Definizione: Sia G un gruppo. Definiamo $\underline{Aut(G)} = \{\varphi : G \longrightarrow G \mid \varphi \text{ è isomorfismo}\}$

Oss: $(Aut(G), \circ)$ è un gruppo (comp. di isomorfismi è isomorfismo e l'inverso c'è)

Definizione: Sia G un gruppo. Definiamo $\underline{Int(G)} = \{\varphi_g : G \longrightarrow G \mid \varphi_g(x) = gxg^{-1}\}$.

Oss: $Int(G)$ è sottogruppo normale di $Aut(G)$:

- $\underline{\varphi_g \in Aut(G)}$
  (a) φ_g è di gruppi:

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y)$$

  (b) φ_g ammette inversa (i.e. iniettiva e surgettiva) ed è $\varphi_{g^{-1}}$

$$\varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x = id(x) \quad \text{(e simmetrica)} \ \forall x \in G$$

- $\underline{Int(G) \text{ è sottogruppo}}$:
  (a) $id = \varphi_e$
  (b) $\varphi_g \circ \varphi_h \in Int(G)$:

$$\varphi_g \circ \varphi_h(x) = \varphi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = \varphi_{gh}(x) \qquad \forall x \in G$$

  (c) $\varphi_g \in Int(G) \Rightarrow \varphi_g^{-1} \in Int(G)$: Vale che $\varphi_g^{-1} = \varphi_{g^{-1}}$

- $\underline{Int(G) \text{ è normale}}$:
  $\forall \psi \in Aut(G)$ deve valere che $\psi\, Int(G) = Int(G)\, \psi$.

$$(\psi \circ \varphi_g)(x) = \psi(gxg^{-1}) = \psi(g)\psi(x)\psi(g^{-1}) = (\varphi_{\psi(g)} \circ \psi)(x) \quad \forall x \in G$$

Fatto Utile 1: Sia G un gruppo $\quad G/Z(G) \cong Int(G)$

Dim:
Considero la mappa

$$F : G \longrightarrow Int(G)$$
$$g \longmapsto \varphi_g : G \longrightarrow G$$

- $\underline{F \text{ è di gruppi}}$:

$$F(gh)(x) = \varphi_{gh}(x) \boxed{\overset{\text{dim Int}}{=}} \varphi_g \circ \varphi_h(x) = [F(g)F(h)](x)$$

- $\underline{F \text{ è surgettiva}}$. Sia $\varphi_g \in Int(G)$, scelgo $g \in G$ e $F(g) = \varphi_g$

- $\underline{\ker F = Z(G)}$

$$\ker F = \{g \in G \mid \varphi_g = id\} = \{g \in G \mid \varphi_g(x) = x \ \forall x\} =$$

$$\ker F = \{g\in G \mid \varphi_g = id\} = \{g\in G \mid \varphi_g(x) = x \ \forall x\} =$$
$$= \{g\in G \mid g^{-1}xg = x \ \forall x\} = \{g\in G \mid gx = xg \ \forall x\} = Z(G)$$

Dunque per il I teo di omomorfismo $G/Z(G) \cong Int(G)$

$\square$

Fatto Utile 2 Sia G gruppo, allora $\frac{G}{Z(G)}$ ciclico $\iff$ G abeliano

Dim:

$\boxed{\Leftarrow}$ Ovvia ($Z(G) = G \Rightarrow G/Z(G) = e$ abeliano)

$\boxed{\Rightarrow}$ Se $G/Z(G)$ è ciclico, allora $G/Z(G) = \langle g \rangle$. Ogni $x\in G$ si scrive in modo unico come $g^i z$ con $z\in Z(G)$. Verifico che G abeliano: siano $x,y\in G$

$$x\cdot y = g^i z_1 \cdot g^k z_2 \overset{z_i\in Z(G)}{\boxed{=}} g^i g^k z_1 z_2 \overset{\text{ciclico}}{\boxed{=}} g^k g^i z_2 z_1 \overset{z_i\in Z(G)}{\boxed{=}} g^k z_2\, g^i z_1 = yx$$

$\square$

Definizione: Una AZIONE di un gruppo G su un insieme X ($G \curvearrowright X$) è una mappa di gruppi

$$\Phi : G \longrightarrow S(X) = \{\text{bigezioni di } X\}$$

Una definizione equivalente è la seguente. Una azione è una mappa

$$\begin{aligned} G\times X &\longrightarrow X \\ (g,x) &\longmapsto g\cdot x \end{aligned}$$

tale che
1) $e\cdot x = x \quad \forall x\in X$
2) $g_1\cdot(g_2\cdot x) = (g_1 g_2)\cdot x \qquad \forall g_1,g_2\in G \ \forall x\in X.$

Definizione: Chiamiamo

- $Stab(x) = \{g\in G \mid g\cdot x = x\}$ lo STABILIZZATORE di x
- $orb(x) = \{y\in X \mid \exists g\in G \text{ t.c. } g\cdot x = y\}$ l' ORBITA di x

Oss: $Stab(x) \leq G$ ed è sottogruppo di G (Verificare)
$orb(x) \subseteq X$ quindi NON ha senso parlare di sottogruppo!

