

# 1 - GLI INSIEMI

## 1) INSIEMI E OPERAZIONI TRA INSIEMI

Un insieme è una collezione di oggetti (del più espresso solo così).

Si indica con una maiuscola: i suoi elementi con la minuscola.

APPARTENENZA:  $s \in S$ ,  $s \notin S$

$\emptyset$  è l'insieme vuoto senza elementi.

$T \subseteq S$  sottoinsieme se  $\forall t \in T \Rightarrow t \in S$

(inclusione propria se  $T \neq S \Rightarrow T \subset S$  o  $T \subsetneq S$ ),  
altrimenti  $T \subseteq S$ .

$\forall$  insieme  $S \Rightarrow \emptyset \subseteq S$

se  $A \subseteq B$  e  $B \subseteq A \Rightarrow A = B$  sono uguali

Un insieme si definisce in due modi:

$A = \{0, 1, 2, 3, 4\}$  oppure  $A = \{n \in \mathbb{N} \mid n < 5\}$

UNIONE:  $A \cup B = \{x \mid x \in A \vee x \in B\}$

INTERSEZIONE:  $A \cap B = \{x \mid x \in A \wedge x \in B\}$

È generalizzato con famiglia non vuota  $\{A_\alpha\}_{\alpha \in I}$  di insiemni, come:

$\bigcup_{\alpha \in I} A_\alpha = \{x \in A_\alpha \text{ per qualche } \alpha \in I\}$

$\bigcap_{\alpha \in I} A_\alpha = \{x \in A_\alpha \text{ per ogni } \alpha \in I\}$

//

Un insieme UNIVERSO con elementi interessati.

COMPLEMENTO:  $\bar{A} = \{x \in U \mid x \notin A\}$

$\Rightarrow B \setminus A = \{x \in B \mid x \notin A\}$

Rappresentazione grafica con diagrammi di VENN

P. CARTESIANO:  $A \times B = \{(a, b) \mid a \in A, b \in B\}$

l'insieme **DEUE PARTI** (dei sottinsieme) di un altro insieme:  $P(A) = \{B \mid B \subseteq A\}$ .  
 è un **SINGLETON** se ha un solo elemento:  $\{a\}$

|| in un calcolatore  $U$  è l' $n$ -pla  $(a_1, \dots, a_n)$ .  
 es.  $U = \{a_1, a_2, a_3, a_4, a_5, a_6\}$   
 $A = \{a_2, a_5, a_6\}$   
 $\Rightarrow A : (0, 1, 0, 1, 1, 0)$  ||

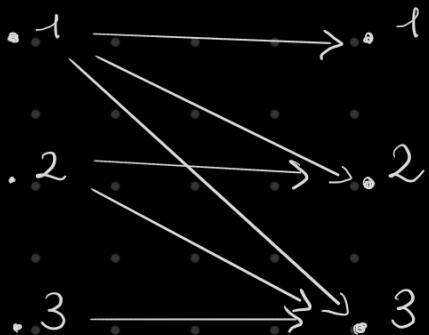
## 2) RELAZIONI

una **RELAZIONE**  $\mathcal{g}$  da  $A$  a  $B$  è un sottinsieme di  $A \times B$ ,  
 se  $A = B \Rightarrow \mathcal{g}$  è su  $A$ .

per  $(a, b) \in \mathcal{g}$  scriviamo  $a \mathcal{g} b$ ,  $a \xrightarrow{\mathcal{g}} b$ ,  $b = g(a)$   
 al livello grafico:

$\mathcal{g} : \leq$  su  $S = \{1, 2, 3\}$

$$\Rightarrow \mathcal{g} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$



|               |   |   |   |
|---------------|---|---|---|
| $\mathcal{g}$ | 1 | 2 | 3 |
| 1             | 1 | 1 | 1 |
| 2             | 0 | 1 | 1 |
| 3             | 0 | 0 | 1 |

**INVERSA**  $\mathcal{g}^{-1}$  da  $B$  ad  $A \Rightarrow b \mathcal{g}^{-1} a$ .

$$\mathcal{g}^{-1} = \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$$

una  $\mathcal{g}$  **DI EQUIVALENZA** soddisfa 3 proprietà:

- 1) **P. RIFLESSIVA**:  $a \mathcal{g} a \quad \forall a \in A$ ;
- 2) **P. SIMMETRICA**:  $a \mathcal{g} b \Rightarrow b \mathcal{g} a \quad \forall a, b \in A$ ;
- 3) **P. TRANSITIVA**:  $a \mathcal{g} b, b \mathcal{g} c \Rightarrow a \mathcal{g} c \quad \forall a, b, c \in A$ .

se  $\mathcal{g}$  di equivalenza  $\Rightarrow a$  è equivalente a  $b$

una **CLASSE DI EQUIVALENZA** modulo  $\mathcal{g}$  di  $a \in A$ :  
 $[a] = \{b \in A \mid b \mathcal{g} a\}$

$[a] = [b] \Leftrightarrow a \sim b$  con  $\sim$  su  $A$

INSIEME QUOTIENTE di  $A$  su  $\sim$ :  $A/\sim = \{[a] \mid a \in A\}$

una PARTIZIONE  $A_\alpha$  di  $A$  contiene parti non vuote di  $A$ , rispetta le condizioni:

1)  $\bigcup_\alpha A_\alpha = A$  ( $A$  è ricoperto)

2)  $A_\alpha \cap A_\beta \neq \emptyset \Leftrightarrow A_\alpha = A_\beta$  (coincidenza o disgiunzione)

THM:  $\sim$  di equivalenza su  $A$ .

l'insieme delle  $[a]$  formano una partizione di  $A$ .

THM: ogni partizione di  $A$  determina una  $\sim$  di equivalenza su  $A$ , dove i sottosezioni della partizione sono classi di equivalenza.

