Lezione 3

Prerequisiti: Lezioni 1, 2. Classi di coniugio e centralizzanti.

Gruppi risolubili.

In questo capitolo introduciamo una nozione che, come vedremo in seguito, funge da raccordo tra la teoria dei gruppi e la teoria dei campi.

Definizione 3.1 Dato un gruppo moltiplicativo G, si dice *gruppo dei commutatori* (o anche *gruppo derivato*) di G il seguente sottogruppo di G

$$G^{(1)} = G' = \left\langle xyx^{-1}y^{-1} \middle| x, y \in G \right\rangle.$$

Ricorsivamente, si definisce, per ogni intero $n > 1$, l'*n-esimo gruppo derivato* di G :

$$G^{(n)} = \left(G^{(n-1)}\right)'.$$

Per convenzione si pone anche $G^{(0)} = G$.

Nota L'elemento $xyx^{-1}y^{-1}$ si dice *commutatore*. Lo si denota anche con $[x, y]$.

Osservazione 3.2

a) Si ha che $G' = \{1_G\}$ se e solo se G è abeliano.

b) Se H è un sottogruppo di G, allora, per ogni $n \geq 1$, $H^{(n)}$ è un sottogruppo di $G^{(n)}$. Ciò si deduce dall'Osservazione 1.8, per induzione.

Definizione 3.3 Il gruppo G si dice *risolubile* se e solo se, per qualche intero $n \geq 0$, $G^{(n)}$ è il gruppo banale.

Dall'Osservazione 3.2 b) segue immediatamente

Proposizione 3.4 Ogni sottogruppo di un gruppo risolubile è risolubile.

Proposizione 3.5 G' è un sottogruppo normale di G.

Dimostrazione: Siano $g, x, y \in G$. Allora

$$gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in G'.$$

In virtù della Proposizione 1.7, ciò basta per concludere. □

Proposizione 3.6 Sia H un sottogruppo normale di G. Allora il gruppo quoziente G/H è abeliano se e solo se $G' \subset H$.

Dimostrazione: Supponiamo che G/H sia abeliano. Allora, per ogni $x, y \in G$,

$$\text{si ha che } Hxy = HxHy = HyHx = Hyx, \text{ da cui } xyx^{-1}y^{-1} \in H.$$

Segue che $G' \subset H$.
Viceversa, supponiamo che $G' \subset H$. Siano $x, y \in G$. Allora

$$HxHy = Hxy = H(yxy^{-1}x^{-1})xy = Hyx(y^{-1}x^{-1}xy) = Hyx = HyHx.$$

Segue che G/H è abeliano. □

Osservazione 3.7 In altri termini, il gruppo derivato è il più piccolo sottogruppo normale tale che il corrispondente gruppo quoziente è abeliano. Quindi, ad esempio, $S_3' = A_3$.

Dalla Definizione 3.1 e dalla Proposizione 3.6 concludiamo che la nozione di gruppo derivato fornisce una successione

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(i)} \rhd \cdots$$

in cui ogni gruppo è sottogruppo normale del precedente (*serie normale*), ed, inoltre, il quoziente di due gruppi consecutivi è un gruppo abeliano. Questa successione, a volte, termina con il sottogruppo banale.

Proposizione 3.8 Un gruppo moltiplicativo G è risolubile se e solo se esiste una successione

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_{n-1} \rhd H_n = \{1_G\},$$

tale che, per ogni indice $i = 0,...,n-1$, il gruppo quoziente H_i/H_{i+1} è abeliano.

Dimostrazione: Una delle due implicazioni è nota. Per provare l'altra, supponiamo che esista una successione del tipo indicato. Essendo per ipotesi G/H_1 abeliano, in virtù della Proposizione 3.6, $G^{(1)} \subset H_1$. Dato un indice $i \in \{0,...,n-1\}$, se $G^{(i)} \subset H_i$, allora, per l'Osservazione 3.2 b), $G^{(i+1)} \subset H_i'$. Essendo H_i/H_{i+1} abeliano, segue che $H_i' \subset H_{i+1}$. Dunque $G^{(i+1)} \subset H_{i+1}$. Per induzione finita si conclude così che

$$G^{(n)} \subset H_n, \text{ da cui } G^{(n)} = \{1_G\}.$$

Ciò prova che G è risolubile. □

Proposizione 3.9 Sia H un sottogruppo normale di G. Allora G è risolubile se e solo se lo sono H e G/H. In particolare, ogni sottogruppo (normale) ed ogni gruppo quoziente di un gruppo risolubile sono risolubili.

Dimostrazione: Sia G risolubile, con $G^{(n)} = \{1_G\}$. Allora H è risolubile in virtù della Proposizione 3.4 (lo è ogni sottogruppo di G). Sia, per ogni $i \geq 0$,

$$K_i = G^{(i)}H/H,$$

in particolare $K_0 = G/H$.

