CAPITOLO E

Gruppi Risolubili e Nilpotenti

Il presente capitolo intende fornire una trattazione, non certo esaustiva, di due importanti argomenti riguardanti i gruppi: la risolubilità e la nilpotenza.

Gli argomenti sono divisi in sei sezioni: le prime tre, sui gruppi risolubili, presentano dapprima un'introduzione riguardante i concetti di *commutatori, serie di composizione e derivato* di un gruppo, essenziali per giungere alla definizione di risolubilità, poi analizzano le conseguenze di tali proprietà e, infine, ampliano la prospettiva intrecciando la questione con un altro argomento fondamentale della teoria dei gruppi, i sottogruppi di Sylow.

Le ultime tre sezioni, introducendo i concetti di *serie centrale* inferiore e superiore, preparano allo studio della nilpotenza dei gruppi finiti. Inoltre, sottolineano l'importanza dei sottogruppi di Frattini nel determinare la nilpotenza del gruppo che li contiene.

E1. Serie normale e di composizione

Definizione E1.1 (Serie subnormale e normale). *Consideriamo una successione di sottogruppi di un gruppo G, in cui ogni sottogruppo è un sottogruppo normale del gruppo che lo precede:*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_\ell.$$

Tale successione è detta serie subnormale *e la indicheremo con Σ. Se ogni G_i è anche un sottogruppo normale di G, chiameremo la successione* serie normale.

I gruppi quozienti $\{G_{k-1}/G_k\}_{k=1}^{\ell}$ vengono chiamati fattori della serie Σ ed il numero dei fattori ℓ viene denominato la *lunghezza* di Σ.

Esempio E1.2. *Siano G un gruppo e H un sottogruppo normale di G. Allora $G \trianglerighteq H \trianglerighteq \{e\}$ risulta sempre una serie normale.*

Esempio E1.3 (gruppo simmetrico). *Sia S_4 un gruppo simmetrico di ordine 24. Definiamo due sottogruppi come segue:*

$$\begin{aligned} H_1 : &= \{e, (12)(34), (13)(24), (14)(23)\}; \\ H_2 : &= \{e, (12)(34)\}. \end{aligned}$$

Allora $S_4 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \{e\}$ è una serie subnormale di S_4 ma non normale.

Per indagare meglio la struttura di un gruppo G, si aspetta normalmente che i fattori delle serie subnormali siano i più semplici possibili. Dal punto di vista dei sottogruppi normali, preferiamo che questi fattori siano semplici. Il seguente risultato dice quando G/H è semplice se $H \trianglelefteq G$.

Proposizione E1.4. *Siano G un gruppo e H un sottogruppo normale di G. Allora il gruppo quoziente G/H è semplice se e solo se H è un sottogruppo normale massimale di G*

DIMOSTRAZIONE. Suppponiamo che G/H sia semplice. Se H non è un sottogruppo normale massimale di G, allora esiste un sottogruppo normale N di G tale che $G \trianglerighteq N \trianglerighteq H$. Quindi N/H è un sottogruppo normale non banale di G/H, contrario alla semplicità di G/H.

Viceversa, se G/H non è semplice, esiste un sottogruppo normale non banale N/H di G/H e risulta $G \trianglerighteq N \trianglerighteq H$. Quest'ultima implica che H non è un sottogruppo normale massimale di G. □

Definizione E1.5 (Serie di composizione). *Sia Σ una serie subnormale di un gruppo G senza ripetizione:*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_\ell$$

in cui ciascun G_k risulta un sottogruppo normale massimale del suo predecessore G_{k-1}. Allora Σ si dice serie di composizione. *I fattori di Σ si chiamano* fattori di composizione.

Esempio E1.6 (gruppo quadrinomio di Klein). *Sia $V_4 = \{e, a, b, ab\}$ il gruppo quadrinomio di Klein* (gruppo abeliano non ciclico di ordine 4). *Allora ci sono, in tutto, tre serie di composizione:*

$$\begin{aligned} V_4 &\trianglerighteq \langle a \rangle \trianglerighteq \{e\}, \\ V_4 &\trianglerighteq \langle b \rangle \trianglerighteq \{e\}, \\ V_4 &\trianglerighteq \langle ab \rangle \trianglerighteq \{e\}. \end{aligned}$$

Esempio E1.7 (gruppo dei quaternioni). *Sia* $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ *il gruppo dei quaternioni. Allora ci sono, in tutto, tre serie di composizione:*

$$\begin{aligned} Q_8 &\trianglerighteq \langle i \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}, \\ Q_8 &\trianglerighteq \langle j \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}, \\ Q_8 &\trianglerighteq \langle k \rangle \trianglerighteq \{\pm 1\} \trianglerighteq \{1\}. \end{aligned}$$

Definizione E1.8 (Serie di raffinamento). *Siano* Σ *e* Ξ *due serie subnormali di un gruppo* G *rispettivamente date da*

$$\begin{aligned} G &= G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_\ell; \\ G &= H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_\kappa. \end{aligned}$$

Si dice che Ξ *è un* raffinamento *di* Σ *se ogni termine di* Σ *compare nella serie* Ξ. *Se poi* Ξ *contiene strettamente* Σ, *allora si parla di* raffinamento proprio.

Si evince che una serie subnormale Σ di G risulta *serie di composizione* se non ammette alcun raffinamento proprio.

Definizione E1.9 (Isomorfismo fra due serie subnormali). *Siano* Σ *e* Ξ *due serie subnormali di un gruppo* G. *Si dice che* Σ *e* Ξ *sono isomorfe se hanno la stessa lunghezza e i rispettivi fattori isomorfi a meno dell'ordine.*

Per la serie di composizione, vale il seguente importante teorema.

