

# MATEMATICA DISCRETA

## G ALGEBRA LINEARE

# DISCRETA: INSIEMI → INSIEMI ↴

INSIEMI A + insieme.  $a \in A$  + l'elemento 'a' appartiene all'insieme A.

Per insieme si intende una collezione di oggetti distinti ben definita, ossia che gli elementi ignorano le ripetizioni e non ci possono essere dubbi sull'appartenenza di un elemento all'interno dell'insieme.

## DEFINIZIONE >

Gli insiemi si definiscono in diversi modi

- DEFINIZIONE DIRETTA:  $A = \{0, 1, 2, 4\}$
- DEFINIZIONE DI 'PUNTI':  $A = \{0, 1, 2, \dots\}$

### TRAMITE GLI INSIEMI NUMERICI:

- $\mathbb{N}$ : Numeri naturali ( $0, 1, 2, 3, \dots$ )
- $\mathbb{Z}$ : Numeri interi ( $\dots -2, 0, 2, 2, \dots$ )
- $\mathbb{Q}$ : Numeri razionali ( $\dots -\frac{1}{2}, 0, \frac{1}{3}, \frac{1}{4}, \dots$ )  $\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \wedge b \neq 0 \}$
- $\mathbb{R}$ : Numeri reali ( $\dots -1.49, -1, 0, 1, 2, \dots$ )
- $\mathbb{C}$ : Numeri complessi ( $a+bi \mid a, b \in \mathbb{R} \wedge c^2 = -1$ )

Ad essi si affiancano i quantificatori:  $\exists$  = esiste,  $\exists!$  = esiste ed è unico,  $\forall$  = per ogni  
 $\neg$  = negazione,  $P(x)$  = proposizione/,  $\rightarrow$  = implicazione

cardinalità: |A|

$\subseteq$  E insiemistica:  $A \subseteq B$  (inclusione stretta)  $A \subseteq B \wedge B \subseteq A \quad (A \in B \text{ sono uguali})$

$\subseteq$  A ⊆ B (inclusione simbolico)

$A \cap B = \{c \mid c \in A \wedge c \in B\}$   
 (intersezione)

$A \cup B = \{c \mid c \in A \vee c \in B\}$   
 (unione)

$\emptyset$  = Insieme vuoto.

## PROPRIETÀ >

Alcune proprietà degli insiemi sono:

- INSIEMI DISGIUNTI: Dati 2 insiemi, essi sono disgiunti se la loro intersezione è  $\emptyset$
- COMPLEMENTO: Dati 2 insiemi  $A \in B$ , il complemento di A in B sono tutti gli elementi del secondo insieme (B) che non stanno nel primo (A)  $\complement_B(A) = \{b \mid b \in B \wedge b \notin A\}$
- DIFFERENZA: Dati 2 insiemi  $A \in B$ , la differenza è formata degli elementi dell'insieme esse che non stanno nell'insieme che dà dell'operatore.

ESEMPIO  $A = \{2n \mid n \in \mathbb{N}\}$   $B = \{3n \mid n \in \mathbb{N}\}$

- $A \cap B = \{2n \wedge 3m \mid n, m \in \mathbb{N}\} = \{6n \mid n \in \mathbb{N}\}$
- $A \cup B = \{2n \vee 3m \mid n, m \in \mathbb{N}\}$
- $B \setminus A = \{c \mid c = 3m \wedge c \neq 2n \mid m, n \in \mathbb{N}\}$
- $A \setminus B = \{c \mid c = 2n \wedge c \neq 3m \mid m, n \in \mathbb{N}\}$

PARTI >  $\mathcal{P}(X) = \{\emptyset, X, \dots\}$

Le parti di un'insieme sono tutti i sottoinsiemi formabili di quell'insieme.

