A DEFINIÇÃO AXIOMÁTICA DO CONJUNTO DOS NÚMEROS NATURAIS.

SANDRO MARCOS GUZZO

Resumo. A construção dos conjuntos numéricos é um assunto clássico na matemática, bem como o estudo das propriedades das operações definidas sobre estes conjuntos. Em geral, em cursos de álgebra e de análise real, os estudantes se familiarizam com a construção dos conjuntos dos números inteiros, dos números racionais e dos números reais. Neste trabalho detalharemos a construção (ou definição axiomática) do conjunto dos números naturais. Tal construção será feita a partir dos axiomas de Peano. Nosso trabalho é definir um conjunto denotado por $\mathbb{N}$, duas operações (adição e multiplicação), uma relação de ordem, e provar as principais propriedades destas operações neste conjunto.
Palavras-Chave: Axiomas de Peano, conjunto dos números naturais.

1. Introdução

A construção de conjuntos numéricos é parte da ementa de certos cursos de graduação. Assumindo a existência do conjunto dos números naturais, pode-se construir o conjunto dos números inteiros, e verificar que este novo conjunto é um anel de integridade sob as operações de adição e multiplicação. De posse do conjunto dos números inteiros pode-se construir o conjunto dos números racionais, e verificar que este novo conjunto é um corpo sob as operações de adição e multiplicação.

O conjunto dos números reais pode então ser construído a partir dos números racionais. Uma das mais tradicionais abordagens é o método dos cortes de Dedekind. Nesta abordagem recomendamos [1]. Outra abordagem bastante comum é o método das sequências de Cauchy. Nesta abordagem recomendamos [2]. Os números reais ainda podem ser construídos diretamente do conjunto dos números inteiros pelo método dos quase-homomorfismos. Nesta abordagem recomendamos [3].

Estas construções partem sempre de um ponto em comum que é o conhecimento de um conjunto primitivo, o qual deseja-se melhorar a estrutura. Na base desta construção está o conjunto dos números naturais. Este por sua vez também pode ser "construído".

Este trabalho tem o objetivo de axiomatizar o conjunto dos números naturais, definir as operações de adição e multiplicação e demonstrar propriedades importantes envolvendo tais operações. Propriedades estas que acabam por embasar a construção dos demais conjuntos numéricos que tomam como base o conjunto dos números naturais. O procedimento que adotaremos neste texto é o sugerido em [4].

2. Construção de $\mathbb{N}$

Começamos nosso trabalho postulando a existência de um conjunto que satisfaz certas propriedades axiomáticas. Tais axiomas são conhecidos como axiomas de Peano.

Sandro Marcos Guzzo é professor da Universidade Estadual do Oeste do Paraná - UNIOESTE, campus de Cascavel.

Postulado 1. Postulamos a existência de um conjunto $\mathcal{P}$ e de uma aplicação $s : \mathcal{P} \to \mathcal{P}$, que a cada $x \in \mathcal{P}$ associa o elemento $s(x) \in \mathcal{P}$, satisfazendo os seguintes axiomas:

$\mathbf{P_i}$ (axioma da infinidade) A aplicação s é injetiva mas não sobrejetiva.

$\mathbf{P_{ii}}$ (axioma da indução) Se $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$, então $S = \mathcal{P}$.

Observe que da não sobrejetividade de s segue que existe (pelo menos) um elemento em $\mathcal{P}$ que não está na imagem $s(\mathcal{P})$. Isto significa que $\mathcal{P} - s(\mathcal{P})$ é não vazio, e portanto $\mathcal{P} \neq \emptyset$. Também, da injetividade de s, temos uma bijeção entre $\mathcal{P}$ e $s(\mathcal{P})$ e isto garante que estes conjuntos possuem o mesmo número de elementos. Se o número destes elementos fosse finito então teríamos obrigatoriamente que s é sobrejetiva. Segue que $\mathcal{P}$ não é finito, e daí o fato de o axioma $\mathbf{P_i}$ ser conhecido como axioma da infinidade.

A aplicação s associada a $\mathcal{P}$ é chamada aplicação sucessor, e o elemento $s(x) \in \mathcal{P}$ é dito elemento sucessor do elemento $x \in \mathcal{P}$. Como $\mathcal{P} - s(\mathcal{P})$ é não vazio existe $x \in \mathcal{P}$ de forma que $x \notin s(\mathcal{P})$, isto é, existe uma elemento de $\mathcal{P}$ que não é sucessor de elemento algum de $\mathcal{P}$. Vamos mostrar que tal elemento é único.

