CAPITOLO C

Azione di Gruppo su un Insieme

La nozione di gruppo che agisce su un insieme generalizza quella di permutazioni di un insieme. La fondamentale rilevanza di questo argomento risiede nel fatto che trova notevoli applicazioni nel calcolo algebrico combinatorio e nello studio delle strutture dei gruppi finiti.

Questo capitolo è interamente dedicato allo studio di questo argomento, dopo aver introdotto le definizioni di orbita e stabilizzatore ed illustrato le relative proprietà, vengono approfondite l'equazione delle classi, transitività e normalità.

C1. Azione di gruppo su un insieme

Definizione C1.1. *Dati un insieme* $\Omega = \{\alpha, \beta, \gamma, \cdots\}$ *ed un gruppo* G, *si dice che* G *agisce su* Ω *quando è assegnata una funzione*

$$\Omega \times G \longrightarrow \Omega$$

che denoteremo così

$$(\alpha, g) \longmapsto \alpha^g \quad \textit{per ogni} \quad \alpha \in \Omega \quad e \quad g \in G$$

tale che valgono le proprietà:

(a) $(\alpha^g)^h = \alpha^{gh}$ *per ogni* $\alpha \in \Omega$ *e* $g, h \in G$.
(b) $\alpha^e = \alpha$ *per ogni* $\alpha \in \Omega$, *dove* e *è l'elemento neutro di* G.

La funzione assegnata si chiama azione *di* G *su* Ω. *Denoteremo con* (G, Ω) *un gruppo* G *che agisce su un insieme* Ω.

Se H è un sottogruppo di G e G agisce su Ω allora anche H agisce su Ω. Se Ω è un gruppo e $G = \mathrm{Aut}(\Omega)$ allora G agisce su Ω.

Se Ω è un insieme qualsiasi, il gruppo simmetrico S_Ω agisce su Ω e così ogni suo sottogruppo.

La nozione di gruppo che agisce su un insieme generalizza quella di gruppo di permutazioni di un insieme.

Lemma C1.2. *Se un gruppo G agisce su un insieme Ω, ogni elemento di G dà luogo ad una permutazione di Ω. Più precisamente, la corrispondenza*

$$\phi : \alpha \longmapsto \alpha^g$$

è, per ogni fissato $g \in G$, una permutazione di Ω.

DIMOSTRAZIONE. Ricordiamo che una permutazione su un generico insieme Ω è una biiezione da Ω su Ω, cioè un'applicazione iniettiva e suriettiva, quindi dobbiamo provare che per ogni $g \in G$:

$$\phi_g : \Omega \longrightarrow \Omega \quad \text{con} \quad \phi_g(\alpha) = \alpha^g$$

è una funzione iniettiva e suriettiva. Se dimostriamo questo per un arbitrario $g \in G$, essa sarà valida per ogni elemento di G.

Siano $g \in G$ e $\alpha, \beta \in \Omega$ tali che $\alpha^g = \beta^g$. Poiché G è un gruppo, ogni suo elemento è invertibile, quindi se $g \in G$ anche $g^{-1} \in G$, pertanto, applicando la definizione di gruppo che agisce su un insieme, possiamo scrivere:

$$\alpha = \alpha^e = \alpha^{(gg^{-1})} = (\alpha^g)^{g^{-1}} = (\beta^g)^{g^{-1}} = \beta^{(gg^{-1})} = \beta^e = \beta.$$

Dunque se due membri hanno la stessa immagine questi risultano coincidenti, cioè ϕ_g è iniettiva.

Sia $\beta \in \Omega$ e poniamo $\gamma = \beta^{g^{-1}}$. Poiché G agisce su Ω si ha $\gamma \in \Omega$ e

$$\gamma^g = (\beta^{g^{-1}})^g = \beta^{(g^{-1}g)} = \beta^e = \beta.$$

Quindi, preso un arbitrario membro del codominio, questo risulta sempre essere l'immagine di un membro del dominio, ne segue che ϕ_g è suriettiva. Dunque ϕ_g è biiettiva da Ω a Ω. □

Nota C1.3. *Sia S_Ω il gruppo simmetrico su Ω, cioè il gruppo che ha come elementi l'insieme delle permutazioni su Ω e, come operazione, l'usuale composizione di funzioni.*

Se un gruppo G agisce su Ω, la corrispondenza

$$\theta : G \longrightarrow S_{|\Omega|} \quad \text{con} \quad g \longmapsto \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^g, & \beta^g, & \gamma^g, & \cdots \end{pmatrix}$$

associa ad ogni elemento $g \in G$, una permutazione di Ω. Tale corrispondenza, che prende il nome di rappresentazione di G come gruppo di permutazioni di Ω, è un omomorfismo. Infatti, premesso che

$$\forall\ g \in G: \quad \Omega = \{\alpha, \beta, \gamma, \cdots\} = \{\alpha^g, \beta^g, \gamma^g, \cdots\}$$

allora se $g, f \in G$, vale

$$\theta(g) \circ \theta(f) = \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^g, & \beta^g, & \gamma^g, & \cdots \end{pmatrix} \circ \begin{pmatrix} \alpha^g, & \beta^g, & \gamma^g, & \cdots \\ (\alpha^g)^f, & (\beta^g)^f, & (\gamma^g)^f, & \cdots \end{pmatrix}$$

$$= \begin{pmatrix} \alpha, & \beta, & \gamma, & \cdots \\ \alpha^{gf}, & \beta^{gf}, & \gamma^{gf}, & \cdots \end{pmatrix} = \theta(g \cdot f).$$

