UNIVERSIDADE FEDERAL DE UBERLÂNDIA - UFU
FACULDADE DE MATEMÁTICA - FAMAT
CAMPUS SANTA MÔNICA

ÊNIO EUSTÁQUIO DE OLIVEIRA

Formação dos Conjuntos dos Números Naturais e dos Inteiros via Relação de Equivalência

Uberlândia - Minas Gerais
Agosto de 2022

ÊNIO EUSTÁQUIO DE OLIVEIRA

Formação dos Conjuntos do Números Naturais e dos Inteiros via Relação de Equivalência

Trabalho de Conclusão de Curso apresentado à Comissão Acadêmica da Faculdade de Matemática da Universidade Federal de Uberlândia como requisito parcial para obtenção da graduação de **Licenciatura em Matemática**.

Orientador: Prof. Dr. Antônio Carlos Nogueira.

Uberlândia - Minas Gerais
Agosto de 2022

Oliveira, Ênio Eustáquio de, 1947 -

Formação dos Conjuntos dos Números Naturais e dos Inteiros via Relação de Equivalência / Ênio Eustáquio de Oliveira. - 2022

43 p. : il.

Orientador: Antônio Carlos Nogueira

Trabalho de Conclusão de Curso - Universidade Federal de Uberlândia, Licenciatura em Matemática.

1. Conjunto dos números naturais. 2. Conjunto dos números inteiros. 3. Axiomas de Peano. 4. Relação de equivalência. 5. Classe de equivalência. I. Antônio Carlos Nogueira. II. Universidade Federal de Uberlândia. III. Faculdade de Matemática. IV. Formação dos Conjuntos dos Números Naturais e dos Inteiros via Relação de Equivalência.

ÊNIO EUSTÁQUIO DE OLIVEIRA

Formação dos Conjuntos dos Números Naturais e dos Inteiros
via Relação de Equivalência

Trabalho de Conclusão de Curso apresentado à Comissão Acadêmica da Faculdade de Matemática da Universidade Federal de Uberlândia como requisito parcial para obtenção da graduação de **Licenciatura em Matemática**.

Trabalho de Conclusão de Curso apresentado e APROVADO em 19/08/2022, pela seguinte Banca Examindadora:

Prof. Dr. Antônio Carlos Nogueira (Orientador)
FAMAT - UFU

Profa. Dra. Érika Maria Chioca Lopes
FAMAT - UFU

Profa. Dra. Marisa de Souza Costa
FAMAT - UFU

Uberlândia - Minas Gerais
19 de Agosto de 2022

Dedicatória

Dedico este trabalho à minha família e amigos.

Agradecimentos

Agradeço a Deus por me dar a oportunidade de conviver com tantas pessoas, na escola, no trabalho, enfim, na vida.

Sinto gratidão e felicidade por ter, durante anos, conhecido e estabelecido amizade com tantos colegas e professores na UFU. Alguns professores ainda dando aulas, outros que já se aposentaram, mas sempre me deram a oportunidade de estabelecer uma grande empatia com os mesmos.

Agradeço em especial ao professor Antônio Carlos Nogueira. Quando pedi para que me orientasse, colocou em prática toda sua paciência, seu conhecimento e sua humildade aceitando meu pedido.

Também, em especial, agradeço a esse meu ex-colega de sala e hoje meu grande amigo, que sempre está pronto a me ajudar e ainda me estimula a fazer o que acho que não sou capaz. Obrigado Ueslei Ferreira Costa.

"A vida pode não ser tão fácil, mas a cada obstáculo superado você ganha força pra seguir em frente." - Ayrton Senna

Resumo

Este trabalho tem como objetivo apresentar a construção lógica formal dos conjuntos dos números naturais e dos inteiros, via Axiomas de Peano. Na construção dos inteiros, usamos o conceito de relação de equivalência e classe de equivalência.

Palavras-chave: conjunto dos números naturais, conjunto dos números inteiros, axiomas de Peano, relação de equivalência, classe de equivalência.

Abstract

This work aims to present the formal logical construction of the sets of natural numbers and integers, via Peano Axiomas. In the construction of integers, we use the concept of equivalence relationship and equivalence class.

Keywords: set of natural numbers, set of integers, Peano axiomas, equivalence relation, equivalence class.

Sumário

Lista de ilustrações

INTRODUÇÃO

Antes de construirmos o conjunto dos números naturais, temos que nos ater a alguns registros históricos a respeito do que aconteceu durante séculos. A matemática partia de verdades evidentes e prosseguia através de raciocínios cuidadosos para descobrir verdades escondidas.

Em todos os tempos, a matemática esteve presente em todas as atividades humanas. Um clássico exemplo da noção intuitiva de contagem era a correspondência entre ovelhas de um rebanho, pedrinhas contidas em pequenos sacos, marcas em ossos de animais ou até mesmo pedaços de madeira, todos utilizados pelos incas. Alguns séculos passaram até o desenvolvimento teórico do conceito de número, que foi lento e complexo e envolveu diversas civilizações. Os babilônios, 2000 a.C, desenvolveram o sistema de numeração sexagesimal.

A fundamentação matemática do conceito de número ocorreu no final do século XIX, através dos trabalhos propostos por Richard Dedekind $(1831-1916)$, Georg Cantor $(1845 - 1918)$ e Giuseppe Peano $(1858 - 1932)$. Esses estudos foram motivados pelas demandas teóricas que surgiram a partir do volume de conhecimento matemático que foi adquirido a partir do cálculo diferencial e integral de Isaac Newton$(1643-1723)$ e Gottfried Wilhelm Leibniz$(1646-1716)$, no século XVII. Depois de uma rápida exposição histórica, passaremos a estudar os axiomas de Peano, e, depois de alguns exemplos, vamos construir o conjunto dos naturais, inteiros e por fim, racionais.

A ideia de número natural sempre esteve presente e associada à ideia de quantidade, isso porque desde os tempos mais remotos, o homem sempre teve a necessidade de contar, como acontece intuitivamente nos primeiros anos escolares, quando conhecemos os números naturais. Neste trabalho, queremos construir o conjunto dos números naturais de uma forma axiomática.

Vamos assumir certos axiomas que são capazes de caracterizar completamente a ideia intuitiva do conjunto dos números naturais, caracterizando rigorosamente tudo que já conhecemos intuitivamente (como conjunto dos números naturais). Para tal, vamos usar os axiomas de Peano.

A seguir, temos fotografias dos três grandes matemáticos envolvidos na fundamentação do conceito de número.

Figura 1 – Richard Dedekind (1831 – 1916). *Fonte:* Wikipédia (Acesso: 15/04/2022).

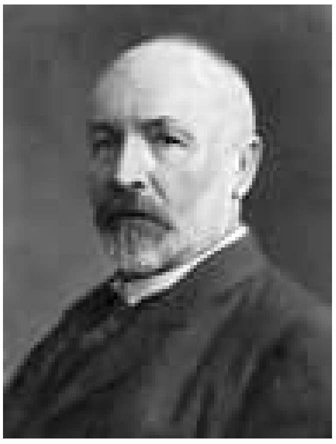

Figura 2 – Georg Cantor (1845 – 1918). *Fonte:* Wikipédia (Acesso: 15/04/2022).

Figura 3 – Giuseppe Peano (1858 – 1932). *Fonte:* Wikipédia (Acesso: 15/04/2022).

