A teoria informal de conjuntos é, apesar das dificuldades que ilustrámos anteriormente, suficientemente precisa para abordar as questões que tradicionalmente ocorrem na Matemática ordinária, e.g. na análise ou na álgebra. Assim sendo, iremos situar-nos neste nível informal.

Até agora mantivemos a possibilidade de as designações «objecto» e «conjunto» poderem significar coisas diferentes, ou seja, mantivemos em aberto a possibilidade de considerar objectos outros que não conjuntos. Embora a escolha possa não parecer imediatamente óbvia para o leitor, assumiremos de agora em diante que *os únicos objectos em consideração na teoria informal de conjuntos são conjuntos*. Isto significa que poderemos apenas formar conjuntos com outros conjuntos. Pelo que foi exposto até agora, o único objecto que pode ser considerado um conjunto é o conjunto vazio. Deste modo, se pretendemos reduzir todo o «universo matemático» à noção de conjunto temos que descrever operações que permitam gerar um universo rico ao ponto de servir aquele propósito, tendo como ponto de partida $\varnothing$.

Uma dessas operações é a operação de *formação de pares não ordenados*. Trata-se da operação que associa a conjuntos x e y o conjunto cujos elementos são exactamente x e y, conjunto esse que denotamos por $\{x, y\}$. (Observe-se que se $x = y$ então $\{x, y\} = \{x\} = \{y\}$ pelo que não devemos tomar aqui a palavra «par» num sentido demasiado restritivo.)

Só com esta operação já nos é possível descrever uma variedade de conjuntos, e.g., $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, etc.

Existem outras operações sobre conjuntos que são de uso corrente em matemática e que facilmente se integram na concepção cantoriana de formação de conjuntos. Exemplos disso são as operações de *união* e *intersecção*. Dados dois conjuntos A e B, a respectiva união, que se denota por $A \cup B$ é o conjunto cujos elementos são os conjuntos que pertencem a pelo menos um dos conjuntos A ou B, i.e., $A \cup B = \{x \mid x \in A \vee x \in B\}$. Já a intersecção de A e B é o conjunto constituído pelos elementos que são comuns a A e B, i.e., $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Estas operações admitem generalizações que, por serem interessantes, iremos descrever a seguir. Dado um conjunto X denotamos por $\cup X$, o conjunto que se designa por *união de* X e que é, $\cup X = \{a \mid (\exists u \in X) a \in u\}$.[1] (Por convenção $\cup\varnothing = \varnothing$.)

Analogamente, a *intersecção de* X é o conjunto, $\cap X = \{a \mid (\forall u \in X) a \in u\}$ (neste caso com $X \neq \varnothing$).[2]

Continuamos a descrever outras operações entre conjuntos. A *diferença* entre dois conjuntos é o conjunto $A - B = \{x \mid x \in A \text{ e } x \notin B\}$. A operação $A - B$ também se representa por $A \setminus B$. Por vezes é importante considerar a *diferença simétrica* de dois conjuntos A e B, que se denota por $A \Delta B$ e é, $A \Delta B = (A - B) \cup (B - A)$.

[1] Quantificações do tipo $(\exists x \in y)\phi$ abreviam fórmulas do tipo $(\exists x)[x \in y \wedge \phi]$.

[2] Quantificações do tipo $(\forall x \in y)\phi$ abreviam fórmulas do tipo $(\forall x)[x \in y \Rightarrow \phi]$.

As operações que descrevemos até ao momento bastam para descrever objectos que são de particular interesse, na medida em que representam os elementos de uma «estrutura matemática» muito importante.

Definição 3.1.— *Dado um conjunto x, o* sucessor *de x é o conjunto que se denota por $S(x)$ e que se define através de $S(x) = x \cup \{x\}$.*

Esta operação de *sucessor de um conjunto*, que acabámos de descrever, permite-nos definir a seguinte sequência de conjuntos:

$$\varnothing, S(\varnothing), S(S(\varnothing)), S(S(S(\varnothing))), S(S(S(S(\varnothing)))), \ldots \textit{ ad infinitum}. \tag{3.1}$$

A sequência anterior obtém-se, partindo de $\varnothing$ e iterando a operação *sucessor*.

