\}$, 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 $\mathbb{V}$.

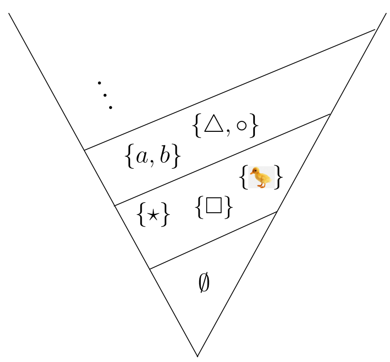


Figura 0.2: Cada $\approx$-classe de equivalência corresponde a uma noção de cardinalidade.

[13]Poderíamos defini-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 apresentado na subseção anterior 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 $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ (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 $X := \mathbb{N}$ por exemplo, $A := \{0, 1, 2\}$ e $B := \{0, 1, 3\}$ 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

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
8 \arrow[u] & 36 \arrow[u] & 81 \arrow[u] & 225 \arrow[u] & 625 \arrow[u] & 1225 \arrow[u] & 2401 \arrow[u] \\
4 \arrow[u] \arrow[ur] & 6 \arrow[u] & 9 \arrow[ul] \arrow[u] \arrow[ur] & 15 \arrow[u] & 25 \arrow[ul] \arrow[u] \arrow[ur] & 35 \arrow[u] & 49 \arrow[ul] \arrow[u] \\
2 \arrow[u] \arrow[ur] & & 3 \arrow[ul] \arrow[u] \arrow[ur] & & 5 \arrow[ul] \arrow[u] \arrow[ur] & & 7 \arrow[ul] \arrow[u] \\
& & & 1 \arrow[ulll] \arrow[ul] \arrow[ur] \arrow[urrr] & & &
\end{tikzcd}$$

[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.

$$
\begin{tikzcd}
 & \{a,b,c\} & \\
\{a,b\} \arrow[ur] & \{a,c\} \arrow[u] & \{b,c\} \arrow[ul] \\
\{a\} \arrow[u] \arrow[ur] & \{b\} \arrow[ul] \arrow[ur] & \{c\} \arrow[ul] \arrow[u] \\
 & \emptyset \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}
$$

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 $y \leq x$. ¶

$$\cdots \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \cdots$$

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 $\min\limits_{a \in A} a$, $\min_{\leq} A$ 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 $\leq$. ¶

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 [2].

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 $\left({}^{\star}_{\star\star}\right)$**.** 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. É importante destacar que a noção de sucessor só faz sentido em boas ordens. 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 $\left({}^{\star}_{\star}\right)$**.** 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* $c \in \mathbb{B}$*:*

sempre que ocorre $b \in X$ *para todo* $b < c$*, 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 $t \in T := \mathbb{B} \setminus X$. $\square$

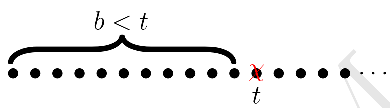


Figura 0.3: Se t fosse o *primeiro* tal que $t \notin X$, então todo $b < t$ pertenceria a X. Logo, $t \in X$!

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:

sempre que vale $\mathcal{P}(b)$ ***para todo*** $b < c$, *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” [4, 5]. 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: $\min \mathbb{B} \in X$ pois não existe $b < \min \mathbb{B}$ e, por isso, 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 ($^{\star}_{\star}$)**.** 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 $(^{\star}_{\star\star})$**.** 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]. ■

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 0.2.20, 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 $(^{\star}_{\star\star})$**.** 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 $(^{\star}_{\star\star})$**.** 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* $b' = \operatorname{suc}_{\mathbb{B}}(b)$*. Em tais condições, se* $X \subseteq \mathbb{B}$ *for tal que*