Il suo *nucleo* (si chiama nucleo dell'azione) è dato da

$$K = \{g \in G \mid \alpha^g = \alpha, \quad \forall\ \alpha \in \Omega\}$$

il quale, per il teorema d'omomorfismo per i gruppi, risulta essere un sottogruppo normale di G. Se $K = \{e\}$, si dice che l'azione è *fedele*, ovvero che G agisce fedelmente su Ω. In tal caso, G è isomorfo ad un sottogruppo del gruppo simmetrico S_Ω sempre per il teorema citato precedentemente; si dirà allora che G è un gruppo di permutazioni di Ω.

Esempio C1.4. *Fissiamo Ω uguale all'insieme degli elementi del gruppo G e definiamo un'azione di G su Ω in questo modo*

$$\forall\ \alpha, g \in G: \quad \alpha^g = \alpha g.$$

Vediamo se l'azione di G su Ω così definita, verifica le proprietà della definizione, sfruttando la proprietà associativa dei gruppi come segue:

- Per ogni $\alpha \in \Omega$ e $g, h \in G$, vale $(\alpha^g)^h = (\alpha g)^h = (\alpha g)h = \alpha(gh) = \alpha^{gh}$.
- Per ogni $\alpha \in \Omega$ e l'elemento neutro e di G, si ha che $\alpha^e = \alpha \cdot e = \alpha$.

Il nucleo dell'azione è l'identità di G (l'elemento neutro di G), quindi essa è un'azione fedele di G su Ω e l'omomorfismo $G \longrightarrow S_\Omega$ è un isomorfismo tra G e un sottogruppo del suo gruppo simmetrico $S_{|G|}$. Tale omomorfismo prende il nome di rappresentazione regolare destra di G, dal momento che esso si ottiene moltiplicando a destra gli elementi di G per un elemento fissato.

La moltiplicazione a sinistra non definisce un'azione (a meno che G non sia abeliano) perché viene meno la condizione [**a**] della definizione dell'azione di un gruppo su un insieme. Sostituendo la suddetta definizione con $\alpha^g = g^{-1}\alpha$, si ha una teoria perfettamente analoga a quella esposta.

Teorema C1.5 (Cayley). *Ogni gruppo G è isomorfo ad un sottogruppo di $S_{|G|}$, il gruppo simmetrico sugli elementi di G. In particolare, un gruppo finito di ordine n è isomorfo ad un sottogruppo di S_n, il gruppo simmetrico di n lettere.* □

C2. Orbita e stabilizzatore

Definizione C2.1. *Se G agisce su Ω e $\alpha \in \Omega$, si chiama* orbita *di α sotto l'azione di G, e si indica con α^G, il sottoinsieme di Ω così definito:*

$$\alpha^G = \{\alpha^g \mid g \in G\}$$

cioè l'insieme dei membri di Ω in cui α è portato dai vari elementi di G. Allora si deduce che

$$\Omega = \bigcup_{\alpha \in \Omega} \alpha^G.$$

Nota C2.2. *Sia G un gruppo che agisce su un insieme Ω e definiamo su Ω la seguente relazione "$\sim$":*

$$\forall \alpha, \beta \in \Omega: \quad \alpha \sim \beta \Longleftrightarrow \exists g \in G \quad \textit{tale che} \quad \alpha^g = \beta.$$

Tale relazione è una equivalenza su Ω e le classi da essa indotte altro non sono che le orbite degli elementi di Ω. Pertanto due orbite o coincidono o sono disgiunte.

L'azione di un gruppo G su un insieme Ω induce, quindi, una partizione su Ω e allora

$$\Omega \quad = \quad \biguplus_{\alpha \in C} \alpha^G$$

dove C è un sistema di rappresentanti delle orbite di Ω. In particolare se Ω è finito, si ottiene l'identità

$$|\Omega| \quad = \quad \sum_{\alpha \in C} |\alpha^G|.$$

Definizione C2.3. *Se G agisce su Ω e $\alpha \in \Omega$, si chiama* stabilizzatore *di α, e si indica con G_α, il sottoinsieme di G così definito:*

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$$

cioè l'insieme degli elementi di G che fissano α.

Esso rappresenta l'insieme degli elementi di G che fissano α. Osserviamo che se un elemento di G appartiene ad ogni stabilizzatore, allora appartiene

al nucleo dell'azione; viceversa, il nucleo K dell'azione di G su Ω si può ottenere come intersezione degli stabilizzatori degli elementi di Ω

$$K \quad = \quad \bigcap_{\alpha \in \Omega} G_\alpha.$$

Le relazioni tra orbite e stabilizzatori sono messe in evidenza dal teorema seguente.