ESEMPIO  $= X = \{1, 2, 3\}$   $\mathcal{P}(X) = \{\emptyset, X, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$

Se l'insieme di partenza è finito, il numero di elementi nelle parti è  $2^n$

## ESEMPPIO

In GZ

num. pari =  $\{a \in \mathbb{Z} \mid a = 2n\}$

num. dispari =  $\{a \in \mathbb{Z} \mid a = 2n+1\}$

num. divisibili per 3 con resto 0 =  $\{a \in \mathbb{Z} \mid a = 3n\}$

num. divisibili per 11 con resto 7

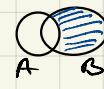
$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \dots$$

Intersezione di insiemi

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \dots$$

Unione di insiemi

$$A \cap B = \emptyset$$

$$A \setminus B$$



DISSETA: INSIEMI • INSIEMI  $\subset$   
PROPRIETÀ DI  $\cup \in \cap >$

Dati 3 insiemi:  $A, B \in C$  si illustrano delle proprietà sull'unione e intersezione degli insiemi:

- $A \subseteq A \cup B, B \subseteq A \cup B$
- $A \cap B \subseteq A, A \cap B \subseteq B$
- $A \cup B = A \Leftrightarrow B \subseteq A$  (6)
- $A \cap B = B \cap A, A \cup B = B \cup A \rightarrow$  Per proprietà commutativa.
- $(A \cap B) \cap C = A \cap (B \cap C) \rightarrow$  Per proprietà associativa.  
 $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \rightarrow$  Per proprietà distributiva.  
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  si distribuisce il "segno".

LEGGI DI DE MORGAN  $>$

Le leggi di De Morgan sono delle proprietà applicabili su sottrazioni e unioni/inters.

- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$  Si distribuisce il meno \ e lo si unisce con l'intersezione
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$  (se unione) o unione (se intersezione)

INTERVALLI  $>$

È possibile definire degli intervalli seguendo la notazione  $[x, y]$  in cui a seconda delle parentesi utilizzate, esse hanno un significato diverso

- $[x, y] = x \text{ e } y \text{ sono} \underline{\text{incluse}} \text{ nell'intervalle.}$  Es:  $B \supseteq [x, y] = \{r \in \mathbb{R} \mid x \leq r \leq y\}$
- $(x, y) = x \text{ e } y \text{ sono} \underline{\text{escluse}} \text{ dall'intervalle.}$  Es:  $B \supseteq (x, y) = \{r \in \mathbb{R} \mid x < r < y\}$

È possibile combinare le parentesi. È possibile anche definire dei semi-intervalli infiniti tramite  $\infty$  (Es:  $(a, \infty)$   $\overline{a} \dots \dots \infty$ ) o infiniti  $(-\infty, b)$  NB: l'infinito non si può includere

RICOPRIMENTO  $> X, A_0 \cup A_1 \dots A_n = X$

Per ricoprimento di un insieme si intende una famiglia di sottinsiemi, la quale se unita da l'insieme di partenza.

PARTIZIONE  $>$

La partizione è una forma di ricoprimento con delle caratteristiche particolari:

- $A_0, A_1, \dots A_n$  sono un ricoprimento
- $A_i = \emptyset \forall i \in \{1, \dots, n\}$  ossia nessun sottoinsieme è vuoto
- $A_i \cap A_j = \emptyset \forall i \neq j \in \{1, \dots, n\}$  ossia nessun sottoinsieme deve avere elementi in comune.

QUOTIENTE DATO DA PARTIZIONE  $> X, A_0, A_1, \dots A_n \quad Q = \{A_0, A_1, \dots A_n\}$

Dato un insieme  $X$  e la famiglia di insiemi che ne forma la partizione, il quoziente di  $X$  secondo la partizione è un nuovo insieme contenente tutte le sottoclassi.

Inoltre, ogni elemento del nuovo insieme viene detto rappresentante

$$x = \bigcup_{i=0}^n A_i \quad Q = \{A_0, A_1, \dots A_n\} \quad A \in Q \models x \in A \text{ rappresentante di } A$$

PRODOTTO CARTESIANO  $> A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

Per prodotto cartesiano si intendono tutte le coppie ordinate formabili a partire da 2 insiemi che ne definiscono l'ordine

CORRISPONDENZA  $> C \subseteq A \times B$

Dato un prodotto cartesiano, il suo sottoinsieme viene detto corrispondenza.

