$AX = B \qquad A \in GL_n(\mathbb{K}), \quad B \in \mathbb{K}^n \qquad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$$\boxed{rg(A) = n = rg(A|B)}$$

$(A|B) \quad n \times (n+1)$

Rouché - Capelli $\Rightarrow$ compatibile

$\dim \Sigma = n - n = 0 \quad \Rightarrow \Sigma$ ha solo un elemento

$$A^{-1}AX = A^{-1}B$$

$$I_n X = A^{-1}B \quad \Rightarrow \boxed{X = A^{-1}B}$$

$V \qquad u_1, \dots, u_k \in V \quad , \quad \underline{\mathcal{B} = (v_1, \dots, v_n)}$ base di V

$\mathrm{Span}(u_1, \dots, u_k) \subset V$

$$u_i = \sum_{j=1}^{n} a_{ji} v_j \qquad A = (a_{ji}) \in M_{n,k}(\mathbb{K})$$

$$\begin{array}{ccc} \left(\begin{matrix} a_{11} \\ \vdots \\ a_{n1} \end{matrix} \right. & \dots & \left. \begin{matrix} a_{1k} \\ \vdots \\ a_{nk} \end{matrix} \right) \\ u_1 & & u_k \end{array}$$

$V \quad (u_1, \dots, u_k)$ lin. indipendenti, $\quad \mathcal{B} = (v_1, \dots, v_n)$

$k \leq n$ (Lemma dello scambio o di Leonitz)

$\Rightarrow \exists \; u_{k+1}, \dots, u_n$ t.c. $(u_1, \dots, u_n)$ base per V

$$u_i = \sum_{j=1}^{n} a_{ji} v_j$$

$a_{j1} v_j$

$0 \neq u_1 = a_{11} v_1 + \dots + a_{n1} v_n \qquad \exists j$ t.c. $a_{j1} \neq 0$

$$v_j = u_1 - a_{j1}^{-1} (a_{11} v_1 + \dots a_{j-1\,1} v_{j-1} + a_{j+1\,1} v_{j+1} + \dots + a_{n1} v_n)$$

$v_j \in \mathrm{Span}(u_1, v_1, \dots, v_{j-1}, v_{j+1}, \dots, v_n) \Rightarrow (u_1, v_1, \dots, v_{j-1}, v_{j+1}, \dots, v_n)$ base

GRUPPI

Def Un gruppo è un insieme $\neq \emptyset$ G dotato di un'operazione binaria $\cdot : G \times G \longrightarrow G$ t.c.

$$(g, h) \longmapsto \underbrace{g \cdot h}_{\text{notazione}}$$

1) $\cdot$ è associativa $\underline{(g \cdot h) \cdot k} = g \cdot (h \cdot k) \quad \forall g, h, k \in G$

$$\underline{| g \cdot h \cdot k |}$$

2) $\exists$ un elemento neutro per $\cdot$, denotato con $1_G \in G$

$$g \cdot 1_G = 1_G \cdot g = g \quad \forall g \in G$$

3) $\forall g \in G \quad \exists \; \underline{g^{-1}} \in G$ t.c. $g \cdot g^{-1} = g^{-1} \cdot g = 1_G$

Se $\cdot$ è anche commutativa si dice che G è un gruppo abeliano (o commutativo)

Spesso l'operazione di un gruppo abeliano è denotata con $+$ (notazione additiva)

$$(g, h) \longmapsto g + h$$

0_G elemento neutro

$-g$ opposto (inverso)

$$g + (-g) = 0_G$$
$$\parallel$$
$$g - g$$

$$\underbrace{g \cdot \cdots \cdot g}_{n \text{ volte}} = g^n \quad \text{(moltiplicativa)}$$

$$\underbrace{g + \cdots + g}_{n \text{ volte}} = ng \quad \text{(additiva)}$$

$$g^{-n} := (g^{-1})^n \qquad n \geq 1$$

$$g^0 := 1_G$$

Esempi

$(G, \cdot)$

$(G, +)$

$(\mathbb{R}, +)$ gruppo abeliano

$(\mathbb{Q}, +)$ " "

$(\mathbb{C}, +)$ " "

$(\mathbb{R}, \cdot)$ non è gruppo!

