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

Ringraziamenti

Davide Ranieri, Federico Allegri, Pietro Crovetto, Francesco Sorce, Leonardo Migliorini, Matteo Gori, Daniele Lapadula, Alessandro Fenu, Leonardo Alfani, Clementina Salamina, Giorgia Capecchi.

§1 Gruppi

§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) $\{\varphi_g | g \in G\} = \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.[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 bisogna verificare che φ_g è ben definita, ma ciò segue dalla chiusura di g per l'operazione. Verifichiamo che sia un omomorfismo:

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

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 $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$; mostriamo prima che $\mathrm{Inn}(G)$ è un sottogruppo di $\mathrm{Aut}(G)$, infatti: $id = \varphi_e \in \mathrm{Inn}(G)$, $\forall g_1, g_2 \in G$ vale che $\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2} \in \mathrm{Inn}(G)$, 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, $(\varphi_g)^{-1} = \varphi_{g^{-1}} \in \mathrm{Inn}(G)$:

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

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

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

ovvero:

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

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

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

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

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

tale applicazione è chiaramente ben definita, ed è surgettiva per come abbiamo definito $\mathrm{Inn}(G)$. 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:

$$\begin{array}{ccc} G & \xrightarrow{\ \phi\ } & \mathrm{Inn}(G) \\ {\scriptstyle \pi_{\ker\phi}}\downarrow & \nearrow_{\sim} & \\ {}^{G}\!/_{\ker\phi} & & \end{array}$$

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:

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

□

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:

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

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 $G \circlearrowleft X$.

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 $\sim$:

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

Da cui:

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

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 $\varphi(G)$.

[3] Alternativamente si può indicare l'immagine con $\varphi_g : x \longmapsto g * x$ dove il simbolo $*$ indica l'azione di g su x.

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:

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

con:

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

[a] Si osserva che il primo $\tau_{(0,l)}$ 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:

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

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

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

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

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

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

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

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

dove si ha che $\varphi_{gh}(x) = \varphi_g \circ \varphi_h(x)$ in quanto φ è un omomorfismo. Infine, preso $g \in \mathrm{St}(x)$, si ha $g^{-1} \in \mathrm{St}(x)$, 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:

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

□

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:

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

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

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

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

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 $|\,\mathrm{St}(x)|\,||G|$, tuttavia, per la proposizione precedente, si ha che: $|\,\mathrm{Orb}(x)|\,||G|$ con $\mathrm{Orb}(x) \subseteq X$.

Ricordando che:

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

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:

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

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

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

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

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

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 :

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

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 $\mathrm{Orb}(x) = \{x\}$ (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 $\exists x \in G : \text{ord}_G(x) = p$. [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 $\exists x \in H : \text{ord}_H(x) = p$, 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:

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

da cui segue che $p \mid |Z(G)| = |G| - \sum pl_x$, 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; mostriamo invece che φ_g è una permutazione, per 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 $H \trianglelefteq G$ 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:

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

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:

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

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 $\varphi_g : G \longrightarrow G : x \longmapsto gx$, 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:

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

da ciò segue che $G \cong \mathrm{Im}(G) \leqslant S(G)$, e se $|G| = n$ si ha che $\mathrm{Im}(G) \leqslant S_n$. □

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:

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

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

con $k = \mathrm{ord}_G(g_2)$. 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:

$$\lambda : G \longrightarrow S(\mathbb{Z}/8\mathbb{Z}) \cong S_8 \text{[a]} : \overline{a} \longmapsto \lambda_a$$

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

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

che permutano gli elementi di X secondo i cicli trovati.

[a] Perché appunto $S(\mathbb{Z}/8\mathbb{Z})$ è l'insieme di permutazioni di un insieme di 8 elementi.
[b] Per $+$ 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 $\forall d \mid n, \exists H \leqslant G : |H| = d$. [a]

[a] La 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 $\exists K \leqslant G,\ |K| = p^{k-1}$.
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 $H_1 H_2 \leqslant G$ 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. □

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

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

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

Soluzione. Procediamo per induzione su n, per $n = 1$ è ovvio, infatti si ha $H_1 = \{e\} \trianglelefteq G$. 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:

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

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:

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

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 $\mathcal{H}_i \leqslant {}^{G}\!/_{Z(G)}$ è sufficiente applicare $\pi^{-1}_{Z(G)}$ alla catena scritta sopra, e si trova:

$$Z(G) = \pi^{-1}_{Z(G)}(\mathcal{H}_m) < \ldots < \pi^{-1}_{Z(G)}(\mathcal{H}_1) < \pi^{-1}_{Z(G)}(\mathcal{G})(= G)$$

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

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

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:

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

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

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

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. □

§1.9 Permutazioni

Ricordiamo brevemente che:

Definizione 1.43. Dato un insieme X si definsce **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:

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

con $|\mathrm{Orb}(x)| = m_x$, 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 $\exists h$:

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

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 $\sigma(\mathrm{Orb}(x)) = \mathrm{Orb}(x)$).

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 scritture 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:

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

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. [4]

Osservazione 1.49 — Si osserva che:

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

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

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

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. □

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:

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

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).

[4] D'ora in avanti si utilizzeranno i termini "permutazione ciclica" e "ciclo" come sinonimi, in quanto una permutazione ciclica è appunto un singolo ciclo non banale.

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. □

Esempio 1.53

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

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

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:

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

infine, per quanto riguarda le permutazioni ottenute dalla composizione di due 2-cilci, possiamo scegliere e permutare due coppie di elementi, come nei casi precedenti, tuttavia, essendo i cicli disgiunti commutanto (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:

$$\binom{4}{2}\frac{2!}{2}\binom{2}{2}\frac{2!}{2}\cdot\frac{1}{2!} = 3$$

e dal conteggio delle permutazioni di S_4 divise per cicli di diversa lunghezza si ottiene: $6 + 8 + 6 + 3 + 1 = 24 = |S_4|$.

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

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

Esempio 1.55

Per quanto detto risulta semplice ad esempio calcolare:

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

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:

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

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

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

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 $d = [l_1, \dots, l_k] \implies d \mid l_i, \forall \in \{1, \dots, k\}$, pertanto:

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

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

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 $i \longmapsto i$, se $i \leq k$, allora la funzione a sinistra manda $i \longmapsto i+1$ e $k \longmapsto 1$, quella a destra lascia fisso i fino al ciclo $(1 \ i)$ che manda $i \longmapsto 1 \longmapsto i+1$ che rimane fisso in $i+1$, mentre $k \longmapsto \dots \longmapsto 1$. □

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:

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

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

Dimostrazione. Osserviamo inizialmente che sgn è ben definita cioè:

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

al denominatore del prodotto vi sono tutte le possibili coppie $i-j$ (in $\{1,\dots,n\}$) 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 $sgn(\sigma) \in \{\pm 1\}$. Mostriamo che sgn è un omomorfismo:

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

da cui:

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

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 σ lascia fissi gli elementi, $\sigma(i) = i, \sigma(j) = j \implies \frac{\sigma(i)-\sigma(j)}{i-j} = 1$.
- $\{i,a\}$ (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 $sgn((a\ b)) = -1$. □

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

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

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

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

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

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

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

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 $k \equiv 1 \pmod 2$, dispari se $k \equiv 0 \pmod 2$.

§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 $b_i \longmapsto b_{i+1}$, a sinistra invece:

$$b_i \overset{\tau^{-1}}{\longmapsto} a_i \overset{\sigma}{\mapsto} a_{i+1} \overset{\tau}{\mapsto} b_{i+1} \qquad \forall i \in \{1, \dots, k\}$$

  Se, invece, $x \neq b_i$, a sinistra si ha $\tau\sigma \underbrace{\tau^{-1}(x)}_{\neq a_1,\dots,a_k}$ (ciò poiché non si parte da alcun b_i), 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:

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

  e quindi $a'_i \longmapsto a'_{i+1}$, 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 $H \leqslant S_n$, allora $H \trianglelefteq S_n$ se e solo se contiene tutte le permutazioni di un certo tipo o nessuna.

