I ESERCITAZIONE DI AM1B

In questa lezione si vogliono introdurre assiomaticamente i numeri naturali, si presenteranno varie forme del principio di induzione ed infine si vedranno alcune applicazioni di tale principio. Nell' appendice c'e una breve descrizione dei naturali a partire dai reali.

1. Assiomi di Peano

Sia $\mathbb{N} = \{1, 2, 3, ...\}$. Attraverso i seguenti postulati noti come assiomi di Peano daremo una definizione che prescinde dalla natura degli elementi di $\mathbb{N}$.

Definizione 1.1. L'insieme dei numeri naturali è costituito da una terna $(\mathbb{N}, \sigma, 1)$ dove $\mathbb{N}$ è insieme, σ è una funzione da $\mathbb{N}$ in $\mathbb{N}$ e 1 è un elemento di $\mathbb{N}$ tali che

$\mathbb{N}_1$) σ è iniettiva
$\mathbb{N}_2$) $1 \notin \operatorname{Im}\sigma$
$\mathbb{N}_3$) ogni sottoinsieme U di $\mathbb{N}$ tale che
 a) $1 \in U$
 b) $k \in U \Rightarrow \sigma(k) \in U$
coincide con tutto $\mathbb{N}$

Osservazione 1.2. L'immagine di σ è $\mathbb{N} \setminus \{1\}$. Infatti l'insieme $\operatorname{Im}(\sigma) \cup \{1\}$ soddisfa ovviamente $\mathbb{N}_3$ sicché coincide con $\mathbb{N}$. D'altra parte $1 \notin \operatorname{Im}(\sigma)$ per $\mathbb{N}_2$.

L'assioma $\mathbb{N}_3$ viene detto *Principio di induzione*.

L'esistenza di una terna che soddisfi tali assiomi è un postulato (cioè si deve accettare senza dimostrazione). In realtà ne esiste essenzialmente una sola.

Proposizione 1.3. *Se esistono due terne $(\mathbb{A}, \sigma, 1)$ e $(\mathbb{A}', \sigma', 1')$ che soddisfano gli assiomi di Peano allora esse sono sostanzialmente identiche. Cioè esiste un' applicazione biunivoca $\varphi : \mathbb{A} \longrightarrow \mathbb{A}'$ tale che*

$$\begin{cases} \varphi(1) = 1' \\ \varphi(\sigma(a)) = \sigma'(\varphi(a)) \end{cases} \tag{1}$$

Dimostrazione. Proviamo che φ definita in (1) è definito su tutto $\mathbb{A}$. Sia S l'insieme dove è definita φ. Allora $1 \in S$ per definizione. Inoltre supponiamo di aver definito $\varphi(a)$. Allora da (1) segue che $\varphi(\sigma(a)) = \sigma'(\varphi(a))$ che è un elemento di $\mathbb{A}'$ e quindi $a + 1 \in S$. Sicché per il principio di induzione valido per $\mathbb{A}$ si ha che $S = \mathbb{A}$ equindi φ è definita su tutto $\mathbb{A}$.

Proviamo ora che φ è biunivoca.

- Suriettività Sia $S' = \operatorname{Im}\varphi$. Allora $1' \in S'$. Inoltre se $a' \in S'$ allora $a' = \varphi(a)$ per qualche $a \in \mathbb{A}$. Sicché
$$\sigma'(a') = \sigma'(\varphi(a)) = \varphi(\sigma(a))$$
e quindi $\sigma'(a') \in S'$ e percio per $\mathbb{A}'_3$ si ha che $S' = \mathbb{A}'$.

- Iniettività Sia $S = \{a \in \mathbb{A} | \varphi(b) = \varphi(a) \Rightarrow a = b\}$.

  Supponiamo per assurdo che $1 \notin S$. Allora esiste $b \neq 1$ tale che $\varphi(b) = \varphi(1) = 1'$. Per 2.3 si ha che $b = \sigma(c)$ per qualche $c \in \mathbb{A}$. Quindi
  $$1' = \varphi(\sigma(c)) = \sigma'(\varphi(c))$$
  ma ciò contraddice $\mathbb{A}'_2$.

  Supponiamo ora che $a \in S$ e proviamo che $\sigma(a) \in S$. Sia $b \in \mathbb{A}$ tale che $\varphi(\sigma(a)) = \varphi(b)$. Allora, per definizione di φ, $\sigma'(\varphi(a)) = \varphi(b)$. Sicché $\varphi(b) \in \operatorname{Im}\sigma'$ ma allora, per 2.3, $\varphi(b) \neq 1'$. Quindi $b \neq 1$ perché $1 \in S$. Perciò, sempre per 2.3, $b = \sigma(c)$ per qualche $c \in \mathbb{A}$. Perciò
  $$\sigma'(\varphi(a)) = \varphi(\sigma(c)) = \sigma'(\varphi(c))$$
  che per l'iniettività di σ' dà luogo a
  $$\varphi(a) = \varphi(c)$$
  Poiché $a \in S$ allora $c = a$ e quindi $\sigma(a) = \sigma(c) = b$.