0 non ha inverso

$(\mathbb{Q}, \cdot)$

$(\mathbb{C}, \cdot)$

NO

$(\mathbb{R} - \{0\}, \cdot)$ gruppo abeliano

$(\mathbb{R}_+, \cdot)$ " " $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$

$(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{Q}_+, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$

Abeliani

$G = \{-1, 1\} \subset \mathbb{Q}$ abeliano

$G = \{1\}$ gruppo banale (G = \{0\} additivo) multiplicativo

$GL_n(\mathbb{K})$ gruppo non abeliano per $n \geq 2$

$\boxed{GL_n(\mathbb{R})}$

X insieme $\rightsquigarrow$ $\Sigma(X) = \{\varphi : X \to X \mid \varphi$ biunivettiva$\}$

gruppo simmetrico di X

$X_n = \{1, \dots, n\}$

$\boxed{\varphi \circ \psi}$ / $1 = id_X$ $\quad \varphi^{-1}$

$\cdot\ \Sigma(X_n) =: \Sigma_n$ finito (non abeliano se $n \geq 3$)

<u>Prop.</u> 1) l'identità (el. neutro) di un gruppo è unica;

2) l'inverso di $g \in G$ è unico $\forall g \in G$

<u>Dim</u>

1) $1, 1' \in G$ identità

$$1 = 1 \cdot 1' = 1'$$

2) $g \in G \rightsquigarrow h, k \in G$ t.c. $hg = gh = 1_G$ e $kg = gk = 1_G$

$$(hg)k = 1_G \cdot k$$

$$\shortparallel$$

$$h(gk) = k \Rightarrow h \cdot 1_G = k \Rightarrow h = k.$$

In un gruppo G

$$\left.\begin{array}{ll} 1) & ab = ac \Rightarrow b = c \\ 2) & ba = ca \Rightarrow b = c \end{array}\right\}$$ legge di cancellazione

<u>OSS</u> $\underbrace{ab = ca}$ $\not\Rightarrow b = c$ (salvo che G sia abeliano)

Dim

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

2) analogo.

G gruppo finito $\quad G = \{g_1, g_2, \ldots, g_n\}$

	g_1	g_2	$\cdots$	g_n
g_1	g_1^2	$g_1 g_2$		$g_1 g_n$
g_2	$g_2 g_1$	g_2^2		$g_2 g_n$
$\vdots$				
g_n	$g_n g_1$	$g_n g_2$	$\cdots$	g_n^2

$(i, j) \rightsquigarrow g_i g_j$

tabella di moltiplicazione di G

$\{-1, 1\}$

	1	-1
1	1	-1
-1	-1	1

$\{ g_1, \dots, g_k \} \subset G$

sono detti generatori di G se $\forall g \in G$ si può scrivere

come $g = g_{i_1}^{\pm 1} \cdots g_{i_t}^{\pm 1}$ $\quad g_{i_t} \in \{ g_1, \dots, g_k \}$

G, G' gruppi $\quad \varphi : G \longrightarrow G'$

(o morfismo)

Def φ è detta omomorfismo di gruppi se

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

$\cdot$ in G $\quad \forall g_1, g_2 \in G \quad$ $\cdot$ in G'

$$\varphi \begin{cases} \text{iniettive} & \rightsquigarrow \text{monomorfismo} \\ \text{suriettive} & \rightsquigarrow \text{epimorfismo} \\ \text{biiettive} & \rightsquigarrow \text{isomorfismo} \end{cases}$$

$\varphi : G \longrightarrow G'$ omomorfismo

$\Rightarrow \varphi(1_G) = 1_{G'}$

<u>Dim</u> $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \cdot \varphi(1_G)$

$\Rightarrow 1_{G'} = \varphi(1_G)$ (legge di cancell.)