Teorema C2.4. *Sia G un gruppo che agisce su un insieme Ω. Allora*

(a) *due orbite o coincidono o sono disgiunte.*
(b) *lo stabilizzatore G_α di un membro $\alpha \in \Omega$, è un sottogruppo di G.*
(c) *se β appartiene all'orbita di α, allora G_β è coniugato di G_α; più precisamente, se $\beta = \alpha^g$, si ha che $G_\beta = G_{\alpha^g} = G_\alpha^g$.*
(d) *l'indice in G dello stabilizzatore di un membro è uguale alla cardinalità dell'orbita del membro*

$$[G : G_\alpha] = |\alpha^G|.$$

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] Siano $\alpha, \beta \in \Omega$ e supponiamo che le rispettive orbite abbiano intersezione non vuota, cioè $\alpha^G \cap \beta^G \neq \emptyset$.

Dimostriamo che $\alpha^G = \beta^G$ tramite la doppia inclusione, osservando che è sufficiente far vedere che

$$\beta \in \alpha^G \qquad \text{e} \qquad \alpha \in \beta^G.$$

Supponendo $\alpha^G \cap \beta^G \neq \emptyset$, ne segue che esiste $\gamma \in \Omega$ tale che

$$\gamma \in \alpha^G \cap \beta^G \quad \Longrightarrow \quad \exists\, g, h \in G : \quad \gamma = \alpha^g = \beta^h$$

da cui segue

$$(\alpha^g)^{g^{-1}} = (\beta^h)^{g^{-1}} \quad \text{e} \quad (\alpha^g)^{h^{-1}} = (\beta^h)^{h^{-1}}$$

quindi

$$\alpha = \beta^{(hg^{-1})} \quad \Longrightarrow \quad \alpha \in \beta^G \quad \Longrightarrow \quad \alpha^G \subseteq \beta^G$$

mentre

$$\beta = \alpha^{(gh^{-1})} \quad \Longrightarrow \quad \beta \in \alpha^G \quad \Longrightarrow \quad \beta^G \subseteq \alpha^G.$$

Pertanto dalla doppia inclusione, si ha $\alpha^G = \beta^G$.

[b] Per la caratterizzazione dei sottogruppi basta dimostrare che

- G_α è chiuso rispetto alla moltiplicazione.
- Per ogni $g \in G_\alpha$ esiste $g^{-1} \in G_\alpha$ tale che $gg^{-1} = g^{-1}g = e$.

Siano $g, h \in G_\alpha$, allora $\alpha^g = \alpha \quad \text{e} \quad \alpha^h = \alpha$. Poiché G agisce su Ω, possiamo scrivere

$$\alpha^{gh} = (\alpha^g)^h = \alpha^h = \alpha \quad \Longrightarrow \quad gh \in G_\alpha$$

pertanto G_α è chiuso. Se $g \in G_\alpha$ allora $\alpha^g = \alpha$, quindi

$$\alpha^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^e = \alpha$$

ne segue che $g^{-1} \in G_\alpha$.

Ora, poiché abbiamo anche dimostrato che ogni elemento di G_α è invertibile, possiamo concludere che G_α è un sottogruppo di G.

[c] Sia $\beta \in \alpha^G$, allora esiste $g \in G$ tale che $\beta = \alpha^g$. Dobbiamo provare che $G_\beta = G_\alpha^g$, dove con G_α^g indichiamo il coniugato di G_α sotto coniugio di g. Proviamola con la doppia inclusione.

"$\subseteq$" Sia $y \in G_\beta \implies \beta^y = \beta$. Ma $\beta = \alpha^g$ pertanto

$$(\alpha^g)^y = \alpha^g \quad \Longrightarrow \quad \alpha^{gy} = \alpha^g \quad \Longrightarrow \quad \alpha^{gyg^{-1}} = \alpha$$

quindi gyg^{-1} appartiene allo stabilizzatore di α per cui vale anche

$$y = g^{-1}(gyg^{-1})g \quad \Longrightarrow \quad y \in G_\alpha^g.$$

Poiché y è un elemento arbitrario di G_β, otteniamo $G_\beta \subseteq G_\alpha^g$.

"$\supseteq$" Sia $x \in G_\alpha^g \implies \exists\, y \in G_\alpha : \; x = g^{-1}yg \implies y = gxg^{-1}$ ora, poiché y appartiene allo stabilizzatore di α, si ha

$$\alpha^{gxg^{-1}} = \alpha \quad \Longrightarrow \quad \alpha^{gx} = \alpha^g \quad \Longrightarrow \quad (\alpha^g)^x = \alpha^g$$

ma $\alpha^g = \beta$, quindi $\beta^x = \beta$, cioè $x \in G_\beta$. In questo caso abbiamo dimostrato che $G_\alpha^g \subseteq G_\beta$ e quindi possiamo concludere che $G_\beta = G_\alpha^g$.

[d] Poiché $G_\alpha \leqslant G$, possiamo considerare l'insieme dei laterali destri di G_α in G, che indichiamo con $\mathcal{L}$:

$$\mathcal{L} = \{G_\alpha g \mid g \in G\}.$$

Definendo l'applicazione

$$\psi : \quad \mathcal{L} \longrightarrow \alpha^G \quad \text{con} \quad \psi(G_\alpha g) = \alpha^g$$

e ricordando che $|\mathcal{L}| = [G : G_\alpha]$, per ottenere la tesi è sufficiente provare che ψ è biiettiva.