  Perciò per $\mathbb{A}_3$ si ha $S = \mathbb{N}$ e quindi φ è iniettiva.

□

Quindi si puo dire che gli assiomi di Peano caratterizzano i numeri naturali. Quello che si deve postulare (cioè accettare senza dimostrazione) è l'esistenza di un insieme che soddisfa tali assiomi. L'intero edificio matematico si basa sull'accettazione dell'esistenza dei numeri naturali. A tal proposito Kronecher pronunciò la famosa frase: *Dio creò i numeri naturali, tutto il resto è opera dell'uomo.*

Per ogni $n \in \mathbb{N}$ $\sigma(n)$ si dice successivo. Costruiamo ora delle operazioni (binarie) su $\mathbb{N}$, cioè delle funzioni da $\mathbb{N} \times \mathbb{N}$ in $\mathbb{N}$.

Somma

Definiamo la somma $s : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$; anziché scrivere $s(m, n)$ scriveremo $m + n$. Per ogni $m \in \mathbb{N}$ poniamo
$$\begin{cases} m + 1 := \sigma(m), \\ m + \sigma(n) := \sigma(m + n) \end{cases}$$
Occorre verificare che tale operazione è definita su tutto $\mathbb{N} \times \mathbb{N}$. Fissiamo $m \in \mathbb{N}$ e proviamo che $m + n$ è definito ogni n. Sia $S = \{n \in \mathbb{N} \text{ tale che } n + m \text{ è definito}\}$. Proviamo che $S = \mathbb{N}$. Per definizione $m + 1 = \sigma(m)$ e quindi $1 \in S$. Supponiamo ora che $n \in S$, supponiamo, cioè, di aver definito $n + m$. Allora proviamo che $\sigma(n) \in S$. Cioè occorre definire che $m + \sigma(n)$. Ma quest'ultimo è, per definizione, $\sigma(m + n)$ che è ben definito in quanto lo è σ. Quindi per $\mathbb{N}_3$ si ha che $S = \mathbb{N}$ e quindi $m + n$ è definito per ogni $n \in \mathbb{N}$. Poiché m è un elemento qualsiasi abbiamo che $m + n$ è ben definita su tutto $\mathbb{N} \times \mathbb{N}$.

La somma verifica le seguenti proprietà

- Associatività. Cioè si ha $(n + m) + k = n + (m + k)$ per ogni $n, m, k \in \mathbb{N}$. Fissati n, m si definisca $S = \{k \in \mathbb{N} | (n + m) + k = n + (m + k)\}$. E' facile vedere che S soddisfa le ipotesi di $\mathbb{N}_3$ e quindi $S = \mathbb{N}$. Facendo variare n, m si ha la tesi.

- Commutatività. Occorre provare che $n+m = m+n$ per ogni $n, m \in \mathbb{N}$. Definiamo $S = \{m \in \mathbb{N} | m + n = n + m \quad \forall n \in \mathbb{N}\}$.

$1 \in S$. Utilizziamo di nuovo l'induzione. Sia $T = \{k \in \ N | k + 1 = 1 + k\}$. Ovviamente $1 \in T$. D'altra parte sia $m \in T$ allora

$$\begin{aligned} \sigma(m) + 1 =& (m+1) + 1 && \text{per definizione di somma} \\ =& (1+m) + 1 && \text{perché } m \in T \\ =& 1 + (m+1) && \text{per associtività della somma} \\ =& 1 + \sigma(m) && \text{per definizione somma} \end{aligned}$$

Se $m \in S$ allora $\sigma(m) \in S$. Infatti per ogni $n \in \mathbb{N}$

$$\begin{aligned} \sigma(m) + n =& (m+1) + n && \text{per definizione di somma} \\ =& m + (1+n) && \text{per associatività} \\ =& m + (n+1) && \text{perché } 1 \in S \\ =& m + \sigma(n) && \text{per definizione di somma} \end{aligned}$$

Quindi, per $\mathbb{N}_3$, $S = \mathbb{N}$.

Prodotto Si definisca il prodotto $p : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. Anziché scrivere $p(m, n)$ scriveremo $m \cdot n$.

