$\mathbb{Z} = \mathbb{N}^2/R$, com R sendo definida por:

$$(a,b)\,R\,(c,d) \text{ sse } a+d = b+c$$

Definimos $+$ (binária), $-$ (unária) e 0 (constante).

$$\forall (a,b)\in\mathbb{N}^2\ \exists!\, n\in\mathbb{N}\ \Big(\underbrace{(a,b)\,R\,(n,0)}_{\frac{(a,b)}{R} = n} \text{ ou } \underbrace{(a,b)\,R\,(0,n)}_{\frac{(a,b)}{R} = -n}\Big)$$

$\mathbb{Z}$ pode ser identificado com o conjunto $\mathbb{N}\cup-\mathbb{N}$, onde $-\mathbb{N} = \{-n : n\in\mathbb{N}\}$. Mais precisamente, a função

$$\begin{aligned} i:\ \mathbb{N}\cup-\mathbb{N} &\to \mathbb{Z} \\ n\in\mathbb{N} &\mapsto (n,0)/R \\ -n\in-\mathbb{N} &\mapsto (0,n)/R \end{aligned}$$

é bijetora.

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

$$\frac{(a,b)}{R} \cdot \frac{(c,d)}{R} = \frac{(ac+bd\,,\, ad+bc)}{R}$$

A idéia intuitiva de $\frac{(a,b)}{R}$ seria $a-b$

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

Se $\frac{(a,b)}{R} = \frac{(a',b')}{R}$, então $\frac{(a,b)}{R} \cdot \frac{(c,d)}{R} = \frac{(a',b')}{R} \cdot \frac{(c,d)}{R}$

$\Updownarrow$

$(a,b)\,R\,(a',b') \Leftrightarrow \boxed{a+b' = b+a'}\,^{*}$, quero provar que

$$(ac+bd\,,\, bc+ad)\,R\,(a'c+b'd\,,\, b'c+a'd)$$

$$(ac+bd)+(b'c+a'd) = (a+b')c + (b+a')d \overset{*}{=} (b+a')c+(a+b')d$$

$= bc+a'c+ad+b'd = (a'c+b'd)+(bc+ad)$. Logo,

$$\frac{(ac+bd\,,\, bc+ad)}{R} = \frac{(a'c+b'd\,,\, b'c+a'd)}{R} \quad \checkmark$$

$n, m \in \mathbb{N}$

$$n \cdot m = \frac{(n,0)}{R} \cdot \frac{(m,0)}{R} = \frac{(nm + 0 \cdot 0,\ n \cdot 0 + 0 \cdot m)}{R} = \frac{(nm, 0)}{R}$$

$$n \cdot (-m) = \frac{(n,0)}{R} \cdot \frac{(0,m)}{R} = \frac{(n \cdot 0 + 0 \cdot m,\ nm + 0 \cdot 0)}{R} = \frac{(0, nm)}{R} = -(nm)$$

$$(-n) \cdot m = \frac{(0,n)}{R} \cdot \frac{(m,0)}{R} = \frac{(0 \cdot m + n \cdot 0,\ 0 \cdot 0 + nm)}{R} = \frac{(0, nm)}{R} \ ''$$

$$(-n)(-m) = \frac{(0,n)}{R} \cdot \frac{(0,m)}{R} = \frac{(0 \cdot 0 + n \cdot m,\ 0 \cdot m + n \cdot 0)}{R} = \frac{(nm, 0)}{R} = nm$$

$$\left(\frac{(a,b)}{R}\cdot\frac{(c,d)}{R}\right)\cdot\frac{(e,f)}{R} = \frac{(ac+bd,\ ad+bc)}{R}\cdot\frac{(e,f)}{R} =$$

$$= \frac{\big((ac+bd)e+(ad+bc)f,\ (ac+bd)f+(ad+bc)e\big)}{R} =$$

$$= \frac{(ace+bde+adf+bcf,\ acf+bdf+ade+bce)}{R} =$$

$$= \frac{\big(a(ce+df)+b(de+cf),\ a(cf+de)+b(df+ce)\big)}{R} =$$

$$= \frac{(a,b)}{R}\cdot\frac{(ce+df,\ cf+de)}{R} = \frac{(a,b)}{R}\cdot\left(\frac{(c,d)}{R}\cdot\frac{(e,f)}{R}\right)$$

$$\underbrace{\frac{(1,0)}{R}}_{=1} \cdot \frac{(a,b)}{R} = \frac{(1\cdot a + 0\cdot b, 1\cdot b + 0\cdot a)}{R} = \frac{(a,b)}{R}$$