DISCRETA: ASSIOMI DI PEOANO E METODO INDUTTIVO • //

DIMOSTRAZIONE DI N: ASSIOMI DI PEOANO >

Per poter dimostrare l'insieme dei numeri naturali, il matematico Giuseppe Peano ha definito 5 assiomi:

Assunzioni  
non dimostrate

- Un qualunque numero  $0 \in \mathbb{N}$
- Ogni numero appartenente a  $\mathbb{N}$  possiede un suo successore  $\forall n \in \mathbb{N}, \exists m \in \mathbb{N} (s(n) \stackrel{\text{m}}{\uparrow})$
- Dati 2 numeri appartenenti a  $\mathbb{N}$ , i loro successori saranno diversi  $\forall a, b \in \mathbb{N} (a \neq b) \Rightarrow s(a) \neq s(b)$
- $\emptyset$  non è il successore di nessun numero di  $\mathbb{N}$   $\forall n \in \mathbb{N} (0 \neq s(n))$
- Se si prende un nuovo insieme  $U$  in cui
  - è presente lo  $0$   $0 \in U$
  - Il nuovo insieme è un sottoinsieme di  $\mathbb{N}$   $U \subseteq \mathbb{N}$
  - Tutti i successori degli elementi fanno parte del nuovo insieme  $\forall a \in U (s(a) \in U)$

Allora  $U = \mathbb{N}$

L'ultimo assioma ha dato vita alla dimostrazione per induzione.

DIMOSTRAZIONE PER INDUZIONE >

La dimostrazione per induzione è un tipo di dimostrazione che si serve di iterazioni e sequenze per concludere le sue stesse dimostrazioni. Essa si serve di:

- Un caso base  $P(0)$
- Un caso induttivo, in cui si assume che  $P(n)$  sia vera e si procede a dimostrare  $P(n+1)$

Così facendo si dimostra che la proprietà funziona  $\forall n \in \mathbb{N}$

ESEMPPIO: Gauß e la somma degli  $n$  numeri  $\in \mathbb{N}$

Il prof. di matematica ostegnò a Gauß e ai suoi compagni di sommare i primi 100 numeri  $\in \mathbb{N}$ . Per fare ciò,

Gauß usò il metodo di scrivere tutti i numeri in 1 riga e poi sotto gli stessi numeri ma in ordine inverso.

1 2 3 ... 98 99 100 Notando, però che se li sommano tutti veniva sempre lo stesso risultato.

100 99 98 ... 3 2 1 Da cui pensò di

- moltiplicare il risultato per il numero di elementi di 1 riga (100)
- dividere il risultato per 2 visto che non aveva bisogno del risultato per 200

Trovando quindi la formula generale per eseguire la sommatoria.

DIMOSTRAZIONE: CASO BASE  $P(1)$

$$\frac{1 \cdot (1+1)}{2} = 1 \quad \text{Verificato}$$

DIMOSTRAZIONE: CASO INDUTTIVO  $P(n+1)$

$$\underline{\text{IPOTESI}} : \frac{n \cdot (n+1)}{2} \quad \underline{\text{TESI}} : \frac{(n+1) \cdot ((n+1)+1)}{2}^{n+2}$$

$$\begin{aligned} \underline{\text{DURORSI}} \\ \frac{n \cdot (n+1)}{2} + (n+1) &= \frac{n^2 + 2n + 2}{2} \\ &= \frac{n^2 + 3n + 2}{2} \end{aligned}$$

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

$$= \frac{n^2 + n + 2n + 2}{2}$$

$$= \frac{n^2 + 3n + 2}{2}$$

Per ipotesi induttiva si dà per verità la somma  $1+2+\dots+n$   
a cui va aggiornata la nuova iterazione  $n+1$

Dopodiché l'obiettivo diventa far coincidere Tesi e dim.

