Appunti Algebra 1

APPUNTI DEL CORSO DI ALGEBRA 1 TENUTO
DALLA PROF. DEL CORSO E DAL PROF. LOMBARDO

Diego Monaco
d.monaco2@studenti.unipi.it

Anno Accademico 2022-23

Indice

§1 Automorfismi

§1.1 Automorfismi di G

Dato un gruppo G possiamo definire l'insieme degli automorfismi di G come segue:

$$\mathrm{Aut}(G) = \{\varphi : G \longrightarrow G | \, \varphi \, \text{isomorfismo}\}$$

si verifica facilmente che $(\mathrm{Aut}(G), \circ)$ è un gruppo, e in particolare $\mathrm{Aut}(G) \leqslant S(G)$, ovvero il gruppo delle permutazioni di G. Si osserva che $id \in \mathrm{Aut}(G)$, $\varphi \in \mathrm{Aut}(G) \implies \varphi^{-1} \in \mathrm{Aut}(G)$ e $\varphi, \psi \in \mathrm{Aut}(G) \implies \varphi \circ \psi \in \mathrm{Aut}(G)$.

Esempio 1.1 (Esempi di automorfismi)
Esempi di insiemi di automorfismi:

- $\mathrm{Aut}(\mathbb{Z}) = \{\pm id\}$.
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$.
- $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$.
- $\mathrm{Aut}(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}}) \cong GL_n(\mathbb{F}_p)$

§1.2 Automorfismi interni

Definizione 1.2. Dato un gruppo G possiamo definire l'omomorfismo di **coniugio**:

$$\varphi_g : G \longrightarrow G : x \longmapsto gxg^{-1}$$

dove l'elemento gxg^{-1} si dice **coniugato** di g.

Proposizione 1.3
Valgono i seguenti fatti:

(1) $\varphi_g \in \mathrm{Aut}(G)$, $\forall g \in G$.

(2) $\{\varphi_g | g \in G\} = \mathrm{Inn}(G) \trianglelefteqslant \mathrm{Aut}(G)$.[a]

[a] $\mathrm{Inn}(G)$ si definisce **gruppo degli automorfismi interni**.

Dimostrazione. Proviamo le due affermazioni:

(1) Per verificare che φ_g è un automorfismo devo verificare che φ_g è ben definita, ma ciò segue dalla chiusura di g per l'operazione, verifichiamo allora che sia un omomorfismo:

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y) \qquad \forall x, y \in G$$

ci resta da verificare che sia una bigezione. Partiamo dalla surgettività, vogliamo verificare che $\forall y \in G$, $\exists g \in G$:

$$\varphi_g(x) = y$$

in tal caso basta prendere $x = gyg^{-1} \in G$. Per l'iniettività si osserva:

$$\ker \varphi_g = \{x \in G | \varphi_g(x) = e\} = \{x \in G | gxg^{-1} = e \iff x = e\} = \{e\}$$

pertanto φ_g è iniettivo.

(2) Verifichiamo che $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$, mostriamo prima che $\text{Inn}(G)$ è un sottogruppo di $\text{Aut}(G)$, infatti: $id = \varphi_e \in \text{Inn}(G)$, $\forall g_1, g_2 \in G$ vale che $\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2} \in \text{Inn}(G)$, infatti:

$$\varphi_{g_1} \circ \varphi_{g_2}(x) = \varphi_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = \varphi_{g_1 g_2}(x)$$

infine, $(\varphi_g)^{-1} = \varphi_{g^{-1}} \in \text{Inn}(G)$:

$$(\varphi_g)^{-1} \circ \varphi_g(x) = (\varphi_g)^{-1}(gxg^{-1}) = x \iff (\varphi_g)^{-1} = \varphi_{g^{-1}}$$

e analogamente per l'inversa a destra. Per verificare la normalità bisogna mostrare che:

$$f \circ \text{Inn}(G) \circ f^{-1} \subseteq \text{Inn}(G) \qquad \forall f \in \text{Aut}(G)$$

ovvero:

$$f \circ \varphi_g \circ f^{-1} \in \text{Inn}(G) \qquad \forall f \in \text{Aut}(G), \forall \varphi_g \in \text{Inn}(G)$$

si osserva che $f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)} \in \text{Inn}(G)$, infatti:

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

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

□

Osservazione 1.4 — Se G è abeliano, allora $\text{Inn}(G) = \{id\}$, infatti:

$$gxg^{-1} = gg^{-1}x = x \qquad \forall x \in G, \forall g \in G$$

Proposizione 1.5
Dato un gruppo G si ha:

$$\text{Inn}(G) \cong {}^{G}\!/_{Z(G)}$$

Dimostrazione. Per dimostrare il teorema ci basta trovare un omomorfismo surgettivo da G in $\text{Inn}(G)$ e poi sfruttare il Primo Teorema di Omomorfismo. Sia:

$$\phi : G \longrightarrow \text{Inn}(G) : g \longmapsto \varphi_g$$

tale applicazione è chiaramente ben definita, ed è surgettiva per come abbiamo definito $\text{Inn}(G)$. Verifichiamo che è un omomorfismo:

$$\phi(g_1 g_2) = \varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2} = \phi(g_1) \circ \phi(g_2) \qquad \forall g \in G$$

dove la penultima uguaglianza è vera per quanto visto nella dimostrazione del (2) della proposizione precedente. A questo punto, per il primo teorema di omomorfismo si ha che:

$$\begin{tikzcd} G \arrow[r, two heads, "\phi"] \arrow[d, two heads, "\pi_{\ker\phi}"'] & \mathrm{Inn}(G) \\ G/\ker\phi \arrow[ur, "\sim"] & \end{tikzcd}$$

dunque:

$$\frac{G}{\ker\phi} \cong \mathrm{Inn}(G)$$

non ci resta che osservare:

$$\ker\phi = \{g \in G | \phi(g) = \varphi_g = id\} = \{g \in G | gxg^{-1} = x, \forall x \in G\} = \\ = \{g \in G | gx = xg, \forall x \in G\} = Z(G)$$

□

Osservazione 1.6 — L'isomorfismo trovato è del tipo $gZ(G) \longmapsto \varphi_g$, ricordiamo che è ben definito per il Primo Teorema di Omomorfismo.

Osservazione 1.7 — Si ricorda che se $G/Z(G)$ è ciclico, allora G è abeliano (e quindi $G/Z(G)$ è banale), infatti, sia:

$$G/Z(g) = \langle gZ(G) \rangle$$

Presi $g_1, g_2 \in G$, si ha che $g_1Z(G) = g^{k_1}Z(G)$ e $g_2Z(G) = g^{k_2}Z(G)$, da cui:

$$g^{-k_1}g_1Z(G) = Z(G) \iff g^{-k_1}g_1 \in Z(G)$$

ovvero $\exists z_1 \in Z(G) : g_1 = g^{k_1}z_1$ e analogamente $g_2 = g^{k_2}z_2$, da cui:

$$g_1g_2 = g^{k_1}z_1g^{k_2}z_2 = g^{k_1}g^{k_2}z_1z_2 = g^{k_1+k_2}z_1z_2$$

e contemporaneamente:

$$g_2g_1 = g^{k_2}z_2g^{k_1}z_1 = g^{k_2}g^{k_1}z_2z_1 = g^{k_2+k_1}z_2z_1 = g^{k_1+k_2}z_1z_2$$

dove nell'ultimo passaggio si è sfruttato il fatto che $k_1, k_2 \in \mathbb{Z}$ e $z_1, z_2 \in Z(G)$. Da ciò segue che G è abeliano.