Prima di tutto, dobbiamo verificare che ψ è ben posta. Infatti, per un laterale destro di G_α con due rapprasentanti diversi $g, h \in G$, si ha che $G_\alpha g = G_\alpha h$. Allora esiste un $x \in G_\alpha$ tale che $h = xg$. Ne segue

$$\psi(G_\alpha h) = \alpha^h = \alpha^{xg} = (\alpha^x)^g = \alpha^g.$$

Siano $g, h \in G$ tali che $\alpha^g = \alpha^h$. Poiché valgono le seguenti implicazioni

$$\alpha^{gh^{-1}} = \alpha \quad \Longrightarrow \quad gh^{-1} \in G_\alpha \quad \Longrightarrow \quad G_\alpha g = G_\alpha h$$

ψ è una applicazione iniettiva. La funzione ψ è ovviamente suriettiva. □

Corollario C2.5. *Se G agisce su Ω, si ha:*

(a) *Ω è unione disgiunta delle orbite $\{\alpha^G\}$ dei suoi membri*

$$\Omega = \biguplus_{\alpha \in C} \alpha^G$$

e quindi, se Ω è finito, vale

$$|\Omega| = \sum_{\alpha \in C} |\alpha^G|$$

dove C è un sistema di rappresentanti per le orbite di Ω.

(b) *Se G è finito, allora*

$$|G| = |\alpha^G| \cdot |G_\alpha| \quad \textit{per ogni} \quad \alpha \in \Omega.$$

DIMOSTRAZIONE. Procediamo per ordine iniziando dal primo punto.

[a] Segue banalmente dal punto **[a]** del Teorema **C2.4**.

[b] Per il teorema di Lagrange

$$|G| = [G : G_\alpha] \cdot |G_\alpha|$$

e per il punto **[d]** del Teorema **C2.4**

$$[G : G_\alpha] = |\alpha^G| \quad \Longrightarrow \quad |G| = |G_\alpha| \cdot |\alpha^G|. \qquad \square$$

Proposizione C2.6. *Siano G un p-gruppo finito* (cioè ogni elemento di G ha come ordine una potenza di p) *che agisce su un insieme Ω finito e*

$$\Omega_0 = \{\alpha \in \Omega \mid \alpha^g = \alpha \quad \forall\ g \in G\}.$$

Allora

$$|\Omega| \equiv |\Omega_0| \pmod{p}.$$

DIMOSTRAZIONE. Se C è un sistema di rappresentanti per le orbite dei membri di Ω, per il punto **[a]** del Corollario **C2.5** si ha

$$|\Omega| = \sum_{\alpha \in C} |\alpha^G|$$

inoltre possiamo scrivere che

$$\Omega_0 = \left\{\alpha \in C \mid \alpha^G = \{\alpha\}\right\}$$

quindi posto

$$D = C \backslash \Omega_0 = \left\{\alpha \in C \mid |\alpha^G| > 1\right\}$$

risulta che D è un sistema di rappresentanti per le orbite di Ω che hanno cardinalità maggiore di 1, dunque

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|.$$

Per ipotesi G è un p-gruppo finito, quindi la sua cardinalità è una potenza di p in base al Corollario **B2.2**, cioè

$$\exists\, n \in \mathbb{N} \quad \text{tale che} \quad |G| = p^n.$$

Osserviamo che per ogni $\alpha \in \Omega_0$, si ha che

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\} = G$$

mentre, se consideriamo $\alpha \in D$, si ha $G_\alpha \neq G$. Infatti

$$\alpha \in D \quad \Longrightarrow \quad [G : G_\alpha] = |\alpha^G| > 1 \quad \Longrightarrow \quad G_\alpha \neq G$$

quindi $|G_\alpha| < p^n$. Anche G_α è un p-gruppo finito, allora $|G_\alpha|$ risulta una potenza di p. Ora, essendo $|\alpha^G| = |G|/|G_\alpha|$, anche l'ordine di α^G è una potenza di p e pertanto

$$\sum_{\alpha \in D} |\alpha^G|$$

è un multiplo di p. Dalla relazione

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|$$

si ha che $|\Omega| - |\Omega_0|$ è un multiplo di p, cioè $|\Omega| \equiv |\Omega_0| \pmod{p}$. □

Applicando il Teorema **C2.4** ed il Corollario **C2.5**, possiamo dimostrare alcune proprietà dei gruppi finiti, introducendo opportune azioni su particolari insiemi. Vediamo un esempio.

Esempio C2.7. *Siano G un gruppo finito e A, B due sottogruppi di G. Allora*

$$|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|} \quad \textit{dove} \quad A \cdot B = \Big\{ab \mid a \in A, b \in B\Big\}.$$

DIMOSTRAZIONE. Sia Ω l'insieme dei sottoinsiemi non vuoti di G:

$$\Omega := \{S \subseteq G \mid S \neq \emptyset\}.$$

Facciamo agire G su Ω definendo $S^g := Sg$ per ogni $g \in G$, dove con Sg indichiamo il prodotto del sottoinsieme S con g. Questa è effettivamente un'azione e la verifica è immediata.

