Appunti di Algebra 1

Del Corso - Patimo

Ludovico Sergiacomi

a.a. 2025/2026

Indice

1 Gruppi

1.1 Gruppi ciclici

Def. Un gruppo G si dice ciclico se $\exists g \in G$ tale che $G = < g >$, dove

$$< g >= \{ g^n \mid n \in \mathbb{C} \}$$

Dunque si avrà

$$|G| = \mathrm{ord_G}(g) = \begin{cases} \min\{ n > 0 \mid g^n = e \ \} \\ \infty \text{ se } g^n \neq e \quad \forall n > 0 \end{cases}$$

Prop. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione. Nel caso in cui $H = \{e\}$, è banale.
Invece, nel caso in cui, $H \neq \{e\} \Rightarrow \exists x \in H \setminus \{e\}$
scegliamo $n_0 = \min\{ n > 0 \mid g^n \in H \}$ e dimostriamo che $H = < g^{n_0} >$ con il doppio contenimento.

- $H \supseteq < g^{n_0} >$ ovvio, perché $g^{n_0} \in H$ e quindi anche tutte le sue potenze.
- $H \subseteq < g^{n_0} >$

  $x \in H \Rightarrow x = g^n$ con $n \in \mathbb{Z}$ poiché $x \in H \subseteq G$. Ora scriviamo, con la divisione euclidea, $n = qn_0 + r$, con $0 \leq r \leq n_0$

  $\Rightarrow g^n = {g^{n_0}}^q g^r \Rightarrow g^r \in H$ perché $g^n \in H$ e $g^{n_0} \in H$. Ma n_0 era il minimo, per cui $r = 0$.

  $\Rightarrow g^n = {g^{n_0}}^q \in < g^{n_0} >$.

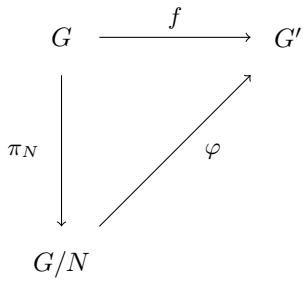
□

Prop. *I sottogruppi di $\mathbb{Z}$, diversi dal sottogruppo banale sono gli $n\mathbb{Z}$ con $n \in \mathbb{N}$.*

Osservazione. $n\mathbb{Z} \supseteq m\mathbb{Z} \Leftrightarrow n \mid m$.

1.2 Teoremi di Omomorfismo

Teorema 1.1 (I Teorema di Omomorfismo)**.** *Siano G, G' gruppi e $f : G \to G$ omomorfismo. Sia inoltre $N \triangleleft G$ con $N \subseteq \mathrm{Ker} f$. Allora $\exists\, \varphi : G/N \to G'$ t.c. il diagramma commuta*



ovvero $f = \varphi \circ \pi_N$, $\mathrm{Im} f = \mathrm{Im}\varphi$, $\mathrm{Ker} f/N = \mathrm{Ker}\varphi$.

Dimostrazione. Dobbiamo costruire $\varphi : G/N \to G'$ e verificare le sue proprietà. Sappiamo che la proiezione π_N è già definita e surgettiva, quindi poniamo $\varphi(xN) = f(x)$, in questo modo il percorso è $x \mapsto xN \mapsto f(x)$ e possono commutare.

Verifichiamo che sia ben definito:

$$\begin{aligned} xN = yN \Rightarrow & \varphi(xN) = \varphi(yN) \Leftrightarrow f(x) = f(y) \\ \Rightarrow & x = yn \Rightarrow f(x) = f(yn) = f(y)f(n) = f(y)e = f(y) \end{aligned}$$

Mi sto chiedendo: se scelgo due rappresentanti per la stessa classe, φ li manda nello stesso elemento? La prima equazione ci dice che succede *sse* $f(x) = f(y)$ e la seconda ci conferma che, date le condizioni, è proprio così. Dunque vale $\varphi(xN) = \varphi(yN)$ come si voleva.

Infine verifichiamo la condizione sui nuclei:

$$\text{Ker}\varphi = \{xN \subseteq G/N \mid \varphi(xN) = e\} = \{xN \mid f(x) = e\} = \{xN \mid x \in \text{Ker}f\} = \text{Ker}f/N$$

□

Teorema 1.2. *Sia G un gruppo ciclico, allora*
$G \cong \mathbb{Z}$ *(e quindi* $|G| = \infty$ *) oppure* $G \cong \mathbb{Z}/n\mathbb{Z}$ *(e quindi* $|G| = n$*)*

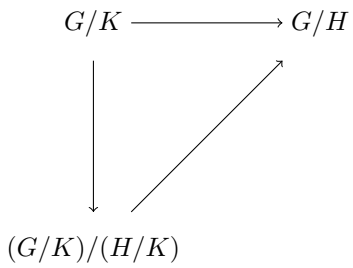
Dimostrazione. Costruisco $\varphi : \mathbb{Z} \to G = < x >$ di modo che:
$1 \mapsto x$ e verifico che $\text{ord}(x) \mid \text{ord}(1) = \infty$
$n \mapsto x^n$ e ottengo φ omomorfismo surgettivo.

Quindi, per il *I Teorema di Omomorfismo*, $G \cong \mathbb{Z}/Ker\varphi$.
Osservando che $Ker\varphi \subseteq \mathbb{Z} \Rightarrow Ker\varphi = n\mathbb{Z}$ per la proposizione precedente, concludiamo $G \cong \mathbb{Z}/n\mathbb{Z}$.
Nel caso in cui φ sia anche iniettivo, $Ker\varphi = \{e\} \Rightarrow G \cong \mathbb{Z}$. □

Teorema 1.3 (II Teorema di Omomorfismo)**.** *Sia G gruppo, e siano $H, K \triangleleft G$, con $K \subseteq H$. Allora*

$$G/H \cong (G/K)/(H/K).$$

Dimostrazione. Vogliamo utilizzare il *I Teorema* in questo modo:



L'idea è partire da $\pi_H : G \to G/H$ che sappiamo essere un omomorfismo, per poi quozientare per K. In questo modo avremo un omomorfismo $\pi' : G/K \to G/H$ tale che $\text{Ker}\pi' = \text{Ker}\pi_H/K$.

Spieghiamo meglio questo passaggio. Abbiamo $\pi_H : G \to G/H$ tale che $\pi_H(g) = gH$. Nel momento in cui quozientiamo per K, otteniamo un diverso omomorfismo $\pi' : G/K \to G/H$ (notiamo che la differenza è sul dominio), tale che $\pi'(gK) = \pi_H(g) = gH$; il nucleo allora diventa

$$\text{Ker}\pi' = \{gK \in G/K \mid \pi'(gK) = e_{G/H}\} = \{gK \in G/K \mid \pi_H(g) = H\} = \text{Ker}\pi_H/K$$

Osserviamo che $\text{Ker}\pi_H = H$ e di conseguenza $\text{Ker}\pi' = H/K$. Abbiamo finito, perché la situazione attuale è proprio quella descritta dal diagramma. Per concludere, il *I Teorema* ci garantisce l'esistenza dell'isomorfismo cercato. □

Teorema 1.4 (III Teorema di Omomorfismo)**.** *Sia G gruppo e H, K sottogruppi normali in G. Allora vale*

$$HK/K \cong H/(H \cap K)$$

Dimostrazione. Definiamo un'applicazione

$$\begin{aligned} \varphi : H &\longrightarrow HK/K \\ h &\longmapsto hK \end{aligned}$$

Vogliamo dimostrare che 1) φ è omomorfismo, 2) φ è surgettivo, 3) $\text{Ker}\varphi = H \cap K$.

