Corso di ALGEBRA (M-Z)

2016-17

I NUMERI NATURALI E il TEOREMA DI DIVISIONE IN Z

Definizione dell'insieme dei numeri naturali. Seguendo la più nota delle definizioni dovuta a Giuseppe Peano (1858-1932), l'insieme dei numeri naturali **N** è definito dalle seguenti proprietà:
(N1) esiste una endofunzione σ di **N** iniettiva,
(N2) esiste un elemento $0 \notin \mathrm{Im}\sigma$.
(N3) (Principio di induzione). Ogni sottoinsieme U di **N** tale che :

$$0 \in U$$

$$\text{se } n \in U \text{ allora } \sigma(n) \in U$$

è necessariamente uguale a **N**.

La funzione σ si dice *successore* e l'esistenza di questa endofunzione, iniettiva ma non suriettiva, comporta che **N** è infinito (un insieme si dice *finito* se ogni endofunzione iniettiva è anche suriettiva).
Attraverso il principio di induzione è possibile definire le *iterazioni* di una endofunzione

$$f : A \to A$$

ponendo:

$$f^0 = \mathrm{id}_A : A \to A \text{ , dove } \mathrm{id}_A \text{ è la } \textit{funzione identità} \text{ (per ogni } a \in A : \mathrm{id}_A(a) = a);$$

$$f^n = f \circ f^{\sigma(n)}, \text{ per ogni } n \in \mathbf{N}.$$

Infatti indicato con D l'insieme dei numeri naturali n per cui f^n è definita, risulta $0 \in D$, se $n \in D$ allora $\sigma(n) \in D$ e quindi necessariamente D =**N**.
Analogamente una successione $\{h(n)\}_{n\in\mathbf{N}}$ è *definita per ricorsione* se è definito il suo valore in 0 e per ogni n il valore $h(\sigma(n))$ in funzione di $h(n)$.
Si dimostra facilmente, sempre per induzione, che

a) $\mathrm{Im}\sigma = \mathbf{N}-\{0\}$,
b) per ogni $n \in \mathbf{N}$: $\sigma^n(0) = n$,
c) per ogni $n \in \mathbf{N}$: 0 non appartiene a $\mathrm{Im}\,\sigma^n$.

Le proprietà N1,N2,N3 permettono di definire sull'insieme dei numeri naturali **N** l'operazione di addizione, quella di prodotto e la relazione d'ordine naturale.

L'addizione è definita da: $m+n = \sigma^n(m)$, mentre il prodotto è definito da $m\cdot n = (\sigma^m)^n(0)$, per ogni $m,n \in \mathbf{N}$.

Le strutture algebriche (**N, +)** e (**N**-{0}**,·)** sono monoidi commutativi (ossia le operazioni sono associative e hanno una unità, rispettivamente 0 e $\sigma(0)=1$). Inoltre l'addizione verifica la legge di cancellazione:

$$m+k = n+k \text{ implica } m = n,$$

vale la proprietà distributiva:

$$m(n+k) = mn+mk$$

e la legge di annullamento del prodotto:

$$mn = 0 \text{ se e solo se } m = 0 \text{ oppure } n = 0$$

L'ordine naturale su **N** è definito da :

$$m \leq n \text{ se e solo se esiste } x \text{ in N tale che } m+x = n$$

e le operazioni risultano *isotoniche*, ossia

$$\text{se } m \leq n \text{ allora } m+k \leq n+k \text{ e } mk \leq nk$$

Inoltre rispetto all'ordine naturale, **N** è un insieme ben ordinato, ossia:

Principio del buon ordinamento. N con la relazione d'ordine naturale è totalmente ordinato e ogni suo sottoinsieme non vuoto ha un primo elemento.

Dim. Per assurdo, sia V un sottoinsieme non vuoto senza primo elemento.
Sia P(n) il seguente enunciato:

$$P(n) : \text{“Per ogni } v \in V \text{ , risulta } n \leq v\text{”}$$

Risulta P(0) vera. Supposta vera P(n), è vera anche P(n+1). Infatti se per ogni $v \in V$ si ha $n \leq v$, allora n è distinto da v altrimenti n sarebbe il primo elemento di V. Quindi per ogni $v \in V$ esiste x tale che $n+x = v$ con $x \neq 0$, da cui $x = \sigma(y) = y+1$ e dunque $n+1+x = v$, ossia $(n+1) \leq v$.
Pertanto si è dimostrato per induzione che P(n) è vera per ogni naturale n, ma ciò è assurdo poiché si avrebbe per ogni $v \in V$ $(n+1) \leq v$ e se $n \in V$ anche $(n+1) \leq n$.

□

Questo principio è equivalente al principio di induzione e può essere usato per dimostrare il

Teorema di divisione in Z. Dati $a,n \in \mathbf{Z}$ e $n > 0$, esiste una sola coppia $(q, r) \in \mathbf{Z} \times \mathbf{Z}$ tale che:

i) $b = qa+r$
ii) $0 \leq r < a$

Dim. Sia M = $\{m \in \mathbf{N} : m = a-nq,\ q \in \mathbf{Z}\}$, M è non vuoto poiché se $a \geq 0$ allora $a \in M$, mentre se $a<0$ allora $a-na \in M$. Pertanto M ha un primo elemento r con $a = qn+r$. Si supponga per assurdo $n \leq r$. In tal caso dovrebbe esistere x tale che $n+x = r$ da cui $a = qn+n+x$, ossia $x \in M$ con $x \leq r$. Ma r è il più piccolo elemento di M, dunque $x = r$ e quindi da $n+x = r$ dovrebbe essere $n = 0$ contro l'ipotesi del teorema. Sia $a = q'n+r'$ con $0 \leq r' < a$, allora $r' \in M$ e dunque $r \leq r'$ ossia $r' = r + x$. Si ha: $a = qn+r = q'n + r + x$, da cui $x = kn$. Pertanto essendo $kn = x \leq r' < n$, si ha $x = 0$ e quindi $r = r'$ e $q = q'$.

□

Per una trattazione approfondita dei temi precedenti consultare: Mac Lane S., Birhoff G.: *Algebra*. Mursia (1985).
.

□