

Lezione del 8/10/2024

MEPVS

Dedekind

$(\mathbb{N}, +)$ L'operazione su un insieme A è una funzione

$$A \times A \rightarrow A$$

↳ l'insieme di tutte le coppie di elementi di A .

A una coppia di elementi di A associamo un altro elemento di A .

"Somma" è una funzione che alla coppia di numeri naturali $(2, 3)$ associa il numero 5

La somma in \mathbb{N} la definiremo per ricorrenza

$$\forall (m, n) \in \mathbb{N}, m + 0 = m; m + S(n) = S(m + n)$$

ES. $m + 0 = m$; $m + 1 = S(m)$, $m + 2 = S(m + 1) = S(S(m))$

Es.

$$3+3 = S(S(S(3))) = 6$$

$$m+n = S(S \dots S(m))$$

Applico a m la funzione S tante volte quante ce ne vogliono per ottenere n a partire da 0.

La definizione per ricorrenza è una buona definizione?

La definizione data definisce in modo univoco l'operazione di somma per tutte le coppie di numeri naturali?

Created with Doceri



TEOREMA di Dedekind (1888) di Ricorrenza o
Ricostruzione

Sia A un insieme, sia $a \in A$ un suo elemento; sia
 $g: A \rightarrow A$. Allora esiste una funzione $f: \mathbb{N} \rightarrow A$
 tale che $f(0) = a$ e $f \circ s = g \circ f$
 \uparrow
 funzione successore

Dimostrazione: Supponiamo che esistano 2 funzioni $f_1 \neq f_2$
 tali che per induzione su n che $f_1(n) = f_2(n) \forall n$

Sia $f_1(0) = f_2(0)$ (primo passo induttivo)

Supponiamo che valga $f_1(n) = f_2(n)$ e vediamo se
 vale anche

$$f_1(n+1) = f_2(n+1)$$

Created with Doceri



Lequede le ipotesi sulle funzioni saranno

$$f_1(S(n)) = g(f_1(n)) = g(f_2(n)) = f_2(S(n)).$$


Dimostrare l'esistenza. Considero i sottoinsiemi
 $H \subseteq \mathbb{N} \times A$ t.c.

1) $(0, a) \in H$

2) $\forall m, b$ se $(m, b) \in H$, allora $(S(m), g(b)) \in H$.

$\mathbb{N} \times A$ soddisfa sia la 1) che la 2) \Rightarrow esistono degli H e tutti contengono $(0, a)$.

Se interseco gli H otterrò un insieme D che contiene ancora $(0, a)$ e soddisfa la 1) e la 2) sarà cioè il piccolo insieme con tali proprietà.

Usa D per definire f e, a tal fine, dimostreremo che
 $\forall n \in \mathbb{N} \exists! b \in A$ t.c. $(n, b) \in D$ 

* la dimostrazione per induzione su m .

Per $m=0$ $(0, a) \in D$ e nessun $c \neq a$ sta in D
perché?

Se così fosse $D - (0, c)$ avrebbe le proprietà 1) e 2)
ma sarebbe più piccolo di D , il che è impossibile.

Quindi, se $m=0$ l'unica coppia $(m, b) \in D$ è (m, a)

Supponiamo che $\forall 0, 1, 2, \dots, m$ valga la proprietà *
e vediamo che vale per $S(m)$

Se c'è un solo b t.c. $(m, b) \in D$ e per la proprietà 2)

$(S(m), g(b)) \in D$. Se esistesse un $c \neq g(b)$ t.c.

$(S(m), c) \in D$ allora come nel caso di $m=0$ si può
considerare $D - (S(m), c)$ e verrebbero ancora le 1) e
le 2). Il che però è assurdo.