Definição 3.2.— *Se Γ é uma operação que associa a cada conjunto x um outro conjunto $\Gamma(x)$ então, a n-ésima iteração de Γ define-se iterativamente através das seguintes relações:*

1. $\Gamma^0(x) = x$;
2. $\Gamma^{n+1}(x) = \Gamma(\Gamma^n(x))$.[3]

[3] Tem-se então que $\Gamma^0(x) = x$; $\Gamma^1(x) = \Gamma(x)$; $\Gamma^2(x) = \Gamma(\Gamma(x))$; $\Gamma^3(x) = \Gamma(\Gamma(\Gamma(x)))$; etc.

A sequência (3.1) pode ser então descrita do modo seguinte:

$$S^0(\varnothing), S^1(\varnothing), S^2(\varnothing), S^3(\varnothing), S^4(\varnothing), \ldots \textit{ ad infinitum}.$$

Simplificando ainda mais a notação e denotando por $\ulcorner n \urcorner$ o conjunto $S^n(\varnothing)$, obtemos a sugestiva sequência:

$$\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner 2 \urcorner, \ulcorner 3 \urcorner, \ulcorner 4 \urcorner, \ldots \textit{ ad infinitum}. \tag{3.2}$$

A notação que utilizámos pode sugerir que estes conjuntos se podem de alguma forma identificar com os números naturais. Alertamos o leitor para o facto de uma tal identificação, baseada meramente numa certa proximidade notacional é prematura. Os números naturais possuem uma estrutura e, a identificação mencionada só é legítima, se estes conjuntos que agora descrevemos puderem reproduzir essa mesma estrutura. Como veremos, isso acontece.

Comecemos por notar algumas propriedades interessantes da sequência (3.2). Calculando explicitamente os conjuntos $\ulcorner n \urcorner$ temos que:

$\ulcorner 0 \urcorner = \varnothing$;
$\ulcorner 1 \urcorner = \{\varnothing\}$;
$\ulcorner 2 \urcorner = \{\varnothing, \{\varnothing\}\}$;
$\ulcorner 3 \urcorner = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$;
$\ulcorner 4 \urcorner = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}$;
$\vdots$
ad infinitum

Ou, visto de outro modo,

$\ulcorner 0 \urcorner = \varnothing$;
$\ulcorner 1 \urcorner = \{\ulcorner 0 \urcorner\}$;

$\ulcorner 2 \urcorner = \{\ulcorner 0 \urcorner, \ulcorner 1 \urcorner\}$;
$\ulcorner 3 \urcorner = \{\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner 2 \urcorner\}$;
$\ulcorner 4 \urcorner = \{\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner 2 \urcorner, \ulcorner 3 \urcorner\}$;
$\vdots$
ad infinitum

A partir destes cálculos é fácil verificar algumas propriedades interessantes.

1. A sequência (??) pode ser linearmente ordenada usando a relação de pertença:

$$\ulcorner 0 \urcorner \in \ulcorner 1 \urcorner \in \ulcorner 2 \urcorner \in \ulcorner 3 \urcorner \in \ulcorner 4 \urcorner \in \cdots$$

   Mais precisamente, tem-se que $m < n$ se e só se $\ulcorner m \urcorner \in \ulcorner n \urcorner$. A mesma relação de ordem pode ser obtida usando a inclusão em vez da relação de pertença, uma vez que se tem $\ulcorner n \urcorner \in \ulcorner m \urcorner$ sse $\ulcorner n \urcorner \subset \ulcorner m \urcorner$, ou seja:

$$\ulcorner 0 \urcorner \subset \ulcorner 1 \urcorner \subset \ulcorner 2 \urcorner \subset \ulcorner 3 \urcorner \subset \ulcorner 4 \urcorner \subset \cdots .$$

2. Cada $\ulcorner n \urcorner$ é o conjunto dos $\ulcorner k \urcorner$ que o precedem na ordenação descrita em 1.

3. $S(\ulcorner n \urcorner) = \ulcorner n + 1 \urcorner$, i.e., $S(\ulcorner 0 \urcorner) = \ulcorner 1 \urcorner$; $S(\ulcorner 1 \urcorner) = \ulcorner 2 \urcorner$; $S(\ulcorner 2 \urcorner) = \ulcorner 3 \urcorner$; etc.

