Analisi I

Paolo Bettelini

Contents

1	Assiomi di Peano	2
2	Principio di induzione	3
3	Combinatorica	4
4	Funzione indicatrice	6
5	Altre proprietà	6
6	Interi relativi	7
7	Definizioni con ordini7.1 Considerazioni7.2 Estremi superiori e inferiori7.3 Conseguenze della proprietà del sup7.4 Esercizi sup	9 10 12 13
8	Esponenziali 8.1 Potenze ad esponente reale e esponziali e logaritmi 8.2 Potenze a esponente reale 8.3 Esponenziali 8.4 Assioma di continuità	16 16 16 17
9	Numeri complessi 9.1 Inclusione dei reali	19 19 19 20 20
10	Distanza fra due insiemi	20
11	Teorema di Ruffini	21
12	Spazi metrici	22
13	Spazi topologici	22
14	Successioni	23

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

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

Allora 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 $E = \{n_0, n_0 + 1, n_0 + 2, \dots\}$ per qualche $n_0 \in \mathbb{N}$.

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

$$E = \{ n \in \mathbb{N} \mid n \ge n_0 \}$$

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

Given a proposition P(n), let

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

 (\Longrightarrow) If $0 \in E$, then P(0) is true.

If $n \in E \implies S(n) \in E$, then $P(n) \implies P(S(n))$.

If the latter conditions are satisfied, then by the axiom of induction, $E = \mathbb{N}$, and thus

$$\forall n \in \mathbb{N}, P(n)$$

 (\Leftarrow) If P(0) is true, then $0 \in E$.

If $P(n) \implies P(S(n))$, then if $n \in E \implies S(n) \in E$.

If the latter conditions are satisfied, then by the principle of induction

$$\forall n \in \mathbb{N}, n \in E$$

and thus $E = \mathbb{N}$.

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 $n \ge 1$, 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 $\xi = n + 1$

$$\frac{n(n+1)}{2} + \xi = \frac{n(n+1)}{2} + \frac{2n}{2} + \frac{2}{2}$$

$$= \frac{n^2 + 3n + 2}{2}$$

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

$$= \frac{\xi(\xi+1)}{2}$$

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

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

Esempio Principio di induzione

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

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

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 $F_n = \{1, 2, 3 \cdots, n\}$.

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

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 $1 \le k \le n$, 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 $1 \le k \le n$, 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 $0 \le k \le n$

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

Teorema Leggi di De Morgan

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

е

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

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 indicatrice

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 $\{f \colon x \to y\}$, 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 $+: \mathbb{N}^2 \to \mathbb{N}$ 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 $m \ge n$.

Definiamo $\mathbb Z$ come l'insieme

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

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

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

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

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

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: $\forall a \in A, \exists 0 \in G \mid 0 \circ a = a \circ 0 = a$
- elemento opposto: $\forall a \in G, \exists a' \mid a + a' = a' \circ a = 0$

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 $+ e \cdot \text{con}$ le prorpietà alle quali siamo abituati.

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

$$ax + b = 0$$

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

$$ax + b + (-b) = -b$$

$$ax = -b$$

$$a^{-1}(ax) = -a^{-1}b$$

$$a^{-1}ax = -a^{-1}b$$

$$x = -\frac{b}{a}$$

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

$$r \le s \implies t + r \le t + s$$

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 $x \le 0$ sono dei minoranti di E. I maggioranti di E sono tutti i valori $x \ge 1$.