Verificati:  $\forall n \in \mathbb{N}$

ESEMPIO 2 : Dimostrazione  $\beta(A)$

Si dimostra la formula  $\beta(A) = 2^{|A|}$

CASO INDUTTIVO  $P(n+1)$  :

IPOTESI :  $\beta(A) = 2^{|A|}$

TESI :  $\beta(B) = 2^{|A+n|} = 2^{(n+1)}$

$|A|-1=|A| \wedge$   
 $A \subseteq B$

CASO BASE  $P(0)$  :  $A = \emptyset$

$\beta(\emptyset) = 1 \rightarrow 1^{\beta(\emptyset)} = 1 \quad \beta(\emptyset) = 1$

Verificata = 1

DUR.

$$2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$$

↑                  ↑  
per              nuova  
ipotesi        iterazione  
induttiva

DISCRETA : INSIEMI FINITI E CALCOLO COMBINATORIO •

INSIEMI EQUIPOLLENTI >  $X, Y \ f: x \rightarrow y \wedge f^{-1}: y \rightarrow x$  biettive  $\wedge |X|=|Y|$

Dati due insiemi, essi sono equipollenti se esiste una funzione biettiva che mappa gli elementi da un insieme nell'altro.

Essendo la funzione biettiva, si dice anche che i due insiemi hanno la stessa cardinalità.

Inoltre si nota che

- Ogni insieme è equipollente tramite la funzione identità  $i: x \rightarrow x \ x \mapsto x$
- È possibile effettuare composizioni di più insiemi :  $X, Y, Z$ .  $f: X \rightarrow Y \ x \mapsto f(x) \ g: Y \rightarrow Z \ y \mapsto g(y)$   $g \circ f: X \rightarrow Z \ x \mapsto g(f(x))$
- Per gli insiemi infiniti  $\mathbb{N}$ , essi sono equipollenti al loro sottoinsieme proprio (sottoinsieme infinito)

INSIEMI INFINTI >  $\mathbb{Z}^N = \{z_n \mid n \in \mathbb{N}\} \quad \mathbb{Z}^N \leq \mathbb{N} \quad |\mathbb{N}| = |\mathbb{Z}^N| \text{ per } n \mapsto z \cdot n \text{ biettiva}$

Un insieme viene detto infinito se è equipollente ad ogni suo sottoinsieme proprio.

CARDINALITÀ DI INSIEMI FINITI >

Per verificare la cardinalità degli insiemi si utilizzano le funzioni e le loro proprietà:

MINORE-UGUALE :  $A, B \quad |A| \leq |B| \rightarrow f: A \rightarrow B$  biettiva  $\vee g: B \rightarrow A$  suriettiva

Dati 2 insiemi  $A, B$ ,  $A$  ha una cardinalità minore-uguale di  $B$  se esiste una funzione che mappi  $A$  in  $B$  iniettiva.

In alternativa, una funzione suriettiva che mappi  $B$  in  $A$ .

INCLUSIONE DI SOTTO-INSIEMI >  $A \subseteq B \rightarrow |A| \leq |B| \quad f: A \rightarrow B \quad a \mapsto a$  uguale  $g: A \rightarrow A \quad a \mapsto a$

Inoltre, se  $A \subseteq B$ , allora  $|A| \leq |B|$  per la funzione di inclusione che per implementazione equivale alla funzione identità del sotto-insieme.

TEOREMA DI ORDINAMENTO DELLA CARDINALITÀ

Dati 2 insiemi qualsiasi  $A, B$ .  $|A| \leq |B| \vee |B| \leq |A|$

TEOREMA DI SHRODER-BERSTEIN

$A, B \quad |A| \leq |B| \wedge |B| \leq |A| \vdash |B| = |A|$

Dati 2 insiemi, se uno è minore-uguale dell'altro e viceversa, allora sono uguali,

Inoltre, supponendo che due insiemi hanno la stessa cardinalità, definendo una qualsiasi funzione  $f$

- iniettiva ) se è allora è
- suriettiva ↗ anche

- biettiva ↙ e di conseguenza deve essere

## DIMOSTRAZIONE INSIEMI FINITI >

Dato un insieme  $I_m = \{1, 2, \dots, m\} \subseteq \mathbb{N}$  valido per ogni  $m \in \mathbb{N}$  con cui  $I_0 = \emptyset$  si procede a dimostrarne alcune caratteristiche.