§1.11 Prodotto diretto

Ricordiamo brevemente che se G_1 e G_2 sono gruppi, allora l'insieme $G_1 \times G_2$ con l'operazione fatta componente per componente prende il nome di **prodotto diretto**.

Esempio 1.69
Presi ad esempio $\mathbb{Z}/7\mathbb{Z}$ e S_4, si ha $\mathbb{Z}/7\mathbb{Z} \times S_4$, con $\sigma = (\overline{1}, (1\ 2\ 3))$ e $\rho = (\overline{4}, (1\ 4\ 2\ 4))$ in $\mathbb{Z}/7\mathbb{Z} \times S_4$ e l'operazione:

$$\sigma \cdot \rho = (\overline{1} + \overline{4}, (1\ 2\ 3) \circ (1\ 4\ 2\ 3)) = (\overline{5}, (1\ 4\ 3\ 2))$$

Osservazione 1.70 — Si ricordano i seguenti fatti:

- Se $H, K \leqslant G$ in generale HK non è un sottogruppo, ma $HK \leqslant G \iff HK = KH$. Ovviamente se uno tra H e K è normale in G, allora questo è sempre vero.
- $H \times K \leqslant G \times G$.

Lemma 1.71
Siano $H, K \trianglelefteq G$ e $H \cap K = \{e\}$, allora $hk = kh$, $\forall h \in H$, $\forall k \in K$.

Dimostrazione. Preso $hkh^{-1}k^{-1}$, si ha:

$$hkh^{-1}k^{-1} = \underbrace{\underbrace{(hkh^{-1})}_{=k'}k^{-1}}_{\in K} = \underbrace{h\underbrace{(kh^{-1}k^{-1})}_{=h'}}_{\in H}$$

dunque $hkh^{-1}k^{-1} \in H \cap K \implies hkh^{-1}k^{-1} = e$, da cui segue la tesi. □

Teorema 1.72
Sia G un gruppo e siano $H, K \trianglelefteq G$ tali che:

(1) HK = G.

(2) $H \cap K = \{e\}$.

Allora $G \cong H \times K$.

Dimostrazione. Definiamo l'applicazione:

$$\varphi : H \times K \longrightarrow G : (h, k) \mapsto hk$$

Si verifica che è un omomorfismo:

$$\varphi((h_1, k_1)(h_2, k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$$

per il Lemma 1.71 si ha che $h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi((h_1, k_1))\varphi((h_2, k_2))$, $\forall h_1, h_2 \in H$, $\forall k_1, k_2 \in K$. Si osserva ora che φ è surgettiva, per l'ipotesi (1); infine, è iniettiva in quanto:

$$\ker \varphi = \{(h, k) \in H \times K | hk = e\} = \{(h, k) \in H \times K | h = k^{-1}\} = \{e\}$$

dove nell'ultima uguaglianza si è usato il fatto che $H \cap K = \{e\}$. □

Osservazione 1.73 — Se abbiamo due sottogruppi G_1 e G_2 e costruiamo $G = G_1 \times G_2$, allora presi:

$$H = G_1 \times \{e_2\} \trianglelefteq G \qquad \text{e} \qquad K = \{e_1\} \times G_2 \trianglelefteq G$$

H, K sono normali, hanno intersezione banale e sono tali che $HK = G$, quindi verifichiamo le ipotesi del teorema, pertanto $G \cong H \times K$.

Esempio 1.74

Sia G un gruppo con $|G| = p^2$, dalla formula delle classi avevamo ottenuto che G è necessariamente abeliano, quindi G è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ o $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Se G è ciclico, allora $G \cong \mathbb{Z}/p^2\mathbb{Z}$. Mostriamo che se non lo è, allora $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e in questo caso tutti gli elementi di G hanno ordine p.
Consideriamo $(e \neq)x \in G$ e $H = \langle x \rangle \trianglelefteq G$ (in quanto G abeliano); prendiamo $y \in G \setminus \langle x \rangle$ e analogamente $K = \langle y \rangle \trianglelefteq G$, da ciò segue che $H \cap K = \{e\}$, infatti H e K sono sottogruppi ciclici di G di ordine p e quindi hanno in comune solo l'elemento neutro. Osservando infine che $HK = G$, per cardinalità:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2$$

le ipotesi del Teorema 1.72 sono verificate, dunque:

$$G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

§1.12 Prodotto semidiretto

Definizione 1.75. Dati due gruppi H, K e l'azione:

$$\varphi : K \longrightarrow \mathrm{Aut}(H)(\leqslant S(H)) : k \longmapsto \varphi_k$$

si dice **prodotto semidiretto** di H e K via φ:

$$H \rtimes_\varphi K$$

(o anche $K_\varphi \ltimes H$) l'insieme ottenuto come prodotto cartesiano $H \times K$ con l'operazione definita da:

$$(h,k)(h',k') = (h \cdot_H \varphi_k(h'), k \cdot_K k')$$

Proposizione 1.76 (Il Prodotto Semidiretto è un gruppo)
Dati due gruppi H, K, allora $H \rtimes_\varphi K$ è un gruppo.

Dimostrazione. Come si verifica facilmente l'operazione indotta dal prodotto semidiretto è associativa, verifichiamo che (e_H, e_K) è l'elemento neutro:

$$(h,k)(e_H,e_K) = (h \cdot \varphi_k(e_H), ke_K) = (he_H, k) = (h,k)$$

dove $\varphi_k(e_H) = e_H$ poiché φ_k è un automorfismo (e quindi in particolare un omomorfismo), a sinistra, invece, si ha:

$$(e_H,e_K)(h,k) = (e_H \cdot \varphi_{e_K}(h), e_K k) = (e_H \cdot id(h), k) = (e_H h, k) = (h,k)$$

Per l'inverso si osserva:

$$(h,k)^{-1} = ((\varphi_k)^{-1}(h^{-1}), k^{-1}) = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$$ [5]

dunque si verifica a destra:

$$(h,k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h \cdot \varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = \\ = (h \cdot id(h^{-1}), e_K) = (hh^{-1}, e_K) = (e_H, e_K)$$

e analogamente a sinistra:

$$(\varphi_{k^{-1}}(h^{-1}), k^{-1})(h,k) = (\varphi_{k^{-1}}(h^{-1}) \cdot \varphi_{k^{-1}}(h), k^{-1}k) = \\ = (\varphi_{k^{-1}}(h^{-1}h), e_K) = (\varphi_{k^{-1}}(e_H), e_K) = (e_H, e_K)$$

□

[5] L'uguaglianza $(\varphi_k)^{-1} = \varphi_{k^{-1}}$ segue dal fatto che φ è un omomorfismo e quindi manda inversi in inversi.

Osservazione 1.77 — Si osserva che $H \rtimes_\varphi K$ è il prodotto diretto se e solo se $\varphi_k = e$, $\forall k \in K$. Infatti:

$$(h,k)(h',k') = (h \cdot \varphi_k(h'), kk') = (hh', kk') \iff \varphi_k(h') = h' \qquad \forall k \in K$$

e dunque $\varphi_k = id_H$.

Teorema 1.78

Sia G un gruppo e siano $H, K \leqslant G$, con $H \trianglelefteq G$, tali che:

(1) $HK = G$.

(2) $H \cap K = \{e\}$.

Allora $G \cong H \rtimes_\varphi K$, dove $\varphi : K \longrightarrow \mathrm{Aut}(H) : k \longmapsto \varphi_k$, con $\varphi_k : h \longmapsto khk^{-1}$.

