Elementi di Algebra e di Matematica Discreta

Insiemi, relazioni

Cristina Turrini
Alice Garbagnati

UNIMI - 2021/2022

index

discreto : opposto di continuo, "separato",
per noi, molto spesso: finito.

Nel corso, due capitoli:

- Rudimenti di Matematica del discreto
  - relazioni tra insiemi (relazioni in un insieme, funzioni)
  - strutture algebriche (gruppi, anelli, campi)
  - proprietà dei numeri interi
  - Algoritmo di divisione
- Algebra Lineare
  - sistemi di equazioni lineari e algortimi di risoluzione
  - matrici
  - spazi vettoriali
  - applicazioni lineari

index

Notazioni

Insieme: concetto primitivo, che non si definisce (si ritiene non a priori).

$A, B, \ldots X \ldots$ insiemi; $a, b, \ldots x \ldots$ elementi

- Se a e' un elemento di A diremo che a appartiene a A e scriveremo $a \in A$. Altrimenti diremo che a non appartiene ad A e scriveremo $a \notin A$;
- Se A e B sono due insiemi, diremo che B e' contenuto in A e scriveremo $B \subset A$ (o $B \subseteq A$) se $\forall b \in B$, $b \in A$; se $B \subset A$ diremo che B e' un sottoinsieme di A;
- Dati due insiemi A e B diremo che essi sono uguali ($A = B$) se $B \subseteq A$ e $A \subseteq B$ (e quindi se ogni elemento di B e' contenuto in A e ogni elemento di A e' un elemento di B);
- L'insieme privo di elementi, e' chiamato insieme vuoto e indicato con $\emptyset$
- $\emptyset \subset A, \quad \forall A.$

Siano A e B due sottoinsiemi di X.

- l'intersezione di A e B e' $A \cap B := \{x \in X \text{ tali che } x \in A \text{ e } x \in B\}$;
- l'unione di A e B e' $A \cup B := \{x \in X \text{ tali che } x \in A \text{ oppure } x \in B\}$;
- il complementare di A e' $A^c := \{x \in X \text{ tali che } x \notin A\}$;
- la differenza fra A e B e' $A - B := \{x \in X \text{ tali che } x \in A \text{ e } x \notin B\}$;

Osservazione: valgono ovviamente le seguenti proprieta':
- $A \cap B \subset A$ e $A \cap B \subset B$;
- $A \subset A \cup B$, e $B \subset A \cup B$;
- $A \cap B \subset A \cup B$.

Definizione: Dato un insieme X, l'insieme delle parti di X e'

$$P(X) := \{A \text{ tale che } A \subset X\} := \{\text{sottoinsiemi di X}\}.$$

Osserviamo che $\emptyset \in P(X)$ per ogni X.

Ci sono due modi per descrivere un insieme A,

- per elencazione: $A = \{a, b, c, \dots\}$
- per proprietà caratterizzante: $A = \{a \in X \quad | \quad P(a)\}$

Esempio Consideriamo gli insiemi:
- $A := \{0, 1, 2, 3, 4\}$
- $B := \{x \in \mathbb{N} \text{ tali che } x \leq 4\}$
- $C := \{0, 2, 4\}$
- $D := \{x \in \mathbb{N} \text{ tali che } x \text{ e' pari }\}$

Gli insiemi A e C sono dati per elencazione.

Gli insiemi B e D sono definiti tramite una proprieta' che caratterizza i loro elementi.

L'insieme B contiene un numero finito di elementi, quindi puo' anche essere dato per elencazione, infatti $A = B$.

D contiene un numero infinito di elementi. Non puo' essere dato per elencazione.