$\sim$  ANTI SIMMETRICA su  $A$  se  $a \sim b$ ,  $b \sim a \Rightarrow a = b$

$\sim$  RELAZIONE DI ORDINE PARZIALE su  $A$  se è riflessiva, antisimmetrica e transitiva  $\Rightarrow A$  è cioè PARZIALMENTE ORDINATO di  $\sim$ . ( $\subseteq$ )

quindi non tutte le coppie devono essere confrontabili, se  $a \neq b \Rightarrow A$  è TOTALMENTE ORDINATO (o totale). ( $\leq$ )

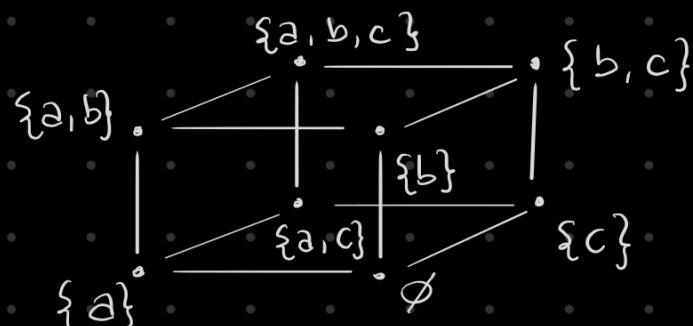
$\sim$  relazione d'ordine con  $\leq$

es.  $A = P(X)$

$$X = \{a, b, c\}$$

ordinato per  $\subseteq$

$$\Rightarrow P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$$



### 3) FUNZIONI

una **FUNZIONE** (o applicazione)  $f$  da  $A$  a  $B$  è una legge che associa ad ogni elemento di  $A$  un elemento di  $B$ .  $f: A \rightarrow B$  (o corrispondenza)

$f$  ha **DOMINIO**  $A$  e **CODOMINIO**  $B$ :  $b = f(a)$  è **IMMAGINE** di  $a$  mediante  $f$ .

$F$  sottoinsieme (relazione), da  $A$  a  $B$ , di  $A \times B$  con  $F = \{(a, f(a)) \mid a \in A\}$  è il **GRAFICO**: ogni  $a$  compare solo in una coppia.

Funzione  $\Rightarrow$  relazione  
l'immagine  $f(S)$  di  $S$  è il sottoinsieme:  
 $f(S) = \{b \in B \mid b = f(s) \text{ per qualche } s \in S\}$   
indicata anche con  $\text{Im } f$ .

la **CONTROIMMAGINE** (inversa) di  $T$  è:

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}$$

c'è sono più tipi di funzioni:

1) **INIETTIVA**:

$$\forall a, a' \in A \quad f(a) = f(a') \Rightarrow a = a'$$

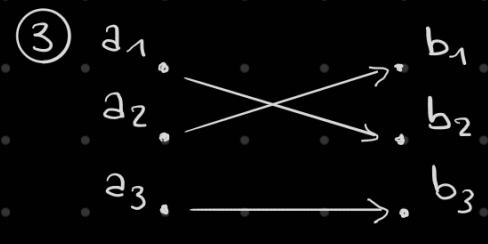
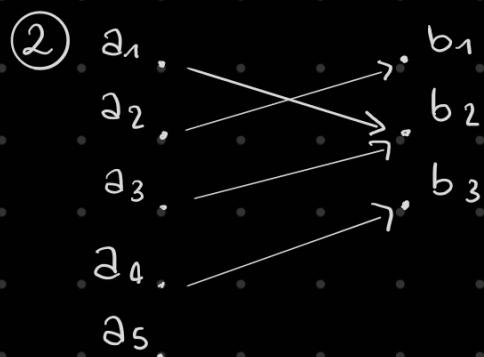
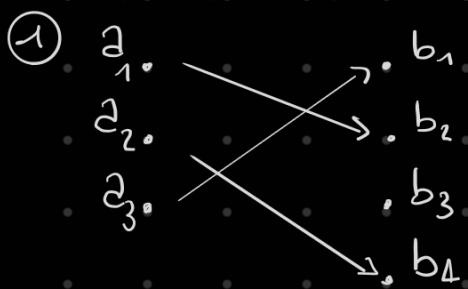
2) **SURIETTIVA**:

$\text{Im } f = B$  o wero

$$\forall b \in B \exists a \in A \mid f(a) = b$$

3) **BIUNIVOCÀ** (o BIUNIVOCA)

iniettiva e suriettiva insieme



4) **COMPOSTA**:

$f: A \rightarrow B$ ,  $g: B \rightarrow C$   
 $\Rightarrow g \circ f: A \rightarrow C$  definita come  
 $(g \circ f)(a) = g(f(a)) \quad \forall a \in A$   
 la composizione è associativa:  
 $h \circ (g \circ f) = (h \circ g) \circ f$

// le eiettive hanno una sola funzione inversa, la cui immagine è un singleton.  
 negli altri casi non si parla di funzione per il loro caso inverso. //

### 5) IDENTICA:

$i_X: X \rightarrow X \mid i_X(x) = x \quad \forall x \in X$   
 se  $f: A \rightarrow B$  è eiettiva  
 $\Rightarrow f^{-1} \circ f = i_A \quad \text{e} \quad f \circ f^{-1} = i_B$

**THM:**  $X$  insieme e  $2 = \{0, 1\}$   
 $\Rightarrow \exists$  CORRISPONDENZA BIUNIVOCATA tra  $P(X)$  e  
 l'insieme  $2^X$  delle funzioni da  $X$  a  $\{0, 1\}$ .

