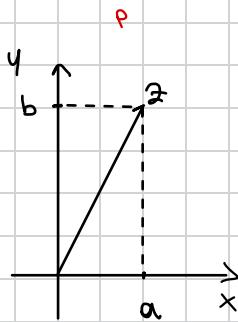


## Interpretazione Geometrica dei numeri complessi



$$z = a + ib$$

$z$  vettore  $(a, b) = \sqrt{}$

- $|z| = \|v\| = \sqrt{a^2 + b^2} \Rightarrow$  Raggio
- $\bar{z}$  è il simmetrico di  $z$  rispetto all'asse  $x$



$$\begin{aligned} \bullet z \cdot \bar{z} &= (a+ib)(a-ib) = a^2 + iba - iba - (-b^2) \\ &= a^2 + b^2 = |z|^2 \end{aligned}$$

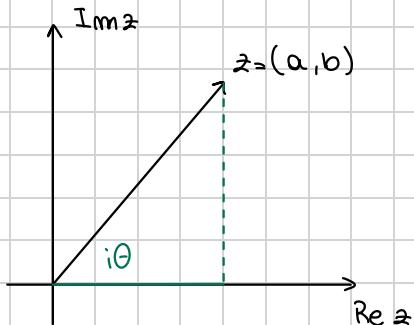
$$\bullet z = a + ib$$

$$\frac{1}{z} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{\overline{z}}{|z|^2}$$

$$\bullet \frac{1}{i} = -i$$

## Forma Trigonometrica dei numeri complessi

Usando Taylor (espansione in serie di potenze) si può vedere che :



$$e^{i\theta} = \cos \theta + i \sin \theta \quad (\theta \in \mathbb{R})$$

$$z = a + ib$$

$$\begin{aligned} z &= r \cos \theta + i r \sin \theta \Rightarrow z = r e^{i\theta} \\ &= r(\cos \theta + i \sin \theta) \end{aligned}$$

**IMPORTANTE**

$$a > 0 \Rightarrow \theta = \arctan \frac{b}{a}$$

$$a = 0 \Rightarrow \theta = \frac{\pi}{2} \Leftrightarrow b > 0$$

$$\Rightarrow \theta = -\frac{\pi}{2} \Leftrightarrow b < 0$$

$$a < 0 \Rightarrow \theta = \pi - \arctan \frac{b}{a}$$

$r, \theta \in \mathbb{R}$  come  $a, b$

Passare da  $z = r e^{i\theta}$  a  $z = a + ib$

$$a = r \cos \theta \quad \text{e} \quad b = r \sin \theta$$

Forme Trigonometriche utili per prodotti e potenze:

$$\begin{aligned} z &= a + ib & z^m &= (a + ib)^m \\ &= z e^{i\theta} & &= r^m e^{im\theta} \end{aligned}$$

$$+ \text{Se } w = s e^{i\varphi} \rightarrow z \cdot w = r \cdot s e^{i(\theta+\varphi)}$$

$$\begin{cases} a = |z| \cos \theta \\ b = i \sin \theta \end{cases}$$

## Radici dei numeri complessi

$\sqrt[m]{z} = z^{\frac{1}{m}}$  tutti i numeri complessi che elevati alla m fanno z.

## TEOREMA FONDAMENTALE DELL'ALGEBRA

Un polinomio di grado m su  $\mathbb{C}$  ha esattamente m radici contate con molteplicità

In formulæ: Dato  $p_m(w) = a_0 + a_1 w + a_2 w^2 + \dots + a_m w^m$

$\exists w_1, \dots, w_m$ , m numeri complessi distinti, t.c.

$$p_m(w) = (w-w_1)(w-w_2) \dots (w-w_m)$$

$$\text{es. } p(w) = (w-3)^3(w-1)$$

3 radice molteplicità 3

1 radice molteplicità 1

Torniamo alle radici

Problema: Fissare  $z$ , trovare  $w$  t.c.  $w^m = z e^{i\theta}$

Fissare  $m$

$$z = \lambda = 1 \cdot e^0 = 1 \cdot e^{i2\pi k}$$

$$m = 1$$

$$w = 1 \Rightarrow$$



$$w^m = z \rightarrow w = z^{\frac{1}{m}} e^{\frac{i\theta}{m}}$$

Sono distinte finché  $\frac{2\pi k}{m}$  diventa multiplo

$$m=2 \quad (z e^{i\theta})^2 = w^2 = 1 \Rightarrow$$

$$z = 1 \quad \text{perché } |z| = 1$$

$$z^2 e^{2i\theta} = 1 \cdot e^{i(0+2k\pi)} \quad K=0 \rightarrow w = e^{i0} = 1$$

$$\Rightarrow w = \sqrt[2]{1} e^{\frac{i2k\pi}{2}}$$

$$K=1 \rightarrow w = e^{i\pi} = -1$$

$$m=3 \quad e^{i\theta} = w^3 = 1 = e^{i2k\pi + i0} \rightarrow 3i\theta = 2k\pi i$$

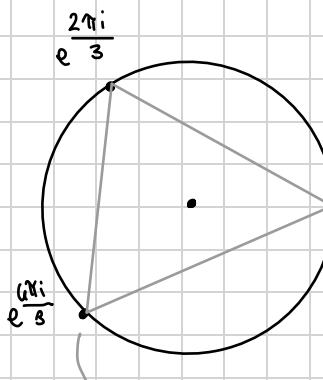
$$\rightarrow \theta = \frac{2k\pi}{3}$$

$$K=0 \rightarrow w = e^{i0} = 1$$

$$K=1 \rightarrow w = e^{i\frac{2\pi}{3}}$$

$$K=2 \rightarrow w = e^{i\frac{4\pi}{3}}$$

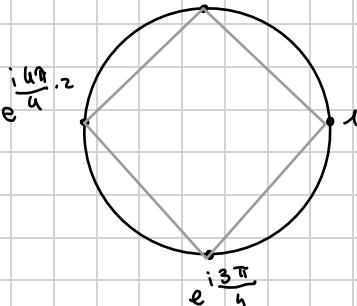
$$K=3 \quad w = e^{i\frac{2\pi \cdot 3}{3}} = e^{i2\pi} = 1$$