Created with Doceri



Se la $*$ è dimostrata e per definizione

$$f: \mathbb{N} \rightarrow A \quad \forall m \in \mathbb{N}$$

t.c. $f(m) = b$ con b unico elemento per cui $(m, b) \in D$

Per la proprietà 1) $f(0) = a$ per la 2) si ha

$$f(S(m)) = g(f(m))$$

ovvero

$$f \circ S = g \circ f \quad \text{Q.E.D.}$$

Created with Doceri



Andiamo a definire in \mathbb{N} la nozione di ordine

$\forall m, n \in \mathbb{N}$, diremo che m è maggiore o uguale a n ($m \geq n$) se $\exists t \in \mathbb{N} \neq \emptyset$
 $m = n + t$

Relazione d'ordine

Proprietà della relazione d'ordine

Intuitiva

1) $\forall m, n \in \mathbb{N}$, se $m \geq n$ e $n \geq m \Rightarrow m = n$

2) $\forall m, n \in \mathbb{N}$, se $m \geq n$ e $n \geq s \Rightarrow m \geq s$
 transitiva

3) $\forall n \in \mathbb{N}$, $n \geq n$ riflessiva

4) $\forall m, n \in \mathbb{N}$ o $m \geq n$ o $n \geq m$ → due elementi sono sempre comparabili

5) $\forall m \in \mathbb{N}$ $m \geq 0$ → 0 è il primo elemento di \mathbb{N}

Created with Doceri



Nuova formulazione del 1° postulato di Peano:

"Ogni sottoinsieme non vuoto di \mathbb{N} contiene un minimo elemento"

Principio del buon ordinamento

Dimostrazione:

$$\forall n \in \mathbb{N} \exists! b \in A \text{ t.c. } (n, b) \in D \quad *$$

Se vale * sia $A \subseteq \mathbb{N}$ t.c. $0 \in A$ e se $m \in A$ allora $s(m) \in A$.

Considero un $A' = \mathbb{N} - A$, per dimostrare il principio di induzione dobbiamo vedere che $A' = \emptyset$.

Per assurdo sia

$A' \neq \emptyset$, allora per la * esiste un minimo elemento $m \in A'$, $m \neq 0$ perché $0 \in A$.

Created with Doceri



Considero allora $m' \text{ f.c. } m = S(m')$ e $m' \in A$
 ma per ipotesi se A contiene un numero contiene
 anche il suo successore e dunque $m \in A$ è assurdo.

Se invece assumiamo che valga il principio di induzione
 considero $A \subseteq \mathbb{N}$ che non abbia un elemento minimo
 e mostriamo che $A \neq \emptyset$. Mostriamo che nessun
 $n \in \mathbb{N}$ sta in A , per induzione su n .

Se $n=0$ ovviamente non sta in A altrimenti sarebbe
 il minimo di A , quindi $0 \in \mathbb{N} - A$. Se ora $n \in \mathbb{N} - A$
 allora anche $S(n) \in \mathbb{N} - A$ perché altrimenti sarebbe
 $S(n) \in A$ ma A non potrebbe avere elementi minori di A .
 Quindi, per il principio di induzione $\mathbb{N} - A = \mathbb{N}$
 e $A = \emptyset$.

Created with Doceri



TEOREMA di UNICITÀ di \mathbb{N}

Sia $(\mathbb{N}', 0, s')$ è un' altra legge che soddisfa gli assiomi di Peano. Allora

\mathbb{N} e \mathbb{N}' sono isomorfi, cioè esiste un'unica biiezione

$$f: \mathbb{N} \rightarrow \mathbb{N}' \text{ t.c. } f(0) = 0' \text{ e } f \circ s = s' \circ f$$

Per la dimostrazione basta ripetere 2 volte il lemma di ricorrenza.

