# Istituzioni di A & G — ALGEBRA, lezioni 14

25/10/22

Ricordiamo

- $(G, \cdot)$ gruppo, $H < G$ induce una relazione di equivalenza sugli elementi di $G$:

$$\forall\, a, b \in G,\ a \sim_H b \quad \Leftrightarrow \quad ba^{-1} \in H \quad \Leftrightarrow \quad \exists\, h \in H \text{ tale che } b = ha.$$

- Le classi di equivalenza sono dette *classi laterali destre di* $H$:

$$Ha = [a]_{\sim_H} = \{ha \mid h \in H\}.$$

- In modo analogo si definisce la relazione di equivalenza

$$\forall\, a, b \in G,\ a \,{}_H\!\sim b \quad \Leftrightarrow \quad a^{-1}b \in H \quad \Leftrightarrow \quad \exists\, h \in H \text{ tale che } b = ah.$$

- Le classi di equivalenza sono dette *classi laterali sinistre di* $H$:

$$aH = [a]_{H\sim} = \{ah \mid h \in H\}.$$

- $\#$ classi laterali sinistre $= \#$ classi laterali destre $= [G : H]$ *indice di* $H$ *in* $G$.

- **Teorema di Lagrange.** $(G, \cdot)$ un gruppo finito, $H < G$. Allora

$$|G| = [G : H]|H|.$$

  In particolare, l'ordine di $H$ divide l'ordine di $G$.

- Il periodo di ogni elemento di un gruppo finito $G$ divide $|G|$.
- Se $G$ è un gruppo finito, allora $x^{|G|} = 1_G$ per ogni $x \in G$.
- Se $G$ è un gruppo di ordine $p$ primo, allora $G$ è ciclico. In particolare, $G \simeq \mathbb{Z}_p$.
- $(G, \cdot)$ gruppo, $N < G$ è detto *sottogruppo normale* se per ogni $a \in G$:

$$aN = Na.$$

  Scriviamo $N \lhd G$, e indichiamo $G/_N\!\sim = G/\!\sim_N$ con $G/N$.

- Un gruppo è detto *semplice* se non ha sottogruppi normali propri.
- **Criterio di normalità.** *$(G, \cdot)$ gruppo, $N < G$. $N$ è normale se e solo se:*

$$\forall\, a \in G,\ \forall\, h \in N :\ aha^{-1} \in N$$

**Teorema 1.** *Siano $(G, \cdot)$ un gruppo e $N \lhd G$: è possibile definire una operazione su $G/N$ rispetto alla quale $G/N$ è un gruppo e la proiezione $\pi : G \to G/N$ è un omomorfismo avente come nucleo $N$. $G/N$ è detto* gruppo quoziente modulo $N$.

Quindi un sottogruppo normale è il nucleo di un omomorfismo. Viceversa:

**Proposizione 2.** *Se $\varphi : G \to G'$ est un omomorfismo di gruppi,* $\mathrm{Ker}(\varphi) \lhd G$.

In altre parole, un sottoinsieme di un gruppo è un sottogruppo normale se e solo se è il nucleo di qualche omomorfismo del gruppo.

dim prop 2: usiamo criterio di normalità:

sia $a \in \ker(\varphi)$, $g \in G$, $gag^{-1} \in \ker(\varphi)$?

$$\varphi(g \cdot a \cdot g^{-1}) \overset{\uparrow}{=} \varphi(g) \cdot \varphi(a) \cdot \varphi(g)^{-1} \overset{\uparrow}{=} \varphi(g) \cdot 1_{G'} \cdot \varphi(g)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} = 1_{G'}$$

$\varphi$ omomorfismo; $a \in \ker\varphi$

$\Rightarrow g \cdot a \cdot g^{-1} \in \ker(\varphi)$

---

Esempio: $\mathrm{sgn}: S_n \longrightarrow \{\pm 1\}$ è omomorfismo

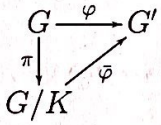
$\sigma \longrightarrow \mathrm{sgn}(\sigma)$

$\ker(\mathrm{sgn}) = A_n$ è sottogruppo normale

**I teorema di isomorfismo, o teorema fondamentale degli omo di gruppi**
*Sia $\varphi : G \to G'$ un omomorfismo, $K = \mathrm{Ker}(\varphi)$, e $\pi : G \to G/K$ la proiezione canonica sul gruppo quoziente. Allora esiste un omomorfismo iniettivo*

$$\bar{\varphi} : G/K \to G'$$

*tale che $\bar{\varphi} \circ \pi = \varphi$, ovvero tale da rendere commutativo il seguente diagramma:*




*In particolare, esiste un isomorfismo $G/K \simeq \mathrm{Im}(\varphi)$*

**Corollario 3.** *Se $\varphi : G \to G'$ un omomorfismo suriettivo, allora $G/\mathrm{Ker}(\varphi) \simeq G'$*

dim (I teorema di isomorfismo)

Definiamo: $\bar{\varphi} : G/K \longrightarrow G'$

$$a/K \longrightarrow \varphi(a)$$

- $\bar{\varphi}$ ben definita: se $a/K = b/K \Rightarrow b \in a \cdot K \Rightarrow$

$\exists\, k \in K$ tale che $b = a \cdot k$. Allora

$$\varphi(b) = \varphi(a \cdot k) = \varphi(a) \cdot \varphi(k) = \varphi(a)$$

($k \in \mathrm{Ker}(\varphi)$)

