APÊNDICE II

CONSTRUÇÃO LÓGICO-FORMAL DO CONJUNTO DOS NÚMEROS INTEIROS

1. Os números inteiros: construção

Nosso objetivo aqui é dar um sentido matemático a todas as expressões do tipo $a - b$, para quaisquer $a, b \in \mathbb{N}$, de maneira a poder tratar como entes do mesmo conjunto tanto aquelas como $7 - 3$, $5 - 1$ e $4 - 0$ quanto aquelas como $3 - 7$, $1 - 3$ e $0 - 2$, por exemplo. Nesse sentido convém observar primeiro que subjacente a cada "diferença" $a - b$ está o par ordenado $(a, b) \in \mathbb{N} \times \mathbb{N}$. Além disso é fácil ver que, por exemplo, a igualdade em $\mathbb{N}$

$$5 - 3 = 9 - 7$$

equivale a $5 + 7 = 9 + 3$. De uma maneira geral, se $a, b, c, d \in \mathbb{N}$, $a \geqslant b$ e $c \geqslant d$, vale a equivalência:

$$a - b = c - d \iff a + d = c + d$$

Essas considerações, aliadas ao fato de que o conjunto dos inteiros a ser construído, deve ser uma "ampliação" de $\mathbb{N}$, ajudam a entender o caminho que tomaremos.

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

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Para a relação $\sim$ valem as propriedades:

- *Reflexiva* pois, como para todo $(a, b) \in \mathbb{N} \times \mathbb{N}$, se verifica $a + b = b + a$, então $(a, b) \sim (a, b)$.
- *Simétrica*, ou seja, se $(a, b) \sim (c, d)$, então $(c, d) \sim (a, b)$ (exercício)
- *Transitiva* pois, se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $a + d = b + c$ e $c + f = e + d$; daí $a + d + f = b + c + f$ e $c + f + b = e + d + b$, o que

implica $a + d + f = e + d + b$ e portanto $a + f = e + b$, ou seja: $(a, b) \sim (e, f)$.

Logo $\sim$ é uma relação de equivalência em $\mathbb{N} \times \mathbb{N}$ e, por conseguinte, 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:

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

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

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a, b)} \mid (a, b) \in \mathbb{N} \times \mathbb{N}\}$$

Por exemplo:

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

É claro que: $\overline{(a, b)} = \overline{(c, d)} \iff (a, b) \sim (c, d) \iff a + d = b + c$. Em particular vale o seguinte: se $a \geqslant b$, então $\overline{(a, b)} = \overline{(a - b, 0)}$, pois $a + 0 = (a - b) + b$; e se $b \geqslant a$, 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 $c = d$.

1.1 Adição em $\mathbb{Z}$

Consideremos os números naturais 4 e 3 escritos sob a forma: $4 = 5 - 1$ e $3 = 7 - 4$. Então: $4 + 3 = (5 - 1) + (7 - 4) = (5 + 7) - (1 + 4)$. Essa observação ajuda a entender a definição a seguir:

DEFINIÇÃO 1 Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ elementos quaisquer de $\mathbb{Z}$. Chama-se *soma de* m *com* n, e se indica por $m + n$, o elemento de $\mathbb{Z}$ definido por:

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

Suponhamos $m = \overline{(a, b)} = \overline{(a_1, b_1)}$ e $n = \overline{(c, d)} = \overline{(c_1, d_1)}$; então $m + n = \overline{(a + c, b + d)}$ e $m + n = \overline{(a_1 + c_1, b_1 + d_1)}$. Como porém $(a, b) \sim (a_1, b_1)$ e $(c, d) \sim (c_1, d_1)$, então $a + b_1 = b + a_1$ e $c + d_1 = d + c_1$, do que resulta (somando membro a membro essas igualdades): $(a+b_1) + (c + d_1) = (b + a_1) + (d + c_1)$ ou $(a + c) + (b_1 + d_1) = (b + d) + (a_1 + c_1)$.

Donde $\overline{(a + c, b + d)} = \overline{(a_1 + c_1, b_1 + d_1)}$. Logo a relação dada por

$$(m, n) \to m + n$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e portanto é uma operação sobre $\mathbb{Z}$. A essa operação chama-se *adição* em $\mathbb{Z}$.

