$$\forall x \forall y \left((xy = 0 \wedge y \neq 0) \to x = 0 \right)$$

$$\forall x \forall y \left(xy = 0 \to (x = 0 \vee y = 0) \right)$$

<u>Dem.</u>

$$y \neq 0 \to \exists z \left(y = s(z) \right).$$

Então: $0 = xy = x\,s(z) \overset{P2}{=} xz + x \to x = 0.$

Exercícios

$$\forall n \geq 4\ \exists a, b\ (n = 2a + 5b)$$

$$\forall x\ \exists a, b\ (x + 4 = 2a + 5b)$$

Ind. em n

Base $(n=4)$ $\exists a, b\ (4 = 2a + 5b)$ Vale $(a = 2$ e $b = 0)$

Passo: H_p.: $\exists c, d\ (n = 2c + 5d)$

Tese: $\exists a, b\ (n + 1 = 2a + 5b)$

$$n + 1 \overset{HP}{=} 2c + 5d + 1$$

1° caso: $d = 0$. $5 \leq n + 1 = 2c + 1 \rightarrow c \geq 2$

$$2c = 2(c - 2 + 2) = 2(c-2) + 2 \cdot 2 = 2(c-2) + 4 \rightarrow$$

$$\rightarrow n + 1 = 2c + 1 = 2(c-2) + 4 + 1 = 2(c-2) + 5 \cdot 1$$

A tese vale com $a = c - 2$ e $b = 1$

2° caso: $d \neq 0$. $5 \leq n + 1 = 2c + 5d + 1 = 2c + 5(d - 1 + 1) + 1$

$$= 2c + 5(d-1) + 5 + 1 = 2c + 6 + 5(d-1) = 2(c+3) + 5(d-1)$$

A tese vale com $a = c + 3$, $b = d - 1$.

Seja $S \neq \emptyset$.

Def. Uma *operação n-ária* em S é uma função de S^n em S. Em particular uma operação 0-ária é uma função de S^0 em S, ou seja, de $\{\emptyset\}$ em S. Então ela pode ser identificada com o único elemento de S que está na imagem e, por isso, operações 0-árias são chamadas *constantes*.

$$\boxed{\begin{array}{l} S^0 = \{\emptyset\} \\ S^{n+1} = S^n \times S \quad \forall n \end{array}}$$

Def. Sejam $f_1, f_2, \ldots, f_k$ operações em S. Então a $k+1$-upla $(S, f_1, \ldots, f_k)$ é dita *estrutura algébrica* sobre S.

Uma estrutura $(S,*)$, $*$ binária, é um <u>semigrupo</u> se $\forall x,y,z \in S$:

(1) $(x*y)*z = x*(y*z)$ (prop. associativa de $*$).

<u>Exemplo</u> X conjunto. $S = X^X = \{ f : X \to X : f \text{ função} \}$.
$(S,\circ)$ é um semigrupo.

Uma estrutura $(S,*,e)$, com $*$ binária e e constante, é um monóide se vale (1) e, $\forall x \in S$,

(2) $x*e = e*x = x$

$(S,\circ,id_X)$ é monóide (ou semigrupo com identidade).

$(\mathbb{N},+,0)$ e $(\mathbb{N},\cdot,1)$ são monóides (comutativos)

Uma operação binária $*$ é comutativa se $\forall x,y$

(3) $x*y = y*x$.

Uma estrutura $(S,*,{}',e)$ com uma op. binária $*$, uma unária $'$ e uma constante e, é dita um <u>grupo</u> se, $\forall x,y,z \in S$, valem: (1), (2),

(4) $x \cdot x' = x' \cdot x = e$

(5) $(x')' = x$.

<u>Exemplo</u> X conjunto. $S_X = \{ f : X \to X \mid f \text{ é função bijetora} \}$
$(S_X, \circ, {}^{-1}, id_X)$ é um grupo (dito <u>grupo das simetrias de X</u>).

Grupos comutativos são chamados grupos abelianos (N. H. Abel).

Uma estrutura $(S, *, +, e)$ é um <u>semianel</u> se:

- $(S, *, e)$ é um monóide comutativo
- $(S, +)$ é um semigrupo

(6) $(x * y) + z = (x + z) * (y + z)$ e $x + (y * z) = (x + y) * (x + z)$

(7) $x + e = e + x = e$

$(\mathbb{N}, +, \cdot, 0)$ é semianel

$(S, *, +, e_1, e_2)$ é semianel com identidade se $(S, *, +, e_1)$ é semianel e e_2 é identidade de $+$.

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

Uma estrutura $(S, *, +, ', e)$ é um anel se:

- $(S, *, ', e)$ é um grupo abeliano
- $(S, +)$ é um semigrupo
- vale (6) e (7)

Def. Sejam $(S, f_1, \dots, f_k)$ e $(T, g_1, \dots, g_k)$ estruturas algébricas do mesmo tipo, ou seja, com a mesma quantidade de operações e aridades.

Seja $\nu(f_i)$ a aridade de f_i $\forall i$.