1. $\varphi(hh') = hh'K = hKh'K = \varphi(h)\varphi(h')$.

2. $\forall h \in H, \forall k \in K, \quad \exists x \in H$ t.c. $\varphi(x) = hkK = hK$ e basta scegliere $x = h$.

3. $\text{Ker}\varphi = \{h \in H \mid \varphi(h)hK = e_{HK/K} = K\} \Leftrightarrow h \in K$. Dunque $h \in H \cap K$.

Il punto 1. è possibile grazie alla normalità di H e K, infatti, sfruttando il fatto che $h'K = Kh'$, cioè la normalità di K, abbiamo

$$hKh'K = hK(h'K) = hK(Kh') = hKKh' = hKh' = h(Kh') = h(h'K) = hh'K$$

.

□

1.2.1 Prodotto diretto di gruppi

Def. Siano G e G' gruppi, allora si definisce il prodotto diretto come

$$G \times G' = \{\, (g, g') \mid g \in G,\ g' \in G' \,\}.$$

Proprietà

- $(a, b) \in G \times G' \Rightarrow \text{ord}(a, b) = \text{mcm}(\text{ord}(a), \text{ord}(b))$
- L'operazione è definita componente per componente:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1',\ g_2 \cdot g_2')$$

Esempio. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ È ciclico? No, per il *TCR* che ci dice $\mathbb{Z}_m \times \mathbb{Z}_n$ ciclico $\Leftrightarrow \text{mcd}(m, n) = 1$. Infatti i suoi elementi – escluso $e = (0,0)$ – sono di ordine 2.

Esempio. $\mathbb{Z}_p \times \mathbb{Z}_p$ non è ciclico, ma ha $p^2 - 1$ elementi di ordine p. Ognuno genera un sottogruppo di ordine p. Quanti sono?

$$\#\text{ sottogruppi di ord } n \text{ ciclici} \quad = \quad \frac{\#\text{ el. di ord } n}{\varphi(n)}$$

1.2.2 Sottogruppi di ordine p^r di $\mathbb{Z}_p^n$

$(\mathbb{Z}/p\mathbb{Z})^n = \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$ è anche spazio vettoriale su $\mathbb{F}_p$ – ovvero il campo con p elementi –, con il prodotto esterno definito "gratis" in questo modo: $k \in \mathbb{Z}_p \to kx \in \mathbb{Z}_p^n = \underbrace{x + \ldots + x}_{\text{k volte}}$.

Quindi il problema di cercare i sottogruppi si traduce nella ricerca di sottospazi di ordine p^r. L'idea è considerare tutte le r-uple di elementi linearmente indipendenti, così da avere tutti i sottospazi possibili (con molti duplicati) e poi dividere per il numero di basi di ordine r. Cioè sto dicendo: prendiamo tutte le basi possibili di sottospazi e poi dividiamo per le possibili basi di ogni sottospazio, così da ottenere solo i sottospazi.

1. **r-uple in $\mathbb{Z}_p^n$**
   per il primo elemento vanno bene tutti, tranne $\underline{0} \longrightarrow p^n - 1$ possibilità;
   per il secondo bisogna escludere la retta di p punti generata dal primo, per avere la linerare indipendenza $\longrightarrow p^n - p$ possibilità;
   si continua in questo modo, escludendo un $p^2, p^3 \ldots p^{r-1}$ elementi.

2. **basi di ordine r**
   si applica la stessa idea, ma questa volta partendo da p^r invece di p^n: stiamo considerando, come il nostro spazio ambiente, un generico sottospazio di dimensione p^r.

Dunque ecco la formula cercata:

$$\frac{p^n - 1 \cdot p^n - p \cdot p^n - p^2 \cdot \ldots \cdot p^n - p^{r-1}}{p^r - 1 \cdot p^r - p \cdot p^r - p^2 \cdot \ldots \cdot p^r - p^{r-1}}$$

Def. Dati due elementi $a, b \in G$ gruppo, si dice commutatore l'elemento $[ab] = aba^{-1}b^{-1}$.

Osservazione. Se il commutatore di due elementi è banale, gli elementi commutano.

Teorema 1.5. *Sia G gruppo e $H, K \triangleleft G$ t.c.*

1. $HK = G$
2. $H \cap K = \{e\}$

Allora $G \cong H \times K$.

Lemma 1.5.1. *Nelle ipotesi del teorema, $\forall h \in H, \forall k \in K$ vale $hk = kh$.*

Dimostrazione. Lavoriamo sul commutatore $[hk]$. Siccome $K \triangleleft G$ abbiamo

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

Similmente, sfruttando $H \triangleleft G$:

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

Dunque $[hk] \in H \cap K \Rightarrow hkh^{-1}k^{-1} = e \Rightarrow hk = kh$ perché l'intersezione è banale per ipotesi. □

Dimostrazione. Definiamo

$$\begin{aligned} f : H \times K &\longrightarrow G \\ (h, k) &\longmapsto hk \end{aligned}$$

e verifichiamo che è un isomorfismo.

- f omomorfismo segue dal *Lemma*

$$f\big((h,k),(h',k')\big) = hh'kk' = hkh'k' = f\big((h,k)\big) f\big((h',k')\big)$$

- f surgettiva per l'ipotesi 1.

$$f(H, K) = HK = G$$

- f iniettiva per l'ipotesi 2.

$$f\big((h,k)\big) = e \Leftrightarrow hk = e \Leftrightarrow h = k^{-1} \Leftrightarrow h, k \in H \cap K = \{e\} \Leftrightarrow (h,k) = (e,e) = e_{H\times K}$$

□

1.2.3 Teorema di Corrispondenza

Teorema 1.6 (Teorema di corrispondenza per i gruppi)**.** *Sia $f : G \to G'$ omomorfismo* ***surgettivo****.*
Allora f induce una corrispondenza biunivoca tra i sottogruppi di G' e i sottogruppi di G che contengono $\mathrm{Ker} f$*.*
La corrispondenza si restringe ai sottogruppi normali e l'indice di sottogruppo (numero di classi laterali).