$x \leq y$ sse $\exists m \in \mathbb{N} \, (x + m = y)$.

$$\frac{(a,b)}{R} \leq \frac{(c,d)}{R} \text{ sse } \exists m \in \mathbb{N} \left(\frac{(a,b)}{R} + \frac{(m,0)}{R} = \frac{(c,d)}{R} \right)$$

$\forall x, y \in \mathbb{Z} \, (x \leq y$ ou $y \leq x)$.

$x = \frac{(a,b)}{R}$, $y = \frac{(c,d)}{R}$. Consideremos $a+d$ e $b+c \in \mathbb{N}$.

Já sabemos que $a+d \leq b+c$ ou $b+c \leq a+d$, ou seja,

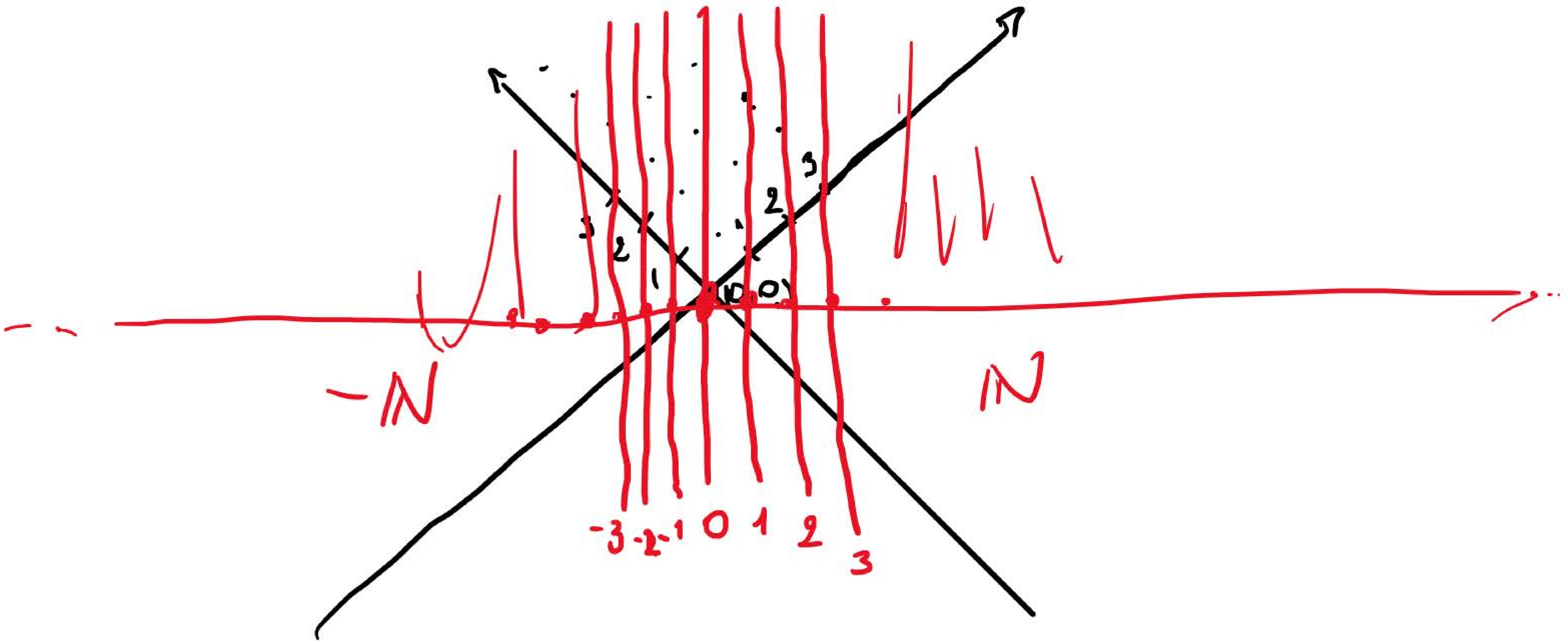
$\exists m \in \mathbb{N} \, (a+d+m = b+c$ ou $a+d = b+c+m)$. Então

