Lezione: Nozioni Perliminari

Logica: Una proposizione è un'affermazione dichiarativa che è vera o falsa.

Esempio: Un pinguino è un animale.

Domande, opinioni e comandi non sono proposizioni.

Connettivi Logici: Siano P, Q, R proposizioni.

Negazione: $\neg P$ è vera se e solo se P è falsa.

Esempio: P = I pinguini possono volare.
Questa proposizione è falsa. Quindi $\neg P$ è vera.

Tavola di verità:

P	$\neg P$
V	F
F	V

Congiunzione: $P \wedge Q$ è vera se e solo se P è vera e Q è vera.

Esempio: P= I pinguini possono volare. Q= I pinguini sono carnivori.
R = I pinguini possono nuotare.

Allora: $P \wedge Q = F$, $P \wedge R = F$, $Q \wedge R = V$

Tavola di verità:

P	Q	$P \wedge Q$
F	F	F
F	V	F
V	F	F
V	V	V

Disgiunzione: $P \vee Q$ è vera se e solo se P è vera oppure Q è vera.
Nota bene: $P \vee Q$ è vera se P è vera e Q è vera.

Esempio: P, Q, R come nell'esempio precedente.

Allora: $P \vee Q = V$, $P \vee \neg Q = F$, $Q \vee R = V$

Tavola di verità:

P	Q	$P \vee Q$
F	F	F
F	V	V
V	F	V
V	V	V

Implicazione: $P \implies Q$ a meno che P sia vera e Q sia falsa

Esempio: P = Se i maiali potessero volare. Q= qualsiasi proposta.

Allora $P \implies Q$ è vera perché P è falsa.

(essere continuato)

Nota: $P \implies Q$ è anche chiamato "implicazione logica" per distinguerlo dal significato colloquiale di "implicazione".

Tavola di verità:

P	Q	$P \implies Q$
F	F	V
F	V	V
V	F	F
V	V	V

Altri modi per dire $P \implies Q$ sono:
(i) Se P allora Q
(ii) P è condizione sufficiente per Q.
(iii) Q è condizione necessaria per P.

Esempio: P = Oggi è Pasqua. Q= Domani è lunedì.
Allora $P \implies Q$.

Coimplicazione (o doppia implicazione): $P \iff Q$ significa "P se e sole se Q"

Esempio: P= Oggi è lunedì. Q= Domani è martedì.
Allora: $P \iff Q$

Tavola di verità:

P	Q	$P \iff Q$
F	F	V
F	V	F
V	F	F
V	V	V

Altri modi per dire $P \iff Q$ sono:
(i) P se e sole se Q
(ii) P è necessaria e sufficiente per Q

Attenzione: P se Q significa $Q \implies P$.

Insiemi:

Intuitivamente, un insieme S è un insieme di oggetti distinti, chiamati elementi di S.
$s \in S$ è la proposizione che s è un elemento di S. La proposizione $\neg(s \in S)$ è scritto $s \notin S$.

Un insieme con un numero finito di elementi può essere descritto elencando i suoi elementi.

$$A = \{1, 2, 3, 4, 5\}$$

Il insieme vuoto, scritto $\emptyset$ oppure $\{\}$, è l'insieme senza elementi. In particolare, se A è un insieme e $a \in A$ allora $a \notin \emptyset$.

Definizione: Sia A un insieme. Per ogni $a \in A$ sia $P(a)$ una proposizione. Allora

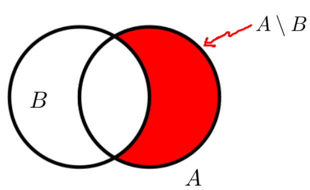
$$\{a \in A \mid P(a)\}$$

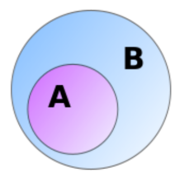
è l'insieme costituito da tutti gli elementi $a \in A$ tali che $P(a)$ è vera.

Definizione: Siano A e B insiemi. Il complemento di B in A è l'insieme

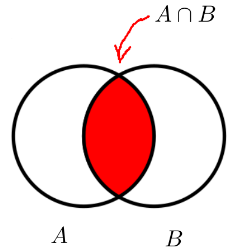
$$A \setminus B = \{ a \in A \mid a \notin B \}$$

Si dice che A è un sottoinsieme di B, scritto $A \subseteq B$, se (e sole se) $A \setminus B = \emptyset$.
Si dice che $A = B$ se (e sole se) $A \subseteq B$ e $B \subseteq A$.





