

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	4
1.1	Automorfismi di G	4
1.2	Automorfismi interni	4
1.3	Azione di un gruppo su un insieme	9
1.4	Azione di coniugio	13
1.5	Applicazioni ai p -gruppi	14
1.6	Teorema di Cauchy	15
1.7	Azione di coniugio su un sottogruppo	16
1.8	Teorema di Cayley	17
1.9	Permutazioni	20
1.10	Classi di coniugio in S_n	26

Ringraziamenti

Federico Allegri, Pietro Crovetto, Davide Ranieri, Francesco Sorce.

§1 Automorfismi

§1.1 Automorfismi di G

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

$$\text{Aut}(G) = \{\varphi : G \longrightarrow G \mid \varphi \text{ isomorfismo}\}$$

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

Esempio 1.1 (Esempi di automorfismi)

Esempi di insiemi di automorfismi:

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

§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) $\varphi_g \in \text{Aut}(G)$, $\forall g \in G$.
- (2) $\{\varphi_g \mid g \in G\} = \text{Inn}(G) \trianglelefteq \text{Aut}(G)$.^a

^a $\text{Inn}(G)$ si definisce **gruppo degli automorfismi interni**.

Dimostrazione. Proviamo le due affermazioni:

- (1) Per verificare che φ_g è un automorfismo bisogna verificare che φ_g è ben definita, ma ciò segue dalla chiusura di G per l'operazione. Verifichiamo che sia un omomorfismo:

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

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:

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

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

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

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

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

ovvero:

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

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

$$\begin{aligned} f \circ \varphi_g \circ f^{-1}(x) &= f(\varphi_g(f^{-1}(x))) = f(g(f^{-1}(x))g^{-1}) = \\ &= f(g)f(f^{-1}(x))f(g^{-1}) = f(g)x(f(g))^{-1} = \varphi_{f(g)} \end{aligned}$$

□

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

$$g x g^{-1} = g g^{-1} x = x \quad \forall x \in G, \forall g \in G$$

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:

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

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:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \text{Inn}(G) \\ \pi_{\ker \phi} \downarrow & \nearrow & \\ G/\ker \phi & & \end{array}$$

dunque:

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

non ci resta che osservare:

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

□

Osservazione 1.6 — L'isomorfismo trovato è del tipo $gZ(G) \mapsto \varphi_g$, 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 $\text{Inn}(G)$ ciclico $\implies G/Z(G)$ ciclico $\implies G$ abeliano da cui:

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

Osservazione 1.9 — $N \trianglelefteq G \iff \forall \varphi_g \in \text{Inn}(G)$ 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:

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

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 $H \leq G$, esso si dice **caratteristico** se è invariante per automorfismi:

$$f(H) = H \quad \forall f \in \text{Aut}(G)$$

Anche in questo caso basta verificare che $f(H) \subseteq H, \forall f \in \text{Aut}(G)$, 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:

$$\text{Aut}(G) \longrightarrow \text{Aut}(H) : f \longmapsto f|_H$$

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:

$$f(Z(G)) \subseteq Z(G) \quad \forall f \in \text{Aut}(G)$$

ovvero:

$$f(z) \in Z(G) \quad \forall f \in \text{Aut}(G), \forall z \in Z(G)$$

dunque bisogna verificare che:

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

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

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

□

Esempio 1.15

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

$$H_1 = \langle (\bar{1}, \bar{0}) \rangle \quad H_2 = \langle (\bar{0}, \bar{1}) \rangle \quad H_3 = \langle (\bar{1}, \bar{1}) \rangle$$

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:

$$f = \begin{cases} (\bar{1}, \bar{0}) \mapsto (\bar{1}, \bar{1}) \\ (\bar{0}, \bar{1}) \mapsto (\bar{0}, \bar{1}) \end{cases}$$

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:

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

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 $H_1 \not\trianglelefteq G$, ma non caratteristico.

A questo punto è facile verificare che:

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

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

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

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

$$\text{Inn}(S_3) \cong S_3 / Z(S_3) \cong S_3$$

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 $\text{Inn}(S_3) \trianglelefteq \text{Aut}(S_3)$ e quindi $\text{Aut}(S_3)$ contiene una copia isomorfa di S_3 come sottogruppo normale, pertanto, se verifichiamo che $|\text{Aut}(S_3)| \leq 6$ abbiamo concluso. Sia $f \in \text{Aut}(S_3)$, 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-cicli² sono completamente determinati, ciò significa che si hanno al più 3! automorfismi, dunque:

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

¹Con τ_i si intendono le trasposizioni che lasciano fisso l'elemento i .