Teorema E1.10 (Jordan-Hölder). *Sia* G *un gruppo finito. Allora due qualunque serie di composizione di* G *sono isomorfe.*

DIMOSTRAZIONE. Sia G un gruppo finito. Proviamo la tesi per induzione su l'ordine di G.

• Per $|G| = 1$, la tesi è ovvia.

• Come ipotesi induttiva assumiamo che la tesi sia vera per tutti i gruppi H con $|H| < |G|$.

• Per il gruppo finito G consideriamo ora due serie di composizioni:

$$\begin{aligned} \mathrm{S}: &\quad G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\}, \\ \mathrm{T}: &\quad G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{e\}. \end{aligned}$$

Se $G_1 = H_1$, allora abbiamo due serie di composizioni

$$\begin{aligned} \mathrm{S}': &\quad G_1 \triangleright G_2 \triangleright \cdots \triangleright G_m = \{e\}, \\ \mathrm{T}': &\quad H_1 \triangleright H_2 \triangleright \cdots \triangleright H_n = \{e\}. \end{aligned}$$

che sono isomorfe per l'ipotesi del passo induttivo perché $|G_1| = |H_1| < |G|$.

Se $G_1 \neq H_1$, G_1 e H_1 sono due sottogruppi normali massimali di G, quindi $G = G_1H_1$. Consideriamo allora una qualunque serie di composizione

$$G_1 \cap H_1 = F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$$

e costruiamo due serie subnormali di G:

$$\begin{aligned} \mathrm{S}'' : &\quad G \rhd G_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}, \\ \mathrm{T}'' : &\quad G \rhd H_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}. \end{aligned}$$

Per il terzo teorema di isomorfismo abbiamo

$$\begin{aligned} G/G_1 = (G_1H_1)/G_1 &\cong H_1/(G_1 \cap H_1) = H_1/F_1, \\ G/H_1 = (G_1H_1)/H_1 &\cong G_1/(G_1 \cap H_1) = G_1/F_1, \end{aligned}$$

dove H_1/F_1 e G_1/F_1 sono gruppi semplici, perché G_1 e H_1 sono sottogruppi normali massimali di G. Allora la $[\mathrm{S}'']$ e la $[\mathrm{T}'']$ sono due serie di composizioni di G isomorfe. Ora, ricordando che $|G_1| < |G|$ e $|H_1| < |G|$, abbiamo che, per l'ipotesi del passo induttivo, la serie di composizione $[\mathrm{S}']$ è isomorfa alla $G_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$ e la serie di composizione $[\mathrm{T}']$ è isomorfa alla $H_1 \rhd F_1 \rhd F_2 \rhd \cdots \rhd F_k = \{e\}$. Dunque la $[\mathrm{S}]$ è isomorfa alla $[\mathrm{S}'']$ e la $[\mathrm{T}]$ è isomorfa alla $[\mathrm{T}'']$. Per la transitività dell'isomorfismo, la $[\mathrm{S}]$ e la $[\mathrm{T}]$ sono isomorfe. □

Da questo teorema, possiamo ricavare subito il seguente risultato.

Corollario E1.11 (Schreier). *Due serie subnormali di un gruppo G ammettono sempre raffinamenti isomorfi.* □

E2. Commutatori e derivati

Sia G un gruppo e siano x, y elementi di G. Si dice *commutatore* della coppia (x, y) e si denota col simbolo $[x, y]$, l'elemento $x^{-1}y^{-1}xy$.

Ovviamente possiamo definire commutatori di ordine superiore, tramite la formula ricorsiva $[x_1, x_2, \cdots, x_{n-1}, x_n] = \big[[x_1, x_2, \cdots, x_{n-1}], x_n\big]$. Questi sono detti *commutatori semplici.*

Più in generale, tutti gli elementi che si possono ottenere tramite commutazioni successive sono detti *commutatori complessi.* (Per esempio, con $a, b, \alpha, \beta, \gamma$ elementi di un gruppo G, $\big[[a, b], [\alpha, \beta, \gamma]\big]$ è un commutatore complesso).

Notiamo ora che,

$$yx[x,y] \;=\; yxx^{-1}y^{-1}xy = xy.$$

Da questa uguaglianza segue che due elementi x e y del gruppo G sono permutabili se e solo se $[x,y] = e$.

In particolare, poi, $\forall x \in G : \; [x,x] = e$, quindi l'unità di G è un commutatore. Inoltre, l'inverso di un commutatore è ancora un commutatore, infatti, se $x, y \in G$, vale

$$[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x].$$

Tuttavia non è assolutamente detto che il prodotto di due commutatori sia un commutatore, sicché l'insieme dei commutatori di un gruppo G, in generale, non è un sottogruppo di G.

Sia G un gruppo e siano H e K sottogruppi di G. Si dice *interderivato* di H e K e si denota con $[H,K]$, il sottogruppo di G generato dall'insieme $\{[h,k] \mid h \in H, k \in K\}$. Poiché, come abbiamo già osservato, $\forall h \in H$ e $\forall k \in K : \; [h,k]^{-1} = [k,h]$, si ha che $[H,K] = [K,H]$.

Consideriamo ora il caso in cui H e K siano normali in G e proviamo che $[H,K]$ è un sottogruppo normale di G. Ricordiamo intanto che se G è un gruppo e $g \in G$, l'applicazione

$$\begin{aligned} \phi_g : \qquad & G \longrightarrow G, \\ & x \longmapsto x^g = g^{-1}xg; \end{aligned}$$

è un isomorfismo. In generale, supponiamo che ϕ sia un omomorfismo fra due gruppi G_1 e G_2. Allora per due generici elementi $x, y \in G_1$, vale l'identità: $\phi\big([x,y]\big) = \big[\phi(x), \phi(y)\big]$. Infatti, l'affermazione segue immediatamente dalla seguente relazione:

$$\phi\big([x,y]\big) = \phi(x^{-1}y^{-1}xy) = \phi^{-1}(x)\phi^{-1}(y)\phi(x)\phi(y) = \big[\phi(x), \phi(y)\big].$$

Pertanto, se H e K sono due sottogruppi normali in G, allora per ogni $g \in G$ vale $[H,K]^g = [H^g, K^g] = [H,K]$, cioè $[H,K]$ è normale in G.

