Algebra I

martedì 29 settembre 2020 11:24

Argomenti del corso.

- Aritmetica ($\mathbb{Z}$ e le sue proprietà)
  Fattorizzazione unica degli interi

[Generalizzazione a strutture simili all'anello degli interi
DOMINI A IDEALI PRINCIPALI. Interi di Gauss $\mathbb{Z}[i]$]

- Aritmetica modulare (classi di resto modulo n)
  palestra di esempi per la Teoria degli anelli e dei gruppi (abeliani)

[TANTE APPLICAZIONI CONCRETE] Teorema cinese dei resti (del resto)

- Teoria dei gruppi (per lo più finiti)
- Teoria dei campi. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Estensioni di campi.
  $\mathbb{R} \subseteq \mathbb{C}$. Algebrici e trascendenti

Introduzione alla Teoria di Galois.

Notazioni. Insiemi, elementi. Appartenenza.

X x Ogni insieme può essere anche un elemento di un altro insieme.

$x \in X$

$X \in \{X\}$

Buonsenso: un insieme è l'informazione di quali elementi contiene. Pertanto due insiemi coincidono se e solo se contengono gli stessi elementi.

$\emptyset$ ← insieme vuoto. non contiene elementi

$\{\emptyset\}$ ← insieme con 1 elemento: l'insieme vuoto.

$X \subseteq Y$ "X è un sottoinsieme di Y"
ogni elemento di X è anche elemento di Y

$X \subseteq Y$ e $X \subset Y$ sono sinonimi. $\subset \neq$ sottoinsieme proprio.

$X \subseteq X$ $\emptyset \subset X$ $X \cup Y$ $X \cap Y$

$$X \setminus Y = \{x \in X \mid x \notin Y\}.$$

$\{1,2,3\}$ $\qquad$ $\{1,1,2\}$

$\mathbb{N} = \{0,1,2,3,\dots\}$ $\qquad$ $P = \{n \in \mathbb{N} \mid$ esiste $k \in \mathbb{N}$ tale che $n = 2k\}$

$$P = \{2k \mid k \in \mathbb{N}\}$$

Pericolo! ⚠ $\qquad R = \{X \text{ insieme} \mid X \notin X\}$

$R \in R$?

Se $R \in R$ allora soddisfa $X \notin X$ e quindi $R \notin R$

Se $R \notin R$ allora soddisfa $X \notin X$ e quindi $R \in R$.

Applicazioni. Iniettività, suriettività. Invertibilità.

$f: X \to Y$ $\qquad$ $x \in X \rightsquigarrow f(x) \in Y$

X, Y: insiemi. $\qquad$ $f(x)$: immagine di x attraverso f.

Iniettività. $x \neq x' \Longrightarrow f(x) \neq f(x')$ $\qquad \forall\, x, x' \in X.$

"elementi distinti hanno immagini distinte"

"ciascun elemento di Y è immagine di al più un elemento di X"

Es: $f: \mathbb{N} \to \mathbb{N}$ $\quad f(n) = 2n$ è iniettiva.

Suriettività $\forall y \in Y$ esiste $x \in X$ t.c. $f(x) = y$.

"ogni elemento di Y è immagine di almeno un elemento di X"

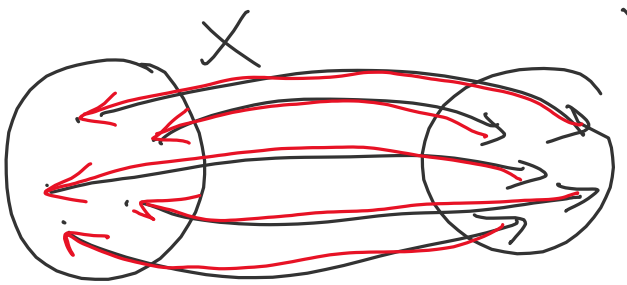
Es: $f: \mathbb{N} \to \mathbb{N}$ $\quad f(n) = 2n$ non è suriettiva

$id: \mathbb{N} \to \mathbb{N}$ $\quad id(n) = n$ è sia iniettiva che suriettiva

$f: X \to Y$

Iniettivo + suriettivo = invertibile, corrispondenza biunivoca. (isomorfismo di insiemi), biiezioni, bigezioni

"ciascun elemento di Y è immagine di esattamente un elemento di X" 1:1



$f^{-1}: Y \to X$

$f \circ f^{-1} = id_Y \qquad f^{-1} \circ f = id_X$

$f: X \to Y$

$\mathrm{Im} f \subseteq Y$

$= \{ y \in Y \mid \text{esiste } x \in X \text{ t.c. } y = f(x) \}$

$= \{ f(x) \mid x \in X \}$

Osservazione

ogni $f: X \to Y$ iniettiva è una corrispondenza biunivoca tra X e $\mathrm{Im} f \subseteq Y$

Se ho $f: X \to Y$ iniettiva, esiste allora un sottoinsieme di Y in corrispondenza biunivoca con X.