Vamos assumir que os conjuntos possuem uma propriedade designada de *propriedade da boa-fundação*. Essa propriedade estabelece que dado um qualquer conjunto não vazio X, existe $a \in X$ tal que $(\forall u \in X) a \cap u = \varnothing$. A introdução deste princípio impede que existam sequências infinitas:

$$x_1 \ni x_2 \ni \cdots \ni x_n \ni x_{n+1} \ni \cdots, \textit{ad infinitum.}$$

Podemos admitir este princípio sem introduzir nenhuma restrição fundamental ao desenvolvimento da matemática. Por outro lado a consideração deste princípio introduz certas vantagens técnicas importantes e esa é a grande razão para o considerarmos. Mas não entraremos aqui em grandes detalhes acerca deste ponto de vista.

Definição 3.3.— *Um conjunto X é* transitivo *se qualquer elemento de X é também um subconjunto de X, i.e., se $a \in X$ então $a \subset X$.*

Definição 3.4.— *Um conjunto transitivo cujos elementos são transitivos diz-se um* ordinal.

4. Os conjuntos $\ulcorner n \urcorner$ são ordinais.

Vamos denotar por ω o conjunto cujos elementos são exactamente os conjuntos da forma $\ulcorner n \urcorner$, ou seja os conjuntos que se obtém de $\varnothing$ iterando a operação de sucessor um número finito de vezes.

3.0.1 Relações e funções

Noções matemáticas fundamentais como o são as de *relação* e de *função* dependem de uma outra, a noção de *par ordenado*. O par ordenado em que a *primeira componente* é x e a *sgunda componente* é y denota-se por $\langle x, y \rangle$. A nossa terminologia sugere que existe uma

ordem associada a cada par ordenado e, de facto, a característica fundamental dos pares ordenados pode traduz-se no seguinte: $\langle x, y\rangle = \langle z, w\rangle$ se e só se $x = z$ e $y = w$. Veremos agora como implementar esta noção no seio da teoria de conjuntos. Recorremos à seguinte definição de Winner e Kuratowsky:

$$\langle x, y\rangle := \{\{x\}, \{x, y\}\}. \tag{3.3}$$

Podemos iterar esta construção de modo a obter *triplos ordenados*, *quádruplos ordenados*, etc., de acordo com o seguinte: $\langle x, y, z\rangle = \langle x, \langle y, z\rangle\rangle$, $\langle x, y, z, w\rangle = \langle x, \langle y, z, w\rangle\rangle$ e, de um modo geral,

$$\langle x_1, x_2, \dots, x_n\rangle = \langle x_1, \langle x_2, \dots, x_n\rangle\rangle. \tag{3.4}$$

(O conjunto $\langle x_1, x_2, \dots, x_n\rangle$ diz-se um n-úplo ordenado.)

Dados conjuntos $A_1, A_2, \dots, A_n$ o *produto cartesiano* $A_1 \times A_2 \times \cdots \times A_n$ é o conjunto,

$$A_1 \times A_2 \times \cdots \times A_n := \{\langle a_1, a_2, \dots, a_n\rangle \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Definição 3.5.— *Uma* relação *é um conjunto R de pares ordenados. O* domínio *de R é o conjunto* $\mathrm{dom}(R) = \{x \mid \langle x, y\rangle \in R, \text{para algum } y\}$. *O contradomínio de R é o conjunto,* $\mathrm{rng}(R) = \{y \mid \langle x, y\rangle \in R, \text{para algum } x\}$, *(a expressão «*rng*» abrevia a locução inglesa «range».)*

Qualquer relação R tem uma *inversa* que se denota por R^{-1} e que se define de acordo com o seguinte: $R^{-1} = \{\langle y, x\rangle \mid \langle x, y\rangle \in R\}$.

