Analisi I

Paolo Bettelini

Contents

1 Assiomi di Peano

Definizione Assiomi di Peano

Gli *assiomi di Peano* incudono i numeri naturali:

- il valore 1 è un numero;
- ogni numero n ha il suo successore $S(n) = n + 1$;
- se $m \neq n$, allora $S(m) \neq S(n)$;
- il numero 1 non è il successore di alcun numero;
- **assioma induttivo:** sia $E \subseteq \mathbb{N}$ tale che $1 \in E$, allora

$$n \in E \implies S(n) \in E$$

L'insieme E è l'insieme $\mathbb{N}$.

La funzione successore è initettiva.

Definizione Sottoinsieme finale

Un sottoinsieme $E \subseteq \mathbb{N}$ si dice *finale* se $E = \{n_0, n_0 + 1, n_0 + 2, \cdots\}$ per qualche $n_0 \in \mathbb{N}$.

Esiste quindi un valore $n \in \mathbb{N}$ tale che

$$E = \{n \in \mathbb{N} \,|\, n \geq n_0\}$$

Proposition

Usando l'assioma indutivo si deduce che se A è un insieme tale che $n_0 \in A$ e $\forall n \in A, S(n) \in A$, allora A è finale.

2 Principio di induzione

Teorema Principio di induzione

Sia $P(n)$ una proposizione dove $n \in \mathbb{N}$, allora

$$P(0) \land (P(n) \implies P(n+1)) \implies \forall n \in \mathbb{N}, P(n)$$

Teorema Equivalenza principio e assioma di induzione

L'assioma induttivo è equivalente al principio di induzione.

Proof Equivalenza assioma e principio di induzione

($\Longrightarrow$) Sia

$$E = \{n \in \mathbb{N} \,|\, P(n)\}$$

Se $P(1)$ è vera e cioè $1 \in E$, e che per ogni n per cui $P(n)$ è vera, e cioè $n \in E$, abbiamo $n+1 \in E$. Allora $E = \mathbb{N}$, che è la conclusione dell'assioma induttivo.

($\Longleftarrow$) TODO: Dimostrare che $E = \mathbb{N}$ sapendo che vale il principio di induzione.

Proposition Principio di induzione forte

Il principio di induzione è equivalente alla seguente forma: sia $P(n)$ una proposizione dove $n \in \mathbb{N}$ tale che

- $P(1)$ è vera;
- $P(k)$ è vera per tutte le $k \leq n$, allora $P(n+1)$ è vera.

Allora $P(n)$ è vera per tutte le n.

Esempio Principio di induzione

Dimostrare che per ogni $n \geq 1$, la somma

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

.

- Il caso base è dato da $n = 1$ dove $1 = \frac{2}{2} = 1$.
- Il caso induttivo è dato dato da $\xi = n + 1$

$$\begin{aligned}
\frac{n(n+1)}{2} + \xi &= \frac{n(n+1)}{2} + \frac{2n}{2} + \frac{2}{2} \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{\xi(\xi+1)}{2}
\end{aligned}$$

Considerando la serie

$$\sum_{k=1}^{n} a_k$$

e impostiamo $j = n - k + 1$, abbiamo che la sommatoria è pari a

$$\sum_{j=1}^{n} a_{n-j+1}$$

Esempio Principio di induzione

Dimostrare che

$$\sum_{k+1}^{n} k^2 = \frac{n(n+1)(n+2)}{6}$$

Esempio Principio di induzione

Per ogni $n \geq 0$ e per ogni $h > -1$,

$$(1+h)^n \geq 1 + nh$$

3 Combinatorica

Il valore $n!$ è pari alla cardinalità dell'insieme di tutte le funzioni fa F_n a F_n che sono biettive. Dove $F_n = \{1, 2, 3 \cdots, n\}$.

$$n! = |\{f : F_n \to F_n\}|$$

Proof Cardinalità di queste funzioni

- Il caso base è F_1, che contiene solo 1 elemento e $1! = 1$.
- Caso induttivo: notiamo che dato l'insieme F_n, aggiungendo un oggetto quest'ultimo possiamo posizionarlo in $n+1$ posizioni. Di conseguenza, il nuovo numero di permutazioni è $n!(n+1) = (n+1)!$.

