

Insiemi disgiunti se $A \cap B = \emptyset$

Proprietà distributiva $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

DeMorgan $\complement(A \cup B) = \complement A \cap \complement B$ e $\complement(A \cap B) = \complement A \cup \complement B$

Partizione di X Una famiglia di sottoinsiemi di X tali che:
- nessuno è vuoto;
- sono a due a due disgiunti;
- la loro unione è tutto X (= ricoprimento).

$P(X)$ è **insieme delle parti** (o insieme **quoziente**) di X ed è una partizione.

Siano A, B finiti con $|A| = n$ e $|B| = m$ allora $|A \times B| = n \cdot m$

Funzione $f: A \rightarrow B$ t.c. $\forall a \in A \exists! b \in B \mid (a, b) \in \Gamma$ dove Γ è il grafico di f
 $b = f(a)$ **immagine di a**
 $Im(f) = f(A) = \{b \in B \mid b = f(a) \text{ per qualche } a \in A\}$ **immagine di f**
 $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ **controimmagine di b**

Due funzioni sono **equivalenti** se hanno stesso dominio, stesso codominio e stesso grafico.

Funzione **identità**: $id_A: A \rightarrow A$, $id_A(a) = a \quad \forall a \in A$

- **Iniettiva** se: $\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$ oppure
 $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
- **Suriettiva** se: $Im(f) = B$ ossia $\forall b \in B \exists a \in A \mid f(a) = b$
- **Biettiva** se sia iniettiva che suriettiva

Composizione di funzioni Siano $f: A \rightarrow B$ e $g: B \rightarrow C$ $g \circ f: A \rightarrow C \quad (g \circ f)(a) = g(f(a))$
Vale la proprietà associativa: $(h \circ g) \circ f = h \circ (g \circ f)$

ATTENZIONE: in generale $g \circ f \neq f \circ g$

Se $g \circ f$ iniettiva, allora f iniettiva

Se $g \circ f$ suriettiva, allora g suriettiva

Se f e g iniettive, allora $g \circ f$ iniettiva

Se f e g suriettive, allora $g \circ f$ suriettiva

Se $g \circ f$ è biettiva, allora f iniettiva e g suriettiva

Funzione inversa di $f: A \rightarrow B$ è la funzione $g: B \rightarrow A$ tale che: $g \circ f = id_A$
 $f \circ g = id_B$

f invertibile sse è biettiva

l'inversa, se esiste, è unica f^{-1}

Due insiemi sono equipotenti se hanno la stessa cardinalità $|A| = |B|$

Se $f: A \rightarrow B$ è iniettiva, allora $|A| \leq |B|$

Se $f: A \rightarrow B$ è suriettiva, allora $|A| \geq |B|$

Un insieme A è infinito se $B \subset A$ e $|A| = |B|$ (equipotente ad un suo sottoinsieme proprio)

$I_n = \{1, 2, 3, \dots, n\}$ insieme finito dei numeri naturali

Siano A e B finiti: $|A \cup B| = |A| + |B| - |A \cap B|$

Siano A, B, C finiti: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Combinatoria

Permutazioni = scambio dell'ordine di n elementi di una sequenza (anagrammi)

- Semplici: $n!$

- Con ripetizioni: $\frac{n!}{\text{numero di volte che ogni elemento compare}(!)}$

Disposizioni = raggruppamento ordinato di k elementi estratti da un insieme che ne contiene n .

- Semplici: $\frac{n!}{(n-k)!}$

- Con ripetizioni: n^k

Combinazioni = raggruppamento di k elementi, presi in qualunque ordine, formato a partire da n elementi.

- Semplici: $\frac{n!}{(n-k)! k!}$

- Con ripetizioni: $\frac{(n+k-1)!}{(n-1)! k!}$

Coefficiente binomiale: $\binom{n}{k} = \frac{n!}{(n-k)! k!}$ (ovvero combinazioni semplici)

Binomio di newton: $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^n \binom{n}{k} y^{n-k} x^k$

Come scegliere cosa usare:

	L'ORDINE CONTA	L'ORDINE NON CONTA
ELEMENTI DISTINTI	Disposizioni semplici	Combinazioni semplici
ELEMENTI RIPETUTI	Disposizioni con ripetizione	Combinazioni con ripetizione

ALGORITMO DI EUCLIDE (MCD)

$MCD(a, b)$ con $a, b \in \mathbb{Z}$ e $b \neq 0$

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

\vdots

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \quad \rightarrow \quad r_n = MCD(a, b) \text{ ultimo resto non nullo}$$

$$r_{n-1} = r_n \cdot q_3 + 0$$

ripercorrendo la catena di uguaglianze (partendo dalla riga del MCD) trovo l'**identità di Bézout**:

$$d = A \cdot a + B \cdot b \quad \text{con } A, B \in \mathbb{Z}$$

Equazione diofantina: $ax + by = c$ con $a, b, c \in \mathbb{Z}$ e $b \neq 0$

Ha soluzione sse $MCD(a, b) \mid c$

Teorema fondamentale dell'aritmetica (fattorizzazione unica)

Ogni numero intero $\neq 0$ si scrive in modo unico come prodotto tra numeri primi.