### $I_m$ è FINITO $\forall m \in \mathbb{N}$

Si dimostra per induzione che per qualsiasi  $n \in \mathbb{N}$ , l'insieme  $I_n$  è finito.

CASO BASE  $m=0$ : Per definizione  $I_0 = \emptyset$  verificata

CASO INDUTTIVO: Ipotesi:  $I_m$  è finito Teosi:  $I_{m+1}$  è finito

Si definisce un nuovo insieme  $X \subseteq I_{m+1}$   $\wedge |X| = |I_{m+1}|$  per convenienza. Da cui:

- Si sa che esiste una funzione iniettiva che mappa  $I_{m+1}$  in se stesso  $\exists f: I_{m+1} \rightarrow I_{m+1}$
- Se si restringe la funzione  $f$  in modo che mappi solo i primi  $m$  elementi:  $f|_{I_m}: I_m \rightarrow I_m$
- Essendo  $f$  iniettiva, lo è anche  $f|_{I_m}$ . Inoltre, essendo la funzione ristretta l'identità è suriettiva, rendendo anche  $f$  tale. dimostrando che  $f|_{I_m}$  ed  $f$  sono biettevole ma non uguali rendendo l'insieme finito in quanto non equipotente ad un suo sottinsieme proprio

Se  
 $f(m+1)=x$

- Nel caso in cui la funzione iniettiva  $f: I_{m+1} \rightarrow I_{m+1}$  per  $m+1$  non restituisca sé stessa, si ri-definisce una nuova funzione  $\delta: I_{m+1} \rightarrow I_{m+1}$  definita da  
 $\delta(j) = j$  se  $j \notin \{x, m+1\} \rightarrow$  ritorna se stessa se non è  $x \circ m+1$   
 $\delta(x) = m+1$   $\delta(m+1) = x$  inverte se  $x$  o  $m+1$
- Ridefinendo una nuova funzione  $f' = \delta \circ f$  essa è biettiva rendendo  $f$  biettiva

$$m \leq n$$

Dati  $m, n \in \mathbb{N}$   $\exists |I_m| \leq |I_n|$

Si dimostra che 2 insiemi  $I$  basati su 2 elementi distinti  $m, n$  hanno cardinalità differente ovvero non sono equipotenti.

Cioè si dimostra ponendo che  $m < n$  di conseguenza  $I_m \subseteq I_n$  dimostrandolo per definizione che  $|I_m| \leq |I_n|$

$m, n \in \mathbb{N} \wedge m \leq n \Rightarrow |I_m| \leq |I_n|$

Analogamente, se  $m \leq n$ , allora  $I_m \subseteq I_n \Rightarrow |I_m| \leq |I_n|$

### Applicazione per ogni insieme

Si dimostra che, dato un insieme qualunque  $X$  finito, esiste un numero  $n \in \mathbb{N}$  per cui  $|X| = |I_n|$ . ossia  $|X| = n \rightarrow$  Def. di contare

$$\begin{array}{c} X \\ \subseteq I_n \\ |X| = n \end{array}$$

## INSIEMI INFINTI > $X, |\mathbb{N}| \leq |X|$

Per insieme infinito si intendono tutti gli insiemi con cardinalità  $\geq \aleph_0$ .

Cioè è dimostrabile tramite la costruzione di sottoinsiemi di  $X$ , che diventano infiniti:  $X' = \{x_0, x_1, \dots, x_n, \dots\} \subseteq X \quad \exists f: \mathbb{N} \rightarrow X' \quad n \mapsto x_{n+1}$

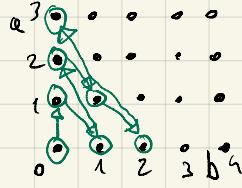
Dopo di che si definisce un'altra funzione  $g: \mathbb{N} \rightarrow X$  in cui  $g = c \circ f$  in cui

- $c$  è la funzione di inclusione  $X' \rightarrow X$  ed è iniettiva
- così facendo si dimostra che grazie a  $g: \mathbb{N} \rightarrow X$