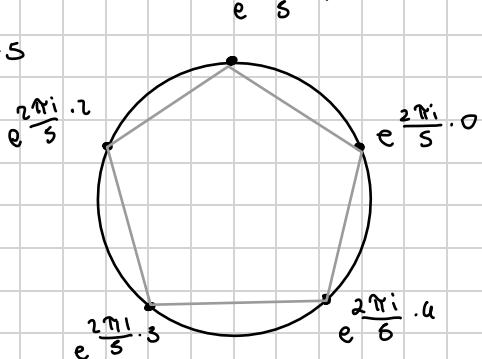
$$w = 1 = e^{i0}$$

Nicogli

$$m=4$$



$$m=5$$



→ le radici emmesime di 1 sono

$$S_m = \{ w \in \mathbb{C} \mid w^m = 1 \}$$

$$= \left\{ w = e^{i \frac{2\pi}{m} \cdot k} \mid k = 0, \dots, m-1 \right\}$$

E sono esattamente i vertici di un poligono regolare con  $m$  lati che ha un vertice in 1.

**Proprietà:** Se  $z_1, z_2 \in S_m \Rightarrow z_1 \cdot z_2 \in S_m$  infatti

$$\begin{aligned} z_1 &= e^{i \frac{2\pi}{m} \cdot k_1} & z_2 &= e^{i \frac{2\pi}{m} \cdot k_2} \\ z_1 \cdot z_2 &= e^{i \frac{2\pi}{m} (k_1 + k_2)} & & \in S_m \end{aligned}$$

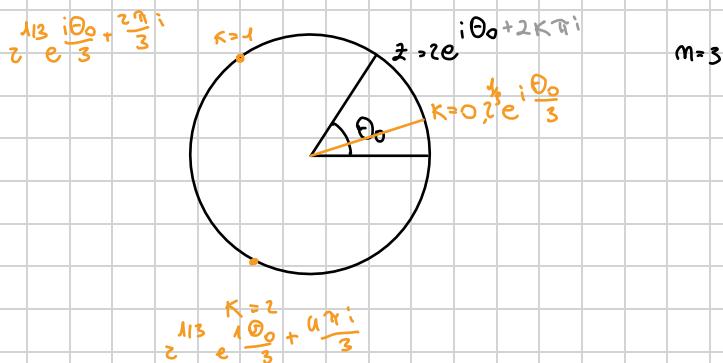
Radici emmesime di un numero  $z \neq 1$

$$\begin{aligned} z &= r e^{i(\theta_0 + i2k\pi)} \\ \text{Cerco } w &= s e^{i\theta} \text{ t.c. } w^m = z \\ &\Leftrightarrow s^m e^{im\theta} = r e^{i(\theta_0 + i2k\pi)} \end{aligned}$$

radice

$$\begin{aligned} s^m &= r \rightarrow s = \sqrt[m]{r} \\ im\theta &= i(\theta_0 + i2k\pi) \\ \rightarrow \theta &= \frac{\theta_0}{m} + \frac{2k\pi}{m} \end{aligned}$$

→ In teoria  $k$  varia su  $\mathbb{Z}$ , ma per  $k \geq m$ , si ripetono i valori  
 $\Rightarrow$  Radici ( $z = r e^{i(\theta_0 + i2k\pi)}$ ) =  $\{ w = r^{\frac{1}{m}} e^{i(\frac{\theta_0}{m} + \frac{i2k\pi}{m})} \mid k = 0, 1, \dots, m-1 \}$



**Errore:** Nelle divisioni con resto non posso moltiplicare per -1

$$\Rightarrow -17 : 6 \quad \xrightarrow{\quad} 17 : 6 = 2 \text{ resto } 5$$

$$-17 = 5 \cdot (-1) + 3$$

$$\downarrow 9 \quad \downarrow 7$$

## Teoria dei Gruppi

- gruppi } muove "strutture"
- campi } algebriche = insiemi su cui possiamo compiere operazioni con certe proprietà
- omomorfismi }
- isomorfismi } applicazioni tra gruppi

**def.** Una operazione su un insieme  $S$  è una funzione  $f: S \times S \rightarrow S$ .

(prende due elementi di  $S$  e restituisce un elemento di  $S$ )

Si indica con  $\ast, +, \cdot, \circ$ .

Proprietà: • Associativa  $(a \ast b) \ast c = a \ast (b \ast c)$  → sempre

• Commutativa  $a \ast b = b \ast a$  bonus es. prodotto tra matrici quadrate  
composizione di funzioni

**def.** Un elemento  $e \in S$  è detto **elemento neutro** per un'operazione  $\ast$  se

$\forall a \in S, a \ast e = e \ast a = a$

es. •  $0$  è l'elemento neutro per  $+$  su  $\mathbb{R}$

• il vettore/matrice nulla è l'elemento neutro per  $+$  su  $\mathbb{R}^m$ /spazi vettoriali

•  $1$  è l'elemento neutro per la moltiplicazione su  $\mathbb{R}$

•  $I$  è l'elemento neutro per la moltiplicazione sulle matrici  $n \times n$ .

**def.** Un elemento  $a \in S$  è detto **invertibile** (rispetto all'operazione  $\ast$ ) se esiste

un altro elemento  $a^{-1}$  detto **inverso** di  $a$ , t.c.  $a \ast a^{-1} = a^{-1} \ast a = e$

es.  $(\mathbb{Z}, +, 0)$   $q \in \mathbb{Z}$

$(M \times M, -, I)$

$$3^{-1} = -3 \quad q^{-1} = -q$$

gli elementi invertibili

sono le matrici invertibili

elemento

neutro

**Notazione** Se  $\ast$  è associativa, denotiamo  $\underline{a \ast a \ast \dots \ast a}$  come  $a^m$   
in verde

**Def.** (**gruppo**) Un gruppo è una **forma**  $(G, \ast, e)$  dove  $G$  è un **insieme**,  $\ast$  è una **operazione associativa** su  $G$  con **elemento neutro**  $e$ , e tale che **ogni elemento di  $G$**  ha un **inverso** in  $G$ .

es.

1.  $(\mathbb{R}, +, 0), (\mathbb{Z}, +, 0), (\mathbb{C}, +, 0), (\mathbb{Q}, +, 0)$  sono gruppi.