Permutazione su X è una biezione $\sigma: X \rightarrow X$

L'insieme di tutte le permutazioni su X è S_X

$S_X \neq \emptyset$ infatti $id \in S_X$

L'operazione su S_X è la composizione

(in generale non commutativa)

Permutazioni su n elementi: S_n $|S_n| = n!$

Potenze: $\sigma^n = \sigma \circ \sigma \circ \dots \circ \sigma$ (n volte) $\sigma^0 = id$

Ciclo di lunghezza 2 = **scambio** o **trasposizione** (in questo caso $\sigma^{-1} = \sigma$)

La composizione di due cicli in generale non è un ciclo.

Due cicli sono **disgiunti** se hanno intersezione nulla \rightarrow cicli disgiunti commutano !

Ogni permutazione si scrive in modo unico come prodotto (composizione) tra cicli disgiunti.

Tipo di una permutazione = lunghezza di ogni suo ciclo disgiunto

I k -cicli in S_n sono $\binom{n}{k} (k-1)!$

Ogni permutazione si può scrivere come prodotto di trasposizioni (la scrittura non è unica)

Parità = numero di scambi che formano la permutazione.

Si può determinare anche a partire dal tipo: se k pari, allora il k -ciclo è dispari (e viceversa)

$pari \circ pari = dispari \circ dispari = pari$

$pari \circ dispari = dispari$

Periodo = minimo intero $k > 0$ tale che $\sigma^k = id$ $per(\sigma) = mcm(\text{tipo di } \sigma)$

Classe di resto mod N $[a]_N = \{b \in \mathbb{Z} \mid b \equiv a \text{ mod } N\} = \{a + kN \mid k \in \mathbb{N}\}$

Le classi di resto mod N formano una partizione di \mathbb{Z}

Rappresentante

canonico:

Ogni classe di resto mod N ha un unico rappresentante r tale che $0 \leq r \leq N-1$

$\mathbb{Z}_N = \{\text{classi di resto mod } N\}$ $|\mathbb{Z}_N| = N$

Inverso moltiplicativo: $[a]_N$ invertibile in \mathbb{Z}_N sse $MCD(a, N) = 1$

$\mathbb{Z}_N^* = \{[a]_N \mid [a]_N \text{ invertibile}\}$

$[a]_N^{-1}$ si trova calcolando l'identità di Bézout per a e N

$1 = A \cdot a + B \cdot b \rightarrow [a]_N^{-1} = [A]_N$

Zero-divisore: $[a]_N$ è uno zero-divisore sse non è invertibile in \mathbb{Z}_N , ovvero sse $MCD(a, N) \neq 1$

La **funzione di Eulero** ci dice quanti elementi contiene \mathbb{Z}_N^* ,

$\varphi(N) = |\mathbb{Z}_N^*|$ ovvero il numero di elementi che sono co-primi con N ,

ovvero il numero di elementi invertibili in \mathbb{Z}_N .

se $N = p$ primo:

- $\varphi(p) = p - 1$
- $\varphi(p^2) = p(p - 1)$
- $\varphi(p^n) = p^{n-1}(p - 1)$ con $n \in \mathbb{N}$

Siano $n, m \in \mathbb{Z}_{>1}$ e $MCD(n, m) = 1 \rightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Strutture algebriche $(A, *)$

A *semigrutto* se $*$ associativa

A *monoide* se è semigrutto e \exists *elemento neutro*

A *gruppo* se è monoide e *ogni elemento ammette un inverso*.

Commutativo/abeliano se associativo + commutativo

Convenzione: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_N$ sono gruppi rispetto alla somma.

$\mathbb{R}^*, \mathbb{Q}^*, \mathbb{Z}_N^*$ sono gruppi rispetto al prodotto.

S_n è gruppo rispetto alla composizione.

Gruppo prodotto:

Siano $(G_1, *_1) = (a_1, b_1)$ $(G_2, *_2) = (a_2, b_2)$ allora $G_1 \times G_2 = (a_1 *_1 a_2, b_1 *_2 b_2)$

$G_1 \times G_2$ commutativo sse G_1 e G_2 sono commutativi.

