Secondo teorema di isomorfismo

Siano G gruppo, $H \triangleleft G$ e $K \leq G$ allora

$$KH/H \cong K/H \cap K$$

Dim

- osserviamo che $HK \leq G$ perchè $H \triangleleft G$ e $H \cap K \triangleleft K$ (si dimostra facilmente)
- definiamo che

$$f: K \longrightarrow KH/H \qquad \text{omomorfismo di gruppo}$$
$$k \longrightarrow kH$$

- dimostriamo che f è suriettivo:

$$xH \in KH/H \Longrightarrow x = kh \text{ con } k \in K \text{ e } h \in H$$

da cui $xH = khH = kH = f(k)$

- dimostriamo che $\ker f = K \cap H$

$$f(k) = kH = H \Longleftrightarrow k \in H$$

Conclusioni

$$\text{I teor. di isom} \Longrightarrow \frac{K}{\ker f} = \frac{K}{K \cap H} \cong \frac{KH}{H}$$

AZIONI DI GRUPPI SU INSIEMI

Def X insieme definiamo

$$\Sigma(X) = \{f : X \to X \mid f \text{ invertibile}\}$$

con il prodotto $fg \overset{def}{=} g \circ f$ è un gruppo (il gruppo delle permutazioni di X)

Osservazioni 1) se consideriamo $\cdot$ il prodotto $f \cdot g \overset{def}{=} g \circ f$ (do un nome al prodotto in $\Sigma(X)$)

ottengo che
$$\tau : (\Sigma(X), \cdot) \longrightarrow (\Sigma(X), \circ)$$
$$\tau(f) = f^{-1}$$

è un isomorfismo di gruppi

Infatti $\tau(f \cdot g) = (f \cdot g)^{-1} = (g \circ f)^{-1} = f^{-1} \circ g^{-1}$

$= \tau(f) \circ \tau(g)$

Inoltre $\sigma : (\Sigma(X), \circ) \longrightarrow (\Sigma(X), \cdot)$

con $\sigma^{-1}(f) = f^{-1}$ è l'inverso di τ

2) Sia $\varphi: X \longrightarrow Y$ una biezione

Definiamo

$$\phi: \Sigma(X) \longrightarrow \Sigma(Y) \quad \text{con} \quad \phi(f) = \varphi \circ f \circ \varphi$$

è un isomorfismo di gruppi [verifica per esercizio]

In particolare

se $X = \{1, \ldots, n\}$ definisco $S_n \stackrel{\text{def}}{=} \Sigma(X)$

il gruppo simmetrico su n elementi

Se Y è un insieme di cardinalità n

allora esiste $\varphi: \{1, \ldots, n\} \longrightarrow Y$ biezione

per cui $\Sigma(Y) \cong S_n$

[Per questo nel caso finito si studiano solo gli S_n]

Def <u>Def</u> Siano G gruppo e X insieme,

una <u>G-azione su X</u> è un omomorfismo

di gruppi $\rho: G \longrightarrow \Sigma(X)$

<u>Esempi</u> 1) $\rho : G \to \Sigma(X)$ con

$\rho(g) = Id_X$ per ogni $g \in G$

Questa si dice <u>azione banale</u> di G su X

2) $\rho : G \longrightarrow \Sigma(G)$

G considerato come insieme

con $\underbrace{\rho(g)}_{\in \Sigma(G)}(h) = hg$

provo che ρ è un omomorfismo:

$$\rho(gg')(h) = hgg' = (hg)g' =$$

$$= (\rho(g)(h))g' = \rho(g')(\rho(g)(h))$$

$$= \rho(g') \circ \rho(g)\ (h) = \rho(g)\rho(g')(h)$$

provo che ρ è iniettiva:

$$\rho(g) = Id_G \Rightarrow \rho(g)(1_G) = g = Id_G(1_G) = 1_G$$

$$\Rightarrow g = 1_G$$

I teor. di isom $\Rightarrow \frac{G}{\ker\rho} \cong G \cong \rho(G) \leq \Sigma(G)$