1 Números Naturais

É natural pensarmos que o conjunto dos números naturais começa do zero e prossegue de um em um. Uma outra ideia mais detalhada é o princípio da indução finita, que consiste em pensar em um subconjunto não-vazio "A" dos números naturais, que contenha um número (6, por exemplo) e chamá-lo de x. Seu sucessor será então $x + 1$ (7), logo o subconjunto conterá o 7 que é $6+1$, conterá o 8 que é $7+1$ e assim sucessivamente. Dessa forma, "A" conteria todos os números naturais a partir do 6; mas, se substituíssemos 6 por zero, então "A" seria igual ao conjunto dos números naturais.

1.1 Axiomas de Peano

Os axiomas de Peano são uma construção rigorosa dessas ideias intuitivas e se apoiam em conceitos matemáticos que já conhecemos ou admitimos conhecidos como os conceitos de conjunto e de função. A ideia é:

A1) Existe um conjunto $\mathbb{N}$ e uma função $s : \mathbb{N} \to \mathbb{N}$ que associa a cada $n \in \mathbb{N}$ o seu sucessor;
A2) s é injetora;
A3) Existe um elemento de "$\mathbb{N}$" que denotaremos como 0 e chamaremos de zero que não está na imagem de s, isto é: $0 \notin Im(s)$.
A4) Se um subconjunto X de $\mathbb{N}$ satisfizer (i) e (ii) abaixo, então $X = \mathbb{N}$:
i) $0 \in \mathbb{N}$;
ii) Se $k \in X$ então $s(k) \in X$.

A função que denominamos de s, vem da palavra *sucessor* de modo que se $x \in \mathbb{N}$, $s(x)$ é chamado *sucessor* de $x \in \mathbb{N}$. Daí somos levados a concluir que elementos diferentes de $\mathbb{N}$ têm sucessores diferentes.

$\mathbb{N}$ se chama **conjunto dos números naturais**, e $\mathbb{N} \neq \emptyset$ pois $0 \in \mathbb{N}$ (pelo axioma A2). Além disso, $s(0) \neq 0$ (pois $0 \notin Im(s)$ e $s(0) \in Im(s)$, então $\mathbb{N}$ contém pelo menos dois elementos, 0 e $s(0)$.

Como por definição "s" é injetora, então $0 \neq s(0)$ e $s(s(0)) \neq s(0)$, assim $s(s(0))$ é mais um elemento de $\mathbb{N}$. Daí, chegamos a conclusão que de forma iterada notamos que os sucessores são distintos dois a dois. Mais adiante isso será provado através de estrutura numérica e de ordem de $\mathbb{N}$.

Nas seções seguintes introduziremos as operações de adição e multiplicação de números naturais e provaremos algumas de suas propriedades básicas.

1.2 Adição de Números Naturais

Definição 1.1. *A adição de números naturais m e n é indicada por $m + n$ e é definida do seguinte modo:*

$$\begin{cases} m + 0 &= m \\ m + s(n) &= s(m + n) \end{cases}$$

A definição acima nos dá que a soma de um número arbitrário com 0 é $m+0 = m$, também que a soma de m com $s(0)$ é $m+s(0) = s(m+0) = s(m)$. Daí podemos escrever ainda $m + s(s(0)) = s(m + s(0)) = s(s(m)) = s(m + 1)$.

Esse processo pode ser formalizado através do princípio da indução que nos mostra que a soma $m + n$ está definida para todos os números naturais.

Lema 1.1. *Para cada natural m fixado anteriormente, $S_m = \{n \in \mathbb{N} \mid m + n$ está definida$\} = \mathbb{N}$.*

Demonstração: Segue da definição de adição que $0 \in S_m$; além disso, se $k \in S_m$ então $s(k) \in S_m$, pois pela definição $m + s(k) = s(m + k)$. Do axioma A4 concluímos que $S_m = \mathbb{N}$. Como m é arbitrário $S_m = \mathbb{N}$, para todo $m \in \mathbb{N}$. O que nos mostra que $m + n$ está definida para todo par(m, n) de números naturais.

$\blacksquare$

Definição 1.2. *Indicaremos por 1 o número natural que é sucessor de 0, ou seja, $s(0) = 1$.*

Proposição 1.1. *Para todo natural m temos que $s(m) = m+1$ e $s(m) = 1+m$, portanto $m + 1 = 1 + m$.*

Demonstração: Primeiro observamos que $m + 1 = m + s(0) = s(m + 0) = s(m)$. Seja $A = \{m \in \mathbb{N} \,|\, s(m) = 1 + m\}$. Note que $0 \in A$, pois $s(0) = 1 = 1 + 0$. Vamos mostrar que para $m \in A$ teremos $s(m) \in A$. Por hipótese $s(m) = 1 + m$, daí $s(s(m)) = s(1 + m) = 1 + s(m)$, mostrando que $s(m) \in A$. Pelo axioma A4, concluímos que $A = \mathbb{N}$.

$\blacksquare$

Teorema 1.1. *O conjunto* $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$.

Demonstração: usando a notação indo-arábica de base 10, temos que: $s(1) = 2, s(2) = 3, s(3) = 4, s(4) = 5, s(5) = 6, s(6) = 7, \dots, s(n) = n + 1, \dots$. Logo, $\mathbb{N}$ contém o conjunto $S = \{0, s(0), s(s(0)), s(s(s(0))), \dots\}$, ou seja, $S = \{0, 1, 2, 3, 4, 5, \dots\}$. O conjunto S foi construído como um subconjunto de $\mathbb{N}$ que contém o "0" e o sucessor de qualquer elemento nele contido. Pelo princípio da indução, segue que $S = \mathbb{N}$.

$\blacksquare$

Em nosso conjunto S, temos $0 \neq 1$, porém ainda não podemos comparar 0 com 1, isto é, ainda temos que formalizar a ideia de que 1 é maior que 0. Para isso temos que definir uma relação de ordem em $\mathbb{N}$. Isto será feito mais adiante.

Exemplo 1.1. *Apresentamos algumas adições em* $\mathbb{N}$.

a) $1 + 1 = s(1) = 2$;
b) $2 + 1 = s(2) = 3$;
c) $2 + 2 = 2 + s(1) = s(2 + 1) = s(2 + s(0)) = s(s(2 + 0)) = s(s(2)) = s(3) = 4$;
d) $0 + 2 = 0 + s(1) = s(0 + 1) = s(1 + 0) = s(1) = 2$.

Algumas das propriedades da adição que parecem óbvias podem ser demonstradas pelos axiomas de Peano e por propriedades demonstradas anteriormente.

Proposição 1.2. *Temos o* 0 *como elemento neutro da adição, ou seja,* $m+0 = m = 0+m$.

Demonstração: Da definição de adição temos que $m + 0 = m$, $\forall\, n \in \mathbb{N}$. Seja $A = \{m \in \mathbb{N} | 0 + m = m\}$. Observe que $0 \in A$, pois $0 + 0 = 0$; além disso se $m \in A$, então $0 + m = m$ e daí $0 + s(m) = s(0 + m) = s(m)$, ou seja, $s(m) \in A$. Pelo axioma A4 segue que $A = \mathbb{N}$.