## INSIEMI NUMERABILI >

Si dicono insiemi numerabili tutti gli insiemi la cui cardinalità =  $|N|$ . Alcuni insiemi numerabili famosi:

$$|N \times N| = |N| \rightarrow N \times N \text{ dai delle coppie ordinate } (a, b) \text{ rappresentabili su un piano}$$



In questo caso si definisce una funzione che mappa la diagonale ad un  $n \in N$   
 $\exists f: N \times N \rightarrow N$  biottiva

$$|\mathbb{Q}| = |N| \rightarrow \text{ogni numero in } \mathbb{Q} \text{ è nella forma}$$

$\frac{n}{m}$  in cui  $n \in \mathbb{Z}$  e  $m \in N \setminus \{0\}$   
 che possono essere descritti come le coppie ordinate  $(n, m) \in \mathbb{Z} \times N$

$$|\mathbb{Q}| \leq |\mathbb{Z} \times N| \quad \text{In cui però si sa che } |\mathbb{Z}| = |N| \text{ per cui}$$

$$|\mathbb{Z} \times \mathbb{Z}| = |N \times N| = |N|$$

$$N \subseteq \mathbb{Q} \Rightarrow |N| = |\mathbb{Q}|$$

$$|N| = |\mathbb{Q}| \text{ per siano due insiemi}$$

$|\mathbb{Z}| = |N| \rightarrow$  È possibile definire una funzione biottiva che mappi gli elementi di  $N$  in  $\mathbb{Z}$ :

$$\begin{aligned} f: N &\rightarrow \mathbb{Z} \\ z_n &\mapsto m \\ 2n+1 &\mapsto -(m+1) \end{aligned}$$

mappando i numeri pari nella parte positiva e i dispari nella parte negativa

## DISCERNITÀ: FUNZIONI • FUNZIONI ↴

Dati 2 insiemi  $A$  e  $B$ , una funzione è la corrispondenza  $\Gamma \subseteq A \times B$  in cui:

- Ad ogni elemento del dominio (gli elementi del 1° insieme) corrisponde un solo elemento del secondo insieme:  $\forall a \exists! b (a \in A \wedge b \in B) \models (a, b) \in \Gamma$
- La corrispondenza  $\Gamma$  viene detta grafico della funzione.  $f: A \rightarrow B$

↑  
Dominio  
↑  
codominio  
Funzione

## FUNZIONI D'INTERESSE >

Altre funzioni di maggior interesse includono:

- FUNZIONE IDENTITÀ:  $Id_A: A \rightarrow A \quad a \mapsto a$   
Dato un'insieme mappa il dominio nel co-dominio.

- FUNZIONE COSTANTE:  $f: A \rightarrow B \quad a \mapsto b \quad b \in B$

Dati 2 insiemi, ad ogni elemento del primo mappa lo stesso nel secondo

- FUNZIONE DI PROIEZIONE SU FATTORI:  $A, B \quad \pi_A: A \times B \rightarrow A \quad \pi_B: A \times B \rightarrow B$

Dato il prodotto cartesiano di 2 insiemi  $A$  e  $B$ , le funzioni fattori di  $A \times B$  sono 2 funzioni che, preso gli elementi della coppia ordinata:

- $\pi_A(a, b)$  restituirà solo la parte di  $A$
- $\pi_B(a, b)$  restituirà solo la parte di  $B$

- FUNZIONE OPERAZIONE:  $A \quad *: A \times A \rightarrow A \quad (a_1, a_2) \mapsto a_1 * a_2$

Dato un'insieme, la funzione operazione è una funzione che mappa il prodotto cartesiano dell'insieme nell'insieme stesso.

- FUNZIONE RESTRITTIVA:  $A, B \quad S \subseteq A \quad f: A \rightarrow B \quad f|_S: S \rightarrow B \quad s \mapsto f(s)$

Dati 2 insiemi  $A, B$  ed un sottoinsieme  $S \subseteq A$ , la funzione restrittiva è una funzione che ha come dominio il sottoinsieme ma dominio invariato.

