Os números naturais - propriedades

Definimos: . $\mathbb{N}$ = o menor conjunto indutivo (ou seja, o menor $\mathbf{I}$ t.q. $0 \in \mathbf{I}$ e $x \in \mathbf{I} \to S(x) \in \mathbf{I}$)

. um elemento de $\mathbb{N}$ é chamado de número natural

. definimos $0 = \emptyset$, $S(x) = x \cup \{x\}$.

Obs: Note que ainda precisa ser mostrado "como são" esses números naturais (que todos são "da forma" como foram definidos os números n's no texto anterior). Por exemplo, precisa ser mostrado que $\forall n \in \mathbb{N}\ n = S(m)$ para algum $m \in \mathbb{N}$ ou que $\forall n \in \mathbb{N}\ n = \{m : m < n\}$, (serão exercícios da Lista 4).

. Temos agora que mostrar várias das propriedades básicas que são importantes/usadas quando se trabalha com os números naturais

. O primeiro passo é definir a ordem. Como a ideia inicial, (a que usamos para nos guiar e chegar a definição de $\mathbb{N}$), era definir cada número como um conjunto de números naturais menores que ele, é natural definir:

Def: A relação $<$ em $\mathbb{N}$ é definida por

$n < m$ se e somente se $n \in m$

Exemplo: $2 < 3$ já que $2 \in 3$.

" "

$\{0,1\}$ $\{0,1,2\}$

• Vamos mostrar que $<$ é de fato uma ordem estrita em $\mathbb{N}$. Daí teremos que $n \leq m \leftrightarrow n < m$ ou $n = m$ é uma ordem em $\mathbb{N}$ (que é a ordem usual).

• Para mostrar isso e várias outras propriedades de $\mathbb{N}$, usamos o P.I.F (que é uma ferramenta fundamental para mostrar fatos sobre os naturais):

Teorema (Princípio da Indução Finita - PIF): Seja $P(x)$ uma propriedade e suponha que:

(a) $P(0)$ é verdade
(b) $P(n) \to P(n+1)$ $\forall n \in \mathbb{N}$

(lembrando: $n+1 = S(n) = n \cup \{n\}$)

Então vale $P(n)$ $\forall n \in \mathbb{N}$.

Dem:

Suponha $P(x)$ tal que temos (a) e (b) do enunciado

Considere o conjunto $A = \{n \in \mathbb{N} : P(n) \text{ vale}\} \subset \mathbb{N}$

Note que
- $0 \in A$ (pela condição (a))
- $n \in A \to n+1 \in A$ (pela condição b)

Mas daí temos que A é um conjunto indutivo.

Logo $\mathbb{N} \subset A$ (pois por definição $\mathbb{N}$ é o menor conjunto indutivo)

$\therefore A = \mathbb{N}$, ou seja, vale $P(n)$ $\forall n \in \mathbb{N}$. //

. O próximo resultado é um primeiro exemplo de como usar o P.I.F para mostrar um fato básico sobre os números naturais

Lema: $0 \leq n \quad \forall n \in \mathbb{N}$

Dem:

Considere $P(x)$ como sendo "$0 \leq x$". Vamos usar o P.I.F.

. $P(0)$ vale pois $0 = 0$ e $\therefore 0 \leq 0$

Suponha que vale $P(n)$, ou seja, $0 \leq n$. Por definição,

$$0 \leq n \longleftrightarrow 0 = n \text{ ou } 0 < n \longleftrightarrow 0 = n \text{ ou } 0 \in n$$

Precisamos mostrar que $0 \leq n+1 = n \cup \{n\}$.

Mas $0 = n$ ou $0 \in n$ $\overset{n \subset n \cup \{n\}}{\Longrightarrow}$ $0 \in n \cup \{n\}$

$\Longrightarrow 0 < n \cup \{n\} = n+1$

$\Longrightarrow 0 \leq n+1$

Logo, usando P.I.F., segue que vale $P(n)$ $\forall n \in \mathbb{N}$, ou seja, $0 \leq n$ $\forall n \in \mathbb{N}$.

. O próximo resultado não usa indução, mas será muito útil:

Proposição: $\forall k, n \in \mathbb{N}$, vale $k < n+1 \longleftrightarrow k < n$ ou $k = n$

Dem: Usando as definições dadas temos:

$$k < n+1 \longleftrightarrow k \in n+1 = n \cup \{n\} \longleftrightarrow$$

$$\longleftrightarrow k \in n \text{ ou } k \in \{n\} \longleftrightarrow$$

$$\longleftrightarrow k \in n \text{ ou } k = n \longleftrightarrow k < n \text{ ou } k = n$$

. O próximo passo é mostrar que a ordem $n < m \leftrightarrow n \in m$ é uma ordem estrita em $\mathbb{N}$. Depois mostraremos que ela é também total, ou seja, que $\forall n, m \in \mathbb{N}$ vale $n < m$ ou $n = m$ ou $m < n$.