Uma função $\alpha : S \to T$ é um homomorfismo se $\forall i = 1, \dots, k$ $\forall x_1, x_2, \dots, x_{\nu(f_i)} \in S$,

$$\alpha\left(f_i\left(x_1, \dots, x_{\nu(f_i)}\right)\right) = g_i\left(\alpha(x_1), \dots, \alpha\left(x_{\nu(f_i)}\right)\right).$$

Ex. $(S, *_S)$ e $(T, *_T)$

$\forall x, y \in S$, $\alpha(x *_S y) = \alpha(x) *_T \alpha(y)$.

Construção de $\mathbb{Z}$

É um caso especial de uma construção chamada "simetrização de um monóide comutativo regular" e que consta na construção de um grupo abeliano a partir do monóide dado, de maneira que o grupo contenha uma cópia isomorfa do monóide.

$(\mathbb{N}, +, 0)$ $\qquad$ $(\mathbb{Z}, +, -, 0)$

unária

$x - y = x + (-y)$

Consideremos o conjunto $\mathbb{N}^2$ e definimos a relação binária R sobre $\mathbb{N}^2$ como segue:

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

R é reflexiva pois $a+b=b+a \Rightarrow (a,b)R(a,b)$

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

$\Leftrightarrow (c,d)R(a,b)$ R é simétrica

$$\left.\begin{array}{l}(a,b)R(c,d) \Rightarrow a+d=b+c \\ (c,d)R(e,f) \Rightarrow c+f=d+e\end{array}\right\} + \Rightarrow a+\cancel{d}+\cancel{c}+f=b+\cancel{c}+\cancel{d}+e$$

$\Rightarrow a+f=b+e \Rightarrow (a,b)R(e,f)$. R transitiva.

Seja $\mathbb{Z} = \mathbb{N}^2/R$

$(0,0)/R = \{(0,0),(1,1),(2,2),\ldots\}$ (0)

$(0,1)/R = \{(0,1),(1,2),(2,3),\ldots\}$ (-1)

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

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

Vamos provar que, se $(a',b')\,R\,(a,b)$, então

$$\frac{(a+c,\ b+d)}{R} = \frac{(a'+c,\ b'+d)}{R}.$$

$$\frac{(a,b)}{R} = \frac{(a',b')}{R} \iff (a,b)\,R\,(a',b') \iff a+b' = b+a'$$

Então $a+c+b'+d = a'+c+b+d \Rightarrow (a+c,\ b+d)\,R\,(a'+c,\ b'+d)$

$b+d+a'+c$

A soma é bem definida.

Definimos, $\forall \frac{(a,b)}{R} \in \mathbb{Z}$: $-\frac{(a,b)}{R} = \frac{(b,a)}{R}$.

Definimos a constante 0 como $0 = \frac{(0,0)}{R} =$

$= \{(a,a) : a \in \mathbb{N}\}$.

Se $\frac{(a,b)}{R} = \frac{(a',b')}{R}$, então $a+b' = b+a'$ e isto

implica $b+a' = a+b'$ e, então, $(b,a)\,R\,(b',a')$.

Logo, $\frac{(a,b)}{R} = \frac{(a',b')}{R} \Rightarrow \frac{(b,a)}{R} = \frac{(b',a')}{R}$.

$-$ é bem definido.

$\forall a,b \in \mathbb{N}\ \exists! n \in \mathbb{N}$ t.q.

$$\frac{(a,b)}{R} = \frac{(n,0)}{R} \quad \text{ou} \quad \frac{(a,b)}{R} = \frac{(0,n)}{R}$$

Dem.

Suponhamos, primeiro, $a \leq b$. Por def., $\exists n \in \mathbb{N}$ t.q. $a+n=b$. Então: $a+n=b \Rightarrow a+n=b+0 \Rightarrow$
$\Rightarrow (a,b)R(0,n) \Rightarrow \frac{(a,b)}{R} = \frac{(0,n)}{R}$.

Se $a \geq b$, então $\exists n \in \mathbb{N}\ (a=b+n) \Rightarrow$
$\Rightarrow a+0=b+n \Rightarrow (a,b)R(n,0) \Rightarrow \frac{(a,b)}{R} = \frac{(n,0)}{R}$.

Se $\exists n$ t.q. $\frac{(a,b)}{R} = \frac{(n,0)}{R} = \frac{(m,0)}{R}$, então

$(n,0)R(m,0)$, ou seja, $\underset{n}{\underset{\|}{n+0}} = \underset{m}{\underset{\|}{0+m}} \Rightarrow n=m$

Caso $\frac{(a,b)}{R} = \frac{(0,n)}{R} = \frac{(0,m)}{R}$ análogo.

Se $\exists m$ t.q. $\frac{(a,b)}{R} = \frac{(n,0)}{R} = \frac{(0,m)}{R} \Rightarrow$

$\Rightarrow (n,0)R(0,m) \Rightarrow n+m=0+0=0 \Rightarrow n=m=0$.

Então, se $\frac{(a,b)}{R} = \frac{(n,0)}{R}$, a classe será denotada simples. por n

se $\frac{(a,b)}{R} = \frac{(0,n)}{R}$, então será den. por $-n$

pois $n = \frac{(n,0)}{R} \Rightarrow -n = \frac{(0,n)}{R}$

$-\frac{(a,b)}{R} = \frac{(b,a)}{R}$

então, se eu decido de chamar n a classe $\frac{(n,0)}{R}$, naturalmente, $-n$ será $-\frac{(n,0)}{R} = \frac{(0,n)}{R}$