$\blacksquare$

Teorema 1.2. *Sejam m, n e p números naturais arbitrários. Temos:*

i) propriedade associativa da adição:

$$m + (n + p) = (m + n) + p$$

ii) propriedade comutativa da adição:

$$n + m = m + n$$

iii) lei do cancelamento da adição:

$$m + p = n + p \Longrightarrow n = m$$

Demonstração:

i) Sejam m e n números naturais em A e seja $A_{m,n} = \{p \in \mathbb{N} \mid m+(n+p) = (m+n)+p\}$. Observe que $0 \in A_{m,n}$ pois $m + (n + 0) = m + n = (m + n) + 0$ Admitamos que $k \in A_{m,n}$ e vamos provar que $s(k) \in A_{m,n}$; veja, $m + (n + s(k)) = m + s(n + k) = s(m + (n + k)) = s((m + n) + k) = (m + n) + s(k)$, e isto mostra que $s(k) \in A$. Portanto, pelo axioma A4, $A_{m,n} = \mathbb{N}$, pois m e n são arbitrários.

ii) Desejamos mostrar que: $n + m = m + n$. Para isto vamos usar indução sobre n. Primeiro mostraremos que $m+1 = 1+m$, $\forall\, m \in \mathbb{N}$. Para $m = 0$, temos $0+1 = 1 = 1+0$ e supondo que $m + 1 = 1 + m$, temos que:

$$1 + s(m) = s(1 + m) = s(m + 1) = m + s(1),$$

ou seja,

$$1 + (m + 1) = m + (1 + 1) = (m + 1) + 1;$$

portanto, pelo princípio de indução, $1 + m = m + 1$, $\forall\, m$.

Suponha agora que $m + n = n + m$, para algum $n \geq 1$; então

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

e, portanto, pelo princípio de indução, segue que $m + n = n + m$, $\forall\, m, n \in \mathbb{N}$.

iii) Queremos mostrar que: $m + p = n + p \Longrightarrow m = n$.

Para $p = 0$, temos: $m + 0 = n + 0 \Longrightarrow m = n$.

Para $p = 1$, temos: $m + 1 = n + 1 \Longrightarrow s(m) = s(n) \Longrightarrow m = n$, pois s é injetora.

Para $p = k$, supondo que $m + k = n + k \Longrightarrow m = n$, então $m + (k + 1) = n + (k + 1) \Longrightarrow s(m + k) = s(n + k) \Longrightarrow m + k = n + k \Longrightarrow m = n$.

■

1.3 Multiplicação de Números Naturais

Definição 1.3. *A multiplicação de dois números naturais m e n é indicada pelo produto $m \cdot n$, sendo definida do seguinte modo:*

$$\begin{cases} m \cdot 0 &= 0 \\ m \cdot (n+1) &= m \cdot n + m \end{cases}$$

Notação 1.1. *Por simplicidade, adotaremos $m \cdot n = mn$.*

Vejamos um exemplo:

$$\begin{aligned} 2 \cdot 3 &= 2 \cdot (2+1) \\ &= 2 \cdot 2 + 2 \\ &= 2 \cdot (1+1) + 2 \\ &= 2 \cdot 1 + 2 + 2 \\ &= 2 \cdot (0+1) + 2 + 2 \\ &= 2 \cdot 0 + 2 + 2 + 2 \\ &= 0 + 2 + 2 + 2 \\ &= 2 + 2 + 2 = 6 \end{aligned}$$

Teorema 1.3. *Para m, n e p naturais arbitrários, seguem as seguintes proposições:*

i) $m, n \in \mathbb{N}$, temos $mn \in \mathbb{N}$, isto é, a multiplicação de fato é uma operação em $\mathbb{N}$;

ii) existência do elemento neutro multiplicativo: $1 \cdot n = n \cdot 1 = n$;

iii) distributividade: $m(n+p) = mn + mp$ e $(m+n)p = mp + np$;

iv) associatividade: $m(np) = (mn)p$;

v) comutatividade: $mn = nm$;

vi) $mn = 0 \Longrightarrow m = 0$ ou $n = 0$.

Demonstração: As demonstrações destas propriedades podem ser feitas usando o princípio de indução. Faremos aqui a prova de (ii); as demais são deixadas para o leitor como exercício. Primeiro mostraremos que $1 \cdot n = n, \forall n$: para $n = 0$, temos, por definição, $1 \cdot 0 = 0$. Supondo que $1 \cdot n = n$, temos, $1 \cdot (n+1) = 1 \cdot n + 1 = n + 1$; logo, por indução, $1 \cdot n = n, \forall n$.

Observe agora que, dado $n \in \mathbb{N}$, $n \cdot 1 = n \cdot (0+1) = n \cdot 0 + n = 0 + n = n$. Assim, fica provado que $1 \cdot n = n \cdot 1 = n, \forall n$.

■

1.4 Relação de Ordem em $\mathbb{N}$

A relação de ordem em $\mathbb{N}$ nos permitirá comparar os números naturais: da formação do conjunto notamos que 0 é menor do que 1, que 1 é menor do que 2 e assim por adiante.

Definição 1.4. *Uma relação R em $\mathbb{N}$ se diz uma relação de ordem sobre um conjunto não vazio em A, se satisfizer, para quaisquer x, y, $z \in A$ dados, as seguintes condições:*

i) reflexividade: xRx;

ii) antisimétrica: se xRy e yRz então $x = y$;

iii) transitividade: se xRy e yRz então xRz.

Um conjunto não vazio A munido de uma relação de ordem, diz-se um *conjunto ordenado*.

Definição 1.5. *Dados m, $n \in \mathbb{N}$, dizemos que mRn se existir $p \in \mathbb{N}$ tal que $n = m + p$.*

Demonstração: Vamos mostrar que R é uma relação de ordem:

i) $\forall\ m \in \mathbb{N}$, mRm, pois $m = m + 0$, portanto R é reflexiva;

ii) Se m, $n \in \mathbb{N}$ tais que mRn e nRm; então existem p, $q \in \mathbb{N}$ tal que $n = m + q$ e $m = n + p \Longrightarrow n = (n+p) + q = n + (p+q) \Longrightarrow p + q = 0 \Longrightarrow p = 0$ e $q = 0$, portanto $m = n$;

iii) Se mRn e nRp, então existem $r, s \in \mathbb{N}$ tais que $n = m + r$ e $p = n + s$; logo $p = n + s = (m + r) + s = m + (r + s)$, e como $r + s \in \mathbb{N}$, temos que mRp.

Concluímos assim que R é uma relação de ordem sobre $\mathbb{N}$; a partir daqui indicaremos esta relação R com o símbolo $\leqslant$.

■

1.5 Lei de Tricotomia

Teorema 1.4. *Para quaisquer m, $n \in \mathbb{N}$, temos que uma e apenas uma das seguintes relações acontece:*

i) $m < n$;

ii) $m = n$;

iii) $m > n$.

Demonstração: Isso mostra que duas dessas relações não podem ocorrer simultaneamente. E mostraremos que uma delas deve ocorrer necessariamente. Note que as relações (*i*) e (*ii*), (*ii*) e (*iii*) são incompatíveis por definição. Para (*i*) e (*iii*) ocorrendo simultaneamente, temos: $n = m + p$ e $m = n + q$; com $p, q \in \mathbb{N}\backslash\{0\}$, daí vem: $n + 0 = n = m + p = (n + q) + p = n + (p + q)$.

Pela lei do corte $p + q = 0 \Longrightarrow p = q = 0$, o que é uma contradição. Ao mesmo tempo, devemos mostrar que uma das três relações acontece.

