

1 Conjuntos, funções e relações: noções básicas

Antes de abordarmos os temas centrais deste curso é conveniente recordar algumas noções básicas usadas sistematicamente no que se segue.

1.1 Conjuntos

Intuitivamente, um conjunto é, nas palavras de Georg Cantor, “uma colecção qualquer de certos objectos distintos da nossa intuição ou pensamento, considerada num todo”.

Esta descrição levanta vários problemas, em particular quanto ao uso do pronome *qualquer*, que só podem ser resolvidos satisfatoriamente por uma *fundação axiomática* da Teoria dos Conjuntos, fora do âmbito desta cadeira (ver a Nota 1.2 no fim desta seção).

Mas, devido à natureza simples dos conjuntos com que teremos ocasião de lidar, esses problemas não nos surgirão no caminho.

Vamos portanto usar o termo **conjunto** e a noção de **pertença** como primitivos, ou seja, não definidos a partir de outros termos, e ater-nos a uma descrição de algumas das noções e propriedades mais elementares da chamada Teoria intuitiva dos Conjuntos, bem como da notação correspondente.

Note-se que essa descrição depende do uso de símbolos lógicos e suas propriedades, que não serão recordados aqui.

1. Um conjunto é completamente determinado pelos seus elementos. Usamos a notação $x \in X$ para dizer que x é um elemento do conjunto X e $x \notin X$ para dizer que x não é um elemento do conjunto X .
2. Um conjunto pode ser definido por extensão, quer dizer, enumerando todos os seus elementos, ou através de uma propriedade que determina que elementos tem o conjunto. Por exemplo, o mesmo conjunto pode ser descrito como

$$\{2, 4, 6\},$$

como

$$\{x : x < 8 \wedge \exists z \in \mathbb{N} : x = 2z\},$$

ou ainda como

$$\{x : x \in \mathbb{R} \wedge x^3 - 12x^2 + 44x - 48 = 0\}$$

onde \mathbb{N} e \mathbb{R} designam os números naturais e os números reais, respectivamente.

3. Existe o conjunto vazio, designado por \emptyset e caracterizado por não ter elementos.
4. Dados conjuntos X e Y existem o conjunto união $X \cup Y$, o conjunto intersecção $X \cap Y$ e o conjunto diferença $X \setminus Y$ definidos respectivamente por

$$X \cup Y = \{x : x \in X \vee x \in Y\}$$

$$X \cap Y = \{x : x \in X \wedge x \in Y\}$$

$$X \setminus Y = \{x : x \in X \wedge x \notin Y\}$$

Quando se consideram subconjuntos de um dado conjunto fixo X , usam-se igualmente as notações A^c ou \overline{A} (complementar de A) para designar $X \setminus A$.

5. Como se verifica facilmente a partir das definições, a união e intersecção de conjuntos são operações comutativas e associativas

$$X \cap Y = Y \cap X, \quad X \cap (Y \cap Z) = (X \cap Y) \cap Z, \quad X \cup Y = Y \cup X, \quad X \cup (Y \cup Z)$$

e distributivas uma sobre a outra:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \quad X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

6. $X \subset Y$ denota o facto de todo o elemento de X ser também elemento de Y :

$$X \subset Y \Leftrightarrow (x \in X \Rightarrow x \in Y)$$

Se $Y \subset X$ mas $Y \neq X$, usa-se a notação $Y \subsetneq X$.

7. Dados subconjuntos A e B de X , verifica-se também facilmente a validade das **Leis de Morgan**:

$$(A \cap B)^c = A^c \cup B^c, \text{ e } (A \cup B)^c = A^c \cap B^c.$$

8. Um elemento $x \in X$ pode por sua vez ser também um conjunto. Em particular, dado um qualquer conjunto X , existe o conjunto das partes de X :

$$\mathcal{P}(X) = \{Y : Y \subset X\}$$

9. Dados conjuntos X e Y , existe o conjunto produto

$$X \times Y = \{(x, y) | x \in X \wedge y \in Y\}$$

ou seja, o conjunto cujos membros são os pares ordenados em que o primeiro elemento pertence a X e o segundo a Y .

Nota 1.1 A definição do produto de dois conjuntos $X \times Y$ pode ser feita a partir das noções anteriores: podemos por exemplo definir

$$X \times Y = \{\{\{a\}, \{a, b\}\} : a \in X \wedge b \in Y\}$$

Ou seja, cada elemento deste conjunto é um conjunto que tem como membros o conjunto que tem como único elemento um $a \in X$ e o conjunto que tem como elementos o mesmo $a \in X$ e um $b \in Y$.

Para vermos que temos uma definição correcta, basta comprovar que

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \implies a = c \wedge b = d$$

Nota 1.2 Sem entrarmos numa discussão séria dos problemas mencionados acima, vamos apenas demonstrar a sua existência por meio do talvez mais célebre exemplo, o Paradoxo de Russel. A ideia de que um conjunto possa ser elemento dele mesmo é talvez um pouco estranha (ou mesmo absurda) mas o facto oposto não levanta dúvidas: todos conhecemos

conjuntos que não são elementos de si próprios.
 Poderíamos então imaginar o conjunto (de conjuntos)

$$U = \{x : x \notin x\};$$

o problema surge quando perguntamos se U é elemento de U : se $U \in U$ então, pela própria definição de U , $U \notin U$. Se supomos que $U \notin U$ somos conduzidos à mesma contradição.

Exercícios I.1

1. Mostrar que para quaisquer conjuntos A , B e C

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

e que

$$(A \cap B)^c = A^c \cup B^c, \text{ e } (A \cup B)^c = A^c \cap B^c,$$

onde, por exemplo, A^c designa o complementar de A na união $X = A \cup B \cup C$: $A^c = X \setminus A$.

2. Define-se a *diferença simétrica* de dois conjuntos como

$$A \triangle B = A \setminus B \cup B \setminus A$$

Mostrar que

- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
- $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

Sugestão: podemos considerar todos os conjuntos envolvidos como subconjuntos de $X = A \cup B \cup C$. A diferença simétrica pode então escrever-se

$$A \triangle B = (A \cap B^c) \cup (A^c \cap B),$$

onde, por exemplo, $A^c = X \setminus A$. Aplicar as propriedades de distributividade entre união e intersecção e as Leis de Morgan, usando um diagrama de Venn.

