

Def. (Azione di un gruppo su un insieme):

Dati un gruppo  $G$  e l'insieme  $X \neq \emptyset$  un' **AZIONE** di  $G$  su  $X$  è una funzione  $G \times X \rightarrow X$ ,  $(a, x) \mapsto ax$  t.c.:

- 1)  $a(bx) = (ab)x \quad \forall a, b \in G \quad \forall x \in X$
- 2)  $1x = x \quad \forall x \in X$

Esempi:

1) Dato  $V$  spazio vettoriale su  $\mathbb{C}$ , la funzione

$$\mathbb{C} \setminus \{0\} \times V \rightarrow V$$
$$(a, x) \mapsto ax \quad \text{è un'azione}$$

2) Dato  $X$  insieme,  $S(X)$  gruppo delle permutazioni su  $X$ , si ha:

$$S(X) \times X \rightarrow X$$
$$(\tau, x) \mapsto \tau(x) \quad \text{è un'azione}$$

3)  $G$  agisce su sé stessa per coniugio:

$a, x \in G \Rightarrow a_x := a \cdot a^{-1} =: f_a(x)$  è un'azione, infatti:

$$\begin{aligned} a(bx) &= a(b \cdot b^{-1})x = a(b \cdot b^{-1})a^{-1} = (ab)x(a b)^{-1} \\ &= abx \end{aligned}$$

4)  $G$  agisce su sé stessa per traslazioni (es. a sinistra):

$(a, x) \mapsto ax$  (prodotto in  $G$ ) è un'azione, infatti

$$a(bx) = (ab)x$$

5)  $G$  agisce su  $P(G)$  tramite il prodotto cartesiano di insiemi, infatti:

1)  $aA := \{ax \mid x \in A\}$  con  $A \subseteq G$

2)  $(a\phi) = \phi$

3)  $G$  agisce per coniugio su  $L(G)$  (sottogruppi di  $G$ ):

$$a_H = aHa^{-1} = \xrightarrow{f_a}(H)$$

4)  $G$  agisce su  $G/\sim_H$ :

$$a(xH) = (ax)H$$

Se l'azione di  $G$  su  $X$  è data, possiamo considerare, per  $a \in G$ , l'azione  $f_a : X \rightarrow X$ . Tale  $f_a$  è biiettiva:

$$f_a^{-1} = f_{a^{-1}}$$

$$f_a(f_{a^{-1}}(x)) = f_a(a^{-1}x) = a(a^{-1}x) = x$$

$\Rightarrow f_a \in S(X)$ , quindi siamo definite l'applicazione  $\varphi : G \rightarrow S(X)$  t.c.  $\varphi(a) = f_a$ . Dimostriamo che tale  $\varphi$  è omomorfismo (ovvero che  $\varphi_{ab} = \varphi_a \circ \varphi_b$ ):

$$\begin{aligned} \varphi(ab) &= f_{ab} = (ab)x = a(bx) \\ &= f_a(bx) = f_a \circ f_b = \varphi(a)\varphi(b) \end{aligned}$$

$\Rightarrow \text{Ker } \varphi$  è detto **NUCLEO DELL'AZIONE** ed è (per il Teorema dell' Omomorfismo) sottogruppo normale di  $G$ . Possiamo caratterizzarla così:

$$a \in \text{Ker } \varphi \Leftrightarrow ax = x \quad \forall x \in X \Leftrightarrow f_a = \text{Id}$$

negli esempi sopra si ha:

3) Azione per coniugio:

$$\text{Ker} = Z(G) = \{a \in G \mid axa^{-1} = x \quad \forall x \in G\} \text{ ed è}$$

il **CENTRO** di  $G$ :

$$axa^{-1} = x \Leftrightarrow ax = xa$$

$\Rightarrow$  dato che è nucleo di un'azione,  $Z(G)$  è  
sottogruppo normale di  $G$

4) Azione per traslazioni:

$$\text{Ker} = \{1\} = \{a \in G \mid ax = x \quad \forall x \in G\}$$

$\Rightarrow$  il nucleo è banale, in questo caso  $\varphi : G \rightarrow S(G)$   
è un automorfismo iniettivo.

Teorema (di Cayley):

$\forall G$  gruppo  $\exists X$  insieme t.c.  $G$  sia isomorfo ad un  
sottogruppo di  $S(X)$

Dim.

Basta prendere  $X = G$ .

q.e.d.

Se  $|G| = n$ , allora  $G$  è isomorfo ad un sottogruppo  
di  $S_n$ , dato che  $S_n \cong S(G)$ .