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

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

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 μ = sup E. Notiamo che ovviamente μ > 0. Possiamo notare che μ² = 2 è impossibile per il teorema di Euclide. Allora, μ potrebbe essere minore di 2 oppure maggiore di 2. Supponiamo che μ² < 2, allora dimostro che ∃x ∈ E tale che x > μ 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

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

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

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

 \mathbf{e}

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

Definizione Numeri reali

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

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

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

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 $\phi_0: \mathbb{Q}_1 \subseteq F_1 \to \mathbb{Q}_2 \subseteq F_2$. Usando la proprietà del sup possiamo eseguire tale mappatura. Dato $x \in F_1$, abbiamo $x = \sup\{r \in \mathbb{Q}_1 \mid r \leq x\} = \sup E_x$. Allora $\phi(x) = \sup\{\phi_0(r) \mid r \in E_x\}$. 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 $n, a_1, a_2, a_3, \dots, a_k, \overline{9} = n, a_1, \dots, a_{k-1}, (a_k+1)$.

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 $x = n, a_1, \dots, a_k \dots$ e $y = m, b_1, \dots, b_k \dots$ che sono due numeri decimali, nessuno dei quali con period 9, allora

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

е

$$x < y \iff n < m \lor (n = m \land a_i = b_i, i < k \land a_k < b_k)$$

Le operazioni sono definite mediante troncamenti. Verificiamo che questo modello di $\mathbb R$ soddisfi la proprietà del sup.

Prendiamo quindi $E \subseteq \mathbb{R}$ non vuoto e sup limitato. Costruiamo il sup mediante un algoritmo.

$$\sup E = \mu = n, a_1, a_2, a_3, \cdots, a_k, \cdots$$

Per ogni $x \in E$ scriveremo $n_x, a(x)_1, a(x)_2, \cdots$. E è non-vuoto e limitato sup, per cui

$$\{n_x \mid x \in E\}$$

è un insieme di numeri in $\mathbb Z$ limitato superiormente. Sia

$$N = \max\{n_x \colon x \in E\}$$

Prendiamo ora tutti gli insiemi

$$E_0 = \{ x \in E \mid n_x = N \} \neq \emptyset$$

Poniamo $a_1 = \max\{a(x)_1 \mid x \in E_0\}$ Abbiamo quindi

$$E_1 = \{x \in E_0 \mid a(x)_1 = a_1\} \neq \emptyset$$

Poniamo ora $a_2 = \max\{a(x)_2 \mid x \in E_1\}$. Con lo stesso metodo troviamo a_3, a_4, \dots , ossia

$$a_k = \max\{a(x)_k \mid x \in E_{k-1}\}$$
 $a_{k+1} = \max\{a(x)_{k+1} \mid x \in E_k\}$

Trovando quindi

$$\mu = N, a_1, a_2, \cdots$$

Dico che μ è un maggiorante di E, e che se $z < \mu$, z non è maggiorante. Sia allora $\overline{x} \in E$, quindi

$$\overline{x} = n_{\overline{x}}, a(\overline{x})_1, a(\overline{x})_2, \cdots$$

Allora $n_{\overline{x}} \leq N$ se $n_{\overline{x}} < N$. $\overline{x} < \mu$. Gli elementi in E_0 sono al massimo a_1 . Se $n_{\overline{x}} = N$ e $n_{\overline{x}} \in E_0$ e $a_1(\overline{x}) = a_1$.

Se $a(\overline{x})_1 < a_1 \implies \overline{x} < \mu$.

Se invece $a(\overline{x})_1 = a_1 \implies \overline{x} \in E_1 \in a(\overline{x})_2 \le a_2$

Fino che ad un certo punto non trovo un decimale diverso.

Iterando, se $\exists k$ tale che $a(\overline{x})_k < a_k \implies \overline{x} < \mu$. Se $\forall k, a(\overline{x})_k = a_k$, allora $\overline{x} = \mu$ e μ è il max di E. Questo procedimento non dimostra che $\mu \in E$.

Mostriamo ora che è il più piccolo dei maggioranti. Sia

$$z = n_z, a(z)_1, a(z)_2, \dots < \mu$$

Deve quindi succedere che o $n_z < N$, e allora $\forall x \in E_0 \neq \emptyset, z < x$, oppure $n_z = N$ e $a(z)_j = a_j$ per tutte le j < k ma $a(z)_k < a_k$. Allora $\mu = \sup E$.