La funzione $\sigma(n)$ è una funzione di permutazione (funzione biettiva che permuta n elementi). Infatti, le permutazione di n sono $n!$, ossia la cardinalità, cioè tutte le funzioni biettive possibili per permutare gli oggetti.

Definizione Disposizioni

Le *disposizioni* di k oggetti scelti fra n oggetti, dove $1 \leq k \leq n$, sono il numero delle funzioni iniettive $f : F_k \to F_n$.

$$D_{n,k} = \frac{n!}{(n-k)!}$$

Definizione Combinazioni

Le *combinazioni* di k oggetti scelto fra n oggetti, dove $1 \leq k \leq n$, sono il numero di sottoinsiemi di F_n di cardinalità k.

$$C_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Abbimao che

$$D_{n,k} = k! \cdot C_{n,k}$$

Lemma Proprietà dei coefficienti binomiali

Per ogni $0 \leq k \leq n$

$$\binom{n}{k} = \binom{n}{n-k}$$

Teorema Leggi di De Morgan

$$(A \cap B)^c = A^c \cup B^c$$

e

$$(A \cup B)^c = A^c \cap B^c$$

con il complementare rispetto a qualche insieme X.

Proof Leggi di De Morgan

$x \in (A \cap B)^c$ è equivalente a $x \notin A \cap B$, che è equivalente a $x \notin A$ o $x \notin B$. Allora $x \in A^c$ o $x \in B^c$, e quindi $x \in A^c \cup B^c$.

Teorema Teorema del binomio

Let $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$.

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

4 Funzione dincatrice

Definizione Funzione indicatrice

Sia X un insieme e $E \subseteq X$. La *funzione caratteristica* di E è data da

$$1_E = \begin{cases} 1 & x \in E \\ 0 & x \notin E \end{cases}$$

Dati due insiemi E e F, abbiamo $E \neq F \implies 1_E \neq 1_F$.

La notazione y^x indica $\{f : x \to y\}$, cioè tutte le funzioni da x a y.

La funzione $\Xi : \mathcal{P}(X) \to \{0, 1\}^X$ è biettiva. La funzione $f : X \to \{0, 1\}$ è pari a $f = 1_E$ per $E = \{x \mid f(x) = 1\}$. Una funzione che ti dice 1 se l'elemento sta nel sottoinsieme, 0 altrimenti. Quindi

$$|\mathcal{P}(X)| = |\{0, 1\}^X| = 2^n$$

5 Altre proprietà

$$\sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k = 0$$

Questa è la somma dei sottoinsiemi con un numero pari di elementi meno quelli con un numero dispari.

6 Interi relativi

In $\mathbb{N}$ è definita la funzione $+\colon \mathbb{N}^2 \to \mathbb{N}$ dove $(m,n) \to m+n$.

Abbiamo chiaramente che $(a,b) = (a',b') \iff a = a' \land b = b'$.

Le prorpietà sono:

- è associativa;
- è distributiva;
- esiste un elemento neutro 0 tale che $m + 0 = m, \forall m \in \mathbb{N}$

Tuttavia, $m - n$ è definito solo per $m \geq n$.

Definiamo $\mathbb{Z}$ come l'insieme

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

Abbiamo allora $\forall n \in \mathbb{Z}, \exists_{=1} n' = -n \,|\, n + (-n) = 0$, e quindi

$$n - m \triangleq n + (-m)$$

Abbiamo quindi la somma $+\colon \mathbb{Z}^2 \to \mathbb{Z}$ che gode di tutte le proprietà precedenti ma in più

$$\forall n \in \mathbb{Z}, \exists -n \,|\, n + (-n) = 0$$

Definizione Gruppo

Un insieme G con un operazione binaria $\circ$ tale che

- **associativa:** $(a \circ b) \circ c = a \circ (b \circ c)$
- **elemento neutro:** $\forall a \in A, \exists 0 \in G \,|\, 0 \circ a = a \circ 0 = a$
- **elemento opposto:** $\forall a \in G, \exists a' \,|\, a + a' = a' \circ a = 0$

Se aggiungiamo la commutatività viene detto *gruppo abeliano*.

Per esempio $(\mathbb{Z}, +)$ è un gruppo abeliano.

La struttura algebrica $(\mathbb{Z}, \circ)$ dove $(a,b) \to a \cdot b$ non è un gruppo abeliano, in quanto non c'è un inverso n^{-1} (c'è solamente per 1 e -1). La divisione si può fare solo se uno è un multiplo dell'altro.

