# Els nombres naturals. Caracterització de $\mathbb{N}$

## 1 Sistemes de Peano

**Definició 1.1** (Sistema de Peano)**.** Un sistema de Peano és una estructura $(A, a, f)$ on $A$ és un conjunt no buit, $a \in A$ i $f : A \to A \setminus \{a\}$ és una bijecció.

**Propietat 1.0.1** (Inducció)**.** Per qualsevol $X \subseteq A$ si $0 \in A$ i $\forall x \in X\ f(x) \in X$, llavors $X = A$.

**Proposició 1.1.** • Existeixen sistemes de Peano.

- Si $(A, a, f)$ i $(B, b, g)$ són sistemes de Peano llavors són isomòrfics. És a dir, existeix una bijecció $h : A \to B$ tal que $h(a) = b$ i $\forall x \in A\ h(f(x)) = g(h(x))$.

## 2 Els nombres naturals

Considerem la funció successor. $S : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ definida per $S(n) = n + 1$. $(\mathbb{N}, 0, S)$ és un sistema de Peano.

### 2.1 Suma en $\mathbb{N}$

**Definició 2.1** (Suma en $\mathbb{N}$)**.** $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que compleix els axiomes de la suma de nombres naturals.

A1) $\forall n \in \mathbb{N} \quad n + 0 = n$.

A2) $\forall n, m \in \mathbb{N} \quad n + S(m) = S(n + m)$.

Això és la definició recursiva de la suma en $\mathbb{N}$. És pot demostrar que és l'única operació que compleix aquestes dues propietats.

**Propietat 2.1.1.** La suma en $\mathbb{N}$ és associativa.

$$\forall n, m, k \in \mathbb{N} \qquad (n + m) + k = n + (m + k)$$

*Demostració.* Sigui $n, m \in \mathbb{N}$ i sigui $X = \{k \in \mathbb{N} \mid (n + m) + k = n + (m + k)\}$. Per inducció es vol demostrar que $X = \mathbb{N}$.
**Cas base:** Si $k = 0$. $(n + m) + 0 = n + m$. De la mateixa manera $n + (m + 0) = n + (m) = n + m$. Per tant $0 \in X$.
**Cas inductiu:** Es suposa que $k \in X$. Es vol veure que $S(k) \in X$.

$$\begin{aligned}(n + m) + S(k) &= S((n + m) + k) && \text{(Per A2)}\\ &= S(n + (m + k)) && \text{(Ja que } k \in X)\\ &= n + S(m + k)\\ &= n + (m + S(k))\end{aligned}$$

Per tant $S(k) \in X$ i aleshores per la propietat d'inducció $X = \mathbb{N}$. □

**Propietat 2.1.2.** La suma en $\mathbb{N}$ és commutativa.

$$\forall n, m \in \mathbb{N} \qquad n + m = m + n$$

**Lema 2.1.** Per cada $n \in \mathbb{N}$ es compleix que $0 + n = n$.

*Demostració.* Per inducció sobre $n$. Si $n = 0$ és evident que $0 + 0 = 0$.
Suposem que $0 + n = n$ es vol veure que $0 + S(n) = S(n)$.

$$\begin{aligned} 0 + S(n) =& S(0 + n) \quad \text{(Per A2)} \\ =& S(n) \quad \text{(Per la HI)} \end{aligned}$$

Per tant es compleix. □

**Lema 2.2.** Per cada $n, m \in \mathbb{N}$ es compleix que $S(n) + m = S(n + m)$.

*Demostració.* Per inducció sobre $m$. Si $m = 0$, fent ús del primer lema es veu que

$$S(n) + 0 = S(n + 0) = S(n)$$

Suposem que $S(n) + m = S(n + m)$ es vol veure per $S(m)$,

$$\begin{aligned} S(n) + S(m) =& S(S(n) + m)) \quad \text{(Per A2)} \\ =& S(S(n + m)) \quad \text{(Per HI)} \\ =& S(n + S(m)) \end{aligned}$$

Per tant es compleix. □

**Proposició 2.1.** La suma és commutativa

*Demostració.* Per inducció sobre $m$. Cas Base: Si $m = 0$ llavors n+0=0+n=n.
Cas inductiu: Suposem $n + m = m + n$. Es vol veure per $S(m)$.

$$\begin{aligned} n + S(m) =& S(n + m) \\ =& S(m + n) \\ =& S(m) + n \end{aligned}$$

Per tant la suma és commutativa. □

**Propietat 2.1.3.** $\forall n, m, k \in \mathbb{N}$,

$$n + k = m + k \to n = m$$

## 2.2 Producte en $\mathbb{N}$

**Definició 2.2** (Producte en $\mathbb{N}$)**.** $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ és l'única operació que compleix

1. $n \cdot 0 = 0$.
2. $n \cdot S(m) = n \cdot m + n$.