Dimostrazione. Costruiamo esplicitamente un isomorfismo tra i due gruppi:

$$\mathcal{F} : H \rtimes_\varphi K \longrightarrow G : (h,k) \longmapsto hk$$

Verifichiamo che è un omomorfismo:

$$\mathcal{F}((h,k)(h',k')) = \mathcal{F}(h \cdot \varphi_k(h'), kk') = \mathcal{F}(h \underbrace{kh'k^{-1}}_{=\varphi_k(h')}, kk') = hkh'k^{-1}kk' = \underbrace{hk}_{=\mathcal{F}(h,k)} \underbrace{h'k'}_{=\mathcal{F}(h',k')}$$

Si vede inoltre che $\mathcal{F}$ è surgettiva per l'ipotesi (1) e iniettiva per la (2), infatti:

$$\ker \mathcal{F} = \{(h,k) \in H \rtimes_\varphi K \mid \mathcal{F}(h,k) = hk = e\} = \{e\}$$

□

Osservazione 1.79 — Si osserva che φ_k è la restrizione al sottogruppo H dell'automorfismo interno $g \longmapsto kgk^{-1}$, poiché $H \trianglelefteq G$, allora la restrizione a H di ogni elemento di $\mathrm{Inn}(G)$ è un automorfismo di H.

Osservazione 1.80 — Sapendo che $G \cong H \rtimes_\varphi K$ e seguendo i passaggi della verifica di omomorfismo al contrario, si ricava che necessariamente φ è esattamente l'azione di coniugio su H.

Osservazione 1.81 — Siano $\overline{H} = H \times \{e_K\}$ e $\overline{K} = \{e_H\} \times K$, si osserva che $\overline{H}, \overline{K} \leqslant G = H \rtimes_\varphi K$, infatti sono chiusi per prodotto (ristretto):

$$(h, e_K)(h', e_K) = (h \cdot \varphi_{e_K}(h'), e_K) = (h \cdot id(h'), e_K) = (hh', e_K)$$

$$(e_H, k)(e_H, k') = (e_H \cdot \varphi_k(e_H), kk') = (e_H, kk')$$

e si verifica facilmente anche per inverso. Si osserva che $\overline{H} \trianglelefteqslant G$[a], in quanto $H = \ker \pi$, con:

$$\pi : H \rtimes_\varphi K \longrightarrow K : (h, k) \longmapsto k$$

con π omomorfismo come si vede:

$$\pi((h, k)(h', k')) = \pi(h \cdot \varphi_k(h'), kk') = kk' = \pi((h, k))\pi((h', k'))$$

Per come li abbiamo presi si nota subito che $\overline{HK} = G$ e $\overline{H} \cap \overline{K} = \{e\}$, quindi valgono le ipotesi del Teorema 1.79, pertanto:

$$\overline{H} \times \overline{K} \cong G = H \rtimes_\varphi K$$

[a] $\overline{K}$ in generale non è normale, lo è solo se il prodotto è diretto, infatti in quel caso vale il Teorema 1.72.

Esempio 1.82 ($S_n \cong \mathcal{A}_n \rtimes_\varphi \langle (1\ 2) \rangle$)

Verifichiamo che S_n è prodotto semidiretto di $H = \mathcal{A}_n$ e $K = \langle (1\ 2) \rangle$ [a] usando il Teorema 1.78, per quanto detto nel (1) del Corollario 1.68 sappiamo che $\mathcal{A}_n \triangleleft S_n$, inoltre, sempre per il punto (1), essendo $|\mathcal{A}_n| = \frac{n!}{2}$, segue per cardinalità che $HK = S_n$. Essendo $\mathcal{A}_n = \ker sgn$ e $\langle (1\ 2) \rangle$ una trasposizione $H \cap K = \{e\}$ (in quanto il nucleo dell'omomorfismo segno contiene solo permutazioni pari), pertanto segue la tesi:

$$S_n \cong \mathcal{A}_n \rtimes_\varphi \langle (1\ 2) \rangle$$

Osserviamo inoltre che:

$$\varphi : \langle (1\ 2) \rangle \longrightarrow \mathrm{Aut}(\mathcal{A}_n) : (1\ 2) \longmapsto \varphi_{(1\ 2)}, id \longmapsto id$$

con $\varphi_{(1\ 2)} : \mathcal{A}_n \longrightarrow \mathcal{A}_n : \rho \longmapsto (1\ 2)\rho(1\ 2)$.

[a] In generale va bene qualsiasi trasposizione (che esiste sempre in S_n per $n \geq 2$).

Esempio 1.83 ($D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$)

Ricordando che $D_n = \langle r, s | r^n = s^2 = id, srs^{-1} = r^{-1} \rangle$, possiamo osservare ancora una volta che le ipotesi del Teorema 1.78 sono soddisfatte. Poiché $\operatorname{ord} r = n$, allora $|\langle r \rangle| = n$, e in particolare $[D_n : \langle r \rangle] = 2 \implies \langle r \rangle \triangleleft D_n$; inoltre, $\langle r \rangle \cap \langle s \rangle = \{id\}$ perché $\det(r_i) = 1$, mentre $\det(sr_i) = -1$, $\forall i \in \{1, \dots, n\}$. Infine, essendo $\operatorname{ord} s = 2$, allora il prodotto di sottogruppi avrà cardinalità:

$$|\langle r \rangle \langle s \rangle| = \frac{|\langle r \rangle||\langle s \rangle|}{|\langle r \rangle \cap \langle s \rangle|} = \frac{2n}{1} = 2n$$

dunque $\langle r \rangle \langle s \rangle = D_n$. Pertanto $D_n \cong \langle r \rangle \rtimes_\varphi \langle s \rangle$, dove $\langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ e $\langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$, quindi:

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$$

con:

$$\varphi : \langle s \rangle \longrightarrow \operatorname{Aut}(\langle r \rangle) : s \longmapsto \varphi_s$$

dove $\varphi_s : \langle r \rangle \longrightarrow \langle r \rangle : r \longmapsto srs^{-1} (= r^{-1})$. Si osserva che deve essere $\operatorname{ord} \varphi_s | \operatorname{ord} s = 2$, quindi ci sono soltanto due possibilità:

$$\varphi_s = \begin{cases} id \\ r \longmapsto r^{-1} \end{cases}$$

nel caso in cui $\varphi_s = id$ si ottiene il prodotto diretto, nell'altro caso si ottiene il prodotto semidiretto che definisce D_n. Se in $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ ci sono altri elementi di ordine due (ad esempio se $\operatorname{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) si possono definire anche altri prodotti semidiretti:

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$$

Rimane il problema di verificare se danno o meno due gruppi isomorfi.

Esempio 1.84 (Gruppi di ordine pq)

Sia $|G| = pq$, per il Teorema Di Cauchy esistono $x, y \in G$ tali che $\operatorname{ord} x = q$, $\operatorname{ord} y = p$, assumiamo (WLOG) $q > p$, allora si ha che:

$$H = \langle x \rangle \triangleleft G$$

poiché $[G : H] = p$, con p più piccolo primo che divide $|G|$. Alternativamente si può vedere che H è caratteristico in G poiché è l'unico sottogruppo di quell'ordine; se $H' < G$ e $|H'| = q$, se fosse $H \neq H'$, allora $H \cap H' = \{e\}$ e quindi:

$$|HH'| = \frac{|H||H'|}{|H \cap H'|} = \frac{q \cdot q}{1} = q^2 > pq$$

quindi H' non può essere un sottogruppo di G. Si verifica che, detto $K = \langle y \rangle$, le ipotesi del Teorema 1.78 sono soddisfatte:

$$HK = G \qquad H \cap K = \{e\} \qquad H \triangleleft G$$

da ciò segue che ogni gruppo di ordine pq è prodotto semidiretto: $G \cong H \rtimes_\varphi K$.