## IMMAGINE > $\text{Im}g(f) = \{ b \in B | \exists a \in A \quad f(a) = b \}$

Per immagine di una funzione si intende l'insieme formato da tutti gli elementi del co-dominio che sono raggiunti dalla funzione

## CONTRO-IMMAGINE > $f^{-1}(b) = \{ a \in A | f(a) = b \}$

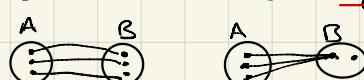
Per contro-immagine si intende l'insieme formato da tutti gli elementi del dominio che sono collegati ad un dato elemento del co-dominio.

N.B.: La controimmagine di un elemento non raggiunto da  $f = \emptyset$

## PROPRIETÀ DELLE FUNZIONI > BIETTIVA = INIEZIONE + SURIETTIVA

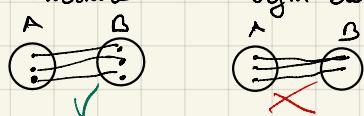
### SURIETTIVA >

Una funzione è suriettiva se ogni elemento del codominio viene raggiunto dalla funzione



### INIEZIONE >

Una funzione è iniezione se ogni elemento del dominio è mappato ad un elemento diverso del co-dominio



## DISCRETA : FUNZIONI • FUNZIONI 2

**COMPOSIZIONE DI FUNZIONI** >  $g: B \rightarrow C, f: A \rightarrow B \quad g \circ f: A \xrightarrow{f} B \xrightarrow{g} C \quad (g \circ f)(a) = g(f(a))$

Per composizione di funzioni si intende l'esecuzione composta di più funzioni. In particolare, verrà eseguita prima la funzione più a dx, poi quelle a sinistra. In essa l'ordine conta.

ESEMPIO :

$$f: N \rightarrow Z \quad n \mapsto -n \quad g: Z \rightarrow Z \quad z \mapsto z+1$$

$$g \circ f: N \rightarrow Z \rightarrow Z \quad n \mapsto -n + 1$$

dom f    codom g  
↓              ↓  
                dom g    codom g

ASSOCIAZIONE DELLE COMPOSIZIONI:  $f: A_1 \rightarrow A_2, g: A_2 \rightarrow A_3, h: A_3 \rightarrow A_4 \models f \circ (g \circ h) \equiv (f \circ g) \circ h$

La proprietà associativa delle funzioni dice che in caso si debba comporre 3 opere funzioni, l'ordine di esecuzione non cambia

$$f: A \rightarrow D$$

**FUNZIONE IDENTITÀ COMPOSTA** >  $A, B$   $\text{id}_A: A \rightarrow A \quad a \mapsto a, \text{id}_B: B \rightarrow B \quad b \mapsto b$

A seconda di dove e come è definita la funzione identità, la sua presenza rende invariata la composizione (= all'altra funzione della comp.). In particolare:

- Se la funzione identità è a dx ed è l'identità del dominio, allora è invariante  $f \circ \text{id}_A \equiv f$
- Se la funzione identità è a sx ed è l'identità del co-dominio, allora è invariante  $\text{id}_B \circ f \equiv f$

**PROPRIETÀ DELLE FUNZIONI CON COMPOSIZIONE** >

Alcune proprietà delle funzioni con la composizione:

- Se la composizione contiene funzioni iniettive, essa sarà iniettiva
- Se la composizione contiene funzioni suriettive, esse saranno suriettive
- Se la composizione contiene funzioni biettive, esse saranno biettive
- Se la composizione è iniettiva, la sua funzione di dx è iniettiva:  $g \circ f \Rightarrow f \text{ è iniettiva}$
- Se la composizione è suriettiva, la sua funzione di sx è suriettiva:  $g \circ f \Rightarrow g \text{ è suriettiva}$
- Se la composizione è biettiva, la sua funzione di dx è iniettiva e di sx è suriettiva:  $g \circ f \Rightarrow g \text{ suriettiva e } f \text{ iniettiva}$

