5 Insiemi numerici

In questo paragrafo vogliamo introdurre, con un certo grado di precisione, le strutture numeriche elementari, alcune delle quali peraltro avevamo assunto parzialmente già note nei paragrafi precedenti.

Studieremo quindi:

- ($\boldsymbol{A}$) Numeri naturali e principio d'induzione.
- ($\boldsymbol{B}$) Numeri interi.
- ($\boldsymbol{C}$) Numeri razionali.
- ($\boldsymbol{D}$) Numeri reali (cenno).
- ($\boldsymbol{E}$) Numeri complessi.
- ($\boldsymbol{F}$) Quaternioni.

($\boldsymbol{A}$) NUMERI NATURALI

Definizione 1. *Si chiama terna di Peano ogni terna* $(\boldsymbol{N}, 0, \sigma)$, *dove:*

(i) $\boldsymbol{N}$ *è un insieme non vuoto;*

(ii) 0 *è un elemento di* $\boldsymbol{N}$*;*

(iii) $\sigma : \boldsymbol{N} \to \boldsymbol{N}$ *è un'applicazione verificante i tre seguenti assiomi, detti assiomi di Peano:*

($\boldsymbol{P}_1$) σ *è iniettiva;*

($\boldsymbol{P}_2$) $0 \notin Im(\sigma)$*;*

($\boldsymbol{P}_3$) *Per ogni* $U \subseteq \boldsymbol{N}$ *tale che* $\begin{cases} (\boldsymbol{a}) & 0 \in U, \\ (\boldsymbol{b}) & \sigma(U) \subseteq U, \end{cases}$ *risulta* $U = \boldsymbol{N}$.

L'applicazione σ *è detta applicazione del successivo. Il terzo assioma di Peano* ($\boldsymbol{P}_3$) *è detto principio d'induzione matematica. Si pone usualmente:*

$$\sigma(0) =: 1, \quad \sigma(1) =: 2, \quad \sigma(2) =: 3, \ ...$$

[dove $0, 1, 2, ...$ *vanno al momento interpretati come simboli e non come numeri naturali!]. Per semplicità si scriverà* $\boldsymbol{N}$ *in luogo di* $(\boldsymbol{N}, 0, \sigma)$.

Se una tale terna di Peano $\boldsymbol{N} = (\boldsymbol{N}, 0, \sigma)$ *esiste ed è unica, è detta insieme dei numeri naturali.*

Che una terna di Peano esista non può però essere dimostrato, ma va invece accettato come assioma (detto *assioma dell'infinito*). L'unicità di $(\boldsymbol{N}, 0, \sigma)$ può essere invece facilmente dimostrata in questa forma: *se* $(\boldsymbol{N}, 0, \sigma)$ *e* $(\boldsymbol{N}', 0', \sigma')$ *sono due terne di Peano, esiste un'unica biiezione* $\varphi : \boldsymbol{N} \to \boldsymbol{N}'$ *tale che* $\sigma'(\varphi(n)) = \varphi(\sigma(n)), \ \forall\, n \in \boldsymbol{N}$.

Dunque i numeri naturali sono un concetto primitivo, ma le proprietà della precedente definizione ci consentono di caratterizzarli, prescindendo dalla loro natura.

Osservazione 1. Dall'assioma ($\boldsymbol{P}_3$) segue subito che

($*$) $\qquad n = \sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big), \ \forall\, n \in \boldsymbol{N}^{\cdot} := \boldsymbol{N} - \{0\}.$

Basta osservare che l'insieme $U = \{0, \sigma(0), \sigma(\sigma(0)), \sigma(\sigma(\sigma(0))), ...\}$ verifica le condizioni ($\boldsymbol{a}$) e ($\boldsymbol{b}$) di ($\boldsymbol{P}_3$). Dunque $U = \boldsymbol{N}$. Da ($*$) segue che

($**$) $\qquad n \neq \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big), \ \forall\, n \in \boldsymbol{N}.$

In base a ($\boldsymbol{P}_2$), $0 \neq \sigma(\sigma\ ...\ \sigma(0))$. Sia $n \in \boldsymbol{N}^{\cdot}$ e [in base a ($*$)] $n = \sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big)$. Se per assurdo fosse $n = \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big)$, allora $\sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big) = \sigma\big(\sigma(\ ...\quad \sigma(\sigma(\sigma(\ ...\quad \sigma(n)\,)))\,)\big)$. Utilizzando ripetutamente l'iniettività di σ, si otterrebbe $0 = \sigma(\sigma\ ...\ \sigma(0))$, cioè $0 \in Im(\sigma)$: assurdo.