Per classificare tutti i gruppi di ordine pq bisogna classificare tutti i possibili prodotti semidiretti $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ a meno di isomorfismo. Osserviamo che un prodotto semidiretto deve avere un'operazione definita da:

$$\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

Essendo $\mathbb{Z}/p\mathbb{Z} = \langle y \rangle$ e $\mathbb{Z}/q\mathbb{Z} = \langle x \rangle$ possiamo scrivere:

$$\varphi : \langle y \rangle \longrightarrow \mathrm{Aut}(\langle x \rangle)(\cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/(q-1)\mathbb{Z}) : y \longmapsto \varphi_y$$

con $\varphi_y : \langle x \rangle \longrightarrow \langle x \rangle : x \longmapsto x^l$. Per definire φ su $\langle y \rangle$ (un dominio ciclico) basta assegnare φ_y con la condizione $\mathrm{ord}\,\varphi_y \mid \mathrm{ord}\, y = p$, inoltre, $\varphi_y \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z} \implies \mathrm{ord}\,\varphi_y \mid q-1$, quindi $\mathrm{ord}\,\varphi_y \mid (p, q-1)$. Distinguiamo due casi:

- Se $p \nmid q-1$, si ha che $\mathrm{ord}\,\varphi_y \mid 1 \implies \varphi_y = id$, dunque l'unico automorfismo possibile di $\mathbb{Z}/q\mathbb{Z}$ è l'identità, pertanto si ha un prodotto diretto tra $\mathbb{Z}/p\mathbb{Z}$ e $\mathbb{Z}/q\mathbb{Z}$ e quindi esiste ed è unico il gruppo di ordine pq, $\mathbb{Z}/pq\mathbb{Z}$.
- Se $p \mid q-1$, allora o $\mathrm{ord}\,\varphi_y = 1$ e quindi ancora $\varphi_y = id$; oppure $\varphi_y = p$, e poiché ci sono $p-1$ elementi di ordine p in $\mathbb{Z}/(q-1)\mathbb{Z}$, abbiamo $p-1$ scelte per φ_y che danno un prodotto semidiretto.

Si osserva che $\mathrm{ord}\,\varphi_y = \mathrm{ord}_{\mathbb{Z}/q\mathbb{Z}^*}(\bar{l})$ e:

$$\varphi_y(x) = x^l \implies (\varphi_y(x))^k = x^{l^k}$$

quindi $\mathrm{ord}\,\varphi_y = p \iff l^p \equiv 1 \pmod q \iff \mathrm{ord}\, l = p$. Le $p-1$ scelte per φ_y danno tutte gruppi isomorfi, quindi se $p \mid q-1$ ci sono esattamente due gruppi di ordine pq a meno di isomorfismo. Infatti, detti:

$$G_1 = \langle x \rangle \rtimes_\varphi \langle y \rangle \qquad \text{e} \qquad G_2 = \langle x \rangle \rtimes_\psi \langle y \rangle$$

con $\varphi_y(x) = x^l$, $\mathrm{ord}\, l = p$ e $\psi_y(x) = x^\lambda$, $\mathrm{ord}\,\lambda = p$, pertanto $\langle l \rangle = \langle \lambda \rangle$ se e solo se $l = \lambda^r$, con $0 < r < p$. Possiamo scrivere l'applicazione:

$$\mathcal{F} : G_1 \longrightarrow G_2 : x \longmapsto x, y \longmapsto y^r$$

che definisce un isomorfismo tra i due gruppi:

$$G_1 = \left\langle x, y | x^q = y^p = 1, yxy^{-1} = x^l \right\rangle \quad \text{e} \quad G_2 = \left\langle x, y | x^q = y^p = 1, yxy^{-1} = x^\lambda \right\rangle$$

Per mostrare che è un isomorfismo basta osservare che:

$$\mathcal{F}(x^q) = (\mathcal{F}(x))^q = id \qquad \text{in quanto } x^q = id$$

e anche:

$$\mathcal{F}(y^p) = (\mathcal{F}(y))^p = id \qquad \text{in quanto } y^p = id$$

ed infine:

$$\mathcal{F}(yxy^{-1}) = \mathcal{F}(x^l)$$

in quanto:

$$\mathcal{F}(yxy^{-1}) = \mathcal{F}(y)\mathcal{F}(x)\mathcal{F}(y^{-1}) = \underbrace{y^r x y^{-r}}_{\in G_2} = x^{\lambda^r} = x^e = \mathcal{F}(x)$$

ciò garantisce che $\mathcal{F}$ ottenuto estendendo l'assegnamento $x \longmapsto x, y \longmapsto y^r$ è un omomorfismo, segue banalmente che è anche una bigezione e quindi è un isomorfismo. [6]

[6] Quest'ultima pagina non è in versione definitiva e necessita di ulteriori revisioni.

§1.13 Teorema di struttura per i gruppi abeliani finiti

Teorema 1.85 (Teorema Di Struttura Dei Gruppi Abeliani Finiti)
Sia G un gruppo abeliano finito, allora G è prodotto diretto di gruppi ciclici, cioè:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

Inoltre tale scrittura è unica se $n_{i+1} \mid n_i$, $\forall i \in \{1, \ldots, s-1\}$.

Osservazione 1.86 (Schema della dimostrazione) — Sia:

$$G(p) = \{g \in G | \operatorname{ord}(g) = p^k, k \in \mathbb{N}\}$$

$G(p)$ prende il nome di **p-componente** o componente di **p-torsione**. Si osserva che:

- $G(p)$ è un sottogruppo di G perché G è abeliano, dunque:

  $$\operatorname{ord}(xy) \mid [\operatorname{ord}(x), \operatorname{ord}(y)] \qquad \forall x, y \in G$$

  quindi se x ed y hanno per ordine una potenza di p, anche il prodotto ha per ordine una potenza di p, quindi $xy \in G(p)$, ed essendo G finito allora $G(p)$ è un sottogruppo. [a]

- $G(p)$ è un sottogruppo caratteristico di G (ciò segue dal fatto che gli automorfismi conservano l'ordine degli elementi, e quindi $G(p)$ viene mandato in $G(p)$).

[a] Si osserva che i p-sottogruppi di Sylow sono p-gruppi.

Teorema 1.87 (I gruppi abeliani sono prodotti loro delle p-componenti)
Sia G un gruppo abeliano, con $|G| = n = p_1^{e_1} \ldots p_s^{e_s}$, con i primi $p_i \neq p_j$, $\forall i \neq j$, allora:

$$G \cong G(p_1) \times \ldots \times G(p_s)$$

Inoltre la decomposizione di G come prodotto di p-gruppi di ordine tra loro coprimi è unica.

Teorema 1.88 (I p-gruppi si spezzano come prodotti di p-gruppi ciclci)
Sia G un p-gruppo abeliano. Esistono e sono univocamente determinati $r_1, \ldots, r_s$ tali che $r_1 \geq r_2 \geq \ldots \geq r_t$ [a], per i quali:

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

[a] L'ordine degli esponenti assicura l'unicità della fattorizzazione.

Segue la dimostrazione del Teorema Di Struttura Dei Gruppi Abeliani Finiti:

Dimostrazione. **Esistenza**: Dato il gruppo G, abeliano e finito, per il Teorema 1.87 si ha:

$$G \cong G(p_1) \times \ldots \times G(p_s)$$

possiamo applicare il Teorema 1.88 ad ognuno dei fattori $G(p_i)$ ed ottere:

$$G \cong G(p_1) \times \ldots \times G(p_s) \cong$$
$$\cong (\mathbb{Z}/p_1^{r_{1_1}}\mathbb{Z} \times \ldots \mathbb{Z}/p_1^{r_{1_{t_1}}}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_s^{r_{s_1}}\mathbb{Z} \times \ldots \mathbb{Z}/p_s^{r_{s_{t_r}}}\mathbb{Z})$$

con $r_{i_1} \geq \ldots \geq r_{i_{t_i}}$. Per il Teorema Cinese del Resto possiamo rimettere assieme i termini formati da primi distinti in modo da mantenere la relazione di divisibilità (e quindi unicità) richiesta dal teorema:

$$\mathbb{Z}/\underbrace{(p_1^{r_{1_1}} \ldots p_s^{r_{s_1}})}_{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/\underbrace{(p_1^{r_{1_t}} \ldots p_s^{r_{s_t}})}_{n_t}\mathbb{Z}$$

dove $t = \max\{t_1, \ldots, t_s\}$ e poniamo $r_{i_h} = 0$ se $h > t_i$. Si osserva che, per come abbiamo riscritto la fattorizzazione si ha: $n_t \mid n_{t-1} \mid \ldots \mid n_1$.
Unicità: Segue dall'unicità del Teorema 1.87 e del Teorema 1.88, infatti se ci fossero due decomposizioni di G diverse con ordini che si dividono in catena, ripercorrendo gli isomorfismi, avremmo all'inizio due diverse decomposizioni per $G(p)$ (o per G come prodotto di p-componenti). □