Para a adição em $\mathbb{Z}$ valem as seguintes propriedades:

a_1 *Associativa*

De fato, se $m = \overline{(a, b)}$, $n = \overline{(c, d)}$ e $r = \overline{(e, f)}$ são elementos genéricos de $\mathbb{Z}$, então:

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

a_2 *Comutativa*: $m + n = n + m$, $\forall m, n \in \mathbb{Z}$. Exercício.

a_3 Existe *elemento neutro*: é a classe $\overline{(0, 0)}$. De fato, para qualquer $\overline{(a, b)} \in \mathbb{Z}$:

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

É óbvio que $\overline{(a, a)} = \overline{(0, 0)}$, para todo $a \in \mathbb{N}$. Usaremos a notação: $0 = \overline{(0, 0)}$, a qual será justificada no item 2.

a_4 Todo $m = \overline{(a, b)} \in \mathbb{Z}$ admite *oposto* (simétrico aditivo). Ou seja, para todo $m \in \mathbb{Z}$ existe $m' \in \mathbb{Z}$ de modo que $m + m' = 0$. Usaremos a notação: $-m = m'$.

Como

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, b + a)} = 0$$
$$\text{então: } m = \overline{(a, b)} \Rightarrow -m = \overline{(b, a)}.$$

Destaquemos ainda a *lei do cancelamento* em $\mathbb{Z}$:

$$m + r = n + r \Rightarrow m = n$$

De fato: $m = m + 0 = m + [r + (-r)] = (m + r) + (-r) =$
$= (n + r) + (-r) = n + [r + (-r)] = n + 0 = n.$

1.2 Subtração em $\mathbb{Z}$

Para cada par de elementos $m, n \in \mathbb{Z}$, chama-se diferença entre m e n e indica-se por $m - n$ o elemento $m + (-n) \in \mathbb{Z}$. Ou seja:

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

Assim, posto que $m - n \in \mathbb{Z}$, quaisquer que sejam $m, n \in \mathbb{Z}$, a relação dada por

$$(m, n) \to m - n$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ — ou seja, é uma operação sobre $\mathbb{Z}$. A essa operação denominamos *subtração* em $\mathbb{Z}$. Esta operação, contudo, não é associativa, nem comutativa e tampouco admite elemento neutro. Sugerimos ao leitor verificar esses fatos.

1.3 Multiplicação em $\mathbb{Z}$

Uma maneira pouco prática de multiplicar os números naturais $3 = 5 - 2$ e $4 = 10 - 6$ seria a seguinte:

$$3 \cdot 4 = (5 - 2) \cdot (10 - 6) = (5 \cdot 10 + 2 \cdot 6) - (5 \cdot 6 + 2 \cdot 10) = 62 - 50 = 12$$

Contudo, a partir daí fica mais fácil entender a

DEFINIÇÃO 2 Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ elementos genéricos de Z. Chama-se *produto* de m por n e indica-se por mn (ou $m \cdot n$) o elemento de $\mathbb{Z}$ definido por:

$$mn = \overline{(ac + bd, ad + bc)}$$

Se $m = \overline{(a, b)} = \overline{(a_1, b_1)}$ e $n = \overline{(c, d)} = \overline{(c_1, d_1)}$, então $mn = \overline{(ac + bd, ad + bc)}$ e $mn = \overline{(a_1c_1 + b_1d_1, a_1d_1 + b_1c_1)}$. Mas como $(a, b) \sim (a_1, b_1)$ e $(c, d) \sim (c_1, d_1)$, então $a + b_1 = b + a_1$ e $c + d_1 = d + c_1$. Daí obtemos: $c(a + b_1) = c(b + a_1)$, $a_1(c + d_1) = a_1(d + c_1)$, $d(b + a_1) = d(a + b_1)$ e $b_1(d + c_1) = b_1(c + d_1)$. Desenvolvendo esses produtos e depois somando membro a membro as igualdades obtidas, feitos a seguir os cancelamentos possíveis, restará

$$(ac + bd) + (a_1d_1 + b_1c_1) = (bc + ad) + (a_1c_1 + b_1d_1)$$

o que pode ser traduzido por:

$$\overline{(ac + bd, ad + bc)} = \overline{(a_1c_1 + b_1d_1, a_1d_1 + b_1c_1)}$$