3. Mostrar que, se $\{A_i : i \in \mathbb{N}\}$ e $\{B_i : i \in \mathbb{N}\}$ são famílias de conjuntos satisfazendo

$$A_i \supset A_{i+1}, \quad B_i \supset B_{i+1}, \quad \forall i \in \mathbb{N}$$

então

$$\bigcap_{i \in \mathbb{N}} (A_i \cup B_i) = \left(\bigcap_{i \in \mathbb{N}} A_i \right) \cup \left(\bigcap_{i \in \mathbb{N}} B_i \right)$$

Sem aquela condição esta igualdade verifica-se ou não?

4. Dada uma família infinita de conjuntos V_n ($n \in \mathbb{N}$), mostrar que
- o conjunto dos elementos que pertencem a um número infinito de conjuntos V_n é dado por $\bigcap_{k \in \mathbb{N}} \bigcup_{n \geq k} V_n$.
 - o conjunto dos elementos que pertencem a todos excepto a um número finito dos conjuntos V_n é dado por $\bigcup_{k \in \mathbb{N}} \bigcap_{n \geq k} V_n$.

Nota 1.3 *Nos exercícios 3 e 4 anteriores usam-se de modo informal o conjunto \mathbb{N} dos números naturais e o conceito de infinito, ambos discutidos mais adiante.*

1.2 Funções e Relações

Intuitivamente, uma função é uma correspondência entre os elementos de um conjunto X (o domínio ou conjunto de partida) e elementos de um conjunto Y (o contradomínio ou conjunto de chegada)

Definição 1.4 *uma função $f : X \rightarrow Y$ diz-se*

1. *injectiva se*

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \quad \forall x_1, x_2 \in X$$

2. *sobrejectiva se*

$$\forall y \in Y \exists x \in X : f(x) = y$$

.

3. *bijectiva se for injectiva e sobrejectiva.*

Definição 1.5 *Se $f : X \rightarrow Y$, $W \subset X$ e $Z \subset Y$ definem-se as*

- *imagem de W por f :*

$$f(W) = \{f(x) : x \in W\}$$

- *imagem inversa de Z por f :*

$$f^{-1}(Z) = \{x \in X : f(x) \in Z\}$$

Exercícios I.2

1. Mostrar que

$$f : \mathbb{N} \rightarrow \mathbb{N}, \quad f(n) = n^2 + n + 1$$

é uma função injectiva mas não sobrejectiva.

2. Mostrar que $d : \mathbb{N} \rightarrow \mathbb{N}$ definida por $d(n)$ ser o número de divisores naturais de n , é uma função sobrejectiva mas não injectiva.
3. Dada uma função $f : X \rightarrow Y$ e $A, B \subset X$, determinar se

$$f(A \cup B) = f(A) \cup f(B) \quad f(A \cap B) = f(A) \cap f(B)$$

Se $C, D \subset Y$ determinar se

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D) \quad f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

Podemos dar uma definição mais formal de função:

Definição 1.6 *Uma função com domínio X e contradomínio Y é um subconjunto $f \subset X \times Y$ satisfazendo a propriedade seguinte: para cada $x \in X$ existe um único $y \in Y$ tal que $(x, y) \in f$.*

Ou seja, identificamos a função f com o que usualmente se chama o seu gráfico, como consequência da habitual representação gráfica de uma função por meio de um sistema de eixos.

Esta definição de função em termos de conjuntos leva a uma outra, mais geral:

Definição 1.7 Uma **relação** (binária) entre X e Y é um subconjunto $R \subset X \times Y$.

Encontraremos diversos tipos especiais de relação particularmente importantes, como as relações de **ordem** ou de **equivalência**, definidas mais à frente.

É usual escolher um símbolo (por exemplo \bowtie) para representar a relação e usa-se então a notação $x \bowtie y$ para significar que $x \in X$ e $y \in Y$ estão na relação, ou seja $(x, y) \in R$. Quando $Y = X$ dizemos abreviadamente que temos uma relação em X (e não entre X e X).

Definição 1.8 Uma relação \mathcal{R} num conjunto X é

- **unívoca** se $\forall x \in X, \exists^1 y \in Y : (x, y) \in f$ onde o símbolo \exists^1 significa “existe um e um só”
- **reflexiva** se $x \mathcal{R} x \forall x \in X$
- **simétrica** se $x \mathcal{R} y \Rightarrow y \mathcal{R} x$
- **anti-simétrica** se $x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$
- **transitiva** se $x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z$

Uma **função** $f : X \rightarrow Y$ não é mais, portanto, do que uma relação unívoca entre X e Y . Naturalmente, usamos a notação habitual $f(x) = y$ em vez de $(x, y) \in f$.

Definição 1.9 • Uma relação reflexiva, transitiva e anti-simétrica chama-se uma **relação de ordem (parcial)**;

- Uma relação reflexiva, transitiva e simétrica chama-se uma **relação de equivalência**;

Exemplo 1.10 : A relação de inclusão \subset definida em $\mathcal{P}(\mathcal{X})$, para qualquer conjunto X , é uma relação de ordem parcial.

Exemplo 1.11 : Dado um conjunto de conjuntos \mathcal{C} , podemos definir uma relação \sim por

$$X \sim Y \Leftrightarrow \exists f : X \rightarrow Y \text{ bijectiva}$$

Como se verifica facilmente, \sim é uma relação de equivalência.

De uma relação de equivalência \mathcal{R} num conjunto X resulta uma decomposição de X numa união de subconjuntos, disjuntos dois a dois, que se chamam as **classes de equivalência** da relação; cada uma dessas classes de equivalência é um subconjunto (não vazio) de X cujos elementos estão em relação entre si. As propriedades reflexiva, simétrica e transitiva de \mathcal{R} garantem que esta definição é coerente e que esses subconjuntos são de facto disjuntos dois a dois.

Exercícios I.3

1. Dada uma função $f : X \rightarrow X$, definimos $f^m : X \rightarrow X$, para $m \in \mathbb{N}$, como a composição de f consigo mesma m vezes; mais precisamente:

$$f^0(x) = x \quad \forall x \in X; \quad \forall m \in \mathbb{N} \quad f^m(x) = f(f^{m-1}(x)) \quad \forall x \in X.$$

Mostrar que a relação \mathcal{O} definida em X por

$$x \mathcal{O} y \text{ se } \exists m, n \in \mathbb{N}_0 : f^m(x) = f^n(y)$$

é uma relação de equivalência.

2. No conjunto $\mathbb{N} \times \mathbb{N} = \{(m, n) : m, n \in \mathbb{N}\}$ definimos a relação \prec do seguinte modo:

$$(m, n) \prec (s, t) \text{ se e só se } m < s \vee (m = s \wedge n \leq t).$$

Verificar que \prec é uma relação de ordem parcial.