✓ $p \in X$, *e*

✓ $\operatorname{suc}_{\mathbb{B}}(b) \in X$ *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 $c = \operatorname{suc}_{\mathbb{B}}(b)$ (que existe pela hipótese sobre $\mathbb{B}$), deve-se ter $b < c$, donde segue que $b \in X$ e, pela hipótese sobre X, $c = \operatorname{suc}_{\mathbb{B}}(b) \in X$, 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 $\operatorname{suc}_{\mathbb{B}}(b)$ 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 $a = \min \mathbb{B}$, $a' = \operatorname{suc}_{\mathbb{B}}(a)$, $a'' = \operatorname{suc}_{\mathbb{B}}(a')$ e $a''' = \operatorname{suc}_{\mathbb{B}}(a'')$, 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 $a'''' := \operatorname{suc}_{\mathbb{B}}(a''')$, $a''''' := \operatorname{suc}_{\mathbb{B}}(a'''')$ 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) $\operatorname{suc}_{\mathbb{B}}(b)$ existe para todo $b \in \mathbb{B}$,

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

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 [4, 5], 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$_i$) $\mathcal{N} \setminus \mathrm{im}\,(s) = \{i\}$;

(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* $(\mathbb{B}, \min \mathbb{B}, \mathrm{suc}_{\mathbb{B}})$ *é um sistema natural, ou seja:*

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

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

(iii) *se* $X \subseteq \mathbb{B}$ *for tal que* $\min \mathbb{B} \in X$ *e* $\mathrm{suc}_{\mathbb{B}}(b) \in X$ *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 $\mathrm{suc}_{\mathbb{B}} \colon \mathbb{B} \to \mathbb{B}$ é injetora.

Explicitamente, deve-se mostrar que se $x, y \in \mathbb{B}$ são distintos, então $\mathrm{suc}_{\mathbb{B}}(x) \neq \mathrm{suc}_{\mathbb{B}}(y)$. 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 $\mathrm{suc}_{\mathbb{B}}(x) < \mathrm{suc}_{\mathbb{B}}(y)$. Ora, pelo Exercício 0.28, já sabemos que $\mathrm{suc}_{\mathbb{B}}(x) \leq \mathrm{suc}_{\mathbb{B}}(y)$. Se tal desigualdade não fosse estrita, teríamos $\mathrm{suc}_{\mathbb{B}}(x) = \mathrm{suc}_{\mathbb{B}}(y)$, resultando em

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

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 0.71. Enfim, chega-se ao seguinte:

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, como [4, 5].

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.

$$\begin{tikzcd}
(A) & 1 \arrow[r, "+1"] & 2 \arrow[r, "+1"] & 3 \arrow[r, "+1"] & 4 \arrow[r, "+1"] & \cdots \\
(B) & \bullet \arrow[r, "+\bullet"] & \bullet\bullet \arrow[r, "+\bullet"] & \bullet\bullet\bullet \arrow[r, "+\bullet"] & \bullet\bullet\bullet\bullet \arrow[r, "+\bullet"] & \cdots \\
(C) & | \arrow[r, "+|"] & || \arrow[r, "+|"] & ||| \arrow[r, "+|"] & |||| \arrow[r, "+|"] & \cdots \\
(D) & i \arrow[r, "s"] & s(i) \arrow[r, "s"] & s(s(i)) \arrow[r, "s"] & s(s(s(i))) \arrow[r, "s"] & \cdots \\
(E) & \emptyset \arrow[r, "\{\}"] & \{\emptyset\} \arrow[r, "\{\}"] & \{\{\emptyset\}\} \arrow[r, "\{\}"] & \{\{\{\emptyset\}\}\} \arrow[r, "\{\}"] & \cdots \\
(F) & \emptyset \arrow[r, "x\mapsto x\cup\{x\}"] \arrow[d, equal, "."] & \{\emptyset\} \arrow[r, "x\mapsto x\cup\{x\}"] \arrow[d, equal, "."] & \{\emptyset,\{\emptyset\}\} \arrow[r, "x\mapsto x\cup\{x\}"] \arrow[d, equal, "."] & \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\} \arrow[r, "x\mapsto x\cup\{x\}"] \arrow[d, equal, "."] & \cdots \\
(G) & 0 \arrow[r, "+1"] & 1 \arrow[r, "+1"] & 2 \arrow[r, "+1"] & 3 \arrow[r, "+1"] & \cdots
\end{tikzcd}$$

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!) de que tais procedimentos podem ser realizados entre conjuntos – e o plural em "axiomas!" não foi um equívoco.