Lemma 1.6.1. *$f : G \to G'$ omomorfismo, allora*

1. *$\forall H \leq G' \quad f^{-1}(H) \leq G$. Inoltre, $H \triangleleft G' \Rightarrow f^{-1}(H) \triangleleft G$.*
2. *$\forall H \leq G \quad f(H) \leq G'$. Inoltre, $H \triangleleft G \Rightarrow f(H) \triangleleft f(G)$.*

Dimostrazione. Dimostrazione in corso... □

Dimostrazione. Basta dimostrare il teorema per $f = \pi_N$, infatti possiamo usare il *I Teorema di Omomorfismo* per ottenere $G/N \cong G'$.
Abbiamo due insiemi che vogliamo mettere in corrispondenza biunivoca:

$$\{H \mid H \leq G, N \subseteq H\} \leftrightarrow \{\mathcal{H} \mid \mathcal{H} \leq G/N\}.$$

Consideriamo due applicazioni

$$\alpha : G \to G/N$$
$$\beta : G/N \to G$$

Vogliamo dimostrare che α e β sono una l'inversa dell'altra, ovvero

$$(\alpha \circ \beta)(\mathcal{H}) = \mathcal{H}$$
$$(\beta \circ \alpha)(H) = H$$

Definiamo $\alpha(H) := \pi_N(H) = \{\pi_N(h) \mid h \in H\} = \{hN \mid h \in H\} = \{xN \mid x \in HN\} = HN/N = H/N$ (poiché $H \supseteq N$) e osserviamo che α è ben definita per il punto 2. del *Lemma*.

Similmente, $\beta(\mathcal{H}) = \pi_n^{-1}(\mathcal{H})$ è ben definita per il punto 1. del *Lemma*.

Verifichiamo ora che siano effettivamente inverse:

1. $(\alpha \circ \beta)(\mathcal{H}) = \pi_N(\pi_N^{-1}(\mathcal{H})) = \mathcal{H}$ visto che la mappa è surgettiva: sto andando da $\mathcal{H}$ a $x \in G$ t.c. $\pi_N(x) = \mathcal{H}$ e poi, viceversa, da x in $\mathcal{H}$.
2. $(\beta \circ \alpha)(H) = \pi_N^{-1}(H/N) = \{x \in G \mid \pi_N(x) = hN \mid h \in H\} = \{x \in G \mid xN = hN\} = \{x \in NH = H\} = H$.

La seconda parte del teorema ci sta dicendo che i sottogruppi normali in G sono in corrispondenza con i sottogruppi normali in G' e che gli indici di sottogruppi in corrispondenza sono, a loro volta, corrispondenti.

□

1.2.4 Teorema di Cauchy per i gruppi abeliani

Teorema 1.7 (Cauchy per gli abeliani)**.** *Sia G gruppo finito e abeliano, p primo t.c. $p \mid |G|$. Allora $\exists x \in G$ t.c.* $\text{ord}(x) = p$.

Dimostrazione. Scriviamo $|G| = pm,\ m \geq 1$ e dimostriamo per induzione su m.

Caso $m = 1$ $\quad |G| = p \Rightarrow G = < x > \quad \text{ord}(x) = p$

Caso $m > 1$ supponiamo la tesi vera per pt con $t < m$. Preso $x \in G, x \neq e$, considero il gruppo ciclico $< x >$. A questo punto abbiamo due possibilità:

1. $p \mid | < x > | = \text{ord}(x)$
2. $p \nmid | < x > | = \text{ord}(x)$

Che risolviamo in questo modo:

1. Ho un gruppo ciclico, di ordine $\text{ord}x = n$, allora mi basta considerare $x^{\frac{n}{p}}$ e ho ottenuto un elemento di ordine p.
2. Considero il gruppo quoziente (G è abeliano, quindi tutti i sottogruppi sono normali e posso stare tranquillo) $G/ < x >$. Ora, siccome $p \mid |G|$ ma $p \nmid | < x > |$, si deve avere $p \mid |G/ < x > |$. Quindi, sfruttando l'induzione forte, ci sarà un elemento $y \in |G/ < x > |$ tale che $\text{ord}[y] = p$. Da cui $p \mid \text{ord}y$ e, con una divisione simile a quella di prima, ottengo un elemento di ordine esattamente p.

□

1.3 Automorfismi

Def. $H \leq G$ si dice caratteristico se è invariante per l'azione del gruppo degli automorfismi. Ovvero

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

Osservazione. Generalizza il concetto di normalità (invarianza per coniugio) in una invarianza generica. Infatti possiamo considerare l'automorfismo φ_g, ovvero il coniugio per g, come un caso particolare di f.

Prop. *Gli **automorfismi** di $\mathbb{Z}/n\mathbb{Z}$ sono isomorfi a $\mathbb{Z}_n^*$.*

Dimostrazione. □

Prop. *Dati H, K gruppi, c'è l'immersione naturale*

$$\mathrm{Aut}(H) \times \mathrm{Aut}(K) \hookrightarrow \mathrm{Aut}(H \times K).$$

*Inoltre, se H e K sono **caratteristici** in $H \times K$, allora ho un isomorfismo.*

Dimostrazione. □

1.4 Azioni di gruppo

Def. Siano G un gruppo e X un insieme, allora si definisce azione di G su X un omomorfismo

$$\begin{aligned} \varphi : G &\longrightarrow S(X) \text{ permutazioni di } X \\ g &\longmapsto \varphi_g : X \to X \end{aligned}$$

dove φ_g, anche scritta $g \cdot (x)$, è una mappa bigettiva.

Esempio. Dati G e $X = G$, abbiamo il coniugio

$$\begin{aligned} \varphi : G &\longrightarrow S(G) \\ g &\longmapsto \varphi_g. \end{aligned}$$

Osservazione.

- $\varphi(g) \circ \varphi(h) = \varphi(gh) \Rightarrow \varphi_g(x) \circ \varphi_h(x) = \varphi_{gh}(x)$;
- $\varphi_{g^{-1}} = \varphi_g^{-1}$ infatti $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{gg^{-1}} = \varphi_e = \mathrm{Id}_{S(X)}$.

1.4.1 Classi di equivalenza, orbite e stabilizzatori

Prop. *$\varphi : G \to S(X)$ induce una relazione di equivalenza su X, definita in questo modo:*

$$x_1, x_2 \in X \qquad x_1 \sim x_2 \;\; se \;\; \exists g \in G \;\; t.c. \;\; \varphi_g(x_1) = x_2.$$

Dimostrazione.

1. $x \sim x$ infatti $\varphi_e(x) = x$;
2. $x \sim y \Rightarrow \varphi_g(x) = y \Rightarrow \varphi_{g^{-1}}(y) = x \Rightarrow y \sim x$;
3. $x \sim y,\ y \sim z \Rightarrow \varphi_g(x) = y,\ \varphi_{g'}(y) = z \Rightarrow z = \varphi_{g'}(\varphi_g(x)) = \varphi_{gg'}(x) \Rightarrow x \sim z$.

□

Def. Le classi di equivalenza si chiamano orbite e si indicano con $\mathrm{Orb}(x)$.

$$\begin{aligned} \mathrm{Orb}(x) &= \{y \in X \mid \varphi_g(x) = y,\ g \in G\} \\ &= \{\varphi_g(x) \mid g \in G\}. \end{aligned}$$

Osservazione. Le classi di equivalenza costituiscono una partizione (due classi o sono disgiunte oppure coincidono), ovvero

$$X = \dot{\bigcup} \{\mathrm{Orb}(x) \mid x \in \mathcal{R} \subset G\}$$

dove $\mathcal{R}$ è un insieme di rappresentanti per le orbite.