TODO: definizione di anello

Per definire gli inversi di tutti i numeri $\neq 0$, si introducono le frazioni $\frac{m}{n}$ con $m \in \mathbb{Z}$ e $n \in \mathbb{N}^+$.

Si dice che due frazioni sono equivalenti $\frac{m'}{n'}$ e $\frac{m}{n}$ se $mn' = m'n$. I numeri razionali sono descritti dalle frazioni quando si identificano con frazioni equivalenti (classe di equivalenza), e le operazioni vengono fatte sulle frazioni. La classe di equivalenza è quindi data relazione $\frac{m}{n} \sim \frac{m'}{n'} \iff mn' = m'n$.

Abbiamo che

$$\frac{m}{n} \cdot \frac{p}{q} \to \frac{mq + pn}{nq}$$

Risulta che i razionali $\mathbb{Q}$ con le operazioni $+$ e $\cdot$ introdotte. Quindi $(\mathbb{Q}, +)$ è un gruppo abeliano, $(\mathbb{Q}^*, \cdot)$ è anch'esso un gruppo abeliano (da notare l'assenza dello 0).

Vale la proprietà distributiva di prodotto rispetto alla somma

$$r \cdot (s + t) = r \cdot s + r \cdot t$$

Quindi $(\mathbb{Q}, +, \cdot)$ è un campo, per cui possiede le operazioni $+$ e $\cdot$ con le prorpietà alle quali siamo abituati.

In particolare, in $\mathbb{Q}$ si possono risolvere le equazioni di primo grado.

$$ax + b = 0$$

con $a, b, x \in \mathbb{Q}$, $x \neq 0$.

$$\begin{aligned} ax + b + (-b) &= -b \\ ax &= -b \\ a^{-1}(ax) &= -a^{-1}b \\ a^{-1}ax &= -a^{-1}b \\ x &= -\frac{b}{a} \end{aligned}$$

Il campo di $\mathbb{Q}$ ha un ordinamento totale dove $r \leq s$ se e solo se $r - s$ è non-negativa.

In $\mathbb{Q}$ è definito un ordinamento che è compatibile ocn le operazioni $+$ e $\cdot$, cioè soddisfa le condizioni

$$r \leq s \implies t + r \leq t + s$$

con $t \in \mathbb{Q}$ e con $t \geq 0$ abbiamo $tr \leq ts$.

Definizione Campo ordinato

Un campo F nel quale è definito un ordinamento per il quale valgono le proprietà appena date, viene detto *ordinato*.

Non tutte le equazioni in $\mathbb{Q}$ sono risolvibili.

Teorema Radice di due

L'equazione

$$x^2 = 2$$

non ha soluzioni in $\mathbb{Q}$.

Proof Radice di due

Supponiamo che esista una frazione ridotta ai minimi termini $r = \frac{m}{n}$, tale che $r^2 = 2$. Abbiamo quindi che $\frac{m^2}{n^2} = 2$, quindi $m^2 = 2n^2$. Ciô ci dice che m^2 è pari. Allora, 2 è un fattore anche di m (siccome la fattorizazzione è unica e non cambia), quindi m è pari. Di conseguenza, se m è divisibile per 2, allora m^2 è divisibile per 4. Abbiamo quindi $4k = n^2$ e quindi n^2 è divisibile per 2, anche n, contro l'ipotesi del fatto che i due numeri fossero coprimi.

7 Definizioni con ordini

Definizione Insieme totalmente ordinato

Un *insieme ordinato* è una tupla $(X, \leq)$ dove X è un insieme e $\leq$ è un ordinamento totale.

Sia anche $E \subseteq X$ un insieme dove $E \neq \emptyset$.

Si dice che $m \in X$ è *maggiorante* di E se $\forall x \in E, x \leq m$.
Se un tale valore esiste, E si dice *superiormente limitato*.

Si dice che $m \in X$ è *minorante* di E se $\forall x \in E, x \geq m$.
Se un tale valore esiste, E si dice *inferiormente limitato*.

L'insieme E si dice *limitato* se è limitato sia inferiormente che superiormente.