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 matemáticos profissionais *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:

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

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 arcabouçou 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: $\mathrm{suc}_{\mathbb{N}}(n) := n + 1$ 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: $0! := 1$ e $(n+1)! := (n+1) \cdot n!$. 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 $F(m) := F_n(m)$ 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 $\operatorname{dom}(f) := \{x : \text{existe } y \text{ tal que } (x, y) \in f\}$ e $\operatorname{im}(f) := \{y : \text{existe } x \text{ tal que } (x, y) \in f\}$, 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 $F := \bigcup \mathcal{F}$ 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 $(^{\star}_{\star})$**.** 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 $\mathbb{B} := X := \mathbb{N}$, $R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $R(n, m) := (n + 1) \cdot m$ e $x := 1$. 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 $\mathbb{B}_{<b} := \{c \in \mathbb{B} : c < b\}$. 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

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

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 $b := \min \mathbb{B}$, 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 $b := \min \mathbb{B}$, então $\mathbb{B}_{<\mathrm{suc}_{\mathbb{B}}(b)} = \{b\}$ e, assim, basta definir $f(b) := x$;
  - ✓ 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 $g(d) := f(d)$ se $d < b$ (i.e., $d \leq c$), e $g(b) := R(c, f(c))$.

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* $\mathcal{F} := \{f_b : b \in \mathbb{B}\}$, que satisfaz as exigências do Lema 0.3.8. Logo, $R_x := \bigcup_{b \in \mathbb{B}} f_b$ 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 $({}^{\star}_{\star\star})$**.** 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 [4, 5].

(+) 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 $+(m, n) := +_m(n)$, que por simplicidade será denotado por $m + n$.

($\cdot$) 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 $\cdot(m, n) := \cdot_m(n)$, que por simplicidade será denotado por $m \cdot n$.

Exercício 0.37 $({}^{\star}_{\star})$**.** 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 $R(n, y) := \mathrm{suc}_{\mathbb{B}}(y)$ e $x := m$; para $\cdot_m$, faça $R(n, y) := y + m$ (que existe pelo passo anterior!) e tome $x := 0$. ■

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 $({}^{\star}_{\star\star})$**.** Complete a demonstração anterior. ■

Exercício 0.39 $({}^{\star}_{\star}\star{}^{\star}_{\star})$**.** 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] $({}^{\star}_{\star\star})$: 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 a injetividade de s assegura $k \neq n$, 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 0.71, toma-se $X := \mathcal{M}$, $x := j$ e faz-se $R_j\colon \mathcal{N} \times \mathcal{M} \to \mathcal{M}$ 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 0.71 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* <u>*isomorfas*</u>*. 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, <u>no contexto acima</u>, 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)$^{\star}_{\star}$ 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 que todo elemento de $\mathbb{B}$ tem 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), para razoável dizer que existe $u' \notin \mathbb{N}$. Acontece que em posse disso, a Proposição 0.2.16 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 [7].

[31]Como na Figura 0.4 da página 33.

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 0.72).

