



IX Semana Acadêmica da FAJESU

Curso de Licenciatura em Matemática

Minicurso: Sobre a Aritmética dos Axiomas de Peano

por

Prof. Dr. Jhone Caldeira Silva

Instituto de Matemática e Estatística - Universidade Federal de Goiás

Taguatinga/DF - Maio de 2010

Resumo

Em seu livro “Arithmetices Principia Nova Methodo Exposita”, Giuseppe Peano estabeleceu importantes axiomas, os quais permitiram construções rigorosas em Álgebra e Análise. A motivação foi o desejo de expressar toda a Matemática em termos de um cálculo lógico. Desejamos apresentar alguns axiomas e demonstrar algumas propriedades básicas por meio do raciocínio lógico.

1 - Introdução

A Aritmética tem início em algum momento da história quando o homem começa a contar e a associar números (mesmo que de forma implícita) a coleções de objetos e seres que faziam parte de sua rotina. Certamente nossos antepassados dispuseram de muita criatividade e poucos recursos para criar as primeiras regras, fazer conjecturas e aceitar “verdades”.

No sentido de contagem, inúmeras “técnicas” foram aplicadas e muitos procedimentos distintos adotados até chegarmos nos modernos sistemas de cálculos hoje conhecidos. Foram necessárias considerações sobre bases e representações de quantidades, bem como a significação dessas representações. Os sistemas foram surgindo, ficando mais amplos, sendo aperfeiçoados e até mesmo melhor compreendidos. No que trata da Teoria dos Números, é interessante observar que tanto os egípcios como os babilônios construíram, ao longo de sua história, um acervo matemático significativo e altamente importante. Desenvolveram tópicos essenciais da Aritmética, da Geometria e da Álgebra. No decorrer dos séculos, limitações sempre eram encontradas sob o ponto de vista científico e, assim, passando pelas histórias de tantos povos, até os dias de hoje, a Matemática pede avanços.

Poderíamos iniciar nossas discussões voltando a conceitos hoje tidos como simples, como, por exemplo, o conjunto dos números naturais. De certo modo, é fascinante conhecer \mathbb{N} sob um enfoque mais formal e completo, vislumbrar a própria construção lógica de \mathbb{N} .

Enquanto a Geometria, 300 anos antes de Cristo, nos *Elementos* de Euclides, já recebia um tratamento lógico-dedutivo, com seus postulados e axiomas, definições e teoremas, a Teoria dos Números esperou muito para ter um tratamento semelhante. A primeira tentativa nesse sentido se deve a Giovanni Campano, que viveu por volta de 1260. Ele procurou fundamentar os números naturais em 4 postulados, sendo o último dos quais afirmava que “um número não pode diminuir indefinidamente”. Isto significa, no fundo, a existência do mínimo de qualquer coleção de números naturais. Posteriormente Gottfried W. Leibniz (1646 – 1716) assinalou que “verdades” tão evidentes como “ $2 + 2 = 4$ ” devem ser objeto de demonstração a partir do conceito de número, o mesmo devendo acontecer com propriedades aparentemente tão óbvias como a comutativa da adição e a comutativa da multiplicação. Mas Leibniz não se alongou no assunto. Chegando-se ao século XIX já era possível à Matemática, no estágio que atingira e no ritmo em que se desenvolvia, continuar se apoiando quase que inteiramente na intuição. Além disso, seus alicerces passaram a ser investigados amplamente e a receber a fundamentação lógica necessária.

Referindo-se aos números, acredita-se que a primeira tentativa séria nesse sentido foi feita por Hermann G. Grassmann (1809 – 1877) que, em 1861, definiu adição e multiplicação de inteiros e demonstrou as propriedades fundamentais dessas operações, usando apenas a função sucessor $x \mapsto x + 1$ e implicitamente o princípio de indução. O primeiro sistema completo de axiomas para a Aritmética foi apresentado por Richard Dedekind (1831 – 1916) em 1888. A axiomática que apresentamos neste minicurso se deve a Giuseppe Peano (1858 – 1932) e data de 1891.

2 - Os Axiomas de Peano

Peano, tendo em vista a fundamentação lógica da Aritmética, escolheu três conceitos como sendo primitivos, a saber: o *zero*, o *número natural* e a relação “*é sucessor de*”. Com o intuito de caracterizá-los, formulou os seguintes axiomas:

P₁– Zero é um número natural.

P₂– Se a é um número natural, então a tem um único sucessor que também é um número natural.

P₃– Zero não é sucessor de nenhum número natural.

P₄– Dois números naturais que têm sucessores iguais são, eles próprios, iguais.