Como a demonstração é longa, vamos quebrá-la em alguns "pedaços", para ficar mais fácil acompanhar.

. Começamos com:

Prop: $<$ é transitiva, ou seja, $\forall k, n, m \in \mathbb{N}$ $k < n$ e $m < n \rightarrow k < n$.

Dem:

Vamos fazer a demonstração por indução em n tomando

$P(n)$: "$\forall k \, \forall m \, (k < m$ e $m < n \rightarrow k < n)$"

. $P(0)$ vale pois $\nexists \, m < 0$ (já que $0 = \emptyset$ e $m < 0 \leftrightarrow m \in \emptyset$)

$\therefore$ $P(0)$ vale trivialmente

. $P(n) \rightarrow P(n+1)$:

Suponha $P(n)$, ou seja, que $\forall k \, \forall m \, (k < m$ e $m < n \rightarrow k < n)$

Queremos mostrar $P(n+1)$, ou seja, que $\forall k \, \forall m \, (k < m$ e $m < n+1 \rightarrow k < n+1)$

Fixe então k e m e suponha que $k < m$ e $m < n+1$. Precisamos mostrar que $k < n+1$.

Pela proposição anterior temos que

$m < n+1 \longleftrightarrow m < n$ ou $m = n$

Logo podemos ter $(k < m$ e $m < n)$ ou $(k < m$ e $m = n)$

Mas:

$k<m$ e $m<n$ $\xrightarrow{\text{Hip de Ind}}$ $k<n \rightarrow k \in n \rightarrow k \in n \cup \{n\} = n+1$

$\rightarrow k<n+1$

e

$k<m$ e $m=n \rightarrow k<n \rightarrow k \in n \rightarrow k \in n \cup \{n\} \rightarrow k<n+1$

Em ambos os casos concluímos que $k<n+1$ como queríamos. Logo vale $P(n+1)$.

$\therefore$ pelo PIF vale $P(n)$ $\forall n$, ou seja, vale que

$\forall k \forall m \forall n \quad (k<m$ e $m<n \rightarrow k<n)$. //

O próximo exercício será usado para mostrar a propriedade assimétrica, mas o resultado dele é interessante por si só. Ele diz que não podemos ter $n \in n$:

Exercício: Mostre que "não vale $n<n$", $\forall n \in \mathbb{N}$ $(\neg(n<n))$

Solução: (tente fazer antes de ler)

Vamos mostrar por indução em n, sendo $P(x)$: "$\neg(x<x)$"

- $P(0)$: se $0<0$, teríamos $\emptyset \in \emptyset$, absurdo $\therefore \neg(0<0)$
- $P(n) \rightarrow P(n+1)$:

Suponha que não vale $n<n$. Temos que mostrar que não vale $n+1<n+1$

Suponha por absurdo que $n+1<n+1$ vale

Por uma proposição anterior,

$n+1 < n+1 \rightarrow n+1 < n$ ou $n+1 = n$

Agora note que $n \in n \cup \{n\}$ (sempre), logo pelas definições dada temos que $n < n+1$.

Pela transitividade segue então que se $n+1 < n$ teremos:

$n+1 < n$ e $n < n+1 \rightarrow n < n$, contra a hipótese de indução

Se $n+1 = n$, da $n+1 < n+1$, concluímos de novo que $n < n$, absurdo.

Logo não podemos ter $n+1 < n+1$, ou seja, vale $\neg(n < n)$. $\forall n \in \mathbb{N}$. Pela P.I.F segue que $P(n+1)$ //

Agora fica fácil mostrar:

Teorema: $<$ é uma ordem estrita em $\mathbb{N}$:

Dem:

Já mostramos que $<$ é uma ordem transitiva. Basta apenas mostrarmos que $<$ é assimétrica, ou seja, que

$n < k \rightarrow$ não $(k < n)$ $\forall k, n \in \mathbb{N}$.

Suponha por absurdo que $\exists k, n \in \mathbb{N}$ tal que $n < k$ e $k < n$. Mas daí pela transitividade teríamos $n < n$, o que não pode acontecer (pelo exercício anterior), absurdo.