$|G| = \text{ordine di } G$

Se $|G_1| = n$ e $|G_2| = m$ allora $|G_1 \times G_2| = n \cdot m$

SOTTOGRUPPI H è sottogruppo di G , e si scrive $H \leq G$, se:

• H chiuso rispetto a $*$

$$a, b \in H \rightarrow a * b \in H$$

• $(H, *)$ è un gruppo

$H \neq \emptyset$ perchè $e \in H$

- l'elemento neutro di H coincide con quello di G ;
- $\forall x \in H$, l'inverso di x in H coincide con l'inverso di x in G .

Criterio per i sottogruppi Sia $(G, *)$ gruppo e $H \subseteq G$ allora $H \leq G$ sse:

• $H \neq \emptyset$

• $\forall x, y \in H \quad x * y^{-1} \in H$

Se f iniettivo \rightarrow Monomorfismo

Se f suriettivo \rightarrow Epimorfismo

Se f biiettivo \rightarrow Isomorfismo

Se $G_1 = G_2 \rightarrow$ Endomorfismo

Isomorfismo
+ \rightarrow Automorfismo
endomorfismo

Sia $(G, *)$ gruppo e $H_1, H_2 \leq G$ allora $H_1 \cap H_2 \leq G$

L'unione di sottogruppi non è in generale un sottogruppo!

Sottogruppi di \mathbb{Z} hanno la forma $N\mathbb{Z}$ per un opportuno $N \in \mathbb{N}$

Laterale sinistro di H in G $gH = \{gh \mid h \in H\}$

Laterale destro di H in G $Hg = \{hg \mid h \in H\}$

G : rappresentante del laterale

Teorema di Lagrange Sia G finito e $H \leq G$ allora $|H|$ divide $|G|$

$f: G_1 \rightarrow G_2$ **omomorfismo** se $\forall x, y \in G_1 \quad f(x *_1 y) = f(x) *_2 f(y)$

Sia f omomorfismo: • $f(e_1) = e_2$

• $f(x^n) = (f(x))^n \quad \forall x \in G_1, \forall n \in \mathbb{Z}$

sia $H \leq G_1$ allora $f(H) \leq G_2$

sia $K \leq G_2$ allora $f^{-1}(K) \leq G_1$

$f(G_1) = \text{Im}(f) \leq G_2$

$\ker(f) = \{x \in G_1 \mid f(x) = e_2\} \leq G_1$

f è un monomorfismo (iniettivo) sse $\ker(f) = \{e_1\}$

Se esiste un isomorfismo $f: G_1 \rightarrow G_2$ si scrive $G_1 \cong G_2$ ovvero sono **isomorfi**.

Due gruppi isomorfi hanno le stesse proprietà.

GRUPPI CICLICI

Sia $H = \{x^n \mid n \in \mathbb{Z}\} \leq G$

siano $z, w \in H$ t.c. $z = x^n$ e $w = x^m$

se $x * w^{-1} = x^n * x^m = x^{n-m} \in H$ allora $H = \langle x \rangle$ **sottogruppo ciclico** generato da x

se $\exists x \in G$ t.c. $\langle x \rangle = G$ allora G è **gruppo ciclico** e x è un suo **generatore**

G ciclico $\rightarrow G$ abeliano (commutativo)

G non abeliano \rightarrow non ciclico

In \mathbb{Z}_N i generatori sono tutti i $[a]_N$ invertibili rispetto alla moltiplicazione (ovvero $[a]_N \in \mathbb{Z}_N^*$)

Sia G ciclico: • Se G infinito allora $G \cong \mathbb{Z}$

• Se $|G| = N$ allora $G \cong \mathbb{Z}_N$

Periodo di $x \in G$ = ordine di $\langle x \rangle$ $per(x) = |\langle x \rangle|$

Se $per(x) = d$ finito allora d è il minimo $n \in \mathbb{Z}$ tale che $x^n = e$

Per il teorema di Lagrange: $per(x)$ divide $|G|$ e $x^{per(x)} = e$

Sia $\mathbb{Z}_n \times \mathbb{Z}_m$ gruppo prodotto: se $MCD(n, m) > 1$ allora $\mathbb{Z}_n \times \mathbb{Z}_m$ non è ciclico

$\mathbb{Z}_n \times \mathbb{Z}_m$ ciclico $\leftrightarrow MCD(n, m) = 1$

CONGRUENZE $ax \equiv b \pmod{N}$ ovvero calcolo $ax - kN = b$ (equazione diofantina)

Come si risolve:

- 1) Esiste soluzione sse $MCD(a, N) \mid b$ quindi applico Euclide
- 2) Risolvo l'identità di Bézout $1 = A \cdot a + B \cdot b$
- 3) Trovo $x \equiv$ rappresentante canonico mod N