Ora, il sottogruppo A è un membro di Ω e B agisce su Ω. Sotto l'azione di B lo stabilizzatore di A è:

$$B_A = \{g \in B \mid A\,g = A\}$$

da cui $B_A = A \cap B$, mentre l'orbita di A è data da:

$$A^B = \{A\,g \mid g \in B\}.$$

Per il Corollario **C2.5**, si ha subito che

$$|A^B| = [B : B_A] = \frac{|B|}{|A \cap B|}.$$

Ma $|Ag| = |A|$ e quindi $|A^B| = \frac{|A \cdot B|}{|A|}$, il numero dei laterali è uguale alla cardinalità di $A \cdot B$ diviso il numero degli elementi di ogni laterale. Ne segue

$$\frac{|B|}{|A \cap B|} = \frac{|A \cdot B|}{|A|}$$

da cui la tesi. □

C3. Equazione delle classi

Per due elementi $a, b \in G$, si dice che b è coniugato ad a in G se esiste un elemento $g \in G$ tale che $b = g^{-1}ag$. Chiameremo coniugio questa relazione, la quale, essendo una relazione di equivalenza, induce una partizione di G in classi di equivalenza disgiunte (le classi di coniugio). Per ogni $\alpha \in G$, indichiamo con $\mathrm{Cl}(\alpha)$ la *classe di coniugio* a cui α appartiene.

Definizione C3.1. *Se $a \in G$, si definisce centralizzante di a in G, e si indica con $C_G(a)$, l'insieme:*

$$C_G(a) = \{x \in G \mid xa = ax\}.$$

$C_G(a)$ è l'insieme degli elementi di G che permutano con a. Inoltre, si definisce centro di un gruppo G, l'insieme

$$Z(G) = \{x \in G \mid xg = gx \quad \forall\, g \in G\}.$$

Evidentemente si ha che

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

Esempio C3.2. *Sia G un gruppo finito, $\Omega = G$ e consideriamo (G, Ω) tramite coniugio nel seguente modo:*

$$\alpha^g = g^{-1}\alpha g \quad \textit{per ogni} \quad \alpha \in \Omega \quad e \quad g \in G.$$

Verifichiamo che si tratta effettivamente di un'azione di G su Ω. Per ogni $\alpha \in \Omega$ e per ogni $g, h \in G$ si vede facilmente che

$$\alpha^e = e^{-1}\alpha e = \alpha \quad e \quad (\alpha^g)^h = h^{-1}(g^{-1}\alpha g)h = (gh)^{-1}\alpha(gh) = \alpha^{gh}.$$

Determiniamo ora, orbite e stabilizzatore sotto l'azione di G.

$$\begin{aligned} \forall\ \alpha \in \Omega: \quad \alpha^G &= \{\alpha^g \mid g \in G\} = \{g^{-1}\alpha g \mid g \in G\} = \mathrm{Cl}(\alpha); \\ G_\alpha &= \{g \in G \mid \alpha^g = \alpha\} = \{g \in G \mid g^{-1}\alpha g = \alpha\} \\ &= \{g \in G \mid \alpha g = g\alpha\} = C_G(\alpha). \end{aligned}$$

Quindi per il punto **[d]** *del* Teorema **C2.4** *segue che*

$$|\mathrm{Cl}(\alpha)| = [G : C_G(\alpha)].$$

Dall'ultimo esempio, si evince che il nucleo dell'azione è il centro $Z(G)$ in G. Ne consegue l'equazione delle classi.

Proposizione C3.3 (Equazione delle classi). *Sia G un gruppo finito. Vale la seguente*

$$|G| = |Z(G)| + \sum_{k=1}^{m} |\mathrm{Cl}(x_k)| = |Z(G)| + \sum_{k=1}^{m} [G : C_G(x_k)]$$

dove $\{x_k\}_{k=1}^m$ è un sistema di rappresentanti delle classi di coniugio di G ciascuna delle quali ha più di un elemento, mentre con $\{C_G(x_k)\}_{k=1}^m$ abbiamo indicato i rispettivi centralizzanti.

DIMOSTRAZIONE. Poiché $\Omega = G$, ne segue che il centro di G coincide con l'insieme

$$\Omega_0 = \{\alpha \in \Omega \mid \alpha^g = \alpha \quad \forall\ g \in G\} = Z(G).$$

Quindi dalla relazione

$$|\Omega| = |\Omega_0| + \sum_{\alpha \in D} |\alpha^G|$$

si ha che

$$|G| = |Z(G)| + \sum_{k=1}^{m} |\mathrm{Cl}(x_k)|$$

dove $D = \{x_1, x_2, \cdots, x_m\}$ costituisce un sistema di rappresentanti delle classi di coniugio ciascuna delle quali contiene più di un elemento. □