3. Considere-se a seguinte relação, que denotamos por exemplo por \bowtie , em $\mathcal{P}(\mathbb{N})$: $X \bowtie Y$ se $X \Delta Y$ é um conjunto finito. Mostrar que \bowtie é uma relação de equivalência.

2 Números Naturais

O conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \dots, n, \dots\}$ e as suas propriedades mais elementares são familiares a todos:

1. Está definida uma operação de soma $a + b \in \mathbb{N}$.
2. Está definida uma operação de produto $a \times b = a \cdot b = ab \in \mathbb{N}$.
3. $a + b = b + a$.
4. $(a + b) + c = a + (b + c)$.
5. $a + b = a + c \implies b = c$.
6. $ab = ba$.
7. $(ab)c = a(bc)$.
8. $\exists 0 \in \mathbb{N} : a + 0 = a \forall a \in \mathbb{N}$.
9. $\exists 1 \in \mathbb{N} : n1 = n, \forall n \in \mathbb{N}$.
10. $ac = bc \wedge c \neq 0 \implies a = b$.
11. $a(b + c) = ab + ac$.

Definição 2.1 $a \leq b \iff \exists n \in \mathbb{N} : a + n = b$.

Usamos a notação $a < b$ com o significado $a \leq b \wedge a \neq b$ ou, de forma equivalente, $a < b \iff \exists n \in \mathbb{N} \setminus \{0\} : a + n = b$.

A relação \leq é evidentemente uma relação de ordem mas satisfaz além disso uma outra condição, que é mais uma das propriedades fundamentais de \mathbb{N} :

12. Se $a, b \in \mathbb{N}$ então verifica-se uma e uma só das condições

$$a < b, b < a, a = b.$$

Além disso,

$$a \leq b \wedge b \leq a \implies a = b$$

Uma relação de ordem com esta propriedade chama-se uma **relação de ordem total**.

Temos finalmente:

13. (*Boa Ordenação*): Se $X \subseteq \mathbb{N}$, $X \neq \emptyset$, então X tem um *primeiro elemento*, isto é

$$\exists x_0 \in X : x < x_0 \implies x \notin X$$

Note-se que, por exemplo, o conjunto dos racionais não negativos satisfaz todas as propriedades 1 – 12 mas não a 13.

Estas propriedades caracterizam completamente o conjunto dos números naturais, isto é, qualquer conjunto que as satisfaça é uma “cópia” de \mathbb{N} , sendo que a propriedade de Boa Ordenação é a crucial.

Veremos mais adiante que esta propriedade tem como consequência

13*. Se $X \subseteq \mathbb{N}$ satisfaz

i. $n_0 \in X$,

ii. $x \in X \implies x + 1 \in X$,

então $X = \mathbb{N}$

Nota 2.2 *É de facto possível definir o conjunto dos naturais do seguinte modo: \mathbb{N} é um conjunto satisfazendo as seguintes propriedades:*

1. *Existe um elemento $0 \in \mathbb{N}$;*

2. *Existe uma função (a função sucessor) injectiva $s : \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$;*

3. *Para qualquer subconjunto $C \subset \mathbb{N}$, se*

i. $0 \in C$,

ii. $\forall x \in \mathbb{N} \ x \in C \implies s(x) \in C$,

então $C = \mathbb{N}$.

A partir destas propriedades, que se tomam como axiomas, podem deduzir-se a existência das operações de soma e produto com todas as propriedades descritas atrás.

Notação 2.3 Usaremos a notação

$$[m] = \{x \in \mathbb{N} : x < m\} = \{0, \dots, m - 1\}$$

Com esta notação $[0] = \emptyset$.

Nota 2.4 De facto, nesta notação está presente uma ideia importante, a saber, a de que poderíamos definir o conjunto dos naturais a partir de noções elementares da teoria de conjuntos, pondo $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, e assim por diante.

2.1 Números Inteiros

Ainda que os números naturais sejam suficientes quando se trata de *contar* ou *ordenar* os elementos de conjuntos suficientemente simples, a necessidade de comparar números entre si e de realizar e compreender com clareza as operações aritméticas, conduz naturalmente à introdução do conjunto dos números inteiros

$$\mathbb{Z} = \{\dots, -n, \dots, -1, 0, 1, \dots, n, \dots\}$$

\mathbb{Z} satisfaz as propriedades 1-12 e fica completamente caracterizado se estabelecermos além disso que

- $\forall a \in \mathbb{Z}, \exists^1(-a) \in \mathbb{Z} : a + (-a) = 0$
- $\forall a \in \mathbb{Z}, a \in \mathbb{N} \vee -a \in \mathbb{N}$

Evidentemente, \mathbb{Z} não satisfaz a propriedade 13 (Princípio da Boa Ordenação). Mas para qualquer $a \in \mathbb{Z}$, o conjunto $\{n \in \mathbb{Z} : n \geq a\}$ já tem essa propriedade.

Os axiomas dos inteiros têm como consequência todas as propriedades bem conhecidas de que destacamos as seguintes

1. $0 \cdot a = 0, \forall a \in \mathbb{Z}$
2. $ab = 0 \implies a = 0 \vee b = 0$
3. $(-a)(-b) = ab$

O estudo mais aprofundado da aritmética dos inteiros será iniciado mais adiante.

Nota 2.5 *Em vez de o definirmos de forma axiomática, o conjunto \mathbb{Z} pode ser construído a partir do conjunto dos naturais da seguinte forma:*

Considere-se o conjunto $\mathbb{N} \times \mathbb{N}$ dos pares ordenados de números naturais, onde definimos a relação \mathcal{R} seguinte:

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow a + d = b + c.$$

Chamemos conjunto dos inteiros ao conjunto das classes de equivalência de \mathcal{R} . Portanto, de acordo com esta definição, um inteiro pode ser representado por um par $(a, b) \in \mathbb{N} \times \mathbb{N}$, mas também por qualquer outro par (c, d) tal que $(a, b)\mathcal{R}(c, d)$.

Esta definição, aparentemente artificial, ganha sentido quando pensamos, como se referiu acima, nos inteiros como o resultado de comparar naturais: o par (a, b) corresponde ao inteiro (no sentido habitual) $b - a$. Note-se que esta operação de subtração, não está bem definida para quaisquer $a, b \in \mathbb{N}$, mas apenas quando $a < b$. Assim, a relação de equivalência \mathcal{R} limita-se a exprimir, na linguagem dos naturais, que $b - a = d - c$ e que portanto ambos os pares (a, b) e (c, d) definem a mesma diferença de naturais.

