Fondamenti di Informatica

per la Sicurezza

a.a. 2003/04

◇ Aspetti matematici dell'Informatica ◇

Stefano Ferrari

Università degli Studi di Milano

Dipartimento di Tecnologie dell'Informazione

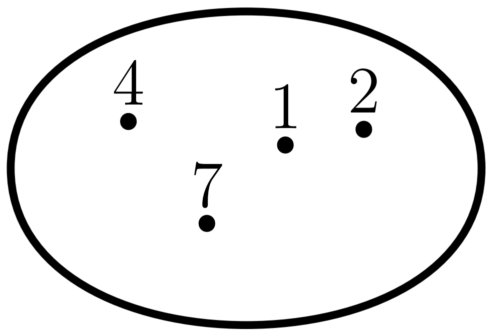
La teoria degli insiemi è il fondamento della matematica

Insieme: Collezione *arbitraria* di *elementi* reali e immaginari

Esempi:

- $\{1, 2, 4, 7\}$ descrizione *estensionale*
- $\{x \mid x \leq 5\}$ descrizione *intensionale*

Descrizione grafica di un insieme



diagrammi di Venn

grafi cartesiani

Insiemi particolari

Insieme universo: $\mathcal{U}$ contiene ogni elemento

Insieme vuoto: $\emptyset = \{\}$ non contiene alcun elemento

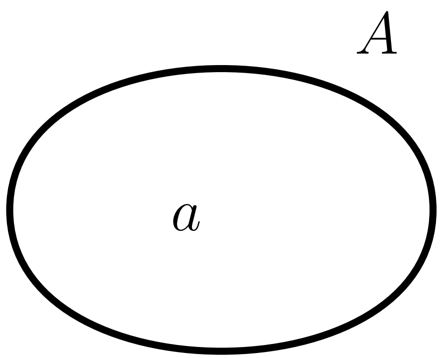
L'insieme universo deve essere definito all'inizio di ogni trattazione.

Esempio: $A = \{$numeri minori di 3$\}$

- $A_1 = \{$numeri *naturali* minori di 3$\}$ $\Leftrightarrow$ $\mathcal{U} \equiv \mathbb{N}$
- $A_2 = \{$numeri *interi* minori di 3$\}$ $\Leftrightarrow$ $\mathcal{U} \equiv \mathbb{Z}$
- $A_3 = \{$numeri *reali* minori di 3$\}$ $\Leftrightarrow$ $\mathcal{U} \equiv \mathbb{R}$

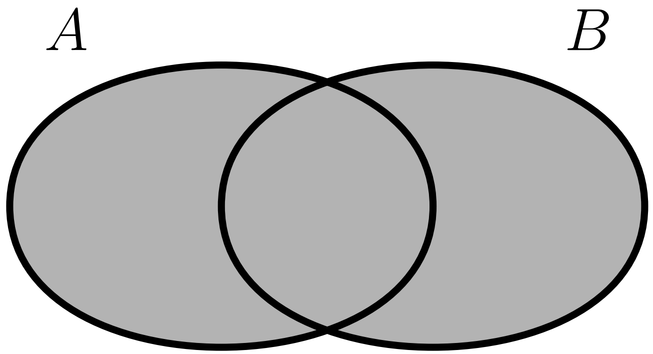
Appartenenza $\in$**,** indica che un elemento appartiene ad un dato insieme:

$$a \in A$$



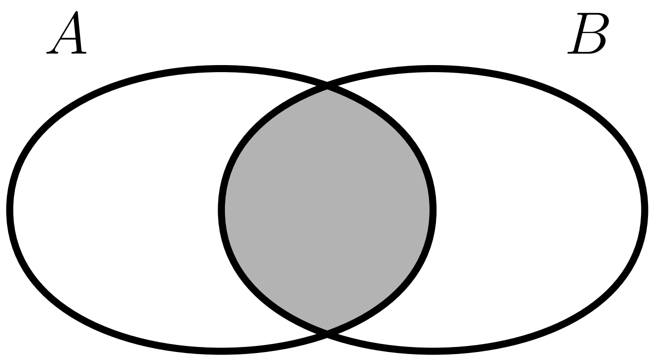
Unione $\cup$**,** compone due insiemi considerando gli elementi di entrambi:

$$A \cup B$$



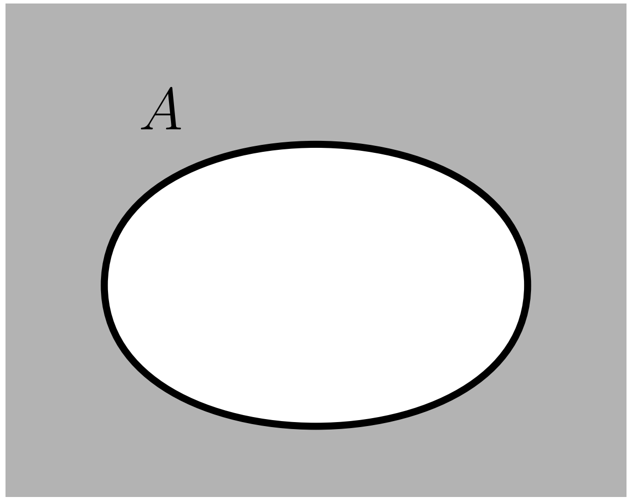
Intersezione $\cap$**,** compone due insiemi considerando solo gli elementi comuni:

$$A \cap B$$



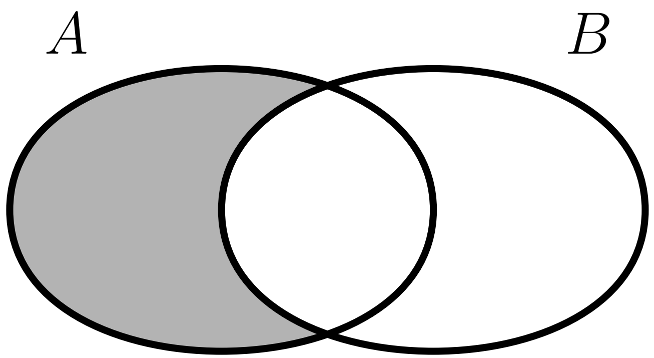
Complemento $-$**,** è l'insieme composto da tutti gli elementi che non appartengono all'insieme dato:

$$-A$$



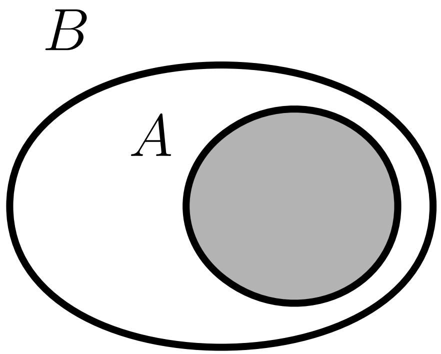
Differenza $\backslash$, compone due insiemi considerando gli elementi del primo che non appartengono al secondo:

$$A \backslash B$$



Sottoinsieme $\subseteq$, indica che ogni elemento del primo insieme appartiene anche al secondo:

$$A \subseteq B$$



Proprietà degli operatori

Idempotenza

$$A \cup A = A \quad \text{e} \quad A \cap A = A$$

Commutatività

$$A \cap B = B \cap A \quad \text{e} \quad A \cup B = B \cup A$$

Associatività

$$A \cap (B \cap C) = (A \cap B) \cap C$$

e

$$A \cup (B \cup C) = (A \cup B) \cup C$$

Proprietà degli operatori (2)

Distribuitività

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

e

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Assorbimento

$$A \cap (A \cup B) = A \quad \text{e} \quad A \cup (A \cap B) = A$$

Doppio complemento

$$\overline{\overline{A}} = A$$

Leggi di De Morgan

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{e} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

Descrizione di un insieme

Ricorsiva o induttiva

$$A = \{x \,|\, x = 1 \text{ o } x = 2 + y, \quad y \in A\}$$

Servono:

- elementi base
- operazioni per individuare i nuovi elementi in base ad alcuni elementi che già appartengono all’insieme

L’insieme descritto è dato dalla *chiusura* dell’insieme base rispetto alle operazioni della regola ricorsiva.

Si definisce *insieme delle parti* (o *insieme potenza*) dell'insieme A, l'insieme $\wp(A)$ costituito da tutti i sottoinsiemi di A:

$$\wp(A) = \{X \mid X \subset A\}$$

Esempio:

$$A = \{a,\, b\} \quad \Rightarrow \quad \wp(A) = \{\emptyset,\, \{a\},\, \{b\},\, A\}$$

Insieme $\{1, 2, 3\} \equiv \{1, 3, 2\} \equiv \{1, 3, 2, 3\}$

Bag $\{1, 2, 3\} \equiv \{1, 3, 2\} \not\equiv \{1, 3, 2, 3\}$

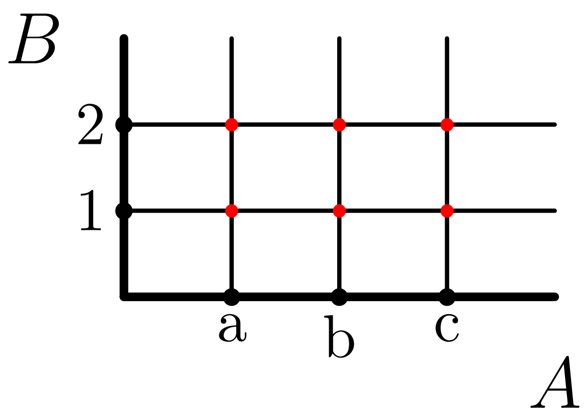
Sequenza $\langle 1, 2, 3\rangle \not\equiv \langle 1, 3, 2\rangle \not\equiv \langle 1, 3, 2, 3\rangle$

Prodotto cartesiano

Il prodotto cartesiano $A \times B$ degli insiemi A e B è formato dalla combinazione degli elementi di A e B.