$A \subseteq B$



Esempio: Sia S un insieme. Allora $\emptyset \subseteq S$ perché $s \in \emptyset$ è sempre falsa.

Definizione: Siano A e B insiemi. L'intersezione di A e B è l'insieme

$$A \cap B = \{ a \in A \mid a \in B \}$$

Esempio: Siano $A = \{m \in \mathbb{Z} \mid 2 \text{ divide } m\}$, $B = \{n \in \mathbb{Z} \mid 3 \text{ divide } n\}$. Allora,

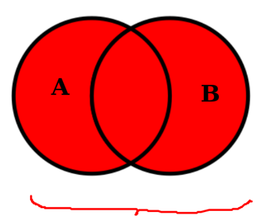
$$A \cap B = \{ q \in \mathbb{Z} \mid 6 \text{ divide } q \}$$

Esercizio: $A \cap B = \{ b \in B \mid b \in A \}$

Di solito nelle nostre discussioni, c'è un insieme ambiente U che contiene tutti gli oggetti in considerazione.

Definizione: Siano A e B sottoinsieme di U. L'unione di A e B è l'insieme

$$A \cup B = \{ u \in U \mid (u \in A) \vee (u \in B) \}$$



$A \cup B$

Esercizio: $A = (A \setminus B) \cup (A \cap B)$

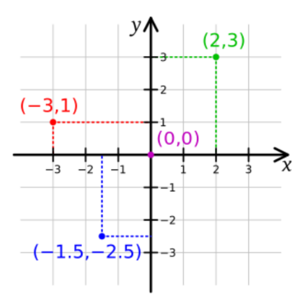
Siano A e B insiemi. Il prossimo concetto primitivo della teoria degli insiemi è il prodotto cartesiano $A \times B$ costituito da coppie ordinate

$$(a, b) \in A \times B$$

Per definizione,

$$(a, b) = (a', b') \iff (a = a') \wedge (b = b')$$

Esempio: $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ è il piano cartesiano.

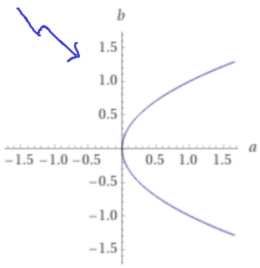


Relazioni e Funzioni

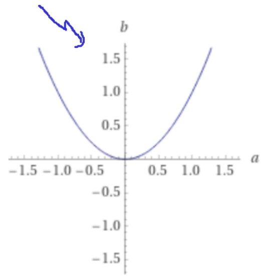
Siano A e B insiemi. Una relazione da A a B è un sottoinsieme $R \subseteq A \times B$.

Esempio: $A = B = \mathbb{R}$

$R_1 = \{(a,b) \in \mathbb{R} \times \mathbb{R} \mid b^2 = a\}$



$R_2 = \{(a,b) \in \mathbb{R} \times \mathbb{R} \mid a^2 = b\}$



Definizione: Una relazione R da A a B definisce una funzione $f : A \to B$ se (e sole se)
(i) Per ogni $a \in A$ esiste un elemento

$$(a,b) \in R$$

(ii) Se $(a,b) \in R$ e $(a,c) \in R$ allora $b = c$.
In questo caso, scriviamo $f(a) = b$.

Esempio: R_1 non soddisfa la condizione (i) perché non c'è nessun elemento della forma $(-1,b) \in R_1$.
R_1 non soddisfa la condizione (ii) perché $(1,1) \in R_1$ e $(1,-1) \in R_1$.
R_2 soddisfa sia condizione (i) che (ii). La funzione associatae è $f(a) = a^2$.

Definizione: Una funzione $f : X \to Y$ si dice:
(i) iniettiva se $f(x) = f(x') \iff x = x'$
(ii) suriettiva se per ogni $y \in Y$ existe $x \in X$ tale che $f(x) = y$.
(iii) biunivoca se f sia iniettiva e suriettiva.

Esempio:
(i) $f(x) = e^x$ è una funzione iniettiva $\mathbb{R} \to \mathbb{R}$. Questa funzione non suriettiva perché e^x è sempre positivia.
(ii) $g(x) = \sin(x)$ è una funzione suriettiva $\mathbb{R} \to [-1,1]$. Questa funzione non iniettiva perché $\sin(x + 2\pi) = \sin(x)$.
(iii) $h(x) = x^3$ è una funzione biunivoca $\mathbb{R} \to \mathbb{R}$.

Lemma: Una funzione $f : X \to Y$ ha una funzione inversa $g : Y \to X$ se e solo se f è biunivoca.