**FUNZIONI INVERSE** >

Dette due funzioni, esse si dicono l'una inversa dell'altra quando

- se il dominio della prima è il co-dominio dell'altra e viceversa:  $f: A \rightarrow B, g: B \rightarrow A$
- se la composizione e la composizione invertita di esse mappano rispettivamente dominio e co-dominio del primo e secondo insieme  $g \circ f: A \rightarrow A$  e  $f \circ g: B \rightarrow B$
- Se la composizione della prima con la seconda funzione danno come risultato l'identità del primo insieme  $g \circ f = \text{id}_A$
- Se la composizione della seconda con la prima funzione danno come risultato l'identità del secondo insieme  $f \circ g = \text{id}_B$

Inoltre, le funzioni inverse sono biettive e se una qualunque funzione è biettiva, allora esiste solo 1 funzione inversa:  $f$  biettiva  $\models \exists! f^{-1}$

**INVERSE COMPOSTA** >  $(g \circ f)^{-1} = g^{-1} \circ f^{-1}$

Se si compongono due funzioni inverse, allora la composizione sarà iniettiva.

## DISCRETA: PERMUTAZIONI • PERMUTAZIONI S. PT. I

DEFINIZIONE >  $X \neq \emptyset$ ,  $f: X \rightarrow X$  biettiva

Dato un insieme, la permutazione di quell'insieme è detta dalla funzione biettiva avente sia come dominio che co-dominio l'insieme di partenza.

PERMUTAZIONI SU INSIEMI FINITI  $\Rightarrow S_n = \text{perm}(X)$

In particolare, le permutazioni su insiemi finiti vengono definite con  $S_n$  in cui  $n$  è il numero di elementi permutati

### PROPRIETÀ DELLE PERMUTAZIONI >

Alcune proprietà delle funzioni sono:

- La funzione identità di un insieme è una permutazione.
- Data una permutazione, la sua inversa è anche una permutazione.  
ESEMPIO:  $\alpha \in S_n$  se  $\alpha$  è biettiva, allora  $\forall x \in X \exists \alpha^{-1}(x)$  per cui anche  $\alpha^{-1}$  è biettiva di conseguenza  $\alpha^{-1}$  è biettiva.  $\alpha^{-1} \in S_n$
- La composizione di 2 permutazioni è a sua volta una permutazione per le proprietà delle composizioni.  $\alpha, \beta \in S_n \quad \alpha \circ \beta \in S_n \wedge \beta \circ \alpha \in S_n$
- Negli insiemi finiti, la cardinalità delle loro permutazioni è  $n!$   
ESEMPIO:  $n=5 \quad |S_5| = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

NOTA ZIONE A TABELLA >  $\alpha: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \rightarrow$  elementi originali  $\alpha \in S_n \quad \alpha^{-1}: \begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

È possibile utilizzare una notazione particolare per definire una permutazione in maniera veloce.

È anche possibile definire composizioni:  $\alpha: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \rightarrow \beta: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \rightarrow$   
 $\beta \circ \alpha: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \quad \alpha \circ \beta: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$

### CICLI >

Data una permutazione finita, definendola in maniera tabellare, è possibile individuarne dei "percorsi" collegando sulla stessa riga gli elementi tra di loro.

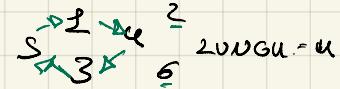
Se la permutazione ha un solo percorso, allora è detto ciclo.

ESEMPIO

$$\alpha: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \quad \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{matrix} \quad \text{è UN CICLO}$$

$$\beta: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \quad \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{matrix}$$

non è un ciclo (2 percorsi)



LUNGHEZZA

### DEFINIZIONE >

Data una permutazione, essa è un ciclo se esiste un sottoinsieme degli elementi della permutazione  $S_n$  collegati tra loro.

$\alpha \in S_n$  ciclico  $\exists \{x_1, x_2, x_3, x_4\} \subset \{1, 2, \dots, n\}$

$$\text{t.c. } \begin{cases} \alpha(x_1) = x_2, \alpha(x_2) = x_3, \alpha(x_3) = x_4, \\ \alpha(x_4) = x_1 \end{cases}$$