$\varphi(g^{-1}) = (\varphi(g))^{-1}$ <u>Dim</u> $1_{G'} = \varphi(1_G) = \varphi(g g^{-1}) =$

$= \varphi(g) \cdot \varphi(g^{-1}) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$

$\Rightarrow \varphi(g^n) = \varphi(g)^n \quad \forall n \in \mathbb{Z}$ se φ omomorfismo

---

Prop. $\varphi : G \longrightarrow G'$ isomorfismo $\Longrightarrow \varphi^{-1} : G' \longrightarrow G$ isomorfismo

Dim. $\varphi^{-1}(uv) = ?$ $\quad u, v \in G' \Rightarrow \exists\, a, b \in G$ t.c.

$u = \varphi(a)$, $v = \varphi(b)$ (φ biiett.)

($a = \varphi^{-1}(u)$, $b = \varphi^{-1}(v)$)

$$\varphi^{-1}(uv) = \varphi^{-1}\big(\varphi(a)\cdot\varphi(b)\big) = \varphi^{-1}\big(\varphi(ab)\big) = (\varphi^{-1}\circ\varphi)(ab)$$

$$= ab = \varphi^{-1}(u)\,\varphi^{-1}(v) \Rightarrow \varphi^{-1} \text{ omomorfismo}$$

Def G è detto gruppo ciclico se è generato da un solo elemento

G ciclico $\iff \exists\, u \in G$ t.c.

$$G = \{ u^n \mid n \in \mathbb{Z} \}$$

Es $T_n \subset \mathbb{C}$ $\quad T_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$

$z, w \in T_n \quad (zw)^n = z^n w^n = 1 \implies zw \in T_n$

$z \in T_n \implies (z^{-1})^n = (z^n)^{-1} = 1 \implies z^{-1} \in T_n$

$1 \in T_n$ $\qquad$ T_n gruppo

Sia $\zeta \in T_n$ una radice primitiva di 1

$\Rightarrow \forall z \in T_n \quad \exists k \in \mathbb{Z}$ t.c. $z = \zeta^k$

$$e^{iy} = \cos y + i \sin y \qquad y \in \mathbb{R}$$

$$z \in T_n \Rightarrow z = e^{i\frac{2k\pi}{n}} \qquad k \in \mathbb{Z}$$

$$\zeta = e^{\frac{2i\pi}{n}}$$

$\# T_n = n$

T_n gruppo abeliano ciclico con n elementi.

Prop. G gruppo ciclico $\Rightarrow$ G abeliano

Dim. $u \in G$ generatore

$$u^n \cdot u^m = u^{n+m} = u^m \cdot u^n$$

$(\mathbb{Z}, +)$ è un gruppo ciclico infinito (0 el. neutro)

1 è generatore

$n \cdot 1 = n$

Def G gruppo, si pone $\# G = o(G)$ e si chiama

<u>ordine di G</u>

$$o(G) \in \mathbb{N} \cup \{\infty\}$$

$$o(T_n) = n$$

$$o(\mathbb{Z}) = \infty$$

$$o(\mathbb{C} - \{0\}) = \infty$$

$$o(\{1, -1\}) = 2$$

$$o(\{1\}) = 1$$

Def G gruppo, $H \subset G$ sottoinsieme. H è detto sottogruppo di G se è chiuso rispetto a

1) moltiplicazione: $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$
2) $1_G \in H$ $\quad (\Rightarrow H \neq \emptyset)$
3) $h \in H \Rightarrow h^{-1} \in H$

un sottogruppo è a sua volta un gruppo con l'operazione indotta da G.

<u>Prop.</u> $H \subset G$ è sottogruppo $\iff$

1) $H \neq \emptyset$

2) $\forall\, h, k \in H \Rightarrow \underline{h k^{-1}} \in H$.

($h - k \in H$ in not. additiva)

<u>Dim.</u> i) $H \neq \emptyset \Rightarrow \exists\, h \in H \underset{(2)}{\Rightarrow} h h^{-1} = 1_G \in H$

ii) $h \in H \underset{(2)}{\Rightarrow} 1_G h^{-1} = h^{-1} \in H$

iii) $h, k \in H \Rightarrow h, k^{-1} \in H \underset{(2)}{\Rightarrow} h (k^{-1})^{-1} = h k \in H$