7.3 Conseguenze della proprietà del sup

Le conseguenze della prorpietà del sup sono:

- proprietà archimedea: $\forall x \in \mathbb{R}, \forall a > 0, \exists n \in \mathbb{N} \mid na > x$ (in realtà vale anche in \mathbb{Q}).
- densità dei razionali nel reali: $\forall x, y \in \mathbb{R}$ dove x < y, esiste $r \in \mathbb{Q} \mid x < r < y$.

Teorema Esistenza delle radici nei reali

$$\forall y > 0, \forall n \in \mathbb{N}, n \ge 1, \exists_{=1} x > 0 \mid x^n = y$$

Proof

Sia

$$E = \{ z \in \mathbb{R} \,|\, z > 0 \land z^n \le y \}$$

Dobbiamo quindi mostrare che E non è vuoto, ed è limitato superiormente. Definiamo $x=\sup E$ e mostriamo che $x^n=y$.

- Non vuoto: se $y \ge 1$, basta scegliere x = 1 in quanto $x^n = 1 \le y$. Altrimenti, se y < 1, poniamo x = y e notiamo che, perché y < 1, allora $y^n < y$, e quindi $y \in E$.
- Limitato superiormente: E è limitato superiormente, infatti 1+y è un maggiorante di E. Se $z \ge (1+y)$, poiché la funzione $t \to t^2$ è crescente per t > 0, si ha $z^n \ge (1+y)^n > (1+y) > y \implies z \notin E$. Sia $x = \sup E$. Dico che $x^n = y$. Dimostro che se suppongo $x^n > y$ allora per k grande

$$\left(x - \frac{1}{k}\right)^n > y$$

e quindi $x - \frac{1}{k}$ è ancora un maggiorante di E, contro l'ipotesi impossibile perché x, che è il sup E, è il più piccolo maggiorante. Invece, se $x^n < y$ allora per k grande

$$\left(x + \frac{1}{k}\right)^n < y$$

allora $x + \frac{1}{k} \in E$ ed è più grande di x, e x non è quindi un maggiorante (assurdo). Visto che x non può essere nè più grande nè più piccolo, $x^n = y$.

• Unicità: notiamo che se $0 < t_1 < t_2 \implies t_1^n < t_2^n$

Possiamo anche mettere $z \geq 0$ così dimostrare che $E \neq \emptyset$ è più facile.

Esercizio: dimostrazione per induzione che $0 < y < 1 \implies y^n < y$, per n > 1. (Che abbiamo usato nell'ultima dimostrazione).

7.4 Esercizi sup

Esercizio

Let

$$E = \left\{ x \in \mathbb{R} \,|\, \frac{1}{2} \le x < 5 \right\}$$

and the sequence

$$F = \{x = x_n \mid x_n = \frac{n+1}{n+2}, \quad n \in \mathbb{N}^*\}$$

Trova inf, sup, min, max (se esistono) di $E, F, E \cup F$ e $E \cap F$.

- E è limitato superiormente e inferiormente. Il minimo è $\frac{1}{2}$, mentre 5 è un maggiorante, è il più piccolo dei maggioranti quindi sup E=5, ma non vi è un massimo.
- F è limitato superiormente in quanto

$$x_n = \frac{n+1}{n+2} < \frac{n+2}{n+2} = 1$$

È limitato inferiormente perché $x_n > 0$. Per verificare sup e inf, è comodo riscrivere

$$x_n = 1 - \frac{1}{n+2}$$

Il temrine n+2 cresce con n, quindi $\frac{1}{n+2}$ decresce al crescere di n e quindi x_n cresce approcciando 1. Allora con n=1 il termine assume il valore più piccolo, ossia $\frac{2}{3}$, quindi il minimo di F. Allora siccome ci avviciamo arbitrariamente a 1, è lecito ipotizzare sup F=1.