$(\mathbb{N}, +, 0)$  non è un gruppo perché non esiste l'inverso (eccetto per 0)

$$3^{-1} = -3 \notin \mathbb{N}$$

2.  $(\mathbb{R}^*, \cdot, 1), (\mathbb{C}^*, \cdot, 1), (\mathbb{Q}^*, \cdot, 1)$  sono gruppi

$(\mathbb{Z}^*, \cdot, 1) \text{ NO, perché non ci sono gli inversi}$

$$a^{-1} = \frac{1}{a} \notin \mathbb{Z}$$

$$\mathbb{S}^* = \mathbb{S} \setminus \{0\}$$

3.  $(\mathbb{R}^m, +, 0), (\mathbb{C}^m, +, 0), (\mathbb{M}_{m \times m}, +, 0)$  sono gruppi

matrice nulla

vettore nulla

sia su  $\mathbb{C}$  che su  $\mathbb{R}$

4. Matrici invertibili  $m \times m$  (sia su  $\mathbb{R}$  che su  $\mathbb{C}$ ):

Sono un gruppo per la moltiplicazione con la matrice identità come elemento neutro d'insieme delle matrici invertibili  $m \times m$  (su  $\mathbb{C}$  o su  $\mathbb{R}$ ) si denota con  $GL(m, \mathbb{R})$  o

Quindi in formule,

$$GL(m, \mathbb{C})$$

$(GL(m, \mathbb{R}), \cdot, I)$  e  $(GL(m, \mathbb{C}), \cdot, I)$  sono gruppi per ogni  $m$ .

Oss. Se  $m$  è l'insieme di tutte le matrici su  $\mathbb{R}$  o su  $\mathbb{C}$ ,  $(m, +, 0)$  non è un gruppo perché per poter sommare due matrici è necessario che abbiano la stessa dimensione.

I gruppi di matrici rispetto alla somma e alla moltiplicazione sono comunque diversi.

All'interno di questi gruppi "fondamentali" possiamo trovare sottogruppi.

**def. (Sottogruppo)** Sia  $(G, *, e)$  un gruppo. Un sottogruppo  $H$  di  $G$  è un insieme  $H \subset G$

tale che:

$$\textcircled{1} \quad e \in H$$

$\textcircled{2} \quad \forall a, b, a * b \in H$  chiuso rispetto a \*

$$\textcircled{3} \quad \forall a \in H, a^{-1} \in H$$

Si indica con  $H \subset G$

Ovvero, un sottogruppo è un gruppo rispetto alle operazioni del gruppo più grande. Praticamente, il sottogruppo eredita l'operazione del gruppo più grande, che a sua volta determina l'elemento neutro.

Quindi l'operazione è associativa di default, devo solo controllare che il sottogruppo contenga l'elemento neutro, sia chiuso rispetto all'operazione, e contenga gli inversi: in formule, la def. di sottogruppo.

## Esempi di sottogruppi

- $(\mathbb{R}, +, 0)$  è un sottogruppo di  $(\mathbb{C}, +, 0)$   $\mathbb{R} \subset \mathbb{C}$
- $(\mathbb{R}^*, \cdot, 1)$  è un sottogruppo di  $(\mathbb{C}^*, \cdot, 1)$   $\mathbb{R}^* \subset \mathbb{C}^*$
- $(m\mathbb{Z}, +, 0)$  è un sottogruppo di  $(\mathbb{Z}, +, 0)$   $m\mathbb{Z} \subset \mathbb{Z}$   
 $\hookrightarrow$  multipli di  $m = \{mk \in \mathbb{Z}, k \in \mathbb{Z}\}$

- le matrici diagonali  $m \times m$  sono un sottogruppo di  $(M_{m \times m}, +, 0)$
- le matrici invertibili diagonali sono un sottogruppo di  $(M_{m \times m}, \cdot, I)$
- $\forall m$ , le radici  $m$ -esime dell'unità  $\delta_m$

$$\delta_m \subset (\mathbb{C}^*, \cdot, 1)$$

Notazione: se  $H$  è un sottogruppo di  $G$ , si scrive  $H \subset G \Rightarrow (\mathbb{Z}, +, 0) \subset (\mathbb{R}, +, 0)$

insieme  
 $\downarrow$  op.  
 $\{$  elem.  
 $\}$  neutro  
 $(G, *, e)$

15.04.24

Come controllo se  $G$  è un gruppo?

- 1) Vedo se l'operazione è ben definita  $g_1 * g_2 \in G \quad \forall g_1, g_2 \in G$
- 2) Esistono inversi  $\forall g \in G \exists g^{-1}, g * g^{-1} = e$

PROPRIETÀ DI  
TUTTI I GRUPPI

es. Se  $G = \text{insieme matrici invertibili } m \times m$

$GL(m)$

$* = \cdot$

$e = \text{matrice nulla}$

la somma di due matrici può non essere  
invertibile  $\Rightarrow$  non è un gruppo

! OK se prendo il prodotto tra matrici

- $(\mathbb{N}, +, 0)$  non è un gruppo perché mancano gli inversi

- $(\mathbb{Z}, \cdot, 1)$  non è un gruppo perché mancano gli inversi

! L'inverso di un numero dipende dall'op. scelta

inverso di 2 rispetto alla somma è -2

moltiplicazione è  $\frac{1}{2}$   $\rightarrow$  notazione  
gruppo  $2^{-1}$

## Tipi particolari di gruppi

- Abeliani e non abeliani
- Finiti e Infiniti

def. (gruppo Abeliano) È un gruppo in cui l'operazione è commutativa.

$$(G, *, e) \quad a * b = b * a \quad \forall a, b \in G$$

def. (gruppo Finito) Un gruppo si dice finito se ha un numero finito di elementi

Q: Quali gruppi finiti conosciamo?

$$\{0, \dots, m-1\} \text{ modulo } m$$

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \cdot, e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

matrici ortogonali con  $\pm 1$

• Radice dell'unità

• permutazioni di  $m$  oggetti

oss. Essere abeliano dipende sia dall'operazione che dall'insieme.