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**. ¶

[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 $X \subsetneq \mathbb{N}_{<n}$, então não existe bijeção entre $\mathbb{N}_{<n}$ e X.*

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 $X \subsetneq \mathbb{N}_{<n+1}$ resultaria numa bijeção entre $\mathbb{N}_{<n}$ e um subconjunto próprio de $\mathbb{N}_{<n}$, contrariando a *hipótese de indução*[33]:

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

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. □

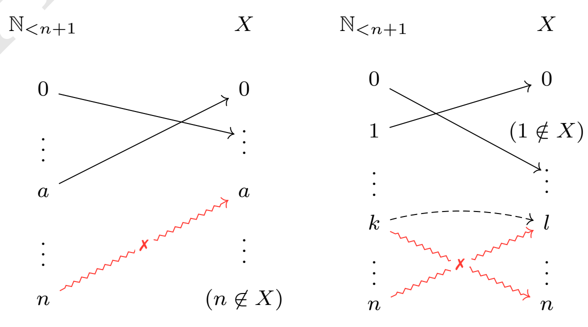


Figura 0.6: A demonstração anterior, em cores.

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]. $\triangle$

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 Exercício 0.61.

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, $\varphi[Y] := \{\varphi(y) : y \in Y\}$ 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:

$$\begin{tikzcd} Y \arrow[r, "\text{bijeção}"] \arrow[d, shift right, "\varphi|_Y"'] & X \arrow[d, "\varphi"] \\ \varphi[Y] \arrow[u, bend right, "(\varphi|_Y)^{-1}"'] \arrow[r, phantom, "\subsetneq"] & \mathbb{N}_{<n} \end{tikzcd}$$

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 ($\star$). $\square$

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

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

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 $|\mathbb{N}| := \infty$?* 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 $T := \{x \in X : x \notin \varphi(x)\}$ 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 $X \to \wp(X)$. $\square$

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

[35] Caso precise revisar esse assunto, confira o Exercício 0.52.

Exercício 0.42 ($^{\star}_{\star\star}$)**.** Mostre que se existe injeção $\mathbb{N} \to Y$, então Y é infinito. Dica: $\mathbb{N}$ está em bijeção com um subconjunto de Y; o que ocorreria com tal subconjunto se Y fosse finito? ■

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 uma injeção $\mathbb{N} \to X$ induz uma função injetora $\mathbb{N} \to \wp(X)$ (certo?)*. 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]. A próxima subseção apresentará um modo simples de contornar o problema, que será retomado na última seção.

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 <u>bijeção</u> $X \to \mathbb{N}$ (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 0.43 ($\star$)**.** 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.

$$
\begin{tikzcd}
 & 0 & 1 & 2 & 3 & 4 & \cdots \\
0 & (0,0) \arrow[r] & (1,0) \arrow[dl] & (2,0) \arrow[d] & (3,0) \arrow[r] & (4,0) \arrow[d] & \\
1 & (0,1) \arrow[r] & (1,1) \arrow[ur] & (2,1) \arrow[dl] & (3,1) \arrow[u] & (4,1) \arrow[dl] & \\
2 & (0,2) \arrow[d] & (1,2) \arrow[l] & (2,2) \arrow[ur] & (3,2) \arrow[dl] & & \\
3 & (0,3) \arrow[r] & (1,3) \arrow[ur] & (2,3) \arrow[dl] & & & \\
4 & (0,4) \arrow[d] & (1,4) \arrow[l] & & & & \\
\vdots & \vdots & & & & &
\end{tikzcd}
$$

[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 $f: X \to Y$ é sobrejetora se, e somente se, existe uma injeção $g: Y \to X$ 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 $g: Y \to X$ 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 $f: X \to Y$ 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 $f: \mathbb{N} \times \mathbb{N} \to \bigcup_{n \in \mathbb{N}} X_n$ 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 $\varphi: \mathbb{N}_{<n} \to X$ 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 0.44 ($^\star_\star$)**.** 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 0.45 (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 $\displaystyle\bigcap_{i\in\mathcal{I}} S_i$ 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 0.46 $(\star)$**.** 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 0.47 ($\star\atop\star$)**.** 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 0.48). 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 $g[Y \setminus f[S]] = X \setminus S$, equivalentemente exprimível como $S = X \setminus g[Y \setminus f[S]]$. Como obter tal S?