P₅– Se uma coleção C de números naturais contém o zero e, também, o sucessor de todo elemento de C , então C é o conjunto de todos os números naturais. (Este axioma é conhecido como *axioma de indução finita*).

A fim de facilitar o tratamento simbólico, iremos utilizar as

Notações:

- 0 para indicar o zero.
- a^+ para indicar o sucessor de um número natural a .
- \mathbb{N} para indicar o conjunto dos números naturais.

Desta forma, podemos reescrever:

P₁– $0 \in \mathbb{N}$.

P₂– $a \in \mathbb{N} \Rightarrow a^+ \in \mathbb{N}$.

P₃– $(\forall a)(a \in \mathbb{N} \Rightarrow a^+ \neq 0)$.

P₄– $a^+ = b^+ \Rightarrow a = b$.

P₅– Se $S \subset \mathbb{N}$ e

(i) $0 \in S$,

(ii) $a \in S \Rightarrow a^+ \in S$,

então $S = \mathbb{N}$.

Observamos que P_1 garante que $\mathbb{N} \neq \emptyset$. Já em P_2 está subentendido a unicidade de a^+ . De P_4 segue que $a \neq b \Rightarrow a^+ \neq b^+$, o que é fácil ver, pois $a^+ = b^+ \Rightarrow a = b$.

Proposição 1. *Se $a \in \mathbb{N}$, então $a^+ \neq a$.*

Demonstração: Seja $S = \{a \in \mathbb{N} : a^+ \neq a\}$. O axioma P_3 nos dá que $0 \in S$. Se $a \in S$, então $a^+ \neq a$ e, assim, $(a^+)^+ \neq a^+$. Logo $a^+ \in S$, sempre que $a \in S$. Por P_5 , temos que $S = \mathbb{N}$. Portanto, para todo $a \in \mathbb{N}$, $a^+ \neq a$. ■

Proposição 2. *Se $b \in \mathbb{N}$, $b \neq 0$, então existe $a \in \mathbb{N}$ tal que $a^+ = b$.*

Demonstração: Seja $S = \{0\} \cup \{y \in \mathbb{N} : y \neq 0 \text{ e } x^+ = y \text{ para algum } x \in \mathbb{N}\}$. Por construção, $0 \in S$. Claramente, $0^+ \in S$. Agora, se $a \in S$ e $a \neq 0$, então $a = b^+$, para algum $b \in \mathbb{N}$. Daí, $a^+ = (b^+)^+$ e, assim, $a^+ \in S$. O axioma P_5 nos leva a concluir que $S = \mathbb{N}$ e, portanto, a demonstração está concluída. ■

Proposição 3. (*Primeiro Princípio de Indução Completa*) - Suponhamos que a todo número natural n esteja associada uma função $P(n)$ tal que:

(i) $P(0)$ é verdadeira.

(ii) $P(r^+)$ é verdadeira, sempre que $P(r)$ é verdadeira.

Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração: Basta mostramos que $S = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\}$ satisfaz as hipóteses de P_5 . Mas isto é imediato. ■

3 - Adição em \mathbb{N}

A adição $(x, y) \mapsto x + y$ em \mathbb{N} é definida mediante as seguintes condições:

- $a + 0 = a$;
- $a + b^+ = (a + b)^+$.

Em $a + b = c$, a e b são as *parcelas* e c é a *soma*.

Adotaremos as

Notações:

- $0^+ = 1$;
- $1^+ = 2$;
- $2^+ = 3$ etc.

Exemplos:

$$1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2;$$

$$1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3;$$

$$1 + 3 = 1 + 2^+ = (1 + 2)^+ = 3^+ = 4;$$

$$r + 1 = r + 0^+ = (r + 0)^+ = r^+, \text{ para todo } r \in \mathbb{N}.$$

Propriedades da Adição

A₁ (Associativa) $a + (b + c) = (a + b) + c, \forall a, b, c \in \mathbb{N}$.

A₂ (Comutativa) $a + b = b + a, \forall a, b \in \mathbb{N}$.

A₃ (Zero é Elemento Neutro) $a + 0 = 0 + a = a, \forall a \in \mathbb{N}$.

A₄ (Lei do Cancelamento da Adição) $a + b = a + c \Rightarrow b = c, \forall a, b, c \in \mathbb{N}$.

Demonstração:

Associativa

Usaremos indução sobre c .

Se $c = 0$, então $a + (b + 0) = a + b = (a + b) + 0$.

Suponhamos que $(a + b) + r = a + (b + r)$. Então:

$$(a + b) + r^+ = [(a + b) + r]^+ = [a + (b + r)]^+ = a + (b + r)^+ = a + (b + r^+).$$

Portanto, $a + (b + c) = (a + b) + c$, para todos $a, b, c \in \mathbb{N}$.