Entre as relações R existem algumas que satisfazem a condição adicional de que para qualquer x existe um único y tal que $\langle x, y\rangle \in R$. As relações que satisfazem esta condição dizem-se funções. Assim, uma função f de A para B é uma relação $f \subset A \times B$ que satisfaz a condição adicional acima mencionada. (Note-se que, neste caso $\mathrm{dom}(f) = A$ e $\mathrm{rng}(f) \subset B$. Para indicar que f é uma função de A para B escrevemos $f : A \to B$.

Se R é uma relação, escrevemos xRy em lugar de escrever $\langle x, y\rangle \in R$. No que diz respeito a funções $f : A \to B$, em vez de escrever $\langle x, y\rangle \in f$ escrevemos $y = f(x)$ (neste caso y diz-se a *imagem de x por f*).

Se $f : A \to B$ e $X \subset A$ a restrição de f a X denota-se $f \restriction X$ e é a função

$$f \restriction X = \{\langle x, y\rangle \mid \langle x, y\rangle \in f \text{ e } x \in X\}.$$

(Observe-se que $f \restriction X = f \cap X \times B$.)

Continuando a considerar $X \subset A$ a *imagem de X por f* denota-se por $f''X$ e é o conjunto $f''X = \{f(x) \mid x \in X\}$. (Observe-se que $f''X = \mathrm{rng}(f \restriction X)$.)

Uma função $f : A \to B$ é *injectiva* se a relação $f(x) = f(y)$ implica que $x = y$ (ou seja objectos diferentes possuem imagens diferentes). É importante observar que f é injectiva se e só se f^{-1}, que é sempre uma relação, é também uma função. Se todo o elemento de B é imagem de algum elemento da A então f diz-se *sobrejectiva*. Dito de outro modo $f : A \to B$ é sobrejectiva se $f''A = B$. Se f é ao mesmo tempo injectiva e sobrejectiva diz-se bijectiva.

Lema 3.1.— *Suponhamos que $f : A \to B$. Suponhamos que $X, Y \subseteq A$ e $W, Z \subseteq B$,*

(1) $f''(X \cup Y) = f''(X) \cup f''(Y)$ *e, mais geralmente*

$$f''(\cup\{A_i \mid i \in I\}) = \cup\{f'' A_i \mid i \in I\};$$

(2) $f''(X \cap Y) \subseteq f''(X) \cap f''(Y)$ *e, mais geralmente*

$$f''(\cap\{A_i \mid i \in I\}) \subseteq \cap\{f'' A_i \mid i \in I\};$$

(3) $X \subseteq Y \Rightarrow f''X \subseteq f''Y$;

(4) $f''\varnothing = \varnothing$;

(5) $f^{-1}(W \cap Z) = f^{-1}(W) \cap f^{-1}(Z)$ *e, mais geralmente*

$$f^{-1}(\cap\{A_i \mid i \in I\}) = \cap\{f^{-1}(A_i) \mid i \in I\};$$

(6) $f^{-1}(W \cup Z) = f^{-1}(W) \cup f^{-1}(Z)$ *e, mais geralmente*

$$f^{-1}(\cup\{A_i \mid i \in I\}) = \cup\{f^{-1}(A_i) \mid i \in I\};$$

(7) $Z \subseteq W \Rightarrow f^{-1}(Z) \subseteq f^{-1}(W)$;

(8) $f^{-1}(\varnothing) = \varnothing$;

(9) $f^{-1}(B \setminus Z) = A \setminus f^{-1}(Z)$.