$$\Downarrow \qquad\qquad \Downarrow$$

$$\frac{(a,b)}{R} + \frac{(m,0)}{R} = \frac{(a+m,b)}{R} = \frac{(c,d)}{R} \qquad \frac{(a,b)}{R} = \frac{(c+m,d)}{R} = \frac{(c,d)}{R} + \frac{(m,0)}{R}$$

Logo, vale a asserção.

$\leq$ é ordem total em $\mathbb{Z}$ também.


-N
N
(0,0)
-3 -2 -1 0 1 2 3
1
2
3
1
2
3

$(\mathbb{N}, +, \cdot, 0, 1)$ é um semianel comutativo com identidade

$(\mathbb{Z}, +, \cdot, -, 0, 1)$ é um anel " " "

$$j : \mathbb{N} \hookrightarrow \mathbb{Z}$$
$$n \longmapsto \overline{(n,0)}_R$$

homomorfismo de semianéis, ou seja:

$\forall m, n \in \mathbb{N}$,

$$j(m+n) = j(m) + j(n)$$

$$j(mn) = j(m)\, j(n)$$

$$j(0) = 0, \quad j(1) = 1$$

Exercícios de indução

$$\forall k \in \mathbb{N} \text{ ímpar}, \quad \sum_{i=0}^{k} (-2)^i = \frac{1-2^{k+1}}{3}$$

k ímpar $\Leftrightarrow$ $\exists n \, (k = 2n+1)$

$$\forall n \in \mathbb{N} \left(3 \cdot \sum_{i=0}^{2n+1} (-2)^i = 1 - 2^{2n+2} \right)$$

Ind. em n

Base $n=0$

$$3 \cdot \left((-2)^0 + (-2)^1 \right) = 1 - 2^{2\cdot 0 + 2}$$

$$3 \cdot (1 + (-2)) = -3 \qquad 1 - 2^2 = 1 - 4 = -3 \quad \checkmark$$

Passo

Hp.: $3 \cdot \sum_{i=0}^{2n+1} (-2)^i = 1 - 2^{2n+2}$

Tese $3 \cdot \sum_{i=0}^{2n+3} (-2)^i = 1 - 2^{2n+4}$

$$3 \cdot \sum_{i=0}^{2n+3} (-2)^i = 3 \left(\sum_{i=0}^{2n+1} (-2)^i + (-2)^{2n+2} + (-2)^{2n+3} \right) =$$

$$= \boxed{3 \cdot \sum_{i=0}^{2n+1} (-2)^i} + 3\left((-2)^{2n+2} + (-2)^{2n+3} \right) \overset{HP}{=}$$

$$= \boxed{1 - 1 \cdot 2^{2n+2}} + 3(-2)^{2n+2} + 3(-2)^{2n+3} \overset{(*)}{=}$$

$$= 1 \underbrace{-1} \cdot 2^{2n+2} \underbrace{+3} \cdot 2^{2n+2} + 3 \cdot (-2)^{2n+3} =$$

$$= 1 + 2 \cdot 2^{2n+2} + 3 \cdot (-2)^{2n+3} =$$

$$= 1 + 2^{2n+3} + 3 \cdot (-2)^{2n+3} =$$

$$= 1 + 2^{2n+3} - 3 \cdot 2^{2n+3} =$$

$$= 1 - 2 \cdot 2^{2n+3} = 1 - 1 \cdot (2 \cdot 2^{2n+3}) = 1 - 2^{2n+4}$$

$\forall n \, \forall k \, \left(n^{2k} = (-n)^{2k} \right)$ (*)