Il massimo di F non esiste. Rimane da far vedere che se z < 1 allora z non è maggiorante $\operatorname{di} F \operatorname{cioè}$

$$x_n - z = (1 - z) - \frac{1}{n+2} > 0$$

- purché $\frac{1}{n+2} < 1-z$ cioè $n > \frac{1}{1-z} 2$. Quindi z non è maggiorante e sup E=1. Verificare che sup $(E \cup F) = \max\{\sup E, \sup F\}$. Abbiamo che sup $E \le \sup F$. In sup è il massimo dei due in quanto uno è maggiore dell'altro, e fa parte dell'insieme, quindi $\sup E \cup F = 5$. Tuttavia, il max non esiste in quando $5 \notin E \cup F$. Analogamente, inf $E \cup F = \frac{1}{2}$. Questo valore è anchde il minimo in quanto fa parte dell'insieme.
- Mostrare con un esempio che non c'è qualcosa di analogo per l'intersezione.

$$E \cap F = \left\{ x_n = \frac{x+1}{x+2} \mid \frac{1}{2} \le \frac{x+1}{x+2} \le 5 \right\}$$

Quindi $F \subseteq E$. Consideriamo allora $E_1 = \begin{bmatrix} \frac{4}{5}, 5 \end{bmatrix}$

$$E_1 \cap F = \left\{ x_n = \frac{x+1}{x+2} \mid \frac{4}{5} \le x_n \le 5 \right\}$$

Per quali n vale che $\frac{4}{5} \le \frac{x+1}{x+2} = x_n$? Abbiamo $4(n+2) \le 5(n+1)$ e quindi $n \ge 3$. Allora $\sup E_1 \cap F = 1$ e non vi è massimo, mentre inf $E_1 \cap F = \frac{4}{5}$ che è anche il minimo.

Posto $E + F = \{x + y \mid x \in E, y \in F\}$ mostrare $\sup E + F = \sup E + \sup F$. Supponiamo quindi che sup E e sup F siano finiti. Siccome, per definizione, $\forall e \in E, e \leq \sup E \in \forall f \in E$ $F, f \leq \sup F$, abbiamo che

$$\forall e \in E, \forall f \in F, e + f \le \sup E + \sup F$$

Per mostrare che questo è il più piccolo dei maggioranti, è comodo riscrivere la definizione di sup dicendo che μ è pari a sup E se:

- 1. $\forall x \in E, x \leq \mu$;
- 2. $\forall \epsilon > 0, \mu \epsilon$ non è maggiorante.

Nota: se $x < \mu$ allora posto $\epsilon = \mu - x$ risulta $x = \mu - \epsilon$. Allora sia $\epsilon > 0$. Diciamo che esistono $e_1 \in E$ e $f_1 \in F$ tali che $e_1 + f_1 > \sup E + \sup F - \epsilon$. Poiché $\sup E$ è, appunto, il supremum, esiste per definizione una $e_1 \in E$ tale che $e_1 > e_1 > \sup E \cdot \frac{\epsilon}{2}$. Analogamente, esiste $f_1 \in F$ tale che $f_1 > \sup F - \frac{\epsilon}{2}$. Da cui $e_1 + f_2 > \sup E - \frac{\epsilon}{2} + \sup F - \frac{\epsilon}{2} = \sup E + \sup F - \epsilon$.

Posto $-E = \{-x \mid x \in E\}$ mostrare che sup $-E = -\inf E$ e inf $-E = -\sup E$.

Dimostrare che il max esiste se e solo se sup E è finito e appartiene a E. Analogamente per il min.