es.  $(GL(m), \cdot, I)$  non abeliano  $\rightarrow$  le matrici quadrate invertibili

$(\text{matrici diagonali invertibili } mxm, \cdot, I)$  sono abeliane

oss. La differenza tra gruppo e sottogruppo è che il sottogruppo eredita l'operazione del gruppo  $\Rightarrow$  non deve contraddirne le proprietà dell'operazione

Notazione: Il numero di elementi di  $G$  si indica:  
1)  $\# G \rightarrow$  cardinalità: si utilizza + spesso  
 $\times$  gli insiemi  
2)  $|G| \rightarrow$  modulo

### esercizio

- 1) Se  $H \subset G$ ,  $G$  gruppo finito  $\Rightarrow |H| \mid |G|$  (il # di elementi di  $H$  divide il numero di  $G$ )
- 2) Riconoscere gli esempi di gruppi e trovare quelli finiti e abeliani

OSS. Un gruppo può non essere abeliano se avere sottogruppi abeliani

(matrici diagonali invertibili sono un sottogruppo abeliano delle matrici diagonali  $(GL(m), \cdot, I)$  che non è abeliano)

Q: un gruppo è un insieme  $G$  o una forma

def. (Gruppo Abeliano)  $(G, *, e)$  se  $*$  è commutativa.

PROPR. DELL'INSIEME CON QUALEVA SR.

$$a * b = b * a \quad \forall a, b \in G$$

def. (Gruppo Finito)  $(G, *, e)$  è finito se ha un numero finito di elementi

Q: Che gruppi finiti conosciamo?

$$\cdot \{0, \dots, m-1\} \text{ modulo } m \quad \cdot \text{Radice dell'unità}$$

$$\cdot G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \dots, e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Matrici di ortogonali con  $\pm 1$

$$g^2 = e$$

OSS. Essere abeliano dipende sia dall'op che dall'insieme

Es.  $(\mathbb{Z}/m\mathbb{Z}), \cdot, I)$  non abeliano

$(\text{matr. diag. invert. } m \times m, \cdot, I)$  sono abeliane

OSS. La differenza tra gruppo e sottogruppo è che il sottogruppo eredita l'operazione del gruppo  
⇒ non devo controllare le proprietà dell'operazione

Notazione: Il num. di elementi di  $G$  si indica: 1)  $\#G$  cardinalità si usa + per gli insiem

2)  $|G|$

Es. Se  $H \subset G$ , a gruppo finito  $= |H| / |G|$

(il # di elem di  $H$  divide il numero di  $G$ )

Es. Riconoscere gli esempi di gruppi delle pag. precedenti e trovare quelli finiti/abeliani

OSS. Un gruppo può non essere abeliano MA avere sottogruppi abeliani

mat inv. e mat diag

Notazione:  $(G, *, e)$  spesso si scrive solo  $G$  (sotto intendo  $*$ ,  $e$ .

→ "posso semplificare gli elementi"

Legge di cancellazione

Se  $(G, *, e)$  è un gruppo, e  $a, b, c \in G \Rightarrow$

$$\begin{aligned} a * b = a * c &\Leftrightarrow b = c && \text{posso semplificare } a \\ b * a = c * a &\Leftrightarrow b = c \end{aligned}$$

potrebbe non esistere

abeliano

$$\stackrel{e}{\cancel{a}} \stackrel{e}{\cancel{b}} \stackrel{e}{\cancel{c}} \rightarrow x+4-4 = z+4-4 \Rightarrow x=z$$

$$\text{es. } (\mathbb{R}, +, 0) \Rightarrow x+4 = z+4 \Leftrightarrow x=z$$

$$(G \text{ finito}, \cdot, I) \Rightarrow AB = CB \Leftrightarrow A = C \quad (\text{invertibili})$$

$$\underbrace{ABB^{-1}}_I = \underbrace{CBB^{-1}}_I \Rightarrow A = C$$

$$\begin{array}{ccc} AC = BC & & \\ A = B & \nearrow & \searrow \\ CA = CB & & \end{array}$$

posso semplificare solo se  $c$  è invertibile

! Se il gruppo è abeliano, l'elem. da semplificare deve essere dello stesso tipo

$AB = CA$  non posso semplificare

dim. (legge di cancellazione)  $(a, *, e)$

Siamo  $a, b, c \in G$   $\exists a^{-1}$

$$\text{Se } a * b = a * c \Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c)$$

associaziva

$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$$

prop. inverso

$$\Rightarrow e * b = e * c$$

prop di e  $\Rightarrow b = c$

Per tornare indietro,

$$\text{se } b = c \Rightarrow a * b = a * c$$

Stessa cosa per  $b * a = c * a$

Dalla legge di cancellazione segue la risolvibilità delle eq. (lineari) ovvero

$\forall a, b \in G$ , l'eq.  $a * x = b$  ha come soluzione unica  $x = a^{-1} * b$

### Theorem Sottogruppi di $\mathbb{Z}$

I sottogruppi di  $\mathbb{Z}$  sono tutti e soli i gruppi della forma  $(b\mathbb{Z}, +, 0)$  con  $b \in \mathbb{Z}$

$(\mathbb{Z}, +, 0)$

$$b\mathbb{Z} = \{ a \in \mathbb{Z}, a = kb, \text{ con } k \in \mathbb{Z} \}$$
$$= \{ \text{multipli di } b \}$$

$$7\mathbb{Z} = \{ \dots -21, -14, -7, 0, 7, 14, 21 \dots \}$$

(oss.  $\Rightarrow \mathbb{Z}$  non ha sottogruppi finiti tranne il sottogruppo banale  $\{0\}$ )

dim. I sottogruppi banali sono  $\{0\} = 0\mathbb{Z}$ , e  $\mathbb{Z} = 1\mathbb{Z} \checkmark$

Suppongo  $H < \mathbb{Z}$  non banale.  $\Rightarrow$  ha elementi  $\neq 0 \Rightarrow$  ha elementi positivi (perche' i soli contengono gli inversi).