Per ogni $m \in \mathbb{N}$ definiamo

$$\begin{cases} m \cdot 1 = m \\ m \cdot \sigma(n) = m \cdot n + m \end{cases}.$$

In modo simile a quanto fatto per la somma si prova che il prodotto è definito su tutto $\mathbb{N} \times \mathbb{N}$.

Inoltre si può provare che il prodotto è commutativo, associativo e che vale la proprietà distributiva, cioè

$$m \cdot (n + k) = m \cdot k + n \cdot k \qquad \text{per ogni } n \in \mathbb{N}$$

Relazione d'ordine Introduciamo su $\mathbb{N}$ una relazione d'ordine nel seguente modo

$$n \leq m \text{ se esiste } k \in \mathbb{N} \text{ tale che } n = m + k$$

e k lo indichiamo con $m - n$. (k se esiste è unico perché σ è iniettiva).

Osservazione 1.4. In molti testi i numeri naturali sono definiti includendovi lo 0. La differenza è puramente formale e non è difficile apportare modificare per passare dalle nostre definizioni alle altre.

2. Principio di induzione e formulazioni equivalenti

D'ora in poi al posto di $\sigma(n)$ scriveremo $n + 1$.

Diamo ora alcune forme equivalenti di tale principio e poi proveremo la loro equivalenza.

$\mathbb{I}$ (Forma forte del principio di induzione) Ogni sottoinsieme $V \subseteq \mathbb{N}$ tale che
  a) $1 \in V$
  b) $n \in V$ ogniqualvolta $k \in V$ per $1 \leq k < n$
  coincide con $\mathbb{N}$.

$\mathbb{P}$ Sia $\mathcal{P}(n)$ un predicato definito per ogni $n \in \mathbb{N}$, che verifica le seguenti proprietà
  a) $\mathcal{P}(1)$ è vero
  b) $\mathcal{P}(n)$ vero $\Rightarrow \mathcal{P}(n+1)$ vero
  Allora $\mathcal{P}(n)$ è vero per ogni $n \in \mathbb{N}$.

$\mathbb{M}$ (Principio del minimo) Ogni insieme non vuoto $S \subseteq \mathbb{N}$ ammette minimo.

Proposizione 2.1. *Le asserzioni* $\mathbb{N}_3$, $\mathbb{P}$, $\mathbb{M}$, $\mathbb{I}$ *sono equivalenti.*

Dimostrazione. $\mathbb{N}_3 \Rightarrow \mathbb{P}$. Sia $\mathcal{P}$ una proposizione che verifica le ipotesi di $\mathbb{P}$. Ciò equivale a dire che $V = \{n \in \mathbb{N}$ tale che $\mathcal{P}(n)$ è vera$\}$ soddisfa le ipotesi di $\mathbb{N}_3$. Sicché $V = \mathbb{N}$ e cioè $\mathcal{P}(n)$ è vera per ogni $n \in \mathbb{N}$.

$\mathbb{P} \Rightarrow \mathbb{M}$. Supponiamo per assurdo esista un sottinsieme $S \subseteq \mathbb{N}$ non vuoto che non ammette minimo. Sia $\mathcal{P}(n) ='' k \notin S$ per ogni $k \leq n''$. Allora $\mathcal{P}(1)$ è vera, altrimenti 1 sarebbe il minimo di S. Inoltre se $P(n)$ è vera allora $P(n+1)$ è vera, altrimenti $n+1$ sarebbe il minimo di S. Sicché, poiché abbiamo supposto valga $\mathbb{P}$, si ha che $\mathcal{P}(n)$ è vera per ogni n e cioè $S = \emptyset$ in contraddizione con le ipotesi che avevamo fatto su S.

$\mathbb{M} \Rightarrow \mathbb{I}$. Sia V un insieme che soddisfa le ipotesi di $\mathbb{I}$. Vogliamo mostrare che $V = \mathbb{N}$. Sia S il complementare di V in $\mathbb{N}$. Supponiamo per assurdo che S non sia l'insieme vuoto. Allora se vale $\mathbb{M}$ segue che S ammette minimo. Sia esso n_0. Allora si ha che $k \in V$ per ogni $1 \leq k < n_0$. Poiché V soddisfa le ipotesi di $\mathbb{I}$ allora $n_0 \in V$ in contraddizione il fatto che $s_0 \in S$. Quindi si ha $S = \emptyset$.

$\mathbb{I} \Rightarrow \mathbb{N}_3$. Ovvio in quanto se un insieme verifica le ipotei di $\mathbb{N}_3$ allora chiaramente verifica anche quelle di $\mathbb{I}$. □

Applicazioni del principio di induzione

In seguito applicheremo il principio di induzione nella forma $\mathbb{P}$.