Si può provare che $G^{(i)}H \lhd G^{(i-1)}H$, quindi, per il Teorema di corrispondenza per i gruppi (vedi Algebra 2, Teorema 9.2), segue che

$$K_i = G^{(i)}H/H \lhd G^{(i-1)}H/H = K_{i-1},$$

ove $K_n = \{H\}$. Infine, in virtù del Teorema 2.2,

$$K_{i-1}/K_i \cong G^{(i-1)}H/G^{(i)}H,$$

ove, in virtù del Teorema 2.4,

$$G^{(i-1)}H/G^{(i)}H = G^{(i-1)}G^{(i)}H/G^{(i)}H \cong G^{(i-1)}/G^{(i)}H \cap G^{(i-1)}.$$

Essendo $G^{(i)}H \cap G^{(i-1)} \supset G^{(i)} = G^{(i-1)}$', dalla Proposizione 3.6 segue che $K_{i-1}/K_i \cong G^{(i-1)}/G^{(i)}H \cap G^{(i-1)}$ è abeliano. Con ciò, in virtù della Proposizione 3.8, è provato che G/H è risolubile.
Viceversa, supponiamo che H e G/H siano risolubili. Esistono allora due successioni

$$G/H = K_0/H \rhd K_1/H \rhd K_2/H \rhd \cdots \rhd K_{n-1}/H \rhd K_n/H = H/H = \{H\}.$$

$$H \rhd H_{n+1} \rhd H_{n+2} \rhd \cdots \rhd H_{m-1} \rhd H_m = \{1_G\}.$$

in cui i quozienti di due gruppi consecutivi sono abeliani. Se ne ricava una successione

$$G = K_0 \rhd K_1 \rhd K_2 \rhd \cdots \rhd K_{n-1} \rhd K_n = H \rhd H_{n+1} \rhd H_{n+2} \rhd \cdots \rhd H_{m-1} \rhd H_m = \{1_G\}.$$

ove, per il Teorema 2.2, $K_i/K_{i+1} \cong \dfrac{K_i/H}{K_{i+1}/H}$ è abeliano. Dalla Proposizione 3.8 si deduce che G è risolubile. □

Osservazione 3.10 In base alla Definizione 3.3 ed all'Osservazione 3.2, ogni gruppo abeliano è risolubile. In generale, però, il calcolo dei gruppi derivati appare poco agevole, e difficile è quindi determinare se un dato gruppo è risolubile. Le Proposizioni 3.8 e 3.9 possono, però, facilitarci il compito. Ciò risulterà subito evidente dallo studio della risolubilità dei gruppi simmetrici, che ci apprestiamo ad effettuare.

Proposizione 3.11 Per ogni $n \geq 3$, $S_n' = A_n$.

Dimostrazione: Poiché S_n/A_n ha ordine 2, è un gruppo abeliano. Quindi, in virtù della Proposizione 3.6, $S_n' \subset A_n$. Per dimostrare l'inclusione contraria, in virtù dell' Esercizio 1.6 b), basta provare che ogni 3-ciclo di S_n è un commutatore. In effetti, per ogni terna di indici i, j, k distinti si ha:

$$(ijk) = (ij)(ik)(ij)(ik). \square$$

Corollario 3.12 I gruppi S_3 e S_4 sono risolubili.

Dimostrazione: Si hanno le serie normali:

$$S_3 \rhd A_3 \rhd \{\mathrm{id}\}$$

$$S_4 \rhd A_4 \rhd V \rhd \{\mathrm{id}\},$$

dove V indica il gruppo di Klein: $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. I quozienti dei gruppi consecutivi sono tutti abeliani, perché sono di ordine 2, 3 oppure 4. □

La situazione cambia radicalmente per i gruppi simmetrici di ordine superiore. Lo dimostriamo in vari passi.

Lemma 3.13 I 3-cicli di S_5 sono a due a due coniugati in A_5.

Dimostrazione: Sia $\alpha = (123)$. Detto $C_{S_5}(\alpha)$ il centralizzante di α in S_5, e detta $\mathrm{Co}_{S_5}(\alpha)$ la sua classe di coniugio in S_5 si ha, in base a quanto visto in Algebra 2, Lezione 7, e in virtù del Teorema di Lagrange (vedi Algebra 2, Teorema 4.2),

$$20 = \left|\mathrm{Co}_{S_5}(\alpha)\right| = \left|S_5 : C_{S_5}(\alpha)\right| = \frac{120}{\left|C_{S_5}(\alpha)\right|}, \text{ da cui } \left|C_{S_5}(\alpha)\right| = 6.$$

D'altra parte, i seguenti elementi commutano con α:

$$\mathrm{id},\ (123),\ (45),\ (132),\ (123)(45),\ (132)(45).$$

Quindi questi sono tutti e soli gli elementi di $C_{S_5}(\alpha)$. L'insieme $C_{A_5}(\alpha)$ si ricava prelevando da questi elementi le permutazioni pari:

$$C_{A_5}(\alpha) = \{\mathrm{id},\ (123),\ \ (132)\}.$$

Segue che

$$\left|\mathrm{Co}_{A_5}(\alpha)\right| = \frac{|A_5|}{\left|C_{A_5}(\alpha)\right|} = \frac{60}{3} = 20.$$