Sia  $b$  il più piccolo intero positivo in  $H$ . (principio del buon ordinamento)

Dimostreremo che  $H = b\mathbb{Z}$

$b\mathbb{Z} \subset H$  Sia  $kb \in b\mathbb{Z}$ . Se  $k > 0 \Rightarrow kb = \underbrace{b+b+\dots+b}_{k \text{ volte}}$

elemento generico

$\Rightarrow kb \in H$  perche'  $H$  chiuso rispetto a  $+$

$$\text{Se } k < 0 \Rightarrow (-k)b = \underbrace{-(b+\dots+b)}_{k \text{ volte}} \in H$$

$\Rightarrow -kb \in H$  perche'  $H$  contiene gli inversi

(Se  $b \in H$ , contiene anche tutti i suoi multipli  $\Rightarrow b\mathbb{Z}$ )

$H \subset b\mathbb{Z}$  Sia  $m \in H$  usando la divisione con resto,  $m = qb + r$  voglio far vedere  $r=0$

Poiché  $qb \in H \Rightarrow r = m - qb \in H$  ma per tesa divisione resto,  $0 \leq r < b$

Poiché  $b$  era il più piccolo intero positivo in  $H \Rightarrow r=0 \Rightarrow m = qb$

Resta da fare vedere che  $b\mathbb{Z} \subset H$ . (avendo che i multipli di un numero sono sottogruppi di  $\mathbb{Z}$ )

•  $\forall g_1, g_2 \in b\mathbb{Z}$  | se  $g_1, g_2 \in b\mathbb{Z} \Rightarrow \exists k_1, k_2 \in \mathbb{Z}$  t.c.

$$g_1 + g_2 \in b\mathbb{Z} \quad g_1 = k_1 b \quad g_2 = k_2 b \\ \Rightarrow g_1 + g_2 = k_1 b + k_2 b = (k_1 + k_2) b$$

$\Rightarrow g_1 + g_2$  è multiplo di  $b \Rightarrow g_1 + g_2 \in b\mathbb{Z}$

,  
 $g$

•  $\forall g \in b\mathbb{Z}, g^{-1} \in b\mathbb{Z}$

$$\text{Se } g = kb \Rightarrow -g = -(kb) = (-k)b \in b\mathbb{Z}$$

### Esempio Gruppo delle Permutazioni

(es. di gruppo finito, tavola di moltiplicazione)

def.

$S_m$  = gruppo delle permutazioni di  $m$  elementi

Prendo un insieme  $T$  con  $m$  elementi li posso rappresentare come  $1, 2, \dots, m$ .

$S_m = \{$  tutte le applicazioni da  $T \rightarrow T$  bijective  $\}$

= Aut( $T$ )

= Automorfismi di  $T$

= tutti i modi in cui posso scambiare gli elem. di  $T$

Esempio  $T = \{1, 2\}$

$$1, 2: 1 \mapsto 1 \quad 2, 1: 1 \mapsto 2$$

composizione  $S_2 = \{(1, 2), (2, 1)\}$

$$2 \mapsto 2 \quad 2 \mapsto 1$$

$(S_2, \circ, e)$

$e = I$ , è la permutazione che mantiene inalterato l'ordine degli elementi ( $1, 2, \dots, n$ )

Esempio  $T = \{1, 2, 3\}$

$S_3 = \{(1, 2, 3), (1, 3, 2), (2, 3, 1), (2, 1, 3), (2, 3, 1), (3, 2, 1), (3, 1, 2)\}$

$$(1, 2, 3): 1 \mapsto 1$$

$$2 \mapsto 3$$

$$3 \mapsto 2$$

$$(2, 3, 1): 1 \mapsto 3$$

$$2 \mapsto 1$$

$$3 \mapsto 2$$

Esercizio Scrivere il gruppo di permutazioni di  $n$  elem. (sotto  $n \cdot 3 \cdot 2 \cdot 1 = n!$ )

Esercizio Dimostrare che  $(S_m, \circ, Id)$  è un gruppo.

- capire chi è  $S_1 \circ S_2$

$$S_2^{-1}$$

$$1 \mapsto b_1, i \mapsto b_i$$

$$\downarrow$$

- Un elemento generico di  $S_m$  si scrive come  $q = (b_1, \dots, b_m)$

$$p = (a_1, \dots, a_m)$$

$$p \circ q = (a_{b_1}, a_{b_2}, \dots, a_{b_m})$$

$$q \circ p = (b_{a_1}, b_{a_2}, \dots, b_{a_m})$$

$$1 \xrightarrow{q} b_1, 1 \xrightarrow{p} a_{b_1}$$

$$2 \xrightarrow{q} b_2, 2 \xrightarrow{p} a_{b_2}$$

$$1 \xrightarrow{p} a_1, 1 \xrightarrow{q} b_{a_1}$$

- Usiamo la composizione × scrivere l'inverso

$$q \text{ cerchiamo } q = p^{-1} \text{ t.c. } q \circ p = (1, 2, \dots, m)$$

$$\text{Se } q = (b_1, \dots, b_m) \Rightarrow q \circ p = (b_{a_1}, b_{a_2}, \dots, b_{a_m}) = (1, 2, \dots, m)$$

$$p = (a_1, \dots, a_m)$$

$$\Rightarrow a_1 \text{ t.c. } b_{a_1} = 1$$

$$a_m \text{ t.c. } b_{a_m} = m$$

$$\exists. \quad q = (2, 4, 1, 3)$$

$$q^{-1} = 1 \cdot (a_1, \dots, a_m)$$

$$b_{a_1} = 1 \Rightarrow b_3 = 1$$

$$b_{a_2} = 2 \Rightarrow$$

$$b_{a_3} = 3$$

$$a_3 = 4$$

$$\circ (3, 1, 4, 2)$$

$$q \circ p = 1 \xrightarrow{p} 1 \xrightarrow{q} 1$$

$$2 \xrightarrow{p} 1 \xrightarrow{q} 2$$

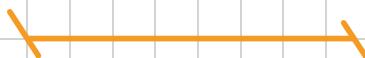
$$\circ S_m \ni Id : Id \rightarrow (1, 2, \dots, m)$$

$$\circ p \circ q \in S_m \quad \forall p, q \in S_m \text{ espl. } *$$

(Alternativa: la composizione di funz. bigettive è bigettiva.)

$$\circ p^{-1} \in S_m \quad \text{Or per la f. espl.}$$

(Alt.: l'inversa di una funz. bigettiva è bigettiva.)