Comutativa

- Primeiramente, mostremos que $0 + a = a$.

Usaremos indução sobre a .

Se $a = 0$, então $0 + 0 = 0$ (usando a definição $a + 0 = a$).

Suponhamos que $0 + r = r$. Então: $(0 + r)^+ = (0 + r)^+ = r^+$.

Portanto, $0 + a = a$, para todo $a \in \mathbb{N}$.

- Mostremos que $b + a^+ = b^+ + a$ por indução sobre a .

Se $a = 0$, então $b + 0^+ = (b + 0)^+ = (0 + b)^+ = 0 + b^+ = b^+ + 0$.

Suponhamos que $b + r^+ = b^+ + r$. Então: $b + (r^+)^+ = (b + r^+)^+ = (b^+ + r)^+ = b^+ + r^+$.

Portanto, $b + a^+ = b^+ + a$, para todos $a, b \in \mathbb{N}$.

- Agora, mostremos que $a + b = b + a$ por indução sobre b .

Se $b = 0$, então $a + 0 = a = 0 + a$.

Suponhamos que $a + r = r + a$. Então: $a + r^+ = (a + r)^+ = (r + a)^+ = r + a^+ = r^+ + a$.

Portanto, $a + b = b + a$, para todos $a, b \in \mathbb{N}$.

Zero é elemento neutro

A definição juntamente com a comutatividade garantem que zero é o elemento neutro da adição.

Deixamos como exercício ao leitor a demonstração de que zero é o único elemento neutro da adição.

Lei do Cancelamento da Adição

Mostremos que $a + b = a + c \Rightarrow b = c$ por indução sobre a .

Se $a = 0$, então $b = a + b = a + c = c$.

Suponhamos que $r + b = r + c \Rightarrow b = c$. Então, supondo que $r^+ + b = r^+ + c$, temos que $(r + b)^+ = (b + r)^+ = b + r^+ = r^+ + b = r^+ + c = c + r^+ = (c + r)^+ = (r + c)^+$.

Por P_4 , segue que $r + b = r + c$. Pela hipótese de indução, $b = c$. ■

Lema 4. *Sejam $a, b \in \mathbb{N}$. Então $a + b = 0 \Rightarrow a = b = 0$.*

Demonstração: Suponhamos que $b \neq 0$. Então, $b = u^+$, para algum $u \in \mathbb{N}$. Daí,

$$0 = a + b = a + u^+ = (a + u)^+,$$

o que é um absurdo. Assim, $b = 0$ e, portanto, $a = 0$. ■

4 - Multiplicação em \mathbb{N}

A operação de multiplicação $(x, y) \mapsto x \cdot y$ em \mathbb{N} é definida mediante as condições:

- $a \cdot 0 = 0$;
- $a \cdot b^+ = a \cdot b + a$.

Numa igualdade $a \cdot b = c$, a e b são os *fatores* e c é o *produto*.

Exemplos:

$$1 \cdot 1 = 1 \cdot 0^+ = 1 \cdot 0 + 1 = 0 + 1 = 1;$$

$$1 \cdot 2 = 1 \cdot 1^+ = 1 \cdot 1 + 1 = 1 + 1 = 2;$$

$$2 \cdot 1 = 2 \cdot 0^+ = 2 \cdot 0 + 2 = 0 + 2 = 2;$$

$$3 \cdot 2 = 3 \cdot 2^+ = 3 \cdot 1 + 3 = ?$$

Propriedades da Multiplicação

$$\mathbf{M}_1 \quad 0 \cdot a = 0, \forall a \in \mathbb{N}.$$

$$\mathbf{M}_2 \text{ (Associativa)} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in \mathbb{N}.$$

$$\mathbf{M}_3 \text{ (Comutativa)} \quad a \cdot b = b \cdot a, \forall a, b \in \mathbb{N}.$$

$$\mathbf{M}_4 \text{ (1 é Elemento Neutro)} \quad 1 \cdot a = a, \forall a \in \mathbb{N}.$$

$$\mathbf{M}_5 \text{ (Lei do Anulamento do Produto)} \quad a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

$$\mathbf{M}_6 \text{ (Lei do Cancelamento da Multiplicação)} \quad a \cdot c = b \cdot c \text{ e } c \neq 0 \Rightarrow a = b.$$

$$\mathbf{M}_7 \text{ (Distributiva da Multiplicação em relação à Adição)} \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \\ (a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in \mathbb{N}.$$

Demonstração:

M_1

Usaremos indução sobre a .

Se $a = 0$, então $0 \cdot 0 = 0$, por definição.

Suponhamos $0 \cdot r = 0$. Então: $0 \cdot r^+ = 0 \cdot r + 0 = 0 + 0 = 0$.