Esercizio

Trovare sup, inf, min, max dell'insieme

$$E = \left\{ x_n = \frac{n-7}{x^2 + 1} \mid n \ge 1 \right\}$$

Questa successione ha sicuramente un minimo in quanto ci sono solamente 6 numeri negativi. Possiamo notare che il denominatore cresce più velocemente del numeratore. Studiamo quindi per quali indici vale $x_n \leq x_{n+1}$. Otteniamo quindi

$$\frac{n-7}{n^2+1} \le \frac{(n+1)-7}{(n+1)^2+1}$$
$$\frac{(n-7)(n^2+2n+2)-(n-6)(n^2+1)}{(n^2+1)(n^2+2n+2)} \le 0$$

Il denominatore è positivo, quindi studiamo il numeratore

$$n^2 - 13n - 8 \le 0$$

Le radici di questo polinomio sono $n_{1,2}=\frac{13\pm\sqrt{201}}{2}$. Di conseguenza, l'espressione è negativa per $\frac{13-\sqrt{201}}{2} < n < \frac{13+\sqrt{201}}{2}$. Notiamo che l'estremo di sinistra è negativo. Notiamo anche che $14^2 < 201 < 15^2$, e quindi l'estremo di destra è compreso fra 14 e $\frac{27}{2}$. Allora, tutte le n intere che soddisfano l'equazione sono n=13. Ne consegue che se $n\geq 14$, $x_n>x_{n+1}$. Il maggiornate e supremum è quindi x_{14} .

8 Esponenziali

8.1 Potenze ad esponente reale e esponziali e logaritmi

Abbiamo definito le radici n-esime come

$$x^{\frac{m}{n}} \triangleq \sqrt[n]{x^m}$$

Si dimostra inoltre che per ogni p intero positivo,

$$x^{\frac{x \cdot p}{n \cdot p}} = x^{\frac{m}{n}}$$

La potenza x^r è quindi ben definita con $r \in \mathbb{Q}^{>0}$. Successivamente, definiamo le potenze negative

$$x^{-r} = (x^-1)^r$$

Abbiamo le consuete proprietà:

- 1. $\forall x > 0, x^0 = 1;$
- 2. $\forall r, s \in \mathbb{Q}, x^r x^s = x^{r+s};$
- 3. $\forall r, s \in \mathbb{Q}, (x^r)^s = x^{rs};$

Con r > 0 posso definire $0^r = 0$ e se $r = \frac{m}{n}$ (ridotta ai minimi termini) con n dispari posso definire $x^{\frac{m}{n}}$

8.2 Potenze a esponente reale

Se x = 1, $\forall a \in \mathbb{R}$, $x^a = 1$. Se x > 1 e r < s, allora $x^r < x^s$

$$r = \frac{m}{p} < s = \frac{n}{p}, m < n$$

$$x^r = \left(\sqrt[p]{x}\right)^m < \left(\sqrt[p]{x}\right)^n$$

Definiamo quindi la potenza reale con a > 1 e x > 1

$$x^a = \sup\{x^r \mid r < a\}$$

Estendiamo la definizione ad a < 0 come

$$x^a = (x^{-1})^{-a}$$

E infinie se 0 < x < 1

$$x^a = (x^{-1})^{-a}$$

8.3 Esponenziali

Fissata una base a > 0 abbiamo poi l'esponenziale che è definita da a^x , $x \in \mathbb{R}$.

Risulta che se a=1, allora la funzione è sempre 1. Se a>1 la funzione è stretta crescente, e strettamente descrescente se 0< a<1.

La funzione è biettiva tra \mathbb{R} e $(0, +\infty)$, quindi è invertibile. La funzione inversa è $y = \log_a(x)$.

Le proprietà dei logaritmi sono analoghe a quelle degli esponenti.

Proposition Proprietà dei logaritmi

$$\begin{split} \log_a(xy) &= \log_a(x) + \log_a(y) \\ \log_a(x^y) &= y \log_a(x) \\ \log_a(b) &= \frac{\log_c(a)}{\log_c(b)} \end{split}$$

Il passaggio da moltiplicazione e somma di logaritmi, potrebbe non avere senso nella seconda forma. E.g $\ln(x(x-1))$ non is può riscrivere come $\ln(x) + \ln(x-1)$ perché, se sono positivi quando moltiplicati, non è detto che lo siano separatamente.