Def. Dato un elemento $x \in X$, si dice stabilizzatore di x l'insieme

$$\mathrm{St}(x) = \{g \in G \mid \varphi_g(x) = x\} \leq G.$$

Prop. $\mathrm{St}(x)$ *è un sottogruppo di* G.

Dimostrazione.

1. $e \in \mathrm{St}(x)$, infatti $\varphi_e(x) = x \quad \forall x \in X$;
2. $g, h \in \mathrm{St}(x) \Rightarrow \varphi_g(x) = x,\ \varphi_h(x) = x \Rightarrow (\varphi_g \circ \varphi_h)(x) = x \Rightarrow \varphi_{gh}(x) = x \Rightarrow gh \in \mathrm{St}(x)$;
3. $g \in \mathrm{St}(x) \Rightarrow \varphi_g(x) = x \Rightarrow \varphi_g^{-1}(x) = x = \varphi_{g^{-1}}(x) \Rightarrow g^{-1} \in \mathrm{St}(x)$.

□

1.4.2 Formula delle classi

C'è una stretta relazione tra **orbite** e **stabilizzatori**, infatti

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

ovvero g è incluso in uno dei laterali dello stabilizzatore. La relazione sarà più chiara grazie alla seguente proposizione.

Prop. *Gli insiemi dei laterali, di fatti, sono in corrispondenza biunivoca con le orbite:*

$$\mathrm{Orb}(x) \longleftrightarrow H\mathrm{St}(x)$$

Dimostrazione. Definisco una mappa

$$\begin{aligned} \varphi : \mathrm{Orb}(x) &\longrightarrow G\mathrm{St}(x) \\ \varphi_g(x) &\longmapsto g\mathrm{St}(x) \end{aligned}$$

e verifico che φ è biiettiva. Per l'iniettività seguo le frecce $\Leftarrow$ della catena scritta sopra: infatti, presi $g\mathrm{St}(x) = h\mathrm{St}(x)$, ciò può anche essere scritto come $g \in h\mathrm{St}(x)$; quindi, partendo dalla fine e risalendo i *sse*, otteniamo $\varphi_g(x) = \varphi_h(x)$ cioè: presi due elementi uguali nel codominio, sono necessariamente immagini di elementi uguali nel dominio, ovvero φ è iniettiva.

Per la surgettività osservo che, preso un generico $g\mathrm{St}(x)$, basta prendere l'elemento $\varphi_g(x)$ nell'orbita, affinché φ funzioni. □

Corollario 1.7.1. *Sia* G *finito, allora vale*

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

Dimostrazione. Infatti

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

e, per quanto appena visto, l'indice di $\mathrm{St}(x)$ in G (ovvero il numero di laterali) è uguale alla cardinalità dell'orbita. □

Osservazione. In particolare, il fatto che $|\mathrm{Orb}(x)|$ divida $|G|$ ci interessa molto.

Tutto ciò risulta molto utile, applicato nel caso del coniugio, da cui possiamo sviluppare quella che viene chiamata **formula delle classi**:

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

Dimostrazione. Osserviamo preliminarmente che

- $\mathrm{Orb}(x) = \mathrm{Cl}(x)$, cioè le orbite sono le classi di coniugio;
- $\mathrm{St}(x) = \{g \in G \mid \varphi_g(x) = gxg^{-1} = x\} = Z_G(x)$, cioè gli stabilizzatori sono i centralizzatori in G.

Poiché le orbite costituiscono una partizione del gruppo, possiamo scrivere

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

dove, al solito, $\mathcal{R}$ è un insieme di rappresentanti per le classi di coniugio.

Osserviamo che un elemento x appartiene al centro $Z(G)$ *sse* la sua orbita è banale, ovvero $\mathrm{Orb}(x) = \{x\}$. Di conseguenza, il suo centralizzatore è tutto il gruppo e ha cardinalità $|G|$.

Quindi possiamo spezzare la sommatoria di prima in questo modo:

$$\begin{aligned} |G| &= \sum_{x \in Z(G)} \frac{|G|}{|Z_G(x)|} \; + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \\ &= \sum_{x \in Z(G)} 1 \; + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \\ &= |Z(G)| \; + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \end{aligned}$$

□

La formula si estende anche ai sottogruppi normali: iniziamo dimostrando la seguente

Prop. *Dato G gruppo, $\mathcal{R}$ insieme di rappresentanti delle classi di coniugio, vale*

$$H \triangleleft G \Leftrightarrow H = \dot{\bigcup_{x \in \mathcal{R}_H}} \mathrm{Orb}(x),$$

dove $\mathcal{R}_H = \mathcal{R} \cap H$.

Dimostrazione.
$\boxed{\Rightarrow}$ Dobbiamo dimostrare che ogni elemento di H appartiene ad almeno un'orbita e, se un elemento appartiene a due orbite, allora esse sono uguali.

- Osserviamo che di sicuro $h \in \mathrm{Orb}(h)$, infatti $h = ehe^{-1}$.
- Supponiamo ora che $h \in \mathrm{Orb}(h)$ e $h \in \mathrm{Orb}(h')$. Allora abbiamo

  $$h \in \mathrm{Orb}(h') \Rightarrow \bar{g}h'\bar{g}^{-1} = h \text{ per un qualche } \bar{g}.$$

  Sfruttando l'appartenenza anche all'altra orbita:

  $$\mathrm{Orb}(h) = \{ghg^{-1} \mid g \in G\} = \{g\bar{g}h'\bar{g}^{-1}g^{-1} \mid g \in G\} = \{\tilde{g}h'\tilde{g}^{-1} \mid \tilde{g} \in G\} = \mathrm{Orb}(h').$$

$\boxed{\Leftarrow}$ Viceversa, se ogni $h \in H$ appartiene ad una e una sola classe di coniugio, allora

$$\forall h \in H \quad h = gh'g^{-1} \text{ per qualche } h' \in H \text{ e qualche } g \in G.$$

Possiamo scrivere,

$$H = \{ghg^{-1} \mid g \in G,\ h \in H\}$$

e quindi,

$$H = gHg^{-1} \text{ al variare di } g \text{ in } G \quad \Rightarrow \quad Hg = gH \text{ ovvero } H \triangleleft G.$$

□

A questo punto vale la **formula delle classi** come segue:

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

cioè includiamo solo gli addendi relativi alle classi di coniugio in H.

Caso dei p-gruppi Gruppi finiti di ordine p^n con p primo e $n \in \mathbb{N}$.
Applichiamo la *formula delle classi* e osserviamo che:

- $p \mid |G|$ ovviamente;
- dato $x \in G \setminus Z(G)$, allora vale $p \mid |Z_G(x)|$, poiché $|Z_G(x)|$ divide la cardinalità del gruppo e dunque non può che essere, a sua volta, del tipo $p^k,\ k < n$. L'ultima condizione vale perché, altrimenti, il centralizzatore di x sarebbe tutto il gruppo, ma questo succede solo per $x \in Z(G)$.