²Come 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:

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

dove $\varphi_g : X \longrightarrow X : x \longmapsto \varphi_g(x)$ ³, con φ_g bigettiva, $\forall g \in G$. Si può definire un'azione anche come:

$$\varphi : G \times X \longrightarrow X : (g, x) \longmapsto \varphi_g(x)$$

Un'azione di G su X si indica con $G \curvearrowright X$.

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 :

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

Da cui:

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

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 $\varphi(G)$.

³Alternativamente si può indicare l'immagine con $\varphi_g : x \longmapsto g * x$, dove $*$ è l'operazione definita su X .

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

$$\text{St}(x) = \{g \in G \mid \varphi_g(x) = x\}$$

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:

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

con:

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

^aSi osserva che il primo $\lambda_{(0,l)}$ è un elemento del gruppo G , mentre il secondo è un'applicazione bigettiva di X .

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 $\sqrt{x^2 + y^2}$:

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

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

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

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

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

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

$$g \text{St}(x) \mapsto \varphi_g(x) \quad \text{e} \quad h \text{St}(x) \mapsto \varphi_h(x)$$

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

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

(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 $\text{St}(x)$, dunque per ogni elemento dell'orbita c'è una classe laterale di $\text{St}(x)$) e surgettiva:

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

e quindi concludiamo che il numero di classi laterali di $\text{St}(x)$ in G è lo stesso della cardinalità di $\text{Orb}(x)$.

Per quanto detto si ha:

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

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

Proposizione 1.25

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

$$|G| = |\text{Orb}(x)| |\text{St}(x)| \quad \forall x \in X$$

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

Ricordando che:

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

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

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

§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:

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

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

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

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 :

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

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 $\frac{|G|}{|Z_G(x)|} = |C_x| = \{x\}$, segue dunque la relazione:

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

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 $\frac{|G|}{|Z_G(x)|} > 1$, poiché se un elemento sta nel centro tutti gli addendi sono 1 per quanto detto, viceversa deve essere che $\frac{|G|}{|Z_G(x)|} = p^k$, $k > 0$, 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 $\exists x \in G : \text{ord}_G(x) = p$. ^a

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

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

da cui segue che $p \mid |Z(G)| = |G| - \sum p l_x$, per quanto premesso ($\forall H \leq G$ si ha $p \nmid |H|$), ed essendo $Z(G) \leq G$, 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 $X = \{H \leq G\}$ e $\varphi : G \rightarrow S(X) : g \mapsto \varphi_g(X)$, con $\varphi_g : X \rightarrow X : H \mapsto gHg^{-1}$. 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:

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

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

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

Per quanto affermato nella [Proposizione 1.25](#) si ha:

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

Osservazione 1.34 — Quindi in generale, dato $H \leq G$ 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:

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

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

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

che equivale a:

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

d'altra parte se H è normale è chiuso per coniugio, ovvero il coniugio di ogni suo elemento è ancora in H ($ghg^{-1} = h', \forall h \in H$) e in particolare ciò significa che:

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

§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:

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

infine, per l'injectività si ha che:

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

da ciò segue che $G \cong \text{Im}(\lambda) \leq S(G)$, e se $|G| = n$ si ha che $\text{Im}(\lambda) \leq S_n$. \square

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

$$g_1 = e \longmapsto \lambda_{g_1} : G \longrightarrow G : g_i \longmapsto g_i$$

$$g_2 \longmapsto \lambda_{g_2} : G \longrightarrow G : x \longmapsto g_2x : g_2^2x \longmapsto \dots \longmapsto g_2^{k-1}x$$

con $k = \text{ord}_G(g_2)$. λ_{g_2} può essere rappresentata mediante la notazione dei cicli:

$$(x, g_2x, \dots, g_2^{k-1}x)$$

preso poi $y \notin \lambda_{g_2}(G)$, si ha analogamente:

$$(y, g_2y, \dots, g_2^{k-1}y)$$

Esempio 1.38

Nel caso in cui $G = \mathbb{Z}/8\mathbb{Z}$ consideriamo l'azione:

$$\lambda : G \longrightarrow S(\mathbb{Z}/8\mathbb{Z}) \cong S_8^a : \bar{a} \longmapsto \lambda_a$$

che, per quanto visto genera ad esempio le applicazioni:^b

$$\begin{aligned} 1 &\longmapsto \lambda_1 : X \longrightarrow X : a \longmapsto 1 + a \implies (0, 1, \dots, 7) \\ 2 &\longmapsto \lambda_2 : X \longrightarrow X : a \longmapsto 2 + a \implies (0, 2, 4, 6)(1, 3, 5, 7) \\ 4 &\longmapsto \lambda_4 : X \longrightarrow X : a \longmapsto 4 + a \implies (0, 4)(1, 5)(2, 6)(3, 7) \end{aligned}$$

che permutano gli elementi di X secondo i cicli trovati.

^aPerché appunto $S(\mathbb{Z}/8\mathbb{Z})$ è l'insieme di permutazioni di un insieme di 8 elementi.

^bPer $+$ si intende la somma modulo 8.

Definizione 1.39. Un'azione λ si dice **fedele** se è iniettiva.

Ad esempio l'azione di rappresentazione regolare a sinistra è fedele:

$$\ker \lambda = \{g \in G | \lambda(g) = id\} = \{g \in G | \lambda_g(e) = e\} = \{g \in G | ge = e\} = \{e\}$$

da cui λ fedele.

Osservazione 1.40 — Esiste anche un'applicazione $\rho : G \longrightarrow S(G) (\cong S_n)$, ($n = |G|$), detta azione di **rappresentazione regolare a destra**, con:

$$g \longmapsto \rho_g : x \longmapsto xg^{-1}$$

Lemma 1.41

Sia G un gruppo abeliano di ordine n , allora $\forall d \mid n, \exists H \leq G : |H| = d$.^a

^aLa dimostrazione non è stata fatta durante il corso, ma è stata comunque aggiunta per completezza.

Dimostrazione. Si consideri innanzitutto il caso $d = p^k$, p primo, e mostriamolo per induzione: per $k = 1$ la tesi è equivalente al **Teorema di Cauchy** (anche solo per i gruppi abeliani). Supponiamo la tesi per $k - 1$. Poiché in particolare $p \mid |G|$ scegliamo un sottogruppo H di G di ordine p ; tale sottogruppo è normale poiché G è abeliano. $p^{k-1} \mid |G/H| \implies$ per ipotesi induttiva $\exists K \leq G/H, |K| = p^{k-1}$.

Prendendo la controimmagine di K tramite la proiezione al quoziente troviamo il sottogruppo di G cercato. A questo punto possiamo scrivere in generale $d = p_1^{k_1} \dots p_s^{k_s}$; per ogni i troviamo sottogruppi H_i di ordini $p_i^{k_i}$ (tutti normali). Si ha quindi che $H_1 H_2 \leq G$ per normalità, inoltre $|H_1 \cap H_2| = 1$ poiché l'ordine di un elemento in tale intersezione deve dividere $(p_1^{k_1}, p_2^{k_2}) = 1$. Pertanto $|H_1 H_2| = p_1^{k_1} p_2^{k_2}$. Ragionando per induzione otteniamo che il sottogruppo $H_1 \dots H_k$ ha ordine d come voluto. \square

Esercizio 1.42. Sia G un gruppo, se $|G| = p^n$, allora esiste:

$$\{e\} = H_n < H_{n-1} < \dots < H_1 < G$$

con $H_i \trianglelefteq G$ e $|H_i| = p^{n-i}$, $\forall i \in \{1, \dots, n\}$.