Seja um número arbitrário $m \in \mathbb{N}$ e M um conjunto definido como: $M = \{x \in \mathbb{N} \mid x = m$ ou $x > m$ ou $x < m\}$. Vamos provar por indução sobre x que $M = \mathbb{N}$. Temos que $0 \in M$, pois $m = 0$ ou $m \neq 0$. Por indução, devemos ter que se $k \in M$ então $k + 1 \in M$. Podemos considerar três opções:

1^a) $k = m$ então $k + 1 = m + 1 \Longrightarrow k + 1 > m$ e portanto $k + 1 \in M$;

2^a) $k > m$, neste caso existe $p \in \mathbb{N}\backslash\{0\}$, tal que $k = m + p$, então $k + 1 = (m + p) + 1 = m + (p + 1) \Longrightarrow k + 1 > m$, logo $k + 1 \in M$;

3^a) $k < m$, neste caso existe $p \in \mathbb{N}\backslash\{0\}$ tal que $m = k + p$, e como $p \neq 0$, então $p = p_1 + 1$ para um certo $p_1 \in \mathbb{N}$, logo $m = k + (p_1 + 1) = k + (1 + p_1) = (k + 1) + p_1$. Se $p_1 = 0 \Longrightarrow m = k + 1$ e $k + 1 \in M$, se $p_1 \neq 0$ então $m > k + 1$ e $k + 1 \in M$.

Pelo princípio de indução, segue que $M = \mathbb{N}$.

■

2 Números Inteiros

2.1 Conceitos Preliminares

Quando construímos o conjunto dos números naturais, as soluções para equações, como $a+x=b$, não seria possível em $\mathbb{N}$, pois se b não for maior ou igual a "a", a equação acima não tem solução em $\mathbb{N}$. Devemos agora propor uma extensão dos números naturais a um conjunto que vamos denominar como conjunto dos números inteiros e simbolizá-los por $\mathbb{Z}$, de forma que, dada uma equação nesse conjunto, ela tenha solução nesse próprio conjunto.

Embora o conjunto dos números naturais possua uma cópia no conjunto dos números inteiros, este não deve ser entendido como subconjunto dos inteiros ($\mathbb{Z}$).

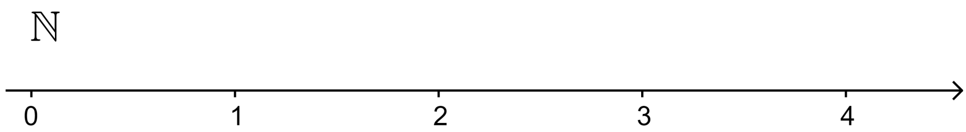

Figura 4 – Reta numérica dos números naturais. *Fonte:* próprio autor.

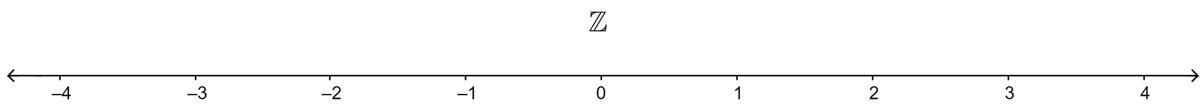

Figura 5 – Reta numérica dos números inteiros. *Fonte:* próprio autor.

Observe que a operação $a-b$ de números naturais não está definida no conjunto dos naturais, pois lá só temos as operações de adição e produto.

Nosso objetivo ao estabelecer o conjunto dos números inteiros é dar sentido às operações do tipo $a-b$ ou $b-a$ quando a e b pertençam ao conjunto dos números naturais independentes da ordem de grandeza dos mesmos. Notamos também uma certa equivalência quando operamos $7-3 \cong 9-5$, o que vamos provar a partir da nossa construção: se trocarmos a operação por adição

$$7+5=9+3$$

a igualdade se verifica; assim,

$$a - b = c - d,$$

com a, b, c, $d \in \mathbb{N}$ equivale a

$$a + d = c + b$$

(perfeitamente explicável em $\mathbb{N}$.)

2.2 Relação de Equivalência em $\mathbb{N} \times \mathbb{N}$

Definição 2.1. *Uma relação R sobre um conjunto $A \neq \emptyset$ é chamada de equivalência se satisfazer, para quaisquer $x, y, z \in A$ dados, as seguintes condições:*

$i)$ reflexividade: xRx;

$ii)$ simétrica: se xRy então yRz;

$iii)$ transitividade: se xRy e yRz então xRz.

O exemplo canônico da relação de equivalência é quando temos uma relação de igualdade. Dentre muitos exemplos de relação de equivalência temos a relação: (congruência). Antes vejamos duas definições.

Definição 2.2. *Sejam os números inteiros a e b dados. Dizemos que **a divide b** (representamos por $a \mid b$) se existir um inteiro k tal que $a \cdot k = b$. Ou seja: $a \mid b \Longleftrightarrow \exists\, k\, inteiro;\ a \cdot k = b$.*

Quando $a \mid b$, dizemos também que $\boldsymbol{a}$ é um **divisor** de $\boldsymbol{b}$ ou, equivalentemente, que $\boldsymbol{b}$ é um **múltiplo** de $\boldsymbol{a}$.

Definição 2.3. *Se a, b e $m \in \mathbb{Z}$ com $m > 0$, dizemos que **a** é **congruente** a **b módulo m** se $m \mid (b - a)$. Denotaremos essa situação por $a \equiv b \mod m$.*

Exemplo 2.1. *Seja a relação $R = \{(a, b) \mid a \equiv b \mod m\}$, mostrar que é uma relação de equivalência em $\mathbb{Z}$.*

$i)$ Reflexiva: $a \equiv a \mod m \Longrightarrow m \mid (a - a) \Longrightarrow m \mid 0$;

$ii)$ Simétrica: $a \equiv b \mod m \Longrightarrow m \mid (b - a) \Longrightarrow \exists\, k \in \mathbb{Z}$ tal que $m \cdot k = b - a \Longleftrightarrow m \cdot (-k) = a - b \Longrightarrow m \mid (a - b) \Longrightarrow b \equiv a \mod m$;

iii) Transitiva: $a \equiv b \mod m$ e $b \equiv c \mod m \Longrightarrow a \equiv c \mod m$. De fato, sejam k_1 e $k_2 \in \mathbb{Z}$ tais que: $mk_1 = b - a \Longleftrightarrow b = mk_1 + a$ e $mk_2 = c - b \Longrightarrow mk_2 = c - (mk_1 + a) \Longleftrightarrow mk_2 + mk_1 = c - a \Longleftrightarrow m(k_1 + k_2) = c - a \Longrightarrow m \mid (c - a) \Longrightarrow a \equiv c \mod m$.

Provando assim que a congruência é uma relação de equivalência em $\mathbb{Z}$.

■

Nosso objetivo é definir um número inteiro como uma classe de equivalência dada por uma relação de equivalência no conjunto $\mathbb{N} \times \mathbb{N}$. Assim, o conjunto $\mathbb{Z}$ dos inteiros será o conjunto de tais classes de equivalência.

Inicialmente, vamos definir relação em $\mathbb{N} \times \mathbb{N}$ (que denotaremos por: $\sim$) e provar que é de equivalência.