Portanto, $0 \cdot a = 0$, para todo $a \in \mathbb{N}$.

M_7

Mostremos que $a \cdot (b + c) = a \cdot b + a \cdot c$ por indução sobre c .

Se $c = 0$, então $a \cdot (b + 0) = a \cdot b = a \cdot b + 0 = a \cdot b + a \cdot 0$.

Suponhamos $a \cdot (b + r) = a \cdot b + a \cdot r$. Então:

$$a \cdot (b + r^+) = a \cdot (b + r)^+ = a \cdot (b + r) + a = a \cdot b + a \cdot r + a = a \cdot b + a \cdot r^+,$$

usando a definição dada para a adição.

Agora, usemos indução sobre c para mostrar que $(a + b) \cdot c = a \cdot c + b \cdot c$.

Se $c = 0$, então $(a + b) \cdot 0 = 0 = 0 + 0 = a \cdot 0 + b \cdot 0$.

Suponhamos $(a + b) \cdot r = a \cdot r + b \cdot r$. Então:

$$(a + b) \cdot r^+ = (a + b) \cdot r + a + b = a \cdot r + b \cdot r + a + b = a \cdot r + a + b \cdot r + b = a \cdot r^+ + b \cdot r^+,$$

usando a definição para a multiplicação, a associatividade e a comutatividade da adição.

Portanto, $(a + b) \cdot c = a \cdot c + b \cdot c$, para todos $a, b, c \in \mathbb{N}$.

M_2

Usaremos indução sobre c .

Se $c = 0$, então $a \cdot (b \cdot 0) = a \cdot 0 = 0$, usando a definição.

Suponhamos $a \cdot (b \cdot r) = (a \cdot b) \cdot r$. Então:

$$a \cdot (b \cdot r^+) = a \cdot (b \cdot r + b) = a \cdot (b \cdot r) + a \cdot b = (a \cdot b) \cdot r + a \cdot b = (a \cdot b) \cdot r^+.$$

Portanto, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todos $a, b, c \in \mathbb{N}$.

M_4

Novamente usaremos indução sobre a .

Se $a = 0$, então $1 \cdot 0 = 0$, por definição.

Suponhamos $1 \cdot r = r$. Então: $1 \cdot r^+ = 1 \cdot r + 1 = r + 1 = r^+$.

Portanto, $1 \cdot a = a$, para todo $a \in \mathbb{N}$.

M_3

Usaremos indução sobre a .

Se $a = 0$, então $0 \cdot b = 0 = b \cdot 0$, usando M_1 e a definição.

Suponhamos $r \cdot b = b \cdot r$. Então:

$$b \cdot r^+ = b \cdot r + b = r \cdot b + 1 \cdot b = (r + 1) \cdot b = r^+ \cdot b,$$

usando M_7 e M_4 .

Portanto, $a \cdot b = b \cdot a$, para todos $a, b \in \mathbb{N}$.

M_5

Suponhamos que $a \cdot b = 0$ e $b \neq 0$. Assim, $b = u^+$, para algum $u \in \mathbb{N}$. Logo, $0 = a \cdot b = a \cdot u^+ = a \cdot u + a$. Pelo Lema, $a \cdot u = a = 0$.

M_6

Deixamos, a princípio, a demonstração da Propriedade M_6 como um exercício. Pesquise e aceite o desafio de demonstrá-la. De todo modo, daremos uma demonstração posteriormente.

■

5 - Relação de Ordem em \mathbb{N}

Define-se a relação \leq (menor do que ou igual) em \mathbb{N} do seguinte modo:

se $a, b \in \mathbb{N}$, dizemos que $a \leq b$ se $b = a + u$ para algum $u \in \mathbb{N}$.

O número u nessas condições é chamado *diferença* entre b e a e é indicado por $u = b - a$, onde b é o *minuendo* e a o *subtraendo*.

Desta forma, a subtração $(a, b) \mapsto a - b$ está definida apenas no caso em que os pares ordenados (a, b) satisfazem $b \leq a$.

Observamos que, o caso particular, em que $u = 0$ ocorre quando a e b são o mesmo elemento (iguais). Desta forma, podemos escrever $a - a = 0$, para todo $a \in \mathbb{N}$.

Algumas Propriedades

(i) $(b - a) + a = b$, sempre que $a \leq b$.

De fato, se $b - a = u$ ($a \leq b$), então $b = a + u = a + (b - a) = (b - a) + a$.

(ii) Se $c \leq a$, então $(a + b) - c = (a - c) + b$.

De fato, seja $a - c = u$ ($c \leq a$). Então $a = c + u$ e, portanto, $a + b = c + u + b = c + (u + b)$. Daí, $(a + b) - c = u + b = (a - c) + b$.