Soluzione. Procediamo per induzione su n , per $n = 1$ è ovvio, infatti si ha $H_1 = \{e\} \leq G$. Supponiamo la tesi vera $\forall 1 \leq k \leq n - 1$, osserviamo che G è un p -gruppo, pertanto il suo centro non è banale:

$$|Z(G)| = p^z \quad z \geq 1$$

sia $\mathcal{G} = G/Z(G)$, essendo $|G/Z(G)| < p^n$ (perché deve essere $|Z(G)| \geq p$), allora vale l'ipotesi induttiva, dunque $|\mathcal{G}| = p^m$, con $m = n - z (< n)$, allora esiste:

$$\mathcal{H}_m = \{e_{\mathcal{G}}\} < \mathcal{H}_{m-1} < \dots < \mathcal{H}_1 < \mathcal{G}$$

con $|\mathcal{H}_i| = p^{m-i}$ e $\mathcal{H}_i \trianglelefteq \mathcal{G}$. Data la proiezione al quoziente:

$$\pi_{Z(G)} : G \longrightarrow \mathcal{G}$$

per il Teorema di Corrispondenza dei sottogruppi, esiste una bigezione tra i sottogruppi di $G/Z(G)$ e i sottogruppi di G che contengono $Z(G)$, la quale preserva normalità e indice del sottogruppo, pertanto preso $\mathcal{H}_i \leq G/Z(G)$ è sufficiente applicare $\pi_{Z(G)}^{-1}$ alla catena scritta sopra, e si trova:

$$Z(G) = \pi_{Z(G)}^{-1}(\mathcal{H}_m) < \dots < \pi_{Z(G)}^{-1}(\mathcal{H}_1) < \pi_{Z(G)}^{-1}(\mathcal{G}) (= G)$$

Segue per il teorema di corrispondenza che $\pi_{Z(G)}^{-1}(\mathcal{H}_i) = H_i \trianglelefteq G$, ovvero si preserva la normalità dei sottogruppi, inoltre, segue sempre dal teorema che:

$$p^i = [\mathcal{G} : \mathcal{H}_i] = [G : H_i] = p^i$$

dunque la catena esiste e $|H_i| = p^{n-i}$ per $1 \leq i \leq m$, essendo $Z(G)$ abeliano, i sottogruppi di ogni suo ordine (che esistono sempre per il [Lemma Di Ranieri](#)) sono normali in $Z(G)$, inoltre $|Z(G)| = p^z$ (dunque si hanno sottogruppi normali di ordine p^l per $l \mid z$), pertanto esiste la catena:

$$\{e\} = H_n < \dots < H_m = Z(G) \quad \text{con } |H_j| = p^{n-j}, \forall m \leq j \leq n$$

bisogna infine verificare che $H_j \trianglelefteq G$, dunque:

$$gH_jg^{-1} = H_j \quad \forall g \in G$$

ma $H_j \subset Z(G)$ (sta nel centro, quindi è invariante per coniugio con tutti i $g \in G$, e in particolare quelli richiesti) dunque è sempre verificata l'ultima uguaglianza. \square

§1.9 Permutazioni

Ricordiamo brevemente che:

Definizione 1.43. Dato un insieme X si definisce **permutazione** un'applicazione bigettiva di X in se stesso.

Indichiamo con $S(X)$ il gruppo delle permutazioni di X e con S_n il gruppo delle permutazioni di un insieme di cardinalità n , che per semplicità indichiamo con $\{1, \dots, n\}$. Le permutazioni si possono indicare in vari modi, ad esempio, preso $\sigma \in S_{12}$ si può rappresentare mediante la matrice di permutazione:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 2 & 4 & 5 & 1 & 9 & 8 & 7 & 6 & 12 & 11 & 10 \end{pmatrix}$$

o anche con la notazione dei cicli:

$$\sigma = (1 \ 3 \ 4 \ 5)(6 \ 9)(7 \ 8)(10 \ 12)$$

ogni ciclo prende il nome di **k -ciclo** (dove k indica la sua lunghezza), come si osserva i cicli di lunghezza 1 sono stati omessi, in quanto lasciano fissi gli elementi, inoltre, i 2-cicli prendono il nome di **trasposizioni**. Formalmente, sia $\sigma \in S_n$ una permutazione di un insieme di n elementi, possiamo considerare l'insieme X , con $|X| = n$, il gruppo $G = \langle \sigma \rangle$ e definire l'azione:

$$\varphi : G = \langle \sigma \rangle \longrightarrow S(X) \cong S_n : \sigma \longmapsto \sigma$$

con $\sigma \in S_n$ e $\sigma : i \longmapsto \sigma(i)$. Osserviamo quindi che:

$$\text{Orb}(x) = \{\sigma(x) | \sigma \in \langle \sigma \rangle\} = \{\sigma^l(x) | l \in \mathbb{N}\} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)\}$$

