Capitolo 1: Concetti matematici di base

Insiemi

$x \in A \iff x$ é elemento dell'insieme A.
$B \subseteq A \iff B$ é un sottoinsieme di A.
$B \subset A \iff B$ é un sottoinsieme proprio di A.
A costituito da n elementi $\iff |A| = n$ é la sua cardinalitá.
$\emptyset$ é l'insieme vuoto; $|\emptyset| = 0$.

Definizione 1 *L'insieme composto da tutti i sottoinsiemi di un insieme A si dice* insieme delle parti *di A, e si indica con $\mathcal{P}(A)$ o con 2^A.*

Lemma 2 $|A| = n \Longrightarrow |\mathcal{P}(A)| = 2^n$.

Definizione 3 *Gli insiemi A e B sono* uguali *$(A = B)$ se ogni elemento di A é anche elemento di B, e viceversa.*

Come dimostrare proprietá su insiemi finiti? Si verifica la proprietá per ogni elemento dell'insieme.
Come dimostrare proprietá su insiemi infiniti? Non si puó verificare la proprietá per ogni elemento dell'insieme, ma si usa il **Principio di induzione matematica**.

Data una proposizione $P(n)$ definita per un generico numero naturale n, essa é vera per tutti i naturali se

- $P(0)$ é vera (base dell'induzione)

- per ogni naturale k, $P(k)$ vera (ipotesi induttiva) implica $P(k+1)$ vera (passo induttivo).

Esempio 4

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Dimostrazione

passo base:

$$\sum_{i=0}^{0} i = \frac{0(0+1)}{2} = 0$$

passo induttivo:

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

Una versione piú generale

Data una proposizione $P(n)$ definita per $n \geq n_0$, essa é vera per tutti gli $n \geq n_0$ se

- $P(n_0)$ é vera (base dell'induzione)

- per ogni naturale $k \geq n_0$, $P(k)$ vera (ipotesi induttiva) implica $P(k+1)$ vera (passo induttivo).

Esempio 5

$$\sum_{i=0}^{n-1} 2^i = 2^n - 1 \ \textit{per} \ n \geq 1$$

$P(n)$ vera per ogni $n \geq n_0$ (versione generale) $\Longleftrightarrow$
$P_{n_0}(n) \equiv P(n - n_0)$ vera per ogni naturale.

Principio di induzione completa

Data una proposizione $P(n)$ definita per $n \geq n_0$, essa é vera per tutti gli $n \geq n_0$ se

- $P(n_0)$ é vera (base dell'induzione)

- per ogni naturale $k \geq n_0$, $P(i)$ vera per ogni i, $n_0 \leq i \leq k$ (ipotesi induttiva), implica $P(k+1)$ vera (passo induttivo).

Esempio 6 *Dimostrare che ogni intero $n \geq 2$ é divisibile per un numero primo.*

Esempio 7 *Data la sequenza di Fibonacci ($F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$), dimostrare che per ogni $n \geq 2$ e per ogni k, $1 \leq k \leq n$ si ha $F_n = F_k F_{n-k} + F_{k-1} F_{n-(k+1)}$.*

Teorema 8 *Per ogni proprietá P il principio di induzione matematica ed il principio di induzione completa sono equivalenti.*

Relazioni e funzioni

Definizione 9 $A \times B = \{\langle x, y\rangle | x \in A \wedge y \in B\}$ *si dice* prodotto cartesiano *di* A *e* B *(notaz:* $A^n = A \times \ldots \times A$*).*

Definizione 10 *Una relazione* n*-aria* R *su* $A_1, A_2, \ldots, A_n$ *é un sottoinsieme del prodotto cartesiano* $A_1 \times \ldots \times A_n$*.*
Il generico elemento di R *é indicato con* $\langle a_1, \ldots, a_n\rangle$*, oppure con il simbolo* $R(\langle a_1, \ldots, a_n\rangle)$*.*
n *si dice* aritá *della relazione (se* $n = 2$ *allora* aRb*).*

Esempio 11 *Che relazioni sono le seguenti?*
$R = \{\langle x, y\rangle \in \mathbb{N}^2 | \exists z \in \mathbb{N}(z \neq 0 \wedge x + z = y)\} \subseteq \mathbb{N}^2$.
$R = \{\langle x, y\rangle | x^2 = y)\} \subseteq \mathbb{N}^2$.