Un valore $m \in X$ si dice *massimo* di E se M è un maggiorante di E e $m \in E$.
Un valore $m \in X$ si dice *minimo* di E se M è un minorante di E e $m \in E$.

7.1 Considerazioni

Nel caso in cui l'insieme E sia finito, vi è un massimo ed un minimo. Tuttavia, in caso contrario, valori massimi e minimi non esistono necessariamente.

Consideriamo per esempio $X = \mathbb{Q}$ ed

$$E = \left\{ r_n = \frac{n-1}{n}, \quad n \in \mathbb{N}^* \right\}$$

Possiamo notare che il valore 0 è il minimo di E. Vi sono diversi minoranti di E, come -1, -30 etc. In generale, tutti i $x \leq 0$ sono dei minoranti di E. I maggioranti di E sono tutti i valori $x \geq 1$.

Tuttavia, non vi è un massimo. Per dimostrarlo prendiamo $r_n \in E$. È facile vedere che r_n non può essere maggiorante in quando se $n' > n$, $r_{n'} > r_n$. Dato qualsiasi r_n, è possibile trovare un altro elemento in E che è maggiore, e per cui non esistono maggioranti.

Notiamo che il numero 1, che è il maggiorante, è infatti il più piccolo dei maggioranti: supponiamo che $z < 1$, verifichiamo quindi che z non è un maggiorante. Il valore z non è maggiorante di E se esiste una $x \in E$ tale che $x > z$. Esiste infatti n tale che $r_n > z$, studiamo quindi la disequazione

$$r_n - z = 1 - \frac{1}{n} - z = (1 - z) - \frac{1}{n} > 0$$

purché $1 - z > 1$. Qualcunque numero più piccolo di z sia dato, si possono fare altri valori maggiori, dati quindi da

$$n > \frac{1}{1-z}$$

7.2 Estremi superiori e inferiori

Definizione Estremo superiore

Sia $E \subseteq X$ un sottoinsieme non-vuoto, diciamo che μ è l'*estremo superiore* di E se μ è un maggiorante di E e μ è il più piccolo del maggioranti. Scriviamo quindi

$$\mu = \sup E$$

Definizione Estremo inferiore

Sia $E \subseteq X$ un sottoinsieme non-vuoto, diciamo che μ è l'*estremo inferiore* di E se μ è un minorante di E e μ è il più grande del minoranti. Scriviamo quindi

$$\mu = \inf E$$

I valori di minimo, massimo, estremo inferiore, estremo superiore, sono unici se esistono. Ci sono sottoinsiemi di $\mathbb{Q}$ che non hanno estremi superiori (e quindi ci sono tante funzioni senza limiti, derivate e integrali. L'analisi in $\mathbb{Q}$ sarebbe quindi un disastro per questo motivo).

Teorema

Sia

$$E = \left\{ r \in \mathbb{Q} \,|\, r \geq 0 \land r^2 \leq 2 \right\}$$

allora, E è non-vuoto, limitato superiormente, ma non esiste il suo estremo superiore.

Proof

- Per dimostrare che $E \neq \emptyset$ possiamo semplicemente darne un elemento, come per esempio 1.
- L'insieme E è banalmente limitato superiormente da tutti i valori $x \geq 2$.
- Supponiamo per assurdo che esista un $\mu = \sup E$. Notiamo che ovviamente $\mu > 0$. Possiamo notare che $\mu^2 = 2$ è impossibile per il teorema di Euclide. Allora, μ potrebbe essere minore di 2 oppure maggiore di 2. Supponiamo che $\mu^2 < 2$, allora dimostro che $\exists x \in E$ tale che $x > \mu$ e quindi che μ non è maggiorante. Consideriamo quindi i numeri razionali della forma

$$\mu + \frac{1}{n}$$

che sono chiaramente più grandi di μ. Possiamo quindi scegliere n sufficientemente grande tale che $(\mu + \frac{1}{n})^2 < 2$, e quindi $\mu + \frac{1}{n} \in E$ in quanto

$$\begin{aligned} 2 - \left(\mu + \frac{1}{n}\right)^2 &= 2 - \mu^2 + \frac{2\mu}{n} + \frac{1}{n^2} \\ &= (2 - \mu^2) - \frac{2\mu}{n} - \frac{1}{n^2} \end{aligned}$$

è chiaramente più grande di $(2 - \mu^2) - \frac{2\mu}{n} - \frac{1}{n}$. Ciò è dato dal fatto che $\frac{1}{n} > \frac{1}{n^2}$.

$$\frac{2\mu + 1}{n} < 2 - \mu^2, \quad n > \frac{2 - \mu^2}{2\mu + 1}$$

Analogamente, si dimostra che μ^2 non può essere nemmeno maggiore di 2, e quindi μ non esiste.