Isso significa que a relação

$$(m, n) \to mn$$

é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e, por isso, uma operação sobre $\mathbb{Z}$. Trata-se, obviamente, da *multiplicação* em Z, da qual destacamos as propriedades a seguir.

m_1 *Associativa*: $m(nr) = (mn)r$, para quaisquer $m, n, r \in \mathbb{Z}$. Exercício.

m_2 *Comutativa*

De fato, se $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ são elementos quaisquer de $\mathbb{Z}$, então

$$mn = \overline{(ac + bd, ad + bc)} = \overline{(ca + db, cb + da)} = nm$$

m_3 Existe *elemento neutro*: é a classe (1, 0), à qual indicaremos apenas por 1 (a justificativa para essa simplificação será vista no item 2), pois:

$$\forall \overline{(a, b)} \in \mathbb{Z} \Rightarrow \overline{(1, 0)} \cdot \overline{(a, b)} = \overline{(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)} = \overline{(a, b)}$$

m_4 *Lei do anulamento do produto*: Se m, n $\in \mathbb{Z}$ e mn = 0, então m = 0 ou n = 0.

Como já observamos anteriormente, todo elemento de $\mathbb{Z}$ pode ser representado univocamente sob uma das seguintes formas: $\overline{(a, 0)}$ ou $\overline{(0, a)}$, para algum a $\in$ IN. Vamos supor, por exemplo, m = $\overline{(a, 0)}$ e n = $\overline{(0, b)}$. Então, por hipótese, mn = $\overline{(0, ab)} = \overline{(0, 0)}$. Daí 0 + 0 = ab + 0 ou ab = 0 (em IN), o que implica a = 0 ou b = 0. Donde m = 0 ou n = 0. Os demais casos não apresentam nenhuma novidade.

d *Distributiva*: Para quaisquer m, n, r $\in \mathbb{Z}$, m + (n + r) = (m + n) + r. Exercício.

O conjunto $\mathbb{Z}$, munido das operações introduzidas através das definições 1 e 2, mais a relação de ordem a ser introduzida no item seguinte, é chamado *conjunto dos números inteiros*. E os elementos de $\mathbb{Z}$, nessas condições, são chamados *números inteiros*.

1.4 Relação de ordem em $\mathbb{Z}$

Se m $\in \mathbb{Z}$, então m = $\overline{(a, 0)}$ ou m = $\overline{(0, a)}$, para algum a $\in$ IN. Assim, se fizermos

$$\begin{array}{ll} \overline{(0, 0)} = 0 & \overline{(0, 1)} = -1 \\ \overline{(1, 0)} = +1 & \overline{(0, 2)} = -2 \\ \overline{(2, 0)} = +2 & \overline{(0, 3)} = -3 \\ \vdots & \vdots \end{array}$$

torna-se válido escrever

$$\mathbb{Z} = \{\ldots, -2, -1, 0, +1, +2, \ldots\}$$

Façamos {0, +1, +2, ...} = $\mathbb{Z}_+$ e {..., −2, −1, 0} = $\mathbb{Z}_-$. Os elementos de $\mathbb{Z}_+$ se dizem *inteiros positivos* e os de $\mathbb{Z}_-$ *inteiros negativos*. Todo elemento m $\in \mathbb{Z}_+^* = \{+1, +2, +3, \ldots\}$ é chamado inteiro *estritamente positivo*; e todo m $\in \mathbb{Z}_-^* = \{\ldots, -3, -2, -1\}$ é um inteiro *estritamente negativo*.

Notemos que se m $\in \mathbb{Z}_+$ (ou $\mathbb{Z}_+^*$), então −m $\in \mathbb{Z}_-$ (ou $\mathbb{Z}_-^*$) e vice-versa. De fato, se por exemplo m = $\overline{(a, 0)}$ (logo m $\in \mathbb{Z}_+$), então −m = (0, a) (que está em $\mathbb{Z}_-$).