Sia G un gruppo. Si dice *derivato* (o *sottogruppo commutatore*) di G e si indica col simbolo G' l'interderivato $[G,G]$, cioè il sottogruppo generato da tutti i commutatori di elementi di G.

Per quanto detto circa l'interderivato, segue immediatamente che il derivato G' è un sottogruppo caratteristico di G, cioè invariante sotto qualunque automorfismo di G; esso à evidentemente un sottogruppo normale di G. Inoltre, poiché due elementi $x, y \in G$ sono permutabili se e solo se $[x,y] = e$, si ha che G è abeliano se e solo se $G' = \{e\}$.

Diamo ora una caratterizzazione del derivato di un gruppo. Il derivato G' di un gruppo G è il minimo sottogruppo normale N di G (*rispetto alla relazione di inclusione*) tale che il quoziente G/N sia abeliano. Questa è una conseguenza del seguente teorema.

Teorema E2.1. *Siano G un gruppo e G' il derivato di G. Allora*

(a) *il quoziente G/G' è un gruppo abeliano.*
(b) *se $N \trianglelefteq G$ e G/N è abeliano, allora $G' \subseteq N$.*
(c) *se $H \leq G$ e $G' \subseteq H$, allora $H \trianglelefteq G$.*

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] Siano $x, y \in G$. Per due laterali $xG', yG' \in G/G'$, abbiamo che $[xG', yG'] = [x, y]G' = G'$; infatti, qualunque siano gli elementi x e y di G, il commutatore $[x, y]$ appartiene a G'. Pertanto i laterali xG' e yG' sono permutabili, cioè G/G' è abeliano.

[b] Sia $N \trianglelefteq G$ tale che G/N sia abeliano. $\forall x, y \in G : \ xN$ e yN sono permutabili e quindi $N = [xN, yN] = [x, y]N$, per cui $[x, y] \in N$. Pertanto G', essendo generato dai commutatori di elementi di G, è contenuto in N.

[c] Basta dimostrare che se $g \in G$ e $h \in H$ allora $h^g = g^{-1}hg \in H$. Dato che G/G' è un gruppo abeliano che contiene H/G' come un sottogruppo, allora per ogni $g \in G$ e $h \in H$, vale la seguente relazione

$$h^g G' = (hG')^{gG'} = (gG')^{-1}(hG')gG' = hG'.$$

Allora esiste $g' \in G'$ tale che $h^g = hg' \in H$, da cui segue che H è un sottogruppo normale di G. □

Teorema E2.2 (Schur). *In un gruppo G, se il centro ha indice finito, allora il derivato di G è finito.*

DIMOSTRAZIONE. Denotiamo con Z il centro del gruppo G e consideriamo l'applicazione:

$$\theta : G/Z \times G/Z \longrightarrow G';$$
$$\theta(xZ, yZ) = [x, y] \ \text{ per } \ x, y \in G.$$

È facile verificare che θ è suriettiva. Quindi

$$|G'| \ \leq \ \left|G/Z \times G/Z\right| = [G : Z]^2$$

che significa che G' è finito. □

Per mezzo del teorema appena provato saremo in grado di dare, in seguito, una caratterizzazione dei gruppi risolubili di ordine finito.

Definizione E2.3. *Sia G un gruppo e si ponga $G^{(0)} = G$. Per un numero naturale k, definiamo $G^{(k)}$ per induzione con $G^{(k)} = (G^{(k-1)})'$. Il sottogruppo $G^{(k)}$ si dice* k-esimo derivato *di G.*

In particolare si ha $G^{(1)} = G'$. Possiamo osservare che

$$G' = [G, G], \quad G'' = [G', G'] = \big[[G, G], [G, G]\big], \quad \cdots .$$

Dunque G'' è normale in G perché per ogni $g \in G$ vale la seguente

$$\begin{aligned} (G'')^g &= \big[[G, G], [G, G]\big]^g \\ &= \big[[G, G]^g, [G, G]^g\big] \\ &= \big[[G^g, G^g], [G^g, G^g]\big] \\ &= \big[[G, G], [G, G]\big] = G''. \end{aligned}$$

Secondo il principio di induzione, possiamo concludere che l'insieme $\{G^{(k)} \mid k \in \mathbb{N}_0\}$ risulta essere una serie normale di G; tale serie è chiamata *serie derivata* di G.

E3. Gruppi risolubili

Definizione E3.1. *Un gruppo G si dice* risolubile *se la sequenza*

$$G \supseteq G' \supseteq G'' \supseteq \cdots \supseteq G^{(k)} \supseteq \cdots$$

in cui ogni gruppo $G^{(k)}$ è il derivato del precedente, termina nell'elemento neutro in un numero finito di passi, cioè esiste un intero nonnegativo ℓ tale che $G^{(\ell)} = \{e\}$.

OSSERVAZIONE: Dal Teorema **E2.1** segue che ogni fattore $G^{(k)}/G^{(k+1)}$ è un gruppo quoziente abeliano.

Diamo ora la caratterizzazione dei gruppi risolubili di ordine finito della cui esistenza avevamo accennato nel paragrafo precedente.

Teorema E3.2. *Un gruppo di ordine finito è risolubile se e solo se ogni fattore, in una serie di composizione da G ad $\{e\}$, è ciclico di ordine primo.*

Questo teorema è stato, storicamente, la prima definizione di risolubilità, ma aveva il grosso limite di non essere applicabile ai gruppi infiniti.