19.04.24

$(S, *, e)$

$* : S \times S \rightarrow S$

esistono gli inversi legge di cancellazione

	Finiti $\xrightarrow{\text{perm}}$ $(S_2, \circ, I)$	Infiniti $(\mathbb{Z}, +, 0), (\mathbb{R}, +, 0), (\mathbb{R}^*, \cdot, 1), (\mathbb{Q}^*, \cdot, 1)$
Abeliani	$(\text{Radici m-esima unità}, \circ, 1)$	$(M_{m \times m}, +, 0), (\mathbb{C}, +, 0), (\mathbb{C}^*, \cdot, 1), (\mathbb{Q}, +, 0)$
Non Abeliani	$\xrightarrow{\text{perm}}$ $(S_m, \circ, I)$	$(GL(m), \cdot, I)$ $\downarrow$ mat. inv. $m \times m$

### Permutazioni $S_m$

Sono i modi possibili di ordinare  $m$  oggetti

$$p \in S_m$$

$$p = (p_1 \dots p_m)$$

$$1 \mapsto p_1$$

$$2 \mapsto p_2$$

$$3 \mapsto p_3$$

$$\dots$$

$$m \mapsto p_m$$

### Tavola di Moltiplicazione

Modo di sintetizzare le proprietà di un gruppo

$S_2$ : (permutazioni di due elementi)

$$S_2 = \{(1,2), (2,1)\}$$

"

id

	$s_1$	$s_2$
$\circ$	$(1,2)$	$(2,1)$
$s_1$	$(1,2)$	$(1,2)$
$s_2$	$(2,1)$	$(1,2)$

Nella posizione  $ij$  metto  $s_j \circ s_i$

Info che ci dà la tavola di moltiplicazione

- Il gruppo è abeliano  $\Leftrightarrow$  è simmetrico rispetto alla diagonale principale
- Vedo subito quale è l'inverso di un elemento: trovo in quale posizione della sua riga/colonna compare  $e$

! In ogni riga e in ogni colonna compare  $e$

• Si vedono bene i sottogruppi (e se sono abeliani)

• Un gruppo si può definire attraverso una tavola di moltiplicazione ( $\equiv$  definire  $*$ )

es.  $S = \{e, b, c, d\}$  insieme di 4 elementi

*	e	b	c	d
e	e	b	c	d
b	b	c	d	e
c	c	d	e	b
d	d	e	b	c

*	e	b	c	d
e	e	b	c	d
b	b	e	d	c
c	c	d	e	b
d	d	c	b	e

### Tavola di moltiplicazione per $S_3$

(avendo come trovare sottogruppi abelliani)

*	(1,2,3)	(2,1,3)	(1,3,2)	(3,2,1)	(2,3,1)	(3,1,2)
(123)	123	213	132	321	231	312
(213)	213	123	312	231	321	132
(132)	132	231	123	312	213	321
(321)	321	312	231	123	132	213
(231)	231	132	321	213	312	123
(312)	312	321	213	132	123	231

Altri sottogruppi: Permutazioni cicliche, preservano ordine circolare

123 123123 ...

$S_3^+ = \{(1,2,3), (231), (312)\}$   
(le permutazioni non cicliche?)

$S_3^- = \{(1,2,3), (321), (213), (132)\} \quad ?$   
 $\rightsquigarrow (213)(321) = (312) \times$  321321 ..

Esempio (gruppo di segni)

.	+	-
+	+	-
-	-	+

Stessa tabella di  $S_2$

(e di qualunque gruppo con due elementi)

CAMP

Un campo è un gruppo (abeliano) con una operazione aggiuntiva  $\cdot$  con certe proprietà

def. un campo è un insieme  $F$  con due operazioni  $+$ ,  $\cdot$  tali che

•  $(F, +, 0)$  gruppo abeliano

•  $(F^*, \cdot, 1)$  gruppo abeliano  $F^* = F \setminus \{0\}$

•  $\forall abc \in F, (a+b)c = ac+bc$  (proprietà distributiva)

Si indica con  $(F, +, \cdot, 0, 1)$  o semplicemente  $(F, +, \cdot)$

OSS In un gruppo le operazioni sono sempre omosociali

• campi con  $\infty$  elementi

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$  (matrici no perché il prodotto non è commutativo)

• compi finiti

$\mathbb{Z}_p = \{ \text{classi di congruenza modulo } p \text{ con } p \text{ primo} \}$

Cosa vuol dire? Perche'  $p$  primo?

## Conguenza modulo m

Sia  $p, q \in \mathbb{Z}$  e sia  $m \in \mathbb{N}$   
non è  
mezzodolmente  
primo

Divisione con resto:  $p = k_1 m + r_1 \quad 0 \leq r_1 < m$

$$* \quad q = k_2 m + r_2 \quad k_1, k_2 \in \mathbb{Z}$$

$p = q \pmod m$  (congruente a  $q$  modulo  $m$ )

Se hanno lo stesso resto, ovvero

$$p = q + km \quad \text{per qualche } k \in \mathbb{Z}$$

( $p = q$  a meno di multipli di  $m$ )

Esempio  $m=7$ : Tutti i multipli di 7 sono uguali mod 7

$$\text{es. } p = -21 \quad p = 35 + (-8) \cdot 7$$

$$q = 35$$

$$m=7 \quad 4 = 11 \pmod 7 \quad \text{perche' } 11 - 4 = 7 = 7 \cdot 1 \text{ e' multiplo di 7}$$

oppure

$$4 : 7 = 0 \quad \bar{r}_4$$

$$11 : 7 = 1 \quad \bar{r}_4$$

$$\text{oppure } 11 = 4 + 1 \cdot 7$$

Due numeri  $p, q \in \mathbb{Z}$  appartengono alla stessa classe di congruenza mod  $m \in \mathbb{N}$  se

- hanno lo stesso resto quando diviso per  $m$

$$p = k_1 m + r_1 \quad \text{com } r_1 = r_2$$

$$q = k_2 m + r_2$$

$$p - q = km \quad \text{com } k \in \mathbb{Z}$$

$$p = q + km \quad \text{com } k \in \mathbb{Z}$$

equivalente

- la loro differenza è multiplo di  $m$

- uno è uguale all'altro a meno di sommare

un multiplo di  $m$

Questo induce una partizione di  $\mathbb{Z}$  in  $m$  classi di equivalenza,

siamo nella  $\rightarrow p \sim q \Leftrightarrow p = q \pmod m \quad (p - q = km, \dots)$

stessa classe ovvero  $p$  è congruente a  $q$  modulo  $m$ .