Definizione 12 *Una relazione* $R \subseteq A^2$ *si dice* relazione d'ordine *se per ogni* $x, y, z \in A$ *valgono le seguenti proprietá:*

- $\langle x, x \rangle \in R$ *(riflessivitá)*
- $\langle x, y \rangle \in R \wedge \langle y, x \rangle \in R \Longleftrightarrow x = y$ *(antisimmetria)*
- $\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \Longleftrightarrow \langle x, z \rangle \in R$ *(transitivitá)*

A *si dice* insieme parzialmente ordinato.

Definizione 13 *Una relazione d'ordine* $R \subseteq A^2$ *tale che* $\langle a, b \rangle \in A^2 \Longleftrightarrow aRb \vee bRa$, *si dice* relazione di ordine totale.

Esempio 14 *"*$\leq$*" é una relazione d'ordine totale su* $\mathbb{N}$*?*

Definizione 15 *Una relazione* $R \subseteq A^2$ *si dice* relazione d'equivalenza *se per ogni* $x, y, z \in A$ *valgono le seguenti proprietá:*

- $\langle x, x \rangle \in R$ *(riflessivitá)*
- $\langle x, y \rangle \in R \Longleftrightarrow \langle y, x \rangle \in R$ *(simmetria)*
- $\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R \Longleftrightarrow \langle x, z \rangle \in R$ *(transitivitá)*

Esempio 16 $E = \{\langle u, v \rangle, \langle p, q \rangle | uq = pv)\}$ *é una relazione d'equivalenza.*

Un insieme A su cui é definita una relazione d'equivalenza R si partiziona in sottoinsiemi (*classi d'equivalenza*); ogni classe contiene solo elementi fra loro equivalenti.

L'insieme delle classi d'equivalenza di A rispetto a R di chiama *insieme quoziente* ($[a] \in A/R$).

Il numero di elementi in A/R si dice *indice* di R (ind(R)).

Esempio 17 *Dato un intero k, definiamo la relazione d'equivalenza* congruenza modulo k*:*

$n \equiv_k m \iff$ *esistono* q, q', r, *con* $0 \leq r < k$, *tali che* $\begin{cases} n = qk + r, \\ m = q'k + r. \end{cases}$

Le classi d'equivalenza sono dette classi resto *rispetto alla divisione per k.*

Definizione 18 *Dato un insieme finito* V *ed una relazione binaria* $E \subseteq V \times V$*, la coppia* $\langle V, E \rangle$ *si definisce* grafo orientato*.*
Se la relazione E *é simmetrica il grafo si dice* non orientato*.*

Operazioni tra relazioni

unione: $R_1 \cup R_2 = \{\langle x, y \rangle | \langle x, y \rangle \in R_1 \vee \langle x, y \rangle \in R_2\}$.

complemento: $\overline{R} = \{\langle x, y \rangle | \langle x, y \rangle \notin R\}$.

chiusura transitiva: $R^+ = \{\langle x, y \rangle | \exists y_i, \ldots, y_n \in A, n \geq 2,$
$y_1 = x, y_n = y, \langle y_i, y_{i+1} \rangle \in R, i = \ldots, n-1\}$.

chiusura transitiva e riflessiva: $R^* = R^+ \cup \{\langle x, x \rangle | x \in A\}$.

Esempio 19 *Sia $G = \langle V, E \rangle$ un grafo orientato. Sia R la relazione tale che xRy sse $x = y$ oppure posso raggiungere y da x percorrendo gli archi. R é la chiusura transitiva e riflessiva di E?*

Esempio 20 *Dimostrare che dato un insieme finito V ed una qualsiasi relazione binaria simmetrica E definita su V^2, E^* è una relazione di equivalenza.*

Esempio 21 *Sia $G = \langle V, E \rangle$ un grafo. Cosa rappresentano le classi d'equivalenza del grafo $G = \langle V, E^* \rangle$?*

Definizione 22 *Si dice che* $R \subseteq X_1 \times \ldots \times X_n$ *é una* relazione funzionale *tra una* $(n-1)$*-pla di elementi e l'*n*-esimo elemento se* $\forall \langle x_1, \ldots, x_{n-1} \rangle \in X_1 \times \ldots \times X_{n-1}$ *esiste al piú un elemento* $x_n \in X_n$ *tale che* $\langle x_1, \ldots, x_n \rangle \in R$.

Definizione 23 *Si definisce* funzione o applicazione *la legge che all'elemento* $\langle x_1, \ldots, x_{n-1} \rangle \in X_1 \times \ldots \times X_{n-1}$ *associa, se esiste, l'unico elemento* $x_n \in X_n$ *tale che* $\langle x_1, \ldots, x_n \rangle \in R$.