DIMOSTRAZIONE. Proviamo separatamente la condizione sufficiente e la condizione necessaria per la validità del teorema.

"$\Longleftarrow$" Supponiamo $G = A_0 \supset A_1 \supset \cdots \supset A_n = \{e\}$, dove A_{i-1}/A_i, $i = 1, 2, \cdots, n$ è ciclico di ordine primo. Dal Teorema **E2.1**, poiché G/A_1 è abeliano, segue che $A_1 \supseteq G'$. Analogamente, $A_2 \supseteq A_1' \supseteq G''$ e, in ultimo $A_n \supseteq G^{(n)}$, quindi $G^{(n)} = \{e\}$ e G è risolubile.

"$\Longrightarrow$" Supponiamo che G sia risolubile e finito. Poiché G/G' è abeliano, nella serie

$$G \supset G' \supset G'' \supset \cdots \supset G^{(n)} = \{e\}$$

esisterà un sottogruppo normale massimale $A_1 \supseteq G'$. Dal fatto che G/A_1 sia abeliano e semplice (cioè non contiene sottogruppi normali propri), segue che G/A_1 è ciclico di ordine primo. Analogamente, poiché A_1 è risolubile, esisterà A_2, sottogruppo normale massimale contenuto in A_1 con $A_1 \supset A_2 \supset A_1' \supseteq G''$, tale che A_1/A_2 è ciclico di ordine primo. Continuando così, avremo

$$G = A_0 \supset A_1 \supset \cdots \supset A_m = \{e\}$$

con A_{i-1}/A_i gruppo ciclico di ordine primo $\forall i = 1, 2, \cdots, m$. Inoltre, secondo il teorema di Jordan-Hölder, date due qualunque serie di composizione di un gruppo finito G, queste sono isomorfe; pertanto vale la tesi. □

Corollario E3.3. *Un gruppo semplice risolubile ha ordine primo.*

DIMOSTRAZIONE. Sia G un gruppo risolubile. Allora $G \neq G'$. Inoltre, dalla semplicità, risulta che $G' = \{e\}$ e $G = G/G'$ è abeliano. Dunque G è un gruppo abeliano semplice, che deve essere un gruppo ciclico di ordine primo. □

Esempio E3.4 (gruppo abeliano). *Ogni gruppo abeliano è risolubile.*

Esempio E3.5. *Il gruppo $\mathbb{Q}_8$ dei quaternioni è risolubile.*

Diamo ora un importante risultato sui p-gruppi finiti.

Teorema E3.6. *Ogni p-gruppo finito è risolubile.*

DIMOSTRAZIONE. Siano p un primo e G un p-gruppo finito di ordine p^n con $n \in \mathbb{N}$. Secondo la Proposizione **D1.4**, possiamo costruire una successione

$$G = G_n \supseteq G_{n-1} \supseteq G_{n-2} \supseteq \cdots \supseteq G_1 \supseteq G_0 = \{e\}$$

dove $\forall k = 0, 1, \cdots, n-1$: G_k è un sottogruppo di G di ordine p^k, pertanto massimale e quindi normale in G_{k+1} grazie alla Proposizione **C5.3**. Allora ogni fattore G_{k+1}/G_k è un gruppo ciclico di ordine p e quindi abeliano. Così la successione è una serie di composizione del gruppo G. Quindi G è risolubile grazie al Teorema **E3.2**. □

Diamo un'ultima caratterizzazione dei gruppi risolubili:

Teorema E3.7. *Sia G un gruppo. Sono equivalenti le seguenti affermazioni:*

(a) *G è risolubile.*

(b) *G ha una serie normale finita*

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_m = \{e\}$$

in cui ogni $A_{i-1}/A_i,\ i = 1, 2, \cdots, m$ è abeliano.

(c) *G ha una serie finita*

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n = \{e\}$$

in cui ogni $B_{j-1}/B_j,\ j = 1, 2, \cdots, n$ è abeliano.

DIMOSTRAZIONE. Proviamo le tre affermazioni ciclicamente.

[a]$\Longrightarrow$[b] Se G è risolubile, allora la sua serie derivata

$$G \supset G' \supset G'' \supset \cdots \supset G^{(m)} = \{e\}$$

è una serie normale finita in cui $G^{(i-1)}/G^{(i)}$ è abeliano per $i = 1, 2, \cdots, m$, quindi vale il punto **[b]**.

[b]$\Longrightarrow$[c] Banale (una serie normale è una serie).

[c]$\Longrightarrow$[a] Se $G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n = \{e\}$ è una serie con B_{j-1}/B_j abeliano per $j = 1, 2, \cdots, n$, allora, poiché $G/B_1 = B_0/B_1$ è abeliano, $B_1 \supseteq G'$. Analogamente, se $B_j \supseteq G^{(j)}$, allora $B_{j+1} \supseteq B_j' \supseteq G^{(j+1)}$. Quindi, in ultimo, $G^{(n)} \subseteq B_n = \{e\}$ e perciò $G^{(n)} = \{e\}$. Pertanto G è risolubile. □

Corollario E3.8. *Un gruppo G è risolubile se ha un sottogruppo normale H tale che sia H che G/H siano risolubili.*

DIMOSTRAZIONE. Consideriamo le due serie

$$G/H \supseteq A_1/H \supseteq \cdots \supseteq A_m/H \supseteq H/H$$

e

$$H \supseteq B_1 \supseteq \cdots \supseteq B_n \supseteq \{e\}$$

rispettivamente per G/H e H, che soddisfano la proprietà **[c]** del teorema precedente. Allora

$$G \supseteq A_1 \supseteq \cdots \supseteq A_m \supseteq H \supseteq B_1 \supseteq \cdots \supseteq B_n \supseteq \{e\}$$