Um par (a, b) representa um natural se $a < b$; o inteiro 0 é representado por qualquer par da forma (a, a) ; o simétrico do inteiro representado por (a, b) é representado por (b, a) .

Resta verificar como se devem definir as operações de soma e produto e a relação de ordem, o que se torna claro se seguimos a interpretação feita de identificar (a, b) com $b - a$:

$$(a, b) + (c, d) = (a + c, b + d)$$

já que

$$(b - a) + (d - c) = (b + d) - (a + c).$$

Do mesmo modo, como

$$(b - a)(d - c) = bd + ac - bc - ad = (bd + ac) - (ad + bc),$$

definimos o produto

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

onde as somas e produtos em cada entrada do par ordenado são as já definidas para os naturais.

E, seguindo a mesma ideia,

$$(a, b) < (c, d) \Leftrightarrow b + c < a + d.$$

O passo final, mas fundamental, desta construção reside em verificar que a definição das operações e da relação de ordem não dependem dos representantes escolhidos: temos de facto que recordar que nesta construção um inteiro não é um par de naturais mas sim uma classe de equivalência desses pares. É necessário portanto garantir que se

$$(a, b)\mathcal{R}(a', b'), \quad (c, d)\mathcal{R}(c', d')$$

se obtém o mesmo inteiro na soma $(a, b) + (c, d)$ que na soma $(a', b') + (c', d')$, e o mesmo para o produto ou para a relação de ordem. Fazemos essa verificação para a soma, deixando as outras como um exercício. Dizer que estas duas somas representam o mesmo inteiro é o mesmo que dizer que

$$((a, b) + (c, d))\mathcal{R}((a', b') + (c', d'));$$

mas, de acordo com a definição de soma a que chegámos anteriormente, isso equivale a

$$(a + c, b + d)\mathcal{R}(a' + c', b' + d')$$

ou seja

$$a + c + b' + d' = b + d + a' + c';$$

ora, como por hipótese

$$(a, b)\mathcal{R}(a', b'), \quad (c, d)\mathcal{R}(c', d'),$$

temos

$$a + b' = b + a' \quad c + d' = d + c'$$

e a igualdade anterior resulta consequência das propriedades da soma de naturais.

Um raciocínio semelhante permite construir o conjunto dos racionais e as suas propriedades, a partir de \mathbb{Z} . Encontraremos mais adiante uma outra situação em que definimos operações entre classes de equivalência a partir de operações nos inteiros.

2.2 Conjuntos finitos e infinitos

Os números naturais são o resultado da abstracção, desenvolvida pela humanidade ao longo de séculos, do acto de contar. Mais precisamente, o acto de contar, como quando conto os livros que tenho numa prateleira, 1, 2, 3, ..., começando, por exemplo, da esquerda para a direita, corresponde a estabelecer uma certa bijecção entre dois conjuntos: o conjunto dos livros na prateleira e um certo conjunto de números. Os números vieram assim substituir outros conjuntos (os dedos das mãos, os nós numa corda...) como conjunto padrão de contagem.

Definição 2.6 *Um conjunto X diz-se finito se existe $m \in \mathbb{N}$ e uma bijecção*

$$f : [m] \rightarrow X$$

Diz-se então que X tem m elementos ou que a cardinalidade de X é m , usando-se a notação $|X| = m$. Um conjunto X diz-se infinito se não for finito.

Pode-se formular estas definições de outros modos; o teorema seguinte ilustra esse facto.

Teorema 2.7 *Dado um conjunto X , as seguintes afirmações são equivalentes:*

- i) X é infinito;*
- ii) Existe uma função $f : \mathbb{N} \rightarrow X$ injectiva;*
- iii) Existe uma função $g : X \rightarrow X$ injectiva e não sobrejectiva.*

Demonstração 2.8 *Note-se que o conjunto \mathbb{N} satisfaz a condição iii): basta tomar*

$$g : \mathbb{N} \rightarrow \mathbb{N}, \quad f(n) = 2n.$$

Se um conjunto X satisfaz a condição ii), ou seja, existe $f : \mathbb{N} \rightarrow X$ injectiva, podemos definir $g : X \rightarrow X$ do seguinte modo

$$g(x) = \begin{cases} x & \text{se } x \notin f(\mathbb{N}) \\ f(2n) & \text{se } x = f(n) \end{cases}$$

que se verifica facilmente ser injectiva mas não sobrejectiva. Portanto ii) \implies iii).

Por outro lado se X satisfaz a condição iii) não pode ser finito; vamos provar isso por absurdo, supondo que existe algum conjunto finito que satisfaz iii); como um conjunto finito está em bijecção com $[n]$ para algum n , isso equivale a supôr que existe algum natural n e uma função $f : [n] \rightarrow [n]$ injectiva mas não sobrejectiva; ora, se isso fosse verdade, existiria, pelo Princípio da Boa Ordenação, um primeiro natural, chamemos-lhe c , com essa propriedade. Vamos chegar a um absurdo mostrando que, pelo contrário, $c - 1$ também teria que satisfazer iii). Note-se que se existisse, ter-se-ia de certeza $c > 1$.

Seja então

$$f : [c] \rightarrow [c]$$

uma função injectiva mas não sobrejectiva; há três casos possíveis:

Se $c - 1$ não pertence à imagem de f , chamemos f' à restrição de f a $\{0, \dots, c - 2\} = [c - 1]$; f' tem imagem contida em $\{0, \dots, c - 2\}$, é injectiva e, como supomos que f é injectiva, $f(c - 1) \notin f'(\{0, \dots, c - 2\})$.

Ou seja,

$$f' : [c - 1] \rightarrow [c - 1]$$

é injectiva e não sobrejectiva.

Se $f(c - 1) = c - 1$, a mesma restrição f' do caso anterior dá-nos uma função de $[c - 1]$ nele próprio, injectiva e não sobrejectiva.

Finalmente, suponhamos que existem $0 \leq a, b < c - 1$ tais que $f(a) = c - 1$ e $f(c - 1) = b$; nesse caso podemos modificar a função trocando estas duas

imagens, ou seja, definimos

$$g : [c] \rightarrow [c], \quad g(x) = \begin{cases} x & \text{se } x \notin \{a, c-1\} \\ b & \text{se } x = a \\ c-1 & \text{se } x = c-1 \end{cases}$$

e caímos no caso anterior.