Osservazione 1.8 — Dunque $\mathrm{Inn}(G)$ ciclico $\implies G/Z(G)$ ciclico $\implies G$ abeliano da cui:

$$\mathrm{Inn}(G) \cong G/Z(G) \cong \{e\}$$

Osservazione 1.9 — $N \trianglelefteq G \iff \forall \varphi_g \in \mathrm{Inn}(G)$ si ha $\varphi_g(N) = N$ (o anche $\varphi_g(N) \subseteq N$). Equivalentemente, i sottogruppi normali di G sono i sottogruppi **invarianti** per automorfismi interni (ovvero sono tali che $gNg^{-1} = N$, $\forall g \in G$). Se

$N \trianglelefteq G$, si può considerare:

$$\mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(N) : \varphi_g \longmapsto \varphi_{g|N}$$

con $\varphi_{g|N} : N \longrightarrow N$ che è un automorfismo, infatti rimane iniettivo, la surgettività segue dal fatto che $\varphi_g(N) = N$, e infine, essendo φ_g un omomorfismo su tutti gli elementi di G, lo sarà in particolare anche su tutti gli elementi di N. Dunque quando si ha un sottogruppo normale, ogni automorfismo interno si restringe a un automorfismo di N.

Abbiamo visto che i sottogruppi normali sono invarianti per automorfismi interni, possiamo generalizzare quest'idea e considerare i sottogruppi invarianti per automorfismi:

Definizione 1.10. Dato un sottogruppo $H \leqslant G$, esso si dice **caratteristico** se è invariante per automorfismi:

$$f(H) = H \qquad \forall f \in \mathrm{Aut}(G)$$

Anche in questo caso basta verificare che $f(H) \subseteq H$, $\forall f \in \mathrm{Aut}(G)$, perché si ha anche che:

$$f^{-1}(H) \subseteq H$$

da cui si ottiene:

$$f(f^{-1}(H)) \subseteq f(H)$$

Osservazione 1.11 — Si osserva che se H è caratteristico in G, allora è invariante per tutti gli automorfismi di G (e quindi in particolare quelli interni), dunque se H è caratteristico in G, allora è anche normale. Il viceversa è falso.

Osservazione 1.12 — Se H è caratteristico in G (dunque normale), si può scrivere un'applicazione:

$$\mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(H) : f \longmapsto f_{|H}$$

dove $f_{|H}$ è un automorfismo di H.

Osservazione 1.13 — Si osserva che se H è l'unico sottogruppo di G di un certo ordine, allora H è caratteristico in G (segue immediatamente dal fatto che gli automorfismi preservano gli ordini degli elementi).

Esercizio 1.14. Il centro di un gruppo, $Z(G)$ è un sottogruppo caratteristico.

Soluzione. Per dimostrare che $Z(G)$ è caratteristico è sufficiente far vedere che:

$$f(Z(G)) \subseteq Z(G) \qquad \forall f \in \mathrm{Aut}(G)$$

ovvero:

$$f(z) \in Z(G) \qquad \forall f \in \mathrm{Aut}(G), \forall z \in Z(G)$$

dunque bisogna verificare che:

$$gf(z) = f(z)g \qquad \forall g \in G$$

poiché f è un automorfismo, allora $\exists h \in G : f(h) = g$, dunque:

$$gf(z) = f(h)f(z) = f(hz) = f(zh) = f(z)f(h) = f(z)g \qquad \forall g \in G$$

$\square$

Esempio 1.15

Sia $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0},\overline{0}),(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{1})\}$, G ha ordine 4 ed ha tre sottogruppi ciclici di ordine 2:

$$H_1 = \langle(\overline{1},\overline{0})\rangle \qquad H_2 = \langle(\overline{0},\overline{1})\rangle \qquad H_3 = \langle(\overline{1},\overline{1})\rangle$$

ed essendo G abeliano si ha $H_1, H_2, H_3 \trianglelefteq G$ (e quindi i sottogruppi sono invarianti per automorfismi interni). Tuttavia nessuno dei sottogruppi è caratteristico, infatti possiamo prendere un automorfismo non banale (e quindi non uno interno) e vedere come i sottogruppi di questo tipo non siano invarianti:

$$f = \begin{cases} (\overline{1},\overline{0}) \longmapsto (\overline{1},\overline{1}) \\ (\overline{0},\overline{1}) \longmapsto (\overline{0},\overline{1}) \end{cases}$$

la definizione della mappa data tuttavia non è completa, perché abbiamo stabilito solo dove vengono mandati i generatori, dobbiamo definire cosa faccia un elemento generico:

$$f((\overline{a},\overline{b})) = af((\overline{1},\overline{0})) + bf((\overline{0},\overline{1})) = (\overline{a},\overline{a}) + (\overline{0},\overline{b}) = (\overline{a},\overline{a+b})$$

a questo punto abbiamo definito completamente l'applicazione (rimarrebbe da verificare che f sia un omomorfismo), e si verifica facilmente che $f(H_1) = H_3$ quindi $H_1 \trianglelefteq G$, ma non caratteristico.