è una serie che soddisfa la stessa suddetta proprietà **[c]** per G; perciò G è risolubile. □

Teorema E3.9. *Tutti i sottogruppi e tutti i gruppi quoziente di un gruppo risolubile sono risolubili.*

DIMOSTRAZIONE. Sia G risolubile e $H \leq G$. Allora dalla definizione di derivato di un gruppo segue che $H' \subseteq G'$, poiché H' è generato da tutti i commutatori di elementi di H e G' è generato da tutti i commutatori di elementi di G. Analogamente, $H'' \subseteq G''$, ecc. Se $G^{(m)} = \{e\}$ per una certa $m \in \mathbb{N}$, allora $H^{(m)} = \{e\}$. Pertanto H è risolubile. Ovviamente può accadere che $H^{(k)} = \{e\}$ già per qualche $k < m$.

Sia ora $W = G/K$ un certo gruppo quoziente di G e consideriamo l'omomorfismo canonico $\varphi : G \longrightarrow W$. Ogni commutatore in W è l'immagine di un commutatore in G, quindi $G' \longrightarrow W'$. Continuando, $G^{(n)} \longrightarrow W^{(n)}$, perciò, se $G^{(n)} = \{e\}$, allora $W^{(n)} = \{e\}$, cioè W è risolubile. Anche in questo caso, naturalmente, può accadere che $W^{(k)} = \{e\}$ già prima per qualche $k < n$. □

Dal confrontando con i teoremi di Sylow possiamo affermare che valgono i seguenti risultati sui gruppi risolubili la cui dimostrazione viene lasciata come esercizio al lettore (si può usare il principio di induzione e l'azione di un gruppo su un insieme).

Teorema E3.10. *Sia G un gruppo risolubile di ordine mn, dove m e n sono numeri naturali coprimi. Allora:*

(a) *G possiede almeno un sottogruppo di ordine m.*
(b) *Due qualunque sottogruppi di ordine m sono coniugati.*
(c) *Un sottogruppo il cui ordine m' divide m è contenuto in un sottogruppo di ordine m.*
(d) *Il numero dei sottogruppi di ordine m può essere espresso come un prodotto in cui ogni fattore*
   - *è congruente a 1 modulo un certo fattore di m;*
   - *è una potenza di un primo.*

Di seguito enunciamo altri tre risultati molto significativi le cui dimostrazioni, tuttavia, sono decisamente complesse e pertanto non possono essere qui riportate.

- Il gruppo simmetrico S_n non è risolubile per $n > 4$.
- Un gruppo di ordine $p^m q^n$, dove p e q sono primi ed m, n interi non negativi, è risolubile (Burnside).
- Ogni gruppo di ordine dispari è risolubile (Feit-Thompson).

E4. Serie centrale inferiore e superiore

Definiamo una serie di sottogruppi di un gruppo G tramite le seguenti regole:

$$\Gamma_1(G) = G \quad \text{e} \quad \Gamma_k(G) = \langle\, [x_1, x_2, \cdots, x_k] \mid \forall x_1, x_2, \cdots, x_k \in G \rangle.$$

Per la proprietà dei commutatori semplici vale che

$$[y_1, y_2, \cdots, y_{k+1}] = \big[[y_1, y_2, \cdots, y_k], y_{k+1}\big].$$

Possiamo notare che per ogni k : $\Gamma_{k+1}(G) \subseteq \Gamma_k(G)$. La serie

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \Gamma_3(G) \supseteq \cdots$$

è detta *serie centrale inferiore* di G.

Teorema E4.1 (Interderivato ricorsivo). $\Gamma_{k+1}(G) = [\Gamma_k(G), G]$.

DIMOSTRAZIONE. Da $[y_1, y_2, \cdots, y_k, y_{k+1}] = \big[[y_1, y_2, \cdots, y_k], y_{k+1}\big]$, abbiamo banalmente la prima inclusione "$\subseteq$". Per provare l'altra inclusione abbiamo bisogno della seguente identità di facilissima verifica:

$$[xy, z] = [x, z]^y\, [y, z] = [x, z]\, [x, z, y]\, [y, z].$$

Ora poniamo

$$\begin{aligned} x &= [a_1, a_2, \cdots, a_k], \\ y &= [a_1, a_2, \cdots, a_k]^{-1}, \\ z &= a_{k+1}. \end{aligned}$$

Allora

$$e = [e, a_{k+1}] = [a_1, a_2, \cdots, a_k, a_{k+1}]^y \, \big[[a_1, a_2, \cdots, a_k]^{-1}, a_{k+1}\big].$$

Così abbiamo l'appartenenza di $\big[[a_1, a_2, \cdots, a_k]^{-1}, a_{k+1}\big]$ a $\Gamma_{k+1}(G)$, conseguenza dell'appartenenza degli altri termini a $\Gamma_{k+1}(G)$. Notiamo che l'interderivato $[\Gamma_k(G), G]$ è generato dagli elementi $[u_1 u_2 \cdots u_n, g]$, dove $u_i = [a_1, a_2, \cdots, a_k]$ oppure $[a_1, a_2, \cdots, a_k]^{-1}$. Abbiamo provato che $[u_i, g] \in \Gamma_{k+1}(G)$. Proviamo per induzione su n che $[u_1 u_2 \cdots u_n, g] \in \Gamma_{k+1}(G)$. Questo si può fare, ponendo nell'identità precedentemente enunciata

$$x = u_1 u_2 \cdots u_{n-1}, \quad y = u_n, \quad z = g;$$

così abbiamo

$$[u_1 u_2 \cdots u_{n-1} u_n, g] = [u_1 u_2 \cdots u_{n-1}, g]^{u_n} [u_n, g].$$

Per l'ipotesi induttiva le due espressioni a destra sono in $\Gamma_{k+1}(G)$. Quindi abbiamo provato l'altra inclusione e, di conseguenza, il teorema. □

Da questo teorema segue un importante corollario.