Notazioni: $f(x_1, \ldots, x_{n-1}) = x_n$;
$f : X_1 \times \ldots \times X_{n-1} \longmapsto X_n$;
dominio $\equiv dom(f) = X_1 \times \ldots \times X_{n-1}$
codominio $\equiv cod(f) = X_n$

Definizione 24 *Si definisce* dominio di definizione *della funzione* f *il sottoinsieme di* $dom(f)$*, denotato con* $def(f) =$
$\{\langle x_1, \ldots, x_{n-1}\rangle \in dom(f) | \exists x_n \in cod(f), f(x_1, \ldots, x_{n-1}) = x_n\}$.

Definizione 25 *Si definisce* immagine *della funzione* f *il sottoinsieme di* X_n*, denotato con* $imm(f) =$
$\{x_n \in X_n | \exists \langle x_1, \ldots, x_{n-1}\rangle \in dom(f), f(x_1, \ldots, x_{n-1}) = x_n\}$.

Definizione 26 *Dato un generico elemento* $x_n \in cod(f)$*, si dice* controimmagine *di* x_n *l'insieme* $f^{-1}(x_n) =$
$\{\langle x_1, \ldots, x_{n-1}\rangle | \langle x_1, \ldots, x_{n-1}\rangle \in def(f) \wedge f(x_1, \ldots, x_{n-1}) = x_n\}$.

Definizione 27 *Se* $def(f) = dom(f)$ *la funzione si dice* totale.
Se $def(f) \subseteq dom(f)$ *la funzione si dice* parziale.

Definizione 28 *Se* $imm(f) = cod(f)$ *la funzione si dice* suriettiva.

Definizione 29 *Se una funzione fa corrispondere ad elementi diversi del dominio di definizione elementi diversi del codominio, essa si dice* iniettiva.

Definizione 30 *Se una funzione é suriettiva, iniettiva e totale, allora la funzione si dice* biettiva.

Teorema 31 *(Pigeonhole principle) Dati due insiemi finiti* A *e* B *tali che* $0 < |B| < |A|$*, non esiste alcuna funzione iniettiva totale* $f : A \longmapsto B$.

Cardinalitá di insiemi infiniti e numerabilitá

Definizione 32 *Due insiemi si dicono* equinumerosi *se esiste una biiezione fra essi (é una relazione di equivalenza).*

Definizione 33 *Dato un insieme finito A, si ha*

$$|A| = \begin{cases} 0 & \text{se } A = \varnothing, \\ n & \text{se } A \text{ é equinumeroso a } \{0,1,\ldots,n\text{-}1\}. \end{cases}$$

Definizione 34 *Un insieme si dice* numerabile *se é equinumeroso a $\mathbb{N}$ ($|A| = \aleph_0$). Un insieme si dice* contabile *se é finito o numerabile.*

Teorema 35 *Se un insieme A é equinumeroso ad un insieme B, con $B \subseteq C$, e C é contabile, allora anche A é contabile.*

Esempio 36 *L'insieme $\mathbb{Z}$ é numerabile (cioé $|\mathbb{Z}| = \aleph_0$); infatti i suoi elementi possono essere messi in corrispondenza biunivoca con $\mathbb{N}$, con la biiezione $f : \mathbb{Z} \longmapsto \mathbb{N}$ tale che*

$$f(i) = \begin{cases} -2i & \text{se } i \leq 0, \\ 2i - 1 & \text{se } 1 \geq 0. \end{cases}$$

Nota che $\mathbb{N} \subset \mathbb{Z}$, ma i due insiemi sono equinumerosi. Puó capitare per insiemi finiti?

Esempio 37 *L'insieme $\mathbb{N}^2$ é numerabile; la corrispondenza biunivoca é data dalla funzione coppia di Cantor*

$$p(i, j) = \frac{(i + j)(i + j + 1)}{2} + i.$$

Insiemi non numerabili

Abbiamo introdotto insiemi numerabili. Esistono insiemi non numerabili?

Per costruirli usiamo la *tecnica di diagonalizzazione* (di Cantor): data una lista di oggetti, si crea un oggetto che non appartiene alla lista mediante un procedimento che lo costruisce garantendo che esso sia diverso da tutti gli oggetti nella lista.

Teorema 38 *L'insieme* $\mathbb{R}$ *dei reali non é numerabile.*

Teorema 39 *L'insieme delle parti di* $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, *non é numerabile.*