Dunque

$$p^n = \underbrace{|G|}_{\text{divisa da p}} = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \underbrace{\frac{|G|}{|Z_G(x)|}}_{\text{divisi da p}} \Rightarrow p \mid |Z(G)|.$$

Osservazione. Ci sta dicendo che il centro di un p-gruppo è non banale.

Siamo quasi pronti per dimostrare il *Teorema di Cauchy* nel caso generale. Dimostriamo il seguente

Lemma 1.7.1. *G non abeliano $\Rightarrow$ $G/Z(G)$ non è ciclico.*

Dimostrazione. Supponiamo che $G/Z(G)$ sia ciclico, ovvero $G/Z(G) =< gZ >$. Allora, presi $x, y \in G$, scriviamo

$$x \in g^k Z(G) \Rightarrow x = g^k z_1$$
$$y \in g^h Z(G) \Rightarrow y = g^h z_2$$

per qualche $h, k \in \mathbb{Z}$. Questo perché i laterali di $Z(G)$ partizionano G, quindi ogni elemento dell'ultimo appartiene ad uno dei laterali del primo.

Lavoriamo sul prodotto:

$$xy = g^k z_1 g^h z_2 = g^k g^h z_1 z_2 = g^{kh} z_1 z_2 = g^{hk} z_1 z_2 = g^h g^k z_1 z_2 = g^h g^k z_2 z_1 = g^h z_2 g^k z_1 = yx.$$

Ovvero tutti gli elementi commutano, quindi G è abeliano, contro l'ipotesi. □

1.4.3 Teorema di Cauchy

Teorema 1.8 (Teorema di Cauchy)**.** *Sia G gruppo e p primo tale che $p \mid |G|$. Allora $\exists g \in G$ t.c. $\mathrm{o}(g) = p$.*

Dimostrazione. Nel caso in cui G sia abeliano, già sappiamo che il teorema è verificato (si veda nelle pagine precedenti). Supponiamo quindi G non abeliano.

Dato $H < G$, lavoriamo per induzione forte sulla sua cardinalità. Ci sono due possibilità:

1. $p \mid |H| \Rightarrow \exists h \in H \subset G$ t.c. $\mathrm{o}(h) = p$ e dunque h è l'elemento cercato;

2. $\forall H < G \quad p \nmid |H|$; allora sfruttiamo la formula delle classi

$$pn = |G| = \underbrace{|Z(G)|}_{\text{non divisa da } p} + \underbrace{\sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}}_{\text{divisa da } p}.$$

Letta modulo p, l'equazione diventa

$$0 = |G| = |Z(G)| + 0 \Rightarrow p \mid Z(G),$$

ma si era detto che p non dividesse la cardinalità di nessun sottogruppo proprio, quindi $Z(G)$ non è proprio, ovvero $Z(G) = G$, cioè G abeliano, contro la nostra ipotesi (avevamo supposto G non abeliano, perché il caso abeliano è già stato dimostrato).

□

1.4.4 Teorema di Cayley

Teorema 1.9 (Cayley)**.** *Ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni. In particolare, detta $|G| = n$, G è isomorfo a un sottogruppo di S_n.*

Dimostrazione. Consideriamo l'applicazione

$$\begin{aligned} \lambda : G &\to S(G) \\ g &\mapsto \varphi_g : G \to G \\ &\qquad x \mapsto gx \end{aligned}$$

e dimostriamo che è un omomorfismo iniettivo.

- λ è ben definito: dobbiamo far vedere che φ_g effettivamente $\in S(G)$.
  φ_g è iniettiva perché
  $$\varphi_g(x) = \varphi_g(y) \;\Leftrightarrow\; gx = gy \;\Leftrightarrow\; x = y,$$
  per legge di cancellazione;
  è surgettiva perché, preso $y \in G$, basta considerare l'elemento $g^{-1}y \in G$, per averne la controimmagine.
- λ è omomorfismo:
  $$\begin{array}{c} \lambda(g_1 g_2) \underset{\downarrow}{=} \varphi_{g_1} \circ \varphi_{g_2} = \lambda(g_1)\lambda(g_2). \\ \varphi_{g_1 g_2}(x) = g_1 g_2 x = \varphi_{g_1}(\varphi_{g_2}(x)) \end{array}$$
- λ è iniettivo:
  $$\ker \lambda = \{g \in G \mid \varphi_g = \mathrm{Id}\} = \{g \in G \mid x = gx \ \forall x \in G\} = \{e\}.$$

□

1.5 Sottogruppo derivato

Def. Si dice sottogruppo derivato di G, il gruppo dei commutatori $[xy]$:

$$G' = \{xyx^{-1}y^{-1} \mid x, y \in G\}.$$

Prop.

1. *G' è banale* sse *G è abeliano;*
2. *G' è caratteristico in G;*
3. *G/G' è abeliano e inoltre G' è il più piccolo sottogruppo di G con questa proprietà (cioè G/N abeliano $\Leftrightarrow G' \subseteq N$).*

Dimostrazione.

1. Ovvio: tutto commuta con tutto e G' viene fuori $= \{e\}$.

2. Presa $f \in \mathrm{Aut}G$, allora $f(G') \subseteq G'$, ovvero

$$f(xyx^{-1}y^{-1}) \in G' \ \forall x, y \in G = f(x)f(y)\underset{\downarrow}{f(x^{-1})}\underset{\downarrow}{f(y^{-1})} = [\underset{\downarrow}{f(x)}\underset{\downarrow}{f(g)}] \in G'.$$
$$f(x)^{-1} \quad f(y)^{-1} \qquad \in G \quad \in G$$

   Quindi è invariante per automorfismi, ovvero caratteristico.

3. G/N abeliano significa che, presi due suoi elementi xN, yN, il loro commutatore è banale, ovvero $\big[[x][y]\big] = xNyNx^{-1}Ny^{-1}N = N = \{[e]\}$.
   Vista la normalità di N, posso farlo commutare e riscrivere l'espressione di prima come:

$$xyx^{-1}y^{-1}N = N \ \Leftrightarrow \ xyx^{-1}y^{-1} \underset{\downarrow}{\in} N \ \forall x, y \in G \ \Leftrightarrow \ G' \subseteq N$$
$$\text{cioè i gen. del derivato stanno in } N$$

□

1.6 Prodotti semidiretti

Def. Dati H, K gruppi e

$$\begin{aligned} \varphi : K &\to \mathrm{Aut}(H) \\ k &\to \varphi_k, \end{aligned}$$

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

$$H \rtimes_\varphi K.$$

Come insieme è il prodotto cartesiano $H \times K$, i cui elementi sono (h, k), ma l'operazione è definita nel modo seguente.

$$(h, k)(h', k') = (h *_H \varphi_k(h'), k *_K k').$$

Teorema 1.10. *$H \rtimes K$ è un **gruppo**.*

Dimostrazione.