Corollario E4.2. $\Gamma_k(G)/\Gamma_{k+1}(G)$ *è nel centro di* $G/\Gamma_{k+1}(G)$.

Infatti, presi $\gamma \in \Gamma_k(G)$ e $g \in G$, abbiamo $[\gamma, g] \in \Gamma_{k+1}(G)$. Ne segue

$$[\gamma\Gamma_{k+1}(G), g\Gamma_{k+1}(G)] = \Gamma_{k+1}(G).$$

Quindi effettivamente è valido il corollario.

Possiamo anche definire una *serie centrale superiore* per un gruppo G.

$$Z_0 = \{e\} \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_i(G) \subseteq Z_{i+1}(G) \subseteq \cdots$$

dove definiamo Z_{i+1} tramite la seguente regola: $Z_{i+1}(G)/Z_i(G)$ è il centro di $G/Z_i(G)$. Tra poco spiegheremo il motivo della dicitura *superiore* e *inferiore* applicata alle serie centrali.

Una serie $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \supseteq A_{m+1} = \{e\}$, in cui ogni A_i/A_{i+1} è nel centro di G/A_{i+1} è chiamata *serie centrale.*

Teorema E4.3. *Sia $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \supseteq A_{m+1} = \{e\}$ una serie centrale per G. Allora $A_i \supseteq \Gamma_i(G)$ per $i = 1, \cdots, m+1$ e $A_{1+m-j} \subseteq Z_j(G)$ per $j = 0, 1, 2, \cdots, m$.*

DIMOSTRAZIONE. Abbiamo $A_1 = G = \Gamma_1(G)$. Supponiamo che $A_i \supseteq \Gamma_i(G)$. Dal fatto che A_i/A_{i+1} è nel centro di G/A_{i+1} segue che $[A_i, G] \subseteq A_{i+1}$. Ma allora, ricordando anche il Teorema **E4.1**, si ha che $\Gamma_{i+1}(G) = [\Gamma_i(G), G] \subseteq [A_i, G] \subseteq A_{i+1}$. Per induzione, questo prova che $A_i \supseteq \Gamma_i(G)$ per $i = 0, 1, 2, \cdots, m$.

Evidentemente si ha che $A_{m+1} \subseteq Z_0(G)$ e $A_m \subseteq Z_1(G)$. Supponiamo ora che per una certa j valga che $A_{1+m-j} \subseteq Z_j(G)$. Allora $U = G/Z_j(G)$ è immagine tramite un omomorfismo di $V = G/A_{1+m-j}$ con $\mathrm{Ker} Z_j(G)/A_{1+m-j}$. Ora A_{m-j}/A_{1+m-j} è nel centro di V, quindi la sua immagine omomorfa in U deve essere nel centro di U. Ma questa immagine è $(A_{m-j}Z_j)/Z_j$, mentre il centro di U è Z_{j+1}/Z_j. Quindi $A_{m-j} \subseteq A_{m-j}Z_j \subseteq Z_{j+1}$, provando la tesi per induzione. □

E5. Gruppi nilpotenti

Nelle sezioni precedenti, abbiamo parlato di gruppi risolubili. Ci sono però proprietà più forti della risolubilità; una di queste è la nilpotenza.

Definizione E5.1. *Un gruppo G è nilpotente se possiede una serie normale finita $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_\ell = \{e\}$, in cui ogni gruppo quoziente A_{i-1}/A_i è nel centro di G/A_i con $i = 1, 2, \cdots, \ell$.*

Ricordando il Teorema **E3.7**, possiamo subito affermare che un gruppo nilpotente è risolubile. Un'altra immediata conseguenza si può evidenziare dal Teorema **E4.3** con il seguente corollario.

Corollario E5.2. *In un gruppo nilpotente G, le serie centrali inferiore e superiore hanno entrambe la medesima lunghezza finita ℓ.*

Infatti, se c'è una serie centrale finita di lunghezza m, il Teorema **E4.3** mostra che le serie centrali inferiore e superiore hanno al più lunghezza m. Inoltre, comparando le due serie, possiamo dedurre che non possono essere di lunghezze differenti, quindi esse hanno la stessa lunghezza ℓ e questo numero ℓ è detto la *classe* del gruppo nilpotente. Un gruppo nilpotente di classe uno è semplicemente un gruppo abeliano.

Possiamo notare che se un gruppo G è nilpotente di classe ℓ, allora ogni commutatore $[a_1, a_2, \cdots, a_{\ell+1}]$ è l'identità, e viceversa, se $[a_1, a_2, \cdots, a_{\ell+1}] = e$, allora G è nilpotente al più di classe ℓ. Indicheremo la proprietà che $[a_1, a_2, \cdots, a_{\ell+1}] = e$ per ogni $a_i \in G$, dicendo che G è *ℓ-nilpotente.*

Teorema E5.3. *Se G è ℓ-nilpotente, allora ogni sottogruppo e ogni gruppo quoziente di G è ℓ-nilpotente.*

DIMOSTRAZIONE. Se G è ℓ-nilpotente, allora necessariamente, per un sottogruppo H, tutti i commutatori $[a_1, a_2, \cdots, a_{\ell+1}]$ con $a_i \in H$, devono essere l'identità. Quindi H è ℓ-nilpotente. Anche se T è un'immagine omomorfa di G, allora ogni commutatore $[b_1, b_2, \cdots, b_{\ell+1}]$ con $b_i \in T$ è immagine di un certo commutatore $[a_1, a_2, \cdots, a_{\ell+1}]$ in G e quindi è l'identità. Perciò T è ℓ-nilpotente. □