(iii) Se $b + c \leq a$, então $a - (b + c) = (a - b) - c$. Neste caso, podemos simplificar a notação da seguinte maneira: $(a - b) - c = a - b - c$.

Seja $a - (b + c) = u$ ($b + c \leq a$). Assim, $a = (b + c) + u$ e, então, $a - b = (b + c) + u - b = u + (b + c) - b = u + (b - b) + c = u + c$. Agora, $(a - b) - c = (u + c) - c = (u - c) + c = u = a - (b + c)$, onde usamos (i) e (ii).

(iv) Se $b \leq a$ e $d \leq c$, então $(a - b) + (c - d) = (a + c) - (b + d)$.

Sejam $a - b = u$ ($b \leq a$) e $c - d = v$ ($d \leq c$). Assim, $a = b + u$ e $c = d + v$. Agora, $(a + c) = (b + d) + (u + v)$ e $(a + c) - (b + d) = u + v = (a - b) + (c - d)$.

Outras Propriedades da Relação de Ordem em \mathbb{N}

As propriedades abaixo podem ser demonstradas por meio de resultados anteriores. Faça uma boa reflexão a respeito de cada uma delas.

O₁ (Reflexiva) $a \leq a, \forall a \in \mathbb{N}$.

O₂ (Antissimétrica) Se $a \leq b$ e $b \leq a$, então $a = b$.

O₃ (Transitiva) Se $a \leq b$ e $b \leq c$, então $a \leq c$.

O₄ (A relação \leq é total) $a \leq b$ ou $b \leq a$.

O₅ (A relação \leq é compatível com a adição) Se $a \leq b$, então $a + c \leq b + c, \forall c \in \mathbb{N}$.

O₆ (A relação \leq é compatível com a multiplicação) Se $a \leq b$, então $a \cdot c \leq b \cdot c, \forall c \in \mathbb{N}$.

Devido às seis propriedades anteriores, dizemos que \leq é uma relação de ordem total sobre \mathbb{N} compatível com a adição e a multiplicação de \mathbb{N} .

Definição 5. *Sejam a, b in \mathbb{N} . Dizemos que a é menor do que b e escrevemos $a < b$ se $b = a + v$, para algum $v \in \mathbb{N}, v \neq 0$.*

Claramente temos que $a < b \Leftrightarrow a \leq b$ e $a \neq b$.

O₇ Se $a < b$, então $a + 1 \leq b$.

O₈ Se X é um subconjunto não vazio de \mathbb{N} , então X possui um elemento m tal que $m \leq x$, para todo $x \in X$ (princípio do menor número natural).

Definição 6. O elemento m descrito na Propriedade O_8 é chamado elemento mínimo de X e é indicado por $m = \min X$.

Exercício: Demonstre que o elemento mínimo de um subconjunto não vazio X de \mathbb{N} é único.

Com efeito, suponhamos que existam $m_1 = \min X$ e $m_2 = \min X$. Sendo $m_1 = \min X$, segue que $m_1 \leq x$, para todo $x \in X$. Em particular, $m_1 \leq m_2$ (pois $m_2 \in X$). Da mesma forma, sendo $m_2 = \min X$, segue que $m_2 \leq m_1$. Portanto, $m_1 = m_2$.

Observação 1: Se X é um subconjunto não vazio de \mathbb{N} , um elemento $M \in X$ (caso exista) tal que $x \leq M$, para todo $x \in X$, é chamado elemento máximo de X e é indicado por $M = \max X$.

No caso em que X possui elemento máximo, este é único (demonstre!).

Em \mathbb{N} , há subconjuntos não vazios que não admitem elementos máximos, por exemplo, o conjunto de todos os múltiplos naturais de 3.

Observação 2: Alternativamente podemos usar $b \geq a$ com o significado $a \leq b$ e $b > a$ com o de $a < b$.

Mais Propriedades da Relação de Ordem em \mathbb{N}

- Se $a \leq b$ e $b < c$, então $a < c$.
- Se $a < b$, então $a + c < b + c, \forall c \in \mathbb{N}$.
- Se $a + c \leq b + c$, então $a \leq b, \forall c \in \mathbb{N}$.
- Se $a \leq b$ e $c \leq d$, então $a + c \leq b + d$.
- Se $a < b$ e $c \neq 0$, então $a \cdot c < b \cdot c$.

- Se $a < b$ e $c \leq d$, então $a + c < b + d$.
- Se $c \leq b$, então $a \cdot (b - c) = a \cdot b - a \cdot c$.