Para completar a demonstração do teorema, tem que se provar que $i) \implies ii)$, o que se faz definindo recursivamente os valores de uma função $f : \mathbb{N} \rightarrow X$: se X é infinito então certamente não é vazio e podemos escolher um elemento $f(1)$; como $X \neq \{f(1)\}$ (caso contrário seria finito), podemos escolher $f(2) \in X \setminus \{f(1)\}$; e em geral, para qualquer $m \in \mathbb{N}$, depois de escolhidos $f(1), \dots, f(m)$, podemos escolher $f(m+1) \in X \setminus \{f(1), \dots, f(m)\}$. A função f assim definida é sem dúvida injectiva. Que este argumento garante de facto que temos uma função definida em \mathbb{N} decorre do Princípio da Boa Ordenação (se f não ficasse definida para todo o $n \in \mathbb{N}$, haveria um primeiro natural para o qual não estava definida e chegaríamos a uma contradição).

Nota 2.9 O argumento esboçado no último parágrafo da demonstração anterior é mais delicado do que possa parecer à primeira vista e remete-nos, mais uma vez, para os fundamentos da Teoria dos Conjuntos: o facto de que, dado um conjunto de conjuntos não vazios, existe uma função que escolhe um elemento de cada um deles, por muito intuitiva que possa ser, não pode ser provado a partir de noções mais elementares e tem que ser, num desenvolvimento rigoroso da Teoria dos Conjuntos, tomado como um axioma (o Axioma da Escolha), que se prova ser equivalente a muitas outras proposições, nem todas tão intuitivas.

Estes argumentos devem ser revistos depois de estudado mais à frente o Princípio de Indução Finita.

A generalização da definição de conjunto finito leva ao conceito geral de **cardinalidade**: dizemos que dois conjuntos X e Y têm a mesma cardinalidade se existe uma bijecção $f : X \rightarrow Y$ e que X tem cardinalidade menor ou igual à de Y se existe $f : X \rightarrow Y$ injectiva. Note-se que, para que seja

possível comparar de modo coerente as cardinalidades de diferentes conjuntos, é necessário demonstrar que se existem

$$f : X \rightarrow Y, \quad g : Y \rightarrow X$$

ambas injectivas, então X e Y têm a mesma cardinalidade; este resultado é o Teorema de Cantor-Schröder-Bernstein, cuja demonstração é esboçada num exercício.

Vamos apenas ilustrar este conceito, mostrando que \mathbb{N} e $\mathbb{N} \times \mathbb{N}$ têm a mesma cardinalidade:

Exemplo 2.10 *Consideremos a função*

$$h : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \quad h(m, n) = 2^m(2n + 1) - 1.$$

Notamos primeiro que h é sobrejectiva: qualquer natural positivo é o produto de uma potência de 2 e de um número ímpar; portanto, se $x \in \mathbb{N}$ e $x + 1 = 2^m(2n + 1)$, então $x = h(m, n)$.

Mas h é também injectiva: suponhamos que $h(m, n) = h(u, v)$, e portanto $2^m(2n + 1) = 2^u(2v + 1)$; se fosse, por exemplo, $u > m$, teríamos $(2n + 1) = 2^{u-m}(2v + 1)$ que seria a igualdade entre um número ímpar e um par, absurdo; logo $m = u$ e portanto $2n + 1 = 2v + 1$, ou seja, $n = v$.

Exercícios I.4

1. Dado um conjunto X mostrar que

- existe uma bijecção entre o conjunto $\mathcal{P}(X)$ dos subconjuntos de X e o conjunto $\{f : X \rightarrow \{0, 1\}\}$ das funções com domínio X e contradomínio $\{0, 1\}$.
- não existe uma função $\phi : X \rightarrow \mathcal{P}(X)$ sobrejectiva.

Sugestão: dada uma função qualquer $\phi : X \rightarrow \mathcal{P}(X)$, considerar o conjunto $Y = \{x \in X \mid x \notin \phi(x)\} \in \mathcal{P}(X)$.

Supondo que este conjunto pertence à imagem de ϕ , isto é, existe $x_0 \in X$ tal que $\phi(x_0) = Y$, será que $x_0 \in Y$?

2. Este exercício é um guia para a demonstração do

Teorema 2.11 (Teorema de Cantor-Schröder-Bernstein) *Para quaisquer conjuntos A e B , se existem funções injectivas*

$$f : A \rightarrow B, \quad g : B \rightarrow A,$$

então existe uma bijecção $h : A \rightarrow B$.

- a) Justificar que basta considerar o caso em que $B \subset A$ e g é a inclusão;
- b) Definem-se recursivamente conjuntos $C_i \subset A$ do seguinte modo:

$$\begin{cases} C_0 = A \setminus B \\ C_{n+1} = f(C_n) \forall n \in \mathbb{N} \end{cases}$$

e $h : A \rightarrow B$ por

$$h(x) = \begin{cases} f(x) & \text{se } x \in \bigcup_{n \geq 0} C_n \\ x & \text{no caso contrário} \end{cases}$$

- c) Provar que se $x, y \in A$ e $x \neq y$ então $h(x) \neq h(y)$ (h é injectiva) separando os diferentes casos: $x, y \in \bigcup_{n \geq 0} C_n$; $x, y \in A \setminus (\bigcup_{n \geq 0} C_n)$; $x \in \bigcup_{n \geq 0} C_n$ e $y \in A \setminus (\bigcup_{n \geq 0} C_n)$;
 - d) Provar que h é sobrejectiva.
3. Usar o Teorema de Cantor-Schröder-Bernstein para mostrar que \mathbb{Q} tem a mesma cardinalidade de $\mathbb{N} \times \mathbb{N}$ e portanto de \mathbb{N} .

3 Princípio de Indução Finita

Como foi já referido, uma consequência importante do Princípio da Boa Ordenação é o seguinte

Teorema 3.1 *Se $X \subset \mathbb{N}$ satisfaz as condições*

- (i) : $k_0 \in X$,
- (ii) : $k \geq k_0, k \in X \implies k + 1 \in X$,

então

$$X \supset \mathbb{N} \setminus [k_0].$$

Demonstração 3.2 *De facto, se o conjunto $Y = \{x \in \mathbb{N} \mid x \geq k_0 \wedge x \notin X\}$ não for vazio, tem que ter, pelo Princípio da Boa Ordenação, um primeiro elemento, chamemos-lhe a . Como $k_0 \in X$, tem-se $k_0 < a$ e portanto $k_0 \leq a - 1$; por outro lado $a - 1 \in X$ uma vez que a é o primeiro elemento do conjunto Y definido atrás.*

Mas a condição ii) do teorema implica então que $a \in X$, uma contradição. Esta contradição decorre de supormos que $Y \neq \emptyset$.