con $|\text{Orb}(x)| = m_x$, con $m_x = \min\{k > 0 | \sigma^k(x) = x\}$, perché se $\sigma^k(x) = x$, allora $\sigma^{k+1}(x) = \sigma(x)$, pertanto, sia $k \in \mathbb{N}$ tale che $\sigma^k(x) \in \{x, \dots, \sigma^{k-1}(x)\}$, allora $\exists h :$

$$\sigma^k(x) = \sigma^h(x) \quad \text{con } 0 \leq h < k$$

Dunque vale che $\sigma^{k-h}(x) = x \in \{x, \dots, \sigma^{k-1}(x)\}$ e per la minimalità di k si ha che $h = 0$. L'azione di $\langle \sigma \rangle$ su X divide X in orbite e su ogni orbita σ agisce ciclicamente (ovvero $\sigma(\text{Orb}(x)) = \text{Orb}(x)$).

Definizione 1.44. Si dice **ciclo** di $\sigma \in S_n$ l'orbita di un elemento $x \in \{1, \dots, n\}$ vista come insieme ordinato:

$$(x, \sigma(x), \dots, \sigma^{m_x-1}(x))$$

Osservazione 1.45 — Un ciclo di lunghezza k (un k -ciclo) ha k scritte distinte, in quanto possiamo scegliere arbitrariamente il primo elemento.

Osservazione 1.46 — Data $\sigma \in S_n$, essa è determinata dalle immagini di $\{1, \dots, n\}$, dunque è determinata dai suoi cicli.

Esempio 1.47

Presa ad esempio $\sigma \in S_{10}$:

$$\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9)$$

chiamiamo i suoi cicli:

$$\sigma_1 = (1\ 2\ 3) \quad \sigma_2 = (4\ 5) \quad \sigma_3 = (6\ 7\ 8\ 9)$$

dove appunto $\sigma_1, \sigma_2, \sigma_3 \in S_{10}$ e:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$$

Definizione 1.48. Una permutazione si dice **ciclica** se ha un unico ciclo (orbita) non banale.

Osservazione 1.49 — Si osserva che:

- Cicli disgiunti commutano.
- L'ordine di una permutazione ciclica è la lunghezza del suo ciclo:

$$\sigma = (x_1, \dots, x_k) \implies \text{ord } \sigma = k$$

quindi $\sigma^k = id$ e se $d < k$, allora $\sigma^d(x_1) = x_{d+1} \neq x_1$.

Proposizione 1.50 (Struttura Delle Permutazioni)

Ogni permutazione si scrive in modo unico (a meno dell'ordine e della scrittura di cicli) come prodotto di cicli disgiunti, ovvero come composizione di permutazioni cicliche che agiscono su insiemi disgiunti.

Dimostrazione. I cicli della permutazione sono univocamente determinati in quanto orbite della permutazione, sappiamo che ogni permutazione si scrive come prodotto dei suoi cicli, e per concludere basta osservare che i cicli disgiunti commutano. \square

Osservazione 1.51 — Si osserva che l'unicità della scrittura di una permutazione vista nella [Proposizione 1.50](#) è effettivamente valida solo nel caso di cicli disgiunti, infatti, prendendo ad esempio:

$$\sigma = (1\ 2)(2\ 4) \in S_4 \quad \text{con} \quad \sigma_1 = (2\ 4) \quad \text{e} \quad \sigma_2 = (1\ 2)$$

non essendo σ_1, σ_2 cicli disgiunti, si osserva che $\sigma_2 \circ \sigma_1 = (2\ 4\ 1)$ e quindi σ era in realtà un 3-ciclo, e la sua fattorizzazione è unica come tale (mentre non era unica come prodotto di cicli non disgiunti).

Corollario 1.52

S_n è generato dalle permutazioni cicliche.