DEFINIÇÃO 3 Sejam m, n $\in \mathbb{Z}$. Diz-se que m *é menor que ou igual a* n e anota-se m $\leqslant$ n se

$$n = m + r$$

para algum r $\in \mathbb{Z}_+$. Neste caso também se pode escrever n $\geqslant$ m, o que se lê: "n *é maior que ou igual a* m".

Se n = m + r, onde r $\in \mathbb{Z}_+^*$, então m se diz *menor que* n. Notação: m < n. É equivalente dizer que n *é maior que* m e anotar n > m.

Em particular $0 \leqslant r$, $\forall r \in \mathbb{Z}_+$, pois r = 0 + r; e $s \leqslant 0$, $\forall s \in \mathbb{Z}_-$, já que 0 = s + (− s). Também: 0 < r, para todo r $\in \mathbb{Z}_+^*$ e r < 0 para todo r $\in \mathbb{Z}_-^*$.

Vejamos agora as propriedades mais importantes da relação $\leqslant$ sobre $\mathbb{Z}$.

o_1 *Reflexiva*: m $\leqslant$ m, $\forall$m $\in \mathbb{Z}$, pois m = m + 0 e 0 $\in \mathbb{Z}_+$.

o_2 *Anti-simétrica*: Vamos supor m $\leqslant$ n e n $\leqslant$ m. Então m = n + r_1, onde $r_1 = \overline{(a, 0)}$, para algum a $\in$ IN, e n = m + r_2, onde $r_2 = \overline{(b, 0)}$, sendo b um conveniente elemento de IN. Então:

$$m = n + r_1 = (m + r_2) + r_1 = m + (r_1 + r_2) = m + \overline{(a + b, 0)}$$

o que implica, pela lei do cancelamento da adição:

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

Daí a + b = 0 (em IN) e portanto a = b = 0. Donde $r_1 = r_2 = 0$ e m = n.

o_3 *Transitiva*: m $\leqslant$ n e n $\leqslant$ q $\Rightarrow$ m $\leqslant$ q. (Fica como exercício.)

o_4 m $\leqslant$ n ou n $\leqslant$ m

Vamos supor m = $\overline{(a, 0)}$ e n = $\overline{(b, 0)}$. Se a $\leqslant$ b, então b = a + c, para algum c $\in$ IN e portanto

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

o que garante a relação m $\leqslant$ n. Se, ao contrário, ocorresse b $\leqslant$ a, então valeria n $\leqslant$ m.

O caso m = $\overline{(0, a)}$ e n = $\overline{(0, b)}$ pode ser encaminhado do mesmo modo. Finalmente, seja m = $\overline{(a, 0)}$ e n = $\overline{(0, b)}$. Então

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

de onde segue n $\leqslant$ m.

Uma conseqüência das considerações anteriores é que: m $\in \mathbb{Z}_-$ e n $\in \mathbb{Z}_+$ $\Rightarrow$ m $\leqslant$ n.

o_5 *Compatibilidade com a adição*: Se m $\leqslant$ n, então m + p $\leqslant$ n + p, para todo p $\in \mathbb{Z}$.

De fato, da hipótese segue que $m + r = n$, para algum $r \in \mathbb{Z}_+$. Assim, para todo $p \in \mathbb{Z}$: $n + p = (m + r) + p = (m + p) + r$. Donde: $m + p \leqslant n + p$.

o_6 *Compatibilidade com a multiplicação*: $m \leqslant n$ e $0 \leqslant p \Rightarrow mp \leqslant np$.

Por hipótese $n = m + r$, onde $r = \overline{(a, 0)}$, para algum $a \in \mathbb{N}$. Supondo $p = \overline{(b, 0)}$, como $pn = pm + pr$, onde $pr = \overline{(ab, 0)} \in \mathbb{Z}_+$, então $pm \leqslant pn$.