$f: A \rightarrow B \Rightarrow$  si definisce  $g_f$  in  $A$  come segue:  
 $a \sim_f b \Leftrightarrow f(a) = f(b)$   
 come relazione di equivalenza.  
 se  $b \in \text{Im } f \Rightarrow f^{-1}(\{b\})$  di  $A$  è FIBRA su  $b$ .  
 le fibre formano una partizione di  $A$  determinata da  $f$ : sono elementi del quoziente  $A/f$   
 se  $f$  definita su  $A \Rightarrow$  quoziente  $A/f$  e si ha  
 la funzione suriettiva  $\pi$  detta PROIEZIONE CANONICA  
 su  $A/f$ :  $\pi: A \rightarrow A/f$ ,  $a \mapsto [a]$ ,  $\pi = f$

4)  $\mathbb{N}$  è il PRINCIPIO DI INDUZIONE MATEMATICA

$\mathbb{N}$  è l'insieme dei NUMERI NATURALI definito dai POSTULATI DI PEANO (assiomi): si ha la terna  $(\mathbb{N}, \sigma, 0)$  con  $\mathbb{N}$  insieme,  $\sigma : \mathbb{N} \rightarrow \mathbb{N}$  e  $0 \in \mathbb{N}$  tali che:

- $\sigma$  è iniettiva
- $0 \in \text{Im } \sigma$
- $\forall U \subseteq \mathbb{N}$  si ha  $0 \in U$  e  $k \in U \Rightarrow \sigma(k) \in U \ \forall k$  preso  $n \in \mathbb{N} \Rightarrow \sigma(n)$  è il suo SUCCESSIVO; è quindi definita  $\leq$  d'ordine  $\leq$

il 3° postulato è il PRINCIPIO DI INDUZIONE MATEMATICA:  $U = \mathbb{N}$

se  $(A, \sigma, 0)$  e  $(A', \sigma', 0')$  verificano i postulati  $\Rightarrow$  sono identici e c'è corrispondenza biunivoca  $\phi$  tra loro:  $\sigma'(\phi(n)) = \phi(\sigma(n))$ .

(accetta che  $\exists \mathbb{N}$  che verifica Peano)

una OPERAZIONE BINARIA è un'operazione di un insieme  $S$  che associa a ogni coppia  $(s_1, s_2) \in S \times S$  un elemento  $s_1 + s_2 \in S$

es. unione tra sottoinsiemi di un insieme:

$$\cup : P(X) \times P(X) \rightarrow P(X) \quad (A, B) \mapsto A \cup B$$

addizione tra interi in  $\mathbb{Z}$ :

$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \quad (a, b) \mapsto a + b$$

||  $a + b \in \mathbb{Z}$  è SOMMA ||

l'operazione è n-aria se com vali  $n$ .

una STRUTTURA ALGEBRICA è un insieme dotato di almeno un'operazione n-aria sull'insieme stesso e che soddisfa gli assiomi.

si definiscono con Peano le operazioni di:

1) SOMMA:

$$n, m \in \mathbb{N}$$

$$n+m = \begin{cases} \underbrace{\sigma(\sigma(\dots\sigma(n))))}_{m \text{ volte}} & \text{se } m > 0 \\ n & \text{se } m = 0 \end{cases}$$

$$\Rightarrow 1 = \sigma(0) \quad e \quad \sigma(n) = n+1$$

## 2) PRODOTTO:

$n, m \in \mathbb{N}$

$$n \cdot m = \begin{cases} \underbrace{n + \dots + n}_{m \text{ volte}} & \text{se } m > 0 \\ 0 & \text{se } m = 0 \end{cases}$$

(da queste ho commutatività e associatività di addizione e moltiplicazione, distributività e elemento neutro dell'addizione, elemento neutro della moltiplicazione)

con il 3° postulato ho le **DIMOSTRAZIONI PER INDUZIONE**.

altre due formalizzazioni del principio sono:

1) ogni  $V \subseteq \mathbb{N}$ , se sono aspettate:

$$\cdot 0 \in V$$

$$\cdot n \in V \text{ quando } k \in V \quad \forall k \mid 0 \leq k \leq n$$

$$\Rightarrow V = \mathbb{N}$$

2) **PRINCIPIO DEL BUON ORDINAMENTO (o MINIMO)**

$T \subseteq \mathbb{N} \mid T \neq \emptyset \Rightarrow T$  contiene un minimo

ovvero  $\exists t \in T \mid t \leq x \quad \forall x \in T$

$X$  è **BEN ORDINATO** se ogni suo sottosinsieme ha un minimo  $\Rightarrow \mathbb{N}$  è bene ordinato.

con ② dimostro che  $\nexists c \in \mathbb{N} \mid 0 < c < 1$

seguo  $a, b \in \mathbb{N} \mid b \neq 0 \Rightarrow \exists q, r \in \mathbb{N} \mid$

$$a = bq + r, \quad 0 \leq r < b$$

una RELAZIONE RICORSIVA ha delle CONDIZIONI INIZIALI: l' $n$ -esimo termine dipende dal precedente ed è

è espresso da una FORMULA CHIUSA che si fornisce una soluzione (la relazione da solo non informa di informazione locale).

## 5) CARDINALITÀ DI INSIEMI

A e B hanno stessa CARDINALITÀ (o potenza), o sono EQUIPOTENTI, se c'è tra di essi una corrispondenza biunivoca (è una relazione d'equivalenza):  $A \sim B$ .  
la cardinalità di A è  $\text{Card}(A)$ .

A è FINITO se per qualche  $n \in \mathbb{N}$   $|n \neq 0|$

$\Rightarrow A \sim I_n = \{0, \dots, n-1\}$ ,  
altrimenti è INFINTO

(cardinalità = n° di elementi)

$\text{Card}(I_n) = n$ ,  $\text{Card}(\mathbb{N}) = \aleph_0$  (alef-zero)

↪ POTENZA DEL NUMERABILE

ogni insieme che ha corrispondenza biunivoca con  $\mathbb{N}$  ha la stessa potenza.

THM: l'unione di un numero finito o di un'infinità di numerabili di insiemi numerabili ha la  $\text{Card}(\mathbb{N})$

gli insiemi  $\mathbb{Z}$  e  $\mathbb{N} \times \mathbb{N}$  sono numerabili.