Teorema E5.4. *Siano G un gruppo ℓ-nilpotente e $H = H_0$ un sottogruppo. Per $k = 1, 2, \cdots$, si denota con $H_k = N_G(H_{k-1})$, il normalizzante di H_{k-1} in G, allora $H_\ell = G$.*

DIMOSTRAZIONE. $H_0 \supseteq Z_0 = \{e\}$ banalmente. Proviamo ora per induzione che $H_m \supseteq Z_m$ per ogni m. Assumiamo vera l'ipotesi del passo induttivo che $H_i \supseteq Z_i$. Allora, dalla definizione di Z_{i+1}, presi $z_{i+1} \in Z_{i+1}$ e $g \in G$, $z_{i+1}^{-1} g^{-1} z_{i+1} g = z_i \in Z_i$, quindi se $g^{-1} = h_i \in H_i$, abbiamo che $z_{i+1}^{-1} h_i z_{i+1} = z_i h_i \in H_i$, e così Z_{i+1} normalizza H_i, da cui $H_{i+1} \supseteq Z_{i+1}$. Pertanto è provato l'asserto per induzione. Da $Z_\ell = G$, ricaviamo infine $H_\ell = G$. □

Corollario E5.5. *Ogni sottogruppo proprio di un gruppo nilpotente è un sottogruppo proprio del suo normalizzante.*

Altrimenti avremmo $H = H_0 = H_1 = H_2 = \cdots = H_\ell$ con $H_k \subset G$.

Corollario E5.6. *Ogni sottogruppo massimale di un gruppo nilpotente è normale di indice primo e contiene il gruppo derivato.*

Infatti, sia M un sottogruppo massimale del gruppo nilpotente G. $N_G(M)$ contiene propriamente M, perciò abbiamo necessariamente che $N_G(M) = G$, oppure $M \lhd G$. Allora, per la massimalità di M, G/M non contiene sottogruppi propri, quindi deve essere un gruppo ciclico di ordine primo. Così M è di indice primo e G/M è abeliano, perciò M contiene il gruppo derivato G' grazie al Teorema **E2.1**.

Corollario E5.7. *Se G è nilpotente e H è un sottogruppo tale che $G = HG'$, allora $H = G$.*

In questa situazione, infatti, se per assurdo $H \neq G$, allora, per il teorema precedente, esiste una serie

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_{\ell-1} \lhd H_\ell = G \quad \text{con} \quad Z_k(G) \subseteq H_k.$$

Per la definizione di serie centrale superiore, si ha che $G/H_{\ell-1}$ è abeliano; quindi $H_{\ell-1} \supseteq G'$ per il Teorema **E2.1**. Ma allora $HG' \subseteq H_{\ell-1}G' = H_{\ell-1} \neq G$, contrariamente alla nostra ipotesi. Quindi dobbiamo avere $H = G$. Notiamo che non abbiamo supposto che G possedesse sottogruppi massimali.

Torniamo ora a parlare di sottogruppi di Sylow con il prossimo teorema che ci fornisce una caratterizzazione dei gruppi nilpotenti finiti:

Teorema E5.8. *Tutti i p-gruppi finiti sono nilpotenti. Un gruppo finito è nilpotente se e solo se è prodotto diretto dei suoi sottogruppi di Sylow.*

DIMOSTRAZIONE. Ogni p-gruppo finito P ha il centro non banale (differente dall'identità). Quindi la serie centrale superiore per P termina con l'intero gruppo, quindi P è nilpotente. Lo stesso vale per il prodotto diretto di p-gruppi finiti. Supponiamo ora che G sia un gruppo finito nilpotente e sia P un p-sottogruppo di Sylow di G. Allora $N_G(P)$ è il suo stesso normalizzante (vedi il Lemma **D4.1**) e, per il Corollario **E5.5**, $N_G(P)$ non può essere un sottogruppo proprio di G. Quindi $P \lhd G$. Essendo ogni sottogruppo di Sylow di G normale, G risulterà essere prodotto diretto dei suoi sottogruppi di Sylow. Questo è giustificato dal Teorema **D5.1**. □

Corollario E5.9 (Wielandt). *Un gruppo finito è nilpotente se e solo se i suoi sottogruppi massimali sono normali.*

DIMOSTRAZIONE. La condizione necessaria segue immediatamente dal Corollario **E5.6** che afferma che i sottogruppi massimali di un gruppo nilpotente sono normali. Per dimostrare che la condizione è sufficiente, consideriamo

un qualunque p-sottogruppo di Sylow P di G. Vogliamo dimostrare che P è normale in G, cioè il suo normalizzante $N_G(P)$ coincide con G. Se così non fosse, essendo $N_G(P)$ un sottogruppo proprio di G, esisterebbe in G un sottogruppo massimale M contenente $N_G(P)$ come sottogruppo. Dato che M è normale in G, allora $N_G(M) = G$. D'altra parte, risulta $M = N_G(M) < G$ per il Lemma **D4.1**. Questa è una contraddizione. Pertanto $N_G(P) = G$ e P è normale in G. Secondo il Teorema **D5.1**, G è prodotto diretto dei sottogruppi di Sylow e quindi nilpotente. □

E6. Sottogruppo di Frattini

Tratteremo in questo paragrafo di un particolare sottogruppo di un gruppo G, il sottogruppo di *Frattini* che, nel caso di gruppi finiti, risulterà essere nilpotente e che, sotto altre condizioni che vedremo in seguito, ci garantirà la nilpotenza dello stesso gruppo G.