Lo schema delle dimostrazioni per induzione è quindi il seguente

- *Base dell'induzione.* Dimostrare che $\mathcal{P}(1)$ è vero.
- *Passo induttivo.*Provare che se supponendo $\mathcal{P}(n)$ vera allora $\mathcal{P}(n+1)$ è vera.

Si conclude che, per il principio di induzione, che $\mathcal{P}(n)$ è vera per ogni n.

Vediamo alcuni esempi.

Esempio 2.2. Per ogni $n \in \mathbb{N}$ per ogni $x \geq -1$, $(x \in \mathbb{R})$ si ha

$$(1+x)^n \geq 1 + nx$$

Base dell'induzione. $\mathcal{P}(1)$ è ovviamente vera

Passo induttivo. Supponiamo sia vera $\mathcal{P}(n)$.

Allora

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n(1+x) \\
&\geq (1+nx)(1+x) && \text{ipotesi induttiva e } x \geq -1 \\
&= 1 + (n+1)x + nx^2 \\
&\geq 1 + (n+1)x && \text{perché } x^2 \geq 0
\end{aligned}$$

Sicché $\mathcal{P}(n+1)$ è vera e quindi per il principio di induzione $\mathcal{P}(n)$ è vera per ogni $n \in \mathbb{N}$.

Osservazione 2.3. L'ipotesi a) di $\mathbb{P}$ si può sostituire con

a') esiste $k \in \mathbb{N}$ tale che $P(k)$è vera

In questo caso si può concludere che $P(n)$ è vera per ogni $n \geq k$. Per vedere ciò basta applicare $\mathbb{P}$ alle proposizioni $\mathcal{Q}(n) = \mathcal{P}(n+k-1)$

Inoltre tenendo conto dell' ipotesi b) di $\mathbb{I}$ si può mostrare che la b) di $\mathbb{P}$ può essere sostituita da

$$\mathcal{P}(k)\text{vero per ogni } 1 \leq k < n \Rightarrow \mathcal{P}(n) \text{ vero}$$

Esempio 2.4. Per ogni $n \geq 6$ si ha

$$2^n n! < n^n$$

Base dell'induzione $\mathcal{P}(6)$ è vera perché

$$2^6 6! = 2^6 3^2 80 < 6^6 = 2^6 3^2 81$$

Passo induttivo Supponiamo sia vera $\mathcal{P}(n)$. Si ha

$$\begin{aligned}
(n+1)^{n+1} =& (n+1)^n (n+1) \\
=& \left(\sum_{k=0}^{n} \binom{n}{k} n^k\right)(n+1) && \text{sviluppo della potenza di un binomio} \\
=& \left(n^n + n(n^{n-1}) + \sum_{k=0}^{n-2} \binom{n}{k} n^k\right)(n+1) \\
>& (2n^n)(n+1) \\
=& 2(2^n n!)(n+1) && \text{per l'ipotesi induttiva} \\
=& 2^{n+1}(n+1)! && \text{per la definizione di fattoriale}
\end{aligned}$$

Sicché la formula è vera per ogni $n \geq 6$. Si osservi che per $n < 6$ è falsa.

Esempio 2.5. Si provi che

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

La prima parte dell'uguaglianza non è nient'altro che la somma dei primi n numeri naturali.

Base dell'induzione Se $n = 1$ si ha

$$1 = \frac{2}{2}$$

che è certamente vero

Passo induttivo Sia vera l'uguaglianza per n. Allora si ha

$$\begin{aligned}
\sum_{k=1}^{n+1} k =& \sum_{k=1}^{n} k + n + 1 \\
=& \frac{n(n+1)}{2} + n + 1 && \text{per ipotesi induttiva} \\
=& \frac{n(n+1) + 2(n+1)}{2} \\
=& \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Esempio 2.6 (Induzione sbagliata)**.** L'induzione è uno strumento molto potente che se non utilizzato con attenzione porta a grossolani errori. Dimostreremo ora che in un qualunque insieme di persone tutti hanno la stessa età.

Base dell'induzione. Se un insieme ha una sola persona ciò è chiaramente vero.

Passo induttivo. Supponiamo quindi che la proposizione sia vera per ogni insieme con al più n persone. Consideriamone uno di $n+1$ persone. Prendiamo due sottinsieme di quest'ultimi: uno formato da n persone ed un altro da 2. Sicché esiste una persona A che appartiene ad entrambi gli insiemi. Per l'ipotesi induttiva si ha che sia le persone del primo insieme che quelle del secondo insieme hanno tutte la stessa età di A. Sicché, applicando il principio induttivo nella forma di 2.3, TUTTI HANNO LA STESSA ETA'. Dove fa acqua il ragionamneto?

