# ALGEBRA 1 - 28 SET 2018

Note Title 9/28/2018

## Automorfismi di un gruppo.

**Def.** Dato un gruppo $G$ definiamo
$$\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ isomorfismo}\}.$$

**Oss.** $\mathrm{Aut}(G)$ è un gruppo.

$id \in \mathrm{Aut}(G)$, $f, g \in \mathrm{Aut}(G) \Rightarrow f \circ g \in \mathrm{Aut}(G)$

(fatti ovvi).

$f \in \mathrm{Aut}(G) \Rightarrow f^{-1} \in \mathrm{Aut}(G)$.

È omomorfismo?

$$f^{-1}(xy) \overset{?}{=} f^{-1}(x) f^{-1}(y)$$

$$\Leftrightarrow \quad f(f^{-1}(xy)) = f(f^{-1}(x) f^{-1}(y)) \qquad \text{ok}$$

$$xy \qquad = f(f^{-1}(x)) f(f^{-1}(y)) = xy$$

**Esempi:** $G = \mathbb{Z}/m\mathbb{Z}$ $\quad \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$

(Sono le funzioni del tipo $f(x) = kx$ dove $(k, m) = 1$)

$G = \mathbb{Z}$ $\quad \mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\} = \mathbb{Z}^*$

$f(x) = kx \qquad k \in \{\pm 1\}$

---

$p$ primo, $k \geq 1$. $\quad G = (\mathbb{Z}/p\mathbb{Z})^k$.

$G$ è uno s.v. con coefficienti in $\mathbb{F}_p$ $(\mathbb{Z}/p\mathbb{Z})$

$kx = x + \dots + x$ ($k$ volte)

Gli omomorfismi del gruppo $G$ sono anche funzioni lineari ($f(kx) = kf(x)$)
Scegliendo una base, si ha una corrispondenza biunivoca fra $Aut(G)$ e $GL_k(\mathbb{Z}/_{p\mathbb{Z}})$

matrici $k \times k$ invertibili

Di più, $Aut(G) \cong GL_k(\mathbb{Z}/_{p\mathbb{Z}})$

$$f \leftrightarrow M \qquad g \leftrightarrow N$$
$$f \circ g \leftrightarrow M \cdot N$$

$$|GL_k(\mathbb{Z}/_{p\mathbb{Z}})| = \underset{1^a \text{ col.}}{(p^k - 1)}\ \underset{2^a \text{ col}}{(p^k - p)}\ \underset{3^a \text{ col}}{(p^k - p^2)} \dots \underset{\text{ultima col}}{(p^k - p^{k-1})}$$

**Def. 2** L'insieme
$$Int(G) = \{ f \in Aut(G) \mid \exists g \in G \text{ con } f(x) = gxg^{-1} \}$$
si dice insieme degli automorfismi interni di $G$.

In effetti, questi sono automorfismi.

omo: $f(xy) = g(xy)g^{-1} = gx\underbrace{g^{-1}g}y g^{-1} = f(x)f(y)$.

iniettivi: $\ker f = \{ x \in G \mid gxg^{-1} = e \}$
$$gxg^{-1} = e \Leftrightarrow gx = g \Leftrightarrow x = e$$

surgettivi: Dato $y \in G$ $\exists x \in G$ t.c. $gxg^{-1} = y$ e cioè $x = g^{-1}yg$

**Oss 2** $Int(G) \trianglelefteq Aut\, G$

Chiamiamo $\varphi_g$ la funzione data che
$$\varphi_g(x) = gxg^{-1}$$

id $\quad id = \varphi_e$.

prodotto $\varphi_g \circ \varphi_h(x) = \varphi_g(h x h^{-1})$

$$= g h x^{-1} h^{-1} g^{-1} = g h x (gh)^{-1}$$

$$= \varphi_{gh}(x)$$

In particolare $\boxed{\varphi_g \circ \varphi_h = \varphi_{gh} \quad *}$

Inverso, $(\varphi_g)^{-1} = \varphi_{g^{-1}}$ (banale).