Idea: "X ha meno elementi di Y" Spoiler: non funziona benissimo!
"Y è più grande di X"

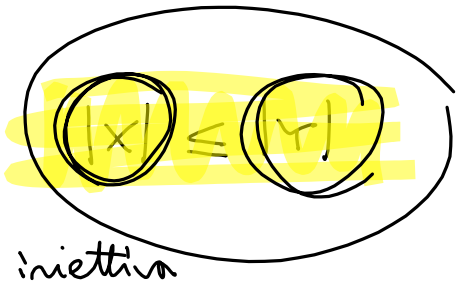
"X è una parte e Y è il tutto".
Per insiemi finiti si traduce in "X ha meno elementi di Y". meno pari

$f: \mathbb{N} \to \mathbb{N}$ iniettiva $f(n) = 2n$ $\mathrm{Im} f = P$

Un sottoinsieme infinito può essere in corrisp. biunivoca

con un suo sottoinsieme proprio $\mathbb{N} \longleftrightarrow \mathbb{P}$.

Versione affidabile



esiste $f: X \to Y$ iniettiva

$|X| \leq |X|$ $\quad id: X \to X$ è iniettiva

$|X| \leq |Y| \quad |Y| \leq |Z| \Longrightarrow |X| \leq |Z|$

↑ la composizione di applicazioni iniettive è iniettiva

? $|X| \leq |Y| \quad |Y| \leq |X| \Longrightarrow |X| = |Y|$

esiste $f: X \to Y$ invertibile.

Teorema di Bernstein – Schröder – Cantor

se esistono $f: X \to Y$ iniettiva e $g: Y \to X$ iniettiva allora esiste $h: X \to Y$ invertibile.

Altra proprietà: se X e Y sono insiemi allora o esiste $f: X \to Y$ iniettiva o esiste $g: Y \to X$ iniettiva

Argomento diagonale di Cantor

X – insieme $\quad P(X)$ – insieme delle parti $= \{$ sottoinsiemi di $X\}$ $\supseteq X$, $\supseteq \emptyset$

Teorema: non esistono applicazioni suriettive $X \to P(X)$.

Dim: Sia $f: X \to P(X)$. Mostro che non è suriettiva esibendo un sottoinsieme di X che non

è nella sua immagine.

$$Y = \{ a \in X \mid a \notin f(a) \} \subseteq X$$

Mostro che Y non è in $\inf$.

Se fosse in $\inf$, sarebbe della forma $Y = f(x)$

Tuttavia: $x \in Y \Rightarrow x \notin f(x) = Y$

$x \notin Y \Rightarrow x \in Y$

$\downarrow$ $f(x)$

Assurdo.

Conclusione: non esistono appl. invertibili $X \to P(X)$

esiste $f: X \to P(X)$ iniettiva

$x \mapsto \{x\}$

$|X| \leq |P(X)|$

$|X| \neq |P(X)|$

La cardinalità di $P(X)$ è più grande di quella di X.

Non esiste una cardinalità massima.

Posso definire un insieme attraverso le proprietà dei suoi elementi SOLO DENTRO UN ALTRO INSIEME

$$\{ x \in X \mid \text{proprietà} \}$$

$\uparrow$ insieme

I numeri naturali e gli assiomi di Peano

$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$ $\quad +, \cdot, \leq$

I numeri naturali sono caratterizzati da 3 proprietà

1. $0 \in \mathbb{N}$
2. esiste $s : \mathbb{N} \to \mathbb{N}$ iniettiva tale che $0 \notin \mathrm{Im}\, s$.
3. $X \subseteq \mathbb{N}$, $0 \in X$, $s(X) \subseteq X \Rightarrow X = \mathbb{N}$

$s(X) = \{s(x) \mid x \in X\}$

Principio di induzione

"Un sottoinsieme di $\mathbb{N}$ che contiene lo 0 e il successivo di ogni suo elemento è tutto $\mathbb{N}$.