Questo è il <u>teorema</u> di <u>Cayley</u>

che dice che ogni gruppo è isomorfo

ad un sottogruppo di un gruppo di

permutazioni

<u>Def</u> Se $\rho : G \longrightarrow \Sigma(X)$ è un monomorfismo

allora l'azione si dice <u>fedele</u>

<u>Corollario teor di Cayley</u> Per ogni $n \in \mathbb{N} \setminus \{0\}$

esistono un numero finito di gruppi

di ordine n a meno di isomorfismi

<u>Dim</u> se $|G| = n$ allora G è isomorfo

ad un sottogruppo di S_n $(\cong \Sigma(G))$

S_n ha al più $\binom{n!}{n}$ sottoinsiemi

con n elementi $(n! = |S_n|)$ $\boxed{\Xi}$

[stime grossolane]

3) $Isom(\mathbb{R}^3)$ agisce su $\mathbb{R}^3$

$GL(n, \mathbb{R})$ agisce su $\mathbb{R}^n$

D_{2n} agisce su $\mathbb{R}^2$

Sono tutte azioni fedeli

<u>Notazione</u>: da adesso in poi se $\rho : G \to \Sigma(X)$ è un azione invece di $\rho(g)(x)$ scriveremo $g(x)$

Attenzione con il prodotto definito

$$g'(g(x)) = gg'(x)$$

<u>Definizione</u>: G agisce su X, $p \in X$ definiamo

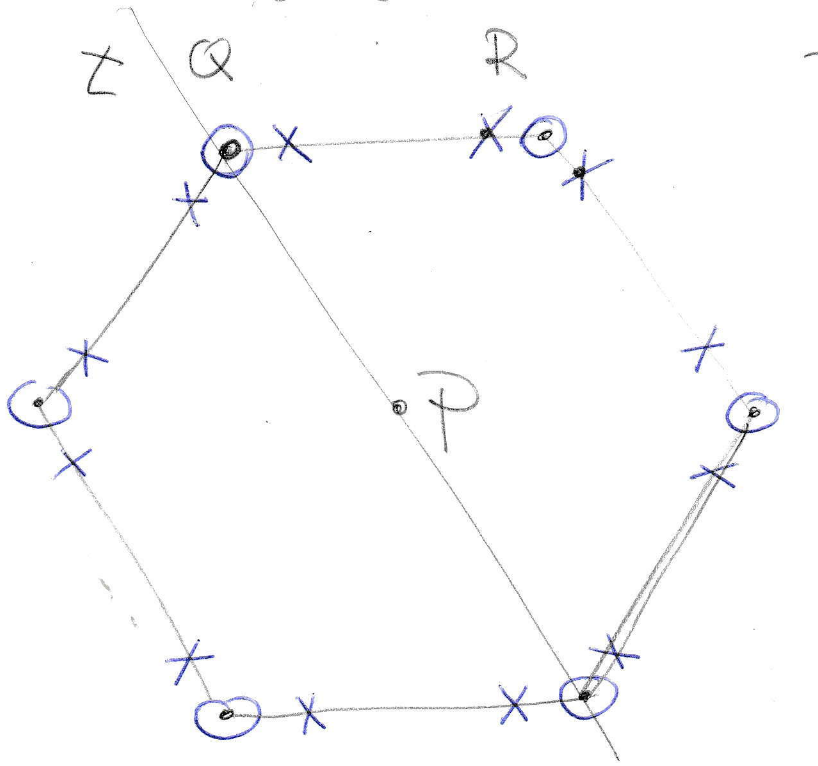
$O_G(p) = \{ g(p) \mid g \in G \} \subseteq X$ l'orbita di p

$stab_G(p) = \{ g \in G \mid g(p) = p \} \leq G$ stabilizzatore di p in G

<u>Esercizio</u> verificare che $stab_G(p)$ è un sottogruppo

Esempio $\mathbb{D}_{12}$ agisce su $\mathbb{R}^2$

t riflessione che fissa Q



$O_{\mathbb{D}_{12}}(P) = \{P\}$ $\mathrm{stab}_{\mathbb{D}_{12}}(P) = \mathbb{D}_{2n}$

$|O_{\mathbb{D}_{12}}(Q)| = 6$ $\mathrm{stab}_{\mathbb{D}_{12}}(Q) = \{Id, t\}$

$|O_{\mathbb{D}_{12}}(R)| = 12$ $\mathrm{stab}_{\mathbb{D}_{12}}(R) = \{Id\}$

[cosa possiamo notare]