Dimostrazione. Segue immediatamente dal fatto che ogni permutazione si ottiene mediante composizione di permutazioni cicliche. \square

Esempio 1.53

Per esempio, preso S_4 , le permutazioni possibili sono cicli del tipo:

$$id \quad (a \ b) \quad (a \ b \ c) \quad (a \ b \ c \ d) \quad (a \ b)(c \ d)$$

per contare il numero di 2-cicli, ci basta scegliere 2 elementi dell'insieme in $\binom{4}{2}$ modi e poi considerare tutti i possibili riordinamenti ciclici (dove la scelta del primo elemento è arbitraria), e ciò può essere fatto in $\frac{2!}{2}$ modi, per un totale di:

$$\binom{4}{2} \frac{2!}{2} = 6$$

e ragionando analogamente per i 3-cicli e i 4-cicli si ottiene:

$$\binom{4}{3} \frac{3!}{3} = 8 \quad \text{e} \quad \binom{4}{4} \frac{4!}{4} = 6$$

infine, per quanto riguarda le permutazioni ottenute dalla composizione di due 2-cicli, possiamo scegliere e permutare due coppie di elementi, come nei casi precedenti, tuttavia, essendo i cicli disgiunti commutano (banalmente perché lasciano fissi gli altri elementi del dominio), quindi bisogna anche dividere per il numero di scambi per i cicli della stessa lunghezza, ovvero $2!$ dunque:

$$\binom{4}{2} \frac{2!}{2} \binom{2}{2} \frac{2!}{2} \cdot \frac{1}{2!} = 4$$

e dal conteggio delle permutazioni di S_4 divise per cicli di diversa lunghezza si ottiene: $6 + 8 + 6 + 4 = 24 = |S_4|$.

Osservazione 1.54 — Quanto visto nell'esempio precedente può essere generalizzato ottenendo:

$$\#\{\sigma \in S_n \mid \sigma \text{ è un } k\text{-ciclo}\} = \binom{n}{k} \frac{k!}{k} = \binom{n}{k} (k-1)!$$

Esempio 1.55

Per quanto detto risulta semplice ad esempio calcolare:

$$\#\{\sigma \in S_{20} \mid \sigma \text{ si fattorizza in cicli del tipo } 2 + 2 + 2 + 4 + 5 + 5\}$$

applicando quanto detto nell'osservazione pretendente si trovano:

$$\frac{\binom{20}{2}\binom{18}{2}\binom{16}{2}1!1!1!}{3!} \cdot \binom{14}{4}3! \cdot \frac{\binom{10}{5}\binom{5}{5}4!4!}{2!}$$

Proposizione 1.56 (Ordine Di Una Permutazione)

Data $\sigma \in S_n$ con $\sigma = \sigma_1 \dots \sigma_k$, con σ_i cicli disgiunti, allora:

$$\text{ord } \sigma = [\text{ord } \sigma_1, \dots, \text{ord } \sigma_k]$$

Dimostrazione. Sia σ_i un l_i -ciclo, ovvero $\text{ord } \sigma_i = l_i$, vogliamo dimostrare che:

$$\text{ord } \sigma = [l_1, \dots, l_k] = d$$

osserviamo che $\sigma^d = (\sigma_1 \dots \sigma_k)^d = \sigma_1^d \dots \sigma_k^d$, in quanto i cicli σ_i sono disgiunti (pertanto commutano), essendo $d = [l_1, \dots, l_k] \implies d \mid l_i, \forall i \in \{1, \dots, k\}$, pertanto:

$$\sigma^d = \sigma_1^d \dots \sigma_k^d = id \implies \text{ord } \sigma = m \mid d$$

d'altra parte, si ha che:

$$\sigma^m = \sigma_1^m \dots \sigma_k^m = id \iff \sigma_i = id, \forall i \in \{1, \dots, k\}$$

dunque $\text{ord } \sigma_i = l_i \mid m, \forall i \in \{1, \dots, k\}$, ovvero $[l_1, \dots, l_k] \mid m$ da cui si conclude che $m = [l_1, \dots, l_k]$. \square

Proposizione 1.57

Le trasposizioni generano $S_n, \forall n \geq 3$.