Normale: $\psi \in Aut(G)$ $\varphi_g \in Int(G)$

$\psi \circ \varphi_g \circ \psi^{-1} \overset{?}{\text{è}} Int(G)$

$(\psi\, Int(G)\, \psi^{-1} \subseteq Int(G))$

Infatti,

$$\psi \circ \varphi_g \circ \psi^{-1}(x) = \psi \circ g(\psi^{-1}(x)) = \psi(g \psi^{-1}(x) g^{-1})$$

$$= \psi(g)\ \underbrace{\psi(\psi^{-1}(x))}_{x} \cdot \underbrace{\psi(g^{-1})}_{(\psi(g))^{-1}}$$

$$= \varphi_{\psi(g)}(x)$$

Prop. Si ha $Int(G) \cong G/Z(G)$ ← centro di $G$

Dim. Considero la funzione $\varphi : G \to Int(G)$ definita da $\varphi(g) = \varphi_g$

$\varphi$ è un omomorfismo (v. sopra $*$)

E' surgettivo per definizione

$\ker \varphi = \{g \in G \mid \varphi_g = \text{identità}\}$

cioè

$$\varphi_g(x) = x \quad \forall x \in G$$
$$\Updownarrow$$
$$g x g^{-1} = x \quad \forall x \in G$$
$$\Updownarrow$$
$$g x = x g \quad \forall x \in G$$
$$\Updownarrow$$
$$g \in Z(G)$$

<u>Oss.</u> ① Se $G$ è abeliano, allora $\mathrm{Int}(G) = \{id\}$

② $G/Z$ o è banale oppure <u>non</u> <u>è</u> <u>ciclico</u>.

$Z(G)$

(Se fosse ciclico, avremmo $G$ = unione delle classi laterali (sinistre) di $G$ e cioè
$$G = \bigcup_{n \in \mathbb{Z}} (xZ)^n = \bigcup_{n\in\mathbb{Z}} x^n Z$$

Se si prendono due elementi $g, h \in G$ si ha
$$g \in x^n Z \qquad h \in x^m Z$$
$$g = x^n z_1 \qquad h = x^m z_2$$
$$\begin{aligned} gh &= x^n z_1 x^m z_2 \\ &= x^n x^m z_1 z_2 \\ &= x^m x^n z_2 z_1 \\ &= x^m z_2 x^n z_1 \\ &= hg \end{aligned}$$
)

$\Downarrow$

cioè $G/Z$ banale.

<u>Altro esempio</u> $\quad G = S_3$.

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

$$S_3 = \langle (12), (13), (23) \rangle$$

L'immagine di ogni automorfismo $f$ di $S_3$ è determinata da $f((12)), f((13)), f((23))$.

Siccome $(12), (13), (23)$ sono tutti e soli gli elementi di ordine 2 in $S_3$,
$$\{f((12)), f((13)), f((23))\} = \{(12), (13), (23)\}$$

Considerando $f \mapsto f|_{\{(12),(13),(23)\}}$

si ottiene una permutazione di questi 3 elementi.

$$\mathrm{Aut}(S_3) \longrightarrow S_3$$
$$f \mapsto f|_{\dots}$$

Questa funzione è un omomorfismo (verifica banale)

INIETTIVO: se $f = id$ su un insieme di generatori, allora $f = id$, $\forall x$.

Quindi $\mathrm{Aut}(S_3)$ è isomorfo a un sottogruppo di $S_3$.

$$(|\mathrm{Aut}\, S_3| \leq 3! = 6)$$

$$\mathrm{Int}(S_3) \cong S_3 / Z(S_3)$$

Ma $Z(S_3) = \{e\}$ (infatti $(ab)(abc) \neq (abc)(ab)$)

Quindi $\mathrm{Int}(S_3) \cong S_3$

$$S_3 \cong \mathrm{Int}(S_3) \leq \mathrm{Aut}(S_3) \leq S_3.$$

SONO TUTTE UGUAGLIANZE.

---

# AZIONI DI UN GRUPPO SU UN INSIEME

$G$ gruppo

$X$ insieme

$S(X)$ = gruppo delle permutazioni di $X$.