Proposizione Consideriamo l'azione $\rho : G \to \Sigma(X)$

Se $O_G(p)$ è insieme finito

$$|O_G(p)| = |G : stab_G(p)|$$

In particolare se G è finito

$$|O_G(p)| = \frac{|G|}{|stab_G(p)|}$$

Dim: definiamo

$$\begin{aligned} \phi : G &\longrightarrow O_G(p) \\ g &\longrightarrow g(p) \end{aligned}$$

è suriettiva per definizione quindi abbiamo che

$$G/\sim_\phi \xleftrightarrow{\text{biezione}} O_G(p)$$

dove $g \sim_\phi h \iff \phi(g) = \phi(h)$

$$g \sim_\phi h \iff g(p) = h(p) \iff h^{-1} \circ g(p) = p$$
$$\iff g h^{-1}(p) = p \iff \underbrace{g h^{-1}}_{} \in stab_G(p)$$

relazione di equivalenza che individua i laterali destri di $stab_G(p)$

$$G/_{\sim\phi} = \{\text{laterali destri di } stab_G(p)\} \xleftrightarrow{\text{biezione}} O_G(p)$$

Se G è finito uso teorema di Lagrange

$\square$

<u>Osservazione</u> Se G è finito, $|O_G(p)|$ è un divisore di G.

<u>Esercizio</u> $O_G(p) = O_G(q) \Rightarrow \exists x$ in G t.c $[stab_G(p)]^x = stab_G(q)$

<u>Definizione</u>: G agisce su X, $Z \subseteq X$ si dice <u>G-invariante</u> se per ogni $z \in Z$ e per ogni $g \in G$ $g(z) \in Z$

<u>Proposizione</u> 1) Le orbite formano una partizione di X

2) $Y \subseteq X$ è un orbita $\Longleftrightarrow$ è un insieme minimo fra quelli G-invarianti

3) ogni insieme G-invariante è unione di orbite

Dimostrazione

1) • $\bigcup_{p \in X} O_G(p) = X$ perchè $p \in O_G(p)$

• dimostriamo che:

$$\boxed{q \in O_G(p) \Rightarrow O_G(p) = O_G(q)} \quad (*)$$

se $q \in O_G(p) \Rightarrow \exists g \in G$ tale che $q = g(p)$

supponiamo $w \in O_G(q)$ allora $\exists \bar{g} \in G$ tale che $\bar{g}(q) = w \Rightarrow \bar{g}(g(p)) = w$

$\Rightarrow g\bar{g}(p) = w \Rightarrow w \in O_G(p)$

(quindi $O_G(p) \supseteq O_G(q)$)

supponiamo $w \in O_G(p)$ allora $\exists \bar{g} \in G$ tale che $\bar{g}(p) = w \Rightarrow \bar{g}(g^{-1}(q)) = w$

$\Rightarrow g^{-1}\bar{g}(q) = w \Rightarrow w \in O_G(q)$

(quindi $O_G(p) \subseteq O_G(q)$)

Abbiamo dimostrato $(*)$ da cui si ricava $O_G(p) \cap O_G(q) \neq \emptyset \Rightarrow O_G(p) = O_G(q)$

2) Siano $q \in O_G(p)$ e $g \in G$, allora $\exists \bar{g}$ tale che $q = \bar{g}(p)$

Allora $g(q) = g(\bar{g}(p)) = \bar{g}(g(p))$

$= g\bar{g}(p) \in O_G(p)$

otteniamo che $O_G(p)$ è G invariante

Sia $Y \subseteq O_G(p)$, Y G-invariante, $Y \neq \emptyset$

Sia $q \in Y \Rightarrow O_G(q) \subseteq Y \subseteq O_G(p)$

Y è G-invariante

si ottiene $O_G(q) = O_G(p) = Y$ $\triangle$

3) dipende dai precedenti $\left(Y = \bigcup_{p \in Y} O_G(p)\right)$ $\blacksquare$

Corollario: se G agisce su X e card $X < \infty$ allora

$$|X| = \sum_{x_i \in \Gamma} |O_G(x_i)|$$

dove Γ contiene esattamente un elemento per ogni orbita