Esercizio: $\{X_i\}_{i \in I_n}$ X_i insieme numerabile

$$\bigcup_{i \in I_n} X_i = X_1 \cup X_2 \cup \dots \cup X_n \quad \text{numerabile}$$

$$\begin{array}{ccccc}
x_1^1 & x_2^1 & x_3^1 & x_4^1 & \cdots \\
x_1^2 & x_2^2 & x_3^2 & \cdots & \\
x_1^3 & & & & \\
\vdots & & & & \\
x_1^n & x_2^n & \cdots & &
\end{array}$$

$\{X_i\}_{i \in \mathbb{N}}$ $\bigcup_{i \in \mathbb{N}} X_i$ è ancora numerabile

possibilità 1:

$$\begin{array}{cccc}
x_1^1 & x_2^1 & x_3^1 & \cdots \\
x_1^2 & x_2^2 & \cdots & \\
\vdots & & &
\end{array}$$

<u>OSS:</u> i numeri primi sono infiniti

<u>Def:</u> $p \in \mathbb{N}$, $p > 1$ _ p si dice PRIMO se i suoi unici divisori sono 1 e p stesso

Per vedere che i primi sono infiniti, si usa l'algoritmo euclideo di divisione:

se per assurdo $\exists\, k \in \mathbb{N}$ t.c. $p_1, \dots, p_k$ sono tutti i primi, potrei definire

$$q := \prod_{i=1}^{k} p_i + 1$$

q non é divisibile per nessuno dei p_i e $q \neq p_i \ \forall i$
ma q non é nemmeno divisibile per nessun altro numero naturale $\downarrow$

$X_1 = \{ x_1^1, x_2^1, x_3^1 \ \dots \}$
$X_2 = \{ x_1^2, x_2^2, \dots \}$
$X_j = \{ x_1^j, x_2^j, \dots \}$

$$q : \bigcup_{i \in \mathbb{N}} X_i \longrightarrow \mathbb{N}$$

$$x_i^1 \longmapsto 2^i$$
$$x_i^2 \longmapsto 3^i$$
$$x_i^j \longmapsto p_j^i \qquad p_j = j\text{-esimo primo}$$

CRITERIO DI DEDEKIND

X insieme è infinito $\Longleftrightarrow$ $X \approx Y$ ad un suo sottoinsieme proprio $Y \subsetneq X$

$A \subseteq B$ $\quad$ $A \subset B$ $\quad$ $A \subsetneq B$

$a \leq b$ $\quad$ $a < b$ $\quad$ $a \lneq b$

<u>lemma</u>: X insieme infinito $\Longrightarrow$ $\exists$ funzione iniettiva $\varphi: \mathbb{N} \hookrightarrow X$.

---

dim. criterio:

($\Longleftarrow$) supponiamo che $\exists$ $Y \subsetneq X$ t.c. $Y \approx X$, e supponiamo per assurdo che X sia finito.
$|X| = n < \infty$

Poiché $Y \subsetneq X$, $\exists$ funzione $f: Y \longrightarrow I_n$ iniettiva ma non suriettiva.

Cioè $\exists$ $m < n$ t.c. $Y \approx I_m$, quindi

$$I_n \approx X \approx Y \approx I_m \Longrightarrow \underset{n \neq m}{I_n \approx I_m} \quad \lightning$$

($\Longrightarrow$) supponiamo che X sia infinito e costruiamo $Y \subsetneq X$ t.c. $Y \approx X$.

Per il lemma, $\exists$ $\varphi: \mathbb{N} \hookrightarrow X$ iniettiva.