Demonstração de Algumas Propriedades

- **Reflexiva:** Basta ver que $a = a + 0$, para todo $a \in \mathbb{N}$.
- **Antissimétrica:** Por hipótese, $b = u + a$ e $a = b + v$, para certos $u, v \in \mathbb{N}$. Daí $a = a + (u + v)$ e, pela lei do cancelamento da adição, $u + v = 0$. Logo, $u = v = 0$, como já foi provado. Portanto, $a = b$.
- **A relação \leq é total:** Para cada $b \in \mathbb{N}$, seja S_b o subconjunto de \mathbb{N} formado pelos elementos n para os quais se verifica ao menos uma das seguintes condições:

(a) existe $u \in \mathbb{N}$ tal que $b = n + u$;

(b) existe $v \in \mathbb{N}$ tal que $n = b + v$.

Como para $n = 0$ a sentença (a) se verifica com $u = b$, então $0 \in S_b$. Seja $r \in S_b$. Se $r = b$, então $r^+ = b^+ = b + 1$ e, portanto, $r^+ \in S_b$, já que verifica (b). Suponhamos agora que $b = r + u$, $u \neq 0$. Então $u = v^+ = v + 1$, para algum $v \in \mathbb{N}$ e, daí, $b = r + (v + 1) = r^+ + v$, ou seja, r^+ satisfaz (a) e, portanto, pertence a S_b . Finalmente, se $r = b + v$, $v \neq 0$, então $r^+ = (b + v)^+ = b + v^+$, o que significa que $r^+ \in S_b$, pois cumpre a condição (b).

Desta forma, $S_b = \mathbb{N}$ e, por isso, para todo $b \in \mathbb{N}$, qualquer que seja o número natural a , ou $b = a + u$ ou $a = b + v$. Isto significa que $a \leq b$ ou $b \leq a$.

- **A relação \leq é compatível com a multiplicação:** Por hipótese, $b = a + u$, para algum $u \in \mathbb{N}$. Assim, $b \cdot c = (a + u) \cdot c = a \cdot c + u \cdot c$, donde resulta que $a \cdot c \leq b \cdot c$.
- **Princípio do Menor Número Natural:** Seja $H = \{n \in \mathbb{N} : n \leq x, \forall x \in X\}$. Como $0 \leq a, \forall a \in X$ ($a = 0 + a$), então $0 \in H$. Consideremos $a \in X$, o que é possível uma vez que $X \neq \emptyset$. Observando que $a < a + 1$, podemos afirmar que $a + 1 \notin H$ (pois se pertencesse,

deveria ocorrer $a + 1 \leq a$) e, assim, $H \neq \mathbb{N}$. Conhecendo-se P_5 , necessariamente existe um elemento $b \in \mathbb{N}$ tal que $b \in H$ e $b + 1 \notin H$ (caso contrário, teríamos $H = \mathbb{N}$). Devemos mostrar que $b = \min X$. Isto de fato é verdade, pois:

(i) como $b \in H$, temos que $b \leq x, \forall x \in X$;

(ii) suponhamos que $b \notin X$. Então $b < x$ para todo $x \in X$ e, assim, $b + 1 \leq x$, também para todo $x \in X$, o que implica que $b + 1 \in H$. Mas isso é impossível. Esta contradição nos leva a concluir que $b \in X$.

Observação 3: Uma pergunta que nos parece razoável após a construção axiomática que apresentamos de \mathbb{N} é a seguinte:

“será que a sequência formada pelo zero e seus sucessores esgota realmente o conjunto dos números naturais?”

Ou seja,

“será que não pode ocorrer $a < r < a^+ = a + 1$ para algum par de elementos $a, r \in \mathbb{N}$?”

Passamos agora à demonstração de que a resposta é negativa.

Suponhamos que $a < r < a + 1$. Então $r = a + u (u \neq 0)$ e $a + 1 = r + v (v \neq 0)$. Portanto,

$$a + 1 = a + (u + v)$$

o que implica que $u + v = 1$. Considerando que $u \neq 0$, então $u = r^+ = r + 1$. Assim, chegamos a

$$1 = u + v = (r + 1) + v = (r + v) + 1$$

e, portanto, $r + v = 0$. Mas disso decorre que $r = v = 0$. Temos uma contradição.

Assim, efetivamente, para todo $a \in \mathbb{N}$:

$$\{x \in \mathbb{N} : a < x < a + 1\} = \emptyset.$$

6 - Lei da Tricotomia em \mathbb{N}

Conhecendo a relação de ordem em \mathbb{N} e suas propriedades, estamos aptos a enunciar uma importante lei: a Lei da Tricotomia em \mathbb{N} .