Oss: Le orbite partizionano X. Dunque $|X| = \sum_{x\in X/G} orb(x)$ dove $X/G = \{\text{insieme delle orbite}\}$
Sicuramente ogni elemento $x\in X$ appartiene a una orbita (a $orb(x)$).
Se adesso $x\in orb(x)$ e $x\in orb(y)$ allora vale che $orb(x) = orb(y)$ infatti $x = g\cdot y$ per un certo $g\in G$. Ma allora se $z\in orb(x)$ cioè $z = h\cdot x \Rightarrow$
$\Rightarrow z\in orb(y)$: $z = h\cdot x = h\cdot g\cdot y = (hg)\cdot y$. (e simmetrico)

Esempio: Sia $G = \mathbb{Z}^* = \{\pm 1\}$ e $X = \mathbb{R}$. Definiamo

Esempio: Sia $G = \mathbb{Z}^* = \{\pm 1\}$ e $X = \mathbb{R}$. Definiamo

$$\begin{aligned} \mathbb{Z}^* \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (g, x) &\longrightarrow g \cdot x \end{aligned}$$

$\longleftarrow$ inteso come moltiplicazione

È ovviamente una azione (II definizione). Chi sono le orbite?
Sia $x \in \mathbb{R}\setminus\{0\} \Rightarrow orb(x) = \{1 \cdot x, -1 \cdot x\} = \{x, -x\}$ cioè sono lui e il suo opposto.
Se $x = 0 \Rightarrow orb(0) = \{0\}$ cioè 0 è fissato da tutti gli elementi di $\mathbb{Z}^*$

Fatto Utile 3 Sia G gruppo $G \curvearrowright X$. Allora

$$\frac{G}{stab(x)} \longleftrightarrow orb(x)$$

È una Bigezione INSIEMISTICA. Stab(x) NON è detto sia normale e orb(x) è un insieme

Dim: Definisco la mappa

$$\begin{aligned} F: \frac{G}{Stab(x)} &\longrightarrow orb(x) \\ g \cdot stab(x) &\longmapsto g \cdot x \end{aligned}$$

Dobbiamo mostrare che

- F è ben definita (se cambio rappresentante l'immagine non cambia)

$g \cdot stab(x) = h \cdot stab(x) \Rightarrow h^{-1}g \in stab(x)$. Devo verificare che $g \cdot x = h \cdot x$:

$$h \cdot x = h \cdot (h^{-1}g) \cdot (x) = (h \cdot h^{-1})\, g \cdot (x) = g \cdot x$$

- F iniettiva:

$$F(g \cdot stab(x)) = F(h \cdot stab(x)) \iff g \cdot x = h \cdot x \iff h^{-1}g \in stab(x)$$

e dunque $h \cdot stab(x) = h \cdot h^{-1}g\, stab(x) = g \cdot stab(x)$

- F surgettiva: Sia $y \in orb(x) \Rightarrow \exists g \in G$ t.c. $g \cdot x = y$. Dunque è sufficiente prendere in partenza $g \cdot stab(x)$.

$\square$

Fatto Utilissimo: Formula delle classi:

$$\boxed{|X| \overset{Oss}{=} \sum_{x \in \frac{X}{G}} |orb(x)| \overset{FU3}{=} \sum_{x \in \frac{X}{G}} \frac{|G|}{|stab(x)|}}$$

Teorema (di Hamilton-Cayley): Sia G un gruppo finito, allora $G \hookrightarrow S_{|G|}$ ovvero G si immerge in $S_{|G|}$.
Dim: Definiamo l'azione di $G \curvearrowright G$ molt. a sinistra

$$G \times G \longrightarrow G$$
$$(g, x) \longmapsto gx$$

Tale mappa è una azione e determina un morfismo di gruppi (II def → I def)

$$\Phi : G \longrightarrow S_{|G|}$$
$$g \longmapsto \varphi_g : G \longrightarrow G$$
$$x \longmapsto gx$$

Dobbiamo verificare che Φ sia iniettivo e abbiamo la tesi.

$\Phi(g) = id \Rightarrow \Phi(g)(x) = \varphi_g(x) = gx = x \quad \forall x \in G$. In particolare

Se scelgo $x = e \Rightarrow g = e$ e dunque Φ iniettivo