Created with Doceri



Le operazioni su \mathbb{N}

L'operazione di somma gode delle seguenti proprietà:

$$S_1) \forall m, n, t \in \mathbb{N}, m + (n + t) = (m + n) + t \quad \underline{\text{associativa}}$$

$$S_2) \forall m \in \mathbb{N}, 0 + m = m + 0 = m \quad \text{essendo } \underline{\text{0 l'elemento neutro}}$$

$$S_3) \forall m, n \in \mathbb{N}, m + n = n + m \quad \underline{\text{commutativa}}$$

S_1 e S_2 le deduco per buone e direzionando la S_3

Per induzione su n .

Se $n = 0$ la S_3 si riduce alla S_2 !

Se $n = 1$ $1 + m = m + 1$ per induzione su m . Per $m = 0$ otteniamo la S_2 se è vero per m anziché per $m + 1$

$$1 + S(m) = 1 + (m + 1) = (1 + m) + 1 = S(m) + 1$$

Supponiamo che $m+n = m+n$ e vediamo che
 $S(m) + m = m + S(m)$.

Avremo che $m + S(n) = S(m+n) = S(n+m) =$
 $= m + S(m) = m + (m+1) = m + (1+m) =$
 $(m+1) + m = S(m) + m. \quad \text{Q.E.D.}$

Una ulteriore proprietà legge moltiplicazione e somma
 $S(m)$ $\forall n, m, t \in \mathbb{N}, n \times (m+t) = (n \times m) + (n \times t)$

propz. distributiva del prodotto rispetto
 alla somma

Created with Doceri



Divisibilità

Un numero naturale a si dice divisibile per un numero naturale b se esiste un naturale c tale che $a = b \cdot c$.
Si dice allora che b è un divisore di a e scrivere $b|a$.

ES.1 Dimostrare che la somma di 5 numeri naturali consecutivi è sempre divisibile per 5.

$$a, a+1, a+2, a+3, a+4$$

$$\begin{aligned} a + (a+1) + (a+2) + (a+3) + (a+4) &= 5a + 10 \\ &= 5(a+2) \end{aligned}$$

Created with Doceri



ES. 2

Dati 3 numeri naturali non nulli tali che la differenza tra il terzo e il secondo sia 2 e che tra il secondo e il primo sia 2.
 dimostrare che uno di essi è divisibile per 3.

Siano $m, m+2, m+4, m \neq 0$

$a \equiv b \pmod{m}$ m divide $b-a$

$m \equiv 0 \pmod{3}$ la tesi è immediata

$m \equiv 1 \pmod{3}$ allora $m+2 \equiv 0 \pmod{3}$

$m \equiv 2 \pmod{3}$ allora $m+4 \equiv 0 \pmod{3}$

Alternanti per induzione.

Created with Doceri



ES. 2

Per alcuni naturali non nulli m, n è possibile che n sia divisore di m e contemporaneamente m sia divisore di n : ciò accade se e solo se $m = n$.

In fatti, se n è divisore di m e m è divisore di n si ha

$$m = b \cdot n \quad \text{e} \quad m = a \cdot n$$

$$a, b \in \mathbb{N}, \quad a \neq 0, \quad b \neq 0.$$

$$\text{Allora} \quad m \cdot m = (a \cdot n) \cdot (b \cdot n) = ab \cdot m \cdot m \Rightarrow \boxed{ab = 1}$$

Così si ha $ab = 1$ nel caso $a = b = 1$

Non può che essere $m = n$.

Created with Doceri



Definizione: Il numero naturale p si dice primo se è maggiore di 1 ed è divisibile soltanto per 1 e per se stesso. Un numero naturale maggiore di 1 non primo si dice composto.

CRIVELLO DI ERATOSTENE

Created with Doceri



Proposizione: Unicità della scomposizione in fattori
" primi.
" La scomposizione in fattori primi è unica. A parte
permutazioni di fattori, un naturale può essere espresso
come prodotto di primi in un solo modo".

Dimostrazione (Lindemann)

Chiusavano numeri enormi: i numeri che possono essere
fattorizzati in prodotti di primi in più modi (a parte
permutazioni).

Created with Doceri