Nota 3.3 *O teorema anterior é de facto logicamente equivalente ao Princípio da Boa Ordenação: vamos assumir que \mathbb{N} tem a propriedade descrita no teorema e seja $X \subset \mathbb{N}$ um conjunto não vazio; queremos mostrar que X tem um primeiro elemento, ou seja, usando a notação entretanto introduzida, queremos provar que existe $x \in X$ tal que $[x] \subset \mathbb{N} \setminus X$. Consideremos o conjunto $C \subset \mathbb{N}$ definido por $C = \{n \in \mathbb{N} : [n] \subset \mathbb{N} \setminus X\}$; temos que $0 \in C$ por definição, mas, como $X \neq \emptyset$, $C \neq \mathbb{N}$, logo terá que existir algum $m \in C$ tal que $m + 1 \notin C$; mas isso significa que $[m] \subset \mathbb{N} \setminus X$ enquanto que $[m + 1] \not\subset \mathbb{N} \setminus X$; como $[m + 1] = [m] \cup \{m\}$, deduzimos que $m \in X$ e como $[m] \subset \mathbb{N} \setminus X$, m é o primeiro elemento de X .*

Este teorema é frequentemente usado da seguinte forma:

3.4 Princípio de Indução Finita: *Se $P(n)$ é uma dada afirmação referente aos números naturais $n \in \mathbb{N}$ tal que :*

i: $P(k_0)$ é verdadeira;

ii: se $k \geq k_0$ e $P(k)$ é verdadeira então $P(k + 1)$ é verdadeira;

então $P(n)$ é verdadeira para qualquer $n \geq k_0$.

Exemplo 3.5 *Ilustramos a aplicação do Princípio de Indução Finita através de um exemplo simples: provar por indução que a igualdade*

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

se verifica para todo o $n \geq 1$.

Começamos por verificar que a igualdade se verifica para $n = 1$, o que é imediato.

Em seguida mostramos que, se a igualdade se verificar para um certo natural n então também se verifica para $n + 1$: de facto, se

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

então

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \left(\sum_{k=1}^n k \right) + (n+1) = \\ &= \frac{n(n+1)}{2} + n+1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

ou seja a igualdade é igualmente válida para $n+1$ como queríamos mostrar. O passo essencial na dedução feita está na segunda igualdade, onde usamos a hipótese de que a igualdade se verifica para n para substituir o somatório $\sum_{k=1}^n k$ por $\frac{n(n+1)}{2}$.

Exemplo 3.6 *Dado $r \neq 1$, provar por indução a fórmula para a soma dos termos de uma progressão geométrica com primeiro termo 1 e razão r :*

$$1 + r + r^2 + \dots + r^n = \sum_{k=0}^n r^k = \frac{1 - r^{n+1}}{1 - r} \quad \forall n \geq 0$$

Mais uma vez, a igualdade é obviamente verdadeira para $n = 0$; de modo semelhante ao do exemplo anterior, se a fórmula é verdadeira para um natural n então, para $n + 1$ temos

$$\begin{aligned} \sum_{k=0}^{n+1} r^k &= \sum_{k=0}^n r^k + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1} = \\ &= \frac{1 - r^{n+1} + (1 - r)r^{n+1}}{1 - r} = \frac{1 - r^{n+2}}{1 - r} \end{aligned}$$

ou seja, a fórmula verifica-se também para $n + 1$.

Ainda como um terceiro exemplo (que tem a particularidade de ter sido a primeira exposição escrita, pelo matemático francês Pascal, da aplicação do Princípio de Indução Finita), provamos a chamada:

Proposição 3.7 Fórmula do Binómio

$$\forall a, b \in \mathbb{R}, \forall n \in \mathbb{N} (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

onde

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

e $n! = 1 \times 2 \times 3 \times \dots \times n$ ou mais precisamente $n! = \prod_{j=1}^n j$ (por convenção $0! = 1$).

Demonstração 3.8 Para simplificar a nossa dedução, convém alargar a definição dos números binomiais $\binom{n}{k}$ a todos os valores inteiros de k :

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{se } 0 \leq k \leq n \\ 0 & \text{se } k < 0 \vee n < k \end{cases}$$

Esta generalização permite reescrever a fórmula como

$$(a + b)^n = \sum_k \binom{n}{k} a^k b^{n-k}$$

onde o símbolo \sum_k significa que o índice k toma todos os valores inteiros: esta soma de “um número infinito” de termos é definida como a soma dos termos não nulos.

Mais uma vez os casos $n = 0$ ou $n = 1$ são de verificação imediata; a demonstração de que a validade da fórmula para um certo n implica a sua validade para $n + 1$ é um pouco mais complicada que a dos exemplos anteriores e faz-se do seguinte modo: supondo então que

$$(a + b)^n = \sum_k \binom{n}{k} a^k b^{n-k}$$

temos

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \sum_k \binom{n}{k} a^k b^{n-k} = \\ &= \sum_k \binom{n}{k} a^{k+1} b^{n-k} + \sum_k \binom{n}{k} a^k b^{n+1-k} = \end{aligned}$$

fazendo $j = k + 1$ no primeiro somatório,

$$= \sum_j \binom{n}{j-1} a^j b^{n+1-j} + \sum_k \binom{n}{k} a^k b^{n+1-k} =$$

designando de novo por k o índice do primeiro somatório,

$$\begin{aligned} &= \sum_k \binom{n}{k-1} a^k b^{n+1-k} + \sum_k \binom{n}{k} a^k b^{n+1-k} = \\ &= \sum_k \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} = \sum_k \binom{n+1}{k} a^k b^{n+1-k} \end{aligned}$$

onde a última igualdade é justificada por

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} =$$

$$\frac{n!k}{k!(n+1-k)!} + \frac{n!(n+1-k)}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!}$$

que é a conhecida propriedade do triângulo de Pascal (fica só por comprovar a igualdade nos casos $k < 1$ e $k > n$, o que é simples).

Nota 3.9 os exemplos anteriores, além de servirem de ilustração da aplicação do Princípio de Indução Finita, são importantes pelos resultados em si, que são igualdades, principalmente as duas últimas, que devem ser conhecidas.