Se abbiamo $\log_2(x^2)$, possiamo riscriverlo come $2\log_2|x|$.

8.4 Assioma di continuità

$$\bigcup_{n \neq 2} \left[\frac{1}{n}; 1 - \frac{1}{n} \right] = (0, 1)$$

Assioma di Dedekind

Se $\{I_n\}$ è una successione di intervalli chiusi della forma $I_n=[a_n;b_n]$ tali che $I_{n+1}\subseteq I_n$ e

$$l(I_{n+1}) = b_{n+1} - a_{n+1} = \frac{1}{2}l(I_n)$$

e quindi

$$l(I_n) = \frac{1}{2^{n-1}}l(I_1)$$

allora esiste $c \in \mathbb{R}$ tale che

$$\bigcap_{n\in\mathbb{N}}I_n=\{c\}$$

Questo assioma non vale nei razionali.

Teorema Assioma di Dedekind equivalenza assioma di completezza

L'assioma di Dedekind è equivalente all'assioma della completezza.

Proof Assioma di continuità equivalenza assioma di Dedeking

- (\Longrightarrow) Sia E un insieme non vuoto e limitato superiormente, dimostriamo che esiste $c = \sup E$. Poiché E è limitato superiormente esiste un b_1 maggiorante di E dove $b_1 \geq e, \forall e \in E$. Poiché E è non vuoto esiste $\overline{e} \in E$ e poniamo $a_1 = \overline{e} - 1$ cosicché $a_1 < \overline{e}$ e a_1 non è maggiornate. Sia $I_1 = [a_1, b_1]$ e sia $m_1 = \frac{a_1 + b_1}{2}$, allora vi sono due casi:
 - m_1 è un maggiorante e allora poniamo $a_2 = a_1$ e $b_2 = m_1$;
 - m_1 non è un maggiorante e allora poniamo $a_2 = m_1$ e $b_2 = b_1$.

Sia $I_2 = [a_2, b_2]$. Iteriamo allora il procedimento otteniamo una successione di intervalli

$$I_n = [a_n, b_n]$$

tali che $I_{n+1} \subseteq I_n$ e $l(I_{n+1}) = \frac{1}{2}l(I_n)$. Per ogni n, a_n non è maggiorante di E, b_n è maggiorante di E. Per l'assioma di continuità $\exists c \in \mathbb{R}$ tale che

$$\bigcap_{n\in\mathbb{N}}I_n=\{c\}$$

La nostra tesi è quindi $c=\sup E$. Supponiamo quindi per assurdo che non sia un maggiorante, allora che esiste un elemento $e\in E$ dove e>c. Per definizione c è in almeno un I_n quindi $a_n\leq c\leq b_n$ e poiché e>c abbiamo $a_1\leq c< e\leq b_n$ perché $e\in E$ e b_n è maggiorante di E per ogni n. Quindi

$$[c,e]\subseteq [a_n,b_n]$$

e allora

$$[c,e] \in \bigcap_{n \in \mathbb{N}} I_n = \{c\}$$

che è quindi una contraddizione. Dobbiamo ora mostrare che c è il più piccolo dei maggioranti. Supponiamo quindi per assurdo che ci sia un altro maggiorante x < c. Poiché $b_n \ge c$ per ogni n abbiamo che $x < c \le b$. Per ipotesi, x è maggiorante di E mentre a_n non è maggiorante di E per ogni n. Quindi per tutte le n esiste un elemento e_n tale che

$$a_n < e_n \le x < c \le b_n$$

e quindi si deduce che l'intervallo $[x,c]\subseteq [a_n,b_n]=I_n$ da cui

$$[c,e] \in \bigcap_{n \in \mathbb{N}} I_n = \{c\}$$

che quindi è assurdo.