Esempio (continuazione) Osserviamo che $C \subset D$ e $C \subset A (= B)$:

$D \cap C = A \cap C = B \cap C = C$
Inoltre $A \cap D = C$

$D \cup C$ e' infinito e coincide con D, $D \cup A$ e' infinito e non coincide con D.
Calcoliamo ora l'insieme delle parti di C:

$$P(C) := \{\emptyset, \{0\}, \{2\}, \{4\}, \{0,2\}, \{0,4\}, \{2,4\}, C\}$$

Osserviamo che C ha 3 elementi e l'insieme delle parti di C ne ha $8 = 2^3$.
Se si scrivesse l'insime delle parti di A si osserverebbe che ha $32 = 2^5$ elementi e quindi osserviamo che al crescere degli elementi di un insieme cresce (molto piu' velocemente) il numero di elementi dell'insieme delle parti

Ricordiamo la seguente notazione:
$\mathbb{N}$ e' l'insieme dei numeri naturali $\mathbb{N} = \{0, 1, 2, \dots\}$,
$\mathbb{Z}$ e' l'insieme dei numeri interi (relativi) $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \dots\}$.

Esempio/Esercizio

- $X = \{x \in \mathbb{N} \quad | \quad x \text{ divide } 12\}$, $Y = \{x \in \mathbb{N} \quad | \quad x \text{ divide } 18\}$
  $X \cap Y = \{1, 2, 3, 6\}$ e $X \cup Y = \{1, 2, 3, 4, 6, 12, 9, 18\}$;
- $A = \{x \in \mathbb{Z} \mid x = 2h, h \in \mathbb{Z}\}$, $B = \{x \in \mathbb{Z} \mid x = 6k, k \in \mathbb{Z}\}$,
  dimostrare che $A \cup B = A$.

  Per mostrare l'uguaglianza bisogna mostrare che $A \subseteq A \cup B$ e
  $A \cup B \subseteq A$. La prima inclusione e' ovvia.
  $A \cup B \subseteq A$?? Occorre mostrare che $\forall x \in A \cup B$ si ha $x \in A$.
  Se $x \in A \cup B$ allora, o $x \in A$ o $x \in B$
  Nel primo caso abbiamo finito, altrimenti osserviamo che se $x \in B$,
  allora $x = 6k = 2(3k) = 2h$ con $k \in \mathbb{Z}$ e $h = 3k$, quindi $x \in A$.

Definizione Se X e' un insieme con un numero finito n di elementi, diciamo che X ha cardinalita' n e scriviamo $|X| = n$.

Proposizione Sia X un insieme finito, con $|X| = n$, allora $|P(X)| = 2^n$.

Definizione Dato un insieme X non vuoto, una *partizione* di X, è una collezione di sottoinsiemi non vuoti A_i di X, $i \in I$, tali che:

- $A_i \cap A_j = \emptyset, \forall \ i \quad \neq j$ (gli A_i sono insiemi disgiunti);
- $X = \cup_{i \in I} A_i$ (gli A_i ricoprono X.).

Esempio $X = \mathbb{N}$,
$A_1 = \{\text{numeri pari}\}, A_2 = \{\text{numeri dispari}\}$,
$\{A_1, A_2\}$ e' una partizione di X.

Esempio $X = \mathbb{N}$,
$A_1 = \{x \in X \text{ tali che } x \leq 5\}, A_2 = \{x \in X \text{ tali che } x > 5\}$,
$\{A_1, A_2\}$ e' una partizione di X.

Esempio $X = \mathbb{N}$,
$A_1 = \{x \in X \text{ tali che } x \leq 5\}, A_2 = \{x \in X \text{ tali che } x > h\}$,
$\{A_1, A_2\}$ e' una partizione di X se $h = 5$, altrimenti non e' una partizione di X.

Esempio $B = \{0, 1, 2, 3, 4\}$, $C = \{0, 2, 4\}$,
$A_1 = B \cap C, A_2 = B - C$, $\{A_1, A_2\}$ e' una partizione di B.

Esempio $B = \{0, 1, 2, 3, 4\}$,
$A_1 = \{0, 3\}, A_2 = \{2\}, A_3 = \{1\}$ $A_4 = \{4\}$ e' una partizione di B.