Teorema C3.4. *Un p-gruppo finito ha il centro non banale.*

DIMOSTRAZIONE. Osserviamo che per un qualsiasi gruppo G, $|Z(G)| \neq 0$, in quanto $Z(G)$ contiene almeno l'elemento neutro. Sia G un p-gruppo finito, dimostriamo che $|Z(G)| > 1$. Per la Proposizione **C2.6**, considerando l'azione di G tramite coniugio su $\Omega = G$ con $\Omega_0 = Z(G)$, si ha che $|G| \equiv |Z(G)| \pmod{p}$. Inoltre, essendo G un p-gruppo abbiamo

$$p \mid |G| \implies p \mid |Z(G)|.$$

Poiché $|Z(G)| \neq 0$, ne segue $|Z(G)| \geq p$. □

Corollario C3.5. *Sia G un gruppo finito di ordine p^2 con p primo. Allora G è abeliano.*

DIMOSTRAZIONE. Se G ha ordine p^2, allora G è un p-gruppo, quindi per il Teorema **C3.4**, il centro $Z(G)$ è non banale, pertanto

$$Z(G) \leq G \implies |Z(G)| \mid |G| = p^2 \implies |Z(G)| \in \{p, p^2\}.$$

Se $|Z(G)| = p^2$, allora $G = Z(G)$ è abeliano. Altrimenti per $|Z(G)| = p$, dato che il centro $Z(G)$ è un sottogruppo normale di G, possiamo considerare il gruppo quoziente $G/Z(G)$ il cui ordine è dato da:

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

quindi $Z(G)$ e $G/Z(G)$ sono dei gruppi ciclici, in quanto il loro ordine è un numero primo. Allora

$$\exists\, a \in G : \; Z(G) = \langle a \rangle,$$
$$\exists\, b \in G \backslash Z(G) : \; G/Z(G) = \langle bZ(G) \rangle;$$

da cui segue che $G = \langle a, b \rangle$; inoltre

$$a \in Z(G) \implies ab = ba$$

perciò G è abeliano. □

C4. Transitività

In questa sezione sarà illustrata una particolare tipologia di azione di un gruppo su un insieme, l'azione transitiva.

Definizione C4.1. *Se G agisce su un insieme Ω, si dice che G è* transitivo *su Ω se esiste una sola orbita*

$$\alpha^G = \Omega \quad \textit{per ogni} \quad \alpha \in \Omega.$$

In altre parole, se dati comunque due elementi $\alpha, \beta \in \Omega$ esiste $g \in G$ tale che $\alpha^g = \beta$, allora l'azione è transitiva.

Poiché Ω è costituito dall'unione disgiunta di orbite, G è transitivo su Ω se $\alpha^G = \Omega$ per almeno un $\alpha \in \Omega$. Inoltre è ovvio che se H è un sottogruppo di G e H è transitivo su Ω, allora G è transitivo su Ω.

Lemma C4.2. *Un gruppo finito G non può essere unione insiemistica di sottogruppi* (propri) *coniugati.*

DIMOSTRAZIONE. Sia G un gruppo finito. Indicato con H un suo sottogruppo proprio, proviamo che

$$G \neq \bigcup_{g \in G} H^g.$$

La tesi è ovviamente vera se H è normale in G. Dunque dobbiamo sostanzialmente provarla quando H è un sottogruppo proprio, ma non normale.

Richiamiamo la nozione di normalizzante di un sottogruppo: Se H è un sottogruppo di G, si definisce normalizzante di H in G l'insieme

$$N_G(H) = \{g \in G \mid H^g = H\}.$$

$N_G(H)$ è un sottogruppo di G; inoltre $H \triangleleft N_G(H)$, in quanto se $g \in H$ ne segue che $H^g = H$, quindi possiamo scrivere

$$H \triangleleft N_G(H) \leq G.$$

Introduciamo ora l'insieme $\mathcal{L}$ dei laterali destri di $N_G(H)$ in G:

$$\mathcal{L} = \{N_G(H)g \mid g \in G\}$$

e poniamo

$$|G| = m, \quad |H| = h \quad e \quad |N_G(H)| = n.$$

Ne segue che

$$|\mathcal{L}| = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{m}{n}.$$

Consideriamo inoltre l'insieme $\mathcal{T}$ dei sottogruppi di G coniugati ad H:

$$\mathcal{T} = \{ H^g \mid g \in G \}$$

e proviamo che l'applicazione

$$\phi: \quad \mathcal{L} \longrightarrow \mathcal{T} \quad \text{con} \quad N_G(H)g \longmapsto H^g$$

è biiettiva. Ovviamente ϕ è ben posta e suriettiva.

Siano $N_G(H)g_1, N_G(H)g_2 \in \mathcal{L}$ due laterali tali che $H^{g_1} = H^{g_2}$. Allora

$$g_1^{-1}Hg_1 = g_2^{-1}Hg_2 \iff (g_1g_2^{-1})^{-1}Hg_1g_2^{-1} = H$$

quindi il coniugato di H rispetto $g_1g_2^{-1}$ coincide con H, pertanto

$$g_1g_2^{-1} \in N_G(H) \implies N_G(H)g_1 = N_G(H)g_2.$$

Dunque ϕ è anche iniettiva. Ne segue

$$|\mathcal{T}| = |\mathcal{L}| = \frac{m}{n}.$$

Osservando che ogni membro di $\mathcal{T}$ contiene l'elemento neutro ed ha cardinalità uguale ad $h \leq n$, risulta

$$\left| \bigcup_{g \in G} H^g \right| \leq (h-1)\frac{m}{n} + 1 \leq (n-1)\frac{m}{n} + 1 = m - \frac{m}{n} + 1 < m$$

perché $m > n$ in quanto H non è normale in G. Pertanto in ogni caso G non può essere unione insiemistica di sottogruppi propri coniugati. □