 (\longleftarrow) TODO (in the future)

9 Numeri complessi

In un campo ordinato e quindi in \mathbb{R} , $x^2 \geq 0$ e vale $x^2 = 0 \iff x = 0$. Quindi l'equazione $x^2 = -1$ non ha soluzione in \mathbb{R} . Estendiamo il campo \mathbb{R} costruendo un campo \mathbb{C} che contiene una immagine isomorfa di \mathbb{R} nel quale $z^2 = -1$ ha soluzioni.

Tuttavia, tale campo non ammette il medesimo ordinamento che avevamo. Definiamo quindi

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

Definiamo l'operazione di addizione

$$+: \mathbb{C} \times \mathbb{C} \to \mathbb{C}$$

in maniera tale che

$$(a,b) + (c,d) \triangleq (a+c,b+d)$$

- 1. anche questa somma è associativa, e commutativa come in \mathbb{R} ;
- 2. l'elemento neutro 0 è la coppia 0,0;
- 3. l'opposto di (a,b) è -(a,b);

Si può rappresentare $\mathbb C$ come punti nel piano. La moltiplicazione è definita come

$$(a,b)\cdot(c,d)\triangleq(ac-db,ad+bc)$$

Questo prodotto è

- 1. è associativo;
- 2. è commutativo;
- 3. l'elemento (1,0) è l'elemento neutro;
- 4. esiste un elemento inverso

$$\forall z = (a, b) \in \mathbb{C} \mid (a, b) \neq (0, 0), \exists z^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) \mid zz^{-1} = (1, 0)$$

Per determinare questa forma basta risolvere $z^{-1} = (x, y)$ dove (a, b)(x, y) = (1, 0).

Abbiamo quindi un campo.

Adesso, notiamo che (0,1)(0,1) = (-1,0).

9.1 Inclusione dei reali

Ogni number $r \in \mathbb{R}$ può essere identificato con il numero complesso (r,0). Cosifacendo, l'applicazione $\varphi \colon \mathbb{R} \to \mathbb{C}$ tale che $\varphi(a) = (a,0)$ preserva le operazioni.

Possiamo poi scrivere z=(a,b) come a(1,0)+b(0,1). Se identifichiamo i=(0,1), possiamo scrivere

$$(a,b) = a + bi$$

che viene detta forma algebrica. Le operazioni di numeri complessi in forma algebrica si forma con le consuete regole del calcolo letterale e l'identità $i^2 = -1$.

9.2 Operazioni algebriche

$$\begin{cases} i^{0} = +1 \\ i^{1} = +i \\ i^{2} = -1 \\ i^{3} = -i \end{cases} \begin{cases} i^{4} = +1 \\ i^{5} = +i \\ i^{6} = -1 \\ i^{7} = -i \end{cases} \dots$$

Dato z = a + bi, diciamo che $\Re(z) = a$ e $\Im(z) = b$.

Definizione Coniugio

Dato
$$z = a + bi \in \mathbb{Z}$$
,

$$\overline{z} = a - bi$$

Chiaramente, $z + \overline{z} = 2\Re(z)$. Possiamo quindi dire che

$$\Re z = \frac{z + \overline{z}}{2}$$

 \mathbf{e}

$$\Im z = \frac{z - \overline{z}}{2i}$$

Proposition Proprietà del coniugio

- involutivo: $\overline{\overline{z}} = z$;
- $\overline{z+w} = \overline{z} + \overline{w};$
- $\overline{zw} = \overline{z} \cdot \overline{w};$ $w \neq 0 \implies \overline{z^{-1}} = (\overline{z})^{-1};$ $w \neq 0 \implies \overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}};$ $\overline{z^n} = (\overline{z})^n \text{ per } n \in \mathbb{Z}.$

Per ogni numero complesso z,

$$\left|z\right|^2 = z\overline{z}$$

e per ogni numero complesso w

$$\overline{w}\overline{z} = wz\overline{w}\overline{z} = z\overline{z}w\overline{w} = |z|^2|w|^2$$

In particolare, $|z^n| = |z|^n$.

La disuguaglianza $||z| - |w|| \le |z - w|$.

