

Insiemi numerici : da $\mathbb{N}$ ad $\mathbb{R}$

Def. I numeri naturali sono una terna $(\mathbb{N}, 0, s)$ dove

- $\mathbb{N}$ è un insieme,
- $0 \in \mathbb{N}$,
- $s: \mathbb{N} \rightarrow \mathbb{N}$ (brutalmente: è il successivo)

Le proprietà di s sono le seguenti (ASSIOMI DI PEANO)

(i) s è iniettiva

(ii) l'immagine di s è $\mathbb{N} \setminus \{0\}$, cioè per ogni $n \in \mathbb{N}$ con $n \neq 0$ esiste $m \in \mathbb{N}$ t.c. $s(m) = n$ (m è unico)

(iii) se un sottoinsieme $A \subseteq \mathbb{N}$ verifica

- $0 \in A$
- $\forall m \in \mathbb{N} [m \in A \Rightarrow s(m) \in A]$

allora per forza $A = \mathbb{N}$.

Oss. L'assioma 3 è il principio di induzione (quello classico deriva prendendo come A l'insieme degli $m \in \mathbb{N}$ per cui un certo predicato P_m è vero)

Teorema Esiste un' unica terna $(\mathbb{N}, 0, s)$ con le proprietà date.

Oss. L'unicità si intende a meno di isomorfismi, cioè se $(\boxed{\mathbb{N}}, \boxed{0}, \boxed{s})$ è un'altra terna, allora esiste un' unica funzione bigettiva

$$\varphi: \mathbb{N} \rightarrow \boxed{\mathbb{N}}$$

tale che

$$\varphi(0) = \boxed{0}$$

$$\varphi(s(m)) = \boxed{s}(\varphi(m)) \quad \forall m \in \mathbb{N}$$

Dim. teorema

Esistenza : deve derivare da un opportuno assioma misterioso della teoria degli insiemi

Unicità : date due forme come sopra, basta definire $\varphi: \mathbb{N} \rightarrow \boxed{\mathbb{N}}$ ponendo

$$\varphi(0) = \boxed{0}$$

ogni altro $n \in \mathbb{N}$ (diverso da 0) lo posso scrivere come $n = S(m)$ e a quel punto pongo

$$\varphi(n) = \boxed{S}(\varphi(m)) \quad \forall n \neq 0$$

Si verifica facilmente che φ è iniettiva e surgettiva e che commuta con la struttura.

$$\text{---} \circ \text{---} \circ \text{---}$$

Operazioni in $\mathbb{N}$

Somma . Voglio definire $a+b$ con a, b in $\mathbb{N}$.

Si pone

- $a+0 = a$ per ogni $a \in \mathbb{N}$
- $a+S(m) = S(a+m)$ per ogni $m \in \mathbb{N}$

(se $b=0$ è definita dalla 1ª, se $b \neq 0$ allora $b=S(m)$ per un qualche m , e allora $a+b$ è definita dalla 2ª).

Esercizio Dimostrare che la somma è commutativa e associativa.

(hiut! è una pena)

Prodotto voglio definire $a \cdot b$. Come sopra

- se $b=0$, allora pongo $a \cdot 0 = 0$
- se $b \neq 0$, allora $b=S(m)$ e pongo $a \cdot b = a \cdot S(m) = a \cdot m + a$

Stesso esercizio di sopra : commutativa e associativa
— o — o —

Definizione di $\mathbb{Z}$ Brutalmente $\mathbb{Z} \ni z = \underbrace{m}_{\in \mathbb{N}} - \underbrace{n}_{\in \mathbb{N}}$

Ufficialmente: prendo $\mathbb{N}^2$ e definisco una relazione di equivalenza ponendo

$$(m_1, n_1) \sim (m_2, n_2) \quad \text{se} \quad m_1 + n_2 = m_2 + n_1$$
$$(u_1 - n_1 = m_2 - n_2)$$

Esercizio : si tratta di una rel. di equiv.

Operazioni in $\mathbb{Z}$: $(u_1, n_1) \underset{\mathbb{Z}}{+} (u_2, n_2) = (u_1 + u_2, n_1 + n_2)$

$$u_1 - n_1 + u_2 - n_2 = (u_1 + u_2) - (n_1 + n_2)$$

$$(u_1, n_1) \underset{\mathbb{Z}}{\cdot} (u_2, n_2) = (u_1 \cdot u_2 + u_1 \cdot n_2 + u_2 \cdot n_1, n_1 \cdot n_2 + n_2 \cdot n_1)$$

Esercizio : dimostrare che passano al quoziente

Esercizio : verificare le proprietà di anello di $\mathbb{Z}$
— o — o —

Definizione di $\mathbb{Q}$ Moralmemente : $\mathbb{Q} \ni q = \frac{m}{n}$ con $n \neq 0$

Prendo $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ e definisco la relazione di equiv.

$$(m_1, n_1) \sim (m_2, n_2) \quad \text{se} \quad m_1 \cdot \underbrace{n_2}_{\in \mathbb{Z}} = m_2 \cdot \underbrace{n_1}_{\in \mathbb{Z}}$$

Esercizi : $\rightarrow$ dim. che è relas. di equiv.
 $\rightarrow$ definire le operazioni
 $\rightarrow$ dimostrare che è un campo.

— o — o —

Costruzione di $\mathbb{R}$ La cosa più comoda è la def. assiomatica.
Poi però bisogna dim. esistenza ed unicità

Esistenza: via sezioni di DEDERIND (DEDERIND CUTS)

Un numero reale è una partizione dei razionali in due sottoinsiemi A e B tali che

- $A \cup B = \mathbb{Q}$ e $A \cap B = \emptyset$
- $A \neq \emptyset$ e $B \neq \emptyset$
- $a \leq b$ per ogni $a \in A$ e ogni $b \in B$
- $\forall a \in A$ esiste $\hat{a} \in A$ tale che $a < \hat{a}$ (è come dire che A non ha max)

Oss. Dato A è automatico che è B , quindi parlare di sezioni di Dedekind è equivalente a parlare di semirette sx in $\mathbb{Q}$ aperte

Pensando in termini di semirette (cioè guardando solo A)

- la somma si definisce bene facendo $A_1 + A_2$
- il prodotto è una pena per via dei segni
- l'ordine è banale (è un confronto tra semirette)
- l'assioma di continuità si riduce a fare l'unione di semirette.

— o — o —

A partire dagli assiomi dei numeri reali, si può dimostrare che $\mathbb{R}$ contiene $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$, cioè esistono applicazioni injettive

$$i: \mathbb{N} \rightarrow \mathbb{R}$$

$$i: \mathbb{Z} \rightarrow \mathbb{R}$$

$$i: \mathbb{Q} \rightarrow \mathbb{R}$$

che preservano la struttura algebrica e di ordinamento.

Come si dimostra l'unicità di $\mathbb{R}$

→ si definisce l'isomorfismo nell'immagine di $\mathbb{N}$

→ $\mathbb{Z}$

→ $\mathbb{Q}$

→ si passa a tutti i reali con il sup, perché ogni reale è il sup di una semiretta di razionali.

— o — o —