Para quaisquer $a, b \in \mathbb{N}$, vale uma e só uma das relações:

$$a = b, a < b \text{ ou } b > a.$$

De fato, por O_4 , temos que $a \leq b$ ou $a \geq b$. Então $b = a + u$ ou $a = b + v$. Supondo $a \neq b$, devemos ter $u \neq 0$ para a primeira possibilidade e $v \neq 0$ para a segunda. Isto significa: $a \neq b \Rightarrow a < b$ ou $b < a$. Se ocorressem simultaneamente $a < b$ e $b < a$, então $b = a + r (r \neq 0)$ e $a = b + s (s \neq 0)$. Assim, $a = a + (r + s)$. Desta forma, $r + s = 0$ e, portanto, $r = s = 0$. Isto é uma contradição. Logo, se $a, b \in \mathbb{N}$, então $a = b, a < b$ ou $a > b$, exclusivamente. Esta é a chamada *Lei da Tricotomia*.

Mais Demonstrações

- M_6 : Queremos mostrar que $a \cdot c = b \cdot c, c \neq 0 \Rightarrow a = b$.

Se $a < b$, então $b = a + v (v \neq 0)$. Logo, $a \cdot c = b \cdot c = (a + v) \cdot c = a \cdot c + v \cdot c$, o que implica $v \cdot c = 0$. Por M_5 , $v = 0$ ou $c = 0$, o que é uma contradição. Analogamente, se prova que não pode ocorrer $b < a$.

- $a \cdot b = 1 \Rightarrow a = b = 1$: Supondo $a \cdot b = 1$, decorre que $a \neq 0$ e $b \neq 0$. Logo $a \geq 1$ e $b \geq 1$. Supondo, por exemplo, $a > 1$, temos que $a = 1 + v (v \neq 0)$. Como $b = 1 + u$ (pois $b \geq 1$), podemos concluir que

$$1 = a \cdot b = (1 + v) \cdot (1 + u) = 1 + u + v + u \cdot v$$

o que leva a

$$v + (u + u \cdot v) = 0$$

e, assim, $u + u \cdot v = v = 0$, o que não é possível. Portanto, $a = 1$ e, conseqüentemente, $b = 1$.

7 - Breves Comentários sobre a Construção Lógico-Formal de \mathbb{Z}

Brevemente, desejamos descrever a construção lógico formal do conjunto dos números inteiros \mathbb{Z} . O objetivo é dar um sentido matemático a todas as expressões do tipo $a - b$, para quaisquer $a, b \in \mathbb{N}$, de maneira a podermos tratar como entes do mesmo conjunto tanto aquelas como $10 - 6$, $8 - 4$, $7 - 3$, $5 - 1$ e $4 - 0$ quanto aquelas como $6 - 10$, $3 - 5$, $2 - 4$, $1 - 3$ e $0 - 2$, por exemplo. Nesse sentido, convém observar primeiramente que subjacente a cada “diferença” $a - b$ está o par ordenado $(a, b) \in \mathbb{N} \times \mathbb{N}$. Ainda, é fácil ver que, por exemplo, a igualdade em \mathbb{N}

$$9 - 6 = 5 - 2$$

equivale a

$$9 + 2 = 5 + 6.$$

De uma maneira geral, se $a, b, c, d \in \mathbb{N}$, $a \geq b$ e $c \geq d$, vale a equivalência:

$$a - b = c - d \Leftrightarrow a + d = b + c.$$

Essas considerações, aliadas ao fato de que o conjunto dos números inteiros a ser construído, deve ser uma “extensão” de \mathbb{N} , ajudam a entender o caminho que apresentaremos.

No conjunto $\mathbb{N} \times \mathbb{N}$, consideremos a relação \approx definida por: para quaisquer (a, b) e (c, d) em $\mathbb{N} \times \mathbb{N}$,

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

Para a relação \approx valem as propriedades:

Reflexiva: Como para todo $(a, b) \in \mathbb{N} \times \mathbb{N}$, se verifica que $a + b = b + a$, temos que $(a, b) \approx (a, b)$.

Simétrica: Suponhamos que $(a, b) \approx (c, d)$. Então $a + d = b + c \Rightarrow c + b = d + a$. Logo, $(c, d) \approx (a, b)$.

Transitiva: Suponhamos que $(a, b) \approx (c, d)$ e $(c, d) \approx (e, f)$. Então $a + d = b + c$ e $c + f = d + e$. Assim, $a + d + f = b + c + f$ e $c + f + b = d + e + b$. Daí, $a + d + f = d + e + b \Rightarrow a + f = b + e$. Desta forma, $(a, b) \approx (e, f)$.