Dato l'azione di  $G$  su  $X$  definiamo

$$x \sim y \Leftrightarrow \exists a \in G \text{ t.c. } ax = y$$

$\Rightarrow \sim$  è relazione di equivalenza (è riflessiva, simmetrica

e transitiva) e le classi di equivalenza sono dette orbite:

$$O(x) = \{ax \mid a \in G\} \text{ con } x \in X$$

$\Rightarrow$  Se  $\exists! O(x) \forall x$ , l'azione si dice TRANSITIVA  
(es. traslazione a sinistra)

Esempio:

Se  $H$  è sottogruppo di  $G$  che agisce su  $X$ , allora  $H$  agisce su  $X$ :

- Su agisce su  $\{1, 2, \dots, n\}$ :  
 $\tau \in S_n \Rightarrow \langle \tau \rangle$  agisce su  $\{1, \dots, n\}$  e le orbite "sono" i cicli disgiunti

Def. (Stabilizzatore):

Sia  $G$  gruppo finito che agisce su  $X$ . Lo STABILIZZATORE di  $x \in X$  è  $G_x = \{a \in G \mid ax = x\}$  ed è sottogruppo di  $G$ :

- 1)  $1 \in G_x$  ( $1x = x \quad \forall x \in X$ )
- 2)  $a, b \in G_x \Rightarrow (ab)x = a(bx) = ax = x \Rightarrow ab \in G_x$
- 3)  $a \in G_x \Rightarrow ax = x \Rightarrow a^{-1}x = a^{-1}(ax) = (a^{-1}a)x = 1x = x \Rightarrow a^{-1} \in G_x$

Proposizione

Dato  $G$  gruppo che agisce su  $X$ , si ha che:

$$|O(x)| = [G : G_x] \quad \forall x \in X$$

Dim.:

$ax = bx \Leftrightarrow a^{-1}bx = x \Leftrightarrow a \sim_{G_x} b$  quindi possiamo definire  $O(x) \rightarrow G/G_x$ ,  $ax \mapsto [a] = aG_x$  che è biiettiva.

q.e.d.

Ciò comporta che  $|O(x)|$  divide  $|G|$  !!!

Esempio (stabilizzazione):

Nell'azione di  $G$  su se stesso per conjugio la stabilizzazione di  $x \in G$  è  $C_x = \{a \in G \mid a_x = x\}$   
 $\Rightarrow a \in C_x \Leftrightarrow axa^{-1} = x \Leftrightarrow ax = xa$ .  $C_x$  è detta CENTRALIZZANTE di  $x$  e si ha:

$$Z(G) = \bigcap_{x \in G} C_x$$

Dato  $G$  gruppo finito, chiamiamo  $x_1, \dots, x_n$  gli elementi t.c.  $O(x_1), \dots, O(x_n)$  sono TUTTE le orbite a 2 a 2 distinte nell'azione per conjugio di  $G$  su se stesso.

Facciamo in modo che  $x_{n+1}, \dots, x_m$  definisca le orbite di 1 solo elemento ( $|O(x_i)| = 1$ ), allora si ha:

$$O(x) = \{x\} \Leftrightarrow x \in Z(G)$$

$$(a_x = x \quad \forall a \in G \Leftrightarrow axa^{-1} = x \Leftrightarrow x \in Z(G))$$

Possiamo allora dire che  $G = O(x_1) \cup \dots \cup O(x_r) \cup Z(G)$  che è una scrittura di insiemni a 2 a 2 disgiunti !!!

Quindi:

$$|G| = |Z(G)| + \sum_{i=1}^r |O(x_i)| = |Z(G)| + \sum_{i=1}^r [G : C_{x_i}]$$

Tale equazione è detta Equazione delle Classi, e si nota che ogni addendo presente al suo interno divide  $|G|$

Def. ( $p$ -gruppo):

$G$  è un  $p$ -gruppo se  $|G| = p^k$  con  $p$  primo,  $k > 0$ , oppure, equivalentemente, se ogni elemento di  $G$  ha ordine una potenza di  $p$ .

→ applicando l'equazione delle classi ad un  $p$ -gruppo si ha:

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^r [G : C_{x_i}]$$

$\underbrace{\quad}_{> 1}$

quindi  $p \mid \sum_{i=1}^r [G : C_{x_i}]$  e segue che:

$$|\mathcal{Z}(G)| = |G| - \sum_{i=1}^r [G : C_{x_i}] \text{ è divisibile per } p$$

⇒  $|\mathcal{Z}(G)| > 1$  cioè ogni  $p$ -gruppo ha centro non banale.

⇒ ciò significa, per esempio, che il centro di un gruppo diedrale di  $2^k$  elementi non è banale.

Mostriamo ora che, data  $p$  primo, ogni gruppo di ordine  $p^2$  è abeliano:

dato  $G$  t.c.  $|G| = p^2$  si ha  $|\mathcal{Z}(G)| = p$  ∨  $|\mathcal{Z}(G)| = p^2$

⇒ se  $|\mathcal{Z}(G)| = p^2$  allora  $\mathcal{Z}(G) = G$  e quindi  $G$  è abeliano

$\Rightarrow$  mostriamo che non può essere  $|\mathcal{Z}(G)| = p$ :

$\Rightarrow$  se  $|\mathcal{Z}(G)| = p$  allora  $|G/\mathcal{Z}(G)| = p$  e quindi  $G/\mathcal{Z}(G)$  è ciclica. Sia  $\alpha \in \mathcal{Z}(G)$  un suo generatore, allora gli elementi di  $G$  sono tutti della forma  $\alpha^m x$  con  $x \in \mathcal{Z}(G)$  e quindi:

$$\begin{aligned}(\alpha^m x)(\alpha^n y) &= \alpha^m \alpha^n xy = \alpha^{m+n}(xy) \\&= (xy)\alpha^{m+n} = (\alpha^n y)(\alpha^m x)\end{aligned}$$