A questo punto è facile verificare che:

$$\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

infatti, ogni automorfismo del gruppo si ottiene fissando l'elemento neutro $(\overline{0},\overline{0}) \longmapsto (\overline{0},\overline{0})$, quindi il numero possibile di bigezioni è al più 3!, occorre verificare che tutte e 6 le funzioni sono omomorfismi. Dimostriamo invece che:

$$\boxed{\mathrm{Aut}(S_3) \cong S_3}$$

Per farlo, poiché S_3 non è abeliano, possiamo osservare che:

$$\mathrm{Inn}(S_3) \cong {}^{S_3}\!/_{Z(S_3)} \cong S_3$$

in quanto l'unico elemento che commuta con tutti gli altri in S_3 è l'identità, quindi $Z(S_3) = \{id\} \cong \{e\}$. Per quanto detto si ha $\mathrm{Inn}(S_3) \trianglelefteq \mathrm{Aut}(S_3)$ e quindi $\mathrm{Aut}(S_3)$ contiene una copia isomorfa di S_3 come sottogruppo normale, pertanto, se verifichiamo che $|\mathrm{Aut}(S_3)| \leq 6$ abbiamo concluso. Sia $f \in \mathrm{Aut}(S_3)$, f può al più scambiare i 3 elementi di ordine 2, d'altra parte, fissate le immagini di τ_1, τ_2, τ_3[1], i due 3-ciclci[2] sono completamente determinati, ciò significa che si hanno al più 3! automorfismi, dunque:

$$\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3 \implies \mathrm{Aut}(S_3) \cong S_3$$

[1]Con τ_i si intendono le trasposizioni che lasciano fisso l'elemento i.
[2]Come si vedrà $S_3 = \langle\tau_1, \tau_2, \tau_3\rangle$

§1.3 Azione di un gruppo su un insieme

Definizione 1.16. Sia G un gruppo e X un insieme, un'**azione** di G su X è un omomorfismo:

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g (= \varphi(g))$$

dove $\varphi_g : X \longrightarrow X : x \longmapsto \varphi_g(x)$, con φ_g bigettiva, $\forall g \in G$.

Esempio 1.17

Sia $X = G$, quindi $\varphi : G \longrightarrow S(G) : g \longmapsto \varphi_g$, con φ_g coniugio, φ è un'azione. Come si è visto nell'(1) della Proposizione 1.3 φ_g è un automorfismo di G (e quindi una bigezione), e φ è un omomorfismo. In questo caso si ha che:

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

Esempio 1.18

Sia V un K-spazio vettoriale, sia:

$$\varphi : K^* \longrightarrow S(V) : \lambda \longmapsto \varphi_\lambda$$

con $\varphi_\lambda : V \longrightarrow V : \underline{v} \longmapsto \lambda\underline{v}$, φ è un'azione di K^* su V.

Sia $\varphi : G \longrightarrow S(X)$ un'azione, φ definisce una relazione di equivalenza su X:

$$x \sim y \iff \exists g \in G : \varphi_g(x) = y$$

ovvero due elementi sono in relazione se esiste un'applicazione $\varphi_g \in S(X)$, per cui un elemento è l'immagine dell'altro mediante tale applicazione. La relazione è appunto di equivalenza, infatti: $x \sim x$, per $g = e$ si ha (essendo φ un omomorfismo) $\varphi_e(x) = id(x) = x$, $x \sim y \implies y \sim x$:

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

infine $x \sim y$, $y \sim z \implies x \sim z$, infatti si avrebbe: $\varphi_g(x) = y$, $\varphi_h(y) = z$ da cui:

$$z = \varphi_h(\varphi_g(x)) = \varphi_{hg}(x) \implies x \sim z$$

Definizione 1.19. Data la relazione di equivalenza $\sim$ si definiscono **orbite** le classi di equivalenza di X rispetto alla relazione $\sim$:

$$\mathrm{Orb}(x) = \{\varphi_g(x) | g \in G\} (\subseteq X)$$

Da cui:

$$X = \dot{\bigcup_{x \in \mathcal{R}}} \mathrm{Orb}(x)$$

Con $\mathcal{R}$ insieme di rappresentanti. Un'orbita è quindi l'insieme di tutte le immagini di un elemento in un insieme, mediante tutte le possibili applicazioni (permutazioni) dell'insieme $\varphi(G)$.

Definizione 1.20. Per ogni $x \in X$ si dice **stabilizzatore** di x:

$$\mathrm{St}(x) = \{g \in G | \varphi_g(x) = x\}$$

Cioè lo stabilizzatore è l'insieme degli elementi di G, che danno origine mediante φ alle applicazioni $\varphi_g \in S(X)$, che lasciano fisso un determinato elemento.

Esempio 1.21

Se $X = \mathbb{R}^2$ e G è il gruppo di traslazioni di vettore $\underline{v} = (0, l)$, allora:

$$\varphi : G \longrightarrow S(X) : \tau_{(0,l)} \longmapsto \tau_{(0,l)}$$

con:

$$\text{Orb}(x, y) = \{(x, y + l) | l \in \mathbb{R}\} \quad \text{e} \quad \text{St}(x, y) = \{\tau_{(0,l)} | (x, y + l) = (x, y)\} = \{id\}$$

Esempio 1.22

Se $X = \mathbb{R}^2$ e G è il gruppo delle rotazioni di centro O, allora:

$$\varphi : G \longrightarrow S(\mathbb{R}^2) : r_\theta \longmapsto r_\theta$$

con:

$$\text{St}(x, y) = \begin{cases} \{id\} & \text{se } (x, y) \neq (0, 0) \\ G & \text{se } (x, y) = (0, 0) \end{cases}$$

e, detta ω la circonferenza di centro O raggio $\sqrt{x^2 + y^2}$:

$$\text{Orb}(x, y) = \{(x', y') \in \mathbb{R}^2 | (x', y') \in \omega\}$$

Proposizione 1.23 ($\text{St}(x) \leqslant G$)

Dato un gruppo G e un'azione $\varphi : G \longrightarrow S(X)$, si ha che $\text{St}(x) \leqslant G$.[a]

[a] In generale lo stabilizzatore non è un sottogruppo normale.

Dimostrazione. Si osserva che $e \in \text{St}(x)$, in quanto $\varphi_e(x) = id(x) = x$, inoltre, presi $g, h \in \text{St}(x)$, ovvero $\varphi_g(x) = \varphi_h(x) = x$, allora:

$$\varphi(gh) = \varphi_{gh}(x) = \varphi_g \circ \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g(x) = x \implies gh \in \text{St}(x)$$

dove si ha che $\varphi_{gh}(x) = \varphi_g \circ \varphi_h(x)$ in quanto φ è un omomorfismo. Infine, preso $g \in \text{St}(x)$, si ha $g^{-1} \in \text{St}(x)$, infatti φ_g è bigettiva e quindi ammette inversa:

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

con $(\varphi_g)^{-1}(x) = (\varphi(g))^{-1}(x) = (\varphi(g^{-1}))(x) = \varphi_{g^{-1}}(x)$ e per quanto detto:

$$\varphi_{g^{-1}}(x) = x \implies g^{-1} \in \text{St}(x)$$

□

Osservazione 1.24 — Sia $x \in X$ e $g, h \in G$, allora:

$$\varphi_g(x) = \varphi_h(x) \iff \varphi_{h^{-1}}(\varphi_g(x)) = x$$

e per le proprietà di omomorfismo dell'azione φ, si ha:

$$\varphi_{h^{-1}}(\varphi_g(x)) = x \iff \varphi_{h^{-1}g}(x) = x \iff h^{-1}g \in \text{St}(x)$$