$\text{Card}(A) \leq \text{Card}(B)$  se  $\exists f: A \rightarrow B$  iniettiva, se  
 $\text{Card}(A) \neq \text{Card}(B) \Rightarrow \text{Card}(A) < \text{Card}(B)$ .

la POTENZA DEL CONTINUO è  $\text{Card}(2^{\mathbb{N}})$ .

$\text{Card}(2^{\mathbb{N}}) > \text{Card}(\mathbb{N})$  }  
 $\text{Card}(2^{\mathbb{N}}) = \text{Card}(\mathbb{R})$  }

l'IPOTESI DEL CONTINUO dice che non si determina la tesi quella del numerabile e quella del continuo, ma non è dimostrabile.

l'IPOTESI GENERALIZZATA DEL CONTINUO dice che  $\forall X \in$

finito  $\exists$  insieme di potenza intermedia tra quella di  $X$  e quella di  $P(X)$ .

## // ASSIOMA DI ZERMEOLO (o della scelta):

classe  $X \neq \emptyset$  di insiemi  $\neq \emptyset$

$\Rightarrow \exists f$  che  $\forall I_\alpha \in X$  associa  $x_\alpha \in I_\alpha$ .

ovvero ogni insieme ha un rappresentante equivalente al THM all'uno ordinamento. //

## 6) CALCOLO COMBINATORIO

dati  $A$  e  $B$  con  $n$  elementi ciascuno  $\Rightarrow$  il n° di corrispondenze biviniche tra loro è  $n!$

se assegnano  $f(x_1), \dots, f(x_n)$  con  $A = \{x_1, \dots, x_n\}$   
 $f: A \rightarrow B$  biuniva  $\Rightarrow f(x_1)$  è un qualunque valore di  $B$  che è  $\neq f(x_1)$  e così via.

se  $A = B \Rightarrow$  le corrispondenze sono PERMUTAZIONI

$S(X)$  è l'insieme delle permutazioni di  $X$ : una composizione di  $S(X) \in S(X)$  ed è associativa.

$\exists i_X$  neutro alla composizione  $| i_X \circ f = f \circ i_X = f \forall f \in S(X)$ .

pueso  $f \in S(X) \Rightarrow \exists f^{-1} \in S(X) | f \circ f^{-1} = f^{-1} \circ f = i_X$

$S(X)$  è un GRUPPO: struttura algebrica.

se  $A$  ha  $n$  elementi e  $B$  ne ha  $m \Rightarrow$  il n° di applicazioni tra i due è  $m^n$ .

con il COEFFICIENTE BINOMIALE. conto quanti sottoinsiemi di  $k$  elementi di un insieme da  $n$  elementi esistono (combinazioni).

$$\binom{n}{k} = \frac{n!}{k! (n-k)!}$$

$$\text{con } \binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

mi permette di

costituire il TRIANGOLO DI TARTAGLIA.

## 2 - I NUMERI

### 1) I NUMERI INTERI

uso  $\mathbb{Z}$  per risolvere equazioni di tipo  $x+n=0$ : è lo insieme degli interi relativi. per spiegare la sua parte negativa parto da  $\mathbb{N} \times \mathbb{N}$  e considero le coppie ordinate di numeri per cui vale:

$$(n, m) \sim (n', m') \iff n + m' = m + n'$$

è una relazione di equivalenza:  $\mathbb{N} \times \mathbb{N}$  è diviso in classi  $(n, m)$  che hanno un rappresentante dove  $n \neq m = 0$ .

$\Rightarrow \mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$  e si decomponga in:

$$\mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^- \text{ dove}$$

$$\cdot \mathbb{Z}^+ = \left\{ \overline{(n, 0)} \mid n \in \mathbb{N}, n \neq 0 \right\} \quad \text{intere positivi}$$

$$\cdot 0 = \overline{(0, 0)}$$

$$\cdot \mathbb{Z}^- = \left\{ \overline{(0, n)} \mid n \in \mathbb{N}, n \neq 0 \right\} \quad \text{intere negativi}$$

$\mathbb{Z}^+ \cup \{0\} = \mathbb{N}$ : è una funzione:  $\mathbb{N} \rightarrow \mathbb{Z}$  iniettiva che associa  $\forall n \in \mathbb{N}$  la classe  $\overline{(n, 0)}$ .

definisce le due operazioni:

$$\cdot \overline{(n, m)} + \overline{(n', m')} = \overline{(n+n', m+m')}$$

$$\cdot \overline{(n, m)} \cdot \overline{(n', m')} = \overline{(nn' + mm', nm + nn')}$$

indichiamo le  $z \in \mathbb{Z}$  come:

$$\overline{(n, 0)} = n, \quad \overline{(0, 0)} = 0, \quad \overline{(0, n)} = -n$$

$\mathbb{Z}$  ha le seguenti proprietà: commutatività, elt. neutro e associatività dell'addizione, elt. opposto, commutatività, associatività e elt. neutro della moltiplicazione, distributività della moltiplicazione sull'add.

un ANELLO COMMUTATIVO CON UNITÀ soddisfa tutte le proprietà precedenti:  $\mathbb{Z} (+, \cdot)$

sia  $a, b \in \mathbb{Z}$ , allora ho:

$$1) a \cdot 0 = 0 \cdot a = 0$$

$$2) (-a) \cdot b = - (a \cdot b)$$

$$3) (-a) \cdot (-b) = a \cdot b$$

$$a \cdot b = 0 \text{ sse } a=0 \text{ o } b=0.$$

il **VALORE ASSOLUTO** di  $a \in \mathbb{Z}$  è:

$$|a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$$

$$\text{vole che } |a| + |b| = |a+b| \text{ e } |a| \cdot |b| = |a \cdot b|.$$

deti  $a, b \in \mathbb{Z} \Rightarrow a \text{ DIVIDE } b \left( \frac{a}{b} \right) \text{ se } \exists c \in \mathbb{Z} \mid b = ac$ , altrimenti  $a \nmid b$ .