Quindi $\mathrm{Co}_{A_5}(\alpha) = \mathrm{Co}_{S_5}(\alpha)$, come volevasi. □

**Teorema 3.14 (Galois-Jordan) Per ogni $n \geq 5$ il gruppo A_n non ha sottogruppi normali propri non banali.

Dimostrazione: Proviamo l'enunciato solo per $n = 5$. Sia H un sottogruppo normale non banale di A_5. Proviamo che ad H appartiene un 3-ciclo. In virtù del Lemma 3.13 e dall'Esercizio 1.6 b), da ciò seguirà che $H=A_5$. Sia $\alpha \in H$, $\alpha \neq \mathrm{id}$, e non sia α un 3-ciclo. Allora le strutture cicliche possibili per α sono (2,2) e (5). Supponiamo, per fissare le idee, che $\alpha = (12)(34)$. Allora, se $\beta = (12)(35)$, ad H appartiene

$$\beta\alpha\beta^{-1}\alpha = (12)(45)(12)(34) = (354).$$

Se invece $\alpha = (12345)$, allora, posto $\beta = (254)$, ad H appartiene

$$\beta\alpha\beta^{-1}\alpha = (143).$$

Ciò conclude la dimostrazione per il caso $n = 5$. La dimostrazione completa si trova, ad esempio, in [G], Proposition 7.7 (seconda edizione, prima edizione: 3.5.8). □

Corollario 3.15 Per ogni $n \geq 5$, A_n è il solo sottogruppo normale proprio non banale di S_n.

Dimostrazione: Sia H un sottogruppo normale proprio non banale di S_n. Allora $H \cap A_n$ è un sottogruppo normale di A_n. Quindi, in virtù del Teorema 3.14, $H \cap A_n = \{\mathrm{id}\}$ oppure $H \cap A_n = A_n$. Nel secondo caso $A_n \subset H$, e quindi $H = A_n$, da cui la tesi. Dimostriamo che il primo caso è da escludere.

Supponiamo per assurdo che sia $H \cap A_n = \{\mathrm{id}\}$. Allora H non è contenuto in A_n, quindi $HA_n = S_n$. Per il Teorema 2.4, si avrebbe

$$S_n / A_n = A_n H / A_n \cong H,$$

da cui $|H| = 2$. Sia $H = \{\mathrm{id}, \sigma\}$. Allora la classe di coniugio di σ in S_n sarebbe $\{\sigma\}$, ma ciò è impossibile, essendo $\sigma \neq \mathrm{id}$. □

Nota Un gruppo privo di sottogruppi normali propri non banali si dice *semplice.* La classificazione di tutti i gruppi semplici finiti (tra cui si trovano, come abbiamo visto, i gruppi alterni di ordine maggiore di 5) è stata a lungo un problema irrisolto. L'arduo compito è stato completato nell'arco di un trentennio (dagli anni cinquanta agli anni ottanta), ed è attualmente in fase di revisione.

Corollario 3.16 Il gruppo S_n è risolubile se e solo se $n \leq 4$.

Dimostrazione: I gruppi S_1 e S_2 sono abeliani, quindi risolubili, i gruppi S_3 e S_4 sono risolubili in base al Corollario 3.12. Per ogni $n \geq 5$, il gruppo S_n ha un sottogruppo isomorfo a S_5. Dalla Proposizione 3.11 e dal Teorema 3.14 si deduce facilmente che S_5 non è risolubile: infatti $S_5^{(2)} = A_5' = A_5$, e quindi $S_5^{(k)} = A_5$ per ogni $k \geq 2$. In virtù della Proposizione 3.4, segue che S_n non è risolubile se $n \geq 5$. □

Esercizio 3.17* Dire se il gruppo D_4 è risolubile.

A volte la risolubilità di un gruppo è determinata dal suo ordine.

Teorema 3.18 Sia p un numero primo. Un gruppo di ordine p^n è risolubile.

Dimostrazione: Sia G un gruppo di ordine p^n. Procediamo per induzione su n. Se $n \in \{0,1\}$, allora G è abeliano, e quindi risolubile. Sia allora $n>1$. In virtù del Lemma 8.8 di Algebra 2, $Z(G)$ è non banale. Se G è abeliano, allora G è risolubile. Altrimenti $Z(G) \neq G$. Allora $Z(G)$ e $G/Z(G)$ sono gruppi di ordini del tipo p^m, con $m<n$. Per l'ipotesi induttiva, essi sono dunque risolubili. La tesi segue pertanto dalla Proposizione 3.9. □

A questo criterio se ne aggiungono altri due, che diamo di seguito senza dimostrazione.

Proposizione 3.19 Un gruppo il cui ordine è prodotto di fattori primi distinti è risolubile.

****Teorema 3.20** (*Burnside*) Siano p, q numeri primi. Un gruppo di ordine $p^h q^k$ è risolubile.

Dimostrazione: [I], Theorem 28.24.

Concludiamo con un famoso e difficile risultato:

Teorema 3.21 (*Feit-Thompson*) Un gruppo di ordine dispari è risolubile.