**Propietat 2.2.1.** El producte és associatiu.

$$(nm)k = n(mk)$$

**Propietat 2.2.2.** El producte és commutatiu.

$$nm = mn$$

**Propietat 2.2.3.** El producte es distribueix sobre la suma.

$$n(m+k) = n \cdot m + n \cdot k \qquad \forall n, m, k \in \mathbb{N}$$

**Propietat 2.2.4.** Sigui $S(0) = 1$. $1 \cdot n = n$

**Propietat 2.2.5.** Si $nm = 0$ llavors $n = 0$ o $m = 0$.

**Propietat 2.2.6.** Si $nk = mk$ i $k \neq 0$ llavors $n = m$.

## 2.3 Exponenciació en $\mathbb{N}$

**Definició 2.3** (Exponenciació)**.** $\exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $\exp(n, m) = n^m$ es defineix a partir dels següents axiomes.

- $n^0 = 1$.
- $n^{S(m)} = n^m \cdot n$.

**Propietat 2.3.1.** $\forall n, m, k \in \mathbb{N}$ es compleix $n^{m+k} = n^m \cdot n^k$.

**Propietat 2.3.2.** $\forall n, m, k \in \mathbb{N}$ es compleix $n^{m \cdot k} = (n^m)^k$.

**Propietat 2.3.3.** $1^n = 1$ i $n^1 = n$ per qualsevol $n \in \mathbb{N}$.

**Propietat 2.3.4.** $0^n = 0$ si $n \neq 0$.

## 2.4 Ordre en $\mathbb{N}$

**Definició 2.4** (Ordre reflexiu en $\mathbb{N}$)**.** Es diu $n \leq m$ si $\exists k \in \mathbb{N}$ tal que $n + k = m$.

**Proposició 2.2.** La relació proposada és un ordre reflexiu.

*Demostració.*

- Propietat reflexiva. $n \leq n$ ja que si es pren $k = 0$ llavors $n = n$.
- Propietat antisimètrica. Suposem $n \leq m$ i $m \leq n$. Llavors podem escriure $n + k = m$ i $m + j = n$ amb $k, j \in \mathbb{N}$. Substituint s'obté

  $$m + j + k = m$$

  i per tant $j + k = 0$. Com que $j, k$ són naturals llavors els dos han de ser 0 i per tant $n = m$.
- Propietat transitiva. Suposem $n \leq m$ i $m \leq k$. Llavors existeixen $j, i \in \mathbb{N}$ tals que $n + j = m$ i $m + i = k$. Per tant $n + j + i = k$ i per tant $n \leq k$.

□

### 2.4.1 Propietats de l'ordre

1. 0 és el menor natural.
$$0 \leq n \qquad \forall n \in \mathbb{N}$$
2. $S(n)$ és el successor immediat de $n$ en l'ordre.
   (a) $n \leq S(n)$.
   (b) Si $\exists k \in \mathbb{N}$ tal que $n \leq k$ i $k \leq S(n)$ llavors $k = n$ o $k = S(n)$.
3. No hi ha un element major.
$$\forall n \in \mathbb{N} \;\; n \leq S(n)$$
4. L'ordre és total. Per qualsevol $n, m \in \mathbb{N}$ es compleix $n \leq m$ o $m \leq n$.
5. $n + k \leq m + k$ implica $n \leq k$.
6. $n \leq m$ implica $n \cdot k \leq m \cdot k$.
7. $n \leq m$ i $k \neq 0$ implica $n \cdot k \leq m \cdot k$.

**Definició 2.5** (Ordre estricte)**.** L'ordre estricte es defineix com
$$n < m \iff n \leq m \text{ i } n \neq m$$

**Proposició 2.3.** $n < m$ si i només si $\exists k \in \mathbb{N}$ i $k \neq 0$ tal que $n + k = m$.

**Teorema 2.1.** L'ordre en $\mathbb{N}$ és un bon ordre. És a dir, tot subconjunt no buit de $\mathbb{N}$ té un mínim.

# 3 Construcció de $\mathbb{Z}$

Es defineix una relació $\sim$ en $\mathbb{N} \times \mathbb{N}$ de manera que
$$\begin{aligned}(n, m) \sim (i, j) &\iff n - m = i - j \\ &\iff n + j = i + m\end{aligned}$$
Com que se suposa que no es sap restar fins ara la relació s'escriu millor de la segona manera.

**Definició 3.1.** Sigui $\sim$ una relació en $\mathbb{N} \times \mathbb{N}$ tal que
$$(n, m) \sim (i, j) \iff n + j = i + m$$

**Lema 3.1.** $\sim$ és una relació d'equivalència en $\mathbb{N} \times \mathbb{N}$.

*Demostració.*
- Reflexivitat: $(n, m) \sim (n, m)$ ja que $n + m = n + m$.
- Simetria: Suposem $(n, m) \sim (i, j)$. Llavors
$$\begin{aligned}n + j &= i + m \\ j + n &= m + i \iff (i, j) \sim (n, m)\end{aligned}$$
- Transitiva: Suposem $(n, m) \sim (i, j)$ i $(i, j) \sim (p, q)$. Llavors $n + j = i + m$ i $i + q = j + p$. Es sumen les dues equacions, es simplifica i s'obté $n + q = m + p$ i per tant $(n, m) \sim (p, q)$.