Definizione 2. *In* $\boldsymbol{N}$ *è definita la seguente relazione di diseguaglianza stretta* $<$: $\forall\, n, m \in \boldsymbol{N}$,

$$n < m \iff m = \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big)$$

[cioè $n < m \iff m$ "è un successivo" di n]. Ad essa resta ovviamente associata la relazione di diseguaglianza debole $\leq$, così definita: $\forall\, n, m \in \boldsymbol{N}$,

$$n \leq m \iff n = m \text{ oppure } n < m.$$

Proposizione 1. *$(\boldsymbol{N}, \leq)$ è un insieme totalmente ordinato, con primo elemento 0.*

Dim. La relazione $\leq$ è riflessiva per definizione. Verifichiamo che è transitiva: se $n < m$ e $m < p$, allora $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$, $p = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$ e dunque $p = \sigma\big(\sigma(\ \dots\ \ \sigma(\sigma(\sigma(\ \dots\ \ \sigma(n)\,)))\,)\big)$. Allora $n < p$. [Se fosse $n = m$ o $m = p$, la transitività sarebbe immediata]. Verifichiamo ora che $\leq$ è antisimmetrica. Sia $n \leq m$, $m \leq n$ e, per assurdo, $n \neq m$. Allora $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$ e $n = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$, da cui $m = \sigma\big(\sigma(\ \dots\ \ \sigma(\sigma(\sigma(\ \dots\, \sigma(m)\,)))\,)\big)$. Ciò è assurdo in base a (**).

Verifichiamo ora che $\leq$ è totale. Siano $n, m \in \boldsymbol{N}^{\cdot}$, con $n \neq m$. Da (*), se $n = \sigma\big(\sigma(\ \dots\ \ \sigma(0)\,)\big)$ ed $m = \sigma\big(\sigma(\ \dots\ \ \sigma(0)\,)\big)$, confrontando tali scritture segue subito che $n = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$ oppure $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$, cioè $n < m$ oppure $m < n$.

Infine, che 0 sia il primo elemento di $\boldsymbol{N}$ è ovvio.

Definizione 3. *Su $\boldsymbol{N}$ è definita la seguente operazione di addizione (o somma) $+ : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ tale che, $\forall\, n, m \in \boldsymbol{N}$,*

$$n + 0 = n; \quad n + \sigma(m) = \sigma(n + m).$$

Si noti che $n + \sigma(0) = \sigma(n + 0) = \sigma(n)$, cioè $\sigma(n) = n + 1$. È per tale motivo che σ è stata chiamata "applicazione del successivo".

Osservazione 2. (*i*) La precedente definizione di somma è di tipo *induttivo* o *ricorsivo*: per calcolare $n + m$ occorre aver calcolato $n + k$, $\forall\, k < n$. La validità logica di un siffatto tipo di definizione discende dal principio d'induzione. Ma non insistiamo oltre su ciò.

(*ii*) Se $n < m$, $\exists!\, h \in \boldsymbol{N}$ tale che $m = n + h$. Sia infatti ad esempio $m = \sigma(\sigma(\sigma(n)))$. Allora

$$m = \sigma(\sigma(\sigma(n + \sigma(0)))) = \sigma(\sigma(n + \sigma(\sigma(0)))) = \sigma(n + \sigma(\sigma(\sigma(0)))) = n + \sigma(\sigma(\sigma(\sigma(0)))) = n + 4.$$

Veniamo ora all'unicità di h. Assumiamo che sia $m = n + h = n + h'$ e, ad esempio, $h < h'$. Allora $\underbrace{\sigma\big(\sigma(\ \dots\ \ \sigma}_{h}(n)\,)\big) = \underbrace{\sigma\big(\sigma(\ \dots\ \ \sigma}_{h'}(n)\,)\big)$ e, in base all'iniettività di σ, $n = \underbrace{\sigma\big(\sigma(\ \dots\, \sigma}_{h'-h}(n)\,)\big)$. Ciò è assurdo in base a (**). Il naturale h viene denotato usualmente $m - n$.