in veue se  $a \neq 0$  è **DIVISORE DEL ZERO** se  $\exists b \neq 0 \mid ab = 0$ .

un **DOMINIO D'INTEGRITÀ** è un anello privo di divisiore dello zero,  $\Rightarrow \mathbb{Z}$  è dominio d'integrità.

un **DIVISORE COMUNE** di  $a, b \in \mathbb{Z}$  è  $c \in \mathbb{Z} \mid c \mid a, c \mid b$ .

se  $\exists c$  divisore comune di  $a$  e  $b \Rightarrow c$  divide ogni  $n \in \mathbb{N} \mid n = sa + tb$  con  $s, t \in \mathbb{Z}$ , ovvero

$$\frac{c}{a} \text{ e } \frac{c}{b} \Rightarrow \frac{c}{sa+tb} \quad \forall s, t \in \mathbb{Z}$$

una **UNITÀ** è un  $a \in \mathbb{Z}$  che divide 1 (elt. invertibile).

in  $\mathbb{Z}$  sono 1 e -1.

$a$  e  $b$  sono **ASSOCIAZIONI** se  $\frac{a}{b}$  e  $\frac{b}{a}$ : ovvero solo  $a = ub$  (opposti).

$a \in \mathbb{Z}$  è **IRRIDUCIBILE** se  $a \neq 0$ ,  $a \neq u$  e  $a = bc$  con  $b, c \in \mathbb{Z} \Rightarrow b$  o  $c$  unità.

$a \in \mathbb{Z}$  è **PRIMO** se  $a \neq 0$ ,  $a \neq u$  e  $\frac{bc}{a}$  con  $b, c \in \mathbb{Z} \Rightarrow a$  divide  $b$  o  $c$ .

ogni  $a \in \mathbb{Z} \mid a$  privo è irriducibile

2) MCD E ALGORITMO EUCLideo

$a, b \in \mathbb{Z} \Rightarrow \text{MCD}(a, b) = d \in \mathbb{Z} \mid$

- $d/a$  e  $d/b$
- se  $d'/a$  e  $d'/b \Rightarrow d'/d$
- $a, b \in \mathbb{Z} \mid \text{MCD}(a, b) = 1$  sono **COPRIMI**.
- DIVISIONE**:  $a, b \in \mathbb{Z}$  e  $b \neq 0 \Rightarrow \exists q, r \in \mathbb{Z} \mid a = bq + r \quad 0 \leq r < |b|$

**THM**: ESISTENZA DEL MCD IN  $\mathbb{Z}$

$$a, b \in \mathbb{Z} \mid a \neq 0 \vee b \neq 0 \Rightarrow \exists d = \text{MCD}(a, b) \wedge \exists s, t \in \mathbb{Z} \mid d = sa + tb.$$

↳ **IDENTITÀ DI BEZOUT**: calcola

tutte le tante  $x, y$  tali che  $ax + by = c$  ha soluzioni solo se  $\text{MCD}(a, b) = d \mid c$ ,  
se  $c \in \mathbb{Z}$  irriducibile  $\Rightarrow$  2 punti.

### 3) FATTORIZZAZIONE IN $\mathbb{Z}$ E CONSEGUENZE

**THM**: FONDAMENTALE DEL' ARITMETICA

$n \in \mathbb{Z} \mid n > 1 \Rightarrow n$  è fattorizzabile in un prodotto di numeri irriducibili  $p_j > 1$ .  
ogni  $z \in \mathbb{Z}$  ha un'unica forma di scrittura in fattorizzazione.

- $a, b \in \mathbb{Z} \Rightarrow \text{mcm}(a, b) = m \mid$
- $m$  multiplo di  $a$  e di  $b$ .
- se  $m'$  multiplo di  $a$  e di  $b \Rightarrow m'$  multiplo di  $m$ .

$$\mid a \cdot b \mid$$

$$\Rightarrow \text{mcm}(a, b) = \frac{|a \cdot b|}{\text{MCD}(a, b)}$$

$\exists \infty$  numeri pari

### 4) I NUMERI RAZIONALI

uso  $\mathbb{Q}$  per risolvere  $ax = b$  con  $a, b \in \mathbb{Z}$  e  $a \neq 0$ .

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) / \sim \quad \text{e si ha:}$$

$(a, b) \sim (c, d) \Leftrightarrow ad = bc$

i suoi elt. sono  $\overline{(a, b)}$

abbiamo le operazioni:

$$\begin{aligned} \cdot \quad \overline{(a, b)} + \overline{(c, d)} &= \overline{(ad + bc, bd)} \\ \cdot \quad \overline{(a, b)} \cdot \overline{(c, d)} &= \overline{(ac, bd)} \end{aligned}$$

i risultati sono in  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

le classi  $0 = \overline{(0, 1)} = \overline{(0, b)}$  e  $1 = \overline{(1, 1)} = \overline{(a, a)}$  sono elt. neutri  $\Rightarrow \mathbb{Q}$  è un anello.

Inoltre  $\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$   $\forall a, b | a \neq 0, b \neq 0$

L'insieme  $\mathbb{Q}$  è un campo e estende  $\mathbb{Z}$ .

Si scrivono gli elt in  $\mathbb{Q}$  come  $uv^{-1}$  con  $u, v \in \mathbb{Z}$  e  $v \neq 0$ :

$\Rightarrow \overline{(a, b)} = \overline{(a, 1)} \overline{(1, b)} = a/b$

## // 5) I NUMERI DI FIBONACCI //

### 6) CONGRUENZE: PRIME PROPRIETÀ E APPLICAZIONI

Una relazione di congruenza modulo un intero positivo  $n$

identifica  $a, b \in \mathbb{Z} | a - b = d$  e  $d$  multiplo di  $n$ , quindi:

$a \equiv b \pmod{n}$  se e solo se  $a \equiv b \pmod{n} \Leftrightarrow a - b = nh$  per  $h \in \mathbb{Z}$ .