Dem.– Exercício. ■

Os naturais

Como prometido vamos agora mostrar que uma das estruturas matemáticas mais importantes—os números naturais–pode ser formalizada no seio da teoria de conjuntos. A estrutura dos números naturais foi caracterizada axiomaticamente por Dedekind e Peano em finais do século XIX, através de um conjunto de axiomas denominados por axiomas de Dedekind-Peano. Os axiomas descrevem uma estrutura do tipo $\langle N^*, S^*, o^*\rangle$, onde o^* é um elemento de N^* e S^* é uma operação unária em N^*, ou seja, uma função $S^* : N^* \to N^*$. Os axiomas são os seguintes:

1. $(\forall n \in N^*)S^*(n) \neq o^*$;
2. $(\forall n, m \in N^*)[n \neq m \Rightarrow S^*(n) \neq S^*(m)]$;
3. $(\forall X \subseteq N^*)[o^* \in X \wedge (\forall n \in N^*)[n \in X \Rightarrow S^*(n) \in X] \Rightarrow X = N^*$.

Teorema 3.1.– *A estrutura* $\mathbb{N} = \langle \omega, S, \ulcorner o \urcorner\rangle$ *satisfaz os axiomas de Dedekind-Peano.*

Dem.— Note-se que $\ulcorner 0 \urcorner = \emptyset$ e que $S(x) = x \cup \{x\}$ não é vazio, pelo que o primeiro axioma é trivialmente satisfeito. Para verificar o segundo axioma consideremos $\ulcorner m \urcorner \neq \ulcorner n \urcorner$. Supondo sem perda de generalidade que $\ulcorner m \urcorner \subsetneq \ulcorner n \urcorner$ tem-se, que $S(\ulcorner m \urcorner) \subseteq \ulcorner n \urcorner \subsetneq S(\ulcorner n \urcorner)$, pelo que $S(\ulcorner m \urcorner) \neq S(\ulcorner n \urcorner)$. Finalmente relativamente ao terceiro axioma, suponhamos que $X \subseteq \omega$ satisfaz $\ulcorner 0 \urcorner \in X$ e $(\forall \ulcorner n \urcorner)[\ulcorner n \urcorner \in X \Rightarrow S(\ulcorner n \urcorner) \in X]$. Suponhamos ainda, tendo em vista a obtenção de um absurdo, que $X \neq \omega$. Fixemos então $\ulcorner n \urcorner$ tal que $\ulcorner n \urcorner \notin X$. Procuremos na sequência $\ulcorner 0 \urcorner \in \ulcorner 1 \urcorner \in \ulcorner 2 \urcorner \in \cdots \in \ulcorner n \urcorner$ o «menor» $\ulcorner k \urcorner$ que não é elemento de X. $\ulcorner k \urcorner \neq \ulcorner 0 \urcorner$ porque por hipótese $\ulcorner 0 \urcorner \in X$. Como na sequência acima qualquer conjunto diferente de $\ulcorner 0 \urcorner$ é sucessor de outro na mesma sequência, existe $\ulcorner m \urcorner$ tal que $S(\ulcorner m \urcorner) = \ulcorner k \urcorner$. Dada a minimalidade de $\ulcorner k \urcorner$ tem que se ter $\ulcorner m \urcorner \in X$, como $\ulcorner m \urcorner \in X \Rightarrow S(\ulcorner m \urcorner) = \ulcorner k \urcorner \in X$, somos forçados a concluir que $\ulcorner k \urcorner \in X$, contradizendo o facto de $\ulcorner k \urcorner \notin X$. Usando redução ao absurdo concluímos que $X = \omega$.

Para simplificar a notação passaremos a denotar a estrutura acima simplesmente por $\mathbb{N}$ e, em vez de designar os seus elementos por $\ulcorner n \urcorner$ designá-los-emos apenas por n, em conformidade com a notação mais usual em matemática.

É importante notar que nesta estrutura se podem definir as operações algébricas usuais de adição, multiplicação e exponenciação e demonstrar as propriedades usuais destas operações. Tudo isto depende dos dois teoremas que se seguem.