$\Rightarrow$  ogni elemento di  $G$  sta in  $\mathcal{Z}(G)$ , perciò  $G$  è abeliano  $\Leftrightarrow$

$\Rightarrow$  Se  $|G| = p^3$  e  $G$  non è abeliano, allora  $|\mathcal{Z}(G)| = p$  ( $D_4$  non è abeliano, ma è un 2-gruppo, quindi  $|\mathcal{Z}(D_4)| = 2$ )

---

Dato  $G$  gruppo, definisco:

$$\cdot \mathcal{Z}_0(G) = \{1\}, \quad \mathcal{Z}_1(G) = \mathcal{Z}(G)$$

$\cdot \mathcal{Z}_{i+1}(G) =$  unico sottogruppo di  $G$  t.c.:

$$\mathcal{Z}_i(G) \subseteq \mathcal{Z}_{i+1}(G) \wedge$$

$$\mathcal{Z}_{i+1}(G)/\mathcal{Z}_i(G) = \mathcal{Z}(G/\mathcal{Z}_i(G))$$

$\Rightarrow$  chi sarà  $\mathcal{Z}_2(G)$ ? Deve essere t.c.:

$$\mathcal{Z}_1(G) \subseteq \mathcal{Z}_2(G) \wedge \mathcal{Z}_2(G)/\mathcal{Z}_1(G) = \mathcal{Z}(G/\mathcal{Z}_1(G))$$

$$\Rightarrow \mathcal{Z}_{i+1} = \pi^{-1}(\mathcal{Z}(G/\mathcal{Z}_i(G)))$$

$$\Rightarrow \{1\} = \mathcal{Z}_0(G) \trianglelefteq \mathcal{Z}_1(G) \trianglelefteq \mathcal{Z}_2(G) \trianglelefteq \dots$$

$\Rightarrow$  in generale, se  $G$  è un  $p$ -gruppo, si ha:

$$\{1\} = Z_0(G) \triangleleft \dots \triangleleft Z_{m-1}(G) \triangleleft Z_m(G) = G$$

e  $Z_{i+1}(G)/Z_i(G)$  è abeliano !!!

Def. (Gruppo Risolubile):

Un gruppo  $G$  si dice **Risolubile** se esistono

$H_0 = \{1\}$ ,  $H_1, \dots, H_m = G$  sottogruppi di  $G$  t.c.:

$$H_0 = \{1\} \triangleleft H_1 \triangleleft \dots \triangleleft H_{m-1} \triangleleft H_m = G$$

con  $H_{i+1}/H_i$  abeliano

L'insieme  $\{H_0 = \{1\}, \dots, H_{m-1}, H_m = G\}$  è detto **SERIE ABELIANA**.

Esempi:

1)  $S_3$  è risolubile:

$$H_0 = \{(1)\}, H_1 = \langle (123) \rangle = A_3, H_2 = S_3$$

$$\Rightarrow H_0 \triangleleft A_3 \triangleleft S_3$$

2)  $S_4$  è risolubile:

dato  $V = \{(1), (12)(34), (13)(24), (14)(23)\}$

(gruppo di Klein) sottogruppo di  $S_4$  e di  $A_4$

(gruppo alterno di  $S_4$ ), si ha che  $V$  è sottogruppo normale di  $A_4$  e  $[A_4 : V] = 3$

$$\Rightarrow H_0 = \{(1)\}, H_1 = V, H_2 = A_4, H_3 = S_4$$

$$\Rightarrow |H_2/H_1| = 3 \quad (\Rightarrow H_2/H_1 \text{ è abeliano})$$

$$\Rightarrow |H_3/H_2| = 2 \quad (\Rightarrow H_3/H_2 \text{ è abeliano})$$

$\Rightarrow S_4$  è risolubile

Supponiamo di avere un gruppo  $G$  con  $|G|=4$   
 $\Rightarrow G = \{1, a, b, c\}$ . Costruiamo la tabella dell'operazione su  $G$ :

N.B.

In ogni riga e colonna ciascun elemento compare ESATTAMENTE 1 VOLTA!!! (Proprietà di  $\cdot$ : definisce una biiezione)

$\Rightarrow$  ci sono 2 alternative:

1)  $a^2 \neq 1$ ,  $\underbrace{a^2 = b}$ :

NON RESTRITTIVO

2)  $a^2 = 1$ :

$$\Rightarrow b^2 = 1$$

.	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

.	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(In ② deve essere necessariamente  $b^2 = 1$ , altrimenti saremmo nuovamente nella situazione precedente)

$\Rightarrow a$  ha ordine 4, quindi (dato che  $|G|=4$ )  
 $G$  è ciclico generato da  $a$ .

$\Rightarrow G$  è detto **GRUPPO DI KLEIN**, e si ha che ogni gruppo di ordine 4 è ciclico oppure è isomorfo al gruppo di Klein.