Definição 2.4. *Para $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Dizemos que (a, b) está relacionado com (c, d) quando $a + d = b + c$. Que será indicada por $(a, b) \sim (c, d)$.*

Assim,

$$(a, b) \sim (c, d) \Longleftrightarrow a + d = b + c. \tag{2.1}$$

Teorema 2.1. *A relação $\sim$ em $\mathbb{N} \times \mathbb{N}$ definida por $(a, b) \sim (c, d)$ é de equivalência se $a + c = b + d$.*

Demonstração: como já definimos anteriormente, uma relação é denominada relação de equivalência, se for: *reflexiva, simétrica e transitiva.*

i) **Reflexiva:** temos $(m, n) \sim (m, n)$, pois $m + n = n + m$ pela propriedade comutativa da adição;

ii) **Simétrica:** temos que $(m, n) \sim (r, s) \Longleftrightarrow (r, s) \sim (m, n)$, pois $(m, n) \sim (r, s) \Longleftrightarrow m + s = n + r \Longleftrightarrow m + s = r + n \Longleftrightarrow s + m = r + n \Longleftrightarrow r + n = s + m \Longleftrightarrow (r, s) \sim (m, n)$ (a propriedade comutativa da adição foi utilizada em várias equivalências);

iii) **Transitiva:** temos que $(m, n) \sim (r, s)$ e $(r, s) \sim (u, v) \Longrightarrow (m, n) \sim (u, v)$, pois de $(m, n) \sim (r, s)$ e $(r, s) \sim (u, v)$ temos:

(1) $(m, n) \sim (r, s) \Longleftrightarrow m + s = n + r$;

(2) $(r, s) \sim (u, v) \Longleftrightarrow r + v = s + u$.

Somando v em (1) e fazendo uma associação, temos que:

$$m + s = n + r \Longleftrightarrow (m + s) + v = (n + r) + v \Longleftrightarrow (m + v) + s = n + (r + v) \tag{2.2}$$

usando (2) em (2.2) ficamos com: $(m + v) + s = n + (s + u) = (n + u) + s$, pela lei do corte vem:

$$m + v = n + u \Longleftrightarrow (m, n) \sim (u, v).$$

■

2.3 Conjunto Quociente $\mathbb{N} \times \mathbb{N} / \sim$

Notação 2.1. *Iremos denotar por* $\overline{(a, b)}$ *a classe de equivalência do par ordenado* (a, b) *pela relação* $\sim$*, assim,*

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid (x, y) \sim (a, b)\}. \tag{2.3}$$

Quando colocamos um traço sobre o par ordenado subentendemos que é uma classe de equivalência.

Exemplo 2.2. *Observemos os seguintes exemplos ilustrativos:*

i) $\overline{(3, 5)} = \{(1, 3), (3, 5), (5, 7), (7, 9), \ldots\}$;

ii) $\overline{(3, 2)} = \{(1, 0), (2, 1), (3, 2), (4, 3), \ldots\}$;

iii) $\overline{(7, 9)} = \{(1, 3), (3, 5), (5, 7), (7, 9), \ldots\}$.

Observe que $\overline{(3, 5)} = \overline{(7, 9)}$.

A partir de então, vamos formar nosso conjunto dos números inteiros.

Definição 2.5. *O conjunto quociente* $\mathbb{N} \times \mathbb{N} / \sim$ *composto pelas classes de equivalência* $\overline{(a, b)}$ *será denotado por* $\mathbb{Z}$ *e o chamaremos de* ***conjunto dos números inteiros****. Deste modo,* $\mathbb{Z} = (\mathbb{N} \times \mathbb{N} / \sim) = \{\overline{(a, b)} \mid (a, b) \in \mathbb{N} \times \mathbb{N}\}$.

Podemos desta maneira representar todos os elementos de $\mathbb{Z}$.

2.4 Operação de Adição em $\mathbb{Z}$

Nosso objetivo agora é definirmos a operação $(+)$ em $\mathbb{Z}$, chamada de adição.

Definição 2.6. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a soma $\overline{(a,b)}+\overline{(c,d)}$ como sendo o inteiro $\overline{(a+c,\, b+d)}$.*

Temos agora que demonstrar que qualquer que sejam os representantes escolhidos das classes de equivalência a adição estará bem definida.

Teorema 2.2. *Se tivermos $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então $\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}$. Logo, a adição de números inteiros está bem definida.*

Demonstração:

Sabemos que $\overline{(a,b)} = \overline{(a',b')}$, então $(a,b) \sim (a',b')$, isto é,

$$\overline{(a,b)} = \overline{(a',b')} \Longrightarrow a + b' = b + a'. \tag{2.4}$$

De modo análogo, $\overline{(c,d)} = \overline{(c',d')}$, então $(c,d) \sim (c',d')$, isto é,

$$\overline{(c,d)} = \overline{(c',d')} \Longrightarrow c + d' = d + c'. \tag{2.5}$$

Temos então: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,\, b+d)}$ e $\overline{(a',b')} + \overline{(c',d')} = \overline{(a'+c',\, b'+d')}$, então podemos mostrar que: $\overline{(a+c,\, b+d)} = \overline{(a'+c',\, b'+d')}$, ou seja, $(a+c)+(b'+d') = (b+d)+(a'+c')$. De fato, somando membro a membro das equação (2.4) e (2.5), temos:

$$(a+c)+(b'+d') = (a+b')+(c+d') = (b+a')+(d+c') = (b+d)+(a'+c') \tag{2.6}$$

Portanto, $\overline{(a+c,\, b+d)} = \overline{(a'+c',\, b'+d')}$.

■

Exemplo 2.3. *Adição: $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,\, b+d)}$.*

i) $\overline{(2,0)} + \overline{(3,0)} = \overline{(2+3,\, 0+0)} = \overline{(5,0)}$;

ii) $\overline{(3,1)} + \overline{(8,5)} = \overline{(3+8,\, 1+5)} = \overline{(11,6)}$.

Como podemos ver $\overline{(5,0)} = \overline{(11,6)}$.

Observação 2.1. *Mostramos com o teorema acima que a operação de adição não depende da escolha dos representantes das classes.*

Teorema 2.3. *A operação de adição em $\mathbb{Z}$ é associativa, comutativa, tem $\overline{(0,0)}$ como elemento neutro.*

Demonstração:

$i)$ Associativa: desejamos mostrar que dados $\overline{(a,b)}, \overline{(c,d)}$ e $\overline{(e,f)}$ em $\mathbb{Z}$, teremos $(\overline{(a,b)} + \overline{(c,d)}) + \overline{(e,f)} = \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)})$. De fato,

$$\begin{aligned}
(\overline{(a,b)} + \overline{(c,d)}) + \overline{(e,f)} &= (\overline{(a+c, b+d)}) + \overline{(e,f)} \\
&= \overline{((a+c)+e, (b+d)+f))} \\
&= \overline{(a+(c+e), b+(d+f))} \\
&= \overline{(a,b)} + \overline{(c+e, d+f)} \\
&= \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)})
\end{aligned}$$

$ii)$ Comutativa: queremos mostrar que para $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, devemos ter $\overline{(a,b)} + \overline{(c+d)} = \overline{(c,d)} + \overline{(a,b)}$. De fato,

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

$iii)$ Existência do elemento neutro da adição $\overline{(0,0)}$: sejam $\overline{(a,b)}$ e $\overline{(0,0)}$ em $\mathbb{Z}$, temos que