Prodotto cartesiano

Definizione Dati due insiemi A e B, il *prodotto cartesiano* di A e B, $A \times B$, è l'insieme costituito da tutte le coppie ordinate $((a,b) \neq (b,a))$ di elementi di A e B, cioè:

$$A \times B = \{(a,b) |\ a \in A,\ b \in B\}.$$

Se $A = B$, $A \times A$ si denota anche con A^2.

Esempio/esercizio

- $A = \{0,1,2\}$, $C = \{0,2,4\}$
  $A \times C = \{(0,0),(0,2),(0,4),(1,0),(1,2),(1,4),(2,0),(2,2),(2,4),\}$.
  $A \times C \neq C \times A$ (infatti $(1,2) \in A \times C$ ma $(1,2) \notin C \times A$).
  Calcolare $A \times C \cup C \times A$ e $A \times C \cap C \times A$.
- $A = \mathbb{R}$ retta cartesiana, $A \times A = \mathbb{R}^2$ piano cartesiano.

Proposizione Se A ha cardinalità $|A| = h$ e B ha cardinalità $|B| = k$ allora $A \times B$ ha cardinalità hk.

Il prodotto cartesiano si estende anche a tre o più insiemi.
Se si considerano n insiemi $A_1, A_2, \ldots, A_n$, il loro prodotto cartesiano è definito così:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \quad | \quad a_i \in A_i, \ \forall i = 1, \ldots, n\}$$

N.B. La scrittura $\{a, b\}$ denota l'insieme i cui elementi sono a e b, quindi la coppia a, b (per cui $\{a, b\} = \{b, a\}$), mentre la scrittura (a, b) denota la coppia ordinata (a, b) (per cui $(a, b) \neq (b, a)$).
Lo stesso accade per $\{a_1, a_2, \ldots, a_n\}$ e $(a_1, a_2, \ldots, a_n)$.

index

Relazioni in un insieme

Siano A e B insiemi. In modo informale possiamo dire che una *relazione* R tra A e B è una legge che a qualche elemento di A associa qualche elemento di B. Quindi data una relazione si creano delle copie (a,b) formate da $a \in A$ e $b \in B$, tale che b e' in relazione con B. Questo da' senso alla seguente definizione.

Definizione Una *relazione* (binaria) R tra due insiemi A e B è un sottoinsieme del prodotto cartesiano $A \times B$.

Sia $R \subset A \times B$ una relazione. Se $(a,b) \in R$ si dice che a è *in relazione con* b (spesso si scrive aRb, invece di $(a,b) \in R$).

Se invece a e b non sono in relazione si scrive $(a,b) \notin R$.

Esempio $A = \{x \in \mathbb{N} \text{ tali che } 1 \leq x \leq 7\}$, $B = \{2,4\}$ $R : a \in A$ e' in relazione con $b \in B$ solo se a e' divisore di b. Allora
$R = \{(1,2),(1,4),(2,2),(2,4),(4,4)\}$.

Esempio $A = \{$ rette del piano $\}$, $B = \{$ punti del piano $\}$, $R : r \in A$ e' in relazione con $b \in B$, se e solo se $b \in r$.

Esempio $A = B = \mathbb{Z}$, $(a,b) \in R$ se $b^2 = a$. Quindi $(1,1)$, $(1,-1)$, $(4,2)$ sono tutti elementi di R. Ma, per esempio, 2 non e' in relazione con nessun elemento.
La stessa relazione ma con $A = B = \mathbb{R}$, da' un risultato totalmente diverso!

Definizioni

- Se $A = B$ e $R = \{(a,a),\ \forall a \in A\} \subset A \times A$ diciamo che R e' la relazione identica (cioe' ogni elemento a e' in relazione solo con se stesso).
- Se $R = A \times B$ diciamo che R e' la relazione totale, cioe' ogni elemento di A e' in relazione con ogni elemento di B.