Dimostrazione. Per dimostrare l'affermazione bisogna mostrare che ogni permutazione è prodotto di trasposizioni (in generale non disgiunte). Poiché ogni permutazione, per quanto affermato nella [Proposizione 1.50](#), è il prodotto di cicli (permutazioni cicliche) disgiunti, è sufficiente mostrare che i cicli sono tutti prodotto di trasposizioni, infatti si può osservare che:

$$(1 \dots k) = (1 \ k)(1 \ k-1) \dots (1 \ 2)$$

dove l'uguaglianza è tra funzioni, quindi ci basta mostrare che danno la stessa immagine. Se $i > k$, allora entrambe le funzioni mandano $i \mapsto i$, se $i \leq k$, allora la funzione a sinistra manda $i \mapsto i+1$ e $k \mapsto 1$, quella a destra lascia fisso i fino al ciclo $(1 \ i)$ che manda $i \mapsto 1 \mapsto i+1$ che rimane fisso in $i+1$, mentre $k \mapsto \dots \mapsto 1$. \square

Osservazione 1.58 — La scrittura di una permutazione come prodotto di trasposizioni non è unica. Ad esempio in S_4 :

$$\sigma = (1\ 2)(2\ 4) = (1\ 2)(3\ 4)(3\ 4)(2\ 4)$$

La seguente proposizione ci mostra invece che è fissata la parità della decomposizione in trasposizioni, cioè se σ si compone come prodotto di m trasposizioni, ogni altra decomposizione come prodotto di trasposizioni ha un numero di trasposizioni con la stessa parità.

Proposizione 1.59

L'applicazione:

$$\text{sgn} : S_n \mapsto \{\pm 1\} : \sigma \mapsto \text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

è un omomorfismo di gruppi. Inoltre, se σ è una trasposizione, allora $\text{sgn}(\sigma) = -1$.

Dimostrazione. Osserviamo inizialmente che sgn è ben definita cioè:

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{\pm 1\}$$

al denominatore del prodotto vi sono tutte le possibili coppie $i - j$ e anche al numeratore poiché σ è bigettiva, l'unica cosa che può cambiare è l'ordine (ovvero potrebbe comparire $i - j$ al numeratore e $j - i$ al denominatore), quindi $\text{sgn}(\sigma) \in \{\pm 1\}$. Mostriamo che sgn è un omomorfismo:

$$\text{sgn}(\sigma \circ \tau) = \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j}$$

da cui:

$$\prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j} = \underbrace{\prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}}_{\text{sgn}(\sigma)} \underbrace{\prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j}}_{\text{sgn}(\tau)} \quad \forall \sigma, \tau \in S_n$$

Ci resta da verificare che il segno di una trasposizione è -1 . Sia $\sigma = (a\ b)$, analizziamo il segno delle varie coppie, distinguiamo le seguenti possibilità:

- $\{i, j\} \cap \{a, b\} = \emptyset$, in tal caso $\sigma(i) = i, \sigma(j) = j \implies \frac{\sigma(i) - \sigma(j)}{i - j} = 1$.
- $\{i, a\}$ (o $\{i, b\}$), in tal caso $\frac{\sigma(i) - \sigma(a)}{i - a} = \frac{i - b}{i - a}$, però vi è anche $\frac{\sigma(i) - \sigma(b)}{i - b} = \frac{i - a}{i - b}$ e quindi il fattore dà 1.
- Infine, nel caso in cui $\{i, j\} = \{a, b\}$ si ha:

$$\frac{\sigma(a) - \sigma(b)}{a - b} = \frac{b - a}{a - b} = -1$$

Dunque si conclude che $\text{sgn}((a\ b)) = -1$. □

Osservazione 1.60 — La proposizione appena vista dimostra quanto detto sopra, ovvero:

$$\sigma = \tau_1 \dots \tau_m \quad \text{con } \tau_i \text{ trasposizione}$$

allora $\text{sgn}(\sigma) = \prod_{1 \leq i \leq m} \text{sgn}(\tau_i) = (-1)^m$.

Definizione 1.61. Una permutazione $\sigma \in S_n$ si dice **pari** se $\text{sgn}(\sigma) = 1$, **dispari** se $\text{sgn}(\sigma) = -1$.

Definizione 1.62. Dato l'omomorfismo $\text{sgn} : S_n \mapsto \{\pm 1\}$, si definisce **gruppo alterno**:

$$\mathcal{A}_n = \ker \text{sgn} = \{\sigma \in S_n \mid \sigma \text{ è pari}\}$$

Osservazione 1.63 — Si osserva che $\mathcal{A}_n \trianglelefteq S_n$, $|\mathcal{A}_n| = \frac{n!}{2}$ e $S_n/\mathcal{A}_n \cong \{\pm 1\}$.