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(0+a, 0+b)} = \overline{(a,b)}$$

■

Teorema 2.4. *(Lei do cancelamento da Adição): Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$ com $\alpha + \beta = \gamma + \beta$ então $\alpha = \gamma$.*

Demonstração: Para $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(m,n)}$, temos que:

$$\begin{aligned}
\alpha + \beta = \gamma + \beta &\iff \overline{(a,b)} + \overline{(c,d)} = \overline{(m,n)} + \overline{(c,d)} \\
&\iff \overline{(a+c, b+d)} = \overline{(m+c, n+d)} \\
&\iff (a+c) + (n+d) = (b+d) + (m+c) \\
&\iff (a+n) + (c+d) = (b+m) + (d+c) \\
&\implies a+n = b+m \\
&\iff \overline{(a,b)} = \overline{(m,n)} \iff \alpha = \gamma
\end{aligned}$$

■

Teorema 2.5. *(Elemento Oposto): Para $\overline{(a,b)} \in \mathbb{Z}$, existe um único $\overline{(c,d)} \in \mathbb{Z}$ tal que $\overline{(a,b)} + \overline{(c,d)} = \overline{(0,0)}$. Tal elemento $\overline{(c,d)}$ será o elemento $\overline{(b,a)}$.*

Demonstração:

$i)$ **Existência:** Para $\overline{(a,b)} \in \mathbb{Z}$, sejam $\overline{(c,d)} = \overline{(b,a)} \in \mathbb{Z}$ e $\overline{(m,n)} \in \mathbb{Z}$ tais que:

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} = \overline{(m,n)} &\iff \overline{(a,b)} + \overline{(b,a)} = \overline{(m,n)} \\
&\iff \overline{(a+b, b+a)} = \overline{(m,n)} \\
&\iff a + b + n = b + a + m \\
&\iff n = m \iff m = n \\
&\iff m + 0 = 0 + n \\
&\iff \overline{(m,n)} = \overline{(0,0)}
\end{aligned}$$

Logo, $\overline{(m,n)} = \overline{(0,0)}$. Portanto, existe um elemento $\overline{(c,d)} = \overline{(b,a)} \in \mathbb{Z}$ tal que $\overline{(a,b)} + \overline{(c,d)} = \overline{(0,0)}$.

$ii)$ **Unicidade:** Suponha que existam $\overline{(c,d)}, \overline{(c',d')} \in \mathbb{Z}$ ambos opostos de $\overline{(a,b)}$. Por ambos serem opostos de $\overline{(a,b)}$, segue que:

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} = \overline{(0,0)} &\iff \overline{(a+c, b+d)} = \overline{(0,0)} \\
&\implies a + c = b + d \qquad (2.7)
\end{aligned}$$

e

$$\begin{aligned}
\overline{(a,b)} + \overline{(c',d')} = \overline{(0,0)} &\iff \overline{(a+c', b+d')} = \overline{(0,0)} \\
&\implies a + c' = b + d' \qquad (2.8)
\end{aligned}$$

Observe que se somarmos o primeiro membro de (2.7) com segundo membro (2.8) e o segundo membro de (2.7) com o primeiro membro de (2.8), teremos:

$$a + c + b + d' = b + d + a + c' \implies c + d' = d + c', \qquad (2.9)$$

portanto, necessariamente devemos ter $\overline{(c,d)} = \overline{(c',d')}$, provando assim a unicidade.

■

Observação 2.2. *O oposto de um elemento $\alpha \in \mathbb{Z}$, como vimos é único, e será denotado por $-\alpha$.*

2.5 Operação de Subtração em $\mathbb{Z}$

A **subtração** em $\mathbb{Z}$ será denotada por $(-)$ e é definida da seguinte maneira:

Definição 2.7. *Se α e $\beta \in \mathbb{Z}$ então $\alpha - \beta = \alpha + (-\beta)$. Assim, a subtração $\alpha - \beta$ é a soma de α com o oposto (ou inverso aditivo, ou simétrico) de β.*

Proposição 2.1. *Sendo α, β e $\gamma \in \mathbb{Z}$, valem:*

i) $-(-\alpha) = \alpha$;

ii) $-\alpha + \beta = \beta - \alpha$;

iii) $\alpha - (-\beta) = \alpha + \beta$;

iv) $-\alpha - \beta = -(\alpha + \beta)$;

v) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$.

Demonstração: Faremos aqui a prova de (ii), as demais são deixadas para o leitor como exercício. Seja $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$; como vimos acima $-\alpha = \overline{(b,a)}$; assim

$$\begin{aligned} -\alpha + \beta &= \overline{(b,a)} + \overline{(c,d)} \\ &= \overline{(b+c, a+d)} \\ &= \overline{(c+b, d-a)} \\ &= \overline{(c,d)} + \overline{(b,a)} \\ &= \beta + (-\alpha) = \beta - \alpha \end{aligned}$$

■

2.6 Operação de multiplicação em $\mathbb{Z}$

A seguir, iremos definir outra operação em $\mathbb{Z}$, a qual indicaremos por " $\cdot$ " e será chamada de **produto**.

Definição 2.8. *Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos o produto $\overline{(a,b)} \cdot \overline{(c,d)}$ como sendo o inteiro $\overline{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}$.*

Notação 2.2. *Por simplicidade, adotaremos $a \cdot b = ab$.*

Teorema 2.6. *A multiplicação em* $\mathbb{Z}$ *está bem definida. se* $\overline{(a,b)} = \overline{(a',b')}$ *e* $\overline{(c,d)} = \overline{(c',d')}$*, então,* $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

Demonstração: Temos que,

$i)$ $\overline{(a,b)} = \overline{(a',b')} \Longrightarrow (a,b) \sim (a',b') \Longrightarrow a + b' = b + a'$;

$ii)$ $\overline{(c,d)} = \overline{(c',d')} \Longrightarrow (c,d) \sim (c',d') \Longrightarrow c + d' = d + c'$.

Multiplicando (i) por c e (ii) por d, teremos as respectivas equações:

$$ac + b'c = bc + a'c \tag{2.10}$$

e

$$ad + b'd = bd + a'd \tag{2.11}$$

que somando seus membros em cruz, ficamos com:

$$\begin{aligned} ac + bd + a'd + b'c &= ad + bc + a'c + b'd \\ \overline{(ac + bd, ad + bc)} &= \overline{(a'c + b'd, a'd + b'c)} \\ \overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(a',b')} \cdot \overline{(c,d)} \end{aligned} \tag{2.12}$$

De maneira análoga, multiplicando (ii) por a' e b' respectivamente, após as operações, obteremos:

$$\overline{(a',b')} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}. \tag{2.13}$$

Comparando (2.12) e (2.13), concluímos que

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$$

■

Teorema 2.7. *A multiplicação em* $\mathbb{Z}$ *é associativa, comutativa, tem elemento neutro* $\overline{(1,0)}$*, vale a distributiva em relação a adição e também, a lei do cancelamento multiplicativo.*

Demonstração:

$i)$ **Associativa:** Para $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(m,n)} \in \mathbb{Z}$, queremos mostrar que $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. De fato,

$$\begin{aligned}
\alpha(\beta\gamma) &= \overline{(a,b)}\cdot(\overline{(c,d)}\cdot\overline{(m,n)})\\
&= \overline{(a,b)}\cdot\overline{(cm+dn,cn+dm)}\\
&= \overline{(a(cm+dn)+b(cn+dm),a(cn+dm)+b(cm+dn))}\\
&= \overline{(acm+adn+bcn+bdm,acn+adm+bcm+bdn)}\\
&= \overline{(acm+bdm+adn+bcn,acn+bdn+adm+bcm)}\\
&= \overline{((ac+bd)m+(ad+bc)n,(ac+bd)n+(ad+bc)m)}\\
&= \overline{(ac+bd,ad+bc)}\cdot\overline{(m,n)}\\
&= (\overline{(a,b)}\cdot\overline{(c,d)})\cdot\overline{(e,f)}\\
&= (\alpha\beta)\gamma
\end{aligned}$$

ii) **Comutativa:** Para $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)} \in \mathbb{Z}$, queremos mostrar que $\alpha\beta = \beta\alpha$. De fato,

$$\alpha\beta = \overline{(a,b)}\cdot\overline{(c,d)} = \overline{(ac+bd,ad+bc)} = \overline{(ca+db,cb+da)} = \overline{(c,d)}\cdot\overline{(a,b)} = \beta\alpha$$

iii) **Tem elemento neutro $\overline{(1,0)}$:** Para $\alpha = \overline{(a,b)}$ e $\beta = \overline{(1,0)} \in \mathbb{Z}$, temos que:

$$\alpha\cdot\beta = \overline{(a,b)}\cdot\overline{(1,0)} = \overline{(a+0,0+b)} = \overline{(a,b)} = \alpha \tag{2.14}$$

iv) **Distributiva em relação a adição:** Para $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(m,n)} \in \mathbb{Z}$, queremos mostrar que $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$. De fato,

$$\begin{aligned}
\alpha(\beta+\gamma) &= \overline{(a,b)}\cdot(\overline{(c,d)}+\overline{(m,n)})\\
&= \overline{(a,b)}\cdot(\overline{(c+m,d+n)})\\
&= \overline{(a(c+m)+b(d+n),a(d+n)+b(c+m))}\\
&= \overline{(ac+am+bd+bn,ad+an+bc+bm)}\\
&= \overline{(a,b)}\cdot\overline{(c,d)}+\overline{(a,b)}\cdot\overline{(m,n)}\\
&= \alpha\beta+\alpha\gamma
\end{aligned}$$

v) **Vale a lei do cancelamento multiplicativo:** Para $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(m,n)} \in \mathbb{Z}$, com $\gamma = \overline{(m,n)} \neq \overline{(0,0)}$, temos que:

$$\begin{aligned}
\alpha\gamma &= \beta\gamma & (2.15)\\
\overline{(a,b)} \cdot \overline{(m,n)} &= \overline{(c,d)} \cdot \overline{(m,n)}\\
\overline{(am+bn, an+bm)} &= \overline{(cm+dn, cn+dm)}\\
am+bn+cn+dm &= an+bm+cm+dn\\
m(a+d)+n(b+c) &= m(b+c)+n(a+d) & (2.16)
\end{aligned}$$

como $\overline{(m,n)} \neq \overline{(0,0)}$, isto implica que $m \neq n$. Sem perda de generalidade, suponha $m > n$ (análogo se $n > m$). Se $m > n$, então existe um $k \in \mathbb{N}\backslash\{0\}$, tal que $m = n + k$.

Substituindo $m = n + k$ em (2.16), ficamos com:

$$\begin{aligned}
(n+k)(a+d)+n(b+c) &= (n+k)(b+c)+n(a+d)\\
na+nd+ka+kd+nb+nc &= nb+nc+kb+kc+na+nd\\
ka+kd &= kb+kc\\
k(a+d) &= k(b+c)\\
a+d &= b+c\\
\overline{(a,b)} &= \overline{(c,d)}\\
\alpha &= \beta & (2.17)
\end{aligned}$$

Comparando (2.15) e (2.17), concluímos que $\alpha\gamma = \beta\gamma \Longrightarrow \alpha = \beta$, desde que $\gamma \neq 0$.

■

2.7 Relação de Ordem em $\mathbb{Z}$

Definição 2.9. *Dados os inteiros $\overline{(a,b)}$ e $\overline{(c,d)}$, escrevemos $\overline{(a,b)} \leqslant \overline{(c,d)}$, lê-se $\overline{(a,b)}$ é menor ou igual a $\overline{(c,d)}$ quando $a + d \leqslant b + c$.*

Proposição 2.2. *A relação ($\leqslant$) é uma relação de ordem em $\mathbb{Z}$, onde ela goza das propriedades reflexiva, antissimétrica e transitiva. Essa relação é compatível com as operações definidas em $\mathbb{Z}$.*

Demonstração:

i) Reflexiva: $m = \overline{(a,b)} \in \mathbb{Z}$, então $m \leqslant m$ pois $a + b = b + a$.

ii) Antissimétrica: Seja $m = \overline{(a,b)}, n = \overline{(c,d)}$ e suponha $m \leqslant n$ e $n \leqslant m$. Então $a + d \leqslant b + c$ e $c + b \leqslant a + d$, logo, como essa desigualdade é em $\mathbb{N}$, segue que $a + d = b + c$, o que é equivalente a dizer que $m = n$.

iii) Transitiva: Demonstração, ver FERREIRA (2010) (p. 53).

iv) Sejam $m = \overline{(a,b)}, n = \overline{(c,d)}, p = \overline{(e,f)}$, elementos de $\mathbb{Z}$. Vamos mostrar que $m \leqslant n \Longrightarrow m + p \leqslant n + p$.

Começamos observando que $m \leqslant n \Longrightarrow a + d \leqslant b + c$ Daí vem que

$$(a + d) + (e + f) \leqslant (b + c) + (e + f) \Longrightarrow (a + e) + (d + f) \leqslant (c + e) + (b + f)$$

ou seja,

$$\overline{(a + e, b + f)} \leqslant \overline{(c + e, d + f)} \Longrightarrow m + p \leq n + p.$$

v) Da mesma forma pode-se mostrar que se $m \leqslant n$ e $p \geqslant 0$, então $mp \leqslant np$.

■

Definição 2.10. *Dados $\overline{(a,b)} \in \mathbb{Z}$, temos:*

i) $\overline{(a,b)}$ *é positivo quando* $\overline{(a,b)} > \overline{(0,0)}$*;*

ii) $\overline{(a,b)}$ *é não negativo quando* $\overline{(a,b)} \geqslant \overline{(0,0)}$*;*

iii) $\overline{(a,b)}$ *é negativo quando* $\overline{(a,b)} < \overline{(0,0)}$*;*

iv) $\overline{(a,b)}$ *é não positivo quando* $\overline{(a,b)} \leqslant \overline{(0,0)}$*.*

Teorema 2.8. *(Lei da tricotomia dos Inteiros) Dados $\alpha, \beta \in \mathbb{Z}$, um e apenas um dos seguintes casos pode ocorrer: $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$.*

Demonstração: FERREIRA (2010) (p. 54).

Observação 2.3. *Se $\overline{(a,b)} \geqslant \overline{(0,0)} \Longleftrightarrow a + 0 \geqslant b + 0 \Longrightarrow a \geqslant b$. Por outro lado, se $\overline{(a,b)} \leqslant \overline{(0,0)} \Longrightarrow a + 0 \leqslant b + 0 \Longrightarrow a \leqslant b$.*

Esta observação está de acordo com a ideia de que a classe de equivalência $\overline{(a,b)}$ representa a “diferença $a - b$”, mais adiante essa ideia terá maior solidez.