- È **chiuso** per l'operazione definita: $kk' \in K$, $\varphi_k(h') \in H \Rightarrow h\varphi_k(h') \in H$.
- È associativa (da fare).
- C'è il **neutro**: (e_H, e_K), infatti

$$\begin{aligned} (e_H, e_K)(h, k) &= (e_H\varphi_{e_K}(h), e_K k) = (e_H \mathrm{Id}(h), k) = (h, k) \\ (h, k)(e_H, e_K) &= (h\varphi_k(e_H), ke_K) = (he_H, k) = (h, k). \end{aligned}$$

- Ci sono gli **inversi**: (h, k) ha come inverso (h', k') fatto in questo modo:

$$\begin{aligned} &(e_h, e_K) = (h, k)(h', k') = (h\varphi_k(h'), kk') \ \Rightarrow \ k' = k^{-1} \\ &h\varphi_k(h') = e_H \ \Leftrightarrow \ \varphi_k(h') = h^{-1} \Leftrightarrow \varphi_k^{-1}(\varphi_k(h')) = \varphi_k^{-1}(h^{-1}) \ \Leftrightarrow \ h' = \varphi_{k^{-1}}(h^{-1}) \end{aligned}$$

  e verifico il viceversa:

$$(h', k')(h, k) = \left(\varphi_{k^{-1}}(h^{-1}), k^{-1}\right)(h, k) = \left(\varphi_{k^{-1}}(h^{-1}\varphi_{k^{-1}}(h), kk^{-1}\right) = \left(\varphi_{k^{-1}}(h^{-1}h), e_K\right) = (e_H, e_K).$$

□

Osservazione. $H \rtimes_\varphi K = H \times K \ \Leftrightarrow \ \varphi_k = \mathrm{Id} \ \forall k \in K$. Infatti ho il prodotto diretto *sse* $(h, k)(h', k') = (hh', kk')$, cioè deve valere:

$$h\varphi_k(h') = hh' \ \Leftrightarrow \ \varphi_k(h') = h' \ \Leftrightarrow \ \varphi_k = \mathrm{Id}.$$

Osservazione. I gruppi così definiti:

$$\overline{H} = H \times \{e_K\} \qquad \overline{K} = \{e_H\} \times K$$

sono sottogruppi di $G = H \rtimes_\varphi K$. Infatti:

$$(h, e_K)(h', e_K) = (h\varphi_{e_K}(h'), e_K e_K) = (hh', e_K) \in \overline{H}$$
$$(e_H, k)(e_H, k') = (e_H \varphi_k(e_H), kk') = (e_H, kk') \in \overline{K}.$$

Similmente, per gli inversi:

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

Inoltre $\overline{H} \triangleleft G$, in quanto $H = \ker \pi$, dove

$$\pi : H \rtimes_\varphi K \to K$$
$$(h, k) \mapsto k$$

e controllo π è omomorfismo perché $\pi\left((h,k)(h',k')\right) = \pi(h\varphi_k(h')kk') = kk' = \pi(h,k)\pi(h',k')$.
$\overline{K}$ in generale non è normale (lo è solo se il prodotto è diretto. Infatti in quel caso si può applicare il teorema visto in precedenza).

$$\overline{H} \times \overline{K} = G, \quad \overline{H} \cap \overline{K} = e = (e_H, e_K).$$

Teorema 1.11. *Sia G gruppo, $H, K < G$, tale che*

1. $H \trianglelefteq G$
2. $H \times K = G$
3. $H \cap K = \{e_G\}$,

allora $G = H \rtimes_\varphi K$, dove

$$\varphi : K \to \mathrm{Aut}(H)$$
$$k \mapsto \varphi_k(h \mapsto khk^{-1})$$

Dimostrazione. Consideriamo

$$F : \ H \rtimes_\varphi K \to G$$
$$(h, k) \mapsto hk$$

e dimostriamo che è un isomorfismo.

1. F omomorfismo

   $$F\left((h,k)(h',k')\right) = F\left((h\varphi_k(h'), kk')\right) = F\left((hkh'k^{-1}, kk')\right) = hkh'k^{-1}kk' = hkh'k' = F((h,k))F((h',k')).$$

2. F iniettivo

   $$e_G = F((h,k)) = hk \Leftrightarrow h = k^{-1} \Rightarrow h, k \in H \cap K = \{e_G\} \Rightarrow (h,k) = (e_G, e_G).$$

3. F surgettivo segue dal punto *2*: ogni elemento dell'insieme G corrisponde corrisponde a un elemento (h, k).

□

Osservazione. Se voglio definire un gruppo "scomposto" devo dire come commutano gli elementi. Se il gruppo ce l'ho già, uso la sua regola, per spezzarlo in sottogruppi.
In questo caso, data la normalità di H in G, la regola è $khk^{-1} = h'$. Il punto è che questa regola è la stessa data da φ_k, ecco perché alla fine sono risultati isomorfi.

1.6.1 Gruppi di ordine pq

Dato G gruppo, tale che $|G| = pq$, con $p < q$ primi, vogliamo scomporlo come prodotto semidiretto di suoi sottogruppi.
Per il *Teorema di Cauchy* possiamo trovare $x, y \in G$ tali che $\text{ord}(x) = q, \text{ord}(y) = p$. Osserviamo che $H = < x > \triangleleft G$, perché ha indice p, con p il più piccolo primo che divida la cardinalità del gruppo.
Alternativamente, possiamo vedere che H è caratteristico in G perché è l'unico sottogruppo di ordine q: se esistesse un $H' < G,\ |H'| = q,\ H' \neq H \Rightarrow H \cap H' = \{e\}$, allora si avrebbe:

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

Quindi abbiamo $H \triangleleft G$, e prendiamo $K = < y >$. Così abbiamo $HK = G, H \cap K = \{e\}$.
Ogni sottogruppo di ordine pq è prodotto semidiretto $G \cong H \rtimes_\varphi K$.