Logo $<$ é uma ordem estrita em $\mathbb{N}$. //

• Falta apenas mostrar que $<$ é total/linear.

Def: Uma ordem estrita $<$ em A é **linear** ou **total** se $\forall a, b \in A$ vale $a<b$, $b<a$ ou $a=b$.

Teorema: $<$ é uma ordem estrita total em $\mathbb{N}$.

Dem:

Já mostramos que $<$ é uma ordem estrita no teorema anterior. Precisamos apenas mostrar que é total.

Temos então que mostrar que $\forall n, m \in \mathbb{N}$, ou $m<n$ ou $n<m$ ou $n=m$.

Vamos mostrar por indução em n, tomando

$P(x)$: " $\forall m$ ($m<x$ ou $m=x$ ou $x<m$)

• $P(0)$ vale:

$P(0)$ é $\forall m$ ($m<0$ ou $m=0$ ou $0<m$)

Mas já mostramos (usando indução) que $\forall m$ ($0 \leq m$).

• $P(n) \rightarrow P(n+1)$:

Suponha $\forall m$ ($m<n$ ou $m=n$ ou $n<m$)

Precisamos mostrar que

$\forall m$ ($m<n+1$ ou $m=n+1$ ou $n+1<m$)

Fixe $m \in \mathbb{N}$ e suponha que vale $m<n$ ou $m=n$.

Como $m < n+1 \leftrightarrow m < n$ ou $m = n$, temos que

$m < n \rightarrow m < n+1$ e

$m = n \rightarrow m < n+1$, e temos o que queríamos.

Suponha então que vale $n < m$ (que é o caso que falta)

Basta mostrar que $m = n+1$ ou $n+1 < m$

Para isso faremos outra indução, agora em m. Ou seja, por indução em m, vamos mostrar que

$\forall m \in \mathbb{N} (n < m \rightarrow m = n+1$ ou $n+1 < m)$, isto é, que

$\forall m \in \mathbb{N} (n < m \rightarrow n+1 \leq m)$

Note que neste caso n é um parâmetro. Vamos fazer a indução tomando

$Q(x)$: $n < x \rightarrow n+1 \leq x$

- $Q(0)$: vale trividmente pois nunca acontece $n < 0$ ($\leftrightarrow n \in \emptyset$)

- $Q(m) \rightarrow Q(m+1)$:

  Suponha $n < m \rightarrow n+1 \leq m$.

  Queremos mostrar "$n < m+1 \rightarrow n+1 \leq m+1$"

  Suponha $n < m+1 = m \cup \{m\}$. Então $n < m$ ou $n = m$ (por uma prop anterior)

  Vamos fazer os dois casos separadamente.

- Se $n < m$, então pela **hipótese da indução**, temos $n+1 \leq m$

  Como $m < m+1$ (pois $m \in m \cup \{m\}$), pela transitividade, segue que $n+1 \leq m+1$, como queríamos.

- Se $n = m$, então $n \cup \{n\} = m \cup \{m\}$, ou seja, $n+1 = m+1$

$\therefore n+1 \leq m+1$.

Logo, pelo P.I.F, vale que $\forall n \in \mathbb{N}$ $n < m \to n+1 \leq m$, o que termina a demonstração. //

- A ordem definida em $\mathbb{N}$ tem uma propriedade a mais importante: ser uma boa ordem.

. Antes de definirmos o que é boa ordem, vamos ver uma outra versão do P.I.F, que às vezes é mais conveniente (e que usaremos a seguir).

Teorema (Princípio da Indução Finita - 2ª versão): Seja $P(n)$ uma propriedade. Suponha que $\forall n \in \mathbb{N}$ seja verdade que:

$P(k)$ vale $\forall k < n \to P(n)$ vale.

Então $P(n)$ vale $\forall n \in \mathbb{N}$

Dem: Exercício (Dica: use P.I.F para $Q(n)$: $P(k)$ vale $\forall k < n$)

. Vamos usar essa versão do P.I.F para mostrar o Princípio da Boa-Ordem

Def: Uma ordem total $<$ em um conjunto A é uma **boa-ordem** se $\forall B \subset A$, $B \neq \emptyset$, B tem $<$-mínimo. (ou $<$-menor elemento)

Neste caso dizemos que $(A, <)$ é **bem-ordenado**

Teorema: $<$ é uma boa-ordem em $\mathbb{N}$

Dem:

Suponha $X \subset \mathbb{N}$, $X \neq \emptyset$. Suponho que X não tem menor elemento (na ordem $<$). Note que $X \neq \mathbb{N}$ pois $\mathbb{N}$ tem menor elemento (já mostramos que $0 \leq n$ $\forall n \in \mathbb{N}$)

Considere $\mathbb{N} \setminus X$. Note que $\forall n \in \mathbb{N}$ vale

$k \in \mathbb{N} \setminus X$ $\forall k < n \rightarrow n \in \mathbb{N} \setminus X$ (caso contrário n seria o menor elemento de X)

tomando $P(x)$: "$x \in \mathbb{N} \setminus X$"

Mas daí pelo PIF (2ª versão), $n \in \mathbb{N} \setminus X$ $\forall n \in \mathbb{N}$, ou seja $X = \emptyset$, absurdo. //

Obs: O Princípio da Boa Ordem e o PIF são na verdade "equivalentes". Suponho que vale o Princípio da Boa Ordem e vamos mostrar que vale PIF (2ª versão). Seja $P(x)$ uma propriedade tal que $\forall n \in \mathbb{N}$ ($P(k)$ vale $\forall k < n \rightarrow P(n)$ vale). Suponha que $\exists m \in \mathbb{N}$ t.q. não vale $P(m)$. Daí $A = \{m \in \mathbb{N};\ P(m) \text{ não vale}\} \neq \emptyset$. Logo pelo Princípio da Boa Ordem $\exists n = \min A$. Note que então $\forall k < n$ $k \notin A$, ou seja vale $P(k)$, o que pela nossa hipótese indução implicaria que vale $P(n)$. Mas daí teríamos $n \notin A$, absurdo pois $n = \min A \in A$.

Operações nos naturais

Vou apenas dizer como pode-se definir as operações nos naturais e fazer alguns comentários.

Soma:

Teorema: Existe uma única operação binária $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que:

(a) $+(m, 0) = m \quad \forall m \in \mathbb{N}$ (i.e., $m + 0 = m$)

(b) $+(m, \underbrace{n+1}_{S(n)}) = S(+(m,n))$ (i.e., $m + S(n) = S(m+n)$)

Obs: A demonstração deste Teorema, usa o Teorema de Recursão, o qual eu não vou fazer no curso (por falta de tempo), apesar de ser um teorema fundamental na Teoria dos Conjuntos. O Teorema de Recursão é a maneira que temos de formalizar (mostrar que de fato vai ser uma função/conjunto) construções onde temos problemas parecidos com o que temos em demonstrações onde o problema é resolvido com o PIF; seja o passo 0 e como ir do n para o $n+1$ (ou como definir o caso $n+1$, usando o passo n). Por exemplo, como definir $f(n) = n!$? Mais que o usual é: definir $1!$, $2! = 1.2$, $3! = 2!.3$, $4! = 3!.4$, ..., $(n+1)! = n!.(n+1)$, e "assim por diante". O Teorema de Recursão ajuda a resolver o problema do "assim por diante".

Notação: $+(m,n) = m+n$

Obs: Fazendo $n=0$ em (b) temos:

$+(m, S(0)) = S(+(m,0)) \overset{(a)}{=} S(m)$

Mas $S(0) = 1$ e $+(m, S(0)) = +(m,1)$.

Logo segue que $+(m,1) = S(m)$, ou seja, $S(m)$ é o mesmo que "somar um", o que justifica a notação $S(m) = m+1$.

Pode-se mostrar as propriedades da soma em $\mathbb{N}$:

Teor: $\forall m,n \in \mathbb{N}$ valem:

(a) $m+0 = m$

(b) $(m+n)+1 = m+(n+1)$

(c) $m+n = n+m$.

Multiplicação:

Pode-se também mostrar a existência da multiplicação (usando de novo o Teorema da Recursão) e que é única:

Teorema: Existe uma única função $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que:

(a) $m \cdot 0 = 0 \quad \forall m \in \mathbb{N}$

(b) $m \cdot (n+1) = m \cdot n + m \quad \forall m, n \in \mathbb{N}$

Obs: No enunciado já usei a notação $m \cdot n$ ao invés de $\cdot(m,n)$.

- Pode-se mostrar as propriedades usuais das operações (comutativa, associativa e distributiva).

- Com isso temos que é possível desenvolver toda a aritmética de Peano.
As demonstrações de que valem os Axiomas de Peano não são difíceis, apenas trabalhosas (usa bastante o P.I.F).

- A partir de agora assumimos as propriedades conhecidas de $+$ e $\cdot$ em $\mathbb{N}$.