Proposição 2. *O conjunto $\mathcal{P} - s(\mathcal{P})$ possui um único elemento.*

Prova. Seja $e \in \mathcal{P} - s(\mathcal{P})$, isto é, $e \in \mathcal{P}$ e $e \notin s(\mathcal{P})$, e consideremos o conjunto

$$S = \{e\} \cup s(\mathcal{P}).$$

Assim, como $e \in \mathcal{P}$ e $s(\mathcal{P}) \subset \mathcal{P}$, temos que $S \subset \mathcal{P}$. Por outro lado, $S \not\subset s(\mathcal{P})$ já que $e \in S$ e $e \notin s(\mathcal{P})$. Vamos mostrar que $s(S) \subset S$. Para isto, seja $y = s(x) \in s(S)$ para algum $x \in S$. Como $x \in S$, então $x = e$ ou $x \in s(\mathcal{P})$. Se $x = e$ então $x \in \mathcal{P}$ e $y = s(x) \in s(\mathcal{P}) \subset S$. Por outro lado, se $x \in s(\mathcal{P}) \subset \mathcal{P}$, então também $s(x) \in s(\mathcal{P}) \subset S$. Segue que $s(S) \subset S$ e do axioma $\mathbf{P_{ii}}$ temos $S = \mathcal{P}$, isto é, $\mathcal{P} = \{e\} \cup s(\mathcal{P})$ e portanto existe um único elemento que está em $\mathcal{P}$ e que não está em $s(\mathcal{P})$. □

O elemento e da proposição anterior, será deste ponto em diante chamado de zero de $\mathcal{P}$, e denotado por $0_{\mathcal{P}}$, ou simplesmente 0. É o único elemento que não é sucessor de nenhum elemento de $\mathcal{P}$, isto é, o único elemento que pertence ao conjunto $\mathcal{P} - s(\mathcal{P})$.

Os axiomas $\mathbf{P_i}$ e $\mathbf{P_{ii}}$ podem ser substituídos por axiomas alternativos (mas equivalentes), para agora contemplar a existência (e unicidade) do elemento $0 \in \mathcal{P} - s(\mathcal{P})$.

Postulado 3. Postulamos a existência de um conjunto $\mathcal{P}$, com um elemento $0 \in \mathcal{P}$, e uma aplicação $s : \mathcal{P} \to \mathcal{P}$, satisfazendo

$\mathbf{P_1}$) $0 \notin s(\mathcal{P})$.

$\mathbf{P_2}$) s é injetiva.

$\mathbf{P_3}$) Se $S \subset \mathcal{P}$ com $0 \in S$ e $s(S) \subset S$, então $S = \mathcal{P}$.

A primeira coisa que precisamos fazer então é mostrar a equivalência entre os postulados 1 e 3.

Proposição 4. *Os postulados 1 e 3 são equivalentes.*

Prova. Suponha então válidos $\mathbf{P_i}$ e $\mathbf{P_{ii}}$. $\mathbf{P_2}$ é consequência imediata de $\mathbf{P_i}$. A proposição 2 garante $\mathbf{P_1}$. Para mostrar $\mathbf{P_3}$, seja $S \subset \mathcal{P}$ tal que $0 \in S$ e $s(S) \subset S$. Então como $0 \in S$ e $0 \notin s(\mathcal{P})$ então $S \not\subset s(\mathcal{P})$. Então temos $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$, e do axioma $\mathbf{P_{ii}}$ temos que $S = \mathcal{P}$, o que prova $\mathbf{P_3}$.

Suponha agora $\mathbf{P_1}$, $\mathbf{P_2}$ e $\mathbf{P_3}$ válidos. De $\mathbf{P_2}$, s é injetiva e como $0 \in \mathcal{P}$ com $0 \notin s(\mathcal{P})$ temos que $\mathcal{P} \not\subset s(\mathcal{P})$ donde s não é sobrejetiva, e isto garante $\mathbf{P_i}$. Para mostrar $\mathbf{P_{ii}}$, seja $S \subset \mathcal{P}$ com $S \not\subset s(\mathcal{P})$ e $s(S) \subset S$. Como $S \not\subset s(\mathcal{P})$ então existe $x \in S \subset \mathcal{P}$ com $x \notin s(\mathcal{P})$ e assim, $x \in \mathcal{P} - s(\mathcal{P})$. Mas o único elemento de $\mathcal{P}$ que não está em $s(\mathcal{P})$ é 0, donde $x = 0$. Assim, $S \subset \mathcal{P}$, com $x = 0 \in S$ e $s(S) \subset S$. De $\mathbf{P_3}$ temos que $S = \mathcal{P}$, o que prova $\mathbf{P_{ii}}$. □

Um fato importante é que não são únicos o conjunto $\mathcal{P}$ e a aplicação s, satisfazendo o postulado 3, e consequentemente o postulado 1. Como exemplo citamos os pares de conjuntos $\mathcal{P}$ e aplicações s,

$$\begin{cases} \mathcal{P}_1 = \{0, 2, 4, 6, 8, 10, \dots\} \\ s_1(n) = n + 2, \quad n \in \mathcal{P}_1, \end{cases}$$

e também

$$\begin{cases} \mathcal{P}_2 = \{1, 10, 100, 1000, 10000, \dots\} \\ s_2(n) = 10 \cdot n, \quad n \in \mathcal{P}_2. \end{cases}$$

Claro que estes exemplos são apenas sugestivos pois ainda não definimos a adição de números naturais, usada na definição de s_1, e nem o produto usado na definição de s_2. Observe que $0 \notin \mathcal{P}_2$ mas isto não é um problema, porque por nossa convenção, 0 é o elemento que não é sucessor de ninguém. Em $\mathcal{P}_2$ este elemento ainda existe porém é o elemento 1.