Ogni intero  $a \equiv r \pmod{n} | 0 \leq r < n$ .

Sia  $n \in \mathbb{Z} | n > 0 \Rightarrow \equiv_n$  è relazione d'equivalenza.

Presi  $a, b, c, d \in \mathbb{Z} \Rightarrow$  valgono le proprietà:

$$a \equiv b \pmod{n}, c \equiv d \pmod{n} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \end{cases}$$

Le classi d'equivalenza sono:

$$\overline{0} = \{kn | k \in \mathbb{Z}\} \text{ e } \overline{1} = \{kn + 1 | k \in \mathbb{Z}\}$$

$$\text{fino } \overline{n-1} = \{kn + n - 1 | k \in \mathbb{Z}\}$$

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$$

$n \in \mathbb{Z} \mid n > 0 \Rightarrow \forall a, b, c, d \in \mathbb{Z} \quad \text{se } a \equiv b \pmod{n}$

$$\Rightarrow \begin{aligned} &\bullet a+c \equiv b+c \pmod{n} \\ &\bullet ac \equiv bc \pmod{n} \end{aligned}$$

$$\bullet a^i \equiv b^i \pmod{n} \quad \forall i \in \mathbb{N}$$

$$\bullet ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}} \quad \text{con } d = (c, n)$$

$$\forall p \text{ primo e } x, y \in \mathbb{Z} \Rightarrow (x+y)^p \equiv x^p + y^p \pmod{p}$$

### THM: PICCOLO TEOREMA DI FERMAT

$$a \in \mathbb{Z} \text{ e } p \text{ primo } \Rightarrow a^p \equiv a \pmod{p}$$

$$\text{se } (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

### CRITERIO DI DIVISIBILITÀ:

per 3/9: sommo cifre e vedo se è multiplo di 3/9

per 2/5: se la cifra 2 destra è divisibile per 2/5

per 4: se le due cifre 2 destra sono divisibili per 4/25

per  $2^k$ : se le ultime  $k$  cifre sono divisibili per  $k$

per 11: se  $\sum_{i=0}^n (-1)^i a_i$  è divisibile per 11

### 7) RISOLUZIONE DI CONGRUENZE E THM CINESE DEL RESTO

una CONGRUENZA LINEARE in  $x$  è un'equazione tipo

$ax \equiv b \pmod{n}$  con  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ : ammette soluzioni solo se  $(a, n) \mid b$ . Le soluzioni ottenibili sono nella forma:

$$x_0 + h \cdot \frac{n}{(a, n)} \quad \text{con } h \in \mathbb{Z} \text{ e } x_0 \text{ soluzione}$$

Sono tutte congruenti tra loro e sono  $(a, n)$ .

Se  $(a, n) = 1 \Rightarrow ax \equiv b \pmod{n}$  ha solo 1 soluzione

$$\left\{ \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \end{array} \right.$$

$$\left\{ \begin{array}{l} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \end{array} \right. \quad \text{con } (n_i, n_j) = 1$$

per  $i \neq j$

$$\Rightarrow \text{si risolve} \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \vdots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

e' necessario che  $\text{MCD}(a_k, n_k) \mid b_k \quad \forall k \in \mathbb{N}$

THM: TEOREMA CHINSE DEL RESTO

$$r_1, \dots, r_s \in \mathbb{Z} \mid r_1, \dots, r_s > 0 \mid (r_i, r_j) = 1 \text{ con } i \neq j \Rightarrow \begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \vdots \\ x \equiv c_s \pmod{r_s} \end{cases}$$

ammette soluzione unica modulo  $r_1, \dots, r_s$

8) FUNZIONE E THM DI EULERO

---



---



---

# FINE APPUNTI LIBRO



## → GRUPPO

un **GRUPPO**  $(G, *)$  è un insieme dotato di un'operazione binaria che verifica le proprietà:

1) associativa,  $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

2)  $\exists$  elt. neutro |  $e * a = a * e = a \quad \forall a \in G$

3)  $\forall a \in G \exists a' \in G$  inverso ad  $a$  |  $a * a' = a' * a = e$

se  $*$  è commutativa  $\Rightarrow G$  è **ABEUANO** (o commutativo).

**PROPOSIZIONE**: l'elt. neutro è unico.

l'elt. inverso è unico.

un sottogruppo  $S$  di  $G$  non vuoto è un gruppo verso la medesima operazione di  $G$ : e è l'inverso  $\in S$ .

## → PERMUTAZIONI

un **GRUPPO SIMMETRICO** è un insieme di permutazioni.  $|S_n| = n!$  si indica con  $\sigma$  la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (123)(45) \rightsquigarrow \text{prodotto di cicli}$$

$S_n$  è associativo e ha elt neutro e inverso: se ha più di 3 elt  $\Rightarrow$  non è chiuso.