Classificazione Per classificare tutti i gruppi di ordine pq, sfruttando la decomposizione che abbiamo appena visto, dobbiamo classificare tutti i possibili prodotti semidiretti $\mathbb{Z}_{/q\mathbb{Z}} \rtimes_\varphi \mathbb{Z}_{/p\mathbb{Z}}$, a meno di isomorfismo.
Quindi cerco gli omomorfismi

$$\varphi : \mathbb{Z}_{/p\mathbb{Z}} \longmapsto \text{Aut}\left(\mathbb{Z}_{/q\mathbb{Z}}\right) \cong \mathbb{Z}^*_{/q\mathbb{Z}} \cong \mathbb{Z}_{/(q-1)\mathbb{Z}}.$$

Usando la notazione moltiplicativa

$$\begin{aligned} \varphi : < y > \cong \mathbb{Z}_p &\longrightarrow \text{Aut}(< x >) \cong \mathbb{Z}^*_{/q\mathbb{Z}} \\ y &\longmapsto \varphi_y(x \mapsto x^\ell). \end{aligned}$$

Per definire φ sul dominio ciclico $< y >$, basta assegnare φ_y con la condizione $\text{ord}(\varphi_y) \mid p$ (voglio che sia omomorfismo e so che $\text{ord}(y) = p$).
Visto che $\varphi_y \in \text{Aut}(< x >)$, che ha ordine $q - 1$, abbiamo due possibilità:

- se $p \nmid q - 1$, l'unica possibilità è $\varphi_y = \text{Id}$, quindi $\exists!$ gruppo di ordine pq: $\mathbb{Z}_{/pq\mathbb{Z}}$, perché il prodotto diventa diretto $(x, y)(x', y') \in \mathbb{Z}_q \rtimes \mathbb{Z}_p = (x\text{Id}(x'), yy') = (xx', yy') = (x, y)(x', y') \in \mathbb{Z}_p \times \mathbb{Z}_q$;
- se $p \mid q-1$, $\text{ord}(\varphi_y)$ può essere 1 (e si ritorna al prodotto diretto) oppure p. In questo secondo caso, ho $p-1$ scelte per φ_y che danno un prodotto semidiretto vero: si tratta di scegliere $\ell = 1, \ldots, p-1$. Questo perché $\text{ord}(\varphi_y) = \text{ord}(l)$:

  $$\varphi_y^k = x^{l^k} \Rightarrow \text{ord}(\varphi_y) = p \Leftrightarrow l^p \equiv 1\ (q) \Leftrightarrow \text{ord}(l) = p.$$

  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.
  Facciamo vedere come questo isomorfismo è costruito: presi

  $$G_1 = < x > \rtimes_\varphi < y > \qquad G_2 = < x > \rtimes_\psi < y >$$

  dove

  $$\varphi_y(x) = x^\ell \ \text{ord}(\ell) = p \qquad \psi_y(x) = x^\lambda \ \text{ord}(\lambda) = p.$$

  I gruppi ciclici $< \ell >$ e $< \lambda >$ sono identici, perché i generatori hanno lo stesso ordine. Allora possiamo scrivere $\ell = \lambda^r$, con $0 < r < p$. Scriviamo allora questo assegnamento:

  $$\begin{aligned} F : G_1 &\longrightarrow G_2 \\ x &\longmapsto x \\ y &\longmapsto y^r. \end{aligned}$$

  Scriviamo bene i gruppi con le regole definiti da φ e ψ.

  $$\begin{aligned} G_1 &= < x, y \mid x^q = y^p = 1\ yxy^{-1} = x^\ell > \\ G_2 &= < x, y \mid x^q = y^p = 1\ yxy^{-1} = x^\lambda > \end{aligned}$$

  Il punto adesso è che vogliamo provare a estendere questo assegnamento, che mi sta dicendo come sostituire delle parole in un gruppo con altre: è come si dicesse: "al posto di x scrivi x e al posto di y scrivi y^r". Se, dopo la sostituzione, sono effettivamente verificate le proprietà di omomorfismo, allora quella sostituzione ne ha indotto uno.

– Intanto vedo che $F(e) = e$, perché $F(e) = F(x^q) \underset{\text{applico la sostituzione}}{=} x^q$ e inoltre $F(x)^q = x^q = e$.

– Similmente $F(e) = F(y^p) \underset{\text{sostituzione}}{=} y^{rp}$ e $F(y)^p = y^{rp} = e$

– Verifico che la relazione sia mantenuta anche dopo F

$$F\left(yxy^{-1}\right) \underset{\text{sostituzione}}{=} F(y)F(x)F(y)^{-1} = y^r x y^{-r} \underset{\text{la guardo in } G_2}{=} x^{\lambda^r} = x^\ell.$$

Sembra di aver barato, applicando l'omomorfismo prima di aver dimostrato che sia effettivamente tale. In realtà sto dicendo: mi piacerebbe che l'assegnamento che ho definito si potesse estendere a un omomorfismo. Cioè, applicato, verifica le proprietà richieste (in questo caso: manda le identità in identità e preserva le relazioni che abbiamo scritto nelle presentazioni dei gruppi).

1.7 Teoremi di Sylow

Def. Sia G un gruppo finito e p primo tale che $|G| = p^n m$, con $(m, p) = 1$ e $n \geq 1$. Un sottogruppo di G di ordine p^n si chiama $\boxed{p\text{-sottogruppo di Sylow}}$.

Teorema 1.12 (Teorema di Sylow)**.** *Sia G gruppo finito, $|G| = p^n m$, $n \geq 1$, $(m, p) = 1$, p primo. Allora*

- Esistenza $\forall \alpha,\ 1 \leq \alpha \leq n,\ \exists H \leq G \ \ t.c. \ \ |H| = p^\alpha$.
- inclusione $\forall\ 1 \leq \alpha \leq n-1$ *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.*
- Coniugio *Due qualsiasi p-sottogruppi di Sylow di G sono coniugati.*
- Numero *Sia $n_p = \#$ dei p-sottogruppi di Sylow di G. Allora $n_p \mid |G|$ e $n_p \equiv 1\ (p)$.*

Dimostrazione.

- Esistenza Sia $\mathcal{M} = \{X \subset G \mid \#X = p^\alpha\}$.
  Chiaramente
  $$|\mathcal{M}| = \binom{p^n m}{p^\alpha} = \prod_{i=0}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}.$$
  Osserviamo che $p \nmid \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$, perché $\forall i = 1, \ldots, p^\alpha - 1$ vale $p^n m - i\ (p) = p^\alpha - i\ (p) = i\ (p)$; se $p \nmid i$, allora $p^n m - i$ e $p^\alpha - i$ non sono divisibili per p; se invece $i = p^k j$, con $(j, p) = 1$, allora per $k < \alpha$ si ha $p^\alpha - i = p^\alpha - p^k j = p^k \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p}$ e similmente $p^n m - i = p^n m - p^k j = p^k \underbrace{(p^{n-k} m - j)}_{\text{non divisibile per } p}$,
  da cui anche il loro quoziente (una volta semplificato p^k) non è divisibile per p.
  Quindi $p^{n-\alpha} || \mathcal{M}|$, cioè "divide esattamente": le potenze più alte non la dividono.
  Ora consideriamo l'azione di G su $\mathcal{M}$, osservando che, preso $M \in \mathcal{M}$, allora $gM \in \mathcal{M}\ \forall g \in G$.
  $$\begin{aligned} \varphi : G &\longrightarrow S(\mathcal{M}) \\ g &\longmapsto \varphi_g : M \mapsto gM. \end{aligned}$$
  Adesso cercheremo di individuare il sottogruppo di ordine p^α che stiamo cercando come lo stabilizzatore di un elemento di $\mathcal{M}$.
  $$\mathcal{M} = \dot{\bigcup}_{i=1}^{s} \mathrm{Orb}(M_i)$$
  e, poiché
  $$p^{n-\alpha} \Big| |\mathcal{M}| = \sum_{i=1}^{s} |\mathrm{Orb}(M_i)| = \sum_{i=1}^{s} \frac{|G|}{|\mathrm{St}(M_i)|},$$
  possiamo dire che
  $$\exists i \ \text{ t.c. } \ p^{n-\alpha+1} \nmid |\mathrm{Orb}(M_i) = \frac{|G|}{|\mathrm{St}(M_i)|} = \frac{p^n m}{|\mathrm{St}(M_i)|}.$$