Dentre todos os conjuntos e aplicações que satisfazem os axiomas de Peano, escolhemos um destes conjuntos e uma destas aplicações e deste ponto em diante os citaremos como o conjunto $\mathbb{N}$ e a aplicação s. O conjunto $\mathbb{N}$ escolhido é chamado conjunto dos números naturais. O conjunto $\mathbb{N}^* = s(\mathbb{N})$ é chamado de conjunto dos números naturais positivos. O número 0 é o (único) número natural que satisfaz $0 \in \mathbb{N} - s(\mathbb{N})$.

Vamos dotar este conjunto de operações e mostrar que estas operações satisfazem propriedades importantes. Primeiro vamos definir uma adição em $\mathbb{N}$. Como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então vamos definir a adição sobre $\mathbb{N}$ definindo indutivamente, primeiro sobre $\{0\}$ e depois sobre elementos de $s(\mathbb{N})$.

Definição 5. Uma aplicação $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sendo que escrevemos $m+n$ para designar $+(m, n)$, que satisfaz

i) $0 + a = a$,

ii) $s(m) + a = s(m + a)$

para todos $m, a \in \mathbb{N}$, é dita adição em $\mathbb{N}$.

Mostraremos que uma tal adição é única em $\mathbb{N}$.

Proposição 6. *Existe uma única aplicação adição em* $\mathbb{N}$.

Prova. Suponha $+$ e $\oplus$ duas aplicações satisfazendo as propriedades (i) e (ii) da definição anterior. Seja

$$S = \{m \in \mathbb{N}; \quad m + n = m \oplus n \quad \text{para todo} \quad n \in \mathbb{N}\}.$$

Então $S \subset \mathbb{N}$. Também $0 \in S$ já que $0 + n = n = 0 \oplus n$ para todo $n \in \mathbb{N}$. Seja $y = s(x) \in s(S)$, para algum $x \in S$. Então $x + n = x \oplus n$ para todo $n \in \mathbb{N}$. Sendo assim, para qualquer $n \in \mathbb{N}$, temos $y + n = s(x) + n = s(x + n) = s(x \oplus n) = s(x) \oplus n = y \oplus n$, e então, $y \in S$. Segue que $s(S) \subset S$ e do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e portanto $m + n = m \oplus n$ para todos $m, n \in \mathbb{N}$, o que mostra a igualdade entre $+$ e $\oplus$. □

Embora $\mathbb{N}$ não seja um grupo, a adição possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento. Vamos então mostrar a validade das propriedades mencionadas para a adição em $\mathbb{N}$.

Teorema 7. *A adição em $\mathbb{N}$ admite elemento neutro, isto é, existe $e \in \mathbb{N}$, tal que $e+a = a = a+e$ para qualquer $a \in \mathbb{N}$.*

Prova. O elemento neutro x da adição, se existir deve ser único, e deve satisfazer $x+a = a = a+x$ para qualquer $a \in \mathbb{N}$. Desta forma, o item (i) da definição da adição, nos diz que se algum elemento neutro existir, este elemento deve ser 0. Vamos então mostrar que 0 satisfaz as duas igualdades.

Claramente o próprio item (i) da definição da adição garante que $0 + a = a$, para todo $a \in \mathbb{N}$, e então vamos mostrar a segunda igualdade. Seja

$$S = \{m \in \mathbb{N}; \quad m = m + 0\}.$$

Naturalmente $S \subset \mathbb{N}$ com $0 \in S$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Como $x \in S$, temos $x + 0 = x$ e disto decorre que $y + 0 = s(x) + 0 = s(x + 0) = s(x) = y$, donde $y \in S$ também. Assim $s(S) \subset S$, e do axioma $\mathbf{P_3}$ segue que $S = \mathbb{N}$. Logo, $0+m = m = m+0$ para todo $m \in \mathbb{N}$, e então 0 é o elemento neutro da adição em $\mathbb{N}$. □

Observe que tradicionalmente seríamos levados a provar primeiro a comutatividade da adição para não precisar provar as duas igualdades no teorema anterior. Entretanto como veremos adiante, para provar a comutatividade da adição, precisaremos da existência do elemento neutro bem como da associatividade da adição.

Teorema 8. *A adição em $\mathbb{N}$ é associativa, isto é, $(x + y) + z = x + (y + z)$, para quaisquer $x, y, z \in \mathbb{N}$.*

Prova. Seja

$$S = \{m \in \mathbb{N}; \quad m + (a + b) = (m + a) + b \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Temos que $S \subset \mathbb{N}$ e $0 \in S$ já que $0 + (a + b) = a + b = (0 + a) + b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ para algum $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x + (a + b) = (x + a) + b$ e também

$$\begin{aligned} y + (a + b) &= s(x) + (a + b) \\ &= s(x + (a + b)) = s((x + a) + b) \\ &= s(x + a) + b = (s(x) + a) + b = (y + a) + b. \end{aligned}$$

Segue que $y \in S$, o que mostra que $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e portanto todo $m \in \mathbb{N}$ satisfaz $m + (a + b) = (m + a) + b$ para quaisquer $a, b \in \mathbb{N}$. Fica mostrada a associatividade da adição. □

Sendo válida a associatividade da adição em $\mathbb{N}$, a partir de agora escreveremos simplesmente $m + a + b$, para indicar $m + (a + b)$ ou $(m + a) + b$. A comutatividade também exigirá um lema auxiliar.