3. Appendice

Avete visto nelle precedenti lezioni come a partire da $\mathbb{N}$ con le sue operazioni sia possibile costruire $\mathbb{R}$.

Esiste un approccio inverso. Si potrebbe definire in modo assiomatico $\mathbb{R}$ e poi definire all'interno dei numeri reali l'insieme $\mathbb{N}$. Mostreremo brevemente questo approccio.

Si definisce $\mathbb{R}$ come l'insieme con le seguenti strutture e le seguenti proprietà:

A) un ordinamento totale
B) un'operazione binaria (detta addizione) associativa, commutativa, con un elemento neutro 0 e tale che ogni elemento ha un inverso
C) un operazione binaria (detta moltiplicazione) associativa, commutativa, con un elememento neutro 1 diverso da zero e tale che ogni elemento non nullo ammetta inverso
D) Inoltre valgono

$$a \le b \Rightarrow a + c \le a + c \qquad \text{per ogni } c \in \mathbb{R}$$
$$0 \le a \text{ e } 0 \le b \Rightarrow 0 \le ab$$
$$a(b+c) = ab + bc \qquad \text{per ogni } a, b, c \in \mathbb{R}(\text{ proprietà distributiva })$$

E) Assioma di Dedekind

D'ora in poi la somma è quella ereditata da $\mathbb{R}$.

Definizione 3.1. Un insieme $S \subset \mathbb{R}$ si dice induttivo se verifica

a) $1 \in S$
b) $x \in S \Rightarrow x + 1 \in S$

Dobbiamo ora definire una terna $(\mathbb{N}, \sigma, 1)$ che soddisfi gli assiomi di Peano.

Definiamo $\mathbb{N}$ come l'intersezione di tutti gli insiemi induttivi.

Osservazione 3.2. La definizione di $\mathbb{N}$ implica ovviamente che $\mathbb{N}$ è contenuto in ogni insieme induttivo.

Proposizione 3.3. $\mathbb{N}$ *è un insieme induttivo.*

Dimostrazione. $1 \in \mathbb{N}$ poiché ,per definizione, 1 appartiene ad ogni insieme induttivo. Inoltre se $x \in \mathbb{N}$ allora $x \in S$ per ogni insieme induttivo S. Sicché per la proprietà b) si ha $x + 1 \in S$ per ogni insieme induttivo. Quindi $x + 1 \in \mathbb{N}$. $\square$

Osservazione 3.4. La proposizione precedente e 3.2 ci dicono che $\mathbb{N}$ è il più piccolo insieme induttivo contenuto in $\mathbb{R}$.

Grazie alla proposizione possiamo definire l'applicazione

$$\begin{aligned} \sigma :&\mathbb{N} \to \mathbb{N} \\ &n \mapsto n+1 \end{aligned}$$

e come elemento 1 possiamo prendere l'1 di $\mathbb{R}$.

Verifica assiomi di Peano

$\mathbb{N}_1$) Se $\sigma_1(n) = \sigma_1(m)$ allora per definizione

$$n + 1 = m + 1$$

da cui segue $n = m$ sottraendo ad ambo i membri 1.

$\mathbb{N}_2$) Proviamo innanzitutto che $\mathbb{R}_+ = \{x \in \mathbb{R} | x > 0\}$ è un insieme induttivo. Chiaramente $1 \in \mathbb{R}_+$. Altrettanto chiaramente se $x > 0$ allora $x + 1 > 0$.

Quindi se 1 appartenesse all'immagine di σ allora dovrebbe essere $\sigma(0) = 1$ e ciò significherebbe che $0 \in \mathbb{N}$. Ma poiché $\mathbb{R}_+$ è un insieme induttivo allora $\mathbb{N} \subseteq \mathbb{R}_+$ (cfr 3.2) e quindi ogni numero naturale è strettamente positivo e quindi $0 \notin \mathbb{N}$. Sicché $1 \notin \operatorname{Im} \sigma$.

$\mathbb{N}_3$) Sia $U \subseteq \mathbb{N}$ un insieme tale che

a) $1 \in U$

b) $k \in U \Rightarrow k + 1 \in \mathbb{N}$

Proveremo che $U = \mathbb{N}$. Infatti le proprietà a) e b) dicono semplicemente che U è insieme induttivo. Quindi per 3.2 $\mathbb{N} \subseteq U$. Poiché per ipotesi $U \subseteq \mathbb{N}$ allora $U = \mathbb{N}$.