Per ora diamo una definizione del sottogruppo di Frattini:

Definizione E6.1. *Sia G un gruppo. Definiamo il sottogruppo di Frattini F di G nel seguente modo: $F = G \bigcap_M M$, dove M varia sui sottogruppi massimali di G se G ha sottogruppi massimali. Mentre $F = G$ se e solo se G non ha sottogruppi massimali.*

Molto interessante è la relazione del sottogruppo di Frattini F con i generatori di G, infatti F contiene gli elementi di G che non generano G. Formalizziamo meglio questo concetto:

Definizione E6.2. *Un elemento x di un gruppo G è detto un non-generatore di G se, per ogni sottoinsieme T di G tale che $G = \langle T, x\rangle$, risulta $G = \langle T\rangle$.*

Notiamo che se $G \neq \{e\}$, sicuramente e è un non-generatore.

Teorema E6.3. *Se un gruppo G è diverso dall'elemento neutro, allora il suo sottogruppo di Frattini F è l'insieme dei non-generatori di G.*

DIMOSTRAZIONE. Sia x un elemento di G. Se c'è un sottogruppo massimale M che non contiene x, allora il gruppo $\langle M, x\rangle$ contiene propriamente M, ed essendo M massimale, deve risultare che $\langle M, x\rangle = G$. Ma qui $\langle M\rangle = M \neq G$. Così x è un generatore essenziale in $\langle M, x\rangle = G$. Allora i non-generatori di G appartengono ai sottogruppi massimali e così ogni non-generatore è un elemento di $F = G \bigcap_M M$. Viceversa, dobbiamo provare che se $y \in F$, allora y è un non-generatore di G. Per ipotesi $G \neq \{e\}$, quindi "e" è

sicuramente un non-generatore. Ora supponiamo che $G = \langle T, y\rangle$ per un certo sottoinsieme T di G. Proviamo che se $\langle T\rangle = H \neq G$, arriviamo ad un assurdo. Osserviamo intanto che y non può appartenere a H se $H \neq G$. Infatti, se così fosse, avremmo $H = \langle H, y\rangle \supseteq \langle T, y\rangle = G$, contrariamente alla nostra ipotesi. Quindi $y \notin H$. Allora, per il Lemma di Zorn, c'è un sottogruppo $K \supseteq H$ massimale e tale che $y \notin K$. Ora $\langle K, y\rangle \supseteq \langle T, y\rangle = G$, quindi $\langle K, y\rangle = G$. Ma, per come abbiamo scelto K, qualunque gruppo che contenga propriamente K deve contenere y. Quindi $K = M$ è un sottogruppo massimale che non contiene y, in contrasto con il fatto che $y \in F = G \underset{M}{\cap} M$. Quindi dobbiamo avere $\langle T\rangle = G$ e così ogni $y \in F$ risulta essere un non-generatore di G. □

OSSERVAZIONE: Nella dimostrazione abbiamo citato il Lemma di **Zorn**, il cui enunciato è il seguente: "Sia S un insieme parzialmente ordinato. Supponiamo che ogni sottoinsieme ordinato di S abbia estremo superiore in S. Allora S ha massimo".

Teorema E6.4. *Il sottogruppo di Frattini di un gruppo finito è nilpotente.*

DIMOSTRAZIONE. Sia G un gruppo finito e F il suo sottogruppo di Frattini che, come sottogruppo caratteristico di G, è un sottogruppo normale. Sia P un p-sottogruppo di Sylow di F. Dunque ogni coniugato di P in G sta in F e così è coniugato a P in F. Quindi P ha tanti coniugati in F quanti in G e così $[G : N_G(P)] = [F : N_F(P)]$. Ma

$$[G : N_F(P)] = [G : F][F : N_F(P)] = [G : N_G(P)][N_G(P) : N_F(P)]$$

quindi $[G : F] = [N_G(P) : N_F(P)]$. Notando che $N_F(P) = F \cap N_G(P)$ ed applicando la equazione dell'Esempio **C2.7**, troviamo che

$$[G : F] = [N_G(P) : F \cap N_G(P)] = [F \circ N_G(P) : F].$$

Da questo concludiamo che $F \circ N_G(P) = G$. Poiché $G = \langle F, N_G(P)\rangle$, abbiamo anche che, togliendo uno alla volta gli elementi di F, essendo F finito, $G = \langle N_G(P)\rangle = N_G(P)$. Così $P \lhd G$ e chiaramente $P \lhd F$. Poiché ogni sottogruppo di Sylow di F è normale, F deve essere prodotto diretto dei suoi sottogruppi di Sylow e quindi è un gruppo nilpotente. □

Teorema E6.5. *Il sottogruppo di Frattini di un gruppo nilpotente contiene il gruppo derivato.*

DIMOSTRAZIONE. Dal Corollario **E5.7** se G è nilpotente e $G = HG'$, allora $G = H$. Questo significa che G' può essere omesso da un qualunque insieme di generatori di G; segue quindi che $F \supseteq G'$. Inoltre, si nota che il viceversa vale per i gruppi finiti. □

Teorema E6.6 (Wielandt). *Se il sottogruppo di Frattini di un gruppo finito G contiene il gruppo derivato G', allora G è nilpotente.*

DIMOSTRAZIONE. Sia P un sottogruppo di Sylow di G. Se $N_G(P) = H \neq G$, allora H è contenuto in un sottogruppo massimale M di G. Ricordiamo che $F \supseteq G'$ per ipotesi e $M \supseteq F$ perché F è contenuto in ogni sottogruppo massimale di G. Poiché G/G' è abeliano, M è un sottogruppo normale di G (vedi il Teorema **E2.1**). D'altra parte, essendo $M \supseteq N_G(P)$, M è il suo stesso normalizzante grazie al Lemma **D4.1**. Questo è assurdo e possiamo concludere che dobbiamo avere $N_G(P) = G$. Essendo i sottogruppi di Sylow di G normali, possiamo dedurre che G è il loro prodotto diretto e quindi è nilpotente. □