**Def.** Un'azione di $G$ su $X$ è un omomorfismo

$$\varphi : G \to S(X)$$

Notazione: scriverò $\varphi_g$ per denotare l'immagine di $\varphi$.

$$\varphi_g : X \to X$$
$$\varphi_g(x) = \dots$$

**Esempio** $G$ gruppo qualsiasi,

$X = G$

$\varphi_g$ = automorfismo interno associato a $g$

$$\varphi_g(x) = g x g^{-1}$$

$$\mathrm{Im}\,\varphi = \mathrm{Int}(G) < S(X)$$

**Es. 2** $G$ gruppo di trasformazioni biunivoche del piano. Si ha un'azione "naturale" di $G$ su $X = \mathbb{R}^2$.

$$f \in G \mapsto f : \mathbb{R}^2 \to \mathbb{R}^2$$

$$\begin{array}{ccc} G & \xrightarrow{\text{inclusione}} & S(X) = S(\mathbb{R}^2) \\ \psi & & \\ \varphi & \longmapsto & \varphi \end{array}$$

Esempio 3 $\qquad G = S_n \qquad X = \{1, \dots, n\}$

$$\varphi : S_n \to S(X) \cong S_n$$
$$\varphi = \text{identità}.$$

$\sim$

| G | X |
|---|---|
| sottogruppi di G | sottoinsiemi di X |

Supponiamo di avere un'azione $\varphi : G \to S(X)$.

Stabilizzatore di un elemento $x \in X$

Def. 1 $\quad \text{Stab}(x) = \{ g \in G \mid \varphi_g(x) = x \}$

$\text{Stab}(x) < G$ $\qquad$ (dimostrazione ovvia)

Nota: In generale $\text{Stab}(x)$ NON È un sottogruppo normale di $G$

Orbita di un elemento

Def 2 $\quad \text{Orb}(x) = \{ y \in X \mid \exists g \in G \ \varphi_g(x) = y \}$

$\text{Orb}(x) \subset X$

Prop. 1 $\quad$ Si ha $\varphi_g(x) = \varphi_h(x)$
$\iff g\,\text{Stab}(x) = h\,\text{Stab}(x)$

(cioè $g, h$ sono nella stessa classe laterale

SINISTRA dello stabilizzatore di $x$).

<u>Dim</u> $\varphi_g(x) = \varphi_h(x) \iff \varphi_h^{-1} \circ \varphi_g(x) = x$

$\iff \varphi_{h^{-1} \cdot g}(x) = x \iff h^{-1} g \in \mathrm{Stab}(x)$

$\iff g \in h\,\mathrm{Stab}(x) \iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$

<u>Prop. 2</u> La relazione nell'insieme $X$ data da

$$x \sim y \iff \exists g \in G \text{ t.c. } \varphi_g(x) = y$$

è una relazione di equivalenza e le sue classi di equivalenza sono le orbite
$(\, cl(x) = \mathrm{Orb}(x))$.

<u>Dim.</u> Rel. di equiv.

$x \sim x \qquad \varphi_e(x) = x$

$x \sim y \Rightarrow y \sim x \qquad \varphi_g(x) = y \Rightarrow \varphi_{g^{-1}}(y) = x$

$x \sim y,\ y \sim z \Rightarrow x \sim z \qquad \varphi_g(x) = y \quad \varphi_h(y) = z$

$$\varphi_h \circ \varphi_g(x) = \varphi_{hg}(x) = z.$$

$cl(x) = \{ y \in X \mid \exists g \in G \ \ \varphi_g(x) = y \}$
$= \mathrm{Orb}(x)$.

$G$ = Rotazioni del piano intorno all'origine.

$\mathrm{Stab}(0) = G$

$P \neq 0 \qquad \mathrm{Stab}(P) = \{ \mathrm{id} \}$

$Orb(O) = \{O\}$

$P \neq O \qquad Orb(P) =$ circonferenza di centro $O$ e raggio $OP$.

$G =$ Traslazioni del piano per un vettore orizzontale

$Stab(P) = \{e\}$

$Orb(P) =$ retta orizzontale per $P$.