Teorema C4.3. *Sia G un gruppo finito transitivo su un insieme Ω. Allora*

(a) *Ω è finito e $|\Omega|$ divide $|G|$.*

(b) *esiste $g \in G$ tale che $\alpha^g \neq \alpha$ per ogni $\alpha \in \Omega$, cioè esiste un elemento di G che muove tutti gli elementi di Ω.*

DIMOSTRAZIONE. Procediamo per ordine partendo dal primo punto.

[a] Poiché G è transitivo su Ω si ha

$$\forall\, \alpha \in \Omega: \quad \alpha^G = \Omega$$

quindi

$$|\Omega| = |\alpha^G| = [G : G_\alpha] < \infty$$

in quanto G è un gruppo finito; inoltre per ogni $\alpha \in \Omega$, si ha che

$$|\Omega| = \frac{|G|}{|G_\alpha|} \implies |\Omega| \mid |G|.$$

[b] Per il Teorema **C2.4** si ha che

$$\forall\, \alpha \in \Omega: \quad G_\alpha \leq G.$$

Inoltre, essendo G transitivo, esiste una sola orbita, quindi per ogni $\beta \in \Omega$, G_β è un sottogruppo coniugato di G_α, cioè tutti gli stabilizzatori di G risultano tra loro coniugati. Per ogni $\alpha \in \Omega$, lo stabilizzatore G_α è un sottogruppo proprio di G, altrimenti esisterebbe un $\alpha \in \Omega$ tale che

$$G = G_\alpha = \{g \in G \mid \alpha^g = \alpha\} \implies \alpha^G = \{\alpha\} \neq \Omega.$$

Poiché G è finito, per il Lemma **C4.2**

$$\exists\, g \in G:\ g \notin \bigcup_{\beta\in\Omega} G_\beta$$

ne segue che $\beta^g \neq \beta$ per ogni $\beta \in \Omega$. □

C5. Normalità

Esaminiamo ora un esempio particolare di azione transitiva.

Esempio C5.1. *Siano G un gruppo e H un sottogruppo di G. Poniamo*

$$\Omega = \{Hx \mid x \in G\}$$

l'insieme dei laterali destri di H in G.

Possiamo ora definire un'azione di G su Ω nel seguente modo:

$$\begin{aligned} \psi: \quad \Omega \times G &\longrightarrow \Omega; \\ (Hx, g) &\longmapsto (Hx)^g = Hxg. \end{aligned}$$

Verifichiamo che si tratta effettivamente di un'azione di G su Ω.

(a) $\forall\ Hx \in \Omega:\quad (Hx)^e = Hxe = Hx.$

(b) $\forall\ g, h \in G:\quad \big((Hx)^g\big)^h = (Hxg)^h = Hxgh = (Hx)(gh) = (Hx)^{gh}.$

Ora, presi due membri qualunque Hx e Hy di Ω, è sempre possibile trovare un $g \in G$ tale che $Hx = (Hy)^g$ (basta porre $g = y^{-1}x$). *Pertanto G risulta essere transitivo su Ω, cioè*

$$(Hx)^G = \Omega.$$

Lo stabilizzatore di Hx è $G_{Hx} = \{g \in G \mid (Hx)^g = Hx\}$, quindi, se g è un elemento dello stabilizzatore di Hx, deve valere

$$(Hx)^g = Hx \iff Hxg = Hx \iff Hxgx^{-1} = H.$$

Dunque $xgx^{-1} \in H$ e $g \in H^x$. Ne segue che

$$G_{Hx} = H^x.$$

Per il risultato ottenuto, il nucleo di tale azione è

$$K = \bigcap_{Hx\in\Omega} G_{Hx} = \bigcap_{x\in G} H^x$$

che risulta anche un sottogruppo normale di G.

Banalmente K è un sottogruppo normale di G contenuto in H. Sia ora T un arbitrario sottogruppo normale di G tale che $T \triangleleft H < G$. Proviamo che T è un sottogruppo di K. Notiamo che vale

$$T \triangleleft G \quad \Longrightarrow \quad \forall\, x \in G: \quad T^x = T.$$

Essendo $T \subset H$, si ha che $T^x \subset H^x$ per ogni $x \in G$ e dunque

$$T = \bigcap_{x \in G} T^x \subset \bigcap_{x \in G} H^x = K.$$

Ne segue che K è il più grande sottogruppo normale di G contenuto in H.

Teorema C5.2 (Poincarè). *Se un gruppo ha un sottogruppo di indice finito, allora necessariamente ha un sottogruppo normale di indice finito.*

DIMOSTRAZIONE. Siano G un gruppo, $H \leq G$ tale che $[G : H] = n$. Preso $\Omega = \{Hx | x \in G\}$, consideriamo l'azione di G su Ω definita nell'Esempio **C5.1**:

$$(Hx, g) \longmapsto (Hx)^g = Hxg$$

avente nucleo

$$K = \bigcap_{x \in G} H^x$$

che come abbiamo visto, è il più grande sottogruppo normale di G contenuto in H; quindi per avere la tesi, basta provare che $[G : K] < \infty$.