ovvero $g\,\mathrm{St}(x) = h\,\mathrm{St}(x)$, in quanto $\mathrm{St}(x) \leqslant G$ e la condizione ottenuta è esattamente quella dell'equivalenza modulo $\mathrm{St}(x)$, quindi:

$$\mathrm{Orb}(x) \longleftrightarrow \text{classi laterali di } \mathrm{St}(x) \text{ in } G$$

cioè due elementi danno la stessa immagine se e solo se stanno nella stessa classe laterale modulo $\mathrm{St}(x)$, e la corrispondenza biunivoca tra orbita e classi laterali è data da:

$$g\,\mathrm{St}(x) \longmapsto \varphi_g(x) \qquad \text{e} \qquad h\,\mathrm{St}(x) \longmapsto \varphi_h(x)$$

che è ben definita per quanto detto all'inizio, è iniettiva:

$$\varphi_g(x) = \varphi_h(x) \iff g\,\mathrm{St}(x) = h\,\mathrm{St}(x)$$

(quindi due elementi di un orbita sono uguali se e solo se lo sono le classi laterali dei rispettivi elementi che generano le applicazioni sono uguali modulo $\mathrm{St}(x)$) e surgettiva:

$$\forall y \in \mathrm{Orb}(x), y = \varphi_g(x) \implies g\,\mathrm{St}(x) \longmapsto y$$

Per quanto detto si ha:

$$|G| = |\mathrm{St}(x)|[G : \mathrm{St}(x)]$$

ma $[G : \mathrm{St}(x)]$ è il numero di classi laterali di $\mathrm{St}(x)$ in G, che è proprio uguale a $|\mathrm{Orb}(x)|$ pertanto vale la seguente:

Proposizione 1.25

Sia G un gruppo finito e X un insieme, allora:

$$|G| = |\mathrm{Orb}(x)||\mathrm{St}(x)| \qquad \forall x \in X$$

Osservazione 1.26 — Si osserva che essendo $\mathrm{St}(x) \leqslant G$, allora è ovvio (per Lagrange) che $|\mathrm{St}(x)| \mid |G|$, tuttavia, per la proposizione precedente, si ha che: $|\mathrm{Orb}(x)| \mid |G|$ con $\mathrm{Orb}(x) \subseteq X$.

Ricordando che:

$$X = \bigsqcup_{x \in \mathcal{R}} \mathrm{Orb}(x)$$

se $|X| < +\infty$ si ha:

$$\boxed{|X| = \sum_{x \in \mathcal{R}} |\mathrm{Orb}(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|\mathrm{St}(x)|}}$$

§1.4 Azione di coniugio

Definizione 1.27. Si parla di **azione di coniugio**, quando si ha un'azione di G su G stesso:

$$\varphi : G \longrightarrow \text{Inn}(G)(\trianglelefteq S(G)) : g \longrightarrow \varphi_g$$

Abbiamo già osservato che è un'azione (ovvero che φ è un omomorfismo). In questo caso:

$$\text{Orb}(x) = \{\varphi_g(x) | g \in G\} = \{gxg^{-1} | g \in G\} = C_x$$

dove C_x prende il nome di **classe di coniugio** di x. Mentre:

$$\text{St}(x) = \{g \in G | \varphi_g(x) = gxg^{-1} = x\} = Z_G(x)$$

dove $Z_G(x)$ si dice **centralizzatore** di x. Per quanto detto in precedenza si ha:

$$|G| = |C_x||Z_G(x)|$$

In particolare $|C_x| \mid |G|$ e :

$$|X| = \sum_{x \in \mathcal{R}} |C_x| = \sum_{x \in \mathcal{R}} \frac{|G|}{|Z_G(x)|}$$

Osservazione 1.28 — C_x è un sottoinsieme, non un sottogruppo di G, poiché non c'è mai l'identità.

Osservazione 1.29 — Osserviamo che $Z_G(x) = G \iff x \in Z(G)$, infatti la per un elemento del centro si ha che $\forall g \in G$ l'elemento commuta, e dunque il suo centralizzatore è tutto il gruppo.