(Relazioni di equivalenza, classi di  $\sim$  e partitioni hanno def. matematiche precise)

Ci sono  $\infty$  elementi e un numero finito di classi ciascuna delle quali contiene  $\infty$  elementi.

Per ogni classe di  $n$  posso scegliere un rappresentante di solito è la classe di resto, ovvero il rappresentante tra 0 e  $n$

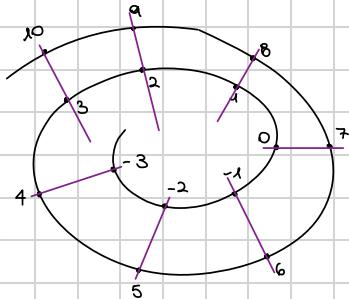
Es.  $m=7$

$$\left\{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \right\}$$

coppia esponente

$\bar{0}$  = tutti i multipli di 7

$\bar{1}$  = tutti i numeri com. resto 1  $\Rightarrow 1, 8, 15, -6, -13 \dots$



Com le classi di congruenza si possono fare somme e moltiplicazioni Modulo  $m$

- le faccio normalmente e tolgo i multipli di  $m$  per ottenerne il coppie esponente che avevo scelto

es.  $m=7$

$$\bar{3} + \bar{5} = \bar{8} = \bar{1}$$

$$\left\{ \bar{0}, \bar{1}, \dots, \bar{6} \right\}$$

$$\bar{8} = \bar{1} \bmod 7 \quad \bar{1} - \bar{8} = -7 = -7(-1) \text{ multiplo di 7}$$

$$\bar{3} \cdot \bar{6} = \bar{18} = \bar{4}$$

$$\bar{4} - \bar{18} = -14 = 7(-2) \text{ multiplo di 7}$$

$$[18 = \cancel{7} + 4]$$

Oss.  $\bar{6} + \bar{5} = \bar{11} = \bar{4} \bmod 7$

$$[\bar{11} = \cancel{7} + 4]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{2} \bmod 9$$

$$[\bar{11} = \cancel{9} + 2]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{3} \bmod 8$$

$$[\bar{11} = \cancel{8} + 3]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{1} \bmod 10$$

$$[\bar{11} = \cancel{10} + 1]$$

$$\bar{6} + \bar{5} = \bar{11} = \bar{11} \bmod m \text{ se } m > 12$$

### Matrici a coefficienti modulo $p$ primo

Posso usare come coefficienti delle matrici le classi di congruenza mod  $p$

Ottengo gruppi finiti non abeliani

il prodotto tra matrici non è abeliano

Es.  $m=3$

$$\left\{ \bar{0}, \bar{1}, \bar{2} \right\}$$

Matrici:

$$\left\{ \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{2} & \bar{0} \end{pmatrix}, \dots, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \dots, \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \dots \right\}$$

Compo  $(K, +, \cdot, e_+, e_\cdot)$   $(K, +, e_+), (K^*, \cdot, e_\cdot)$   
 $(K, +, \cdot, 0, 1)$  Abeliani

Esempi  $C, \mathbb{R}, \mathbb{Z}_p$  primo

$\mathbb{Z}_p = \{\text{classi di congruenza modulo } p\}$  ok per  $p \in \mathbb{N}$   
 $= \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{p-1}\}$

Teo Se  $p$  primo,  $\mathbb{Z}_p$  è un compo (no dim) Se  $p$  non è primo, potrebbero non esistere gli inversi moltiplicativi  
ex.  $p=3 \quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} \Leftrightarrow$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

diagonale

*	0	1	2
0	0		
1		1	2
2		2	1

diagonale

• Cosa succede se  $p$  non è primo?

es.  $p=4 \quad \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

.	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

fuori dal gruppo

$\Rightarrow$  non è un gruppo

due moni ha l'inverso

Gli elementi che creano problemi se  $p$  non è primo  
sono i divisori di  $p$

Eseguire le tavole di moltiplicazione per  $(\mathbb{Z}_6, +)$   $(\mathbb{Z}_6^*, \cdot)$

$(\mathbb{Z}_6, +)$   $(\mathbb{Z}_6^*, \cdot)$

#### CURIOSITÀ

de classi di congruenza si possono usare per generare numeri pseudocasuali

Lc a (linear congruential generator)

seed:  $x_0$  m. intero

$x_{n+1} = (ax_n + c) \bmod m$  parametri

variabili

Tante possibili scelte delle relazioni tra a, c, m.

**Teo. (Hull-Dobell Thm)** • Se  $\text{MCD}(m, c) = 1$  (relativamente primi)

•  $(a-1)$  divisibile per tutti i fattori primi di  $m$

•  $(a-1)$  divisibile per  $4$  se anche  $m$  lo è

$\Rightarrow$  periodo dei numeri generati è  $= a m$

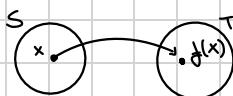
**OMOAFORFISMI e ISOMAFORFISMI** (tra gruppi e tra applicazioni lineari)

Applicazioni e funzioni:

da  $\mathbb{R}^m / \mathbb{C}^m$  in se (spazi vettoriali)

def. Dati due insiemi  $S$  e  $T$  una funzione (o applicazione)  $f: S \rightarrow T$  è qualcosa che associa ad ogni elemento  $x \in S$  uno ed uno solo elemento  $f(x) \in T$ .

$S$  si dice **dominio**.



$T$  si dice **codomino**.