(*iii*) L'addizione in $\boldsymbol{N}$ verifica la proprietà associativa: $(n + m) + p = n + (m + p)$, $\forall\, m, n, p \in \boldsymbol{N}$. Per verificare tale proprietà si segue un procedimento induttivo. Si ha infatti, posto $p = 1$:

$$(n + m) + 1 = \sigma(n + m) = n + \sigma(m) = n + (m + 1).$$

Allora, posto $p = 2$: $(n+m)+2 = (n+m)+\sigma(1) = \sigma((n+m)+1) = \sigma(n+(m+1)) = n+\sigma(m+1) = n + (m + \sigma(1)) = n + (m + 2)$.

Assumendo quindi $(n+m)+(p-1) = n+(m+(p-1))$, si verifica che $(n+m)+p = n+(m+p)$.

Definizione 4. *Su $\boldsymbol{N}$ è definita la seguente operazione di moltiplicazione (o prodotto) $\cdot : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ tale che, $\forall\, n, m \in \boldsymbol{N}$,*

$$n \cdot 0 = 0; \quad n \cdot \sigma(m) = n \cdot m + n.$$

In particolare, $n \cdot 1 = n \cdot \sigma(0) = n \cdot 0 + n = 0 + n = n$, cioè $n \cdot 1 = n$. Anche tale definizione è induttiva.

La verifica delle proprietà della somma e del prodotto è, come osservato nella precedente osservazione, piuttosto laboriosa. Ci limitiamo quindi ad elencarne le principali, senza dimostrazione.

Proposizione 2. *Le operazioni di somma e prodotto verificano le seguenti proprietà:*

(1) $(n + m) + p = n + (m + p)$, $\forall\, n, m, p \in \boldsymbol{N}$ (proprietà associativa della somma);

(2) $n+0=n=0+n,\ \forall\, n\in\boldsymbol{N}$ *(esiste l'elemento neutro della somma,* 0*);*
(3) $n+m=m+n,\ \forall\, n,\, m\in\boldsymbol{N}$ *(proprietà commutativa della somma);*
(4) $(nm)p=n(mp),\ \forall\, n,\, m,\, p\in\boldsymbol{N}$ *(proprietà associativa del prodotto);*
(5) $n\cdot 1=n=1\cdot n,\ \forall\, n\in\boldsymbol{N}$ *(esiste l'elemento neutro del prodotto,* 1*);*
(6) $nm=mn,\ \forall\, n,\, m\in\boldsymbol{N}$ *(proprietà commutativa del prodotto);*
(7) $mn=0 \iff m=0$ *oppure* $n=0$*;*
(8) $mn=1 \iff m=n=1$*;*
(9) $\begin{cases}(m+n)p=mp+np,\\ m(n+p)=mn+mp,\end{cases}\quad \forall\, m,\, n,\, p\in\boldsymbol{N}$ *(proprietà distributive a destra e sinistra);*
(10) $m+n_1=m+n_2 \implies n_1=n_2$ *(legge di cancellazione della somma);*
(11) $mn_1=mn_2,\ m\neq 0 \implies n_1=n_2$ *(legge di cancellazione del prodotto);*
(12) $n_1<n_2 \iff n_1+n<n_2+n,\ \forall\, n\in\boldsymbol{N}$*;*
(13) $n_1<n_2 \iff n_1 n<n_2 n,\ \forall\, n\in\boldsymbol{N},\ n\neq 0$*;*
(14) $\forall\, m,\, n\in\boldsymbol{N},\ n\neq 0,\ \exists\, p\in\boldsymbol{N}$ *tale che* $m<np$ *(proprietà archimedea di* $\boldsymbol{N}$*).*

IL PRINCIPIO D'INDUZIONE

Poiché $\sigma(k)=k+1,\ \forall\, k\in\boldsymbol{N}$, l'assioma di Peano $(\boldsymbol{P}_3)$ può essere riformulato in questo modo:

$(\boldsymbol{P}_3)$ *Per ogni* $U\subseteq\boldsymbol{N}$ *tale che* $\begin{cases}(\boldsymbol{a})\ \ 0\in U,\\ (\boldsymbol{b})\ \ k\in U \implies k+1\in U\ \ [\forall\, k\geq 0],\end{cases}$ *risulta* $U=\boldsymbol{N}$.