· $\bar{\varphi}$ è omomorfismo:

$\bar{\varphi}(a/K \cdot b/K) = \bar{\varphi}(ab/K) = \varphi(ab) = \varphi(a)\cdot\varphi(b) = \bar{\varphi}(a/K)\cdot\bar{\varphi}(b/K)$ ($\varphi$ omomorfismo)

· $\bar{\varphi}$ è iniettiva: se $\bar{\varphi}(a/K) = 1_{G'} \Rightarrow$

$\bar{\varphi}(a/K) = \varphi(a) = 1_{G'} \Rightarrow a \in \ker\varphi \Rightarrow$ 6

$\Rightarrow a/K = \ker\varphi = 1_{G/K}$

· Abbiamo diagramma:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi\downarrow & \nearrow_{\bar{\varphi}} & \\ G/K & & \end{array}$$

sia $a \in G$ $\quad \bar{\varphi}\circ\pi(a) = \bar{\varphi}(\pi(a)) = \bar{\varphi}(a/K) = \varphi(a)$

□

7

**Esercizio.** Dimostrare che $\mathrm{SL}_n(\mathbb{R})$ è sottogruppo normale di $\mathrm{GL}_n(\mathbb{R})$.

TC: $SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det(A) = 1 \} < GL_n(\mathbb{R})$

criterio di normalità:

sia $A \in SL_n(\mathbb{R})$, $B \in GL_n(\mathbb{R})$, $B \cdot A \cdot B^{-1} \in SL_n(\mathbb{R})$ ?

$$\det(B \cdot A \cdot B^{-1}) = \det(B) \cdot \det(A) \cdot \det(B^{-1}) =$$

$$= \det(B) \cdot \det(B)^{-1} = 1$$

□

**Esercizio.** Siano $G$ e $H$ gruppi finiti aventi ordini primi fra loro. Dimostrare che $\mathrm{Hom}(G, H)$ contiene solo un elemento, descrivendolo.

sia $|G| = m$, $|H| = n$

dim: sia $\varphi \in \mathrm{Hom}(G, H)$. Allora $\mathrm{Im}(\varphi) < H$

$\Rightarrow$ $|\mathrm{Im}(\varphi)| \mid |H|$

Anche: $G/\ker(\varphi) \simeq \mathrm{Im}(\varphi)$ $\Rightarrow$ $|\mathrm{Im}(\varphi)| = \left|G/\ker(\varphi)\right| =$

$= \dfrac{|G|}{|\ker(\varphi)|}$ $\Rightarrow$ $|\mathrm{Im}(\varphi)| \mid |G|$

Cioè $|\mathrm{Im}(\varphi)| \mid m, n$ $\Rightarrow$ $|\mathrm{Im}(\varphi)| = 1$ $\Rightarrow$

$\mathrm{MCD}(m, n) = 1$

$\mathrm{Im}(\varphi) = \{1_H\}$ $\Rightarrow$ $\varphi : G \to H$ unico omomorfismo

$g \longrightarrow 1_H$

**Esercizio.** Sia $(G, \cdot)$ un gruppo. Dimostrare che l'applicazione

$$\begin{aligned} \varphi : G &\to G \\ g &\mapsto g^2 \end{aligned}$$

è un omomorfismo se e solo se $G$ è abeliano. Nel caso $G$ sia abeliano, stabilire se $\varphi$ è o meno un automorfismo.

dim:

$\varphi$ omo $\iff \forall g, h \in G \quad (gh)^2 = \varphi(gh) = \varphi(g)\,\varphi(h) = g^2 h^2$

$\iff \forall g, h : (gh)(gh) = (gh)^2 = g^2 h^2 \iff \forall g, h \in G : hg = gh$

↑ legge cancellativa

$\iff$ $G$ abeliano

Nel caso $G$ abeliano, $\varphi$ non è sempre automorfismo

i) $\mathbb{Z}_5 \to \mathbb{Z}_5$ automorfismo

$a \longrightarrow 2a$

$0 \longrightarrow 0$

$\bar{1} \longrightarrow \bar{2}$

$\bar{2} \longrightarrow \bar{4}$

$\bar{3} \longrightarrow \bar{6} = \bar{1}$

$\bar{4} \longrightarrow \bar{8} = \bar{3}$

ii) $\mathbb{Z}_6 \to \mathbb{Z}_6$ non è automorfismo

iii) $(\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ non è automorfismo

$x \longrightarrow x^2$

**Esercizio.** Sia $(G, \cdot)$ un gruppo abeliano di ordine $n$, e sia $m$ un intero coprimo con $n$. Dimostrare che l'applicazione

$$\begin{aligned} \varphi : G &\to G \\ g &\mapsto g^m \end{aligned}$$

è un automorfismo.

dim: $\varphi$ omomorfismo perchè $(G, \cdot)$ abeliano

• vediamo $\varphi$ automorfismo studiando il $\ker(\varphi)$.

• $g \in \ker(\varphi) \Rightarrow g^m = 1 \Rightarrow \text{ord}(g) \mid m$

Ma $\text{ord}(g) \mid n$ (Lagrange) $\Rightarrow$

$\text{ord}(g) \mid n, m \Rightarrow \text{ord}(g) = 1 \Rightarrow g = 1_G$

$MCD(n, m) = 1$

Cioè, $\ker(\varphi) = \{1_G\}$