Lema 9. *Para qualquer $n \in \mathbb{N}$ tem-se $s(n) = n + s(0)$.*

Prova. Seja
$$S = \{n \in \mathbb{N}; \quad s(n) = n + s(0)\}.$$

Então $S \subset \mathbb{N}$ e do item (i) da definição da adição, $0 \in S$. Também, seja $y = s(x) \in s(S)$, para algum $x \in S$. Desta forma $s(x) = x + s(0)$. Usando isto e o item (ii) da definição da adição, obtemos
$$s(y) = s(s(x)) = s(x + s(0)) = s(x) + s(0) = y + s(0),$$
e assim, $y = s(x) \in S$, donde $s(S) \subset S$. Segue de $\mathbf{P_3}$ que $S = \mathbb{N}$, e portanto $s(n) = n + s(0)$ para qualquer $n \in \mathbb{N}$. □

Teorema 10. *A adição em* $\mathbb{N}$ *é comutativa, isto é,* $m + n = n + m$ *para quaisquer* $m, n \in \mathbb{N}$.

Prova. Seja
$$S = \{m \in \mathbb{N}; \quad m + a = a + m \quad \text{para todo} \quad a \in \mathbb{N}\}.$$

Claramente $S \subset \mathbb{N}$ e pelo Teorema 7 temos $0 + a = a = a + 0$, isto é, $0 \in S$. Dado $y = s(x) \in s(S)$ para algum $x \in S$, então para todo $a \in \mathbb{N}$ temos $x + a = a + x$ e usando o lema 9 e a definição de adição, temos
$$\begin{aligned} y + a &= s(x) + a = s(x + a) \\ &= s(a + x) = s(a) + x \\ &= a + s(0) + x = a + s(0 + x) = a + s(x) = a + y. \end{aligned}$$
Então $y \in S$ o que mostra que $s(S) \subset S$ e pelo axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$. Segue a comutatividade da adição. □

Mostraremos agora a validade da lei do cancelamento para a adição em $\mathbb{N}$.

Teorema 11. *Para quaisquer* $x, y, m \in \mathbb{N}$*, se* $x + m = y + m$ *então* $x = y$.

Prova. Consideremos o conjunto
$$S = \{m \in \mathbb{N}; \quad a + m = b + m \quad \Rightarrow \quad a = b, \quad \text{para quaisquer} \quad a, b \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ com $0 \in S$ já que, se $a+0 = b+0$ então $a = b$ para quaisquer $a, b \in \mathbb{N}$. Agora, tomemos $y = s(x) \in s(S)$ para $x \in S$. Queremos mostrar que $y = s(x) \in S$ e para isto suponhamos que $a + s(x) = b + s(x)$ para $a, b \in \mathbb{N}$ arbitrários. Então disto decorre que
$$s(x + a) = s(x) + a = s(x) + b = s(x + b).$$

Da injetividade de s segue que $x + a = x + b$ e como $x \in S$ então segue que $a = b$. Desta forma $y = s(x) \in S$, e do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$, o que significa que para qualquer $m \in \mathbb{N}$, se $a + m = b + m$ então $a = b$, quaisquer que sejam $a, b \in \mathbb{N}$. □

Vamos agora dotar o conjunto $\mathbb{N}$ de uma relação de ordem (total). Definimos em $\mathbb{N}$, a relação $\leq$ dada por,
$$a \leq b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in \mathbb{N} \quad \text{tal que} \quad a + n = b.$$

Escrevemos também $a < b$ para designar que $a \leq b$ com $a \neq b$. Observe que se $a < b$ então $a \neq b$ e assim, o número $n \in \mathbb{N}$ tal que $a + n = b$ é obrigatoriamente diferente de 0. Resumindo,
$$a < b, \quad \text{se e somente se,} \quad \text{existe} \quad n \in \mathbb{N}^* \quad \text{tal que} \quad a + n = b.$$

Vamos verificar primeiro que $\leq$ é de fato uma relação de ordem.

Proposição 12. *A relação $\leq$ é uma relação de ordem (parcial) em $\mathbb{N}$.*

Prova. Dado qualquer $a \in \mathbb{N}$, temos $a \leq a$, uma vez que $a + 0 = a$. Desta forma $\leq$ é reflexiva.

Dados $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$, então temos que existem $m, n \in \mathbb{N}$, que satisfazem $a + m = b$ e $b + n = a$. Assim, $a + m + n = b + n = a = a + 0$, e da lei do cancelamento em $\mathbb{N}$ (Teorema 11), segue que $m + n = 0$, donde $m + n \notin s(\mathbb{N})$. Vamos mostrar que $m \notin s(\mathbb{N})$. De fato, procedendo contrapositivamente se $m \in s(\mathbb{N})$ então $m = s(x)$ para algum $x \in \mathbb{N}$ e segue que $m + n = s(x) + n = s(x + n) \in s(\mathbb{N})$, o que garante que $m + n \in s(\mathbb{N})$. Isto prova que $m \notin s(\mathbb{N})$ e como o único elemento de $\mathbb{N}$ que não está em $s(\mathbb{N})$ é 0, temos que $m = 0$. Desta forma, $b = a + m = a + 0 = a$, e que a relação é anti-simétrica.