Dall'assioma $(\boldsymbol{P}_3)$ segue il *"metodo di prova per induzione"*:

Proposizione 3. *Sia* $\mathcal{P}(n)$ *un'affermazione da dimostrare, definita* $\forall\, n\in\boldsymbol{N}$*. Se*

(i) $\mathcal{P}(0)$ *è vera,*

(ii) $\mathcal{P}(k)$ *vera* $\implies \mathcal{P}(k+1)$ *vera* $\quad[\forall\, k\geq 0]$*,*

allora $\mathcal{P}(n)$ *è vera,* $\forall\, n\in\boldsymbol{N}$*.*

La (i) è detta "base induttiva", la (ii) è detta "passo induttivo", l'ipotesi " $\mathcal{P}(k)$ *vera" [in (ii)] è detta "ipotesi induttiva".*

Dim. Posto $U:=\{n\in\boldsymbol{N}\ :\ \mathcal{P}(n)\ \text{è vera}\}$, bisogna verificare che $U=\boldsymbol{N}$.
Poiché vale (i), U verifica la condizione $(\boldsymbol{a})$ di $(\boldsymbol{P}_3)$. Poiché vale (ii), U verifica anche la condizione $(\boldsymbol{b})$ di $(\boldsymbol{P}_3)$. Da $(\boldsymbol{P}_3)$ segue che $U=\boldsymbol{N}$.

Osservazione 3. La base induttiva può essere anche riferita ad un naturale $k_0>0$. In tal caso il passo induttivo (ii) va verificato per ogni $k\geq k_0$.

Il passo induttivo (ii) può essere ovviamente anche formulato in questo modo:
(ii) $\mathcal{P}(k-1)$ vera $\implies \mathcal{P}(k)$ vera $\quad[\forall\, k\geq 1]$.

Esiste una seconda formulazione del principio d'induzione, detta *forma forte* (o *seconda forma*) *del principio d'induzione*:

$(\boldsymbol{P}_3')$ *Per ogni* $V\subseteq\boldsymbol{N}$ *tale che* $\begin{cases}(\boldsymbol{a})\ \ 0\in V,\\ (\boldsymbol{b}')\ \ \{0,1,\dots,k\}\subseteq V \implies k+1\in V\ \ [\forall\, k\geq 0],\end{cases}$ *risulta* $V=\boldsymbol{N}$.

L'assioma $(\boldsymbol{P}_3')$ fornisce il seguente *"metodo di prova per induzione forte"*:

Proposizione 4. *Sia* $\mathcal{P}(n)$ *un'affermazione da dimostrare, definita* $\forall\, n\in\boldsymbol{N}$*. Se:*

(i) $\mathcal{P}(0)$ *è vera,*

(ii') $\mathcal{P}(h)$ *vera,* $\forall\, h = 0, 1, \ldots k, \implies \mathcal{P}(k+1)$ *vera* $\quad [\forall\, k \geq 0]$,

allora $\mathcal{P}(n)$ *è vera,* $\forall\, n \in \boldsymbol{N}$.

Dim. Posto $V := \{n \in \boldsymbol{N} \,:\, \mathcal{P}(n) \text{ è vera}\}$, bisogna verificare che $V = \boldsymbol{N}$.

L'insieme V verifica le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b'})$ di $(\boldsymbol{P}'_3)$, in quanto valgono (i) e (ii). Allora da $(\boldsymbol{P}'_3)$ segue che $V = \boldsymbol{N}$.

Vogliamo ora dimostrare che $(\boldsymbol{P}_3)$ è equivalente a $(\boldsymbol{P}'_3)$. A tale scopo conviene utilizzare un terzo assioma, ad essi equivalente. Tale assioma, detto *principio del minimo* o *principio del buon ordinamento* [abbreviato $\boldsymbol{BO}$] è il seguente:

*(**BO**) Ogni sottoinsieme non vuoto* $T \subseteq \boldsymbol{N}$ *ha un minimo [cioè* $\exists\, t_0 \in T \,:\, t_0 \leq t,\ \forall\, t \in T$, *cfr.* **Def. 4.6***].*

Teorema 1. *I tre assiomi* $(\boldsymbol{P}_3)$, $(\boldsymbol{P}'_3)$ *e* $(\boldsymbol{BO})$ *sono equivalenti.*

Dim. Dimostreremo che $(\boldsymbol{P}'_3) \implies (\boldsymbol{P}_3) \implies (\boldsymbol{BO}) \implies (\boldsymbol{P}'_3)$.