Sia $\quad Z = \mathrm{Im}(\varphi)$

$\qquad Z' = Z \setminus \varphi(1) \neq Z$

Ora costruiamo un'applicazione biettiva da Z a Z':

Oss: $\psi : \mathbb{N} \longrightarrow Z$ biettiva

(ψ è φ dove ho ristretto il codominio da X a $Z = \mathrm{Im}(\varphi)$)

$\psi' : \mathbb{N} \setminus \{1\} \longrightarrow Z'$ biettiva

$$\begin{aligned} \sigma : \mathbb{N} &\longrightarrow \mathbb{N}\setminus\{1\} \quad \text{biettiva} \\ n &\longmapsto n+1 \end{aligned}$$

$$\begin{tikzcd} Z \arrow[r, "\psi^{-1}"'] \arrow[rrr, bend right, "f"', "\text{biettiva}"] & \mathbb{N} \arrow[r, "\sigma"'] & \mathbb{N}\setminus\{1\} \arrow[r, "\psi'"'] & Z' \end{tikzcd}$$

Definiamo $Y := X \setminus \{\varphi(1)\}$ $\qquad Y \subsetneq X$

$Y = (X \setminus Z) \cup Z'$

$X = (X \setminus Z) \cup Z$

e costruiamo:
$$g : X \longrightarrow Y$$
$$x \longmapsto \begin{cases} x & \text{se } x \in X \setminus Z \\ f(x) & \text{se } x \in Z \end{cases}$$

g è una biezione per costruzione: $X \approx Y$ $\quad \#$

Prop: $\mathbb{R}$ non é numerabile.

dim: é sufficiente mostrare che $A = [0,1]$ non é numerabile.

Ogni $x \in A$ ha una <u>rappresentazione decimale</u>

$$0,x_0x_1x_2x_3 \dots \qquad x_i \in \{0,1,\dots,9\}$$

Tale rappresentazione é unica se si usa la convenzione che non si possa avere un numero infinito di cifre $\neq 0$:

$$0,2455679999\dots = 0,245568$$
$$0,999999\dots = 1$$

Supponiamo per assurdo che $\exists\, f : \mathbb{N}_0 \to A$ biettiva.

$\forall n \in \mathbb{N}_0$: $\quad f(n) = 0,x_{n,0}\,x_{n,1}\,x_{n,2}\,x_{n,3}\dots \qquad x_{n,i} \in \{0,1,\dots,9\}$

$\forall i \in \mathbb{N}_0$ scegliamo $a_i \in \{0,1,\dots,9\}$ con la proprietá $a_i \neq 0, 9, x_{i,i}$

Se definiamo $y \in A$: $\quad y = 0,a_0a_1a_2a_3a_4\dots$

Siccome f é una biezione, necessariamente $y = f(k)$ per un certo $k \in \mathbb{N}_0$

$$0,a_0a_1a_2a_3\dots = y = f(k) = 0,x_{k,0}\,x_{k,1}\,x_{k,2}\dots$$

la k-esima cifra decimale é a_k

la k-esima cifra decimale é $x_{k,k}$

$\Downarrow$

$\#$

Prop: X insieme, allora X non é equipotente al suo insieme delle parti: $X \not\sim \mathcal{P}(X)$.

dim: supponiamo che $\exists \ \varphi : X \longrightarrow \mathcal{P}(X)$ biezione.

Definiamo il sottoinsieme $Y \subseteq X$:

$$Y = \{ x \in X \mid x \notin \varphi(x) \}.$$

Siccome φ in particolare é suriettiva, $\exists \ a \in X$ t.c. $Y = \varphi(a)$.

Allora ci sono 2 possibilitá:

1) $a \in Y = \varphi(a)$, ma $Y = \{ x \mid x \notin \varphi(x) \}$
$\Longrightarrow a \notin \varphi(a) = Y$ $\lightning$

2) $a \notin Y = \varphi(a)$, allora $a \in Y = \varphi(a)$ $\lightning$

φ non puó essere suriettiva né tantomeno biettiva $\#$

GRUPPI

Def: Un gruppo $(G, \star)$ è un insieme G munito di un'operazione $\star$ che gode delle seguenti proprietà:

- ASSOCIATIVA: $\forall x, y, z \in G$:
$$x \star (y \star z) = (x \star y) \star z = x \star y \star z$$
- ESISTENZA ELEMENTO NEUTRO:
$\exists\, u \in G$ tale che $\forall x \in G$: $x \star u = u \star x = x$
- ESISTENZA DELL'INVERSO:
$\forall x \in G\ \exists\, \underset{G}{\underset{\Uparrow}{x'}}$ tale che: $x \star x' = x' \star x = u$.

$$\left(\text{OPERAZIONE: } \quad \begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & x \star y \end{array}\right)$$

esempi: $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ $(\mathbb{C}, +)$ ✓

$(\mathbb{N}_0, +)$ non è un gruppo

$(\mathbb{Q}^*, \cdot)$ ✓

$(\mathbb{Z}^*, \cdot)$ non è un gruppo

$$GL_n(\mathbb{R}) = \{ A \in \mathbb{R}^{n,n} \mid \det(A) \neq 0 \}$$

$(GL_n(\mathbb{R}), \cdot)$ ✓

prodotto riga × colonna

Prop: In un gruppo $(G, \star)$ l'elemento neutro é unico.

dim: se u_1 e u_2 sono 2 elementi neutri allora:

$$u_1 = u_1 \star u_2 = u_2 \implies u_1 = u_2 \quad \#$$

perché u_2 é elt. neutro

perché u_1 é elt. neutro

Prop: In un gruppo $(G, \star)$ l'inverso di ogni elemento é unico.

dim: $x \in G$, siano y_1 e y_2 2 suoi inversi, allora:

$$y_1 = y_1 \star u = y_1 \star (x \star y_2)$$

perché u é elt. neutro

perché y_2 é un inverso di x

$$= (y_1 \star x) \star y_2 = u \star y_2 = y_2$$

associatività

perché y_1 é un inverso

perché u é elt. neutro

$$\implies y_1 = y_2 \quad \#$$

Def: Un gruppo $(G, \star)$ é detto ABELIANO se l'operazione $\star$ é commutativa:

$$\forall x, y \in G : x \star y = y \star x$$

• Generalmente in un gruppo si usa la NOTAZIONE MOLTIPLICATIVA:

operazione "=" $\cdot$

elem. neutro "=" 1_G

inverso "=" x^{-1}

• Se il gruppo é abeliano, si usa spesso la NOTAZIONE ADDITIVA:

operazione "=" $+$

elem. neutro "=" 0_G

inverso "=" $-x$

<u>esempio</u>: $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$

$a \equiv_n b \quad (a = b \pmod n)$

significa che $a-b$ é divisibile per n: $a-b = q \cdot n$

$$\bar{a} = \{ b \in \mathbb{Z} \mid b \equiv_n a \} = \{ b \in \mathbb{Z} \mid b = a + nq \}$$

$\mathbb{Z}_n$ = insieme quoziente

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

Su $\mathbb{Z}_n$ definiamo l'operazione $+$:

$\bar{x}, \bar{y} \in \mathbb{Z}_n$: $\quad \bar{x} + \bar{y} := \overline{x+y}$

⚠ dobbiamo verificare che la definizione sia <u>ben posta</u>, cioé che non dipenda dal rappresentante della classe di equivalenza che abbiamo scelto.

Sia $\boxed{x' \in \overline{x}}$, $\boxed{y' \in \overline{y}} \overset{?}{\Longrightarrow} \overline{x'} + \overline{y'} = \overline{x+y}$

$x' = x + nq$ $\qquad$ $y' = y + np$

$$x' + y' = (x + nq) + (y + np) = x + y + n(q+p)$$

cioé $\quad x' + y' \in \overline{x+y}$ $\quad$ cioé $\quad \overline{x'+y'} = \overline{x+y}$ ✓

- $+$ é associativa
  (perché $+$ é associativa su $\mathbb{Z}$)
- elem. neutro: $\overline{0}$
- inverso: $-\overline{x} = \overline{-x}$

Siccome $+$ é anche commutativa, $(\mathbb{Z}_n, +)$ é un gruppo abeliano.