Dados agora $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$, então existem $m, n \in \mathbb{N}$ tais que $a + m = b$ e $b + n = c$. Assim, $a + (m + n) = (a + m) + n = b + n = c$, e então $a \leq c$ já que $m + n \in \mathbb{N}$. Temos portanto a transitividade da relação $\leq$. □

Queremos provar agora que esta ordem é total. Para isto usaremos um lema auxiliar de fácil demonstração.

Lema 13. *Para qualquer $n \in \mathbb{N}$ temos que $n \leq s(n)$.*

Prova. Naturalmente, para qualquer $n \in \mathbb{N}$,

$$n + s(0) = s(0) + n = s(0 + n) = s(n),$$

e como $s(0) \in \mathbb{N}$, então $n \leq s(n)$. □

Proposição 14. *A relação de ordem $\leq$ é total em $\mathbb{N}$.*

Prova. Seja $a \in \mathbb{N}$ arbitrário, e considere o conjunto

$$S_a = \{n \in \mathbb{N}; \quad a \leq n \quad \text{ou} \quad n \leq a\}.$$

Então $S_a \subset \mathbb{N}$. Como $0 + a = a$ então $0 \leq a$ e com isto $0 \in S_a$. Mostraremos que $s(S_a) \subset S_a$. Seja $y = s(x) \in s(S_a)$ para algum $x \in S_a$. Desta forma, $x \leq a$ ou $a \leq x$.

Se $a \leq x$, como $x \leq s(x)$ então da transitividade de $\leq$ segue que $a \leq s(x)$ donde $s(x) \in S_a$, isto é, $y \in S_a$.

Se $x \leq a$ então $x + k = a$ para algum $k \in \mathbb{N}$. Se $k = 0$ então não há o que mostrar pois daí $a = x$ e podemos utilizar o caso $a \leq x$. Se $k \neq 0$ então $k \in s(\mathbb{N})$, donde $k = s(m)$ para algum $m \in \mathbb{N}$. Então $s(x)+m = s(x+m) = s(m+x) = s(m)+x = k+x = a$. Segue que $s(x) \leq a$ e então $s(x) \in S_a$, ou ainda, $y \in S_a$.

Em qualquer caso, temos $s(S_a) \subset S_a$. Segue do axioma $\mathbf{P_3}$ que $S_a = \mathbb{N}$. Assim, dados $m, n \in \mathbb{N}$ arbitrários, temos que $m \in S_n$ e da definição de S_n, temos que $m \leq n$ ou $n \leq m$, e o conjunto $\mathbb{N}$ é totalmente ordenado. □

Nestes termos, dados $a, b \in \mathbb{N}$, temos $a \leq b$ ou $b \leq a$. Se considerarmos separadamente a possibilidade $a = b$, temos então a propriedade tricotômica da relação de ordem, ou $a = b$, ou $a < b$, ou $b < a$.

Definiremos agora uma multiplicação em $\mathbb{N}$. Novamente, como $\mathbb{N} = \{0\} \cup s(\mathbb{N})$ então definiremos a multiplicação em $\mathbb{N}$ indutivamente, definindo-a primeiro sobre $\{0\}$ e depois sobre os elementos de $s(\mathbb{N})$.

Definição 15. Uma aplicação $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sendo que escrevemos $m \cdot n$ ou simplesmente mn para indicar $\cdot(m, n)$, que satisfaz

i) $0 \cdot a = 0$,

ii) $s(m) \cdot a = (m \cdot a) + a$

para todos $m, a \in \mathbb{N}$, é dita multiplicação em $\mathbb{N}$.

Para o item (ii) vamos supor, deste ponto em diante, que a multiplicação tem preferência sobre a adição, e então escreveremos simplesmente $m \cdot a + a$ em vez de $(m \cdot a) + a$. Mostraremos, como no caso da adição, que a multiplicação é única em $\mathbb{N}$.

Proposição 16. *Existe uma única aplicação multiplicação em* $\mathbb{N}$.

Prova. Sejam $\cdot$ e $\odot$ duas multiplicações em $\mathbb{N}$. Consideremos

$$S = \{m \in \mathbb{N}; \quad m \cdot a = m \odot a, \quad \text{para todo} \quad a \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ e também $0 \in S$ já que $0 \cdot a = 0 = 0 \odot a$ para todo $a \in \mathbb{N}$. Seja $y = s(x) \in s(S)$ para algum $x \in S$. Nestes termos, para qualquer $a \in \mathbb{N}$ temos $x \cdot a = x \odot a$ e disto $y \cdot a = s(x) \cdot a = x \cdot a + a = x \odot a + a = s(x) \odot a = y \odot a$, o que garante que $y \in S$ e que $s(S) \subset S$. Do axioma $\mathbf{P_3}$, temos $S = \mathbb{N}$ e então para todos $a, m \in \mathbb{N}$ é válida a igualdade $m \cdot a = m \odot a$, donde segue a igualdade entre $\cdot$ e $\odot$. $\square$

A multiplicação possui propriedades similares às propriedades da adição. Entretanto, as demonstrações destas propriedades são mais extensas para a multiplicação. A multiplicação possui elemento neutro, é comutativa, associativa e vale a lei do cancelamento (com restrições). A prova da existência do elemento neutro precisará de um lema auxiliar.

Lema 17. *Dados* $a, b \in \mathbb{N}$, *se* $a \cdot b = 0$, *então* $a = 0$ *ou* $b = 0$.