Se G è finito, evidentemente la tesi è banale in quanto

$$K \triangleleft H < G \quad \Longrightarrow \quad [G : K] = \frac{|G|}{|K|} < \infty.$$

Supponendo G infinito, proviamo che $|W|$ è finito, dove $W = \{Kg \mid g \in G\}$.

Nella dimostrazione del Lemma **C4.2**, abbiamo visto che esiste una biiezione tra l'insieme dei laterali destri di $N_G(H)$ in G e l'insieme dei sottogruppi di G coniugati ad H, quindi

$$|\{H^x \mid x \in G\}| = [G : N_G(H)] = m \leq n$$

in quanto $H \triangleleft N_G(H) < G$ e $[G : N_G(H)] \leq [G : H] = n$. Dunque esistono m elementi $x_1, x_2, \cdots, x_m \in G$ tali che

$$K = \bigcap_{\lambda=1}^{m} H^{x_\lambda}.$$

Ora, ogni laterale di K in G è $Kg = \left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g$, quindi

$$W = \left\{Kg \mid g \in G\right\} = \left\{\left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g \,\middle|\, g \in G\right\}$$

ma

$$\left(\bigcap_{\lambda=1}^{m} H^{x_\lambda}\right)g = \bigcap_{\lambda=1}^{m} \left(H^{x_\lambda}g\right)$$

pertanto ogni laterale di K in G è una intersezione dei laterali

$$H^{x_1}g, H^{x_2}g, \cdots, H^{x_m}g.$$

Posto

$$\mathfrak{W} = \left\{ \bigcap_{\lambda=1}^{m} H^{x_\lambda}g_\lambda \mid g_\lambda \in G \right\}$$

si ha che $W \subset \mathfrak{W}$, inoltre poiché due sottogruppi coniugati hanno lo stesso indice, risulta

$$[G : H^{x_\lambda}] = [G : H] = n.$$

Siccome per ogni H^{x_λ} vi sono n laterali, si ha che la cardinalità di $\mathfrak{W}$ è minore o uguale a n^m. Pertanto $|W| \leq n^m \implies [G : K] \leq n^m$. □

Proposizione C5.3. *Siano G un gruppo finito e p il più piccolo divisore primo dell'ordine di G. Sia H un sottogruppo di G di indice p. Allora H è un sottogruppo normale di G. In particolare*

(a) *un sottogruppo di indice 2 in un gruppo finito è normale.*
(b) *un sottogruppo di indice p in un p-gruppo finito è normale.*

DIMOSTRAZIONE. È facile vedere che l'enunciato principale implica immediatamente i due punti [**a**] e
textbf[b].

Siano G un gruppo finito, H un sottogruppo di G tale che $[G : H] = p$, dove p è il più piccolo divisore primo dell'ordine di G.

Poniamo $\Omega := \{Hx \mid x \in G\}$ e consideriamo l'azione di G su Ω così definita

$$(Hx, g) \longmapsto (Hx)^g = Hxg.$$

Tale azione corrisponde ad un omomorfismo ϑ tra G ed S_Ω, il gruppo simmetrico di ordine $p!$ (perché S_Ω è il gruppo delle permutazioni di Ω). Il nucleo dell'omomorfismo ϑ (anche il nucleo dell'azione di G su Ω) dato da

$$K = \bigcap_{x \in G} H^x$$

risulta un sottogruppo normale di G, per cui G/K è isomorfo ad un sottogruppo di S_Ω. Per il teorema di Lagrange, si ha che

$$|G/K| \;\Big|\; |S_\Omega| = p!.$$

Inoltre G/K è certamente non banale, in quanto

$$K < H: \quad |G/K| \geq [G:H] = p.$$

Sia ora q un arbitrario numero primo che divide $|G/K|$, allora risulta che

$$q \mid p! \quad \Longrightarrow \quad q \mid 1 \cdot 2 \cdots (p-1) \cdot p \quad \Longrightarrow \quad q \leq p.$$

Inoltre vale

$$q \,\big|\, |G/K| \quad \Longrightarrow \quad q \big|\, |G| \quad \Longrightarrow \quad q \geq p$$

perché p è il più piccolo divisore primo di $|G|$. Allora $p = q$. Ne segue che G/K è un p-gruppo finito, in quanto p è l'unico divisore primo di $|G/K|$ e il suo ordine è una potenza di p.

Supponendo che $|G/K| = p^n$ risulta

$$p^n \mid p! \quad \Longrightarrow \quad n = 1$$

perché G/K è non banale. Allora $|G/K| = p = [G:H]$.

Ricordando $K \leq H \leq G$ si ha che

$$p = [G:K] = [G:H] \cdot [H:K] = p[H:K] \implies [H:K] = 1$$

pertanto

$$[H:K] = 1 \quad \text{e} \quad K \leq H \quad \Longrightarrow \quad H = K.$$

Dunque H è un sottogruppo normale di G. □