Com isso, temos que \approx é uma relação de equivalência em $\mathbb{N} \times \mathbb{N}$ e, conseqüentemente, determina uma partição neste conjunto em classes de equivalência. Para cada $(a, b) \in \mathbb{N} \times \mathbb{N}$, indicaremos por $\overline{(a, b)}$ a classe de equivalência determinada por $(a, b) \in \mathbb{N} \times \mathbb{N}$. Assim,

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} : (x, y) \approx (a, b)\} = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x + b = y + a\}.$$

O conjunto quociente de $\mathbb{N} \times \mathbb{N}$ por \approx , ou seja, o conjunto de todas as classes de equivalência $\overline{(a, b)}$, para qualquer $(a, b) \in \mathbb{N} \times \mathbb{N}$, será indicado por \mathbb{Z} . Ou seja,

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \approx = \left\{ \overline{(a, b)} : (a, b) \in \mathbb{N} \times \mathbb{N} \right\}.$$

Exemplos:

$$\overline{(5, 2)} = \{(3, 0), (4, 1), (5, 2), (6, 3), \dots\}.$$

$$\overline{(2, 5)} = \{(0, 3), (1, 4), (2, 5), (3, 6), \dots\}.$$

É fácil ver que $\overline{(a, b)} = \overline{(c, d)}$ se, e somente se, $(a, b) \approx (c, d)$ se, e somente se, $a + d = b + c$. Em particular, vale o seguinte:

se $a \geq b$, então $\overline{(a, b)} = \overline{(a - b, 0)}$, pois $a + 0 = (a - b) + b$; e se $b \geq a$, então $\overline{(a, b)} = \overline{(0, b - a)}$, uma vez que $a + (b - a) = b + 0$. Assim, se $\overline{(a, b)} \in \mathbb{Z}$, então $\overline{(a, b)} = \overline{(c, 0)}$ ou $\overline{(a, b)} = \overline{(0, c)}$, para algum $c \in \mathbb{N}$. E essa maneira de representar o elemento $\overline{(a, b)}$ é única pois, por exemplo, se $\overline{(c, 0)} = \overline{(d, 0)}$, então $c + 0 = d + 0$ e daí $c = d$.

Adição em \mathbb{Z}

Escrevamos $4 \in \mathbb{N}$ e $3 \in \mathbb{N}$ sob a forma $4 = 5 - 1$ e $3 = 7 - 4$. Então:

$$4 + 3 = (5 - 1) + (7 - 4) = (5 + 7) - (1 + 4).$$

Definição 7. Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ em \mathbb{Z} . A soma de m com n é dada por

$$m + n = \overline{(a + c, b + d)}.$$

Propriedades da Adição em \mathbb{Z}

A₁ Associativa.

A₂ Comutativa.

A₃ $\overline{(0, 0)}$ é elemento neutro.

A₄ $m = \overline{(a, b)} \in \mathbb{Z}$ admite oposto, a saber, $-m = \overline{(b, a)}$.

Subtração em \mathbb{Z}

Definição 8. Para cada par $m, n \in \mathbb{Z}$, a diferença entre m e n , $m - n$, é o elemento $m + (-n) \in \mathbb{Z}$:

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

A subtração em \mathbb{Z} não é associativa, nem comutativa e não admite elemento neutro.

Multiplicação em \mathbb{Z}

Já que $3 = 5 - 2$ e $6 = 10 - 4$, podemos escrever:

$$3 \cdot 6 = (5 - 2) \cdot (10 - 4) = (5 \cdot 10 + 2 \cdot 4) - (5 \cdot 4 + 2 \cdot 10) = 58 - 40 = 18.$$

Isto motiva a

Definição 9. Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ em \mathbb{Z} . Chama-se produto de m por n , $m \cdot n$, o elemento de \mathbb{Z} dado por

$$m \cdot n = \overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}.$$

Propriedades da Multiplicação em \mathbb{Z}

M₁ Associativa.

M₂ Comutativa.

M₃ $\overline{(1, 0)}$ é elemento neutro.

M₄ Lei do Anulamento do Produto: $m \cdot n = 0 \Rightarrow m = 0$ ou $n = 0$.

M₅ Distributiva da Multiplicação em relação à Adição:

$$m \cdot (n + r) = m \cdot n + m \cdot r$$

Claramente há muitos detalhes a serem estudados a respeito das operações definidas sobre \mathbb{Z} e suas propriedades. Fica o convite ao leitor de aprofundar os estudos e investigar não somente estas como outras questões.

Referências Bibliográficas

- [1] DOMINGUES, H. H. *Fundamentos de Aritmética*, São Paulo: Atual, 1991.
- [2] FILHO, E. A. *Teoria Elementar dos Números*, São Paulo: Nobel, 2. ed. 1985.
- [3] GOMES, O. R. & SILVA, J. C. *Estruturas Algébricas para Licenciatura: Introdução à Teoria dos Números*, Brasília: Ed. do Autor, 2008.