Esempio di dim. per induzione

$0 + 1 + 2 + \dots + N = \frac{N(N+1)}{2}$ $\quad (\star_N)$ $\quad \forall N \in \mathbb{N}$.

$N = 0$ $\quad 0 \stackrel{?}{=} \frac{0(0+1)}{2}$ ✓ $(\star_0)$ $\quad \forall n \in \mathbb{N}$.

Se $(\star_N)$ è vera per $N = n$ è vera anche per $N = n+1$

$0 + 1 + 2 + \dots + n = \frac{n(n+1)}{2}$ $\quad \star_n$ lo so

$\underbrace{0 + 1 + 2 + \dots + n}_{=} + (n+1) \stackrel{?}{=} \frac{(n+1)(n+2)}{2}$ $\quad \star_{n+1}$ ✓

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

$X = \{n \in \mathbb{N} \mid (\star)_n \text{ è vera}\}$

$0 \in X$ (base dell'induzione) $\quad$ $n \in X \Rightarrow n+1 \in X$ (passo induttivo; ipotesi induttiva; $n+1 = S(n)$)

$\Rightarrow X = \mathbb{N}$ cioè $(*)_n$ è vero per ogni $n \in \mathbb{N}$.

Principio di buon ordinamento

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

Esiste una versione del principio di induzione detta induzione forte.

Sostituisco $n \in X \Rightarrow n+1 \in X$ con

$0, 1, 2, \dots, n \in X \Rightarrow n+1 \in X$

Il principio di buon ordinamento segue dal principio di induzione

$U \subseteq \mathbb{N}$ $\quad$ $\emptyset \neq U$ $\quad$ Voglio mostrare che ha elemento minimo.

Es: $U \subseteq \mathbb{N}$ senza elemento minimo e mostro che $U = \emptyset$.

Dim: $X = \mathbb{N} \setminus U$ $\quad$ $0 \in X$? Sì, perché se invece $0 \in U$ ne sarebbe l'elemento minimo.

$0, 1, 2, \dots, n \in X$ (non stanno in U) $\quad$ È vero che anche $n+1 \in X$?

$n+1$ può stare in U?

No perché ne sarebbe l'elemento

$n+1 \in X$

Per induzione forte $X = \mathbb{N} \Longrightarrow U = \emptyset$.

$\mathbb{N} \setminus U$

Dim per induzione
Dim per induzione forte
Dim per minimo controesempio
Dim per discesa infinita

sono equivalenti

A partire dagli assiomi di Peano si costruiscono tutte le strutture aggiuntive di $\mathbb{N}$ e si dimostrano tutte le proprietà ben note.

$+, \cdot, \leq$

$0 + a = a + 0 = a$ El neutro

$a + b = b + a$ comm

$(a+b)+c = a+(b+c)$ ass

$1 = s(0)$

$0 \cdot a = a \cdot 0 = 0$ ← 0 assorbe

$1 \cdot a = a \cdot 1 = a$ el. neutro

$a \cdot b = b \cdot a$ comm

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ass.

$a \cdot (b+c) = a \cdot b + a \cdot c$ $(a+b) \cdot c = a \cdot c + b \cdot c$ distr.

$a + c = b + c \iff a = b$ cancell.

$ac = bc,\ c \neq 0 \iff a = b$

$\leq$ è una rel. d'ordine totale ← prox. volta.

$0 \leq a$

$a \leq 0 \Longrightarrow a = 0$

$b = a + 1 \longrightarrow a = b$

$a \leq b < a+1 \longrightarrow$ $a = b$

$a \leq a+b$

$a \leq c \Longrightarrow$ esiste b t.c. $c = a+b$ " $b = c-a$ "

$a \leq b \Longrightarrow a+c \leq b+c$

$a \leq c,\ b \leq d \Longrightarrow a+b \leq c+d$

$b \neq 0 \Longrightarrow a \leq ab$

$ab = 0 \Longrightarrow a = 0$ opp $b = 0$

$b \leq c \Longrightarrow ab \leq ac$

$a \neq 0 \quad ab \leq ac \Longrightarrow b \leq c$

$a \leq c,\ b \leq d \Longrightarrow ab \leq cd$

$ab = 1 \Longrightarrow a = b = 1.$