Sia R una relazione su un insieme X (quindi $R \subset X \times X$), allora diciamo che R e'

- *riflessiva* se $(x,x) \in R, \quad \forall x \in X, \quad$ equivalentemente se xRx per ogni $x \in X$
- *simmetrica* se $(x,y) \in R \quad \Rightarrow \quad (y,x) \in R$, , cioe' se vale "$x$ in relazione con y implica y in relazione con x".
- *antisimmetrica* se $(x,y) \in R$ e $(y,x) \in R \quad \Rightarrow \quad x = y$, cioe' se vale "$x$ in relazione con y e y in relazione con x, implica $x = y$"
- *transitiva* se $(x,y) \in R$ e $(y,z) \in R \Rightarrow (x,z) \in R$, cioe' se x e' in relazione con y e y e' in relazione con z, allora x e' in relazione con z.

Esempio

- Sia $A = \{0,1,2,3,4\}$ e $R_1 =''<''$, cioe' "essere minore di" Allora

  $R_1 := \{(0,1),(0,2),(0,3),(0,4),(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}.$

  In particolare R_1 e' non riflessiva, non simmetrica, antisimmetrica e transitiva.

- Se invece $R_2 =''\leq''$, allora

  $$R_2 = R_1 \cup \{(0,0),(1,1),(2,2),(3,3),(4,4)\}$$

  ed R_2 e' riflessiva.

- $B = \{rette\}$, $R_3 =$"essere parallele o cioncidenti".
  E' riflessiva, e' simmetrica ed e' transitiva

Definizione Sia R una relazione in X. Diciamo che R e' una *relazione di equivalenza* se e'una relazione

- riflessiva
- simmettrica
- transitiva

Spesso indicheremo le relazione di equivalenza con il simbolo $\sim$.

Esempio $X = \{\text{rette nel piano}\}$, $R =$"essere parallele o coincidenti".
La relazione R e' una relazione di equivalenza.

Esempio: $X = \mathbb{N}$, R : nRm se e solo se $\exists k \in \mathbb{N}$ tale che $n = km$ (relazione: n e' mulitplo di m).

- R e' riflessiva ($k = 1$);
- R e' antisimmetrica (se $n = km$ e $m = hn$, allora $m = hkm$, quindi $h = k = 1$ e $n = m$)
- e' transitiva (se $n = mk$ e $m = ho$ allora $n = kho$)

In particolare R non e' relazione di equivalenza.

Vedremo altre relazioni di equivalenza nelle prossime lezioni.

Definizione Sia R una relazione su un insieme X, diciamo che R e' una *relazione d'ordine* se R e'

- riflessiva;
- antisimmetrica;
- transitiva

Spesso indicheremo le relazione d'ordine con il simbolo $\preceq$.

Esempio $X = \mathbb{N}$, $R =$"$\leq$" e' una relazione d'ordine.

Quindi le relazioni d'ordine generalizzano agli insiemi (non necessariamente di numeri) la relazione gia' nota "$\leq$" che esiste fra i numeri interi, relativi, razionali, reali.

Definizioni Sia X un insieme e $\preceq$ una relazione d'ordine su X. Si dice che l'insieme X con la relazione $\preceq$ e' un insieme parzialmente ordinato.

Due elementi x e y in X si dicono *confrontabili* se $x \preceq y$ oppure $y \preceq x$ (cioe' se x e' in realzione con y oppure, viceversa, y e' in relazione con x).

Un insieme si dice *totalmente ordinato* se e' parzialmente ordinato e ogni coppia di elementi di X e' confrontabile (cioe' presa una qualsiasi copia di elementi x e y, allora o $X \preceq y$ o $y \preceq x$).

In questo caso la relazione si dice di *ordine totale*.

Esempio: $(\mathbb{N}, \leq)$ e' un insieme totalmente ordinato.

Osservazione L'insieme $\mathbb{C}$ non ammette una relazione di ordine totale.

Esempio: $A = \{a, b, c\}$, $R := \{(a,a), (a,b), (a,c), (b,b), (c,c)\}$ e'

- riflessiva;
- antisimmetrica;
- transitiva.