Antes de dar outro exemplo convém desde já fazer algumas observações:

- É muito natural perguntar “de onde vem” a fórmula que é enunciada para provar. Ou seja, aparentemente, para provar uma certa proposição através do Princípio de Indução Finita, é preciso saber já o que se vai provar.

Em muitos casos o resultado a provar é sugerido por cálculos em casos particulares ou por um raciocínio menos rigoroso. O Princípio de Indução Finita serve então para comprovar a conjectura formulada.

Mas é verdade que muitos dos resultados que provamos por aplicação do Princípio de Indução Finita podem ser provados com outras abordagens. Um exemplo disso é a dedução da igualdade do primeiro exemplo apresentada num exercício.

- O Princípio de Indução Finita é por vezes mal entendido como um mero artifício formal; a necessidade de provar

$$P(k) \text{ é verdadeira} \implies P(k+1) \text{ é verdadeira}$$

para finalmente concluir que $P(k)$ é verdadeira (para todo o $k \geq k_0$, claro) pode criar a ideia errada de que estamos a admitir antecipadamente o resultado que queremos provar.

Na verdade, o que se prova naquele passo é a implicação. Como se sabe, o facto de uma implicação $a \implies b$ entre duas proposições ser verdadeira significa apenas que *se* a for verdadeira então b é verdadeira: formalmente o valor lógico de $a \implies b$ é o mesmo de $(\neg a) \vee b$, onde \neg significa negação, e esta proposição só é falsa se a for verdadeira e b falsa.

É por isso que a prova da implicação tem que ser acompanhada pela verificação de que $P(k_0)$ é verdadeira. Uma boa maneira de compreender isso é através do seguinte exemplo: suponhamos que, devido a uma gralha, o primeiro exemplo acima é enunciado assim: provar por indução que

$$\sum_{k=1}^n k = \frac{n^2 + n + 1}{2} \forall n \geq 1;$$

se assumirmos que a igualdade é verdadeira para um certo n então temos, para $n + 1$.

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \sum_{k=1}^n k + (n + 1) = \\ &= \frac{n^2 + n + 1}{2} + (n + 1) = \frac{n^2 + n + 1 + 2(n + 1)}{2} = \\ &= \frac{n^2 + 3n + 3}{2} = \frac{(n^2 + 2n + 1) + n + 2}{2} = \frac{(n + 1)^2 + (n + 1) + 1}{2}; \end{aligned}$$

provámos portanto que *se* a igualdade se verifica para n também se verifica para $n + 1$, ou seja, verificámos a segunda condição para a aplicação do Princípio de Indução Finita. No entanto, aquela igualdade é obviamente falsa.

Exercícios I.5

1. "Adivinhar", calculando os primeiros casos, uma fórmula para cada uma das seguintes somas e demonstrá-las :

- a) $1 + 3 + 5 + \dots + (2n - 1) = \sum_{k=1}^n (2k - 1)$;

$$\text{b) } 1^3 + 2^3 + 3^3 + \cdots + n^3 = \sum_{k=1}^n k^3;$$

2. Determinar experimentalmente uma relação de recorrência satisfeita pelo número máximo (que designamos R_n) de regiões definidas por n rectas no plano. Obter uma fórmula fechada para R_n e demonstrar a sua validade.
3. Analisar a seguinte dedução da fórmula

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

justificando cada um dos passos:

$$\sum_{k=1}^{n+1} k^2 = \sum_{k=0}^n (k+1)^2 = \sum_{k=1}^n k^2 + 2 \sum_{k=1}^n k + (n+1)$$

Portanto

$$2 \sum_{k=1}^n k = (n+1)^2 - (n+1) = n(n+1)$$

Determinar, usando o mesmo método, uma fórmula fechada para a soma:

$$S_n = \sum_{k=0}^n k^2.$$

4. (*Números de Fibonacci*) Considerar a sucessão de inteiros definida por recorrência por

$$\begin{aligned} F_1 &= 1; F_2 = 1; \\ F_n &= F_{n-1} + F_{n-2}, \quad n > 2. \end{aligned}$$

F_n é chamado o n -ésimo número de Fibonacci.

a) Provar que

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$$

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$$

b) "Adivinhar" e demonstrar identidades para as seguintes expressões:

$$F_2 + F_4 + F_6 + \cdots + F_{2n} = ???; \quad F_{n+1}^2 - F_n F_{n+2} = ???$$

5. O jogo das Torres de Hanoi consiste no seguinte: existem três casas e uma pilha de n discos, de tamanhos decrescentes da base para o topo, na primeira casa; pretende-se mover a pilha para a terceira casa, cumprindo as seguintes regras: só se pode mover um disco de cada vez; não se podem colocar discos maiores sobre discos menores.

Qual é o menor número de movimentos (dependente de n , claro) necessário para terminar o jogo?

6. Demonstrar que, para todo o $n \geq 1$,

$$2(\sqrt{n+1} - 1) < \sum_{k=1}^n \frac{1}{\sqrt{k}} < 2\sqrt{n}.$$

7. Consegue provar por indução em n que

$$\forall n \in \mathbb{N} : \quad \frac{1}{2} \frac{3}{4} \cdots \frac{2n-1}{2n} = \prod_{k=1}^n \frac{2k-1}{2k} < \frac{1}{\sqrt{3n}} ?$$

E se fôr

$$\forall n \in \mathbb{N} : \quad \frac{1}{2} \frac{3}{4} \cdots \frac{2n-1}{2n} = \prod_{k=1}^n \frac{2k-1}{2k} < \frac{1}{\sqrt{3n+1}} ?$$

8. Demonstrar que, para todo o $n \geq 2$,

$$\sum_{k=1}^n \frac{1}{k^2} \leq \frac{7}{4} - \frac{1}{n}.$$

9. Mostrar que é possível colorir com duas cores as regiões planas definidas por n circunferências, de modo a que regiões com um arco de fronteira comum tenham cores diferentes.

10. Mostrar que, dados n quadrados, é possível recortá-los em polígonos de modo a formar com estes um novo quadrado.

Sugestão: O único caso difícil é $n = 2$.

11. a) Provar por indução que, para todo o $n \geq 1$,

$$\sum_{k=1}^n \frac{1}{k(k+2)} = \frac{n(3n+5)}{4(n+1)(n+2)};$$

b) Deduzir (sem usar indução) uma fórmula semelhante para a soma $\sum_{k=1}^n \frac{1}{k(k+p)}$ onde p é um inteiro positivo .