Osservazione 1.64 — Per quanto detto nella [Proposizione 1.57](#), un k -ciclo si può scrivere nella forma:

$$(1 \dots k) = \underbrace{(1 \ k)(1 \ k-1) \dots (1 \ 2)}_{k-1 \text{ trasposizioni}}$$

dunque un k -ciclo è pari se $k \equiv 0 \pmod{2}$, dispari se $k \equiv 1 \pmod{2}$.

§1.10 Classi di coniugio in S_n

Teorema 1.65

Due permutazioni in S_n sono coniugate se e solo se hanno la stessa decomposizione in cicli disgiunti.

Dimostrazione. Mostriamo le due implicazioni:

- Presa $\sigma = (a_1 \dots a_k)$ e $\tau \in S_n$, vogliamo dimostrare che $\tau \circ \sigma \circ \tau^{-1}$ è ancora un k -ciclo. Sia $\tau(a_i) = b_i$, allora $\tau \sigma \tau^{-1} = (b_1 \dots b_k)$, con $b_i \neq b_j, \forall i \neq j$, poiché τ è bigettiva; verifichiamo l'uguaglianza mostrando che le due funzioni coincidono per tutti gli elementi. Si osserva che nel ciclo a destra accade semplicemente che $b_i \mapsto b_{i+1}$, a sinistra invece:

$$b_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} b_{i+1} \quad \forall i \in \{1, \dots, k\}$$

Se, invece, $x \neq b_i$, a sinistra si ha $\tau \sigma \tau^{-1}(x)$ (cioè poiché non si parte da alcun b_i),
 $\neq a_1, \dots, a_k$
 quindi $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$, e quindi $\tau \circ \tau^{-1}(x) = x$; a destra invece, non essendo x alcun b_i viene lasciato fisso, ciò conclude che le due funzioni sono uguali e che quella a sinistra è quindi un k -ciclo.

- Mostriamo ora che due permutazioni con la stessa fattorizzazione in cicli disgiunti sono coniugate. Siano:

$$\sigma = (a_1 \dots a_l)(b_1 \dots b_s) \dots (z_1 \dots z_t)$$

$$\rho = (a'_1 \dots a'_l)(b'_1 \dots b'_s) \dots (z'_1 \dots z'_t)$$

per dimostrare la tesi è sufficiente trovare $\tau \in S_n$ tale che $\tau \circ \sigma \circ \tau^{-1} = \rho$. Scegliamo τ definita da:

$$\tau(a_i) = a'_i, \tau(b_i) = b'_i, \dots, \tau(z_i) = z'_i$$

ed eventualmente si aggiungono altri elementi. Verifichiamo allora che $\tau \circ \sigma \circ \tau^{-1} = \rho$, consideriamo (WLOG) il primo ciclo:

$$a'_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} a'_{i+1}$$

e quindi $a'_i \mapsto a'_{i+1}$, pertanto $\tau \circ \sigma \circ \tau^{-1}$ e ρ coincidono sempre.

□

Esempio 1.66

In S_5 le classi di coniugio di $\sigma = (1\ 2)(3\ 4)$ sono $C_\sigma = \{(a\ b)(c\ d) \in S_5\}$, con:

$$\#C_\sigma = \frac{\binom{5}{2}\binom{3}{2}1!1!}{2!} = 15$$

e da ciò si ricava anche che:

$$\#Z_{S_5}(\sigma) = \frac{|S_5|}{|C_\sigma|} = \frac{5!}{15} = 8$$

Esempio 1.67

Sia $\sigma = (3\ 5)(14) \in S_5$ e sia $\rho = (1\ 2)(3\ 4)$, cerchiamo $\tau \in S_5$ tale che:

$$\tau \circ \sigma \circ \tau^{-1} = \rho$$

si può scegliere $\tau = (1\ 3)(2\ 5)$, da cui:

$$(1\ 3)(2\ 5)(3\ 5)(14)(1\ 3)(2\ 5) = (1\ 2)(3\ 4) = \rho$$

Corollario 1.68

Valgono i seguenti fatti:

- (1) Il numero di classi di coniugio in S_n è uguale al numero di partizioni di n .
- (2) Se $H \leq S_n$, allora $H \trianglelefteq S_n$ se e solo se contiene tutte le permutazioni di un certo tipo o nessuna.