Quindi e' relazione d'ordine.

Ma b e c non sono confrontabili, quindi non e' una relazione di ordine totale.

Date delle relazione di ordine, si possono generalizzare dei concetti gia' noti negli insiemi numerici ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$),

Definizioni: Sia $(X, \preceq)$ un insieme parzialmente ordinato.

Un elemento $a \in X$ si dice *massimo* di X se $\forall x \in X$ si ha $x \preceq a$.

Un elemento $b \in X$ si dice *minimo* di X se $\forall x \in X$ si ha $b \preceq x$.

Sia $Y \subseteq X$. Anche Y risulta parzialmente ordinato da $\preceq$.

Un elemento $s \in X$ si dice *estremo superiore* di Y, e si scrive $s = Sup(Y)$, se

- $\forall y \in Y$ si ha $y \preceq s$;
- se $x \in X$ è tale che $y \preceq x, \forall y \in Y$, allora anche $s \preceq x$.

Un elemento $t \in X$ si dice *estremo inferiore* di Y, e si scrive $t = Inf(Y)$, se

- $\forall y \in Y$ si ha $t \preceq y$;
- se $x \in X$ è tale che $x \preceq y, \forall y \in Y$, allora anche $x \preceq t$.

index

Applicazioni

Una relazione R tra due insiemi (non vuoti) A e B è detta *applicazione*, o *funzione*, se $\forall a \in A$ esiste uno e un solo $b \in B$ tale che aRb.

Di solito, se R è una applicazione tra A e B, si scrive

$$R : A \to B,$$

e se aRb, si scrive $b = R(a)$.

A e B vengono detti rispettivamente *dominio* e *codominio* di R.

Dato a, l'elemento $R(a)$ viene detto *immagine* di a tramite R.

L'insieme $R(A) = \{b \in B \quad | \quad \exists a \in A \quad b = R(a), \}$ viene detto *immagine* di R.

Dato $b \in B$, un qualsiasi $a \in A$ tale che $R(a) = b$ viene detto *retroimmagine* o *controimmagine* di b.

L'insieme (che può anche essere vuoto) delle retroimmagini di b viene denotato con $R^{-1}(b)$, ossia $\quad R^{-1}(b) = \{a \in A \quad | \quad R(a) = b\}$.

Due applicazioni F e G tali che $F, G : X \to Y$ si dicono uguali ($F = G$) se $\forall x \in X, F(x) = G(x)$.

Esempi: Sia $A = B = \mathbb{Z}$.

La relazione Φ, definita da $a\Phi b$ se e solo se a è il doppio di b, non è una applicazione perché 3 non è associato ad alcun b.

La relazione Ψ definita da $a\Psi b$ se e solo se $a = b^2$, non è una applicazione perché 9 è in relazione sia con 3 che con -3.

La relazione Θ definita da $a\Theta b$ se e solo se a è la metà di b, è una applicazione, perché ogni intero a, esiste $b(= 2a)$ tale che $a\Theta b$.

Definizioni Sia $F : A \to B$ un'applicazione. Si dice che F e':

- *iniettiva* se $F(a) = F(b) \Rightarrow a = b$, ossia se ogni elemento di B ammette al più una controimmagine;
- *suriettiva* se $\forall b \in B, \exists a \in A$ tale che $F(a) = B$, ossia se $F(A) = B$, ossia se ogni elemento di B ammette almeno una controimmagine;
- *biettiva* o *biunivoca* se è sia iniettiva che suriettiva, cioe' ogni elemento $b \in B$ ammette esattamente una controimmagine.

Esempi

- $f : \mathbb{Z} \to \mathbb{Z}$ tale che $f(x) = 2x$:
  e' iniettiva (dati due x_1 e x_2 se $f(x_1) = f(x_2)$ significa che $2x_1 = 2x_2$, quindi $x_1 = x_2$),
  ma non suriettiva (non esiste la retroimmagine di 3).