Teorema 3.2 (Recursão).— *Dadas duas funções $g : X \times X^k \to X$ e $h : X^k \to X$, existe uma única função $f : \mathbb{N} \times X^k \to X$ que satisfaz*

$$f(0, x_1, \dots, x_k) = h(x_1, \dots, x_k), \quad f(S(n), x_1, \dots, x_k) = g(f(n, x_1, \dots, x_k), x_1, \dots, x_k).$$

Dem (Esboço).— Consideremos $k = 1$ apenas com o intuito de simplificar a exposição. O caso geral adapta-se facilmente a partir deste caso. Consideremos então dadas funções h e g como no enunciado.

Queremos mostrar que existe uma única função $f : \mathbb{N} \times X \to X$ satisfazendo

$$\begin{aligned} f(0, x) &= h(x); \\ f(n+1, x) &= g(f(n, x), x). \end{aligned} \tag{3.5}$$

Designemos por *n-aproximação* uma função cujo domínio é $\{0, 1, 2, \dots, n\} \times X$ e que, no seu domínio, satisfaz as equações acima. Por indução demonstra-se facilmente que para cada $n \in \mathbb{N}$ existem n-aproximações: para $n = 0$ a função $f_0 : \{0\} \times X \to X$ definida por

$$f_0 = \{\langle \langle 0, x \rangle, h(x) \rangle \mid x \in X\}$$

é uma 0-aproximação. Se existe uma n-aproximação, digamos f_n então também existe uma $n+1$-aproximação f_{n+1}. Basta definir,

$$f_{n+1} = f_n \cup \{\langle \langle n+1, x \rangle, g(f_n(n, x)) \rangle \mid x \in X\}.$$

Por indução conclui-se assim que para qualquer $n \in \mathbb{N}$ existe uma n-aproximação. Usando também indução é fácil demonstrar que para cada $n \in \mathbb{N}$ existe uma única n-aproximação. A função f pode finalmente definir-se como a união $f = \cup\{f_n \mid n \in \mathbb{N}\}$ ■

Usando este resultado podemos definir as operações algébricas nos números naturais. A soma é definida de acordo com o seguinte (1) $n + 0 = n$; (2) $n + S(m) = S(n + m)$ (observe-se que de acordo com esta definição se tem $n+1 = n+S(0) = S(n+0) = S(n)$).

Quanto à multiplicação de números naturais ela pode definir-se também por recursão, de acordo com: (1) $n \cdot 0 = 0$; (2) $n \cdot S(m) = (n \cdot m) + n$.

Finalmente podemos definir a operação de exponenciação: (1) $n^0 = 1$; (2) $n^{S(m)} = n^m \cdot n$.

Já vimos atrás que os números naturais podem ser ordenados e, é fácil verificar que essa ordenação pode ser definida à custa da operação de adição.

Definição 3.6.— *Escrevemos $m < n$ se $m \in n$ (ou, de forma equivalente $m \subset n$). Escrevemos ainda $m \leq n$ se $m < n$ ou $m = n$.*

Tem-se então,

$$n \leq m \equiv (\exists k) n + k = m \quad \text{e} \quad n < m \equiv (\exists k \neq 0) n + k = m.$$

Tendo em conta que $n+1$ é o sucessor de n, ou seja, $s(n) = n+1$, os teoremas de indução e recursão são frequentemente enunciados nas formas seguintes, que são equivalentes às que já enunciámos.

Teorema 3.3 (Indução).— *Se $X \subset \mathbb{N}$ e,*

1. $0 \in X$
2. $(\forall n)[n \in X \Rightarrow n + 1 \in X]$

então, $X = \mathbb{N}$.

Corolário 3.3.1.— *Suponhamos que ϕ é uma propriedade dos números naturais. Supondo que são verdadeiros $\phi(0)$ e $(\forall n)[\phi(n) \Rightarrow \phi(n + 1)]$ então, podemos concluir que $(\forall n)\phi(n)$ é verdadeira em $\mathbb{N}$.*

Dem.— Basta aplicar o teorema anterior ao conjunto $X = \{n \in \mathbb{N} \mid \phi(n)\} \subseteq \mathbb{N}$ e aplicar o teorema anterior.