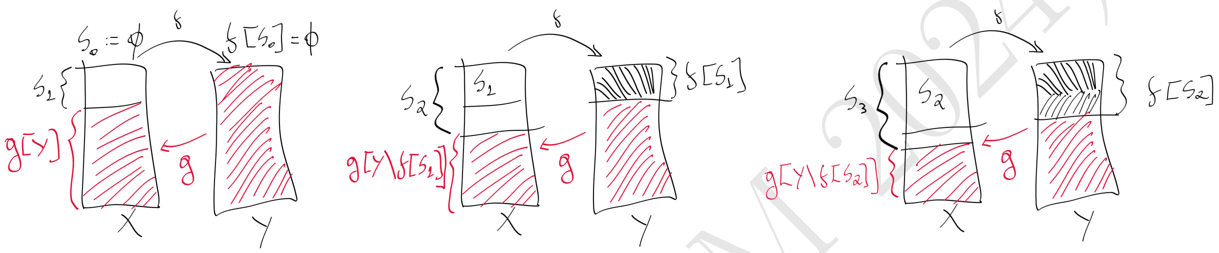


Figura 0.7: Heurística da construção recursiva do conjunto S.

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

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

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

Exercício 0.48 ($\star\atop\star$)**.** 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 [9].

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 0.49 $({}^{\star}_{\star\star})$**.** Sobre $Z := \mathbb{N}\times\mathbb{N}$, 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 $\overline{(a,b)} +' \overline{(c,d)} := \overline{(a+c,b+d)}$, 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

$$(a-b) +' (c-d) := (a+c)-(b+d),$$

tal qual aprendemos na escola.

Exercício 0.50 $({}^{\star}_{\star}\star{}^{\star}_{\star})$**.** 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

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

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 0.51 $({}^{\star}_{\star\star})$**.** Sobre $Q := \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$, 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 por diante*. 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 raiz 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 0.45). 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 e como resolvê-lo: 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 [11] ou a envolvente discussão de Penelope Maddy [6] – se preferir algo mais modesto, o texto de Joel D. Hamkins [3] 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 [7].

✓ Finalmente, para o Teorema 0.4.13, com $\mathcal{A} := \wp(X) \setminus \{\emptyset\}$, 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 $\mathcal{O}(s) := f(X \setminus \operatorname{im}(s))$, 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.

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 $R := \{x \in V : x \notin x\}$, 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 $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, 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 $\omega + 1 := \omega \cup \{\omega\}$, ganha-se novamente um ordinal, e ao definir $\omega + 2 := \omega + 1 \cup \{\omega + 1\}$... 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 [7].

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 0.52 (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 0.53 ((!))**.** 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 0.54 ($^{\star}_{\star}$)**.** 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 0.55 ($^{\star}_{\star}$)**.** Mostre que se $|A| = |B|$, então $|\wp(A)| = |\wp(B)|$. ■

Exercício 0.56 ($^{\star}_{\star}$)**.** Sejam A, B, C e D conjuntos. Mostre que se $|A| \leq |C|$ e $|B| \leq |D|$, então $|A^B| \leq |C^D|$. ■

Exercício 0.57 ($^{\star}_{\star}$)**.** 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 0.61.

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 0.58 $({}^{\star}_{\star\star})$**.** 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 0.59 ((!))**.** 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 0.60 $({}^{\star}_{\star})$**.** Seja $f\colon X \to Y$ uma função. Mostre que $\mathcal{P} := \{f^{-1}[\{y\}] : y \in \operatorname{im}(f)\}$ é uma partição de X. ■

Exercício 0.61 $({}^{\star}_{\star\star})$**.** 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 0.54.