Sugestão: $\frac{1}{k(k+p)} = \frac{1}{p} \left(\frac{1}{k} - \frac{1}{k+p} \right)$.

12. Demonstrar que se $-1 < a_i < 0$, para todo o $1 \leq i \leq n$, então

$$\prod_{i=1}^n (1 + a_i) \geq 1 + \sum_{i=1}^n a_i.$$

13. Demonstrar, por indução em n , que

$$\forall n \in \mathbb{N} (b_i > 0 \forall i \leq n \wedge \prod_{i=1}^n b_i = 1) \Rightarrow \sum_{i=1}^n b_i \geq n$$

Nota: $\prod_{i=1}^n b_i$ designa o produto dos b_i , com $1 \leq i \leq n$.

Sugestão: Se $b_i = 1 \forall i$, o resultado é evidente; caso contrário, notar que se $b_1, b_2, b_3, \dots, b_{n+1}$ são $n+1$ reais positivos tais que $\prod_{i=1}^{n+1} b_i = 1$, então $b_1 b_2, b_3, \dots, b_{n+1}$ são n reais positivos cujo produto é 1; podemos supôr

além disso que, por exemplo, $b_1 < 1 < b_2$; mostrar que se $0 < a < 1 < b$, então $ab < a + b - 1$.

14. Usar o resultado do problema anterior para demonstrar o seguinte: dados n números reais positivos a_i , $1 \leq i \leq n$, verificam-se as desigualdades

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$$

ou seja, usando a notação para somatórios e produtos,

$$\frac{n}{\sum_{i=1}^n \frac{1}{a_i}} \leq \sqrt[n]{\prod_{i=1}^n a_i} \leq \frac{\sum_{i=1}^n a_i}{n}$$

As fórmulas acima representam, respectivamente, as médias harmónica, geométrica e aritmética dos números a_i , $1 \leq i \leq n$.

15. Usar as desigualdades do exercício anterior para provar

- a) $\sum_{k=0}^n \frac{1}{n+k} > \frac{2}{3} \forall n \geq 1$;
 b) $\sum_{k=0}^{2n+1} \frac{1}{n+k} > 1 \forall n \geq 1$;

Uma outra forma equivalente e por vezes de aplicação mais directa do Princípio de Indução Finita é a seguinte:

3.10 Princípio de Indução Finita ("FORTE"):

Se $P(n)$ é uma dada afirmação referente aos números naturais $n \in \mathbb{N}$ tal que :

i : $P(k_0)$ é verdadeira;

ii : $k \geq k_0$ e $P(k_0), P(k_0 + 1), \dots, P(k)$ verdadeiras, implica que $P(k + 1)$ é verdadeira;

então $P(n)$ é verdadeira para qualquer $n \geq k_0$.

O argumento da demonstração da equivalência dos dois resultados é resumidamente este: O Princípio de Indução Finita ("FORTE") implica o Princípio de Indução Finita, uma vez que se $P(k) \implies P(k+1)$ então também

$$P(k_0) \wedge P(k_0 + 1) \wedge \cdots \wedge P(k) \implies P(k + 1);$$

portanto, se as condições do Princípio de Indução Finita estão satisfeitas também as do Princípio de Indução Finita ("FORTE") o estão.

Mas reciprocamente o Princípio de Indução Finita implica o Princípio de Indução Finita ("FORTE"): aplicar este último a $P(k)$ é o mesmo que aplicar o Princípio de Indução Finita a $Q(k) \Leftrightarrow P(k_0) \wedge \cdots \wedge P(k)$.

Exemplo 3.11 *Como aplicação desta forma do princípio considere-se o seguinte exemplo: seja x_n a sucessão definida pela seguinte recorrência*

$$x_0 = 0, x_1 = 1; \quad x_{n+1} = 2x_n - x_{n-1} \quad \forall n > 1$$

Calculando $x_2 = 2$, $x_3 = 3$, somos naturalmente levados a conjecturar que se tem $x_n = n$ para todo o $n \geq 0$. Como o termo de ordem $n+1$ é definido à custa dos dois termos anteriores, é mais fácil fazer a demonstração através do Princípio de Indução Finita ("FORTE"): o caso $n = 0$ é estabelecido pela própria definição da sucessão; supondo agora que $x_k = k$ para todo o $k \leq n$, concluímos facilmente que temos

$$x_{n+1} = 2x_n - x_{n-1} = 2n - (n - 1) = n + 1$$

Exercício 3.12 *Usar o Princípio de Indução Forte para demonstrar que a soma dos ângulos internos de um polígono convexo com n lados é $(n - 2)\pi$.*

Nota 3.13 (Definições por recorrência) *A ideia da definição recursiva de uma sucessão, em que cada termo é definido em função de um ou mais termos anteriores, foi já referida informalmente e é de grande importância.*

Uma sucessão com termos num conjunto X não é mais do que uma função $f : \mathbb{N} \rightarrow X$, usualmente apresentada na forma $f(n) = x_n$; quando definimos a recursão $x_{n+1} = F(x_n)$,

ou seja, $f(n+1) = F(f(n))$, com um certo valor inicial x_0 , deve notar-se que, logicamente, estamos a admitir já a existência da função que queremos definir.

Uma dedução mais rigorosa da existência dessas funções pode ser feita do seguinte modo: seja $F : X \rightarrow X$ uma função qualquer e $x_0 \in X$. Provamos por indução que para todo o $n > 0$ existe uma única função $f_n : [n] \rightarrow X$ satisfazendo as propriedades

- $f_n(0) = x_0$;
- $f_n(k+1) = F(f_n(k)) \quad \forall k < n-1$.

Fica claro que se $n < m$ a função f_n é a restrição de f_m a $[n]$. Definimos então $f : \mathbb{N} \rightarrow X$ pela igualdade $f(n) = f_m(n)$ para qualquer $m > n$; se virmos cada função como uma relação, isto é, como um conjunto de pares ordenados $(k, f_n(k)) \in \mathbb{N} \times X$, podemos simplesmente dizer que definimos f como sendo a união das f_n ; prova-se então que f é a única função com domínio \mathbb{N} e contradomínio X que satisfaz aquelas propriedades, ou seja, temos o teorema seguinte:

Teorema 3.14 (Teorema da Recursão Finita) *Seja X um conjunto, $x_0 \in X$, e $F : X \rightarrow X$ uma função. Então existe uma única função $f : \mathbb{N} \rightarrow X$ tal que*

- $f(0) = x_0$;
- $f(n+1) = F(f(n)) \quad \forall n \in \mathbb{N}$.