Observação 2.4. *Se* $\overline{(a,b)}$ *é positivo com* $a > b$*, então existe* $m \in \mathbb{N}\backslash\{0\}$ *tal que* $a = b+m$*. Esta igualdade equivale a:* $\overline{(a,b)} = \overline{(m,0)}$*. Analogamente* $\overline{(a,b)} < \overline{(0,0)}$*, então nesse caso existe* $m \in \mathbb{N}$*, tal que* $\overline{(a,b)} = \overline{(0,m)}$*.*

Estas observações e a lei da tricotomia em $\mathbb{Z}$ nos dizem que:

$$\mathbb{Z} = \{\overline{(0,m)} \mid m \in \mathbb{N}\backslash\{0\}\} \cup \{\overline{(0,0)}\} \cup \{\overline{(m,0)} \mid m \in \mathbb{N}\} \tag{2.18}$$

sendo essa união acima disjunta. Temos ainda:

$i)$ **Inteiros negativos:**

$$\mathbb{Z}_{-}\backslash\{0\} = \{\overline{(0,m)} \mid m \in \mathbb{N}\backslash\{0\}\}, \;\; \mathbb{Z}_{-} = \{\overline{(0,m)} \mid m \in \mathbb{N}\backslash\{0\}\} \cup \{\overline{(0,0)}\} \tag{2.19}$$

$ii)$ **Inteiros não negativos:**

$$\mathbb{Z}_{+}\backslash\{0\} = \{\overline{(m,0)} \mid m \in \mathbb{N}\backslash\{0\}\}, \;\; \mathbb{Z}_{+} = \{\overline{(m,0)} \mid m \in \mathbb{N}\backslash\{0\}\} \cup \{\overline{(0,0)}\} \tag{2.20}$$

Podemos notar que o conjunto dos números inteiros não negativos, $\mathbb{Z}_{+}$, está em bijeção com $\mathbb{N}$. Esta bijeção mostra que $\mathbb{Z}_{+}$ é uma cópia algébrica de $\mathbb{N}$.

Teorema 2.9. *Seja* $f : \mathbb{N} \longrightarrow \mathbb{Z}$ *dada por:* $f(m) = \overline{(m,0)}$ *então* f *é injetora e valem as seguintes propriedades:*

i) $f(m+n) = f(m) + f(n)$*;*

ii) $f(mn) = f(m) \cdot f(n)$*;*

iii) Se $m \leqslant n$*, então* $f(m) \leqslant f(n)$*.*

Demonstração:

Vamos verificar primeiro que f é injetora, vejamos $f(m) = f(n) \Leftrightarrow \overline{(m,0)} = \overline{(n,0)} \Leftrightarrow m + 0 = n + 0 \Leftrightarrow m = n$.

(i) Tome $m, n \in \mathbb{N}$, então $f(m+n) = \overline{(m+n,0)} = \overline{(m,0)} + \overline{(n,0)} = f(m) + f(n)$.

(ii) Tome $m, n \in \mathbb{N}$, então $f(mn) = \overline{(mn,0)} = \overline{(m,0)} \cdot \overline{(n,0)} = f(m) \cdot f(n)$.

(iii) Se $m \leq n$, então por definição temos $n = m + r$, para algum $r \in N$. Portanto temos $f(n) = \overline{(n,0)} = \overline{(m+r,0)} = \overline{(m,0)} + \overline{(r,0)} = f(m) + \overline{(r,0)}$. Então temos que $f(m) \leq f(n)$.

■

Observe que o conjunto $f(\mathbb{N}) = \mathbb{Z}_+$ possui a mesma estrutura algébrica de $\mathbb{N}$.

Exemplo 2.4. *Temos que* $2 + 5 = 7$ *em* $\mathbb{N}$*, que pela* f *corresponde a:* $\overline{(2,0)} + \overline{(5,0)} = \overline{(7,0)}$ *em* $\mathbb{Z}$*. Do mesmo modo,* $2 \cdot 5 = 10$ *que corresponde pela* f *a:* $\overline{(2,0)} \cdot \overline{(5,0)} = \overline{(2 \cdot 5 + 0 \cdot 0, 2 \cdot 0 + 0 \cdot 5)} = \overline{(10,0)}$.

Ainda a relação $2 \leqslant 5$ se preserva via f. Como $\overline{(2,0)} \leqslant \overline{(5,0)} \Longleftrightarrow 2 + 0 \leqslant 5 + 0$, portanto $2 \leqslant 5$, o que confirma que a ordenação em $\mathbb{Z}$ é uma extensão da ordenação em $\mathbb{N}$.

Assim, no que se refere aos aspectos algébricos e à ordenação, $\mathbb{Z}_+$ é uma cópia de $\mathbb{N}$, obtida através de f. Assim, podemos identificar $\mathbb{N}$ com $\mathbb{Z}_+$ e considerar $\mathbb{N} \subset \mathbb{Z}$. Mais especificamente, com essa identificação o número natural 0 passa a se confundir com o número inteiro $\overline{(0,0)}$, o número natural 1 com o número inteiro $\overline{(1,0)}$, e assim por diante. Feita esta identificação, passaremos então a denotar o inteiro $\overline{(0,0)}$ simplesmente por 0, o inteiro $\overline{(1,0)}$ simplesmente por 1, o inteiro negativo $\overline{(0,1)}$ simplesmente por -1 e, assim por diante. Feitas as observações e identificações acima, se $x = \overline{(a,b)} \in \mathbb{Z}$, então $x = \overline{(a,b)} = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,0)} + [-\overline{(b,0)}]$. Assim, em consequência da identificação feita, segue que $x = a - b$. Logo, todo inteiro é igual à diferença (em $\mathbb{Z}$) de dois números naturais.

Por outro lado, se $a, b \in \mathbb{N}$, novamente levando em conta a identificação de $\mathbb{N}$ com $\mathbb{Z}_+$, temos:

$$a - b = \overline{(a,0)} - \overline{(b,0)} = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,b)}$$

o que mostra que a subtração de dois números naturais é sempre possível em $\mathbb{Z}$. Isto, no fundo, era o que se tinha em vista com a construção do conjunto dos números inteiros.

Referências Bibliográficas

[1] BOYER, C. B. & MERZBACH, U. C.; [tradução de Helena Castro], São Paulo - Brasil (2012), **História da Matemática.** *Tradução da* $3^{\underline{a}}$ *edição americana -* $4^{\underline{a}}$ *reimpressão (2018), Editora Edgar Blücher Ltda.*

[2] FERREIRA, J; (2015), **Construção dos Números.** *Editora SBM* - $1^{\underline{a}}$ *edição.*

[3] GUERREIRO, S. (1989), **Curso de Análise.** *Escolar Editora.*

[4] HYGINO H. DOMINGUES & GELSON IEZZI; (1982), **Algébra Moderna.** *Atual Editora* - $5^{\underline{a}}$ *edição.*

[5] LIMA, E.L.; (2012), **Curso de Análise - Volume 1.** *Editora IMPA* - $14^{\underline{a}}$ *edição.*

[6] PITOMBEIRA, J. B. & ROQUE, T. M.; Rio de Janeiro, Brasil (2012), **Tópicos de História de Matemática.** *SBM.*