Esempio 1.89
Sia $G \cong \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, e raggruppando in base all'ordine degli elementi otteniamo i p-sottogruppi:

$$G \cong \underbrace{(\mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})}_{G(2)} \times \underbrace{(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})}_{G(3)} \times \underbrace{(\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})}_{G(5)}$$

e per il Teorema Di Struttura possiamo riscrivere il prodotto in ordine decrescente (rimettendo assieme p-gruppi cicli di ordine massimo):

$$G \cong \mathbb{Z}/(2^3 \cdot 3 \cdot 5^2)\mathbb{Z} \times \mathbb{Z}/(2^2 \cdot 3 \cdot 5)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Esempio 1.90

Classificare i gruppi abeliani di ordine 1000. Per fare ciò osserviamo che $1000 = 2^3 \cdot 5^3$, allora:

$$G = G(2) \times G(5)$$

con $|G(2)| = 2^3$, e $|G(5)| = 5^3$ pertanto le p-componenti possono essere scritti come prodotto di gruppi ciclici nei seguenti modi:

$$G(2) \cong \begin{cases} \mathbb{Z}/2^3\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \quad \text{e} \quad G(5) \cong \begin{cases} \mathbb{Z}/5^3\mathbb{Z} \\ \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases}$$

Dunque i gruppi abeliani di ordine 1000 (a meno di isomorfismo) sono $3 \cdot 3 = 9$, in quant per il Teorema di Struttura abbiamo una fattorizzazione unica come prodotto di gruppi cicli finiti, e per tale fattorizzazione abbiamo 3 scelte per il 3-Sylow e 3 scelte per il 5-Sylow.

Dimostriamo ora il Teorema 1.87

Dimostrazione. **Esistenza**: Sia $|G| = n$, con $n = p_1^{e_1} \dots p_s^{e_s}$, procediamo per induzione su s. Nel caso in cui $s = 1$, si ha $|G| = p_1^{e_1} \implies G = G(p_1)$. Supponiamo la tesi vera $\forall m : 2 \leq m < n$, possiamo scrivere $n = mm'$ con $(m, m') = 1$ e $m, m' < n$, allora (in notazione additiva) vogliamo verificare che:

$$G \cong mG \times m'G$$

È facile verificacare che $mG, m'G < G$ (basta verificare la chiusura per l'operazione), ed essendo G abeliano si ha anche $mG, nG \triangleleft G$; si verifica inoltre che, essendo $(m, m') = 1$, allora $\exists h, k \in \mathbb{Z}$:

$$mh + m'k = 1 \implies m(gh) + m'(gk) = g \qquad \forall g \in G \implies G \subseteq mG + m'G$$

il contrario è ovvio, dunque:

$$mG + m'G = G$$

Inoltre, sia $x \in mG \cap m'G$, ovvero $x = mg = m'g'$, allora si osserva che $m'x = m'mx = nx = 0$ e $mx = mm'x = nx = 0$, dunque:

$$\operatorname{ord}(x) \mid m \qquad \text{e} \qquad \operatorname{ord}(x) \mid m' \implies \operatorname{ord}(x) \mid (m, m') = 1 \implies x = 0$$

Quindi $mG \cap m'G = \{e\}$, pertanto sono verificate ipotesi del Teorema 1.72, dunque è vero che $G \cong mG \times m'G$. Osserviamo che:

$$mG = G_{m'} = \{g \in G | m'g = 0\} \qquad \text{e} \qquad m'G = \{g \in G | mg = 0\}$$

Verifichiamo (WLOG) $m'G = G_m$ mostrando la doppia inclusione tra insiemi; $m'G \subseteq G_m$, ovvero $m'x \in G_m$, perché $mm'x = nx = 0$, viceversa, preso $x \in G_m$, ovvero $mx = 0$, per quanto visto sopra abbiamo che:

$$\underbrace{mx}_{=0} h + m'kx = x \implies x = m'(kx) \implies x \in m'G$$

quindi $G_m \subseteq m'G \implies m'G = G_m$. Pertanto possiamo scrivere:

$$G \cong G_m \times G_{m'}$$

Poiché $|G_m|, |G_{m'}| < |G|$, perché G_m contiene tutti e soli gli elementi di G di ordine che divide m, inoltre $G_m \neq \{0\}$ (per Cauchy, dato che $1 < m < n$), quindi $G_{m'} \lneq G$ e viceversa. Possiamo quindi applicare l'ipotesi induttiva e scrivere:

$$G_m = \prod_{i \in I} G(p_i) \qquad \text{e} \qquad G_{m'} = \prod_{j \in J} G(p_j)$$

con $I \cup J = \{1, \dots, s\}$ e $I \cap J = \emptyset$ (poiché $(m, m') = 1$).
Unicità: La scrittura come prodotto di p-componenti è unica, perché se G fosse anche isomorfo ad altri p-gruppi:

$$G \cong H_1 \times \ldots \times H_n \qquad \text{con } H_i \ p_i\text{-gruppo e } H_i < G$$

allora $H_i \subseteq G(p_i)$ (in quanto $G(p_i)$ contiene tutti gli elementi di ordine potenze di p_i), ma:

$$|G| = |H_1| \dots |H_s| = |G(p_1)| \dots |G(p_s)| \implies |H_i| = |G(p_i)| \qquad \forall i \in \{1, \dots, s\}$$

quindi segue che $H_i = G(p_i)$, $\forall i \in \{1, \dots, s\}$. □

Lemma 1.91
Sia G un p-gruppo abeliano, e sia x_1 un elemento di ordine massimo in G, preso $\overline{x} \in G/\langle x_1 \rangle$ esiste $y \in \pi^{-1}(\overline{x}) : \text{ord}_G(y) = \text{ord}_{G/\langle x_1 \rangle}(\overline{x})$.

Dimostrazione. Osserviamo che $\pi^{-1}(\overline{x}) = x + \langle x_1 \rangle$, dunque $y \in \pi^{-1}(\overline{x})$ è della forma:

$$y = x + ax_1$$

Sappiamo che $\pi(y) = \pi(x) = \overline{x}$, allora $p^r = \text{ord}(\pi(y)) = \text{ord}(\overline{x}) \mid \text{ord}(y)$ (per le proprietà di omomorfismo), scegliamo y (cioè a) in modo che:

$$0 = p^r y = p^r x + p^r a x_1 \iff p^r x = -p^r a x_1$$

dove $\text{ord}(\overline{x}) = p^r \implies p^r x \in \langle x_1 \rangle \implies p^x r = b x_1$, tuttavia, dato che x_1 ha ordine massimo p^{r_1}, deve essere che $r \leq r_1$, ma:

$$0 = p^{r_1} x = p^{r_1 - 4} p^r x = p^{r_1 - r} b x_1$$

ma $\text{ord}(x_1) = p^{r_1} \implies p^r \mid b \implies b = p^r b_1$. Scegliendo $a = -b_1$ si ha:

$$p^r y = p^r x - p^r b_1 x_1 = b x_1 - \underbrace{p^r b_1}_{=b} x_1 = 0$$

□

Dimostriamo ora il Teorema 1.88:

Dimostrazione. **Esistenza**: Sia G un p-gruppo, $|G| = p^n$, proviamo la tesi per induzione su n. Per $n = 1$ si ha che $|G| = p \implies G \cong \mathbb{Z}/p\mathbb{Z}$, e quindi la tesi è verificata. Supponiamo la tesi vera per $1 \leq m < n$ e proviamola per n; sia $x_1 \in G$ un elemento di ordine massimo, $\text{ord}(x) = p^{r_1}$:

- Se $r_1 = n$, allora G è ciclo $\implies G \cong \mathbb{Z}/p^n\mathbb{Z}$.z
- Se $r_1 < n$, poiché G è abeliano si ha $\langle x_1 \rangle \triangleleft G$, quindi possiamo considerare $G/\langle x_1 \rangle$ che ha ordine $p^{n-r_1} < p^n$, dunque vale l'ipotesi induttiva ed il gruppo quoziente può essere fattorizzato come prodotto di gruppi ciclici:

  $$G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle$$ [7]

  sia $\text{ord}(\overline{x_i}) = p^{r_i}$, e supponiamo di aver scritto il prodotto diretto in modo ordinato, con $r_2 \geq \ldots \geq r_t$. Consideriamo la proiezione al quoziente:

  $$\pi : G \longrightarrow G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle$$ [8]

  per il Lemma 1.91 esistono $x_2, \ldots, x_t \in G$ tali che $\text{ord}_G(x_i) = \text{ord}_{G/\langle x_1 \rangle}(\overline{x_i}) = p^{r_i}$. Vogliamo mostrare allora che:

  $$H = \langle x_2, \ldots, x_t \rangle \cong \langle x_2 \rangle \times \ldots \times \langle x_t \rangle$$

  ovvero che il sottogruppo di G finitamente generato da $x_2, \ldots, x_t$ è isomorfo al prodotto diretto dei singoli sottogruppi ciclici generati dai medesimi elementi. Consideriamo di nuovo la proiezione al quoziente modulo $\langle x_1 \rangle$, ma ristretta ad H:

  $$\pi_{|H} : H \longrightarrow G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle : a_2x_2 + \ldots + a_tx_t \longmapsto (a_2\overline{x_2}, \ldots, a_t\overline{x_t})$$

  è un isomorfismo, infatti π è un omomorfismo, è surgettivo (in quanto si possono mandare tutti i generatori x_i di H nelle t-uple di generatori di $G/\langle x_1 \rangle$); per l'iniettivà si osserva che gli elementi del nucleo sono del tipo:

  $$\pi(a_2x_2 + \ldots + a_tx_t) = (a_2\overline{x_2}, \ldots, a_t\overline{x_t}) = (0, \ldots, 0) \iff a_i\overline{x_i} = 0 \quad \forall i \in \{2, \ldots, t\}$$

  cioè se e solo se $\text{ord}_{G/\langle x_1 \rangle}(\overline{x_i}) = p^{r_i} \mid a_i$, $\forall i \in \{2, \ldots, t\}$. Segue che $\pi_{|H}$ è un isomorfismo e si ha:

  $$H \cong \langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle \cong \langle x_2 \rangle \times \ldots \times \langle x_t \rangle$$

  Dove l'ultimo isomorfismo dervia dal fatto che abbiamo scelto elementi di ordini uguali, che quindi generano gli stessi gruppi ciclici a meno di isomorfismo. Mostriamo che $G \cong \langle x_1 \rangle \times H (\cong \langle x_2 \rangle \times \ldots \times \langle x_t \rangle)$ e per farlo verifichiamo che le ipotesi del Teorema 1.72 siano soddisfatte.
  Per mostrare che l'intersezione è banale, consideriamo un elemento in quest'ultima, ovvero un elemento che può essere scritto come:

  $$a_1x_1 = a_2x_2 + \ldots + a_tx_t$$

[7] Dunque si ha $|\langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle| = p^{n-r_1}$.
[8] L'isomorfismo tra i due gruppi è quello che manda $(G/\langle x_1 \rangle \ni) \overline{g} = a_2\overline{x_2} + \ldots + a_t\overline{x_t}$ (poiché $G/\langle x_1 \rangle$ è finito è anche finitamente generato) in $(a_2\overline{x_2}, \ldots, a_t\overline{x_t})(\in \langle \overline{x_2} \rangle \times \ldots \times \langle \overline{x_t} \rangle)$.

applicando π alle due scritture si ha:

$$\overline{0} = a_2\overline{x_2} + \ldots + a_t\overline{x_t} \iff (a_2\overline{x_2}, \ldots, a_t\overline{x_t}) = (\overline{0}, \ldots, \overline{0})$$

in quanto $G/\langle x_1\rangle \cong \prod_{i=2}^{t} \langle \overline{x_i}\rangle$, dunque l'unica possibilità di annullare la somma scritta è che $a_i \equiv 0 \pmod{p^{r_1}}$ (ovvero a_i è multiplo dell'ordine di $\overline{x_i}$), $\forall i \in \{2, \ldots, t\}$, da ciò segue che anche nel gruppo di partenza $a_i = 0$ e quindi $a_1x_1 = 0$, pertanto $\langle x_1\rangle \cap H = \{0\}$. Per mostrare che $\langle x_1\rangle + H = G$, osserviamo che $\langle x_1\rangle + H = G \subseteq G$ e che la sua cardinalità è:

$$|\langle x_1\rangle + H| = \frac{|\langle x_1\rangle||H|}{|\langle x_1\rangle \cap H|} = \frac{p^{r_1} \cdot p^{n-r_1}}{1} = p^n$$

Le ipotesi sono soddisfatte e quindi $G \cong \langle x_1\rangle \times H \cong \langle x_1\rangle \times \ldots \times \langle x_t\rangle$.

Unicità: Sia $|G| = p^n$ e procediamo ancora per induzione su n. Per $n = 1$ segue sempre $G \cong \mathbb{Z}/p\mathbb{Z}$ e quindi la tesi è verificata. Supponiamo la tesi vera per $m < n$ e proviamola per n; sia:

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_s}\mathbb{Z}$$

dove supponiamo $r_1 \geq \ldots \geq r_t$ e $k_1 \geq \ldots \geq k_s$. Deve essere necessariamente che $t = s$, perché, considerando:

$$G_p = \{g \in G | pg = 0\}$$

con G_p gruppo caratteristico (poiché gli isomorfismi conservano gli ordini degli elementi) e quindi:

$$G_p \cong (\mathbb{Z}/p\mathbb{Z})^t \cong (\mathbb{Z}/p\mathbb{Z})^s \implies t = s$$

Qunidi le lunghezze delle fattorizzazioni sono uguali, per concludere ci basta utilizzare l'ipotesi induttiva al gruppo pG (con $|pG| = p^{n-t}$):

$$pG \cong \frac{p\mathbb{Z}}{p^{r_1}\mathbb{Z}} \times \ldots \times \frac{p\mathbb{Z}}{p^{r_t}\mathbb{Z}} \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t-1}\mathbb{Z} \cong \mathbb{Z}/p^{k_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_t-1}\mathbb{Z}$$

quindi G_p ha decomposizione unica, da cui:

$$r_1 - 1 = k_1 - 1, \ldots, r_t - 1 = k_t - 1 \iff r_1 = k_1, \ldots, r_t = k_t$$

□

Osservazione 1.92 — Il Lemma 1.91 non vale in generale per quozienti qualsisi, ad esempio:

$$\mathbb{Z}/p^2\mathbb{Z}\big/\langle p\rangle \cong \frac{\mathbb{Z}/p^2\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z}$$

e con la proiezione:

$$\pi : \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \frac{\mathbb{Z}/p^2\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z} : 1 \longmapsto \overline{1}$$

con $\overline{1}$ che ha ordine p nel gruppo di arrivo, mentre:

$$\pi^{-1}(\overline{1}) = \{1 + kp\}_{k=1,\ldots,p-1}$$

con $1 + kp$ che ha ordine p^2, $\forall k : 1 \leq k \leq p$, dunque stiamo quozientando per un elemento che non ha ordine massimo; nelle condizioni del lemma, invece, stiamo quozientando per un elemento di ordine massimo.