$A_n \subseteq S_n$  contiene le permutazioni pari (con segno +1) e  $|A_n| = n!/2$ .

il n° di trasposizioni, che formano un ciclo, dà la parità:

es.  $\sigma = (123)(45)$  ↗ ordine 3 ↘ ordine 2

$$\text{Ordine } (\sigma) = \text{mcm}(3, 2) = 6$$

es.  $\sigma = (143) = (13)(14)$  è pari (2 trasposizioni)

es.  $\sigma = (142)(35)$

$$\sigma^{-1} = (241)(53)$$

es. generale

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 2 & 3 & 1 \end{pmatrix} = (1\ 4\ 2\ 6)(3\ 5)$$

$$\text{Ordine } (\sigma) = \text{mcm}(4, 2) = 4$$

$$\sigma = (14)(12)(16)(35) \Rightarrow \text{pari}$$

$$\sigma^{-1} = (6\ 2\ 4\ 1)(5\ 3)$$

$$\Rightarrow (a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_1\ \dots)\ \dots\ (a_1\ a_k)$$

per scomporre i cicli in trasposizioni

VI ST  
DA  
SOLA



# APPUNTI LEZIONI

## → ANELLO

a) se  $A = \{ \} \mid A \neq \emptyset$  è insieme di 2 o più elementi finiti  
+ e:  $\Rightarrow$  si ha  $(A, +, \cdot)$

↪ supporto / sostegno dell'anello

valgono le seguenti proprietà:

- 1)  $(A, +)$  è un gruppo abeliano
- 2)  $(A, \cdot)$  dove  $\cdot$  è associativa
- 3) LEGGI DISTRIBUTIVE:  $\forall a, b, c \in A$

$$\text{se } a \cdot (b+c) = a \cdot b + a \cdot c \Leftrightarrow (b+c) \cdot a = ba + ca$$

4) se  $(A, \cdot)$  commutativo  $\Rightarrow A$  commutativo

5) A unitario se  $(A, \cdot)$  ha elt. neutro.

es.  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo e unitario

## → MATEMATICA

$m, n \geq 1$   $M_{m,n}(\mathbb{R})$  è l'insieme delle matrici a coefficienti reali in  $\mathbb{R}$  di dimensione  $m \times n$  con  $m$  righe e  $n$  colonne.

$\Rightarrow M = (m_{i,j})$  con  $i \in \{1, \dots, m\}$ ,  $j \in \{1, \dots, n\}$

e  $M_{m,n}(\mathbb{R}) = \{ M = (m_{i,j}) \text{ con } i \in \{1, \dots, m\}, j \in \{1, \dots, n\} \}$

### SOMMA:

considero  $(M_{m,n}(\mathbb{R}), +)$  e  $A, B \in M_{m,n}(\mathbb{R})$  dove  $A = (a_{i,j})$  e  $B = (b_{i,j}) \Rightarrow A+B = (a_{i,j} + b_{i,j})$ .

Sono solo se hanno  $m \times n$  uguali.

**PROPOSIZIONE:** sia  $m, n \in \mathbb{N} \mid m, n \geq 1$

$\Rightarrow (M_{m,n}(\mathbb{R}), +)$  è un gruppo abeliano

### PRODOTTO:

si considera  $m = n \Rightarrow$  M quadrata di ordine  $n$

$A = (a_{i,j})$  e  $B = (b_{i,j})$

$A \cdot B = C = (c_{i,j})$  dove  $c_{i,j} = \sum_{l=1}^n a_{i,l} \cdot b_{l,j}$

**PROPOSIZIONE:**  $(M_{m,n}(\mathbb{R}), +, \cdot)$  è un anello unitario e non commutativo

dimo: unitario perché  $I_n = I = (m_{i,j})$  matrice di identità è l'el. neutro

$$m_{i,j} = \begin{cases} 1 & \text{se } i=j \\ 0 & \text{altimenti} \end{cases} \quad (\text{id})$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\forall A \in M_{m,n}(\mathbb{R}) \quad A \cdot I_n = A$$

non abeliano perché il prodotto tra matrici non è commutativo  $A \cdot B \neq B \cdot A$ .

es. anello dei polinomi a coefficienti reali in una indeterminata  $x$ :  $\mathbb{R}[x] = \{ \text{polinomi}, p(x) = \sum_{i=0}^n a_i x^i \text{ con } a_i \in \mathbb{R} \text{ e } n \geq 0 \}$

$(\mathbb{R}[x], +, \cdot)$  è un anello unitario e abeliano.

el. neutro è  $1 = 1 \cdot x^0$

## → CAMPO

anche detto corpo commutativo.

sia  $(A, +, \cdot)$  anello  $\Rightarrow A$  è un campo se  $(A, +)$  e  $(A \setminus \{0\}, \cdot)$  sono gruppi abeliani.

es.  $(\mathbb{Q}, +, \cdot)$  è campo dei numeri razionali.

es.  $(\mathbb{R}, +, \cdot)$  è campo dei numeri reali.

## → RELAZIONE

**RELAZIONE BINARIA**: sia  $X$  insieme  $| X \neq \emptyset$

sia  $R \subseteq X \times X$  relazione binaria.

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

una **RELAZIONE DI EQUIVALENZA**  $R$  è tale su  $X$  se:

1) p. riflessiva:  $\forall a \in X \quad a Ra \Leftrightarrow (a, a) \in R$

2) p. simmetria:  $\forall a, b \in X \quad aRb \Leftrightarrow bRa$

3) p. transitività:  $\forall a, b, c \in X \quad aRb, bRc \Leftrightarrow aRc$

se  $R$  di equivalenza  $\Leftrightarrow a = b$  equivalente

es.  $X$  insieme,  $a, b \in X$ ,  $aRb$  e  $a = b$

$\Rightarrow R$  d'equivalenza

es.  $X = \{zette del piano euclideo\}$

$r, r' \in X$  e  $rRr'$ , se  $r \parallel r' \Rightarrow R$  d'equivalenza

sia  $R$  d'equivalenza su  $X$ ,  $a \in X$  è **CLASSE D'EQUIVALENZA** di  $X$  |  $[a] = \{b \in X \mid aRb\}$ .  $a$  è **RAPPRESENTANTE** di  $[a]$ .

l'**INSIEME QUOTIENTE** di  $X$  su  $R$  ( $X$  modulo  $R$ ) è

l'insieme  $X/R = \{[a] \mid a \in X\}$

osservazioni:

1)  $\forall a \in X \Rightarrow a \in [a]$

2)  $\forall a \in X \quad [a] \neq \emptyset$  perché  $aRa \Rightarrow a \in [a]$   $\square$