2. Imersão de $\mathbb{N}$ em $\mathbb{Z}$

Mostraremos agora, dentro da construção que fizemos, em que termos se pode considerar $\mathbb{N}$ como parte de $\mathbb{Z}$.

Seja $f: \mathbb{N} \to \mathbb{Z}$ definida por $f(a) = \overline{(a, 0)}$, para todo $a \in \mathbb{Z}$. Ou seja:

$$\begin{aligned} f(0) &= \overline{(0, 0)} = 0 \\ f(1) &= \overline{(1, 0)} = +1 \\ f(2) &= \overline{(2, 0)} = +2 \\ &\vdots \end{aligned}$$

Então:

- $\operatorname{Im}(f) = \{f(a) \mid a \in \mathbb{N}\} = \mathbb{Z}_+ = \{0, +1, +2, +3, \ldots\}$.
- $f(a) = f(b) \Rightarrow \overline{(a, 0)} = \overline{(b, 0)} \Rightarrow a = b$, o que mostra que f é injetora.
- $f(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)} + \overline{(b, 0)} = f(a) + f(b)$, $\forall a, b \in \mathbb{N}$
- $f(ab) = \overline{(ab, 0)} = \overline{(a, 0)} \cdot \overline{(b, 0)} = f(a)\,f(b)$, $\forall a, b \in \mathbb{N}$
- Se $a \leqslant b$, então $b = a + c$, para algum $c \in \mathbb{N}$ e portanto

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

o que significa que

$$f(a) \leqslant f(b)$$

Assim, no que se refere aos aspectos algébricos e à ordenação, $\mathbb{Z}_+$ é uma cópia de $\mathbb{N}$, obtida através de f. Daí porque se pode identificar $\mathbb{N}$ com $\mathbb{Z}_+$ e considerar $\mathbb{N} \subset \mathbb{Z}$. Mais especificamente, nessa identificação o número natural 0 passa a se confundir com o inteiro $0 = \overline{(0, 0)}$, o natural 1 com o inteiro $+1 = \overline{(1, 0)}$, e assim por diante. A função f considerada costuma ser chamada de *imersão* de $\mathbb{N}$ em $\mathbb{Z}$, por razões óbvias em face das propriedades que destacamos a seu respeito.

Isso posto, se $x = \overline{(a, b)} \in \mathbb{Z}$, então $x = \overline{(a, b)} = \overline{(a, 0)} + \overline{(0, b)} = \overline{(a, 0)} + [-\overline{(b, 0)}]$ e, em conseqüência da identificação feita, $x = a - b$. Logo, todo inteiro é igual à diferença (em $\mathbb{Z}$) entre dois números naturais.

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

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

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

2.1 O princípio do menor inteiro

A identificação que fizemos de $\mathbb{N}$ com $\mathbb{Z}_+$ torna válida a demonstração que fizemos em 3.3 do princípio do menor inteiro:

o_7 Seja $S \subset \mathbb{Z}$, $S \neq \varnothing$. Se S admite uma cota inferior (e portanto infinitas), então S possui mínimo.

EXERCÍCIOS

352. Se $a, b, c, d \in \mathbb{Z}$, prove que:

a) $(a - b)(c - d) = (ac + bd) - (ad + bc)$

b) $(a + b)(c - d) = (ac + bc) - (ad + bd)$

353. Sejam x e y inteiros tais que $xy = 1$. Prove que $x = y = 1$ ou $x = y = -1$.

354. Prove que: $a < b + c \iff a - b < c$.

355. Se $p > 0$, prove que $a - p < a$, para todo $a \in \mathbb{Z}$.

356. Prove que: $x^2 = x \Rightarrow x = 0$ ou $x = 1$.

357. Para todo $a \in \mathbb{Z}$, mostre que

$$a - 1 = \text{máx}\{x \in \mathbb{Z} \mid x < a\}$$

358. Se $a < b$ e $c < d$, mostre que $a - d < b - c$.

359. Prove que: $a < b$ e $c < d \Rightarrow bc + ad < ac + bd$.

360. Mostre que, para todo $n \in \mathbb{Z}$, o conjunto $\{x \in \mathbb{Z} \mid n < x < n + 1\}$ é vazio.