§1.14 Teorema Di Sylow

Osservazione 1.93 — Dato un gruppo G finito cosa possiamo dire dell'esistenza di elementi e sottogruppi di un certo ordine? Riepiloghiamo di seguito i principali risulati visti:

- $H \leqslant G \implies |H| \mid |G|$ (Teorema Di Lagrange).
- $\forall p$ primo tale che $p \mid |G|$, $\exists x \in G : \text{ord}_G(x) = p$ (Teorema Di Cauchy).
- Se G è ciclco, $\forall d \mid |G|$, $\exists x \in G : \text{ord}_G(x) = d$ (per definizione di gruppo ciclico).
- G è ciclco se e solo se $d = |G|$.
- Se G è abeliano $\forall d \mid |G|$, $\exists H \leqslant G$ tale che $|H| = d$ (Lemma Di Ranieri).

L'ultimo fatto può essere ricavato (alternativamente) dal Teorema di Struttura, infatti:

$$G = G_{p_1} \times \ldots \times G_{p_r}$$

con $|G| = p_1^{e_1} \ldots p_r^{e_r}$, se $d = p_1^{a_1} \ldots p_r^{a_r}$, bisogna verificare che per ogni i esiste $H_{p_i} \leqslant G_{p_i}$ tale che $|H_{p_i}| = p^{a_i}$. Poiché:

$$G = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \ldots \mathbb{Z}/p^{n_s}\mathbb{Z} \qquad \text{con } \sum n_i = e$$

possiamo costruire sottogruppi di ogni ordine [9]; inoltre, dato che G è abeliano il prodotto di sottogruppi è un sottogruppo:

$$H_{p_1} \ldots H_{p_r} < H$$

e inoltre:

$$H_{p_1} \ldots H_{p_r} \cong H_{p_1} \times \ldots \times H_{p_r}$$

poiché $H_{p_i} \cap H_{p_j} = \{e\}$, dunque:

$$|H_{p_1} \ldots H_{p_r}| = \prod |H_{p_i}| = \prod p_i^{a_i} = d$$

e quindi otteniamo il sottogruppo di ordine d voluto.

Osservazione 1.94 — Se G non è abeliano e $d \mid |G|$ non è detto che G abbia sottogruppi di ordine d.

[9] Ad esempio $|H_p| = p^{72}$, preso $G_p = \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z}$, può essere ottenuto come $H_p = \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z} \times p^{18}\mathbb{Z}/p^{30}\mathbb{Z}$.

Esempio 1.95 ($\mathcal{A}_4$ non contiene sottogruppi di ordine 6)

Sappiamo che $|\mathcal{A}_4| = 4!/2 = 12$, se $\exists H < \mathcal{A}_4$ di ordine 6, allora $H \triangleleft \mathcal{A}_4$; per Cauchy $\exists x \in H : \text{ord}(x) = 2$, con $x = (a\ b)(c\ d)$, deve essere quindi che:

$$\mathcal{C}\ell_{\mathcal{A}_4}(x) \subset H$$

poiché $H \triangleleft \mathcal{A}_4$ e per definizione è unione di classi di coniugio in $\mathcal{A}_4$. Sappiamo che:

$$\mathcal{C}\ell_{\mathcal{A}_4}(x) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Visto che $|\mathcal{C}\ell_{\mathcal{A}_4}((a\ b)(c\ d))| = 3$, allora $\mathcal{C}\ell_{\mathcal{A}_4}((a\ b)(c\ d)) = \mathcal{C}\ell_{S_4}((a\ b)(c\ d))$, dunque se $H \triangleleft \mathcal{A}_4 \implies H \supset \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = V$ [a], allora $V < H$, ma $4 \nmid 6 \implies$ assurdo.

[a] V prende il nome di **gruppo di Klein** o **Klein 4-group**.

Lemma 1.96

Sia G un p-gruppo e $H \lneq G$, allora $H \lneq N_G(H)$.

Dimostrazione. □

Definizione 1.97. Dato G un gruppo finito e p un primo, tali che $|G| = p^n m$, con $p^n \parallel |G|$ e $n \geq 1$ e $(m, p) = 1$, allora un sottogruppo di G di ordine p^n prende il nome di **p-sottogruppo di Sylow** (**p-Sylow**).[10]

[10] I p-sottogruppi di Sylow possono anche essere pensati come p-sottogruppi di ordine massimale.

Teorema 1.98 (Teorema Di Sylow)

Sia G un gruppo finito, con $|G| = p^n m$, con p primo, $n \geq 1$ e $(m, p) = 1$ [a], allora:

(1) $\forall \alpha : 0 \leq \alpha \leq n$, $\exists H \leqslant G : |H| = p^\alpha$. (Esistenza)

(2) $\forall \alpha : 0 \leq \alpha \leq n-1$, ogni sottogruppo di ordine p^α è contenuto in un sottogruppo di ordine $p^{\alpha+1}$. In particolare, ogni p-sottogruppo è contenuto in un p-sottogruppo di Sylow. (Inclusione)

(3) Due qualunque p-sottogruppi di Sylow di G sono coniugati (quindi tutti i p-sottogruppi di ordine massimale sono isomorfi). (Coniugio)

(4) Sia n_p il numero di p-sottogruppi di Sylow di G, allora: (Numero)

$$n_p \mid |G| \qquad \text{e} \qquad n_p \equiv 1 \pmod{p} \qquad \text{e} \qquad n_p = [G : N_G(S)]$$

[a] Ovvero $p^n \parallel |G|$, o anche $\nu_p(|G|) = n$ (dove con ν_p intendiamo la valutazione p-adica).

Dimostrazione. Dimostriamo tutte le affermazioni del teorema:

(1) Dimostriamo che $\forall \alpha : 0 \leq \alpha \leq n$ esiste almeno un sottogruppo di ordine p^α; sia $\mathcal{M} = \{X \subset G | \#X = p^\alpha\}$, allora:

$$|\mathcal{M}| = \binom{|G|}{|X|} = \binom{p^n m}{p^\alpha} = \frac{p^n m(p^n m - 1)\dots(p^n m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)\dots(p^\alpha - p^\alpha + 1)}$$ [11]

Possiamo riscrivere il prodotto dei termini nel modo seguente:

$$\prod_{i=0}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

dove nell'ultimo passaggio abbiamo raccolto il primo termine, $p^{n-\alpha}m$, e lo abbiamo portato fuori dalla produttoria.
Osserviamo a questo punto che $p^{n-\alpha}$ è la più grande potenza di p che divide $|\mathcal{M}|$[12], infatti, si osserva che $p \nmid \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$, cioè $\forall \in \{1, \dots, p^\alpha - 1\}$ si ha che $p \nmid \frac{p^n m - i}{p^\alpha - i}$, come si osserva infatti:

$$\nu_p(p^n m - i) = \nu_p(p^\alpha - i) = \nu_p(i)$$

dunque, se $p \nmid i \implies p^n m - i$ e $p^\alpha - i$ non sono divisibili per p; se fosse $i = p^k j$, con $(j, p) = 1$, allora $p^\alpha - i = p^\alpha - p^k j = p^k \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p}$, con $k < \alpha$, (analogamente per $p^n m - i$), per quanto abbiamo detto deve essere necessariamente che:

$$p^{n-\alpha} \parallel |\mathcal{M}|$$

ovvero $p^{n-\alpha}$ è l'esatta potenza di p che divide $|\mathcal{M}|$. Consideriamo $M \in \mathcal{M}$, allora $gM \in \mathcal{M}$, $\forall g \in G$, dunque possiamo considerare l'azione:

$$\phi : G \longrightarrow S(\mathcal{M}) : g \longmapsto \varphi_g$$

[11] Si osserva che abbiamo semplificato al numeratore e al denominatore il termine $(p^n m - p^\alpha)!$.
[12] O anche $p^{n-\alpha} \parallel |\mathcal{M}|$, o ancora $\nu_p(|\mathcal{M}|) = n - \alpha$.