Prova. Procederemos pela contrapositiva. Suponha que $a \neq 0$ e $b \neq 0$, ou ainda, $a, b \in s(\mathbb{N})$. Existem então $x, y \in \mathbb{N}$ tais que $a = s(x)$ e $b = s(y)$. Assim, das definições de multiplicação e de adição,

$$a \cdot b = s(x) \cdot s(y) = x \cdot s(y) + s(y) = s(y) + x \cdot s(y) = s(y + x \cdot s(y)),$$

e então, $a \cdot b \in s(\mathbb{N})$ o que garante que $a \cdot b \neq 0$. O resultado fica então demonstrado contrapositivamente. $\square$

Teorema 18. *Existe* $i \in \mathbb{N}$ *tal que* $i \cdot a = a = a \cdot i$ *para qualquer* $a \in \mathbb{N}$*;*

Prova. Sabemos que $0 \cdot a = 0$, e portanto na procura por um elemento $i \in \mathbb{N}$ tal que $i \cdot a = a$ para qualquer $a \in \mathbb{N}$, vemos que i não pode ser o elemento 0. Então $i \in s(\mathbb{N})$, e desta forma $i = s(x)$ para algum $x \in \mathbb{N}$. Sendo assim, x deverá satisfazer $s(x) \cdot a = a$, ou ainda $x \cdot a + a = a = 0 + a$. Mas pela lei do cancelamento para a adição, x deve satisfazer $x \cdot a = 0$. Do lema anterior, $x = 0$ ou $a = 0$, e como desejamos a igualdade para $a \in \mathbb{N}$ arbitrário, devemos ter $x = 0$ e desta forma $i = s(x) = s(0)$.

Mostraremos que $s(0)$ satisfaz portanto as duas igualdades desejadas. De fato, $s(0) \cdot a = 0 \cdot a + a = 0 + a = a$ para qualquer $a \in \mathbb{N}$. Agora, para mostrar a segunda igualdade, seja

$$S = \{n \in \mathbb{N}; \quad n \cdot s(0) = n\}.$$

Desta forma, $S \subset \mathbb{N}$ e também $0 \in S$, pois $0 \cdot s(0) = 0$. Dado $y = s(x) \in s(S)$, para algum $x \in S$, temos então $x \cdot s(0) = x$ e usando também o lema 9 decorre que,

$$y \cdot s(0) = s(x) \cdot s(0) = x \cdot s(0) + s(0) = x + s(0) = s(x) = y.$$

Então temos que $y \in S$, o que mostra que $s(S) \subset S$ e do axioma $\mathbf{P_3}$, $S = \mathbb{N}$. Temos assim que $a \cdot s(0) = a$ para todo $a \in \mathbb{N}$. □

O elemento $s(0) \in \mathbb{N}$ é então o elemento neutro da multiplicação, e naturalmente este é o elemento sucessor do elemento $0 \in \mathbb{N}$. Chamaremos o elemento $s(0)$ de unidade do conjunto $\mathbb{N}$ e representaremos este elemento de agora em diante por 1. Desta forma, temos $1 = s(0)$ e também $1 \cdot a = a = a \cdot 1$ para qualquer $a \in \mathbb{N}$.

Com a notação $s(0) = 1$ e o lema 9 temos imediatamente que $s(x) = x + s(0) = x + 1$, para qualquer $x \in \mathbb{N}$. De outra forma, o sucessor de um número natural x é o número natural $x + 1$.

Queremos agora mostrar que a multiplicação é associativa e comutativa. Para provar isto, precisaremos primeiro da distributividade da multiplicação em relação à adição. Esta por sua vez utilizará um lema auxiliar. Este lema refere-se ao produto por 0 pela esquerda. A definição de multiplicação já garante em seu item (i) que $0 \cdot a = 0$ para qualquer $a \in \mathbb{N}$. Mas como ainda não mostramos a comutatividade da multiplicação, precisaremos provar também que $a \cdot 0 = 0$ para todo $a \in \mathbb{N}$.

Lema 19. *Para todo* $a \in \mathbb{N}$, *temos* $a \cdot 0 = 0$.

Prova. Consideremos o conjunto

$$S = \{m \in \mathbb{N}; \quad m \cdot 0 = 0\}.$$

Temos que $S \subset \mathbb{N}$ e como $0 \cdot 0 = 0$ então $0 \in S$. Também seja $y = s(x) \in s(S)$ para $x \in S$. Então $x \cdot 0 = 0$ e decorre disto que $y \cdot 0 = s(x) \cdot 0 = x \cdot 0 + 0 = x \cdot 0 = 0$. Segue que $y \in S$ e que $s(S) \subset S$. Pelo axioma $\mathbf{P_3}$, $S = \mathbb{N}$, donde $a \cdot 0 = 0$ para todo $a \in \mathbb{N}$. □

Teorema 20. *Para quaisquer* $x, y, z \in \mathbb{N}$, *temos* $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ *e também* $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$, *isto é, a operação multiplicação é distributiva com relação à operação adição em* $\mathbb{N}$.