es. modulo 12:

$$\overline{11} + \overline{3} = \overline{14} = \overline{2}$$

$$\overline{23} + \overline{3} = \overline{26} = \overline{2}$$

$$\overline{11} - \overline{3} = \overline{11} + \overline{-3} = \overline{8} = \overline{11} + \overline{9} = \overline{20}$$

$$\overline{-3} = \overline{9}$$

<u>esempi:</u> • $\mathbb{K}[x] = \{$polinomi in una variabile a coefficienti in $\mathbb{K}\}$

$\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \dots$

$(\mathbb{R}[x], +)$ é un gruppo abeliano.

somma di 2 polinomi

• X insieme

$B(X)$ = insieme delle biezioni di X in se stesso

$= \{ f : X \to X \mid f$ é biettiva$\}$

$(B(X), \circ)$ é un gruppo non abeliano

composizione di funzioni

• $I_n = \{1, 2, \dots, n\}$

Una biezione $s: I_n \to I_n$ é detta PERMUTAZIONE

Il gruppo $(B(I_n), \circ)$ si chiama GRUPPO SIMMETRICO DI ORDINE n e si denota S_n - $\mathfrak{S}_n$

<u>es:</u> $S_3 = ?$

permutazioni di $I_3 = \{1, 2, 3\}$ (con la composizione)

$S_3 = \{ id, p_1, p_2, p_3, q_1, q_2 \}$

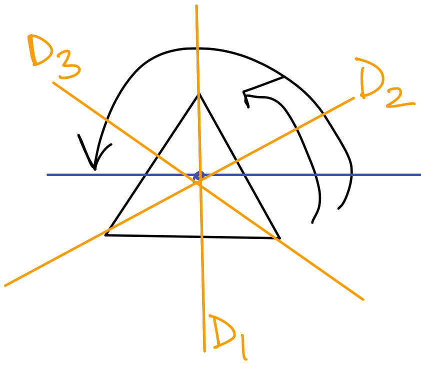
$p_1: \begin{array}{l} 2 \mapsto 3 \\ 3 \mapsto 2 \\ 1 \mapsto 1 \end{array}$ $\quad p_2: \begin{array}{l} 1 \mapsto 3 \\ 3 \mapsto 1 \\ 2 \mapsto 2 \end{array}$ $\quad p_3: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{array}$

$q_1: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{array}$ $\quad q_2: \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{array}$

$|S_n| = n!$

• **GRUPPO DIEDRALE** : Δ_n (D_n)

l'insieme delle isometrie di un poligono regolare con n lati è un gruppo (non abeliano) rispetto alla composizione.



$$\Delta_3 = \{id, R_1, R_2, D_1, D_2, D_3\}$$

R_1 = rotazione $\frac{2}{3}\pi$

R_2 = rotazione $\frac{4}{3}\pi$

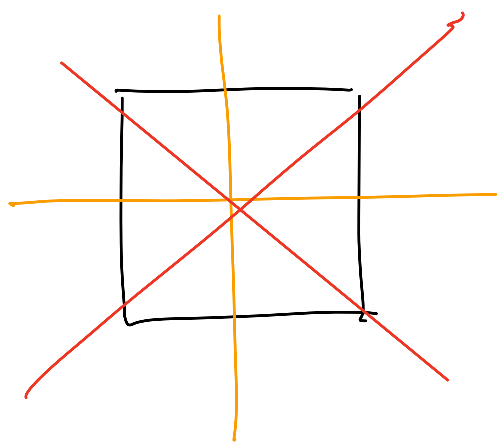
$id = R_3$ = rotazione di $\frac{6}{3}\pi = 2\pi$

D_1, D_2, D_3 = riflessioni rispetto agli assi

$$\Delta_4 = \{id, R_1, R_2, R_3, \text{4 riflessioni}\}$$

↓

rotazioni di multipli di 90°



$$|\Delta_n| = 2n$$