- $|wz| = |w| \cdot |z|$;
- $|w + z| \le |w| + |z|$.

Da dimostrare: $|z + w|^2 \le (|z| + |w|)^2$.

9.3 Passaggio polari e cartesiane

Dato $x+iy=r(\cos\theta+i\sin\theta)$ e il punto polare (r,θ) abbiamo

$$r = \sqrt{x^2 + y^2}$$

 \mathbf{e}

$$\theta = \arctan\left(\frac{y}{x}\right)$$

De Moivre 9.4

$$z^{n} = r^{n}(\cos\theta + i\sin\theta)^{n} = \sum_{k=0}^{n} \binom{n}{k} i^{k} (\cos\theta)^{n-k} (\sin\theta)^{k}$$

10 Distanza fra due insiemi

La distanza (minima) fra due insiemi è definita come

$$\operatorname{dist}(S,R) = \inf\{d(z,w) \,|\, z \in S \land w \in R\}$$

11 Teorema di Ruffini

Dato un polinomio $p(z), z_0$ è una radice di p(z) se esiste un polinomio q(z) con deg $q(z) = \deg p(z) - 1$ tale che

$$p(z) = (z - z_0)q(z)$$

, cioè se p(z) è divisibile per $z-z_0$.

La radice z_0 ha moltiplicità $m \ge 1$ se p(z) è divisibile per $(z-z_0)^m$ ma non per $(z-z_0)^{m+1}$.

12 Spazi metrici

Definizione Metrica della valle

La funzione di distanza della metrica della valle fra due punti a=(x,y) e b=(t,u) è definita come

$$d(a,b) = \begin{cases} |y-u| & x=t \\ |y|+|x-t|+|u| & x \neq t \end{cases}$$

Definizione Distanza in un grafo

Distanza in un grafo

 $d(a,b) = \inf\{\text{lunghezza dei cammini che congiungono a e b}\}$

Definizione Insieme aperto in spazio metrico

Un sottoinsieme $A \subseteq X$ è aperto se tutti i punti sono interni in A.

13 Spazi topologici

Un punto x_0 è isolato in E se $\exists r > 0$ tale che $(x_0 - r, x_0 + r) \cap E = \{x_0\}.$

Teorema

Sia $E \subseteq \mathbb{R}$ (vale in qualsiasi spazio metrico) e sia $x_0 \in \mathbb{R}$. Sono equivalenti:

1. x_0 è di accumulazione cioè $\forall r > 0$,

$$((x_0 - r, x_0 + r) \setminus \{x_0\}) \cap E \neq \emptyset$$

2. $\forall r > 0, (x_0 - r, x_0 + r) \cap E$ è infinito (ogni intorno contiene infiniti punti di E).

Proof

- (\Longrightarrow) Dimostriamo la contronominale. Assumiamo quindi che $\exists r>0$ tale che $A=(x_0-r,x_0+r)\cap E$ è finito, e quindi $A=\{x_0,x_1,\cdots,x_n\}$ dove x_1,x_2,\cdots,x_n sono gli elementi di $(x_0+r,x_0-r)\cap E$ diversi da x_0 . Chiaramente, esiste un $0<\epsilon<\min\{|x_0-x_1|,|x_0-x_2|,\cdots,|x_0-x_n|\}$. Siccome l'insieme è finito, ϵ esiste ed è strettamente positivo. Quindi, per definizione x_0 non è di accumulazione.
- (\Leftarrow) Trivial.

14 Successioni

Diciamo che $M = \max x_n$ se $\forall n x_n < M$ e $\exists n' \, | \, x_{n'} = M$. Analogamente il min.

Definiamo inoltre $\sup_n x_n = \sup\{x_n \, | \, x \in \mathbb{N}\}$ Analogamente per l'inf.

Definizione Proprietà soddisfatta definitivamente

Data una proprietà P, una successione $\{x_n\}$ soddisfa la proprietà P definitivamente se $\exists N \,|\, \forall n, P(n) \geq N$.