$a \in \mathbb{Z} \quad n \in \mathbb{N}$

$a^0 = 1$

$a^n = a^{n-1} \cdot a$

<u>Indução em k</u>

$n^{2 \cdot 0} = n^0 = 1 \,, \quad (-n)^{2 \cdot 0} = (-n)^0 = 1$ ✓

<u>Hp.</u> $n^{2k} = (-n)^{2k}$

<u>Tese</u> $n^{2k+2} = (-n)^{2k+2}$

$(-n)^{2k+2} = (-n)^{2k+1} \cdot (-n) = (-n)^{2k} \cdot (-n) \cdot (-n)$

$\overset{HP}{=} n^{2k} \cdot n \cdot n = n^{2k+2}$

$\forall a \in \mathbb{Z}\ \forall n, m \in \mathbb{N}\ \left(a^{n+m} = a^n \cdot a^m \right)$

<u>Ind. em m.</u>

<u>Base m=0</u> $a^{n+0} = a^n$ e $a^n \cdot a^0 = a^n \cdot 1 = a^n$ ✓

<u>Hp</u> $a^{n+m} = a^n \cdot a^m$

<u>Tese</u> $a^{n+(m+1)} = a^n \cdot a^{m+1}$

$$a^{n+(m+1)} = a^{(n+m)+1} = a^{n+m} \cdot a \overset{HP}{=} \left(a^n \cdot a^m\right) \cdot a =$$

$$= a^n \left(a^m \cdot a\right) = a^n \cdot a^{m+1} .$$

$\forall a \in \mathbb{Z}\ \forall m, n \in \mathbb{N}\ \left(a^{mn} = (a^m)^n \right)$

<u>Ind. em n.</u>

<u>Base n=0</u> $a^{m \cdot 0} = a^0 = 1$, $(a^m)^0 = 1$ ✓

<u>Hp.</u> $a^{mn} = (a^m)^n$

<u>Tese</u> $a^{m(n+1)} = (a^m)^{n+1}$

$$a^{m(n+1)} = a^{mn+m} = a^{mn} \cdot a^m \overset{HP}{=} (a^m)^n \cdot (a^m)^1 =$$

$$= (a^m)^{n+1} \quad ✓$$

$\underline{\text{Def.}}$ $0! = 1$ $\quad n \in \mathbb{N}$

$n! = (n-1)! \cdot n \quad \forall n > 0$

$\forall n \geq 4 \ (n! > n^2)$

$\underline{\text{Base } n=4}$

$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

$4^2 = 16 \qquad 4! > 4^2$

$\underline{\text{Hp.}}$ $n! > n^2$

$\underline{\text{Tese}}$ $(n+1)! > (n+1)^2$

$(n+1)! = n!(n+1) > n^2 \cdot (n+1)$

$> (n+1) \cdot (n+1) = (n+1)^2$ ✓

$\boxed{[n^2 > n+1]}$

Base $n=4$: $4^2 = 16 > 5 = 4+1$

$\underline{\text{Hp}}$ $n^2 > n+1$

$\underline{\text{Tese}}$ $(n+1)^2 > n+2$

$n^2 + 2n + 1 \overset{HP}{>} n+1+2n+1 =$

$= 3n+2 = \boxed{2n} + n+2 >$

$\geq n+2$ ✓

$\forall k \ ((k+4)! > (k+4)^2)$

Base $k=0$

$(0+4)! = 24$, $(0+4)^2 = 16$ ✓

$\underline{\text{Hp}}$ $(k+4)! > (k+4)^2$

$\underline{\text{Tese}}$ $(k+5)! > (k+5)^2$

$(k+5)! = (k+4)!(k+5) \overset{HP}{>}$

$> (k+4)^2 \cdot (k+5) > (k+5)(k+5)$

$\forall k \ ((k+4)^2 > k+5)$

$\underline{\text{Base } k=0}$ $4^2 = 16 > 5$

$\underline{\text{Hp}}$ $(k+4)^2 > k+5$

$\underline{\text{Tese}}$ $(k+5)^2 > k+6$

$(k+5)^2 = k^2 + 2k + 25 =$

$= (k^2 + k + 19) + k + 6 > k+6$

✓