3)  $aRb \Leftrightarrow [a] = [b]$  perché  $a \in [a] = [b] \Rightarrow a \in [b] \Rightarrow aRb$   
e perché  $bRa \Rightarrow [a] \subseteq [b] \wedge [b] \subseteq [a]$   $\square$

4)  $[a], [b] \in X/R \Rightarrow [a] \cap [b] = \emptyset \oplus [a] = [b]$

5)  $X = \bigcup_{a \in X} [a]$  l'insieme è disgiunto

$\hookrightarrow$  **PARTIZIONE**

## → RELAZIONE D'ORDINE

S insieme |  $S \neq \emptyset$ , si è  $\leq$  una relazione binaria su S.

quindi  $\leq \in S \times S$ .  $\leq$  è di **ORDINE PARZIALE** se soddisfa:

1) p. riflessiva:  $\forall x \in S \quad x \leq x$ .

2) p. antisimmetrica:  $\forall x, y \in S \quad x \leq y \wedge y \leq x \Rightarrow x = y$

3) p. transitività:  $\forall x, y, z \in S \quad x \leq y \wedge y \leq z \Rightarrow x \leq z$

es.  $\mathbb{N}$  e  $\leq$  come minore o uguale

$\Rightarrow \forall a, b \in \mathbb{N} \quad a \leq b \Leftrightarrow \exists c \in \mathbb{N} \mid b = a + c$

es. S insieme e  $\mathcal{P}(S) = \{X \mid X \subseteq S\}$

$\hookrightarrow$  insieme potenza, famiglie / insieme delle parti / partizioni.

$\subseteq$  relazione di inclusione inclusistica  $X \subseteq Y$  è  
relazione d'ordine.

es.  $\mathbb{N}$  è relazione di divisibilità

$\Rightarrow a|b$  (a divide b)  $\Leftrightarrow \exists c \in \mathbb{N} \mid b = a \cdot c$ , perché

• | è riflessiva:  $a = a \cdot 1 \Rightarrow a|a$

• | è antisimmetrica:  $a|b \wedge b|a \Rightarrow a=b?$

$a|b \Leftrightarrow b = ah$  e  $b|a \Leftrightarrow a = bk$   $k, h \in \mathbb{N}$

$\Rightarrow k \cdot h \in \mathbb{N} \Rightarrow k \cdot h = 1 \Rightarrow k=1 \wedge h=1$

$\Rightarrow b = bkh \Rightarrow b = bk \Rightarrow b = 1$

• | è transitiva:  $a|b \wedge b|c \Rightarrow a|c?$

$a|b \Leftrightarrow b = ah$  e  $b|c \Leftrightarrow c = bk$

$\Rightarrow c = ahk \Rightarrow a|c$

sia  $(S, \leq)$  con  $\leq$  relazione d'ordine parziale su S

$\Rightarrow S$  è un INSIEME PARZIALMENTE ORDINATO oppure  
POSET (Partially Ordered SET)

una relazione d'ordine è TOTALE se vale che

$\forall x, y \in S \quad x \leq y \vee y \leq x$ .

es.  $(\mathbb{N}, \leq)$ ,  $\leq$  è d'ordine totale.

es.  $(\mathbb{N}, |)$ , | è solo parziale.  $3 \nmid 2$

es.  $(P(\mathbb{N}), \subseteq)$ ,  $\subseteq$  non è totale.  $\{2\} \subsetneq \{3\}$

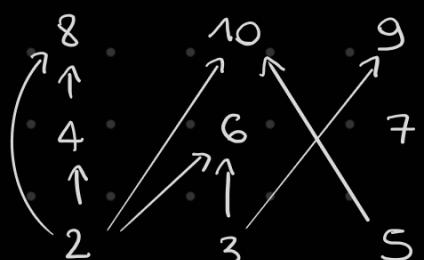
→ RAPPRESENTARE POSET

(DAG)

lo faccio tramite i DIAGRAMMI DI HASSE.

i nodi sono i valori e tra di loro c'è un arco se  
tutto se sono in relazione.

$S = \{2, \dots, 10\}$  e | relazione



## → PRINCIPIO DI INDUZIONE

sia  $P_n$  proprietà com  $n \in \mathbb{N}$ : se  $P_0$  è vera e se, fissato  $n$ ,  $P_n$  è vera  $\Rightarrow P_{n+1}$  è vera  
(base dell'induzione e passo induttivo)

$P_n$  è vera  $\forall n \in \mathbb{N}$

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

$P_0 = 0 \quad \checkmark$

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

$$n^2 + n + 2n + 2 = n^2 + 2n + n + 2$$

□

## → PRINCIPIO DEL BUON ORDINAMENTO

sia  $T \subseteq \mathbb{N} \mid T \neq \emptyset \Rightarrow T$  ammette un MINIMO,  
ovvero  $\exists m \in T \mid \forall t \in T \quad m \leq t$ .

DIMOSTRAZIONE:  $a, b \in \mathbb{N} \mid b \neq 0, b \leq a$

$$\Rightarrow \exists q, r \in \mathbb{N} \mid a = b \cdot q + r \text{ dove } 0 \leq r < b$$

↳ quoziente e resto

se  $b = a \Rightarrow q = 1$  e  $r = 0$

se  $b < a \Rightarrow T = \{x \in \mathbb{N} \mid b < x \leq a\} \neq \emptyset$

si applica il buon ordinamento  $\Rightarrow T$  ha minimo

$$m = q+1 \text{ con } q \geq 1$$

$$q+1 \text{ minimo di } T \Rightarrow q \notin T \Rightarrow b \cdot q \leq a$$

$$b(q+1) > a$$

$$\Rightarrow bq \leq a < b(q+1) \Rightarrow 0 \leq \underbrace{a - bq}_r < b$$

$$\Rightarrow bq + r = a \Rightarrow bq + a - bq = a \quad \square$$