$\begin{matrix} S \\ \downarrow \\ T \end{matrix}$

Notazione  $f(x) = t$

$f: x \mapsto t = f(x)$

- $f, g$  sono uguali se hanno lo stesso dominio  $S$  e codomino  $T$
- $\forall x \in S, f(x) = g(x)$

- Applicazione  $\text{Id}$  su un insieme  $X$  associa ad ogni elemento di  $X$  se stesso:

$\text{Id}_X: X \mapsto X$  (funzione va da  $x$  in  $x$ )

$\text{Id}_X(x) = x \quad \forall x \in X$

$\text{Id}_X: X \mapsto X$

es. .  $f: \mathbb{R} \rightarrow \mathbb{R}$

DOM, CODOM =  $\mathbb{R}$  | IMM. di  $\mathbb{R}$  è  $\mathbb{R}^+$  (radi > 0) | IMM. di  $\mathbb{N}$  sono i num.

$x \mapsto 3e^x$  [  $f(x) = 3e^x$  ]

CONTROIMM. di  $3$  è  $x=0$

3e<sup>0</sup>

$\cdot f: M_{2 \times 2} \rightarrow \mathbb{R}$   $f(\text{mat. diag.}) = \sqrt{\lambda_1 \lambda_2}$   $f(\text{mat. inv.}) = \det \{ \lambda \}$   $f^{-1}(0) = \{ \text{mat. non invert.} \}$

$A \mapsto \det A$  [  $f(A) = \det A$  ]

$\cdot f: \text{insiemi esercizi umani} \rightarrow \mathbb{N}$

persona  $\mapsto$  numero di compiti

$\cdot f: \mathbb{Z} \rightarrow \mathbb{Z}$   $f(z) = 5z = \text{multipli di } 5$   $f(3\mathbb{Z}) = 15\mathbb{Z}$  (imm.)  $f^{-1}(10\mathbb{Z}) = 2\mathbb{Z}$

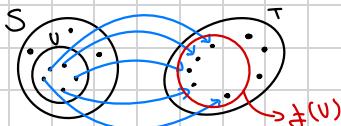
$a \mapsto 5a$   $f(a) = 5a$

### IMMAGINE e CONTROIMMAGINE

Sia  $f: S \rightarrow T$  sia  $U \subseteq S$

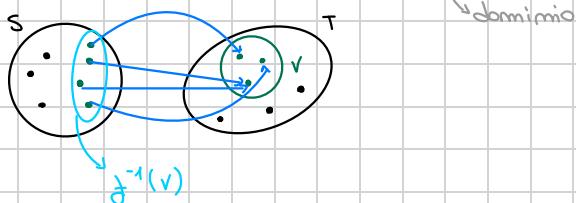
def.:  $d'$  l'immagine di  $U$  secondo  $f$  è l'insieme  $f(U) = \{ t \in T : \exists s \in U, f(s) = t \} \subset T$

(l'immagine sta nel codomino)



def. Se  $V \subseteq T$  la composizionemagine/priamimmagine di  $V$  secondo  $f$  è l'insieme

$$f^{-1}(V) = \{s \in S \mid f(s) \in V\} \subset S$$



! Possiamo guardare l'immagine di tutto il dominio  $S$ .

**INIEZIATIVITÀ e SURIEZIATIVITÀ**

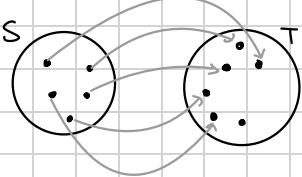
$$f: S \rightarrow T$$

def:  $f: S \rightarrow T$  è iniettiva se  $\forall s, u \in S$

$$s \neq u \Rightarrow f(s) \neq f(u)$$

ovvero: •  $f(u) = f(s) \Leftrightarrow s = u$

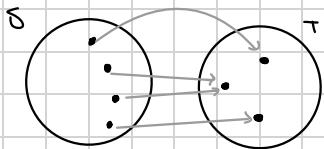
• elementi distinti di  $S$  vengono mandati in elementi distinti di  $T$



def.  $f: S \rightarrow T$  è suriettiva se  $f(S) = T$

ovvero: • ogni elemento di  $T$  ha una priamimmagine in  $S$

•  $\forall t \in T \exists s \in S$  tale che  $f(s) = t$



IMPORTANTE  $f$  è sia iniettiva che suriettiva si dice **BIETTIVA**.

es: riguardo gli esempi, stabilire se iniettive, suriettive o biettive

! Attenzione: Dipende da come definiamo dominio e codominio

$$\text{es } f: \mathbb{R} \rightarrow \mathbb{R}$$

$$a \mapsto |a|$$

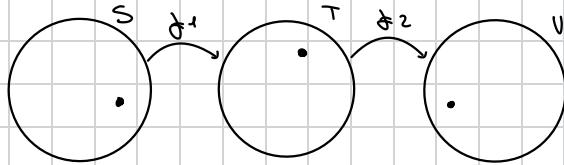
non è iniettiva perché  $|a| = a$

$$f: \mathbb{R}^+ \rightarrow \mathbb{R}^+ \text{ iniettiva e suriettiva} = \text{Id}_{\mathbb{R}^+}$$

Ruolo Speciale:  $f: S \rightarrow S$  da un insieme in se stesso  
(endomorfismi/operatore)

Se biettive: (automorfismi/isomorfismi)

## Composizione



$$f_2 \circ f_1 : S \rightarrow U$$

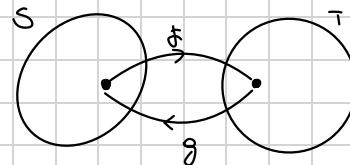
$$s \mapsto f_2(f_1(s))$$

Inversa (se esiste)

$f : S \rightarrow T$  è invertibile se  $\exists g : T \rightarrow S$

tal che  $g \circ f = Id_S$  e  $f \circ g = Id_T$

$g$  si dice inversa di  $f$ ,  $g = f^{-1}$



Proposizione

Sia  $f : S \rightarrow T$  sono equivalenti:

- $f$  è invertibile
- $f$  è biettiva
- $\forall t \in T \ \exists! s \text{ t.c. } f(s) = t$

! Attenzione: dipende dalle scelte di dom. e codom.

es  $f : \mathbb{R} \rightarrow \mathbb{R}^+$   $f(x) = x^2$  non è invertibile

$f : \mathbb{R}^+ \rightarrow \mathbb{R}^+$   $f(x) = x^2$  è invertibile

RECLUPERARE LEZIONE VENERDÌ