Prova. Consideremos

$$S = \{m \in \mathbb{N}; \quad m \cdot (a + b) = m \cdot a + m \cdot b, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Claro que $S \subset \mathbb{N}$ e que $0 \in S$ já que $0 \cdot (a + b) = 0 = 0 + 0 = 0 \cdot a + 0 \cdot b$ para quaisquer $a, b \in \mathbb{N}$. Agora suponha $y = s(x) \in s(S)$, para $x \in S$. Então $x \cdot (a + b) = x \cdot a + x \cdot b$ e usando isto temos

$$\begin{aligned} y \cdot (a + b) &= s(x) \cdot (a + b) = x \cdot (a + b) + (a + b) \\ &= x \cdot a + x \cdot b + a + b \\ &= x \cdot a + a + x \cdot b + b \\ &= s(x) \cdot a + s(x) \cdot b = y \cdot a + y \cdot b. \end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos $S = \mathbb{N}$ e a distributividade à esquerda da multiplicação em relação à adição. Para provar a distributividade à direita, consideremos o conjunto

$$T = \{m \in \mathbb{N}; \quad (a+b)\cdot m = a\cdot m + b\cdot m, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Então $T \subset \mathbb{N}$ e usando o lema 19 temos que $(a+b)\cdot 0 = 0 = 0+0 = a\cdot 0 + b\cdot 0$ para quaisquer $a, b \in \mathbb{N}$, e então $0 \in T$. Agora suponha $y = s(x) \in s(T)$ para $x \in T$. Então $(a+b)\cdot x = a\cdot x + b\cdot x$ e usando o fato que $s(x) = x+1$, temos

$$\begin{aligned}
(a+b)\cdot y &= (a+b)\cdot s(x) = (a+b)\cdot(x+1)\\
&= (a+b)\cdot x + (a+b)\cdot 1\\
&= a\cdot x + b\cdot x + a + b\\
&= a\cdot x + a + b\cdot x + b\\
&= a\cdot x + a\cdot 1 + b\cdot x + b\cdot 1\\
&= a\cdot(x+1) + b\cdot(x+1)\\
&= a\cdot s(x) + b\cdot s(x) = a\cdot y + b\cdot y.
\end{aligned}$$

Temos então que $y \in T$, e por conseguinte $s(T) \subset T$. Do axioma $\mathbf{P_3}$ temos $T = \mathbb{N}$. A multiplicação é portanto distributiva também à direita em relação à adição. □

Teorema 21. *Para quaisquer* $x, y, z \in \mathbb{N}$, *temos* $x\cdot(y\cdot z) = (x\cdot y)\cdot z$.

Prova. Seja

$$S = \{m \in \mathbb{N}; \quad m\cdot(a\cdot b) = (m\cdot a)\cdot b, \quad \text{para todos} \quad a, b \in \mathbb{N}\}.$$

Temos $S \subset \mathbb{N}$ e também $0 \in S$ pois $0\cdot(a\cdot b) = 0 = 0\cdot b = (0\cdot a)\cdot b$ para quaisquer $a, b \in \mathbb{N}$. Seja agora $y = s(x) \in s(S)$ com $x \in S$. Então para quaisquer $a, b \in \mathbb{N}$ temos $x\cdot(a\cdot b) = (x\cdot a)\cdot b$ e disto temos

$$\begin{aligned}
y\cdot(a\cdot b) &= s(x)\cdot(a\cdot b)\\
&= x\cdot(a\cdot b) + a\cdot b\\
&= (x\cdot a)\cdot b + a\cdot b\\
&= (x\cdot a + a)\cdot b = (s(x)\cdot a)\cdot b = (y\cdot a)\cdot b.
\end{aligned}$$

Então $y \in S$ e $s(S) \subset S$. Do axioma $\mathbf{P_3}$ temos que $S = \mathbb{N}$ e fica provada a associatividade da multiplicação. □

Teorema 22. *Para quaisquer* $m, n \in \mathbb{N}$, *temos* $m\cdot n = n\cdot m$.

Prova. Considerando

$$S = \{m \in \mathbb{N}; \quad m\cdot a = a\cdot m, \quad \text{para todos} \quad a \in \mathbb{N}\},$$

temos $S \subset \mathbb{N}$. Também, usando a definição da multiplicação e o lema 19, temos $a\cdot 0 = 0 = 0\cdot a$ para todo $a \in \mathbb{N}$, o que garante que $0 \in S$. Suponha agora $y = s(x) \in s(S)$ para $x \in S$. Então para todo $a \in \mathbb{N}$ temos $x\cdot a = a\cdot x$ e também

$$\begin{aligned}
y\cdot a &= s(x)\cdot a = x\cdot a + a\\
&= a\cdot x + a\cdot 1\\
&= a\cdot(x+1) = a\cdot s(x) = a\cdot y.
\end{aligned}$$

Segue que $y \in S$ e então $s(S) \subset S$. O axioma $\mathbf{P_3}$ garante que $S = \mathbb{N}$ e portanto $m \cdot a = a \cdot m$ para todos $a, m \in \mathbb{N}$. □

A lei do cancelamento também é válida para a multiplicação, com uma certa restrição, como dito antes. Como sabemos que $0 \cdot x = 0 = 0 \cdot y$ para quaisquer $x, y \in \mathbb{N}$, isto nos diz que $a \cdot x = a \cdot y$ não pode garantir que $x = y$ no caso em que $a = 0$. Entretanto se $a \neq 0$ então podemos garantir este cancelamento.