- $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ tale che $f(x) = x^2$ dove $\mathbb{R}_{\geq 0}$ e' l'insieme dei numeri reali non negativi (quindi maggiori o uguali di 0):
  e' suriettiva (per ogni numero naturale $y \in \mathbb{R}_{\geq 0}$ esiste $x \in \mathbb{R}$ tale che $x^2 = y$, infatti prendo $x := \sqrt{y}$),
  ma non e' iniettiva (se $x_1 = 1$ e $x_2 = -1$, allora $x_1 \neq x_2$ ma $f(x_1) = f(x_2) = 1$).

- $f : \mathbb{Q} \to \mathbb{Q}$ tale che $f(x) = 2x$:
  e' iniettiva (come prima)
  e' suriettiva (la controimmagine di 3 e' $3/2$ e piu' in generale la controimmagine di y e' $y/2$).
  Quindi e' biiettiva.

Definizione Date due applicazioni $F : A \to B$ e $G : B \to C$, si può definire un'applicazione $G \circ F : A \to C$, che viene detta *composizione* di F con G, così:

$$(G \circ F)(a) = G(F(a)), \quad \forall a \in A.$$

Proposizione: La composizione di applicazioni è associativa (ossia se $F : A \to B$, $G : B \to C$ e $H : C \to D$, si ha $H \circ (G \circ F) = (H \circ G) \circ F$.
Osservazione In generale, se si può considerare la composizione di F con G, non è detto che si possa anche considerare la composizione di G con F.

Nel caso di applicazioni $F, G : A \to A$ sono possibili sia la composizione $F \circ G$ che la composizione $G \circ F$. Tuttavia queste composizioni sono in generale applicazioni diverse, ossia la composizione di applicazioni non è commutativa.

Esempio: Siano F e G le applicazioni $F, G : \mathbb{Z} \to \mathbb{Z}$ definite rispettivamente da $F(x) = 3x$ e da $G(x) = x + 1$, risulta $(G \circ F)(2) = G(6) = 7$, mentre $(F \circ G)(2) = F(3) = 9$.

Dato un insieme A, l'applicazione $id_A : A \to A$ definita da $id_A(a) = a \quad \forall a \in A$ viene detta applicazione *identica* o *identità*.

Proposizione Sia $F : B \to C$ un'applicazione e si considerino le applicazioni identiche $id_B : B \to B$ e $id_C : C \to C$. Risulta $F \circ id_B = F$ e $id_C \circ F = F$.

Date due applicazioni $\Phi : A \to B$ e $\Psi : B \to A$, se accade che sia $\Psi \circ \Phi = id_A$ si dice che Φ è *inversa destra* di Ψ (e che Ψ è *inversa sinistra* di Φ).

Se si ha sia $\Psi \circ \Phi = id_A$ che $\Phi \circ \Psi = id_B$, si dice che Φ e Ψ sono una *inversa* dell'altra.

Proposizione Le applicazioni biunivoche ammettono inversa.

dimostrazione. Sia $F : X \to Y$ biunivoca. Per ogni $y \in Y$ esiste uno e un solo $x_y \in X$ tale che $F(x_y) = y$. Considero la funzione $G : Y \to X$ tale che $y \mapsto x_y$.
Si verifica che $(G \circ F)(x) = G(F(x)) = G(y) = x$, e
$(F \circ G)(y) = F(G(y)) = F(x_y) = y$, quindi
$\forall x \in X,\ (G \circ F)(x) = x$ e quindi $G \circ F = id_X$ e
$\forall y \in Y,\ (F \circ G)(y) = y$ e quindi $F \circ G = id_Y$.
Di conseguenza F e G sono inverse e in particolare F ammette un'inversa .
c.v.d.

L'applicazione $F : \mathbb{Z} \to \mathbb{Z}$ definita da $F(x) = x + 1$ ammette inversa (ossia sia inversa destra che inversa sinistra) e tale inversa è definita da $G(x) = x - 1$.