È facile verificare che inf, sup, min, max se esistono sono unici. Se esiste il massimo di E, allora esiste il $\sup E$ e coincidono. Infatti, il massimo esiste se esiste $\sup E$ e $\sup E \in E$.

In $\mathbb{Q}$ (e poi in $\mathbb{R}$), se E non è limitato superiormente (cioè non ha maggiornate cioè $\forall M \in \mathbb{Q}, \exists e \in E$ tale che $e > M$) si dice che

$$\sup E = +\infty$$

Analogamente se E non è limitato inferiormente si dice che

$$\inf E = -\infty$$

Possiamo quindi notare che

$$\sup \emptyset = -\infty$$

e

$$\inf \emptyset = +\infty$$

Definizione Numeri reali

Definiamo $\mathbb{R}$ come un campo totalmente ordinato nel quale vale la seguente proprietà del sup:

$$\forall E \subseteq \mathbb{R}, \quad E \neq \emptyset \wedge E \text{ limitato sup. esiste}$$

La proprietà del sup è equivalente all'assioma della scelta.

Bisogna tuttavia dimostrare l'unicità di questa costruzione e la sua esistenza.

Teorema Teorema di unicità

Siano F_1 e F_2 due campi ordinati nei quali vale la proprietà del sup di prima. Allora, esiste una biezione $\phi\colon F_1 \to F_2$ tale che è un isomorfismo del gruppo additivo $\phi(x +_{F_1} y) = \phi(x) +_{F_2} \phi(y)$ per ogni $x, y \in F_1$ e $\phi(-x) = -\phi(x)$ per ogni $x \in F_1$. Se aggiungiamo anche che $\phi(x \cdot_{F_1} y) = \phi(x) \cdot_{F_2} \phi(y)$ per tutte le $x, y \in F_1$ e $\phi(x^{-1}) = \phi(x)^{-1}$ abbiamo un isomorfismo di campo. Se aggiungiamo anche che $x \leq y \iff \phi(x) \leq \phi(y)$, abbiamo quindi un isomorfismo di campo ordinato.

Date le proprietà di un campo, ogni campo genera un insieme dei razionali $\mathbb{Q}$. Chiaramente, diversi campi generano $\mathbb{Q}$ diversi ma con gli stessi elementi in un certo senso. Possiamo mappare un insieme dei razionali di un campo a quello di un altro.

È facile definire $\phi_0 \colon \mathbb{Q}_1 \subseteq F_1 \to \mathbb{Q}_2 \subseteq F_2$. Usando la proprietà del sup possiamo eseguire tale mappatura. Dato $x \in F_1$, abbiamo $x = \sup\{r \in \mathbb{Q}_1 \,|\, r \leq x\} = \sup E_x$. Allora $\phi(x) = \sup\{\phi_0(r) \,|\, r \in E_x\}$. Così viene esteso ϕ a tutto. Bisognerebbe tuttavia dimostrare che le proprietà classiche vengano preservate.

Per dimostrare l'esistenza è necessario considerare

$$\mathbb{R} = \{ \text{ numeri decimali } n, a_1, a_2, a_3, \cdots \} \text{ finiti o infiniti periodici o meno}$$

dove $a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Con la prescrizione che $n, a_1, a_2, a_3, \cdots, a_k, \overline{9} = n, a_1, \cdots, a_{k-1}, (a_k + 1)$.

I numeri reali possono essere anche definiti mediante le sezioni di Dedekind. Alternativamente si possono definire mediante le successioni di Cauchy.

Definizione di somma e prodotto: Prendiamo $x = n, a_1, \cdots, a_k \cdots$ e $y = m, b_1, \cdots, b_k \cdots$ che sono due numeri decimali, nessuno dei quali con period 9, allora

$$x = y \iff n = m \wedge a_k = b_k$$

e

$$x > y \iff n > m \wedge a_k > b_k$$

Le operazioni sono definite mediante troncamenti,