Teorema 23. *Para quaisquer* $a, x, y \in \mathbb{N}$, *se* $a \neq 0$ *e* $a \cdot x = a \cdot y$, *então* $x = y$.

Prova. Supondo $a \neq 0$, então temos que $a \in s(\mathbb{N})$ e $a = s(m)$ para algum $m \in \mathbb{N}$. Sejam também $x, y \in \mathbb{N}$ tais que $a \cdot x = a \cdot y$. Como a relação de ordem em $\mathbb{N}$ é total, então temos $x \leq y$ ou $y \leq x$. Vamos analisar cada um dos casos.

Se $x \leq y$ então existe $k \in \mathbb{N}$ tal que $x + k = y$. Assim,

$$\begin{aligned} s(m) \cdot x = a \cdot x &= a \cdot y \\ &= a \cdot (x + k) \\ &= a \cdot x + a \cdot k = s(m) \cdot x + s(m) \cdot k. \end{aligned}$$

Da lei do cancelamento para a adição, temos que $s(m) \cdot k = 0$, e do lema 17, temos que obrigatoriamente $k = 0$, uma vez que $s(m) \neq 0$. Sendo assim, $y = x + k = x + 0 = x$.

Analogamente, se $y \leq x$ então existe $l \in \mathbb{N}$ tal que $y + l = x$. Então também

$$s(m) \cdot y = a \cdot y = a \cdot x = a \cdot (y + l) = s(m) \cdot y + s(m) \cdot l,$$

donde segue que $s(m) \cdot l = 0$ e como $s(m) \neq 0$ então $l = 0$. Logo, $x = y + l = y + 0 = y$, e isto encerra esta demonstração. □

Apenas como complemento desta seção mostraremos agora a compatibilidade das operações de adição e multiplicação para com a relação de ordem em $\mathbb{N}$. Isto significa que dados $a, b \in \mathbb{N}$ arbitrários, se $a \leq b$ então $a + m \leq b + m$, e também $a \cdot m \leq b \cdot m$ para qualquer $m \in \mathbb{N}$.

Teorema 24. *Dados* $a, b \in \mathbb{N}$ *com* $a \leq b$ *então, para qualquer* $m \in \mathbb{N}$ *temos* $a + m \leq b + m$.

Prova. Sejam então $a, b \in \mathbb{N}$ com $a \leq b$. Então existe $k \in \mathbb{N}$ tal que $a + k = b$. Então usando a comutatividade e a associatividade da adição em $\mathbb{N}$, temos

$$(a + m) + k = (a + k) + m = b + m,$$

para qualquer $m \in \mathbb{N}$. Isto garante que $a + m \leq b + m$. □

Teorema 25. *Dados* $a, b \in \mathbb{N}$ *com* $a \leq b$ *então, para qualquer* $m \in \mathbb{N}$ *temos* $a \cdot m \leq b \cdot m$.

Prova. Dados $a, b \in \mathbb{N}$ com $a \leq b$, então existe $k \in \mathbb{N}$ tal que $a + k = b$. Então usando a distributividade da multiplicação com relação à adição em $\mathbb{N}$, temos

$$a \cdot m + k \cdot m = (a + k) \cdot m = b \cdot m,$$

para qualquer $m \in \mathbb{N}$. Segue que $a \cdot m \leq b \cdot m$. □

Observe que o conjunto dos números naturais não possui um elemento máximo. Isto é fácil de ser observado, pois já mostramos que para qualquer elemento $x \in \mathbb{N}$ temos que $s(x) \in \mathbb{N}$ e também $x \leq s(x)$. Isto é, dado qualquer número natural x sempre existe outro número natural (o sucessor de x) maior que x.

3. Considerações finais

Outras construções dos números naturais também são conhecidas. Uma destas consiste em definir o conjunto dos números naturais como sendo um conjunto de conjuntos encaixados. Definimos inicialmente o elemento 0 como sendo o conjunto vazio, isto é,

$$0 = \emptyset.$$

Construímos agora recursivamente o sucessor de cada elemento (conjunto) x como sendo $s(x) = \{x\}$. A aplicação s neste caso também é dita a aplicação sucessor. Observe que desta forma temos

$$\begin{aligned}
&0 = \emptyset \\
&1 = s(0) = \{0\} = \{\emptyset\} \\
&2 = s(1) = \{1\} = \{\{\emptyset\}\} \\
&3 = s(2) = \{2\} = \{\{\{\emptyset\}\}\} \\
&\vdots
\end{aligned}$$

Outra construção baseada nesta ideia é definir $0 = \{\}$ e a partir deste elemento construir os sucessores de cada conjunto x como sendo $s(x) = x \cup \{x\}$. Nesta ideia deixamos como exercício para o leitor interessado obter o conjunto de tais números naturais.

Referências

[1] Guidorizzi, Hamilton L. *Um curso de cálculo.* Volume 1, 5^a edição, Rio de Janeiro: Livros Técnicos e Científicos, 2001.

[2] Monteiro, L. H. Jacy. *Elementos de Álgebra.* 2^a edição, Rio de Janeiro: Livros Técnicos e Científicos, 1978.

[3] Street, Ross. *An efficient construction of the real numbers.* Gazette of the Australian Mathematical Society **12** (1985) 57–58.

[4] Sah, Chih-Han. *Abstract algebra.* New York: Academic Press, 1967.