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

Exercício 0.62 $({}^{\star}_{\star})$**.** 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 0.63 $({}^{\star}_{\star\star})$**.** Mostre que para X finito, uma função $f\colon X \to X$ é injetora, e somente se, é sobrejetora. ■

Exercício 0.64 $({}^{\star}_{\star})$**.** O resultado acima permanece válido para X infinito? ■

Exercício 0.65 $({}^{\star}_{\star})$**.** 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 0.66 $({}^{\star}_{\star})$**.** Seja $f\colon X \to Y$ uma função, com Y enumerável e X não-enumerável. Mostre que existe $y \in Y$ tal que $X' := \{x \in X : f(x) = y\}$ é não-enumerável. ■

Exercício 0.67 $({}^{\star}_{\star})$**.** Seja $\psi\colon X \to Y$ uma função bijetora. Mostre que se $\mathcal{P}$ é uma partição de X, então $\psi(\mathcal{P}) := \{\psi[P] : P \in \mathcal{P}\}$ 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 0.68 $({}^{\star}_{\star\star})$**.** Mostre que existe uma partição $\mathcal{P} := \{P_n : n \in \mathbb{N}\}$ 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 0.69 $({}^{\star}_{\star})$**.** Sejam $(\mathbb{S}, \leq)$ e $(\mathbb{T}, \leq)$ ordens parciais. Uma função $f : \mathbb{S} \to \mathbb{T}$ 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 $f^{-1} : \mathbb{T} \to \mathbb{S}$ 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 0.70 $(\star)$**.** Convença-se de que funções estritamente monótonas são injetoras. ■

Exercício 0.71 $({}^{\star\star}_{\star\star})$**.** 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.

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 para todo $n \in \mathcal{N}$ ocorre $n \leq s(n)$ e $s(n) \not\leq n$. Dica: para a segunda parte, com $X := \{n \in \mathcal{N} : s(n) \not\leq n\}$, 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 0.72 $\left(\substack{\star\star\\\star\star}\right)$**.** Suponha que você tenha que dar um curso de Análise em que $0 \notin \mathbb{N}$. Como definir, recursivamente, as operações de soma e multiplicação em $\mathbb{N}$? ■

0.6 Linguagem algébrica: anéis e corpos

0.7 Corpos ordenados

0.8 Supremos e ínfimos

0.9 Completude (no sentido de Dedekind)

0.10 Isomorfismos e a unicidade da reta real

0.11 Exercícios adicionais

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
$A \nsubseteq B$	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

Referências Bibliográficas

[0] A. F. Beardon. *Limits: a new approach to real analysis*. Undergraduate Texts in Mathematics. Springer, 1997.

[1] L. Bukovský. *The structure of the real line*. Monografie Matematyczne 71. Birkhäuser Basel, 1 edition, 2011.

[2] J. Ferreirós. *Labyrinth of thought: A history of set theory and its role in modern mathematics*. Birkhäuser Basel, 2ª edition, 2007.

[3] J. D. Hamkins. *Lectures on the Philosophy of Mathematics*. MIT Press, 2021.

[4] E. L. Lima. *Análise Real, Volume 1: Funções de uma Variável*. IMPA, 2006.

[5] E. L. Lima. *Curso de Análise, Volume 1*. IMPA, 14 edition, 2017.

[6] P. Maddy. *Defending the Axioms: On the Philosophical Foundations of Set Theory*. Oxford University Press, USA, 2011.

[7] R. M. Mezabarba. Teoria maliciosa dos conjuntos, 2023. manuscrito, disponível em https://github.com/mezabarbarm/MaliciousSetTheory.

[8] R. M. Mezabarba. Um curso fechado e limitado de análise real, 2023. manuscrito, disponível em https://github.com/mezabarbarm/AnalysisZero.

[9] T. Roque. *História da Matemática - Uma Visão Crítica, Desfazendo Mitos e Lendas*. Zahar, 2012.

[10] E. Schechter. *Handbook of Analysis and Its Foundations*. Academic Press, 1996.

[11] S. Shapiro, editor. *The Oxford Handbook of Philosophy of Mathematics and Logic*. Oxford Handbooks in Philosophy. Oxford University, 2005.

[12] T. Tao. *Analysis I*. Texts and Readings in Mathematics. Springer, 3 edition, 2016.

Índice Remissivo