Ora come ora, la frazione potrebbe essere divisibile per p^n, però ci vogliamo assicurare che la massima potenza di p che la divide sia $p^{n-\alpha}$: in questo modo vale effettivamente $p^{n-\alpha+1} \nmid$ la frazione. Quindi ci deve essere un fattore p^α al denominatore.

$$p^\alpha \mid |\mathrm{St}(M_i)| = t \;\Rightarrow\; t \geq p^\alpha.$$

D'altro canto, preso $x_i \in M_i$, la funzione così definita

$$\begin{aligned} \mathrm{St}(M_i) &\longrightarrow M_i \\ y &\longmapsto yx \end{aligned}$$

è iniettiva: $yx = y'x \Leftrightarrow y = y'$. Di conseguenza $t = |\mathrm{St}(M_i)| \leq |M_i| = p^\alpha \;\Rightarrow\; t = p^\alpha$. Ecco trovato un sottogruppo di G di ordine p^α:

$$\mathrm{St}(M_i) = \{g \in G \mid \varphi_g(M_i) = gM_i = M_i\}.$$

- Inclusione Sia S un p-Sylow di G, ovvero $S < G,\ |S| = p^n$. Sia $H \leq G, |H| = p^\alpha$.
  Chiamiamo $X = \{$ classi laterali di S in $G\ \}$, quindi

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

  Consideriamo l'azione di H su X data da

$$\begin{aligned} \varphi : H &\longrightarrow S(X) \\ h &\longmapsto \varphi_h : gS \mapsto hgS. \end{aligned}$$

  Osserviamo che

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

  (perché gli stabilizzatori, come sottogruppi, hanno cardinalità che divide quella di H, quindi è del tipo p^k).
  Poiché $p \nmid m$, $\exists i$ t.c. $a_i = 0 \Rightarrow \mathrm{Orb}(g_i S) = \{g_i S\},\ \mathrm{St}(g_i S) = H$. Quindi $\forall h \in H,\ hg_i S = g_i S \Rightarrow H \subset g_i S g_i^{-1}$ (perché $hg_i s = g_i s' \Rightarrow h = g_i s' s^{-1} g_i^{-1} \Rightarrow h = g_i \tilde{s} g_i^{-1} \Rightarrow h \in g_i S g_i^{-1}$.
  Visto che $|g_i S g_i^{-1}| = |S|$, H è contenuto in un p-Sylow di G.
  Questo dimostra, nel frattempo, la parte del Coniugio. Infatti, se $|H| = p^n$ (cioè H è p-Sylow), sfruttiamo quanto appena visto (sarebbe porre $\alpha = n$) e abbiamo $H \subset g_i S g_n^{-1}$ e, poiché hanno la stessa cardinalità, si ha proprio $H = g_i S g_i^{-i}$.

Lemma 1.12.1. *Sia G p-gruppo e $H \lneq G$, allora $N_G(H) \gneq H$, dove $N_G(H)$ indica il normalizzatore in G di H, ovvero il sottogruppo $\{g \in G \mid gHg^{-1} = H\}$.*

Applichiamo il *Lemma* a H, posta $|H| = p^\alpha,\ \alpha \leq n-1$. Allora $H \lneq S \Rightarrow H \lneq N_S(H)$. Visto che $N_S(H) \leq S$, per *Lagrange* ha cardinalità p^k. Quindi il $N_S(H)/H$ è un p-gruppo (gruppo di ordine una potenza di p) non banale (visto che è sottoinsieme stretto). Per *Cauchy* $\exists \overline{x}$ t.c. $\mathrm{ord}\,(\overline{x}) = p$.
Usando il teorema di *Corrispondenza*, che stabilisce la corrispondenza π_H tra i sottogruppi di $N_S(H)$ che contengono H e quelli di $N_S(H)/H$, abbiamo che $\pi_H^{-1}(< \overline{x} >)$ è un sottogruppo di $N_S(H)$, che contiene H, di ordine $p^{\alpha+1}$. La cardinalità è dovuta al fatto che

$$[N_S(H)/H \;: < \overline{x} >] = \frac{p^k}{p^\alpha} \cdot 1/p = \frac{p^k}{p^{\alpha+1}} = [N_S(H) \;:\; \pi_H^{-1}(< \overline{x} >)] = \frac{p^k}{|\pi_H^{-1} < \overline{x} > |}.$$

- Numero Detto $n_p = \#$ p-Sylow, esso vale $[G : N_G(S)]$.
  Infatti $\#$ p-Sylow $=$ $\#$ coniugati di S (ricordiamo che S era un p-Sylow) $= \dfrac{|G|}{|\mathrm{St}(S)|}$ (dove lo stabilizzatore è per l'azione dei coniugi) $= \dfrac{|G|}{|N_G(S)|}$. Di conseguenza $n_p \mid |G|$ e abbiamo dimostrato la prima parte.

Ora dobbiamo mostrare che $n_p \equiv 1\ (p)$.
Sia

$$\begin{aligned} \varphi : S &\longrightarrow S(X) \\ s &\longmapsto \varphi_s : H \mapsto sHs^{-1}, \end{aligned}$$

dove $X = \{p\text{−Sylow di } G\}$. φ_s induce un'unica orbita banale per S: $\mathrm{Orb}(S) = \{sSs^{-1}\} = \{S\}$. Per quanto riguarda gli altri $H \in X$, abbiamo

$$\mathrm{Orb}(H) = \{sHs^{-1} \mid s \in S\} = \{H\} \ \Leftrightarrow\ sHs^{-1} = H\ \forall s \in S$$

ovvero $S \subseteq N_G(H)$. Di conseguenza $SH < N_G(H)$ perché $shHh^{-1}s^{-1} = sHs^{-1} = H$. Ma questo è assurdo perché, se $S \neq H$,

$$|SH| = \frac{|S||H|}{|S \cap H|} = \underset{\substack{\downarrow \\ k < n}}{\frac{p^n \cdot p^n}{p^k}} = p^{2n-k} \nmid |G|.$$

Quindi le orbite degli altri non sono banali. Dalla formula delle classi si ha

$$n_p = |X| = \sum_{i=1}^{r} |\mathrm{Orb}(H_i)| + |\mathrm{Orb}(S)| = \sum_{i=1}^{r} \frac{|S|}{|N_S(H_i)|} + |\mathrm{Orb}(S)| = \sum_{i=1}^{r} \underset{\substack{\downarrow \\ \text{perché } N_S(H_i) < S}}{p^{a_i}} + 1 = pf + 1 \ \Rightarrow\ n_p \equiv 1\ (p).$$

□