Teorema 3.4 (Recursão).— *Dadas duas funções $g : X \times X^k \to X$ e $h : X^k \to X$, existe uma única função $f : \mathbb{N} \times X^k \to X$ que satisfaz*

$$f(0, x_1, \dots, x_k) = h(x_1, \dots, x_k), \quad f(n + 1, x_1, \dots, x_k) = g(f(n, x_1, \dots, x_k), x_1, \dots, x_k).$$

Por vezes é conveniente considerar o seguinte princípio dito de *indução completa*. Aparentemente mais forte, o princício é de facto equivalente ao princípio de indução que enunciámos acima.

Teorema 3.5 (Indução completa).— *Suponhamos que $X \subseteq \mathbb{N}$ satisfaz*

$$(\forall n)[(\forall k < n) k \in X \Rightarrow n \in X] \tag{3.6}$$

então, $X = \mathbb{N}$.

Dem.— Basta aplicar o teorema 3.3 ao conjunto $Y = \{n \mid (\forall k < n)k \in X\}$. Em primeiro lugar $0 \in Y$ porque temos $(\forall k < 0)k \in X$. De facto, esta fórmula é equivalente a $(\forall k)[k < 0 \Rightarrow k \in X]$ sendo a implicação trivialmente verdadeira (o antecedente é sempre falso). Suponhamos agora que para um dado $n \in \mathbb{N}$ se tem $(\forall k < n)k \in X$, queremos demonstrar que também é verdade que $(\forall k < n + 1)k \in \mathbb{N}$. Usando a implicação 3.6 podemos concluir que se tem $n \in X$, mas então tem-se

$$n \in X \wedge (\forall k < n)k \in X,$$

que é equivalente a $(\forall k < n + 1)k \in X$. O princípio de indução permite-nos então concluir que $(\forall n)n \in X$, ou seja, $(\forall n)(\forall k < n)k \in X$ mas, isto é equivalente a dizer que $X = \mathbb{N}$, como se pretendia.

Corolário 3.5.1.— *Suponhamos que ϕ é uma propriedade dos naturais. Suponhamos que*

$$(\forall n)[(\forall k < n)\phi(k) \Rightarrow \phi(n)]$$

então, podemos concluir que $(\forall n)\phi(n)$ é verdadeira em $\mathbb{N}$.

As seguintes propriedades podem ser todas estabelecidas por indução

1. $(\forall m, n, k)(m + n) + k = m + (n + k)$;
2. $(\forall m, n, k)(mn)k = m(nk)$;
3. $(\forall m, n)mn = nm$;
4. $(\forall m, n)m + n = n + m$;
5. $m(n + k) = mn + mk$;
6. $(\forall m, n, k)n^{m+k} = n^m \cdot n^k$;
7. $(\forall m, n, k)(n^m)^k = n^{mk}$;
8. $(\forall m, n, k)m^k \cdot n^k = (mn)^k$.

Exercício 1.— *Descubra o erro na seguinte demonstração por indução.* Consideremos a propriedade $\phi(n) \equiv (\forall X)[X$ é um conjunto finito com n elementos $\Rightarrow X = \varnothing]$. Tem-se: $(\forall n)\phi(n)$. Podemos constatar que $\phi(0)$ é verdade pois qualquer conjunto com zero elementos é vazio. Suponhamos que dado $n \in \mathbb{N}$ se tem $\phi(n)$, i.e., qualquer conjunto com n elementos é vazio. Vejamos que também se tem $\phi(n + 1)$. Consideremos um conjunto arbitrário X com $n + 1$ elementos, ou seja,

$$X = \{x_1, x_2, \dots, x_n, x_{n+1}\}$$

Tem-se que

$$X = \{x_1, x_2, \dots, x_n, x_{n+1}\} = \{x_1, \dots, x_n\} \cup \{x_1, \dots, x_{n+1}\}$$

Como os dois conjuntos da direita têm n elementos, são vazios pela hipótese de indução. Mas a união de dois conjuntos vazios é vazia, pelo que $X = \varnothing$. Por indução concluí-se então que $(\forall n)\phi(n)$.