Osservazione 1.30 — Per un'azione di coniugio ha che $x \in Z(G)$ se e solo se $\text{Orb}(x) = \{x\}$ (ovvero $\varphi_g(x) = x$, $\forall g \in G$).

$$|G| = \sum_{x \in Z(G)} \frac{|G|}{|Z_G(x)|} + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

ma, per quanto detto, se $x \in Z(G)$, allora $\dfrac{|G|}{|Z_G(x)|} = |C_x| = \{x\}$, segue dunque la relazione:

$$\boxed{|G| = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}}$$

che prende il nome di **formula delle classi** (di coniugio).

§1.5 Applicazioni ai p-gruppi

Definizione 1.31. Si definisce **p-gruppo** un gruppo di ordine p^n, con p primo e $n \geq 1$.

Se G è un p-gruppo la formula delle classi diventa:

$$p^n = |G| = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

con $|Z(G)| = p^z$, $0 \leq z \leq n$, facciamo due osservazioni fondamentali:

(1) Il centro di un p-gruppo non è mai banale, infatti, se osserviamo la formula delle classi, si ha:

$$p^n = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \implies |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \equiv 0 \pmod p$$

con $\dfrac{|G|}{|Z_G(x)|} > 1$, poiché se un elemento sta nel centro tutti gli addendi sono 1 per quanto detto, viceversa deve essere che $\dfrac{|G|}{|Z_G(x)|} = p^k x$, $k > 0$, poiché G è un p-gruppo, dunque:

$$|Z(G)| \equiv 0 \pmod p \implies |Z(G)| \geq 2$$

e quindi il centro di un p-gruppo non è mai banale.

(2) Un gruppo di ordine p^2 è abeliano, infatti, si ha:

$$|G| = p^2 \implies |Z(G)| = \begin{cases} 1 & \text{non può accadere per (1)} \\ p & \text{no perché allora } G/Z(G) \text{ ciclico, ma } G \text{ non è abeliano} \\ p^2 & \end{cases}$$

dunque l'unica possibilità è che $Z(G) = G \iff G$ abeliano.

§1.6 Teorema di Cauchy

Teorema 1.32 (Teorema di Cauchy)
Dato un gruppo G e un primo p, se $p \mid |G|$, allora $\exists x \in G : \operatorname{ord}_G(x) = p$. [a]

[a] Si considera già noto il teorema per gruppi abeliani.

Dimostrazione. Sia $|G| = pn$, procediamo per induzione su n, nel caso $n = 1$ il teorema è ovvio. Supponiamo vera la tesi per i gruppi di ordine pm, con $1 \leq m < n$ e proviamola per n. Distinguiamo due casi:

- Se esiste $H \lneq G$ con $p \mid H$, ovvero $|H| = pm \implies$ vale il teorema di Cauchy per ipotesi induttiva (essendo $m < n$), quindi $\exists x \in H : \operatorname{ord}_H(x) = p$, ma essendo $H \subset G \implies x \in G$ e quindi la tesi è vera.

- Se $\forall H \lneq G$ si ha $p \nmid |H|$, allora si può applicare a G la formula delle classi:

$$pn = |G| = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

ricordando il centralizzatore di x è uno stabilizzatore (e quindi un sottogruppo di G), si ha $p \nmid |Z_G(x)|$, e quindi:

$$p \,\Bigg|\, \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

da cui segue che $p \mid |Z(G)| = |G| - \sum p l_x$, per quanto premesso ($\forall H \lneq G$ si ha $p \nmid |H|$), ed essendo $Z(G) \leqslant G$, l'unica possibilità è che $Z(G) = G$ e vale il teorema poiché è già stato dimostrato per il caso in cui G è abeliano.