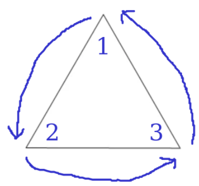
Lemma: Siano X e Y insiemi finiti con lo stesso numero di elementi. Allora, le seguenti sono equivalenti:
(i) $f : X \to Y$ è iniettiva.
(ii) $f : X \to Y$ è suriettiva.
(iii) $f : X \to Y$ è biunivoca.

$\boxed{\text{Permutazione}}$

Sia X un insieme. Una permutazione di X è una funzione biunivoca $f : X \to X$

Esempio: $X = \{1, 2, 3\}$, $f(1) = 2$, $f(2) = 3$, $f(3) = 1$

Esempio: Sia X l'insieme dei vertici di un poligono P. Sia $f : P \to P$ una simmetria.
Allora, $f : X \to X$ è biunivoca. Quindi $f : X \to X$ è una permutazione di X.



$f(1) = 2$, $f(2) = 3$, $f(3) = 1$

Esempio: Siano $f, g : X \to X$ permutazioni. Allora, la funzione composta $h = f \circ g$ è una permutazione.

Lemma : Siano $f : X \to Y$ e $g : Y \to Z$ funzioni e $h = f \circ g$. Allora,
(i) f, g iniettiva $\implies h$ iniettiva.
(ii) f, g suriettiva $\implies h$ suriettiva.
(iii) f, g biunivoca $\implies h$ biunivoca.

Esercizio: Dimostrare il lemma

Dimostrazione per assurdo

Un modo per dimostrare che una proposizione P è vera è mostrare che assumere che $\neg P$ sia vero porta a una contraddizione. Più precisamente, esiste una proposizione Q tale che

$$\neg P \implies Q \wedge (\neg Q) \quad \text{è vero}$$

Poiché $Q \wedge (\neg Q)$ è sempre falsa, ne segue che P è vera.

Teorema (Euclide): Esistono infiniti numeri primi.
Dimonstrazione: Sia S l'insieme di tutti i numeri primi. Supponiamo che S sia finito e che sia m il prodotto degli elementi di S. Chiaramente nessun elemento di S può dividere $m+1$. Quindi, $m+1$ è primo o ha un fattore primo che non è contenuto in S. Ma questo contraddice l'ipotesi che S sia l'insieme di tutti i numeri primi.

Teorema Fondamentale dell'aritmetica: Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.

Corollario: Se p è un numero primo e n è numero naturale tale che p divide n^2 allora p divide n.

Teorema (La scuola pitagorica): $\sqrt{2}$ non è un numero razionale.

Dimonstrazione: Supponiamo che

$$\sqrt{2} = \frac{a}{b}$$

dove a e b sono numeri naturali senza fattore comune. Allora

$$2 = \frac{a^2}{b^2} \implies 2b^2 = a^2$$

e quindi 2 divide a^2. Per il collorario, 2 divide a. Scrive $a = 2c$. Allora,

$$2b^2 = a^2 = (2c)^2 = 4c^2 \implies b^2 = 2c^2$$

Per il collorario, 2 divide b. Così, 2 è un fattore comune di a e b. Ciò contraddice l'ipotesi che a e b non abbiano un fattore comune.

Come volevasi dimostrare

Principio d'induzione

Sia m un numero naturale. Per ogni numero naturale $n \geq m$, sia $P(n)$ una proposizione.
Per mostrare che $P(n)$ è vera per ogni numero naturale $n \geq m$, è sufficiente mostrare:
(a) $P(m)$ è vera.
(b) Se $P(n)$ è vera allora $P(n+1)$ è vera.

Varianti: La parte (b) può essere sostituita da
(b') Se $P(m), \ldots, P(n)$ sono vere allora $P(n+1)$ è vera.

Nota: Il Teorema Fondamentale dell'Aritmetica è un esempio di teorema dove si usa (b') invece di (b). In questo corso, si usa spesso (b') per dimostrare con induzione sulla dimensione.

Esempio: La somma dei primi n numeri naturali è $\frac{n(n+1)}{2}$.

$$m = 1, \qquad P(n) : \quad \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

(a) $P(1) = 1 = \frac{(1)(1+1)}{2}$ è vera.

(b) $$P(n) = \frac{n(n+1)}{2} \implies P(n+1) = \sum_{k=1}^{n+1} k = (n+1) + \sum_{k=1}^{n} k$$
$$= (n+1) + \frac{n(n+1)}{2} = \frac{2(n+1) + n^2 + n}{2}$$
$$= \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

Quindi, P(n+1) è vero. Questo completa la dimostrazione per induzione.