

$A \in \text{Mat}_{n \times n}(\mathbb{R})$

(Vedi pag 150  
a sinistra)

$A$  sia invertibile (o come si può dire:  
non singolare)

$GL_n(\mathbb{R}) = \{ A \in \text{Mat}_{n \times n}(\mathbb{R}), \text{invertibili} \}$

è un gruppo rispetto al prodotto  
righe per colonne. (GRUPPO LINEARE GENERALE)

1)  $A, B$  invertibili cioè

$$\begin{array}{ll} \exists A^{-1} : & A \cdot A^{-1} = I = A^{-1} \cdot A \\ \exists B^{-1} : & B \cdot B^{-1} = I = B^{-1} \cdot B \end{array}$$

$\Rightarrow A \cdot B$  invertibile? Sì:

$$\begin{aligned} B^{-1}A^{-1} &: \text{è l'inversa di } AB \\ \text{infatti } (AB)(B^{-1}A^{-1}) &\stackrel{\text{prod. righe}}{=} A(BB^{-1})A^{-1} \\ &= A \cdot I \cdot A^{-1} = AA^{-1} = I \end{aligned}$$

prod.  
righe  
x colonne  
è inv.

Quindi il prodotto  $R \cdot C$  è esterno a  $GL_2(\mathbb{R})$

2) associativa: Si perché vale in  $M_{2 \times 2}(\mathbb{R})$

3)  $I$  (che è invertibile per def.) è eleme. neutro  
rig. al prod.

4)  $\forall A \in GL_n(\mathbb{R}) \quad \exists A^{-1}$

GRUPPO. non commutativo.

$(\mathbb{Z}_6, \circ) \rightarrow$  gruppo degli el. invert.  
rig. al prod.  
 $\{[1]_6, [5]_6\}$

$(\mathbb{R}^2, *)$  con operazione:

Vedi 5° ultimo  
es. pag 156

$$(a, b) * (c, d) = (ac, b+d)$$

1)  $*$  è chiusa? Si

2)  $*$  è associativa?

- $\in \mathbb{R}$
- +  $\in \mathbb{R}$

$$\begin{aligned} ((a, b) * (c, d)) * (e, f) &= (ac, b+d) * (e, f) = \\ &= ((ac)e, (b+d)+f) = (a(ce), b+(d+f)) = \\ &= (a, b) * (ce, d+f) = (a, b) * ((c, d) * (e, f)) \\ &= (a, b) \end{aligned}$$

Si! Allo stesso modo si vede che  $*$  è commutativa

3) Neutro

Verifichiamo se esiste  $(1, 0)$  neutro

$$(a, b) * (1, 0) = (a \cdot 1, b+0) = (a, b)$$

Neutro destro

$\Rightarrow$  Neutro sin.

E' un monoido

4) Inverso. E' vero che  $\forall (a, b)$  esiste  $(c, d)$  tale che

$$(ac, b+d) = (1, 0) ?$$

No  $(0, b)$  non è invertibile: non è un gruppo

Lo sarebbe con la stessa operazione

$(\mathbb{R}^* \times \mathbb{R}, *)$

Un gruppo ciclico:  $A = \{a^n, n \in \mathbb{Z}\}$ , con  $a$  elemento di un gruppo non è necessariamente infinito.

Ad es. se il gruppo è

$$(\mathbb{Z}, +), a = 3$$

$$\begin{aligned} A &= \left\{ \text{multipli di } 3 \text{ liberi} \right\} = \left\{ 3n, n \in \mathbb{Z} \right\} = \\ &= 3\mathbb{Z}: \text{infiniti elementi} \end{aligned}$$

Ma se il gruppo è

$$(\mathbb{R}, \circ) \quad e \quad a = -1$$

$$A = \left\{ a^n, n \in \mathbb{Z} \right\} = \{1, -1\} \text{ è finito}$$

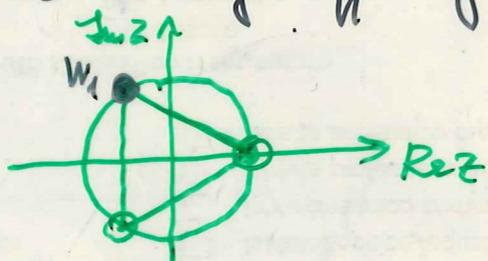
Ancora

le  $n$  radici  $n$ -esime di  $\neq$  in  $(\mathbb{C}, \circ)$

sono un sottogruppo finito, generato dalla 1ª radice diversa di 1

Ad es.

$$n = 3$$



$w_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$  è la 1ª radice diversa da 1  
(corrisponde all'argomento  $\theta = 0 + \frac{2\pi}{3}$ )

$$w_1^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

$$w_1^3 = 1$$

$g: (\mathbb{Z}_4, +) \longrightarrow (\text{radici di } i, \cdot)$

$g([k]_4) \mapsto i^k$

$$[2]_4 = [1]_4 + [1]_4 = 2[1]_4$$

$$[3]_4 = [1]_4 + [1]_4 + [1]_4 = 3[1]_4$$

$$[0]_4 = 0[1]_4$$

Così  $(\mathbb{Z}_4, +)$  è un gruppo ciclico generato da  $\alpha = [1]_4$

$$g([2]_4) = g([1]_4) \cdot g([1]_4) = (g([1]_4))^2$$

$$g([3]_4) = (g([1]_4))^3$$

$$g([0]_4) = (g[1]_4)^0$$

verificare che lo faccia.

$g([k]_4) = i^k$  è omomorfismo

e' un isomorfismo.