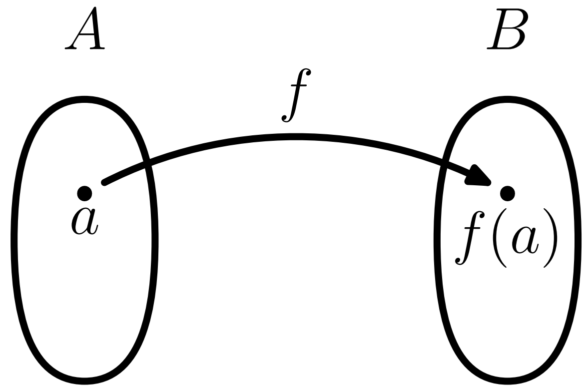
Es.:

$$A = \{a,\, b,\, c\} \qquad B = \{1,\, 2\}$$



$$A \times B = \{\langle a,\, 1\rangle,\, \langle a,\, 2\rangle,\, \langle b,\, 1\rangle,\, \langle b,\, 2\rangle,\, \langle c,\, 1\rangle,\, \langle c,\, 2\rangle\}$$

Una funzione $f : A \rightarrow B$ è una regola per abbinare ad ogni elemento a dell'insieme A un elemento $f(a)$ dell'insieme B.

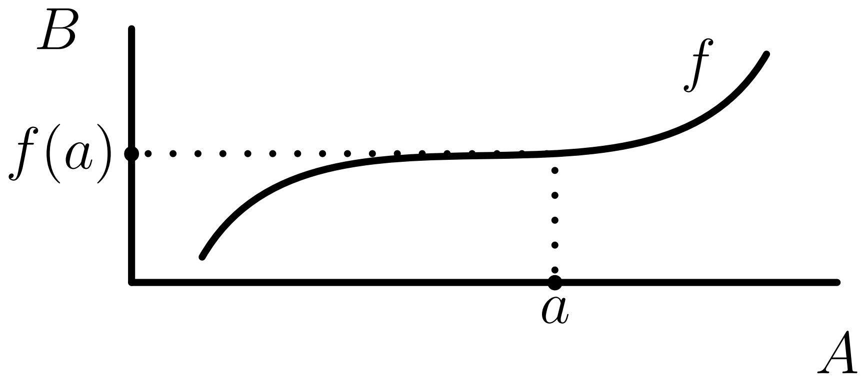


A è il *dominio* di f

B è il *codominio* di f

a è detto *argomento*

$f(a)$ è la sua *immagine*



Funzioni: esempi

$$square : \mathbb{Z} \rightarrow \mathbb{N}, \qquad square(x) = x^2$$

Esiste x tale per cui $square(x) = 5$?
Per quale x vale $square(x) = 9$?

$$abs : \mathbb{Z} \rightarrow \mathbb{N}, \qquad abs(x) = \begin{cases} +x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

$$g : \mathbb{Z} \rightarrow \mathbb{N}, \qquad g(x) = 2x^2 + x$$

$$I : \mathcal{U} \rightarrow \mathcal{U}, \qquad I(u) = u$$

Una funzione si dice

suriettiva se ogni elemento del codominio è immagine di un elemento del dominio

iniettiva se ad elementi distinti del dominio corrispondono immagini distinte nel codominio

biiettività se la funzione è suriettiva ed iniettiva

Isomorfismo

Una funzione biiettiva $f : A \rightarrow B$ si dice *isomorfismo* tra A e B.
L'isomorfismo comporta:

- corrispondenza uno ad uno tra gli elementi di A e quelli di B
- esistenza della funzione *inversa* $f^{-1} : B \rightarrow A$

Composizione di funzioni

La *composizione* di due funzioni è l'applicazione di una al risultato dell'altra:

$f : A \rightarrow B$ e $g : B \rightarrow C$

$h : A \rightarrow C, \qquad h(a) = g(f(a))$

La composizione di una funzione e della sua inversa dà la funzione identità, I:

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

Funzioni a più argomenti

$f : A \longrightarrow B$	funzione unaria (*monadica*)
$f : A_1 \times A_2 \longrightarrow B$	funzione binaria (*diadica*)
$f : A_1 \times A_2 \times A_3 \longrightarrow B$	funzione ternaria (*triadica*)
$f : A_1 \times \cdots \times A_n \longrightarrow B$	funzione n-aria (n-*adica*)