$(\boldsymbol{P}'_3) \implies (\boldsymbol{P}_3)$. Preso un insieme $U \subseteq \boldsymbol{N}$ verificante le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b})$ di $(\boldsymbol{P}_3)$, bisogna provare che $U = \boldsymbol{N}$. Basta dimostrare che U verifica $(\boldsymbol{b'})$ [perché allora, per $(\boldsymbol{P}'_3)$, $U = \boldsymbol{N}$]. Sia $\{0, 1, \ldots k\} \subseteq U$. In particolare $k \in U$ e quindi, per $(\boldsymbol{b})$, $k+1 \in U$. Dunque U verifica $(\boldsymbol{b'})$.

$(\boldsymbol{P}_3) \implies (\boldsymbol{BO})$. Per assurdo, esista un sottoinsieme non vuoto $T \subseteq \boldsymbol{N}$, privo di minimo. Certo T ha almeno due elementi distinti [altrimenti avrebbe minimo]. Poniamo

$$U := Minor(T) = \{k \in \boldsymbol{N} \,:\, k \leq t,\ \forall\, t \in T\} \quad [\text{cfr. } \textbf{Def. 4.7}].$$

Poiché $T \subseteq \boldsymbol{N}$, allora $0 \in U$ e dunque U verifica la condizione $(\boldsymbol{a})$ di $(\boldsymbol{P}_3)$. Osserviamo ora che $U \neq \boldsymbol{N}$ [se infatti $t_1, t_2 \in T$, con $t_1 < t_2$, allora $t_2 \notin U$]. Ne segue che U non verifica la condizione $(\boldsymbol{b})$ [altrimenti $U = \boldsymbol{N}$, in base a $(\boldsymbol{P}_3)$]. Pertanto esiste $k \in U$ tale che $k+1 \notin U$. Poiché $k \in U$, allora $k \leq t,\ \forall\, t \in T$. Si verifica subito che $k \in T$ [altrimenti, se $k \notin T$, allora $k < t,\ \forall\, t \in T$ e dunque $k+1 \leq t,\ \forall\, t \in T$, da cui $k+1 \in U$: assurdo]. Allora k è il minimo di T: assurdo, per l'ipotesi fatta su T.

$(\boldsymbol{BO}) \implies (\boldsymbol{P}'_3)$. Preso un insieme $V \subseteq \boldsymbol{N}$ verificante le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b'})$ di $(\boldsymbol{P}'_3)$, bisogna provare che $V = \boldsymbol{N}$. Per assurdo, sia $V \subset \boldsymbol{N}$ e sia $T = \boldsymbol{N} - V$ (non vuoto). Per l'assioma $(\boldsymbol{BO})$, T ha il minimo, diciamo t_0. Poiché $0 \in V$, allora $t_0 \neq 0$ [e dunque $t_0 - 1 \in \boldsymbol{N}$]. L'insieme $\{0, 1, \ldots, t_0 - 1\}$ è contenuto in V [perché t_0 è il minimo di T] e, poiché V verifica $(\boldsymbol{b'})$, allora $t_0 \in V$: assurdo.

Osservazione 4. Una semplice conseguenza del principio del buon ordinamento è la dimostrazione del seguente "ovvio" risultato [peraltro già conseguenza del fatto che $\boldsymbol{N}$ è totalmente ordinato]:

$(*)$ $\quad \nexists\, m \in \boldsymbol{N}$ tale che $0 < m < 1$.

Per verificare tale affermazione, assumiamo per assurdo che $\exists\, m \in \boldsymbol{N}$ tale che $0 < m < 1$. Moltiplicando tale diseguaglianza per m si ottiene

$$0 < m^2 < m \quad \text{e quindi} \quad 0 < m^2 < m < 1.$$

Rimoltiplicando per m: $0 < m^3 < m^2 < m < 1$. Iterando tale procedimento:

$$0 < m^k < m^{k-1} < \ \ldots\ < m^3 < m^2 < m < 1.$$

Ma allora l'insieme $T = \{m^k,\ \forall\, k \geq 0\}$ è privo di minimo: assurdo.

Si noti che, ad esempio, la proprietà archimedea di $\boldsymbol{N}$ [cfr. **Prop. 2**(*14*)] può essere dimostrata