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 $\boxed{\text{ciclico}}$ 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 $N \lhd G$ con $N \subseteq \mathrm{Ker} f$. Allora $\exists\, \varphi : G/N \to G'$ t.c. il diagramma commuta*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_N"'] & G' \\ G/N \arrow[ur, "\varphi"'] & \end{tikzcd}$$

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:

$$\begin{tikzcd}
G/K \arrow[r] \arrow[d] & G/H \\
(G/K)/(H/K) \arrow[ur] &
\end{tikzcd}$$

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

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

.

$\square$

1.3 Prodotto diretto di gruppi

Def. Siano G e G' gruppi, allora si definisce il $\boxed{\text{prodotto diretto}}$ 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?

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

1.3.1 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 $\boxed{\text{commutatore}}$ 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 $H, K \lhd G$ 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 $K \lhd G$ abbiamo

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

Similmente, sfruttando $H \lhd G$:

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

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.

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

□

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

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.

□

1.5 Teorema di Cauchy

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.* $\mathrm{ord}(x) = p$.

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

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

Caso $m > 1$ $\quad$ 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. $p \mid |<x>| = \mathrm{ord}(x)$
2. $p \nmid |<x>| = \mathrm{ord}(x)$

Che risolviamo in questo modo:

1. Ho un gruppo ciclico, di ordine $\mathrm{ord}x = n$, 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 $\mathrm{ord}[y] = p$. Da cui $p \mid \mathrm{ord}y$ e, con una divisione simile a quella di prima, ottengo un elemento di ordine esattamente p.

□

1.6 Automorfismi

Def. $H \leq G$ si dice $\boxed{\text{caratteristico}}$ 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. □

1.7 Azioni di gruppo

Def. Siano G un gruppo e X un insieme, allora si definisce $\boxed{\text{azione}}$ 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 $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{gg^{-1}} = \varphi_e = \mathrm{Id}_{S(X)}$.

1.7.1 Classi di equivalenza, orbite e stabilizzatori

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

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

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 $\boxed{\text{orbite}}$ 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 $\boxed{\text{stabilizzatore}}$ 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. $g \in \mathrm{St}(x) \Rightarrow \varphi_g(x) = x \Rightarrow \varphi_g^{-1}(x) = x = \varphi_{g^{-1}}(x) \Rightarrow g^{-1} \in \mathrm{St}(x)$.

□

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. □

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).

$\square$