□

**Definició 3.2** (El conjunt $\mathbb{Z}$)**.** El conjunt $\mathbb{Z}$ és el conjunt quocient de la relació $\sim$.
$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$
$\overline{(n, m)}$ representa el nombre $n - m$. Els naturals en $\mathbb{Z}$ són de la forma $(n, 0)$.

## 3.1 Suma en $\mathbb{Z}$

**Definició 3.3** (Suma en $\mathbb{Z}$)**.** Es defineix $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ com

$$\overline{(n,m)} + \overline{(i,j)} = \overline{(n+i, m+j)}$$

**Proposició 3.1.** La definició és independent dels representants escollits. Si $(n,m) \sim (n',m')$ i $(i,j) \sim (i',j')$ llavors $(n+i, m+j) \sim (n'+i', m'+j')$.

*Demostració.* Si $(n,m) \sim (n',m')$ llavors $n + m' = n' + m$ i si $(i,j) \sim (i',j')$ llavors $i + j' = i' + j'$. Es sumen les dues equacions

$$\begin{aligned} n + m' &= m + n' \\ i + j' &= i' + j \\ n + m' + i + j' &= m + n' + i' + j \\ (n+i) + (m'+j') &= (m+j) + (n'+i') \end{aligned}$$

Per tant $(n+i, m+j) \sim (n'+i', m'+j')$. □

### 3.1.1 Propietats de la suma

**Propietat 3.1.1.** La suma és associativa.

**Propietat 3.1.2.** La suma és commutativa.

*Demostració.* Sigui $a = \overline{(n,m)}$ i $b = \overline{(i,j)}$.

$$\begin{aligned} a + b &= \overline{(n,m)} + \overline{(i,j)} \\ &= \overline{(n+i, m+j)} \\ &= \overline{(i+n, j+n)} \\ &= b + a \end{aligned}$$

□

**Propietat 3.1.3.** $\forall a \in \mathbb{Z}$, $a + \overline{(0,0)} = a$.

*Demostració.* Sigui $a = \overline{(n,m)}$. Llavors

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

□

**Propietat 3.1.4.** $-a = \overline{(m,n)}$ és l'element oposat per $a = \overline{(n,m)}$.

**Observació 3.1.1.** $(\mathbb{Z}, +)$ és un grup abelià. S'han estès els nombres naturals a un grup.

## 3.2 Producte en $\mathbb{Z}$

**Definició 3.4** (Producte en $\mathbb{Z}$)**.** $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ es defineix com

$$\overline{(n,m)} \cdot \overline{(i,j)} = \overline{(ni + mj, nj + mi)}$$

**Proposició 3.2.** La definició és independent dels representants escollits.

### 3.2.1 Propietats del producte en $Z$

**Propietat 3.2.1.** El producte és associatiu.

**Propietat 3.2.2.** El producte és commutatiu.

**Propietat 3.2.3.** El producte és distribueix sobre la suma. $\forall a, b, c \in \mathbb{Z}$, $a(b+c) = ab + bc$.

**Propietat 3.2.4.** Per qualsevol $a \in \mathbb{Z}$, $a \cdot (1, 0) = a$.

**Observació 3.2.1.** $(\mathbb{Z}, +, 0, \cdot, 1)$ és un anell abelià unitari.

## 3.3 Ordre en $\mathbb{Z}$

**Definició 3.5** (Ordre reflexiu en $\mathbb{Z}$)**.** En l'ordre de $\mathbb{Z}$ $\overline{(n,m)} \leq \overline{(i,j)}$ si i només si $n + j \leq m + i$.

**Proposició 3.3.** La definició és independent dels representants escollits.

## 3.4 Immersió canònica de $\mathbb{N}$ en $\mathbb{Z}$

Sigui $f : \mathbb{N} \to \mathbb{Z}$ una funció tal que $n \mapsto \overline{(n, 0)}$.

- $f$ és injectiva.
- $\mathbf{rec}\, f = \{a \in \mathbb{Z} \mid a \geq f(0)\}$.
- $f(a + b) = f(a) + f(b)$.
- $f(a \cdot f(b) = f(a) \cdot f(b)$.
- En aquest sentit es pot dir que $\mathbb{N} \subseteq \mathbb{Z}$ però més precisament

$$\{(n, 0) \mid n \in \mathbb{N}\} \subseteq \mathbb{Z}$$

# 4 Construcció de $\mathbb{Q}$

En $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ es defineix una relació d'equivalència $\sim$ de manera que $\overline{(a, b)} = \frac{a}{b}$.

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

Fàcilment es veu que $\sim$ és una relació d'equivalència i es defineix el conjunt quocient com el conjunt dels nombres racionals.

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$$

**Observació 4.0.1.** $(\mathbb{Q}, +, \cdot, 0, 1, \leq)$ és un cos ordenat.