□

§1.7 Azione di coniugio su un sottogruppo

Sia $X = \{H \leqslant G\}$ e $\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g(X)$, con $\varphi_g : X \longrightarrow X : H \longmapsto gHg^{-1}$. Si verifica facilmente che φ è un omomorfismo, per verificare l'iniettività si osserva che:

$$\varphi_g(H) = \varphi_g(K) \iff gHg^{-1} = gKg^{-1} \iff H = K$$

mentre per la surgettività si ha che $\forall H \in X, \exists L \in X$:

$$\varphi_g(L) = H \iff gLg^{-1} = H \implies L = g^{-1}Hg$$

inoltre si ha anche:

$$\mathrm{Orb}(H) = \{\varphi_g(H) | g \in G\} = \{gHg^{-1} | g \in G\} \quad \mathrm{St}(H) = \{g \in G | \varphi_g(H) = H\} = N_G(H)$$

dove $\mathrm{Orb}(H)$ è l'insieme dei coniugati di H, mentre $\mathrm{St}(H) = N_G(H)$ prende il nome di **normalizzatore** di H.

Osservazione 1.33 — Si osserva che $N \trianglelefteq G$ se e solo se $\mathrm{Orb}(H) = \{H\} \iff N_G(H) = G$, ovvero se H è sempre chiuso per coniugio in G.

Per quanto affermato nella Proposizione 1.25 si ha:

$$|G| = |\mathrm{Orb}(H)||N_G(H)| \implies |\mathrm{Orb}(H)| = \frac{|G|}{|N_G(H)|}$$

Osservazione 1.34 — Quindi in generale, dato $H \leqslant G$ si ha che $\#\{gH\} = [G : H]$ e $\#\{gHg^{-1}\} = [G : N_G(H)]$.

Osservazione 1.35 (Sulla definizione di sottogruppo normale) — I sottogruppi normali possono essere ridefiniti nella maniera seguente, $H \trianglelefteq G$ se e solo se:

$$H = \dot{\bigcup_{h \in H}} C_h$$

cioè un sottogruppo è normale se e solo se è l'unione delle classi di coniugio dei suoi elementi. Infatti:

$$H \trianglelefteq G \iff ghg^{-1} \in H \qquad \forall h \in H, \forall g \in G$$

che equivale a:

$$C_h = \{ghg^{-1} | h \in H\} \subseteq H \quad \forall h \in H \implies \dot{\bigcup_{h \in H}} C_h \subseteq H$$

d'altra parte se H è normale è chiuso per coniugio, ovvero il coniugio di ogni suo elemento è ancora in H e in particolare ciò significa che:

$$H \subseteq \dot{\bigcup_{h \in H}} C_h$$

§1.8 Teorema di Cayley

Teorema 1.36

Ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni. In particolare, se $|G| = n$, allora G è isomorfo a un sottogruppo di S_n.

Dimostrazione. Definiamo la mappa:

$$\lambda : G \longrightarrow S(G) : g \longmapsto \varphi_g$$

con $\varphi_g : G \longrightarrow G : g \longmapsto gx$, l'applicazione λ prende il nome di **rappresentazione regolare a sinistra** di G, si vuole dimostrare che λ è un omomorfismo iniettivo. Osserviamo innanzitutto che λ è ben definita, cioè $\varphi_g \in S(G)$, infatti φ_g è iniettiva (segue dalle leggi di cancellazione) e surgettiva, perché $\forall y \in G$, $\exists g^{-1}y \in G : \varphi_g(g^{-1}y) = y$. Verifichiamo che λ è un omomorfismo:

$$\lambda(g_1g_2) = \varphi_{g_1g_2}$$

con $\varphi_{g_1g_2}(x) = \varphi_{g_1} \circ \varphi_{g_2}(x)$, $\forall x \in G$, e quindi:

$$\lambda(g_1g_2) = \lambda(g_1)\lambda(g_2) \qquad \forall g_1, g_2 \in G$$

infine, per l'iniettività si ha che:

$$\ker \lambda = \{g \in G | \lambda(g) = \varphi_g = id = \varphi_e\} = \{e\}$$

□

Osservazione 1.37 — In generale, dato $G = \{g_1 = e, g_2, \ldots, g_n\}$ e $\lambda : G \longrightarrow S(G) \cong S_n$, si ha che:

$$g_1 = e \longmapsto \varphi_{g_1}$$