dove $\varphi_g : \mathcal{M} \longrightarrow \mathcal{M} : M \longmapsto gM$ è una bigezione. Data l'azione ϕ sappiamo che:

$$\mathcal{M} = \dot{\bigcup_{i=1}^{s}} \operatorname{Orb}(M_i) \implies |\mathcal{M}| = \sum_{i=1}^{s} |\operatorname{Orb}(M_i)| = \sum_{i=1}^{s} \frac{|G|}{|\operatorname{St}(M_i)|}$$

unendo ciò a quanto detto si ha che $p^{n-\alpha} \parallel \sum_{i=1}^{s} \frac{|G|}{|\operatorname{St}(M_i)|}$, quindi non tutte le orbite possono essere divisibili per una potenza maggiore di $p^{n-\alpha}$, ovvero esiste almeno un i tale per cui $p^{n-\alpha+1} \nmid |\operatorname{Orb}(M_i)|$(ovvero non può essere diviso per una potenza più grande di quanto detto), da ciò segue: $p^{n-\alpha+1} \nmid |\operatorname{Orb}(M_i)| = \frac{|G|}{|\operatorname{St}(M_i)|} = \frac{p^n m}{|\operatorname{St}(M_i)|}$, pertanto deve essere necessariamente che:

$$p^{\alpha} \mid |\operatorname{St}(M_i)| = t$$

cioè, affinché il rapporto non sia divisibile per p^{α}, al denominatore deve esserci una potenza di p maggiore o uguale ad α. D'altra parte, sia $x \in M_i$, la funzione:

$$\varphi_x : \operatorname{St}(M_i) \longrightarrow M_i : y \longmapsto yx$$

è iniettiva[13], dunque $t = |\operatorname{St}(M_i)| \leq |M_i| = p^{\alpha}$, segue quindi $t = p^{\alpha}$, pertanto $\operatorname{St}(M_i)$ è il sottogruppo di ordine p^{α} cercato.

(2) Sia S un p-sottogruppo di Sylow di G, con $|S| = p^n$, e sia $H \leqslant G$, con $|H| = p^{\alpha}$; consideriamo l'insieme ${}^{G}\!/_{S} = X$ dato dalle classi laterali di S in G, allora:

$$|X| = [G : S] = \frac{p^n m}{p^n} = m$$

Consideriamo l'azione di H su X data da:

$$\varphi : H \longrightarrow S(X) : h \longmapsto \varphi_h$$

con $\varphi_h : X \longrightarrow X : gS \longmapsto hgS$ bigezione; per la formula delle classi si ha:

$$m = |X| = \sum_{i=1}^{r} |\operatorname{Orb}(g_i S)| = \sum_{i=1}^{r} \frac{|H|}{|\operatorname{St}(g_i S)|} = \sum_{i=1}^{r} p^{a_i}$$

(essendo p-gruppi). Poiché per ipotesi $p \nmid m$, allora esiste i tale che $a_i = 0$ (dunque c'è un 1 nella fattorizzazione che impedisce la divisibilità di m per p) $\implies \operatorname{Orb}(g_i S) = \{g_i S\} \implies \operatorname{St}(g_i S) = H$ (ovvero per tale i si ha una classe laterale $g_i S$ la cui orbita è solo se stessa, e quindi il suo stabilizzatore è tutto H). Da ciò segue che $\forall h \in H$:

$$hg_i S = g_i S \iff hg_i \in g_i S \iff h \in g_i S g_i^{-1} \iff H \subset g_i S g_i^{-1}$$

dove $|g_i S g_i^{-1}| = |S|$ dunque $g_i S g_i^{-1}$ è un p-Sylow ed H di ordine p^{α} è contenuto in un p-Sylow. Questo dimostra il punto (3), ovvero due p-Sylow di G sono coniugati, infatti la relazione trovata vale per ogni α ed in particolare prendendo $|H| = p^n \implies H \leqslant g_i S g_i^{-1}$ ma i due sottogruppi hanno lo stesso ordine, quindi $H = g_i S g_i^{-1}$; pertanto, tutti i p-Sylow per ogni p sono coniugati tra loro in G.
Per completare la dimostrazione del punto (2) utilizziamo il risulato del Lemma 1.95, considerando $|H| = p^{\alpha}$, con $\alpha \leq n-1$ e $H \lneq S$, dunque $H \lneq N_S(H)$ [14], sia

[13] Si vede che $\varphi_x(y) = \varphi_x(z) \iff yx = zx \iff y = z$.
[14] Si noti che abbiamo preso il normalizzatore di H in S.

ora $\frac{N_S(H)}{H}$, esso è un p-gruppo non banale e per il Teorema di Cauchy esiste una classe laterale $\overline{x}(= xH)$ di ordine p, infine, per il Teorema di Corrispondenza [15], $\pi_H^{-1}(\langle\overline{x}\rangle)$ è un sottogruppo di $N_S(H)$ che contiene H (sempre per il Teorema Di Corrispondenza) ed ha ordine $p^{\alpha+1}$ (poiché stiamo considerando la controimmagine di un sottogruppo con p elementi, ciascuno dei quali fatto da classi laterali di p^α elementi, dunque la cardinalità della controimmagine si ottiene moltiplicando la fibra di ciascun elemento, che appunto ha ordine p^α, per il numero di elementi p).

(4) Sia n_p il numero dei p-sottogruppi di Sylow, per quanto detto al punto (3) i p-sottogruppi di Sylow sono tutti coniugati, dunque per ciò che abbiamo visto sul numero di coniugi rispetto all'azione di coniugio si ha $n_p = |\mathcal{C}\ell(S)| = [G : N_G(S)]$, da cui:

$$n_p = \frac{|G|}{|N_G(S)|} \implies |G| = n_p|N_G(S)| \implies n_p \mid |G|$$

Sia X l'insieme dei p-Sylow di G, consideriamo l'azione di coniugio:

$$\phi : S \longrightarrow S(X) : s \longmapsto \varphi_s$$

con $\varphi_s : X \longrightarrow X : H \longmapsto sHs^{-1}$ bigezione; ϕ ha un'unica orbita banale, ovvero quella del gruppo S, $\mathrm{Orb}(S) = \{S\}$, infatti, per ogni altra orbita si ha:

$$\mathrm{Orb}(H) = \{sHs^{-1} | s \in S\} = \{H\} \iff sHs^{-1} = H \qquad \forall s \in S$$

ovvero:

$$S \subset N_G(H) \qquad \forall s \in S$$

ma sappiamo anche che $H \lneq N_G(H)$, pertanto si deve avere che:

$$HS < N_G(H)$$

(poiché S normalizza H il prodotto di sottogruppi da un sottogruppo), ma questo è assurdo se $S \neq H$, perché avremmo:

$$|SH| = \frac{|S||H|}{|S \cap H|} = \frac{p^n \cdot p^n}{p^k} \overset{16}{=} p^{2n-k} \nmid |G|$$

Quindi esiste un'unica orbita banale e applicando la formula delle classi otteniamo:

$$n_p = |X| = \sum_{i=1}^{r} \underbrace{|\mathrm{Orb}(H_i)|}_{p^{a_i} \neq 1} + \underbrace{|\mathrm{Orb}(S)|}_{=1} = pf + 1 \qquad f \in \mathbb{Z}$$

o equivalentemente $n_p \equiv 1 \pmod{p}$.

□

[15] Tra i sottogruppi di $\frac{N_S(H)}{H}$ ed i sottogruppi di $N_S(H)$ che contengono H.
[16] $k < n$.

Corollario 1.99

Sia G un gruppo abeliano finito, $\forall p$ primo tale che $p \mid |G|$, $G(p)$ è l'unico p-Sylow di G. Inoltre G è il prodotto diretto dei suoi p-Sylow:

$$G \cong G(p_1) \times \ldots \times G(p^r)$$

con $|G| = \prod p_i^{e_i}$.